



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ | ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΜΣ «ΨΗΦΙΑΚΕΣ ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑ»

Διπλωματική Εργασία

**«Ανάλυση της χρήσης λογισμικού και plugin
ασφάλειας στο WordPress»**

ΡΑΜΠΑΒΙΛΑ ΑΡΤΕΜΙΣ

(ΠΚΜ 202026)

Επιβλέπων Καθηγητής: Χριστόφορος Νταντογιάν

ΚΕΡΚΥΡΑ, ΜΑΡΤΙΟΣ 2022



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ | ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΜΣ «ΨΗΦΙΑΚΕΣ ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑ»

Διπλωματική Εργασία

«Ανάλυση της χρήσης λογισμικού και plugin ασφάλειας στο WordPress»

ΡΑΜΠΑΒΙΛΑ ΑΡΤΕΜΙΣ
(ΠΚΜ 202026)

Τριμελής Επιτροπή

Χριστόφορος Νταντογιάν
Επίκουρος Καθηγητής
Τμήμα Πληροφορικής
Ιόνιο Πανεπιστήμιο

Αγγελική Τσώχου
Επίκουρη Καθηγήτρια
Τμήμα Πληροφορικής
Ιόνιο Πανεπιστήμιο

Ελένη Χριστοπούλου
ΕΔΙΠ
Τμήμα Πληροφορικής
Ιόνιο Πανεπιστήμιο

ΚΕΡΚΥΡΑ, ΜΑΡΤΙΟΣ 2022

Περιεχόμενα

ΠΕΡΙΛΗΨΗ.....	5
ABSTRACT.....	6
1. ΕΙΣΑΓΩΓΗ.....	7
1.1 Σκοπός Εργασίας.....	7
1.2 Μεθοδολογία Εργασίας	7
1.3 Διάρθρωση Εργασίας.....	7
2. ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ.....	9
2.1 Κρίσιμες ευπάθειες (Security risk, 2021 OWASP Top 10)	9
2.1.1 A01:2021-Broken Access Control	10
2.1.2 A02:2021-Cryptographic Failures.....	11
2.1.3 A03:2021-Injection.....	12
2.1.4 A04:2021-Insecure Design.....	12
2.1.5 A05:2021-Security Misconfiguration (Λανθασμένη διαμόρφωση ασφάλειας)....	13
2.1.6 A06:2021-Vulnerable and Outdated Components	13
2.1.7 A07:2021-Identification and Authentication Failures	14
2.1.8 A08:2021-Software and Data Integrity Failures.....	15
2.1.9 A09:2021-Security Logging and Monitoring Failures	15
2.1.10 A10:2021-Server-Side Request Forgery.....	16
2.2 Είδη επιθέσεων.....	17
2.2.1 Brute force attacks	17
2.2.2 Denial of service (DoS Attack).....	17
2.2.3 Distributed denial of service (DDoS attack).....	17
2.2.4 Cross-site Scripting (XSS)	17
2.2.5 SQL Injection Attacks	18
2.2.6 Backdoor Hack.....	18
3. ΠΛΑΤΦΟΡΜΑ WORDPRESS ΚΑΙ ΕΝΙΣΧΥΣΗ ΑΣΦΑΛΕΙΑΣ	19
3.1 Επιλογή ασφαλούς και αξιόπιστου Web Hosting.....	20
3.2 Ενημερωμένο WordPress	22
3.3 Αντίγραφα ασφάλειας (Backups)	23
3.4 Χρήση πιστοποιητικού SSL.....	24
3.5 Web Application Firewall (WAF)	24
3.6 Ασφάλεια σύνδεσης χρήστη (Login Page Security).....	24
3.6.1 Ισχυροί Κωδικοί πρόσβασης.....	24

3.6.2 Αλλαγή ή διαγραφή του προκαθορισμένου ονόματος χρήστη “admin”	25
3.6.3 Έλεγχος ταυτότητας δύο παραγόντων (Two-Factor Authentication).....	25
3.6.4 Ερώτηση ασφάλειας κατά την σύνδεση.....	25
3.6.5 Περιορισμός προσπαθειών σύνδεσης.....	25
3.6.6 Αυτόματη αποσύνδεση ανενεργών χρηστών.....	26
3.6.7 Αλλαγή του URL εισόδου στην διαχείριση.....	26
3.7 Ασφάλεια αρχείων	26
3.7.1 Απενεργοποίηση επεξεργασίας αρχείων	26
3.7.2 Απενεργοποίηση εκτέλεσης της PHP σε συγκεκριμένους φακέλους.....	26
3.7.3 Απενεργοποίηση εμφάνισης καταλόγου αρχείων (directory listing).....	27
3.7.4 Απόκρυψη αρχείων wp-config και .htaccess.....	27
3.8 Αλλαγή του προθέματος wp_ της βάσης δεδομένων.....	27
3.9 Απενεργοποίηση XML-RPC στο WordPress.....	28
3.10 Αρχεία καταγραφής συμβάντων (Logging).....	28
3.11 Απόκρυψη της έκδοσης του WordPress	28
3.12 Έλεγχος και παρακολούθηση της ιστοσελίδας (Monitoring).....	29
3.13 Σάρωση για κακόβουλο λογισμικό και ευπάθειες.....	29
3.14 Εγκατάσταση plugin ασφάλειας (Security Plugin)	29
4. ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ.....	31
4.1 Ερευνητικά ερωτήματα.....	31
4.2 Σχεδιασμός ερωτηματολογίου	31
4.3 Δείγμα έρευνας	32
4.4 Ερωτηματολόγιο	32
5. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ.....	40
6. ΣΥΜΠΕΡΑΣΜΑΤΑ.....	63
7. ΑΝΑΦΟΡΕΣ.....	65

ΠΕΡΙΛΗΨΗ

Τα τελευταία χρόνια οι απαιτήσεις για χρήση διαδικτυακών εφαρμογών και υπηρεσιών έχουν αυξηθεί ραγδαία. Με την επανάσταση του διαδικτύου άνοιξε ένας νέος δρόμος στην επικοινωνία, τις αγορές, τις συναλλαγές, την αναζήτηση πληροφορίας, την καταχώρηση δεδομένων κ.α. Το διαδίκτυο αποτελεί πλέον τμήμα της καθημερινής ζωής των ανθρώπων με τους χρήστες του να αυξάνονται διαρκώς. Οι διαδικτυακές εφαρμογές αναπτύσσονται διαρκώς και εμπλουτίζουν το περιεχόμενο και την λειτουργικότητά τους για να μπορέσουν να ανταπεξέλθουν στις απαιτήσεις των χρηστών. Ταυτόχρονα αυξάνεται ο όγκος της διακινούμενης πληροφορίας στο διαδίκτυο και η επεξεργασία ιδιωτικών δεδομένων που μπορεί να είναι ευαίσθητα.

Όπως στον φυσικό κόσμο έτσι και στο διαδίκτυο υπάρχουν κακόβουλοι χρήστες που θέλουν να εκμεταλλευτούν ευαίσθητες πληροφορίες και όχι μόνο, προς όφελός τους. Για το λόγο αυτό προσπαθούν να βρουν τρόπο να εισβάλουν στις διαδικτυακές εφαρμογές, όπως είναι οι ιστοσελίδες, και να κλέψουν δεδομένα ή να δημιουργήσουν πρόβλημα στο σύστημα. Οι προγραμματιστές και οι διαχειριστές των ιστοσελίδων θα πρέπει να λαμβάνουν μέτρα για την ασφάλεια των συστημάτων αλλά και των χρηστών. Ο τρόπος για να γίνει αυτό είναι η μείωση των ευπαθειών που παρουσιάζει ένα σύστημα έτσι ώστε ο επιτιθέμενος να μην μπορεί να βρει τρόπο να εισέλθει σε αυτό. Στην παρούσα εργασία παρουσιάζονται οι πιο σημαντικές ευπάθειες διαδικτυακών εφαρμογών για το 2021 σύμφωνα με τον οργανισμό OWASP και οι πιο κοινοί τύποι επιθέσεων στις εφαρμογές αυτές.

Ένα από τα πιο δημοφιλή εργαλεία για την δημιουργία ιστοσελίδων αποτελεί το WordPress. Είναι δωρεάν και εύκολο στην χρήση με αποτέλεσμα κάποιος που δεν έχει εξειδικευμένες γνώσεις στον προγραμματισμό να μπορεί να δημιουργήσει μια ιστοσελίδα. Παρότι είναι ένα από τα πιο ασφαλή λογισμικά διαχείρισης περιεχομένου, λόγω της μεγάλης ομάδας προγραμματιστών ασφάλειας που το υποστηρίζει, η λάθος διαχείρισή του μπορεί να επιφέρει πολλά προβλήματα ασφάλειας. Υπάρχει ένας μεγάλος αριθμός από πρακτικές ασφάλειας που θα πρέπει να υιοθετούν οι διαχειριστές των ιστοσελίδων, όπως η δημιουργία ισχυρών κωδικών πρόσβασης, η ασφάλεια των αρχείων και της βάσης δεδομένων, η σάρωση για κακόβουλο λογισμικό, η εγκατάσταση plugin ασφάλειας κ.α. Αντικείμενο έρευνας σε αυτή την εργασία αποτελεί η χρήση του λογισμικού και plugin ασφάλειας από τους προγραμματιστές, διαχειριστές των ιστοσελίδων.

Λέξεις κλειδιά: Ιστοσελίδες, WordPress, Ευπάθειες, Επιθέσεις, Ασφάλεια, Plugin.

ABSTRACT

In recent years the demands for the use of web applications and services have increased rapidly. With the internet revolution, a new way was opened in communication, shopping, transactions, information search, data entry, etc. The internet is now a part of people's daily lives with its users constantly increasing. Web applications are constantly evolving and enriching their content and functionality to meet the demands of users. At the same time, the volume of information circulating on the internet and the processing of private data that may be sensitive is increasing.

As in the natural world, so on the internet there are malicious users who want to exploit sensitive information and not only, to their advantage. This is why they are trying to find a way to invade web applications, such as websites, and steal data or cause problems in the system. Website developers and administrators should take steps to ensure the security of both systems and users. The way to do this is to reduce the vulnerabilities of a system so that the attacker cannot find a way to enter it. This paper presents the most important vulnerabilities of web applications for 2021 according to OWASP and the most common types of attacks on these applications.

One of the most popular web design tool is WordPress. It is free and easy to use so that someone who does not have specialized knowledge in programming can create a website. Although it is one of the most secure content management system, due to the large group of security developers that support it, its mismanagement can cause many security problems. There are a number of security practices that administrators should adopt, such as creating strong passwords, securing files and databases, scanning for malware, installing security plugins, and more. The object of research in this paper is the use of software and security plugins by developers and administrators.

Keywords: Websites, WordPress, Vulnerabilities, Attacks, Security, Plugin.

1. ΕΙΣΑΓΩΓΗ

1.1 Σκοπός Εργασίας

Με την ανάπτυξη των Τεχνολογιών της Πληροφορίας και Επικοινωνίας (ΤΠΕ) υπάρχει ανάγκη για ανάπτυξη καινοτόμων διαδικτυακών εφαρμογών που θα παρέχουν λειτουργικότητα και ασφάλεια. Οι άνθρωποι χρησιμοποιούν το διαδίκτυο καθημερινά για να αναζητήσουν πληροφορίες, να πραγματοποιήσουν αγορές, να επικοινωνήσουν, να μοιραστούν δεδομένα, να καταχωρήσουν δεδομένα σε υπηρεσίες, να προωθήσουν την δουλειά τους και την επιχείρησή τους κ.α.

Αυτά τα δεδομένα μπορεί να γίνουν στόχος για κάποιους κακόβουλους χρήστες που προσπαθούν να αποκτήσουν πρόσβαση στις διαδικτυακές εφαρμογές για να τα υποκλέψουν ή να δημιουργήσουν προβλήματα στο σύστημα διαχείρισης τους. Γι' αυτό το λόγο θα πρέπει οι διαχειριστές των ιστοσελίδων να λαμβάνουν τα κατάλληλα μέτρα για αποφυγή των επιθέσεων στα συστήματά τους.

Σκοπός της εργασίας είναι να αναδείξει τις ευπάθειες των διαδικτυακών εφαρμογών που τις κάνουν ευάλωτες σε επιθέσεις αλλά και τα πιο κοινά είδη επιθέσεων. Επίσης στόχος είναι να αναδειχθούν οι καλές πρακτικές ασφάλειας που συμβάλουν στην μείωση του κινδύνου για επιθέσεις. Τέλος με την έρευνα που διεξήχθη σκοπός είναι να αναδειχθεί κατά πόσο οι προγραμματιστές και οι διαχειριστές των ιστοσελίδων χρησιμοποιούν καλές πρακτικές και plugin ασφάλειας για να προστατέψουν τις ιστοσελίδες τους από επιθέσεις.

1.2 Μεθοδολογία Εργασίας

Για την παρούσα εργασία αναζητήθηκαν πληροφορίες από ελληνική και αγγλική βιβλιογραφία αλλά και από το διαδίκτυο. Ως αποτέλεσμα της μελέτης των πληροφοριών αυτών προέκυψε μια βιβλιογραφική ανασκόπηση των σημαντικότερων σημείων που αφορούν τις ευπάθειες που παρουσιάζουν οι διαδικτυακές εφαρμογές, τις πιο κοινές επιθέσεις που καταγράφονται στα συστήματα αυτά, καθώς και τους τρόπους αντιμετώπισής τους. Για το πρακτικό μέρος της εργασίας έγινε διεξαγωγή έρευνας με χρήση ηλεκτρονικού ερωτηματολογίου, παρουσίαση των αποτελεσμάτων και διεξαγωγή συμπερασμάτων.

1.3 Διάρθρωση Εργασίας

Η παρούσα εργασία αποτελείται από έξι κεφάλαια. Στο κάθε ένα από αυτά παρουσιάζεται ένα συγκεκριμένο κομμάτι που αφορά στην ασφάλεια των διαδικτυακών εφαρμογών. Γίνεται παρουσίαση της έρευνας που διεξήχθη, σύνθεση των αποτελεσμάτων, εξαγωγή συμπερασμάτων και παρουσίαση των μελλοντικών δυνατοτήτων της έρευνας.

Πιο αναλυτικά στο δεύτερο κεφάλαιο γίνεται μια αναφορά στις απειλές ασφάλειας που έχουν να κάνουν με την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Η ευπάθεια ενός συστήματος μπορεί να αποτελεί απειλή για την

ασφάλειά του, επομένως σε αυτό το κεφάλαιο θα αναλύσουμε τις 10 πιο σημαντικές ευπάθειες των διαδικτυακών εφαρμογών σύμφωνα με τον οργανισμό OWASP. Επίσης θα γίνει αναφορά στα πιο κοινά είδη επιθέσεων στις εφαρμογές αυτές.

Στο τρίτο κεφάλαιο, αρχικά, γίνεται αναφορά στην πλατφόρμα WordPress και σε κάποια στατιστικά στοιχεία σχετικά με την χρήση της και στην συνέχεια αναφέρονται οι καλές πρακτικές ασφάλειας που θα πρέπει να χρησιμοποιούν οι προγραμματιστές και διαχειριστές των ιστοσελίδων WordPress προκειμένου να διατηρήσουν τον ιστότοπό τους ασφαλή.

Στο τέταρτο κεφάλαιο παρατίθεται η μεθοδολογία της έρευνας, τα ερευνητικά ερωτήματα και η σύνθεση του ερωτηματολογίου.

Στο πέμπτο κεφάλαιο παρουσιάζονται τα αποτελέσματα της έρευνας και στο έκτο κεφάλαιο κλείνει η παρούσα εργασία με τα συμπεράσματα.

2. ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ

Στις περισσότερες περιπτώσεις, όταν αναφερόμαστε σε ζητήματα ασφάλειας που συνδέονται με τις τεχνολογίες πληροφορικής και επικοινωνιών, χρησιμοποιούμε τον όρο ασφάλεια πληροφοριών (information security). Η ασφάλεια πληροφοριών παραδοσιακά αναφέρεται στην προστασία ορισμένων ιδιοτήτων (properties) της πληροφορίας, με κυριότερες την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability). Σύμφωνα με το πρότυπο ISO/IEC 27000 (2014) του Διεθνούς Οργανισμού Τυποποίησης (International Organization for Standardization – ISO), οι παραπάνω έννοιες ορίζονται ως εξής:

- **Εμπιστευτικότητα:** Η ιδιότητα της πληροφορίας να μη διατίθεται και να μην αποκαλύπτεται σε μη εξουσιοδοτημένα άτομα, οντότητες, ή διεργασίες.
- **Ακεραιότητα:** Η ιδιότητα της πληροφορίας να είναι ακριβής και πλήρης.
- **Διαθεσιμότητα:** Η ιδιότητα της πληροφορίας να είναι προσβάσιμη και κατάλληλη για χρήση, όταν την αιτείται μία εξουσιοδοτημένη οντότητα. [2]

Επίσης στην ορολογία της ασφάλειας της διακινούμενης πληροφορίας στο διαδίκτυο αναφέρονται συχνά οι παρακάτω όροι:

- **Αδυναμία ή Ευπάθεια (Vulnerability)** συστήματος, υπηρεσίας ή πρωτοκόλλου ορίζεται ένα ελάττωμα που υπάρχει στον σχεδιασμό ή την υλοποίηση το οποίο μπορεί να εκμεταλλευτεί κάποιος εισβολέας (intruder) για να παραβιάσει το σύστημα και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή πόρους αυτού.
- **Απειλή (threat)** είναι η οντότητα που μπορεί να προκαλέσει μη εξουσιοδοτημένη αποκάλυψη πληροφοριών, παραβίαση της ασφάλειας του συστήματος, ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος κ.α.
- **Επίθεση (attack)** είναι η εκμετάλλευση μιας αδυναμίας ή ευπάθειας από έναν εισβολέα για την πραγματοποίηση μιας απειλής. [1]

2.1 Κρίσιμες ευπάθειες (Security risk, 2021 OWASP Top 10)

Όπως στον πραγματικό κόσμο, έτσι και στο διαδίκτυο, τα θύματα επιλέγονται σύμφωνα με το πόσο εύκολοι στόχοι είναι. Ένας κακοποιός θα ψάξει και θα προσπαθήσει να βρει τον πιο εύαλωτο στόχο, αυτόν με τις μικρότερες αντιστάσεις. Έτσι ακριβώς συμβαίνει και στον κυβερνοχώρο, ο επιτιθέμενος σαρώνει και βρίσκει τον πιο αδύναμο στόχο. Οι επίδοξοι εισβολείς συχνά ανακαλύπτουν ευπάθειες στα συστήματα πολύ πιο γρήγορα από ότι οι προγραμματιστές και οι διαχειριστές ασφάλειας προκαλώντας παραβιάσεις και δυσλειτουργίες.

Στην παρούσα ενότητα, θα παρουσιαστούν και θα αναλυθούν οι δέκα κυριότερες ευπάθειες των διαδικτυακών εφαρμογών για το 2021 σύμφωνα με τον διεθνή οργανισμό OWASP. Το Open Web Application Security Project® (OWASP) είναι ένα μη κερδοσκοπικό ίδρυμα που εργάζεται για τη βελτίωση της ασφάλειας του λογισμικού. Μέσω έργων

λογισμικού ανοιχτού κώδικα υπό την καθοδήγηση της κοινότητας, δεκάδων χιλιάδων μελών και κορυφαίων εκπαιδευτικών και εκπαιδευτικών συνεδρίων, το Ίδρυμα OWASP είναι η πηγή για τους προγραμματιστές και τους τεχνολόγους για την ασφάλεια του ιστού.

Είναι μια ανοιχτή κοινότητα αφιερωμένη στο να δίνει τη δυνατότητα στους οργανισμούς να συλλάβουν, να αναπτύξουν, να αποκτήσουν, να λειτουργήσουν και να διατηρήσουν εφαρμογές που μπορούν να εμπιστευτούν. Όλα τα έργα, τα εργαλεία, τα έγγραφα, τα φόρουμ είναι δωρεάν και ανοιχτά σε όποιον ενδιαφέρεται να βελτιώσει την ασφάλεια των εφαρμογών. Το Ίδρυμα OWASP ξεκίνησε την 1η Δεκεμβρίου 2001 και ενσωματώθηκε ως μη κερδοσκοπικός φιλανθρωπικός οργανισμός των Ηνωμένων Πολιτειών στις 21 Απριλίου 2004.

Ένας πρωταρχικός στόχος του OWASP είναι να εκπαιδεύσει προγραμματιστές, σχεδιαστές, αρχιτέκτονες, διαχειριστές και οργανισμούς σχετικά με τις συνέπειες των πιο κοινών και πιο σημαντικών αδυναμιών ασφάλειας εφαρμογών Ιστού. Οι ευπάθειες λογισμικού μεταβάλλονται συνεχώς, γι' αυτό οι προγραμματιστές καλούνται να ενημερώνονται τακτικά για τις νέες επιθέσεις και τους τρόπους προφύλαξης από αυτές. Για τον λόγο αυτό ο οργανισμός έχει αναπτύξει το «OWASP Top 10» το οποίο παρέχει βασικές τεχνικές και οδηγίες για την προστασία από αυτές τις προβληματικές περιοχές υψηλού κινδύνου και το οποίο επικαιροποιείται συχνά για να ενημερώνονται οι προγραμματιστές ώστε να παράγουν όσο το δυνατόν πιο ασφαλείς εφαρμογές. Παρακάτω θα δούμε τις πιο σημαντικές ευπάθειες που έδωσε ο οργανισμός για το 2021. [3]

2.1.1 A01:2021-Broken Access Control: Ανέρχεται από την 5^η θέση το 2017 στην 1^η ως τον πιο σοβαρό κίνδυνο ασφάλειας διαδικτυακών εφαρμογών. Με τον έλεγχο πρόσβασης οι χρήστες ενεργούν εντός των προβλεπόμενων αδειών τους. Αν κάποιος χρήστης αποκτήσει πρόσβαση εκτός των ορίων του τότε υπάρχει κίνδυνος μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, τροποποίηση ή διαγραφή δεδομένων και εκτέλεση κάποιας λειτουργίας πέρα από τις αρμοδιότητές του. Κάποια κοινά τρωτά σημεία του ελέγχου πρόσβασης είναι:

- ♦ Όταν η πρόσβαση είναι διαθέσιμη σε οποιονδήποτε, ενώ θα έπρεπε να παρέχεται μόνο για συγκεκριμένες δυνατότητες, ρόλους ή χρήστες.
- ♦ Παράκαμψη ελέγχων πρόσβασης τροποποιώντας τη διεύθυνση URL, την κατάσταση της εσωτερικής εφαρμογής ή τη σελίδα HTML ή χρησιμοποιώντας ένα εργαλείο επίθεσης που τροποποιεί αιτήματα API.
- ♦ Όταν παρέχεται το μοναδικό αναγνωριστικό ενός χρήστη, επιτρέπεται η προβολή ή η επεξεργασία του λογαριασμού του από άλλους.
- ♦ Ανύψωση προνομίου. Όταν για παράδειγμα ενεργεί κάποιος ως διαχειριστής αλλά είναι συνδεδεμένος ως χρήστης.
- ♦ Η εσφαλμένη διαμόρφωση CORS επιτρέπει την πρόσβαση API από μη εξουσιοδοτημένες/μη αξιόπιστες πηγές.

Ο έλεγχος πρόσβασης είναι αποτελεσματικός μόνο σε αξιόπιστο κώδικα από την πλευρά του διακομιστή ή API χωρίς διακομιστή, όπου ο εισβολέας δεν μπορεί να τροποποιήσει τον έλεγχο πρόσβασης ή τα μεταδεδομένα. Προκειμένου να μην αποτύχει ο έλεγχος πρόσβασης θα πρέπει:

- ✓ Να γίνεται εφαρμογή μηχανισμών ελέγχου πρόσβασης.

- ✓ Απενεργοποίηση της λίστας καταλόγων (directory listing) και διαβεβαίωση ότι τα μεταδεδομένα αρχείων και τα αρχεία αντιγράφων ασφάλειας δεν υπάρχουν στον διακομιστή.
- ✓ Καταγραφή των αποτυχημένων ελέγχων πρόσβασης και ειδοποίηση των διαχειριστών όταν χρειάζεται. [4]

2.1.2 A02:2021-Cryptographic Failures: Μετατοπίζεται στην 2^η θέση. Παλαιότερα γνωστό ως A3:2017-Sensitive Data Exposure, ήταν περισσότερο σύμπτωμα παρά η βασική αιτία. Το ανανεωμένο όνομα εστιάζει σε αστοχίες που σχετίζονται με την κρυπτογραφία. Αυτή η κατηγορία οδηγεί συχνά σε έκθεση ευαίσθητων δεδομένων ή σε παραβίαση του συστήματος.

Προτεραιότητα έχει να καθοριστούν οι ανάγκες προστασίας των δεδομένων κατά την μεταφορά και παραμονή. Δεδομένα όπως κωδικοί πρόσβασης, αρχεία υγείας, προσωπικές πληροφορίες, αριθμοί πιστωτικών καρτών, απαιτούν πρόσθετη προστασία, ειδικά αν εμπίπτουν στην νομοθεσία περί απορρήτου π.χ. στον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (GDPR) ή κανονισμούς, π.χ. προστασία οικονομικών δεδομένων όπως το πρότυπο ασφάλειας δεδομένων PCI (PCI DSS). Υπάρχει ευπάθεια όταν:

- ◆ Χρησιμοποιούνται παλαιοί ή αδύναμοι κρυπτογραφικοί αλγόριθμοι ή πρωτόκολλα.
- ◆ Μεταδίδονται δεδομένα σε καθαρό κείμενο μέσω μη ασφαλών πρωτοκόλλων μεταφοράς δεδομένων όπως το HTTP.
- ◆ Χρησιμοποιούνται προεπιλεγμένα κλειδιά κρυπτογράφησης, δημιουργούνται ή επαναχρησιμοποιούνται αδύναμα κλειδιά κρυπτογράφησης.
- ◆ Δεν επιβάλλεται η κρυπτογράφηση.
- ◆ Δεν υπάρχει σωστή επικύρωση πιστοποιητικών διακομιστή.
- ◆ Γίνεται χρήση κωδικών πρόσβασης ως κρυπτογραφικά κλειδιά.
- ◆ Γίνεται χρήση καταργημένων συναρτήσεων κατακερματισμού όπως MD5 ή SHA1 ή χρησιμοποιούνται μη κρυπτογραφικές συναρτήσεις κατακερματισμού όταν χρειάζονται κρυπτογραφημένες.

Προκειμένου να περιοριστεί η συγκεκριμένη ευπάθεια χρειάζεται:

- ✓ Ταξινόμηση δεδομένων που επεξεργάζονται, αποθηκεύονται ή μεταδίδονται από μια εφαρμογή. Προσδιορισμός των δεδομένων που είναι ευαίσθητα σύμφωνα με τους νόμους περί απορρήτου, τις ρυθμιστικές απαιτήσεις ή τις επιχειρηματικές ανάγκες.
- ✓ Μη αποθήκευση ευαίσθητων δεδομένων που δεν χρειάζονται. Δεδομένα που δεν υπάρχουν δεν μπορούν να κλαπούν.
- ✓ Κρυπτογράφηση όλων των δεδομένων που παραμένουν στάσιμα.
- ✓ Χρήση ενημερωμένων και ισχυρών αλγορίθμων, πρωτοκόλλων και κλειδιών. Σωστή διαχείριση κλειδιών.
- ✓ Κρυπτογράφηση δεδομένων κατά την μεταφορά με ασφαλή πρωτόκολλα όπως HTTP Strict Transport Security (HSTS).
- ✓ Απενεργοποίηση της προσωρινής αποθήκευσης για απάντηση αιτημάτων που περιέχουν ευαίσθητα δεδομένα.
- ✓ Εφαρμογή απαιτούμενων ελέγχων σύμφωνα με την ταξινόμηση των δεδομένων.
- ✓ Αποφυγή χρήσης πρωτοκόλλων παλαιού τύπου, για τη μεταφορά ευαίσθητων δεδομένων, όπως FTP και SMTP. [5]

2.1.3 A03:2021-Injection: Αυτή η κατηγορία ολισθαίνει στην 3^η θέση. Είναι μια ευπάθεια που επιτρέπει σε έναν εισβολέα να μεταφέρει κακόβουλο κώδικα μέσω μιας εφαρμογής σε άλλο σύστημα. Αυτό μπορεί να περιλαμβάνει την διακινδύνευση τόσο των συστημάτων υποστήριξης όσο και άλλων πελατών που συνδέονται με την ευάλωτη εφαρμογή. Τα αποτελέσματα αυτής της ευπάθειας επιτρέπουν σε έναν εισβολέα:

- ◆ Να εκτελέσει κλήσεις λειτουργικού συστήματος σε μια μηχανή-στόχο.
- ◆ Να παραβιάσει τις αποθήκες δεδομένων υποστήριξης.
- ◆ Να παραβιάσει συνεδρίες άλλων χρηστών.
- ◆ Να εξαναγκάσει ενέργειες για λογαριασμό άλλων χρηστών ή υπηρεσιών.

Οι πιο γνωστοί τύποι επιθέσεων injection είναι οι SQL Injection, OS Command Injection, Cross-Site Scripting (XSS), Object Relational Mapping (ORM), LDAP, Expression Language (EL) or Object Graph Navigation Library (OGNL) injection.

Ο καλύτερος τρόπος για να προσδιορίσετε εάν οι εφαρμογές σας είναι ευάλωτες σε επιθέσεις injection είναι να αναζητήσετε τον πηγαίο κώδικα για όλες τις κλήσεις προς εξωτερικούς πόρους. Επιπλέον, επιβεβαιώστε ότι όλα τα δεδομένα εισόδου που παρέχονται από τον χρήστη είναι καθαρά και ότι τα δεδομένα που παρέχονται από τον χρήστη που εξάγονται είναι σωστά κωδικοποιημένα. Για την προστασία από αυτή την ευπάθεια χρειάζεται:

- ✓ Η επικύρωση των εισροών: εκτελείται για να διασφαλιστεί ότι μόνο σωστά διαμορφωμένα δεδομένα εισέρχονται στη ροή εργασιών σε ένα σύστημα πληροφοριών, αποτρέποντας τη διατήρηση λανθασμένων δεδομένων στη βάση δεδομένων και την πρόκληση δυσλειτουργίας διαφόρων στοιχείων. Η επικύρωση των εισροών θα πρέπει να γίνεται όσο το δυνατόν νωρίτερα στη ροή δεδομένων, κατά προτίμηση μόλις ληφθούν τα δεδομένα από το εξωτερικό μέρος.
- ✓ Εφαρμογή του ελάχιστου προνομίου: Μια άλλη ισχυρή προστασία από επιθέσεις injection είναι να διασφαλίσετε ότι η εφαρμογή Ιστού εκτελείται μόνο με τα προνόμια που χρειάζεται οπωσδήποτε για να εκτελέσει τη λειτουργία της.
- ✓ Χειρισμός εξαιρέσεων και επιστρεφόμενων κωδικών: Εάν πρέπει να χρησιμοποιηθεί μια εξωτερική εντολή, οποιεσδήποτε πληροφορίες χρήστη εισάγονται στην εντολή θα πρέπει να ελέγχονται αυστηρά. Πρέπει να τεθούν σε εφαρμογή μηχανισμοί για την αντιμετώπιση τυχόν σφαλμάτων, χρονικών ορίων ή μπλοκαρίσματος κατά τη διάρκεια της κλήσης. Όλοι οι κωδικοί εξόδου, επιστροφής και κωδικοί σφάλματος από την κλήση θα πρέπει να ελέγχονται για να διασφαλιστεί ότι η αναμενόμενη επεξεργασία πραγματοποιήθηκε. Τουλάχιστον, αυτό θα σας επιτρέψει να διαπιστώσετε ότι κάτι έχει πάει στραβά. Διαφορετικά, η επίθεση μπορεί να συμβεί και να μην εντοπιστεί ποτέ. [6]

2.1.4 A04:2021-Insecure Design: Αυτή είναι μια νέα κατηγορία για το 2021, η οποία εστιάζει στους κινδύνους που σχετίζονται με τα ελαττώματα της αρχιτεκτονικής του σχεδιασμού. Κάνει έκκληση για περισσότερη χρήση μοντελοποίησης απειλών, ασφαλών μοτίβων σχεδιασμού και αρχιτεκτονικών αναφορών. Ο μη ασφαλής σχεδιασμός είναι μια ευρεία κατηγορία που αντιπροσωπεύει διαφορετικές αδυναμίες, που εκφράζονται ως "ελλιπής ή αναποτελεσματικός σχεδιασμός ελέγχου". Διακρίνουμε μεταξύ ελαττωμάτων σχεδιασμού και ελαττωμάτων υλοποίησης για κάποιο λόγο, έχουν διαφορετικές βασικές αιτίες και αποκατάσταση. Ένας ασφαλής σχεδιασμός μπορεί να εξακολουθεί να έχει

ελαττώματα υλοποίησης που οδηγούν σε τρωτά σημεία που μπορεί να αξιοποιηθούν. Ένας ανασφαλής σχεδιασμός δεν μπορεί να διορθωθεί με μια τέλεια εφαρμογή, καθώς εξ ορισμού, δεν δημιουργήθηκαν ποτέ απαραίτητοι έλεγχοι ασφαλείας για την άμυνα έναντι συγκεκριμένων επιθέσεων. Η ασφαλής σχεδίαση είναι μια κουλτούρα και μια μεθοδολογία που αξιολογεί συνεχώς τις απειλές και διασφαλίζει ότι ο κώδικας έχει σχεδιαστεί και δοκιμαστεί άρτια για την αποτροπή γνωστών μεθόδων επίθεσης. Δεν είναι ούτε πρόσθετο ούτε εργαλείο που μπορείτε να προσθέσετε στο λογισμικό. [7]

2.1.5 A05:2021-Security Misconfiguration (Λανθασμένη διαμόρφωση ασφάλειας): Αυτή η κατηγορία ανεβαίνει από το 6# της προηγούμενης έκδοσης. Μια εφαρμογή μπορεί να είναι ευάλωτη εάν:

- ◆ Λείπει η ενίσχυση της ασφάλειας σε οποιοδήποτε επίπεδο της εφαρμογής ή υπάρχουν ακατάλληλα διαμορφωμένα δικαιώματα στις υπηρεσίες cloud.
- ◆ Ενεργοποιούνται ή εγκαθίστανται περιττές λειτουργίες.
- ◆ Οι προεπιλεγμένοι λογαριασμοί και οι κωδικοί πρόσβασής τους εξακολουθούν να είναι ενεργοποιημένοι και αμετάβλητοι.
- ◆ Για τα αναβαθμισμένα συστήματα, οι πιο πρόσφατες δυνατότητες ασφαλείας είναι απενεργοποιημένες ή δεν έχουν διαμορφωθεί με ασφάλεια.
- ◆ Οι ρυθμίσεις ασφαλείας στους διακομιστές εφαρμογών, τα πλαίσια εφαρμογών (π.χ. Struts, Spring, ASP.NET), βιβλιοθήκες, βάσεις δεδομένων κ.λπ., δεν έχουν οριστεί σε ασφαλείς τιμές.
- ◆ Το λογισμικό είναι ξεπερασμένο ή ευάλωτο.

Χωρίς μια συντονισμένη, επαναλαμβανόμενη διαδικασία διαμόρφωσης ασφαλείας εφαρμογών, τα συστήματα διατρέχουν υψηλότερο κίνδυνο.

Για την αποφυγή αυτής της ευπάθειας θα πρέπει να εφαρμόζονται ασφαλείς διαδικασίες εγκατάστασης όπως:

- ✓ Μια πλατφόρμα χωρίς περιττά στοιχεία, χαρακτηριστικά, δείγματα. Θα πρέπει να γίνεται κατάργηση ή απεγκατάσταση των μη χρησιμοποιούμενων λειτουργιών και πλαισίων.
- ✓ Έλεγχος και ενημέρωση των διαμορφώσεων που είναι κατάλληλες για όλες τις σημειώσεις ασφαλείας, τις ενημερώσεις και τις ενημερώσεις κώδικα ως μέρος της διαδικασίας διαχείρισης ενημερώσεων κώδικα.
- ✓ Μια αυτοματοποιημένη διαδικασία για την επαλήθευση της αποτελεσματικότητας των διαμορφώσεων και των ρυθμίσεων σε όλα τα περιβάλλοντα. [8]

2.1.6 A06:2021-Vulnerable and Outdated Components: Αυτή η κατηγορία είχε προηγουμένως τον τίτλο «Using Components with Known Vulnerabilities» και ανεβαίνει στην κατάταξη από το #9 το 2017. Μια εφαρμογή είναι πιθανότατα ευάλωτη όταν:

- ◆ Οι διαχειριστές δεν γνωρίζουν τις εκδόσεις όλων των στοιχείων που χρησιμοποιούν.
- ◆ Το λογισμικό είναι ευάλωτο, δεν υποστηρίζεται ή είναι παλιό. Αυτό περιλαμβάνει το λειτουργικό σύστημα, τον διακομιστή ιστού/εφαρμογών, το σύστημα διαχείρισης βάσεων δεδομένων (DBMS), τις εφαρμογές, τα API και όλα τα στοιχεία, τα περιβάλλοντα χρόνου εκτέλεσης και τις βιβλιοθήκες.

- ♦ Όταν δεν γίνεται τακτικά σάρωση για ευπάθειες και εγγραφή σε ενημερωτικά δελτία ασφαλείας που σχετίζονται με τα στοιχεία που χρησιμοποιούνται.
- ♦ Η μη διόρθωση και αναβάθμιση της υποκείμενης πλατφόρμας.
- ♦ Ο μη έλεγχος της συμβατότητας των ενημερωμένων, αναβαθμισμένων ή διορθωμένων βιβλιοθηκών.

Για να περιοριστεί αυτή η ευπάθεια θα πρέπει:

- ✓ Να γίνει αφαίρεση μη χρησιμοποιούμενων χαρακτηριστικών, στοιχείων, αρχείων.
- ✓ Παρακολούθηση συνεχώς πηγών όπως Common Vulnerability και Exposures (CVE) και National Vulnerability Database (NVD) για τρωτά σημεία στα στοιχεία. Και εγγραφή σε ειδοποιήσεις μέσω email για ευπάθειες ασφαλείας που σχετίζονται με στοιχεία που χρησιμοποιούνται.
- ✓ Προτίμηση πιστοποιημένων πακέτων για την μείωση της πιθανότητας συμπερίληψης ενός τροποποιημένου, κακόβουλου στοιχείου.
- ✓ Παρακολούθηση για βιβλιοθήκες και στοιχεία που δεν συντηρούνται ή δεν δημιουργούν ενημερώσεις κώδικα ασφαλείας για παλαιότερες εκδόσεις.

Κάθε οργανισμός πρέπει να διασφαλίζει ένα διαρκές σχέδιο για την παρακολούθηση, τη διαλογή και την εφαρμογή ενημερώσεων ή αλλαγών διαμόρφωσης, για τη διάρκεια ζωής της εφαρμογής. [9]

2.1.7 A07:2021-Identification and Authentication Failures: Αυτή η κατηγορία ονομαζόταν στο παρελθόν Broken Authentication και βρισκόταν στην 2^η θέση. Πλέον περιλαμβάνει και ευπάθειες που σχετίζονται με αποτυχίες αναγνώρισης. Η επιβεβαίωση της ταυτότητας του χρήστη, ο έλεγχος ταυτότητας και η διαχείριση περιόδου λειτουργίας είναι κρίσιμης σημασίας για την προστασία από επιθέσεις που σχετίζονται με τον έλεγχο ταυτότητας. Ενδέχεται να υπάρχουν αδυναμίες ελέγχου ταυτότητας εάν η εφαρμογή:

- ♦ Επιτρέπει brute force ή άλλες αυτοματοποιημένες επιθέσεις.
- ♦ Επιτρέπει προεπιλεγμένους, αδύναμους ή γνωστούς κωδικούς πρόσβασης, όπως "Password1" ή "admin/admin".
- ♦ Χρησιμοποιεί αδύναμες ή αναποτελεσματικές διαδικασίες ανάκτησης διαπιστευτηρίων και ξεχασμένου κωδικού πρόσβασης, όπως "απαντήσεις που βασίζονται στη γνώση", οι οποίες δεν μπορούν να είναι ασφαλείς.
- ♦ Λείπει ή είναι αναποτελεσματικός ο έλεγχος ταυτότητας πολλαπλών παραγόντων.
- ♦ Εκθέτει το αναγνωριστικό περιόδου σύνδεσης στη διεύθυνση URL.
- ♦ Επαναχρησιμοποιεί το αναγνωριστικό περιόδου σύνδεσης μετά την επιτυχή σύνδεση.
- ♦ Δεν ακυρώνει σωστά τα Session ID. Οι περίοδοι σύνδεσης χρήστη ή τα διακριτικά ελέγχου ταυτότητας δεν ακυρώνονται σωστά κατά την αποσύνδεση ή μια περίοδο αδράνειας.

Για να αποτραπεί αυτή η ευπάθεια θα πρέπει:

- ✓ Να εφαρμόζεται έλεγχος ταυτότητας πολλαπλών παραγόντων.
- ✓ Να μην χρησιμοποιούνται τα προεπιλεγμένα διαπιστευτήρια (Όνομα και κωδικός) ειδικά για τους διαχειριστές.
- ✓ Να εφαρμόζεται έλεγχος για αδύναμους κωδικούς πρόσβασης.

- ✓ Να περιορίζονται ή καθυστερούνται ολοένα και περισσότερο οι αποτυχημένες προσπάθειες σύνδεσης, χωρίς όμως να δημιουργείται ένα σενάριο άρνησης υπηρεσίας. Καταγραφή όλων των αποτυχιών και ειδοποίηση των διαχειριστών όταν εντοπίζονται επιθέσεις brute force, credential stuffing και άλλες.
- ✓ Χρήση ενός ασφαλούς, ενσωματωμένου διαχειριστή συνεδρίας από την πλευρά του διακομιστή που δημιουργεί ένα νέο τυχαίο αναγνωριστικό συνεδρίας με υψηλή εντροπία μετά τη σύνδεση. Το αναγνωριστικό περιόδου σύνδεσης δεν πρέπει να βρίσκεται στη διεύθυνση URL, αλλά να αποθηκεύεται με ασφάλεια και να ακυρώνεται μετά την αποσύνδεση, την αδράνεια και τα απόλυτα χρονικά όρια. [10]

2.1.8 A08:2021-Software and Data Integrity Failures: Πρόκειται για μια νέα κατηγορία για το 2021, η οποία εστιάζει στην δημιουργία υποθέσεων σχετικά με ενημερώσεις λογισμικού και κρίσιμα δεδομένα χωρίς επαλήθευση της ακεραιότητας. Οι αποτυχίες ακεραιότητας λογισμικού και δεδομένων σχετίζονται με κώδικα και υποδομή που δεν προστατεύει από παραβιάσεις ακεραιότητας. Ένα παράδειγμα αυτού είναι όταν μια εφαρμογή βασίζεται σε προσθήκες, βιβλιοθήκες ή λειτουργικές μονάδες από μη αξιόπιστες πηγές, αποθήκες και δίκτυα παράδοσης περιεχομένου (CDN). Μια μη ασφαλής διοχέτευση CI/CD μπορεί να εισαγάγει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, κακόβουλου κώδικα ή παραβίασης του συστήματος. Τέλος, πολλές εφαρμογές περιλαμβάνουν πλέον λειτουργία αυτόματης ενημέρωσης, όπου οι ενημερώσεις κατεβαίνουν χωρίς επαρκή επαλήθευση ακεραιότητας και εφαρμόζονται στην προηγούμενη αξιόπιστη εφαρμογή. Οι εισβολείς θα μπορούσαν ενδεχομένως να ανεβάσουν τις δικές τους ενημερώσεις για διανομή και εκτέλεση σε όλες τις εγκαταστάσεις.

Για να αποτραπεί η συγκεκριμένη ευπάθεια χρειάζεται:

- ✓ Χρήση ψηφιακών υπογραφών ή παρόμοιων μηχανισμών για επαλήθευση ότι το λογισμικό ή τα δεδομένα προέρχονται από την αναμενόμενη πηγή και δεν έχουν τροποποιηθεί.
- ✓ Η βεβαιότητα ότι υπάρχει μια διαδικασία αναθεώρησης για αλλαγές κώδικα και διαμόρφωσης για να ελαχιστοποιηθεί η πιθανότητα να εισαχθεί κακόβουλος κώδικας ή διαμόρφωση στη διοχέτευση λογισμικού.
- ✓ Η βεβαιότητα ότι τα ανυπόγραφα ή μη κρυπτογραφημένα σειριακά δεδομένα δεν αποστέλλονται σε μη αξιόπιστους πελάτες χωρίς κάποια μορφή ελέγχου ακεραιότητας ή ψηφιακή υπογραφή για τον εντοπισμό παραβίασης ή επανάληψης αναπαραγωγής των σειριακών δεδομένων. [11]

2.1.9 A09:2021-Security Logging and Monitoring Failures: Η κατηγορία αυτή βρισκόταν στην 10^η θέση και ονομαζόταν A10:2017-Insufficient Logging & Monitoring. Βοηθά στον εντοπισμό, την κλιμάκωση και την απόκριση σε ενεργές παραβιάσεις. Χωρίς καταγραφή και παρακολούθηση, οι παραβιάσεις δεν μπορούν να εντοπιστούν. Ανεπαρκής καταγραφή, ανίχνευση, παρακολούθηση και ενεργή απόκριση εμφανίζεται ανά πάσα στιγμή όταν:

- ◆ Τα ελεγχόμενα συμβάντα, όπως οι συνδέσεις, οι αποτυχημένες συνδέσεις και οι συναλλαγές υψηλής αξίας, δεν καταγράφονται.
- ◆ Οι προειδοποιήσεις και τα σφάλματα δημιουργούν, καθόλου, ανεπαρκή ή ασαφή μηνύματα καταγραφής.

- ◆ Τα αρχεία καταγραφής εφαρμογών και API δεν παρακολουθούνται για ύποπτη δραστηριότητα.
- ◆ Τα αρχεία καταγραφής αποθηκεύονται μόνο τοπικά.
- ◆ Η εφαρμογή δεν μπορεί να εντοπίσει, να κλιμακώσει ή να ειδοποιήσει για ενεργές επιθέσεις σε πραγματικό χρόνο ή σχεδόν σε πραγματικό χρόνο.

Είστε ευάλωτοι σε διαρροή πληροφοριών κάνοντας ορατά τα συμβάντα καταγραφής και ειδοποίησης σε έναν χρήστη ή έναν εισβολέα. Για να αποτραπεί αυτή η ευπάθεια θα πρέπει οι προγραμματιστές να εφαρμόζουν ορισμένα στοιχεία ελέγχου όπως:

- ✓ Όλες οι αποτυχημένες προσπάθειες σύνδεσης, ελέγχου πρόσβασης και επικύρωσης από την πλευρά του διακομιστή θα πρέπει να καταγράφονται με επαρκή στοιχεία χρήστη για τον εντοπισμό ύποπτων ή κακόβουλων λογαριασμών και να διατηρούνται για αρκετό χρόνο ώστε να επιτρέπεται η καθυστερημένη εγκληματολογική ανάλυση.
- ✓ Τα αρχεία καταγραφής δημιουργούνται σε μια μορφή που μπορούν να διαχειριστούν με ευκολία.
- ✓ Τα δεδομένα καταγραφής κωδικοποιούνται σωστά για την αποτροπή επιθέσεων στα συστήματα καταγραφής ή παρακολούθησης.
- ✓ Οι συναλλαγές υψηλής αξίας έχουν μια διαδρομή ελέγχου με στοιχεία ελέγχου ακεραιότητας για την αποφυγή παραβίασης ή διαγραφής.
- ✓ Καθιέρωση ή υιοθέτηση ενός σχεδίου αντιμετώπισης περιστατικών και αποκατάστασης. [12]

2.1.10 A10:2021-Server-Side Request Forgery: Τα σφάλματα SSRF εμφανίζονται κάθε φορά που μια εφαρμογή Ιστού ανακτά έναν απομακρυσμένο πόρο χωρίς να επικυρώνει τη διεύθυνση URL που παρέχεται από τον χρήστη. Επιτρέπει σε έναν εισβολέα να εξαναγκάσει την εφαρμογή να στείλει ένα επεξεργασμένο αίτημα σε έναν απροσδόκητο προορισμό, ακόμη και όταν προστατεύεται από τείχος προστασίας, VPN ή άλλου τύπου λίστα ελέγχου πρόσβασης δικτύου (ACL).

Καθώς οι σύγχρονες εφαρμογές Ιστού παρέχουν στους τελικούς χρήστες βολικές δυνατότητες, η ανάκτηση μιας διεύθυνσης URL γίνεται ένα συνηθισμένο σενάριο. Ως αποτέλεσμα, η συχνότητα εμφάνισης SSRF αυξάνεται. Επίσης, η σοβαρότητα του SSRF γίνεται υψηλότερη λόγω των υπηρεσιών cloud και της πολυπλοκότητας των αρχιτεκτονικών.

Οι προγραμματιστές μπορούν να αποτρέψουν το SSRF εφαρμόζοντας μερικούς ή όλους τους ακόλουθους ελέγχους:

Σε επίπεδο δικτύου:

- ✓ Τμηματοποίηση της λειτουργίας απομακρυσμένης πρόσβασης σε πόρους σε ξεχωριστά δίκτυα για μείωση του αντίκτυπου του SSRF.
- ✓ Εφαρμογή των πολιτικών "άρνησης από προεπιλογή" του τείχους προστασίας ή κανόνες ελέγχου πρόσβασης στο δίκτυο για να αποκλεισμό όλης εκτός από τη βασική κίνηση στο εσωτερικό του δικτύου.

Σε επίπεδο εφαρμογής:

- ✓ Καθαρισμός και επικύρωση όλων των δεδομένων εισόδου που προέρχονται από τον πελάτη.
- ✓ Απενεργοποίηση των ανακατευθύνσεων HTTP.

- ✓ Η χρήση λίστας άρνησης δεν ωφελεί στην μείωση του SSRF, καθώς οι επιτιθέμενοι έχουν λίστες, εργαλεία και δεξιότητες για να παρακάμψουν τις λίστες άρνησης. [13]

2.2 Είδη επιθέσεων

Στην ενότητα αυτή παρουσιάζονται οι πιο κοινοί τύποι επιθέσεων απέναντι στις διαδικτυακές εφαρμογές.

2.2.1 Brute force attacks: Οι επιθέσεις brute force είναι από τις πιο κοινές στις ιστοσελίδες WordPress. Σε αυτόν τον τύπο επίθεσης ο επιτιθέμενος προσπαθεί να μαντέψει τον σωστό συνδυασμό του ονόματος χρήστη (username) και του κωδικού (password) για να μπορέσει να έχει πρόσβαση στην διαχείριση της ιστοσελίδας. Εκτελεί χιλιάδες προσπάθειες σύνδεσης το λεπτό με διαφορετικά στοιχεία μέχρι να πετύχει τα σωστά. Αν καταφέρει να αποκτήσει πρόσβαση τότε μπορεί να προκαλέσει πολλά προβλήματα όπως η κλοπή προσωπικών δεδομένων, η μόλυνση με κακόβουλο λογισμικό και ιούς, η αποστολή spam mail από την ιστοσελίδα κ.α. [14]

2.2.2 Denial of service (DoS Attack): Οι επιθέσεις άρνησης παροχής υπηρεσιών στοχεύουν κυρίως στην διαθεσιμότητα του δικτύου ή του συστήματος, στην παρεμπόδιση της ομαλής λειτουργίας του και στην εξάντληση των πόρων του δικτύου έτσι ώστε αυτό να μην μπορεί να ανταπεξέλθει στις λειτουργίες που χρειάζεται. Στοχεύει για παράδειγμα στον αριθμό των πακέτων που μπορεί να χειριστεί ταυτόχρονα ένας δρομολογητής ή τις διεργασίες που πρέπει να φέρει εις πέρας ο κεντρικός εξυπηρετητής στο δίκτυο. Εκμεταλλεύεται τα μέσα του δικτύου σε τέτοιο βαθμό ώστε να δημιουργηθεί συμφόρηση και να μην μπορεί να εξυπηρετηθεί κανένας άλλος. Η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση έχει ως αποτέλεσμα να μην μπορούν να εξυπηρετηθούν αυτοί που πραγματικά θέλουν την υπηρεσία. Με την εκδήλωση μιας τέτοιας επίθεσης μπορεί να υπάρχει είτε απώλεια των μηνυμάτων που μεταδίδονται, είτε καθυστέρηση στην εξυπηρέτηση, είτε πλήρης άρνηση παροχής υπηρεσιών. [15]

2.2.3 Distributed denial of service (DDoS attack): Οι επιτιθέμενοι με τη χρήση δουρειών ίππων αποκτούν τον έλεγχο σε πολλούς υπολογιστές ανυποψίαστων χρηστών. Σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο και φυσικά μετά από την υπερβολική ζήτηση που αντιμετωπίζει, καταρρέει. [16]

2.2.4 Cross-site Scripting (XSS): Σε αυτό το είδος της επίθεσης οι κακόβουλοι χρήστες χρησιμοποιούν το πρόγραμμα περιήγησης του επισκέπτη για να επιτεθούν στην ιστοσελίδα. Υποδύονται τον επισκέπτη για να παραβιάσουν την σελίδα. Οι περισσότεροι ιστότοποι έχουν πεδία εισαγωγής (όπως φόρμα επικοινωνίας ή εγγραφής ή ενότητα για σχόλια) όπου οι επισκέπτες μπορούν να εισάγουν δεδομένα. Τα πεδία αυτά ενεργοποιούνται από ένα πρόσθετο. Γενικά, τα πρόσθετα διασφαλίζουν ότι τα δεδομένα

που εισάγονται στα πεδία δεν είναι κακόβουλα όπως ένα απόσπασμα κώδικα. Αλλά εάν τα πρόσθετα αναπτύξουν ευπάθεια XSS, μπορούν να επιτρέψουν στον επισκέπτη να εισάγει κακόβουλα δεδομένα ή μη αξιόπιστα δεδομένα.

Για παράδειγμα, ένα ευάλωτο πρόσθετο σχολίων επιτρέπει στους επισκέπτες να εισαγάγουν έναν κακόβουλο σύνδεσμο. Όταν κάνετε κλικ στον σύνδεσμο, ενεργοποιείται κακόβουλος κώδικας ή κακόβουλο javascript και σας ζητείται άδεια πρόσβασης στα cookies του προγράμματος περιήγησής σας. Φαίνεται ότι ο ιστότοπός σας, σας ζητά να εκτελέσετε μια συγκεκριμένη λειτουργία. Είναι πολύ πιθανό να παραμελήσετε το κόλπο και να επιτρέψετε την πρόσβαση στα cookies του προγράμματος περιήγησής σας. Επιτρέποντας την πρόσβαση στα cookies του προγράμματος περιήγησής σας, εκθέτετε ευαίσθητες πληροφορίες σε έναν χάκερ. Τα cookies προγράμματος περιήγησης αποθηκεύουν κάθε είδους πληροφορίες, συμπεριλαμβανομένων των διαπιστευτηρίων σύνδεσής σας. Μόλις αποκτήσει πρόσβαση στα διαπιστευτήρια σύνδεσής σας, ο επιτιθέμενος μπορεί να σας μιμηθεί και να συνδεθεί στον ιστότοπό σας. Μόλις αποκτήσει πρόσβαση στον ιστότοπό σας, μπορεί να κλέψει ευαίσθητα δεδομένα, να αποθηκεύσει παράνομα αρχεία και φακέλους, να ανακατευθύνει τους επισκέπτες σας σε άλλους κακόβουλους ιστότοπους, να εξαπολύσουν επιθέσεις σε άλλους ιστότοπους κ.α. Τέτοιες κακόβουλες δραστηριότητες έχουν τη δυνατότητα να καταστρέψουν τον ιστότοπό σας. [17,18]

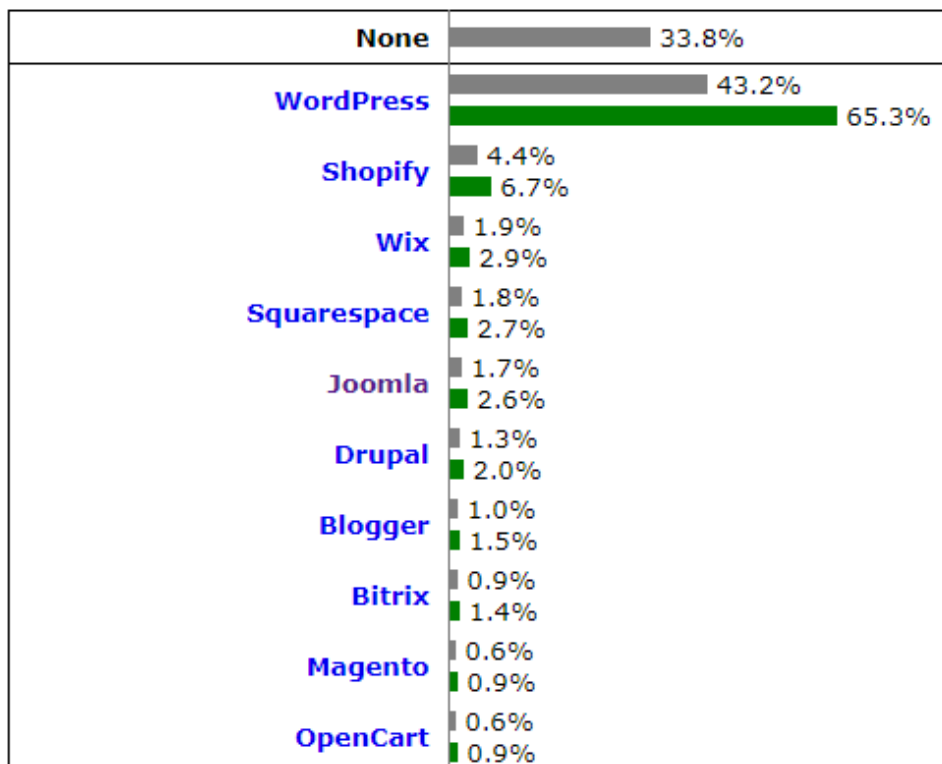
2.2.5 SQL Injection Attacks: Σχεδόν κάθε ιστότοπος έχει ένα πεδίο εισαγωγής όπως μια φόρμα επικοινωνίας, μια γραμμή αναζήτησης ιστότοπου ή μια ενότητα σχολίων που επιτρέπει στους επισκέπτες να εισάγουν δεδομένα. Ορισμένοι ιστότοποι επιτρέπουν επίσης στους επισκέπτες να ανεβάζουν έγγραφα και αρχεία εικόνων. Συνήθως αυτά τα δεδομένα γίνονται αποδεκτά και αποστέλλονται στη βάση δεδομένων για επεξεργασία και αποθήκευση. Αυτά τα πεδία χρειάζονται κατάλληλη διαμόρφωση για την επικύρωση και την απολύμανση των δεδομένων προτού μεταφερθούν στη βάση δεδομένων. Αυτό θα διασφαλίσει ότι γίνονται αποδεκτά μόνο έγκυρα δεδομένα. Εάν λείπουν αυτά τα μέτρα, οι επιτιθέμενοι το εκμεταλλεύονται και εισάγουν κακόβουλο κώδικα. [19]

2.2.6 Backdoor Hack: Αφού ο επιτιθέμενος αποκτήσει πρόσβαση στην ιστοσελίδα μπορεί να εγκαταστήσει ένα είδος κακόβουλου κώδικα που ονομάζεται backdoor. Πρόκειται για πολύ μικρό κομμάτι κώδικα πολύ καλά κρυμμένο που είναι δύσκολο να εντοπιστεί και δίνει την δυνατότητα στους επιτιθέμενους να έχουν ένα ανοικτό σημείο πρόσβασης στην ιστοσελίδα στο μέλλον. Μπορεί να τοποθετηθεί οπουδήποτε μέσα στην ιστοσελίδα, από τα αρχεία μέχρι την βάση δεδομένων. [20]

3. ΠΛΑΤΦΟΡΜΑ WORDPRESS ΚΑΙ ΕΝΙΣΧΥΣΗ ΑΣΦΑΛΕΙΑΣ

Το WordPress είναι ελεύθερο λογισμικό ανοικτού κώδικα το οποίο είναι γραμμένο σε PHP και MySQL και χρησιμοποιείται ως σύστημα διαχείρισης περιεχομένου (Content Management System - CMS). Είναι σχεδιασμένο ώστε να επιτρέπει στους προγραμματιστές να συνεισφέρουν τις ιδέες τους για την βελτίωση της πλατφόρμας κάνοντας αλλαγές στον κώδικα. Είναι εντελώς δωρεάν, οποιοσδήποτε μπορεί να εγκαταστήσει το λογισμικό στον server του και να δημιουργήσει οποιουδήποτε τύπου ιστοσελίδα. Είναι αρκετά εύκολο στην χρήση έτσι ώστε να μπορούν να το χρησιμοποιήσουν και όσοι δεν έχουν εμπειρία στον προγραμματισμό. Διαθέτει ένα ιδιαίτερα φιλικό περιβάλλον εργασίας στον χρήστη (User Interface - UI), με την δυνατότητα εγκατάστασης έτοιμων προτύπων (themes) αλλά και πρόσθετων λειτουργιών (plugins) με ένα μόνο κλικ. Επίσης είναι αρκετά φιλικό προς τις μηχανές αναζήτησης της Google με αποτέλεσμα το υψηλό SEO. Υποστηρίζει όλους τους τύπους πολυμέσων, κείμενο, ήχο, εικόνα, βίντεο. [21]

Είναι το πιο δημοφιλές σύστημα διαχείρισης περιεχομένου (CMS) σε όλο τον κόσμο. Χρησιμοποιείται από το 43,2% όλων των ιστοσελίδων στο διαδίκτυο, ενώ κατέχει το 65,3% στην αγορά των CMS. Περισσότερες από 30 εκ. ιστοσελίδες έχουν δημιουργηθεί με το WordPress. Από αυτές οι 39,427 ιστοσελίδες είναι στην Ελλάδα. [22, 23, 24, 25]



Εικόνα 1: Usage Statistics of CMS, January 2022 (www.w3Techs.com)

This report shows the market share trends for content management systems since January 2011.

	2011 1 Jan	2012 1 Jan	2013 1 Jan	2014 1 Jan	2015 1 Jan	2016 1 Jan	2017 1 Jan	2018 1 Jan	2019 1 Jan	2020 1 Jan	2021 1 Jan	2022 1 Jan	2022 10 Jan
WordPress	55.3%	54.3%	54.8%	59.8%	60.7%	58.8%	58.5%	60.0%	59.7%	62.1%	64.1%	65.2%	65.3%
Shopify				0.3%	0.7%	1.0%	1.3%	1.8%	2.6%	3.4%	5.2%	6.6%	6.7%
Wix			<0.1%	0.2%	0.3%	0.4%	0.6%	0.9%	1.8%	2.3%	2.4%	2.9%	2.9%
Squarespace	0.2%	0.2%	0.1%	0.3%	0.5%	0.8%	1.1%	1.5%	2.6%	2.7%	2.3%	2.7%	2.7%
Joomla	10.9%	9.5%	8.7%	9.3%	8.6%	7.5%	7.2%	6.5%	5.4%	4.6%	3.6%	2.6%	2.6%
Drupal	6.1%	6.5%	7.2%	5.5%	5.1%	4.9%	4.8%	4.6%	3.5%	3.0%	2.5%	2.0%	2.0%
Blogger	2.7%	3.0%	3.5%	3.3%	2.9%	2.7%	2.4%	1.9%	1.4%	1.5%	1.6%	1.5%	1.5%
Bitrix	0.8%	0.9%	1.0%	1.0%	1.1%	1.3%	1.4%	1.5%	1.2%	1.5%	1.7%	1.4%	1.4%
Magento				2.7%	2.8%	2.9%	2.7%	2.4%	1.9%	1.5%	1.2%	1.0%	0.9%
OpenCart					0.9%	1.0%	0.9%	0.8%	0.8%	0.8%	1.0%	0.9%	0.9%
PrestaShop			0.9%	1.1%	1.2%	1.3%	1.3%	1.3%	1.4%	1.1%	0.8%	0.7%	0.7%
Webflow									0.2%	0.2%	0.4%	0.7%	0.7%
Weebly			0.1%	0.3%	0.4%	0.4%	0.4%	0.4%	0.7%	0.6%	0.5%	0.5%	0.5%
Tilda									0.1%	0.2%	0.4%	0.5%	0.5%
HubSpot CMS						0.1%	0.2%	0.2%	0.2%	0.2%	0.3%	0.4%	0.4%
Bigcommerce					0.4%	0.4%	0.4%	0.4%	0.4%	0.4%	0.4%	0.4%	0.4%
GoDaddy Website Builder					0.2%	0.1%	0.1%	0.1%	0.3%	0.4%	0.4%	0.4%	0.4%
TYPO3	2.6%	2.0%	2.1%	1.6%	1.6%	1.5%	1.4%	1.5%	1.3%	0.9%	0.5%	0.4%	0.4%
Gatsby										0.1%	0.3%	0.4%	0.4%

Εικόνα 2: Historical yearly trends in the usage statistics of CMS (www.w3techs.com)

Το WordPress είναι από τις πιο ασφαλής πλατφόρμες CMS χάρη στην ομάδα που το υποστηρίζει. Από την έναρξή του το 2003, έχει υποστεί συνεχή βελτίωση, ώστε το βασικό του λογισμικό να μπορεί να αντιμετωπίσει και να μετριάσει τις κοινές απειλές ασφάλειας, συμπεριλαμβανομένης της λίστας Top 10 του οργανισμού OWASP (Open Web Application Security Project) που αναγνωρίζει τις πιο κοινές ευπάθειες όπως είδαμε στην προηγούμενη ενότητα.

Η ομάδα ασφάλειας του WordPress αποτελείται από περίπου 50 ειδικούς, συμπεριλαμβανομένων κορυφαίων προγραμματιστών και ερευνητών ασφάλειας, οι οποίοι σε συνεργασία με την ηγετική ομάδα του WordPress και την υποστήριξη της παγκόσμιας κοινότητας του WordPress, εργάζεται για τον εντοπισμό και την επίλυση θεμάτων ασφάλειας που μπορεί να προκύψουν στο βασικό λογισμικό που είναι διαθέσιμο για διανομή και εγκατάσταση στο *WordPress.org*. [26]

Πέρα από την προσπάθεια που γίνεται από την ομάδα ασφάλειας του WordPress, θα πρέπει οι προγραμματιστές/διαχειριστές ιστοσελίδων να είναι προσεκτικοί στην διαχείριση του λογισμικού. Θα πρέπει να υιοθετούν πρακτικές/τεχνικές ενίσχυσης της ασφάλειας (*hardening techniques*) της ιστοσελίδας. Οι περισσότερες από αυτές παρουσιάζονται παρακάτω.

3.1 Επιλογή ασφαλούς και αξιόπιστου Web Hosting

Ένα πρώτο μέρος της ασφάλειας του ιστοτόπου, αφορά το περιβάλλον της φιλοξενίας. Κύρια αρμοδιότητα του παρόχου φιλοξενίας (Web Hosting) είναι να παρέχει ένα ασφαλές και αποτελεσματικό περιβάλλον φιλοξενίας στον πελάτη. Είναι υπεύθυνος για οποιοδήποτε

θέμα ασφάλειας προκύψει σε αυτό το περιβάλλον, το οποίο είναι κυρίως οι servers. Ο πάροχος θα φροντίσει για την φυσική και την ψηφιακή ασφάλεια των υποδομών του. Από εκεί και πέρα ο διαχειριστής της ιστοσελίδας είναι υπεύθυνος για θέματα ασφάλειας που μπορεί να προκύψουν λόγω ευπαθειών στην ιστοσελίδα.

Στην περίπτωση που η ιστοσελίδα μοιράζεται τον ίδιο server με άλλες ιστοσελίδες (shared hosting), σκεφτείτε την ως ένα διαμέρισμα μιας πολυκατοικίας. Ο ιδιοκτήτης της πολυκατοικίας είναι υπεύθυνος για την γενικότερη ασφάλεια του κτηρίου έτσι ώστε ένας κλέφτης να μην μπορεί να εισέλθει στο κτήριο. Ωστόσο, ο ένοικος είναι υπεύθυνος για την ασφάλεια του διαμερίσματός του. Αν για παράδειγμα αφήσει ανοιχτό το παράθυρο και μπει ο κλέφτης τότε είναι δική του ευθύνη και όχι του ιδιοκτήτη της πολυκατοικίας.

Κάποιες από τις ενέργειες που θα πρέπει να κάνει ο πάροχος φιλοξενίας για να παραμείνουν ασφαλείς από επιθέσεις οι υποδομές του αλλά και οι σελίδες που φιλοξενεί αναφέρονται παρακάτω:

- ✓ **Παρακολούθηση δικτύου (Network Monitoring):** Έλεγχος σε τακτική βάση του εσωτερικού δικτύου για εισβολές ή ασυνήθιστες δραστηριότητες.
- ✓ **Web Application Firewall:** Χρησιμοποιώντας ένα τοίχος προστασίας ο πάροχος μπορεί να μπλοκάρει επιθέσεις τύπου cross-site forgeries (CSF), cross-site scripting (XSS), SQL injections και άλλα.
- ✓ **Προστασία από επιθέσεις DDoS:** Η εγκατάσταση εργαλείων που παρακολουθούν και μετρίζουν αυτές τις επιθέσεις είναι απαραίτητη.
- ✓ **Χρήση SFTP αντί για FTP:** Το πρωτόκολλο μεταφοράς αρχείων (FTP), μεταφέρει δεδομένα χωρίς κρυπτογράφηση αφήνοντας τους χρήστες εκτεθειμένους σε επιθέσεις man-in-the-middle και υποκλοπή δεδομένων. Γι' αυτό ενδείκνυται η χρήση ενός ασφαλούς πρωτοκόλλου μεταφοράς αρχείων σε ένα κρυπτογραφημένο κανάλι.
- ✓ **Buck-up:** Δημιουργία αντιγράφων ασφάλειας σε τακτική βάση.
- ✓ **Secure Sell (SSH):** Οι διαχειριστές θα πρέπει να χρησιμοποιούν τη λίστα επιτρεπόμενων διευθύνσεων IP για απομακρυσμένη πρόσβαση χρησιμοποιώντας SSH.
- ✓ **SSL/TLS Συνδέσεις:** Κάθε σύνδεση με τον πάροχο θα πρέπει να είναι κρυπτογραφημένη για την προστασία των χρηστών από man-in-the-middle επιθέσεις. Με την κρυπτογραφημένη σύνδεση που παρέχουν τα πιστοποιητικά ασφάλειας SSL/TLS τα δεδομένα του χρήστη είναι ασφαλή από υποκλοπή και παραβίαση λογαριασμού.
- ✓ **Antivirus και Antimalware:** Χρησιμοποιώντας προγράμματα προστασίας από ιούς για τον server και εφαρμογές προστασίας από κακόβουλο λογισμικό, ο κεντρικός υπολογιστής μπορεί να εντοπίσει άμεσα κακόβουλα αρχεία και είτε να καθαρίσει το αρχείο είτε να αποκλείσει την ύπαρξη του.
- ✓ **Αναβάθμιση ή διαγραφή μη χρησιμοποιούμενων εφαρμογών από τον server:** Οποιαδήποτε πρόσθετη εφαρμογή στον διακομιστή ενέχει κινδύνους ευπάθειας είτε από σφάλματα στον κώδικα είτε από το να επιτρέπεται στην εφαρμογή να εκτελείται χωρίς ενημέρωση κώδικα. Γι' αυτό θα πρέπει να διαγράφεται αν δεν χρησιμοποιείται ή να ενημερώνεται στην πιο πρόσφατη έκδοση.
- ✓ **Κωδικοί πρόσβασης:** Οι χρήστες, ειδικά όσοι έχουν προνόμια υψηλού επιπέδου, θα πρέπει να αλλάζουν συχνά τους κωδικούς πρόσβασής τους.

- ✓ **HTTP Strict Transport Security (HSTS):** Η ρύθμιση της κεφαλίδας HSTS σε Strict-Transport-Security θα μεταφέρει τους χρήστες από μια σύνδεση HTTP στο HTTPS και θα αναγκάσει τα προγράμματα περιήγησης να στέλνουν cookies μόνο μέσω κρυπτογραφημένων καναλιών, γεγονός που θα μειώσει την παραβίαση cookie.

Ένας ασφαλής διακομιστής προστατεύει το απόρρητο, την ακεραιότητα και τη διαθεσιμότητα των πόρων που βρίσκονται σε αυτόν. Παρότι ο πάροχος φιλοξενίας προσφέρει ασφάλεια σε ένα συγκεκριμένο επίπεδο, ο διαχειριστής της ιστοσελίδας πρέπει να γνωρίζει που ξεκινάει και που σταματάει η δική του ευθύνη.

Οι περισσότερες επιθέσεις δεν αφορούν τόσο την υποδομή στην οποία φιλοξενείται η ιστοσελίδα αλλά τις ευπάθειες που υπάρχουν στην ίδια την ιστοσελίδα και την κακή διαχείρισή της. Παρακάτω θα δούμε τις πρακτικές που θα πρέπει να ακολουθήσει ο διαχειριστής για να διατηρήσει στο μέγιστο την ασφάλεια της ιστοσελίδας. [27]

3.2 Ενημερωμένο WordPress

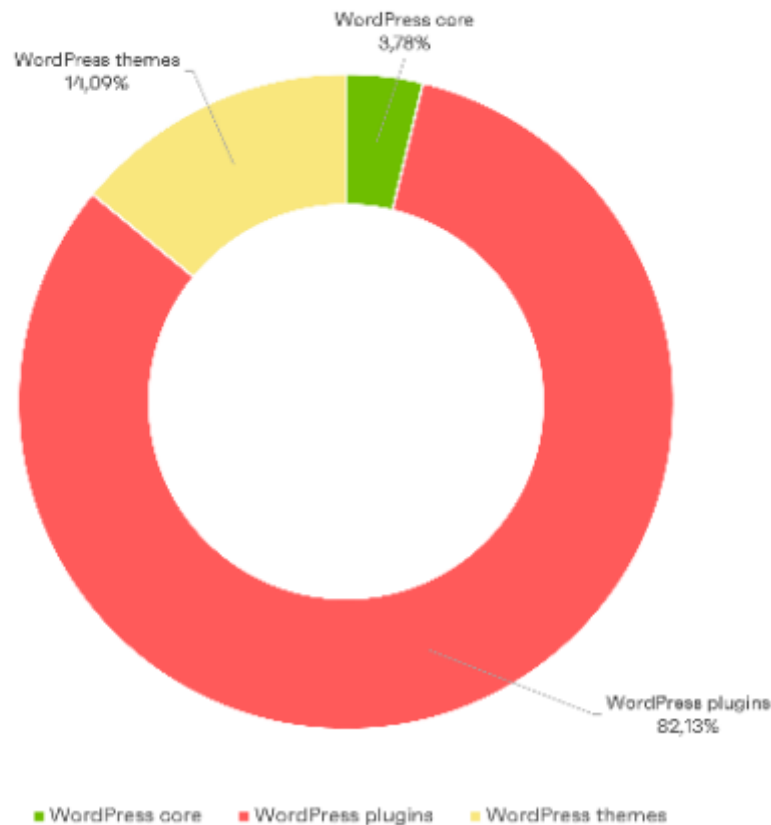
Όπως αναφέραμε στην αρχή το WordPress είναι ένα λογισμικό ανοικτού κώδικα το οποίο συντηρείται και ενημερώνεται τακτικά. Από προεπιλογή εγκαθίστανται αυτόματα κάποιες μικρές ενημερώσεις, όμως κάποιες άλλες θα πρέπει να γίνουν χειροκίνητα. Θα πρέπει να χρησιμοποιείται πάντα η πιο πρόσφατη ενημερωμένη έκδοση του WordPress, καθώς ένας από τους πιο συχνούς λόγους παραβίασης είναι η μη αναβαθμισμένη εγκατάσταση.

Επιπρόσθετα το WordPress διαθέτει χιλιάδες πρόσθετα (plugins) και θέματα (themes) τα οποία μπορεί ο διαχειριστής να εγκαταστήσει στην ιστοσελίδα. Αυτά συντηρούνται από τρίτους προγραμματιστές, οι οποίοι ελευθερώνουν συχνά ενημερωμένες εκδόσεις. Αυτές οι ενημερώσεις είναι ζωτικής σημασίας για την ασφάλεια και την σταθερότητα της ιστοσελίδας, καθώς καλύπτουν ενδεχόμενα κενά στην ασφάλεια που έχουν προκύψει σε προηγούμενες εκδόσεις. Για τον λόγο αυτό θα πρέπει να ενημερώνονται τα πρόσθετα αλλά και τα θέματα στην πιο πρόσφατη έκδοσή τους. Επίσης, αν η έκδοση κάποιου πρόσθετου ή θέματος δεν ενημερωθεί για μεγάλο χρονικό διάστημα καλό είναι να αντικατασταθεί και αν υπάρχουν εγκατεστημένα πρόσθετα που δεν χρησιμοποιούνται είναι καλή πρακτική να διαγράφονται.

Τέλος συστήνεται η χρήση και εγκατάσταση αξιόπιστων θεμάτων (themes) που έχουν προγραμματιστεί από επαγγελματίες και όχι η χρήση δωρεάν ή σπασμένων θεμάτων καθώς είναι πολύ πιθανό να περιέχουν κακόβουλο κώδικα. [28, 31]

Σύμφωνα με έρευνα της εταιρίας “Patchstack”, που διεξήχθη το 2020, οι ευπάθειες σε μια ιστοσελίδα WordPress, δεν αφορούν τόσο τον πυρήνα του λογισμικού WordPress, αλλά τα themes και τα plugins που εγκαθιστούν οι διαχειριστές στην ιστοσελίδα τους, όπως φαίνεται και στην εικόνα. [33]

Vulnerabilities on WordPress core, themes and plugins.



Εικόνα 3: Vulnerabilities on WordPress core, themes and plugins.

3.3 Αντίγραφα ασφάλειας (Backups)

Στην πρώτη γραμμή της άμυνας απέναντι στις επιθέσεις, παίρνουν θέση τα αντίγραφα ασφάλειας. Επειδή τίποτα δεν μπορεί να είναι 100% ασφαλές, τα αντίγραφα ασφάλειας μπορούν να βοηθήσουν στην γρήγορη ανάκτηση της ιστοσελίδας σε περίπτωση που κάτι πάει στραβά. Τα αντίγραφα ασφάλειας θα πρέπει να είναι αξιόπιστα και να διατηρούν την ακεραιότητα των δεδομένων. Αυτό επιτυγχάνεται με κρυπτογράφηση των αντιγράφων, με την χρήση αλγορίθμου MD5 Hash σε κάθε αρχείο και την τοποθέτηση των αντιγράφων σε μέσα μόνο για ανάγνωση.

Μια αποτελεσματική στρατηγική δημιουργίας αντιγράφων ασφαλείας περιλαμβάνει την αντιγραφή του συνόλου της εγκατάστασης του WordPress (αρχεία και βάση δεδομένων) σε τακτά χρονικά διαστήματα και την διατήρησή τους σε μια αξιόπιστη τοποθεσία. Η καλύτερη πρακτική είναι να δημιουργούνται αντίγραφα καθημερινά ακόμα και κάθε λεπτό ανάλογα και το είδος της σελίδας (πχ eshop) και να φυλάσσονται σε έναν απομακρυσμένο server ή στο cloud. Υπάρχουν αρκετά πρόσθετα που μπορούν να

χρησιμοποιηθούν για την δημιουργία αντιγράφων ασφάλειας, όπως *UpdraftPlus*, *VaultPress*, *BlogVault*, *BackWPup*, *Duplicator*. [28, 31]

3.4 Χρήση πιστοποιητικού SSL

Το HyperText Transfer Protocol Secure (HTTPS) είναι η κρυπτογραφημένη έκδοση του HTTP. Αυτό σημαίνει ότι τα δεδομένα που κινούνται ανάμεσα στον browser ενός χρήστη και στην ιστοσελίδα είναι ασφαλή από επιθέσεις υποκλοπής δεδομένων. Για να ενεργοποιηθεί η HTTPS σύνδεση για μια ιστοσελίδα, χρειάζεται ένα πιστοποιητικό Secure Socket Layer (SSL). Αυτό επικυρώνει την ιστοσελίδα ώστε οι χρήστες να γνωρίζουν ότι οι πληροφορίες τους προστατεύονται.

Το πιστοποιητικό αυτό παρέχεται δωρεάν από τον πάροχο (Let's encrypt) ή μπορεί να αγοραστεί. [28, 31]

3.5 Web Application Firewall (WAF)

Το τείχος προστασίας μπλοκάρει την κακόβουλη κίνηση πριν φτάσει στην ιστοσελίδα. Τοποθετείται ανάμεσα στον server που φιλοξενεί την ιστοσελίδα και στο δίκτυο. Οι πιο κοινοί τύποι firewall που μπορούν να χρησιμοποιηθούν σε μια ιστοσελίδα WordPress είναι:

- ✚ Σε επίπεδο DNS: φιλτράρει τους πιο κοινούς τύπους απειλών πριν επηρεάσουν τον server.
- ✚ Σε επίπεδο εφαρμογής WordPress: φιλτράρει την κίνηση αφού φτάσει στον server αλλά πριν φτάσει στην ιστοσελίδα. [31]

3.6 Ασφάλεια σύνδεσης χρήστη (Login Page Security)

Μέσα από την σελίδα login επιτρέπεται η σύνδεση των χρηστών στην περιοχή διαχείρισης της ιστοσελίδας. Υπάρχουν πάρα πολλά bots τα οποία προσπαθούν να αποκτήσουν πρόσβαση στην περιοχή διαχείρισης χρησιμοποιώντας συχνές brute force επιθέσεις. Για την προστασία από τέτοιες επιθέσεις χρειάζεται να τηρούνται κάποιες καλές πρακτικές άμυνας, τις οποίες αναφέρουμε στην συνέχεια.

3.6.1 Ισχυροί Κωδικοί πρόσβασης

Οι περισσότερες επιθέσεις σε ιστοσελίδες WordPress γίνονται με κλεμμένους κωδικούς πρόσβασης. Κωδικοί πρόσβασης χρησιμοποιούνται στην περιοχή διαχείρισης του WordPress (admin area), στον λογαριασμό FTP, στη βάση δεδομένων, στον λογαριασμό φιλοξενίας (hosting account) και στις διευθύνσεις ηλεκτρονικού ταχυδρομείου με το domain της σελίδας. Χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης, δύσκολα μπορεί κάποιος να τους μαντέψει και βοηθά στην αποτροπή επιθέσεων brute force.

Ένας άλλο μέτρο μείωσης του κινδύνου παραβίασης λογαριασμού είναι να μην δίνεται πρόσβαση στον οποιονδήποτε. Αν υπάρχει μια μεγάλη ομάδα προγραμματιστών τότε ο

καθένας θα πρέπει να έχει τους δικούς του ισχυρούς κωδικούς και περιορισμένη πρόσβαση ανάλογα με τον ρόλο του. Αυτό μπορεί να το πετύχει ο διαχειριστής δημιουργώντας διαφορετικούς λογαριασμούς χρηστών (user accounts) και περιορίζοντας τις ενέργειες που μπορεί να κάνει ο κάθε ένας. [29, 30]

3.6.2 Αλλαγή ή διαγραφή του προκαθορισμένου ονόματος χρήστη “admin”

Κατά την εγκατάσταση του WordPress, δημιουργείται ο αρχικός λογαριασμός διαχειριστή με το username “admin”. Η διατήρηση αυτού του ονόματος χρήστη, αποτελεί σημαντικό κενό ασφάλειας, γιατί οι επιτιθέμενοι γνωρίζουν ήδη την μισή πληροφορία και το μόνο που χρειάζεται για να παραβιάσουν τον λογαριασμό, είναι να βρουν τον κωδικό. Επομένως είναι καλή πρακτική η δημιουργία νέου λογαριασμού με δικαιώματα διαχειριστή με διαφορετικό όνομα χρήστη ή η τροποποίηση του ήδη υπάρχοντος. [29, 31]

3.6.3 Έλεγχος ταυτότητας δύο παραγόντων (Two-Factor Authentication or Two-Step Authentication)

Όπως αναφέραμε προηγουμένως για την είσοδο του διαχειριστή στην σελίδα θα πρέπει να εισαγάγει όνομα χρήστη και κωδικό πρόσβασης. Αυτή η διαδικασία επαλήθευσης των στοιχείων ονομάζεται διαδικασία ελέγχου με έναν παράγοντα. Για να ενισχυθεί η ασφάλεια σύνδεσης μπορεί να προστεθεί ακόμα ένας παράγοντας ελέγχου. Τέτοιοι παράγοντες είναι, το δακτυλικό αποτύπωμα, η ίριδα του ματιού, η χροιά της φωνής, η σάρωση barcode από το κινητό ή κάποιες ερωτήσεις και απαντήσεις που έχουν οριστεί από τον διαχειριστή. Για να επιτευχθεί αυτή η διαδικασία χρειάζεται η εγκατάσταση κάποιου πρόσθετου που να την υποστηρίζει όπως τα, [iThemes Security](#), [Two-factor authentication](#), [WP 2FA](#), [Wordfence Security](#), [SiteGround Security](#) κ.α. [30, 31]

3.6.4 Ερώτηση ασφάλειας κατά την σύνδεση

Προσθέτοντας μια ερώτηση ασφάλειας στην σελίδα σύνδεσης της διαχείρισης του WordPress, με την εγκατάσταση του πρόσθετου [WP Security Questions](#), δυσκολεύει την μη εξουσιοδοτημένη πρόσβαση κακόβουλων χρηστών.

3.6.5 Περιορισμός προσπαθειών σύνδεσης

Το WordPress από εγκατάσταση, επιτρέπει στους χρήστες να προσπαθήσουν να συνδεθούν στον λογαριασμό τους όσες φορές θέλουν, χωρίς να μπλοκάρει τις αποτυχημένες προσπάθειες σύνδεσης. Έτσι ένας επιτιθέμενος μπορεί να κάνει πολλές απόπειρες για να βρει τον κωδικό και η ιστοσελίδα είναι ευπαθής σε επιθέσεις brute force. Αυτό μπορεί να διορθωθεί περιορίζοντας τις αποτυχημένες προσπάθειες σύνδεσης που μπορεί να πραγματοποιήσει ο χρήστης. Εάν υπάρχει εγκατεστημένο τοίχος προστασίας (Web Application Firewall) από τον διαχειριστή ή τον πάροχο φιλοξενίας δεν υπάρχει λόγος

ανησυχίας, αν όχι τότε μπορεί να εγκατασταθεί κάποιο πρόσθετο όπως τα [Login LockDown](#) και [Limit Login Attempts](#). Επίσης, αν παρατηρηθεί ότι κάποια διεύθυνση IP έχει πολλές αποτυχημένες προσπάθειες μπορεί να μπλοκαριστεί. [29, 30, 31]

3.6.6 Αυτόματη αποσύνδεση ανενεργών χρηστών

Οι συνδεδεμένοι χρήστες μπορεί κάποια στιγμή να απομακρυνθούν από την οθόνη και να αφήσουν τον λογαριασμό τους εκτεθειμένο σε κάποια επίθεση. Οπότε είναι καλή πρακτική να αποσυνδέονται αυτόματα μετά από συγκεκριμένο χρονικό διάστημα ανενεργούς σύνδεσης. Αυτό μπορεί να γίνει με την χρήση του plugin [Inactive Logout](#). [31]

3.6.7 Αλλαγή του URL εισόδου στην διαχείριση

Από προεπιλογή, η σύνδεση στο WordPress γίνεται από την διεύθυνση «yoursite.com/wp-admin». Η αλλαγή αυτής της διεύθυνσης, μπορεί να αποτρέψει προσπάθειες παραβίασης καθώς όταν ο επιτιθέμενος θα επισκέπτεται το προεπιλεγμένο url θα βλέπει μήνυμα λάθους 404 και όχι την φόρμα σύνδεσης. Το plugin που μπορεί να βοηθήσει σε αυτή την ενέργεια είναι το [WPS Hide Login](#). [29]

3.7 Ασφάλεια αρχείων

3.7.1 Απενεργοποίηση επεξεργασίας αρχείων

Το WordPress παρέχει την δυνατότητα επεξεργασίας κώδικα μέσα από τον editor, για την επεξεργασία των plugins και themes. Η επεξεργασία αυτή σε λάθος χέρια μπορεί να αποτελέσει κίνδυνο για την ασφάλεια της ιστοσελίδας, γι' αυτό συστήνεται να απενεργοποιείται αυτή η δυνατότητα. Ένας τρόπος είναι να προστεθεί ο παρακάτω κώδικας στο αρχείο wp-config.php:

1. `// Disallow file edit`
2. `define( 'DISALLOW_FILE_EDIT', true );`

Εναλλακτικά αυτό μπορεί να γίνει μέσα από κάποιο plugin όπως το [Sucuri](#). [31]

3.7.2 Απενεργοποίηση εκτέλεσης της PHP σε συγκεκριμένους φακέλους

Με την απενεργοποίηση εκτέλεσης των αρχείων PHP σε συγκεκριμένους φακέλους που δεν χρειάζεται να εκτελείται, όπως οι φάκελοι /wp-includes/ και /wp-content/uploads/, προστατεύεται η ιστοσελίδα από “backdoor” πρόσβαση των αρχείων αυτών. Έτσι ώστε να μην μπορεί ένας κακόβουλος χρήστης να ανεβάσει κάποιο αρχείο και να προκαλέσει ζημιά στην ιστοσελίδα. Για να γίνει αυτό θα πρέπει να δημιουργηθεί ένα αρχείο .htaccess στο οποίο θα προστεθεί ο κώδικας:

- 1 `<Files *.php>`

```
2    deny from all
3    </Files>
```

Και στην συνέχεια θα ανέβει μέσα στους φακέλους που προαναφέρθηκαν.

Οι περισσότερες ιστοσελίδες έχουν στον κεντρικό (root) φάκελο της εγκατάστασης του WordPress, το αρχείο .htaccess. Πρόκειται για ένα ισχυρό αρχείο διαμόρφωσης που λέει στον server πως να χειρίζεται ορισμένα πράγματα στην ιστοσελίδα. Όπως ο τρόπος ανακατεύθυνσης των χρηστών, η προστασία φακέλων, η αποτροπή εμφάνισης καταλόγου αρχείων (directory listing) κ.α. Όμως μπορεί ο διαχειριστής να το δημιουργήσει και να το χρησιμοποιήσει μέσα στους φακέλους όπως προαναφέραμε. [29, 31]

3.7.3 Απενεργοποίηση εμφάνισης καταλόγου αρχείων (directory listing)

Όταν ο web server δεν μπορεί να εντοπίσει το αρχείο index σε έναν φάκελο, τότε εμφανίζει την λίστα όλων των αρχείων και υποφακέλων (directory listing) που βρίσκονται εντός αυτού του φακέλου. Η εμφάνιση του καταλόγου των αρχείων θεωρείται κενό ασφαλείας καθώς εμφανίζει σε οποιονδήποτε χρήστη την δομή των αρχείων της ιστοσελίδας, αρχεία που περιέχουν ευαίσθητες πληροφορίες (π.χ. wp-config.php) και επιτρέπει την λήψη ή εκτέλεση μεμονωμένων αρχείων. Για να αποτραπεί το directory listing θα πρέπει να προστεθεί η ακόλουθη γραμμή στο αρχείο .htaccess: `Options All -Indexes`. [29, 30, 31]

3.7.4 Απόκρυψη αρχείων wp-config και .htaccess

Όπως αναφέραμε προηγουμένως τα αρχεία wp-config και .htaccess επιτελούν πολύ σημαντικό έργο. Επομένως, είναι ωφέλιμο να τα αποκρύψουμε από πιθανούς εισβολείς. Για να επιτευχθεί αυτό θα πρέπει να μεταβούμε στα αρχεία αυτά και να προσθέσουμε τον παρακάτω κώδικα. [32]

Απενεργοποίηση πρόσβασης στο
.htaccess:

```
#Block access to .htaccess
<Files .htaccess>
order allow, deny
deny from all
</Files>
```

Απενεργοποίηση πρόσβασης στο
wp-config.php:

```
#Block access to wp-config.php
<Files wp-config.php>
order allow, deny
deny from all
</Files>
```

3.8 Αλλαγή του προθέματος wp_ της βάσης δεδομένων

Η βάση δεδομένων αποτελείται από πίνακες που το όνομά τους ξεκινάει με το πρόθεμα wp_ (π.χ. wp_links, wp_comments, wp_users, wp_posts κ.α.). Το πρόθεμα αυτό χρησιμοποιείται από προεπιλογή κατά την εγκατάσταση του WordPress, αν ο διαχειριστής δεν επιλέξει κάτι διαφορετικό. Επομένως οι επιτιθέμενοι είναι εύκολο να μαντέψουν το

όνομα του πίνακα και να προβούν σε επιθέσεις SQL injection. Η ασφάλεια της βάσης δεδομένων ενισχύεται αλλάζοντας το πρόθεμα wp_. [29, 31]

3.9 Απενεργοποίηση XML-RPC στο WordPress

Το XML-RPC είναι ένα πρωτόκολλο το οποίο επιτρέπει την απομακρυσμένη πρόσβαση και δημοσίευση άρθρων. Αν και χρήσιμο σε ορισμένες περιπτώσεις, είναι ένα χαρακτηριστικό το οποίο αποτελεί επίσης μεγάλο πρόβλημα στην ασφάλεια του WordPress. Με το XML-RPC, ένας χάκερ μπορεί να χρησιμοποιήσει τη λειτουργία system.multicall για να δοκιμάσει χιλιάδες κωδικούς πρόσβασης με 20 ή 50 αιτήματα, ας πούμε. Αν δεν δημοσιεύονται άρθρα με τη χρήση τρίτων εργαλείων και υπηρεσιών, τότε προτείνεται να απενεργοποιηθεί το XML-RPC για να αυξηθεί η ασφάλεια στο WordPress. Η απενεργοποίησή του μπορεί να γίνει με τα πρόσθετα, [Asset CleanUp: Page Speed Booster](#) και [Disable XML-RPC](#). [29, 31]

3.10 Αρχεία καταγραφής συμβάντων (Logging)

Ένα αρχείο καταγραφής συμβάντων (log file) φανερώνει τι έγινε, από ποιον και πότε. Καταγράφει την IP και τις ενέργειες που έκανε ο εισβολέας, χωρίς όμως να δώσει το όνομα χρήστη που συνδέθηκε. Μια επίθεση αφήνει πάντα ίχνη, είτε σε αρχεία καταγραφής ή στο σύστημα αρχείων. Μέσω των αρχείων καταγραφής αναγνωρίζονται επιθέσεις όπως - Cross Site Scripting (XSS), Remote File Inclusion (RFI), Local File Inclusion (LFI), προσπάθειες brute force attack κ.ά. Κάποια plugin που υποστηρίζουν αυτή την λειτουργία είναι, [WP Activity Log](#), [Activity Log](#), [Audit Trail](#), [Sucuri Auditing tool](#), [Defender Security – Malware Scanner](#), [Login Security & Firewall](#) κ.α. [32]

3.11 Απόκρυψη της έκδοσης του WordPress

Όσο λιγότερα γνωρίζει ένας επιτιθέμενος για την ιστοσελίδα τόσο πιο δύσκολο γίνεται το έργο του. Αν δεν γνωρίζει την έκδοση του WordPress που έχει εγκατασταθεί τότε δεν θα γνωρίζει και τα κενά ασφαλείας που μπορεί να την συνοδεύουν, ειδικά αν πρόκειται για παλαιότερη έκδοση, με αποτέλεσμα να μην μπορεί να έχει άμεσο στόχο. Για τον λόγο αυτό είναι καλή πρακτική να αποκρύπτεται η έκδοση, είτε προσθέτοντας τον παρακάτω κώδικα στο functions.php του theme:

```
/* Hide WP version strings from scripts and styles  
* @return {string} $src  
* @filter script_loader_src  
* @filter style_loader_src  
*/  
function remove_wp_version_strings( $src ) {  
    global $wp_version;
```

```

parse_str(parse_url($src, PHP_URL_QUERY), $query);
if ( !empty($query['ver']) && $query['ver'] === $wp_version ) {
    $src = remove_query_arg('ver', $src);
}
return $src;
}
add_filter( 'script_loader_src', 'remove_wp_version_strings' );
add_filter( 'style_loader_src', 'remove_wp_version_strings' );
/* Hide WP version strings from generator meta tag */
function remove_metatag_version() {
    return "";
}
add_filter('the_generator', 'remove_metatag_version');

```

Είτε μέσω κάποιου πρόσθετου όπως είναι το [Asset Cleanup: Page Speed Booster](#). Επίσης, καλό είναι να αφαιρεθεί και το αρχείο `readme.html` από τον κεντρικό φάκελο της εγκατάστασης, καθώς εμπεριέχει την έκδοση του WordPress. [29]

3.12 Έλεγχος και παρακολούθηση της ιστοσελίδας (Monitoring)

Ένα επόμενο μέτρο άμυνας απέναντι στις επιθέσεις είναι η ρύθμιση ενός συστήματος ελέγχου και παρακολούθησης που θα μπορεί να ανιχνεύσει ύποπτες κινήσεις στην ιστοσελίδα. Αυτό περιλαμβάνει την παρακολούθηση της ακεραιότητας των φακέλων, τις αποτυχημένες προσπάθειες σύνδεσης, την σάρωση για κακόβουλο λογισμικό και άλλα. Όσο πιο γρήγορα εντοπιστεί η απειλή τόσο πιο γρήγορη θα είναι η αντίδραση για την αντιμετώπισή της. Η εγκατάσταση ενός security plugin όπως τα [SiteAlert – Uptime, Speed, and Security Monitoring for WordPress](#), [Website File Changes Monitor](#), [Manage Backup & Monitor – WP Umbrella](#) [WordPress Monitoring & Automatic Backups](#) κ.α. μπορούν να βοηθήσουν σε αυτή την ενέργεια. [28,32]

3.13 Σάρωση για κακόβουλο λογισμικό και ευπάθειες

Παρόλα τα μέτρα ασφάλειας που μπορεί να πάρουμε και πάλι υπάρχουν πιθανότητες μια ιστοσελίδα να πέσει θύμα κάποιου κακόβουλου χρήστη. Γι' αυτό πρέπει να σαρώσουμε την ιστοσελίδα για τυχόν κακόβουλο λογισμικό (malware) και ευπάθειες (vulnerabilities). Αυτό μπορεί να γίνει με κάποιο plugin ασφάλειας. [28, 30]

3.14 Εγκατάσταση plugin ασφάλειας (Security Plugin)

Οι πιο πολλές από τις ενέργειες που αναφέραμε παραπάνω αλλά και ακόμη περισσότερες μπορούν να γίνουν με την εγκατάσταση ενός plugin ασφάλειας. Υπάρχουν

εκατοντάδες πρόσθετα ασφάλειας διαθέσιμα και ο προγραμματιστής μπορεί να αναζητήσει το κατάλληλο. Κάποια από αυτά αναφέρονται παρακάτω:

Wordfence Security: Από τα πιο δημοφιλή plugin ασφάλειας. Προσφέρει τείχος προστασίας που μπλοκάρει την κακόβουλη κίνηση, σάρωση για κακόβουλο περιεχόμενο, προστασία από επιθέσεις brute force περιορίζοντας τις προσπάθειες σύνδεσης. Επίσης προσφέρει ασφάλεια στην σύνδεση με έλεγχο ταυτότητας δύο παραγόντων (2FA), με προσθήκη CAPTCHA, απενεργοποίηση του XML-RPC κ.α.

Jetpack: Άλλο ένα δημοφιλές πρόσθετο. Προσφέρει αυτόματο real time backup, σάρωση για κακόβουλο περιεχόμενο, προστασία από επιθέσεις brute force, παρακολούθηση της κίνησης των χρηστών και του περιεχομένου, 2FA, αυτόματη αναβάθμιση μεμονομένων plugin κ.α.

All In One WP Security & Firewall: Ένα πρόσθετο που μειώνει τον κίνδυνο ασφάλειας ελέγχοντας για τρωτά σημεία και εφαρμόζοντας τις πιο πρόσφατες συνιστώμενες πρακτικές και τεχνικές ασφάλειας. Ενισχύει την ασφάλεια σύνδεσης των χρηστών, την ασφάλεια της βάσης δεδομένων, την ασφάλεια των φακέλων και των αρχείων. Προσφέρει firewall και προστασία από επιθέσεις brute force.

SiteGround Security: Περιορίζει τις προσπάθειες σύνδεσης, χρησιμοποιεί έλεγχο ταυτότητας δύο παραγόντων, αποκρύπτει την έκδοση του WordPress, απενεργοποιεί το XML-RPC, διαγράφει το αρχείο readme.txt, παρακολουθεί την δραστηριότητα των αρχείων καταγραφής συμβάντων (log files), σε περίπτωση επίθεσης αποσυνδέει όλους τους χρήστες και ζητάει επανέκδοση κωδικών.

iThemes Security: Μερικές από τις δωρεάν παροχές αυτού του πρόσθετου είναι η ασφάλεια σύνδεσης των χρηστών με 2FA και reCaptcha, η απόκρυψη του url σύνδεσης, έλεγχος των αδειών χρήσης των αρχείων, αντίγραφα ασφάλειας των βάσεων δεδομένων, παρακολούθηση για αλλαγές στα αρχεία, προστασία από επιθέσεις brute force.

Defender Security: Με λίγα μόνο κλικ και αυτό το πρόσθετο προσφέρει ενίσχυση στην ασφάλεια της ιστοσελίδας. Προστατεύει από επιθέσεις brute force, SQL injections, cross-site scripting XSS και άλλες ευπάθειες.

Shield Security: Μερικά από τα δωρεάν χαρακτηριστικά αυτού του πρόσθετου είναι η παρακολούθηση της δραστηριότητας, η απενεργοποίηση του XML-RPC, απενεργοποίηση επεξεργασίας αρχείων, εντόπιση πρόσθετων που δεν χρησιμοποιούνται, εντοπίζει και μπλοκάρει τα spam σχόλια, απόκρυψη του url σύνδεσης, χρήση firewall, εντοπίζει τα κακόβουλα ρομπότ που έχουν σχεδιαστεί για να στοχεύουν τα στοιχεία σύνδεσής σας στο WordPress, είτε με νόμιμα ονόματα χρήστη είτε με πλαστά ή άδεια ονόματα χρήστη.

BulletProof Security: Το επόμενο πρόσθετο προσφέρει επίσης ασφάλεια σύνδεσης χρηστών, firewall, σάρωση για κακόβουλο περιεχόμενο, παρακολούθηση ενεργειών των χρηστών και αλλαγών στα αρχεία, αποσύνδεση ανενεργών χρηστών, αλλαγή του προθέματος της βάσης δεδομένων, αντίγραφο ασφάλειας της βάσης δεδομένων, επιλογές αυτόματης ανανέωσης της εγκατάστασης WordPress, αρχεία καταγραφής συμβάντων.

Sucuri Security: Έλεγχος δραστηριότητας, παρακολούθηση ακεραιότητας αρχείων, απομακρυσμένη σάρωση κακόβουλου λογισμικού, παρακολούθηση λίστας αποκλεισμού, ενέργειες ασφάλειας μετά την παραβίαση, ειδοποιήσεις ασφάλειας και στην premium έκδοση παρέχει και firewall.

MalCare Security: Σάρωση και κατάργηση κακόβουλου λογισμικού, web application firewall, χρήση captcha για προστατευμένη σύνδεση.

4. ΜΕΘΟΔΟΛΟΓΙΑ ΕΡΕΥΝΑΣ

4.1 Ερευνητικά ερωτήματα

Για τον σχεδιασμό του ερωτηματολογίου χρειάστηκε να λάβουμε υπόψη τα ερευνητικά ερωτήματα που δημιουργήθηκαν και από το θεωρητικό μέρος της εργασίας. Τα ερωτήματα αυτά περιλαμβάνουν:

- ✚ Το εκπαιδευτικό υπόβαθρο των προγραμματιστών/διαχειριστών ιστοσελίδων και την εμπειρία τους.
- ✚ Το είδος των ιστοσελίδων που διαχειρίζονται και πόσο σημαντική θεωρούν την ασφάλεια της ιστοσελίδας.
- ✚ Επίσης ποιές πρακτικές χρησιμοποιούν για να διατηρήσουν τον ιστότοπό τους ασφαλή.
- ✚ Χρησιμοποιούν κάποιο plugin ασφάλειας; Αν ναι ποιο χρησιμοποιούν;

4.2 Σχεδιασμός ερωτηματολογίου

Το ερωτηματολόγιο το οποίο παρουσιάζεται στην συνέχεια χωρίστηκε σε 4 βασικές ενότητες ως εξής:

- ✚ Στην πρώτη ενότητα ζητούνται κάποια δημογραφικά χαρακτηριστικά όπως είναι το φύλο, η ηλικία, η εκπαίδευση και αν το αντικείμενο σπουδών είναι σχετικό με τον τομέα της Πληροφορικής.
- ✚ Στην δεύτερη ενότητα προσπαθούμε να αναζητήσουμε την εμπειρία των χρηστών στην δημιουργία και διαχείριση ιστοσελίδων WordPress.
- ✚ Στην τρίτη ενότητα τα ερωτήματα αφορούν τις πρακτικές ασφάλειας που χρησιμοποιούν οι διαχειριστές όπως η δημιουργία αντιγράφων ασφαλείας, η ενημέρωση της εγκατάστασης των plugins και των themes, η χρήση πιστοποιητικού SSL και WAF κ.α. Στο τέλος της ενότητας οι συμμετέχοντες καλούνται να απαντήσουν αν χρησιμοποιούν κάποιο plugin ασφάλειας. Αν απαντήσουν ΟΧΙ το ερωτηματολόγιο είναι έτοιμο προς υποβολή, ενώ αν απαντήσουν ΝΑΙ μεταφέρονται στην τέταρτη και τελευταία ενότητα.
- ✚ Στην τέταρτη ενότητα οι συμμετέχοντες καλούνται να απαντήσουν σε ερωτήσεις σχετικά με την χρήση των plugins.

4.3 Δείγμα έρευνας

Το δείγμα της έρευνας προέρχεται από την ομάδα της ελληνικής κοινότητας του WordPress στο Facebook, από επιχειρήσεις κατασκευής ιστοσελίδων σε Πάτρα, Αίγιο και Κέρκυρα και από μεμονωμένους προγραμματιστές που γνώριζε ή ερευνήτρια. Σύνολο συγκεντρώθηκαν 68 απαντήσεις.

4.4 Ερωτηματολόγιο

Στην συνέχεια παρατίθενται σε εικόνες το ερωτηματολόγιο.



Έρευνα χρήσης λογισμικού και plugin ασφάλειας στο Wordpress

Σας ευχαριστούμε για την πρόθεσή σας να συμμετάσχετε σε αυτήν την έρευνα που διενεργείται στο πλαίσιο της διπλωματικής μου εργασίας στο ΠΜΣ Ψηφιακές Εφαρμογές και Καινοτομία του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου.

Το ερωτηματολόγιο απευθύνεται σε προγραμματιστές, δημιουργούς ή διαχειριστές ιστοσελίδων Wordpress.

Σκοπός της έρευνας είναι η κατανόηση του βαθμού χρήσης πρακτικών ασφάλειας και εγκατάστασης λογισμικού και plugin για την ενίσχυση της ασφάλειας της ιστοσελίδας Wordpress. Δεν υπάρχουν σωστές ή λάθος απαντήσεις, καθώς μας ενδιαφέρουν μόνο οι πρακτικές που ακολουθείτε για την ενίσχυση της ασφάλειας στο wordpress.

Η έρευνα περιλαμβάνει τη συμπλήρωση 21 ερωτήσεων. Η χρονική διάρκεια που θα απαιτηθεί για τη συμπλήρωση όλων των ερωτήσεων είναι περίπου 5 λεπτά.

Επισημαίνεται ότι το ερωτηματολόγιο και η επεξεργασία των απαντήσεων είναι ανώνυμα και πραγματοποιούνται από την φοιτήτρια αποκλειστικά στο πλαίσιο της διπλωματικής της εργασίας.

Ευχαριστούμε για το χρόνο και τη συνεισφορά σας.

Δημογραφικά στοιχεία

Φύλο

- ☐ Άνδρας
- ☐ Γυναίκα
- ☐ Δεν απαντώ

Ηλικία

- ☐ Κάτω από 18
- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65+

Εκπαίδευση *

- ☐ Δημοτικό
- ☐ Γυμνάσιο/ Λύκειο
- ☐ ΙΕΚ
- ☐ ΑΕΙ/ ΤΕΙ
- ☐ Μεταπτυχιακό/Διδακτορικό

Αντικείμενο σπουδών *

- ☐ Πληροφορική
- ☐ Άλλο

[Πίσω](#)

[Επόμενο](#)



Σελίδα 2 από 5

Εκκαθάριση
φόρμας

Εμπειρία

Κατασκευάζετε ή διαχειρίζεστε ιστοσελίδες Wordpress *

- ☐ Επαγγελματικά
- ☐ Ερασιτεχνικά

Εμπειρία στην κατασκευή ιστοσελίδων Wordpress *

- ☐ Έχω δημιουργήσει ή διαχειριστεί από 1 έως 5 ιστοσελίδες
- ☐ Έχω δημιουργήσει ή διαχειριστεί από 6 έως 15 ιστοσελίδες
- ☐ Έχω δημιουργήσει ή διαχειριστεί από 16 έως 30 ιστοσελίδες
- ☐ Έχω δημιουργήσει ή διαχειριστεί από 31 ιστοσελίδες και πάνω

Ποιο είναι το είδος της ιστοσελίδας που διαχειρίζεστε; *

- ☐ Blog
- ☐ Εταιρική
- ☐ E-shop
- ☐ Άλλο: _____

Πίσω

Επόμενο

Σελίδα 3 από 5

Εκκαθάριση
φόρμας

Ασφάλεια στις ιστοσελίδες Wordpress

1. Πόσο σημαντική πιστεύετε ότι είναι η ενίσχυση της ασφάλειας στην ιστοσελίδα Wordpress; *

	1	2	3	4	5	
Καθόλου σημαντική	☐	☐	☐	☐	☐	Πολύ σημαντική

2. Κάθε πότε ενημερώνετε την εγκατάσταση του Wordpress, τα themes και τα plugins; *

- ☐ Αμέσως μόλις βγει νέα έκδοση
- ☐ Λίγες ημέρες αφότου βγει η νέα έκδοση
- ☐ Δεν τα ενημερώνω
- ☐ Άλλο: _____

3. Κάθε πότε δημιουργείτε αντίγραφα ασφάλειας (Backups); *

- ☐ Κάθε λεπτό (Live backup)
- ☐ Μια φορά την ημέρα
- ☐ Μία φορά την εβδομάδα
- ☐ Μία φορά τον μήνα
- ☐ Δεν κρατάω αντίγραφα ασφάλειας
- ☐ Άλλο: _____

4. Χρησιμοποιείτε πιστοποιητικό SSL; *

- ☐ Ναι, χρησιμοποιώ το δωρεάν πιστοποιητικό "Let's Encrypt"
- ☐ Ναι, χρησιμοποιώ ένα αγορασμένο πιστοποιητικό SSL
- ☐ Όχι, δεν χρησιμοποιώ

5. Χρησιμοποιείτε Web Application Firewall (WAF); *

☐ ΝΑΙ

☐ ΟΧΙ

6. Ποια από τις παρακάτω ενέργειες για την ασφάλεια σύνδεσης των διαχειριστών ή/και των χρηστών εκτελείτε; *

☐ Πολιτικές ασφάλειας στην δημιουργία κωδικών πρόσβασης

☐ Αλλαγή του ονόματος χρήστη "admin"

☐ Ερώτηση ασφάλειας κατά την σύνδεση

☐ Έλεγχος ταυτότητας δύο παραγόντων (Two Factor Authentication - 2FA)

☐ Περιορισμός προσπαθειών σύνδεσης

☐ Αλλαγή του URL εισόδου στην διαχείριση

☐ Τίποτα από τα παραπάνω

☐ Άλλο: _____

7. Ποια από τις παρακάτω πρακτικές εφαρμόζετε για την ασφάλεια των αρχείων; *

☐ Απενεργοποίηση επεξεργασίας αρχείων

☐ Απενεργοποίηση εκτέλεσης της PHP σε συγκεκριμένους φακέλους (πχ /wp-includes, /wp-content/uploads)

☐ Απενεργοποίηση εμφάνισης καταλόγου αρχείων (directory listing)

☐ Απόκρυψη αρχείων wp-config και .htaccess

☐ Τίποτα από τα παραπάνω

☐ Άλλο: _____

8. Ποια από τις παρακάτω πρακτικές ασφάλειας εφαρμόζετε; *

- ☐ Σάρωση για κακόβουλο λογισμικό και ευπάθειες
- ☐ Έλεγχος και παρακολούθηση της ιστοσελίδας (Monitoring)
- ☐ Αρχεία καταγραφής συμβάντων (Logging)
- ☐ Απόκρυψη της έκδοσης του WordPress
- ☐ Αυτόματη αποσύνδεση ανενεργών χρηστών
- ☐ Αλλαγή του προθέματος wp_ της βάσης δεδομένων
- ☐ Απενεργοποίηση XML-RPC
- ☐ Τίποτα από τα παραπάνω
- ☐ Άλλο: _____

9. Χρησιμοποιείτε κάποιο plugin ασφάλειας; *

☐ ΝΑΙ

☐ ΟΧΙ

[Πίσω](#)[Επόμενο](#)

Σελίδα 4 από 5

[Εκκαθάριση φόρμας](#)

Αν η απάντηση είναι ΟΧΙ τότε γίνεται υποβολή του ερωτηματολογίου. Αν η απάντηση είναι ΝΑΙ ο χρήστης μεταφέρεται στην επόμενη και τελευταία ενότητα!

Plugin Ασφάλειας

10. Ποιο ή ποια από τα παρακάτω plugins ασφάλειας χρησιμοποιείτε; *

- ☐ Wordfence Security
- ☐ Jetpack
- ☐ All In One WP Security & Firewall
- ☐ SiteGround Security
- ☐ iThemes Security
- ☐ Defender Security
- ☐ Shield Security
- ☐ BulletProof Security
- ☐ Sucuri Security
- ☐ MalCare Security
- ☐ Κανένα από τα παραπάνω

11. Ποιο από τα παρακάτω plugins χρησιμοποιείτε για διαχείριση ασφαλών κωδικών πρόσβασης; *

- ☐ Password Strength Settings for WooCommerce
- ☐ Password Policy Manager
- ☐ Χρησιμοποιώ ένα all-in-one security plugin που περιέχει αυτή την λειτουργία.
- ☐ Δεν χρησιμοποιώ κάποιο
- ☐ Άλλο: _____

12. Ποιο από τα παρακάτω plugins χρησιμοποιείτε για την διατήρηση αντιγράφων ασφαλείας; *

- ☐ UpdraftPlus WordPress Backup Plugin
- ☐ BackWPup – WordPress Backup Plugin
- ☐ Backup & Staging – BlogVault Backups
- ☐ Duplicator – WordPress Migration Plugin
- ☐ Χρησιμοποιώ ένα all-in-one security plugin που περιέχει αυτή την λειτουργία.
- ☐ Δεν χρησιμοποιώ κάποιο
- ☐ Άλλο: _____

13. Ποιο από τα παρακάτω plugins χρησιμοποιείτε για σάρωση για κακόβουλο λογισμικό, ιούς και ευπάθειες; *

- ☐ AntiVirus
- ☐ WP Cerber Security, Anti-spam & Malware Scan
- ☐ Titan Anti-spam & Security
- ☐ MalCare Security
- ☐ Χρησιμοποιώ ένα all-in-one security plugin που περιέχει αυτή την λειτουργία.
- ☐ Δεν χρησιμοποιώ κάποιο
- ☐ Άλλο: _____

14. Ποιο από τα plugins ασφαλείας που χρησιμοποιείτε δεν αναφέρεται στις προηγούμενες ερωτήσεις;

Η απάντησή σας _____

[Πίσω](#)

[Υποβολή](#)

Σελίδα 5 από 5

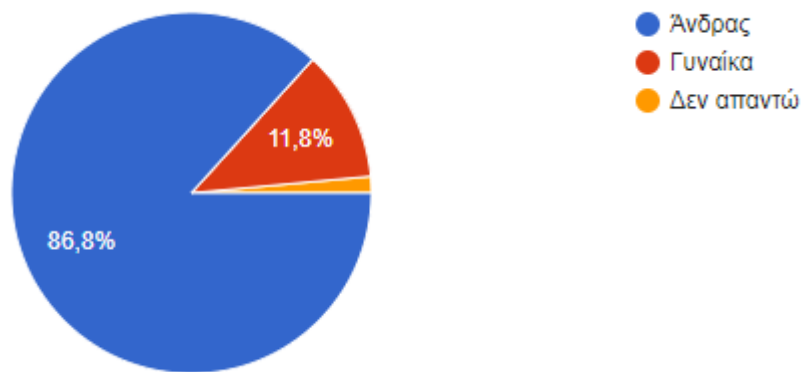
Εκκαθάριση
φόρμας

5. ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΡΕΥΝΑΣ

Σε αυτό το κεφάλαιο θα παρουσιαστούν τα αποτελέσματα της έρευνας με ερωτηματολόγιο χρησιμοποιώντας περιγραφική στατιστική.

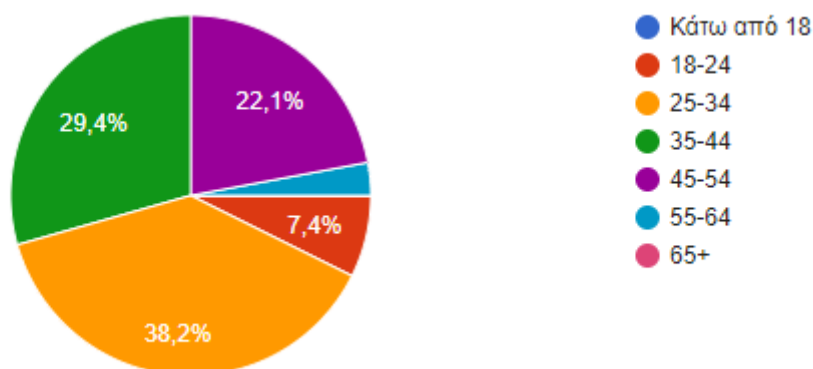
1^η Ενότητα: Δημογραφικά στοιχεία

Ξεκινώντας με τα δημογραφικά στοιχεία, όπως θα δούμε στο παρακάτω διάγραμμα, το μεγαλύτερο ποσοστό των συμμετεχόντων είναι άνδρες σε ποσοστό 86,8%, ενώ οι γυναίκες φτάνουν μόλις στο 11,8%.



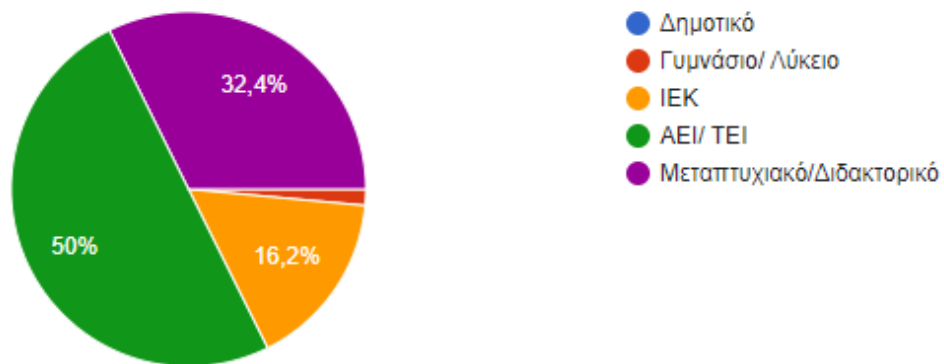
Διάγραμμα 1: Φύλο

Οι ηλικίες των συμμετεχόντων κυμαίνονται από 18 έτη έως 64 έτη, με το μεγαλύτερο μέρος να ανήκει στις ηλικίες 25-34 σε ποσοστό 38,2% (26 άτομα) και ακολουθούν οι ηλικίες 35-44 σε ποσοστό 29,4% (20 άτομα). Το μικρότερο ποσοστό μόλις 2,9% (2 άτομα) ανήκει στις ηλικίες 55-64.



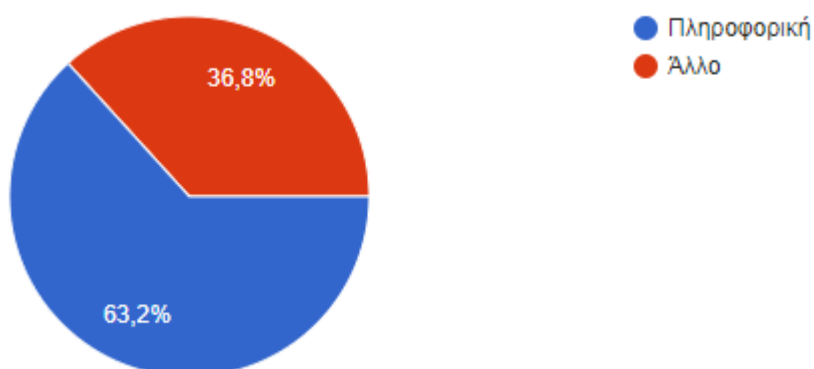
Διάγραμμα 2: Ηλικία

Όσον αφορά την εκπαίδευση των συμμετεχόντων, πρόκειται για υψηλό επίπεδο κατάρτισης καθώς σε ποσοστό 50% (34 άτομα) είναι απόφοιτοι ΑΕΙ/ΤΕΙ, ενώ σε ποσοστό 32,4% (22 άτομα) είναι κάτοχοι Μεταπτυχιακού/Διδακτορικού. Σε ποσοστό 16,2% (11 άτομα) είναι απόφοιτοι ΙΕΚ, ενώ μόλις το 1,5% (1 άτομο) είναι απόφοιτος Γυμνασίου/Λυκείου.



Διάγραμμα 3: Εκπαίδευση

Από αυτούς το μεγαλύτερο ποσοστό 63,2% (43 άτομα) έχουν αντικείμενο σπουδών την Πληροφορική, ενώ το 36,8% (25 άτομα) έχουν άλλο αντικείμενο σπουδών.



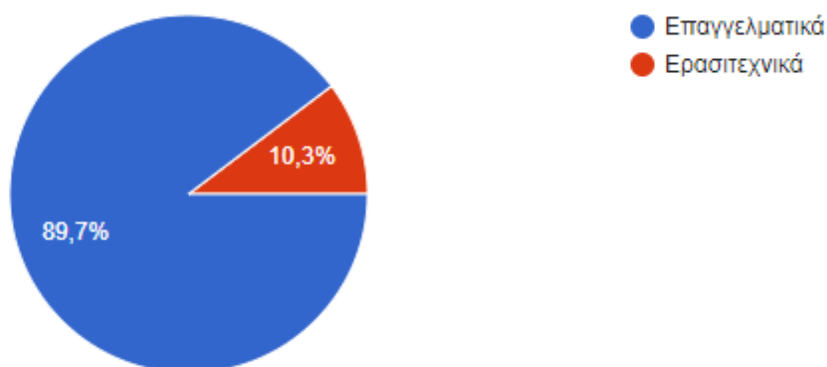
Διάγραμμα 4: Αντικείμενο Σπουδών

2^η Ενότητα: Εμπειρία

Στην επόμενη ενότητα αναζητάμε να μάθουμε την εμπειρία που έχουν οι συμμετέχοντες στην δημιουργία και διαχείριση ιστοσελίδων, αν είναι επαγγελματίες ή

ερασιτέχνες, καθώς και το είδος των ιστοσελίδων που διαχειρίζονται. Αυτό θα μας βοηθήσει να βγάλουμε συμπεράσματα για το κατά πόσο οι δύο κατηγορίες χρησιμοποιούν πρακτικές και plugin ασφάλειας.

Στο πρώτο διάγραμμα αυτής της ενότητας βλέπουμε ότι το 89,7% (61 άτομα) των συμμετεχόντων στην έρευνα δημιουργούν ή διαχειρίζονται ιστοσελίδες WordPress επαγγελματικά ενώ μόλις το 10,3% (7 άτομα) είναι ερασιτέχνες.



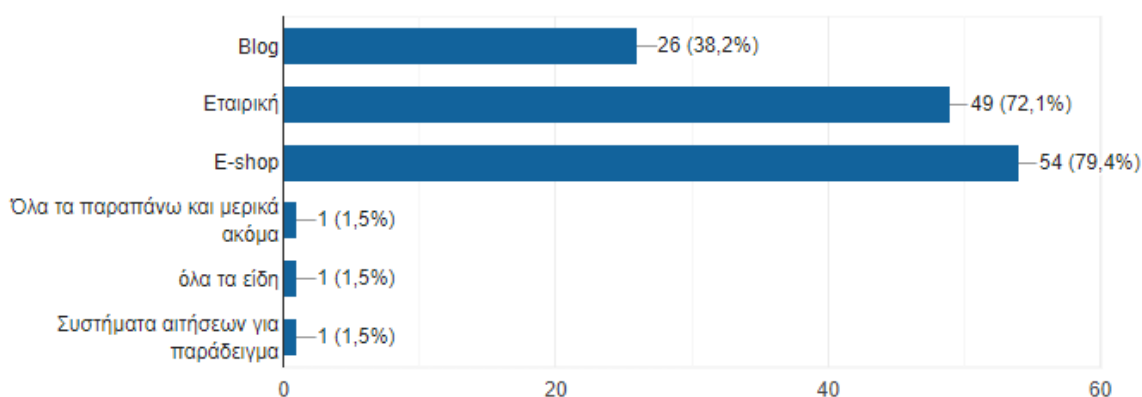
Διάγραμμα 5: Κατασκευάζετε ή διαχειρίζετε ιστοσελίδες WordPress

Στην συνέχεια ρωτήσαμε τους συμμετέχοντες σχετικά με τον αριθμό των ιστοσελίδων που έχουν δημιουργήσει ή διαχειριστεί για να κατανοήσουμε καλύτερα το επίπεδο της εμπειρίας τους. Έτσι, σε ποσοστό 54,4% (37 άτομα) απάντησαν ότι έχουν δημιουργήσει ή διαχειριστεί πάνω από 30 ιστοσελίδες, που σημαίνει ότι έχουν μεγάλη εμπειρία. Ακολουθούν σε ποσοστό 17,6% (12 άτομα) όσοι έχουν διαχειριστεί από 16 έως 30 ιστοσελίδες και σε ποσοστό 11,8% (8 άτομα) όσοι έχουν διαχειριστεί από 6 έως 15 ιστοσελίδες. Τέλος το ποσοστό με την μικρότερη εμπειρία είναι της τάξης του 16,2% (11 άτομα) που έχουν δημιουργήσει από 1 έως 5 ιστοσελίδες.



Διάγραμμα 6: Εμπειρία στην κατασκευή ιστοσελίδων WordPress

Η τελευταία ερώτηση αυτής της ενότητας αφορά το είδος των ιστοσελίδων που διαχειρίζονται οι προγραμματιστές. Όπως βλέπουμε στο παρακάτω διάγραμμα το 79,4% αφορά στην διαχείριση eshop, το 72,1% στην διαχείριση εταιρικών ιστοσελίδων και το 38,2 στην διαχείριση blog. Υπήρξαν ακόμα τρεις απαντήσεις που αναφέρουν ότι διαχειρίζονται όλα τα είδη ιστοσελίδων καθώς και συστήματα αιτήσεων.

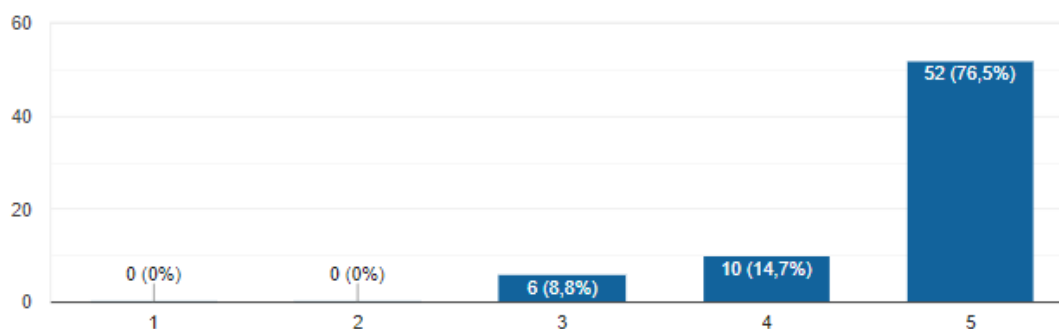


Διάγραμμα 7: Ποιο είναι το είδος της ιστοσελίδας που διαχειρίζεστε;

3^η Ενότητα: Ασφάλεια στις ιστοσελίδες WordPress

Σε αυτή την ενότητα τα αποτελέσματα έδειξαν κατά πόσο οι προγραμματιστές ή διαχειριστές ιστοσελίδων WordPress χρησιμοποιούν πρακτικές για να ενισχύσουν την ασφάλεια των ιστοσελίδων τους.

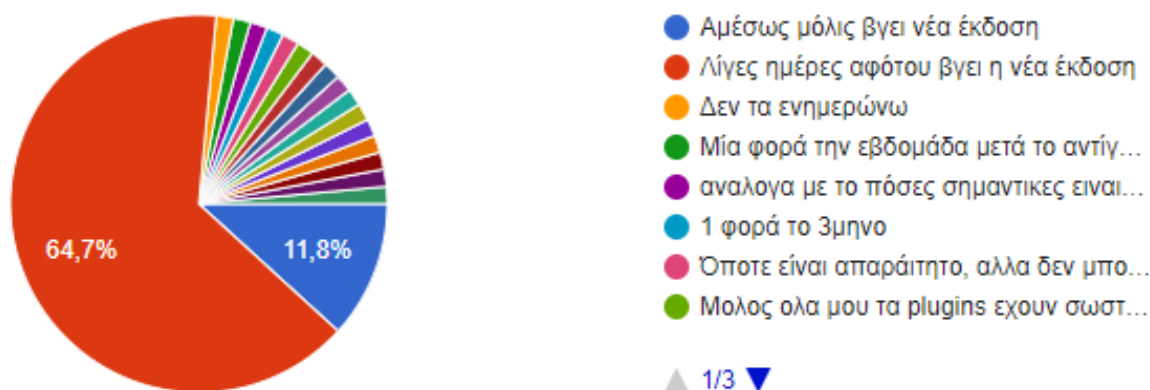
Αρχικά έγινε μια αναγνωριστική ερώτηση για να κατανοήσουμε πως βλέπουν οι διαχειριστές την ασφάλεια. Αν δηλαδή την θεωρούν σημαντική ή όχι. Τα αποτελέσματα έδειξαν ότι οι περισσότεροι από αυτούς την θεωρούν εξαιρετικά σημαντική και αυτό είναι ένα πολύ ενθαρρυντικό στοιχείο. Πιο συγκεκριμένα το 76,5% απάντησε ότι θεωρεί πολύ σημαντική την ασφάλεια της ιστοσελίδας ενώ το 14,7% και το 8,8% λιγότερο σημαντική.



Διάγραμμα 8: Πόσο σημαντική πιστεύετε ότι είναι η ενίσχυση της ασφάλειας στην ιστοσελίδα WordPress; (1- Καθόλου, 5- Πολύ)

Η επόμενη ερώτηση αφορά την ενημέρωση της εφαρμογής WordPress, των themes και των plugins. Οι συμμετέχοντες έπρεπε να απαντήσουν ποιός είναι ο χρόνος στον οποίο γίνονται οι ενημερώσεις (updates) στα παραπάνω. Αν γίνεται αμέσως μόλις βγει νέα έκδοση, λίγες μέρες μετά ή καθόλου. Εδώ το ερωτηματολόγιο συγκέντρωσε πλήθος απαντήσεων πέραν των καθορισμένων. Πιο αναλυτικά σε ποσοστό 64,7% (44 άτομα) απάντησαν ότι εγκαθιστούν τις ενημερώσεις λίγες ημέρες αφότου βγει νέα έκδοση. Αμέσως μετά με ποσοστό 11,8% (8 άτομα) έρχεται η απάντηση ότι οι ενημερώσεις γίνονται αμέσως μόλις βγει νέα έκδοση, ενώ μόλις το 1,5% (1 άτομο) απάντησε ότι δεν εγκαθιστά καθόλου ενημερώσεις. Στην συνέχεια είχαμε 15 μεμονωμένες διαφορετικές απαντήσεις σε ποσοστό 1,5% η κάθε μία, οι οποίες έχουν ως εξής:

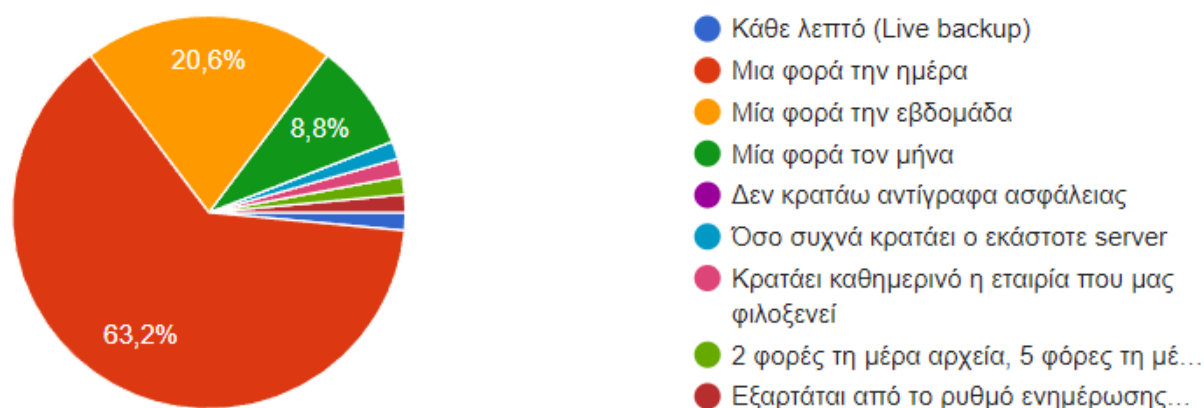
- ✓ Μια φορά τον χρόνο με τη συμφωνία του πελάτη.
- ✓ Αφού πρώτα δοκιμαστεί κάποια έκδοση και περίπου 3 μήνες μετά.
- ✓ Όταν υπάρχουν διορθώσεις κενών ασφαλείας και όταν οι εκδόσεις είναι stable.
- ✓ 1-2 φορές τον χρόνο.
- ✓ 1-6 μήνες.
- ✓ Στην αρχή τού νέου Μήνα.
- ✓ Σε μηνιαία βάση.
- ✓ Εφόσον τα κάνω test σε τοπική εγκατάσταση.
- ✓ Μια φορά το εξάμηνο.
- ✓ Plugins σε μεγάλα updates, WordPress σπάνια γιατί σπάνε πράγματα.
- ✓ Μόλις όλα μου τα plugins έχουν σωστή και επιβεβαιωμένη υποστήριξη από το theme και την έκδοση του wp.
- ✓ Όποτε είναι απαραίτητο, αλλά δεν μπορείς σε όλα τα Website να ψάχνεις κάθε μέρα ποιό έχει updates. Δεν θα κάνεις άλλη δουλειά μετά.
- ✓ 1 φορά το 3μηνο.
- ✓ Ανάλογα με το πόσες σημαντικές είναι οι ενημερώσεις.
- ✓ Μία φορά την εβδομάδα μετά το αντίγραφο ασφαλείας.



Διάγραμμα 9: Κάθε πότε ενημερώνετε την εγκατάσταση του WordPress, τα themes και τα plugins;

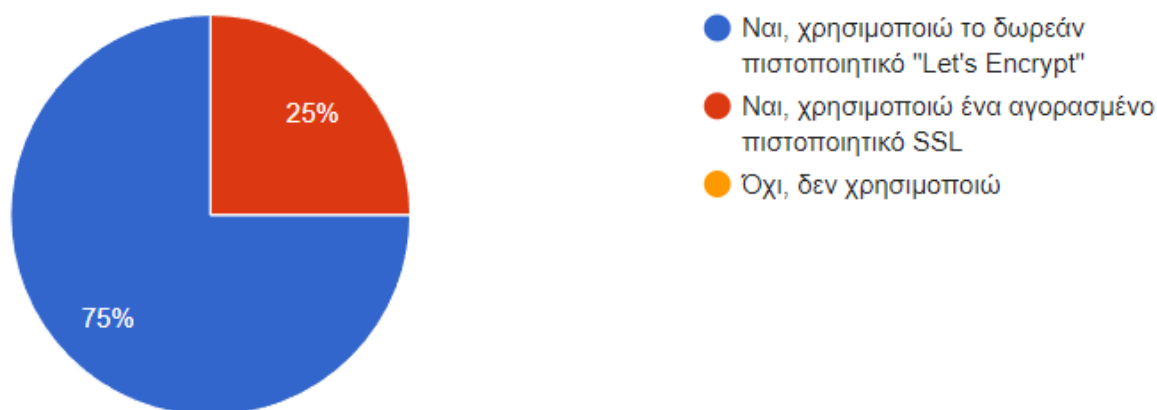
Η επόμενη ερώτηση αφορά την δημιουργία αντιγράφων ασφαλείας (backups). Το 63,2% (43 άτομα) απάντησαν ότι κρατούν αντίγραφα ασφαλείας μια φορά την ημέρα, ενώ το 20,6% (14 άτομα) μία φορά την εβδομάδα. Ένα μικρότερο ποσοστό των ερωτηθέντων μόλις 8,8% (6 άτομα) συγκεντρώνουν αντίγραφα ασφαλείας μια φορά τον μήνα, ενώ μόλις το 1,5% (1 άτομο) παίρνει αντίγραφα κάθε λεπτό (Live Backup). Επίσης είχαμε ακόμα 4 απαντήσεις σε ποσοστό 1,5% όπως αναφέρονται στην συνέχεια:

- ✓ Όσο συχνά κρατάει ο εκάστοτε server.
- ✓ Κρατάει καθημερινό η εταιρία που μας φιλοξενεί.
- ✓ 2 φορές τη μέρα αρχεία, 5 φορές τη μέρα βάσεις.
- ✓ Εξαρτάται από το ρυθμό ενημέρωσης περιεχομένου του site.



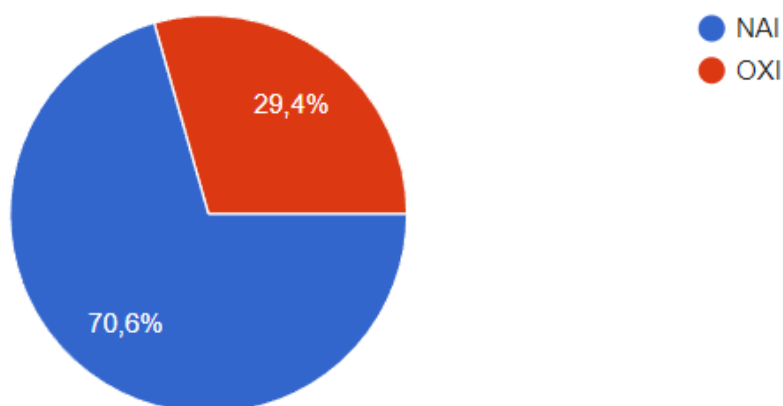
Διάγραμμα 10: Κάθε πότε δημιουργείτε αντίγραφα ασφαλείας (Backups);

Στην συνέχεια ρωτήσαμε τους συμμετέχοντες αν χρησιμοποιούν κάποιο πιστοποιητικό SSL. Σε ποσοστό 75% (51 άτομα) απάντησαν ότι χρησιμοποιούν το δωρεάν πιστοποιητικό «Let's Encrypt», ενώ το 25% (17 άτομα) απάντησαν ότι έχουν αγοράσει κάποιο πιστοποιητικό SSL. Με τον έναν ή τον άλλο τρόπο όλοι οι συμμετέχοντες το χρησιμοποιούν, κανένας δεν απάντησε ότι δεν το χρησιμοποιεί. Βέβαια το δωρεάν πιστοποιητικό δεν είναι τόσο αξιόπιστο όταν πρόκειται για συναλλαγές, σε αυτές τις περιπτώσεις θα ήταν καλύτερα ένα αγορασμένο SSL. [34] Δεδομένου ότι το 79% των συμμετεχόντων διαχειρίζονται eshop ίσως αυτή να μην είναι μια καλή πρακτική.



Διάγραμμα 11: Χρησιμοποιείτε πιστοποιητικό SSL;

Επόμενο σημαντικό στοιχείο για την ασφάλεια της ιστοσελίδας αποτελεί το Web Application Firewall (WAF). Το 70,6% (48 άτομα) απάντησε ότι χρησιμοποιεί WAF, ενώ το 29,4% (20 άτομα) δεν χρησιμοποιεί.

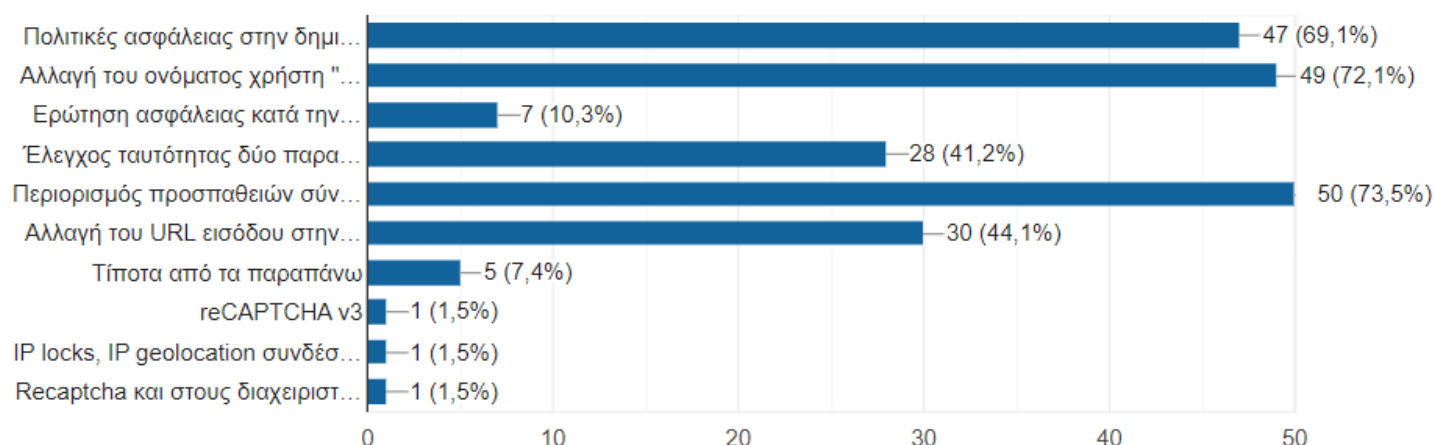


Διάγραμμα 12: Χρησιμοποιείτε Web Application Firewall (WAF);

Υπάρχουν κάποιες ενέργειες που μπορούν να κάνουν οι διαχειριστές για να εξασφαλίσουν την ασφαλή σύνδεση την δική τους αλλά και των χρηστών. Στο παρακάτω διάγραμμα βλέπουμε ποιές από αυτές εκτελούν περισσότερο οι διαχειριστές. Πιο συγκεκριμένα ο περιορισμός προσπαθειών σύνδεσης (Limit Login Attempts) συγκεντρώνει το μεγαλύτερο ποσοστό 73,5%, ακολουθεί η αλλαγή του ονόματος χρήστη "admin" με ποσοστό 72,1% και οι πολιτικές ασφάλειας στην δημιουργία κωδικών πρόσβασης με ποσοστό 69,1%. Λιγότερο εκτελούν οι διαχειριστές την αλλαγή του URL εισόδου στην διαχείριση με ποσοστό 44,1% και τον έλεγχο ταυτότητας δύο παραγόντων με ποσοστό 41,2%. Ερώτηση ασφάλειας κατά την σύνδεση χρησιμοποιεί μόνο το 10,3%, ενώ ένα

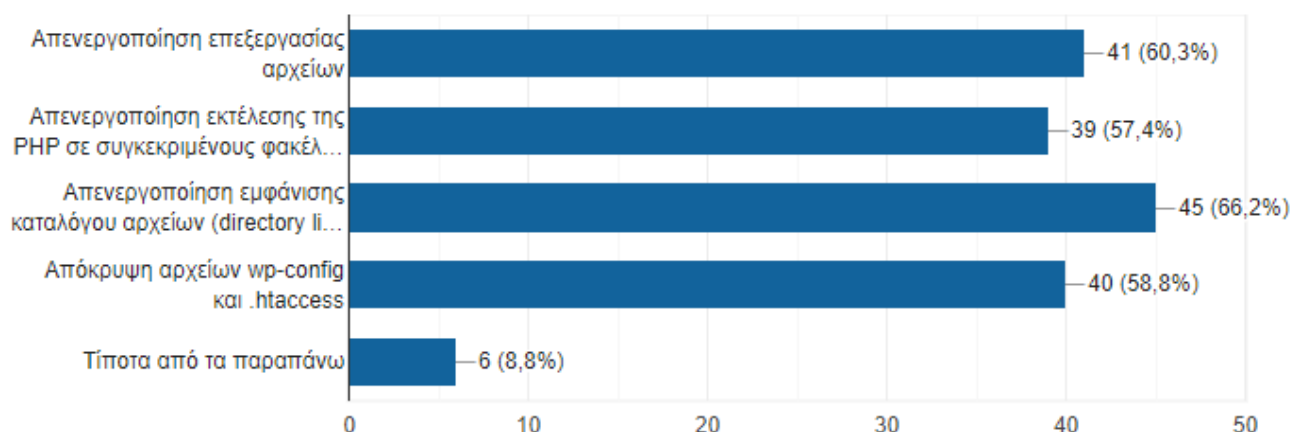
ποσοστό 7,4% δεν εκτελεί καμία από τις παραπάνω ενέργειες. Τέλος, είχαμε και 3 επιπλέον απαντήσεις με ποσοστό 1,5% όπως αναφέρονται παρακάτω:

- ✓ reCAPTCHA v3
- ✓ IP locks, IP geolocation συνδέσεις μόνο από Ελλάδα
- ✓ Recaptcha και στους διαχειριστές κλειδωμά wr admin



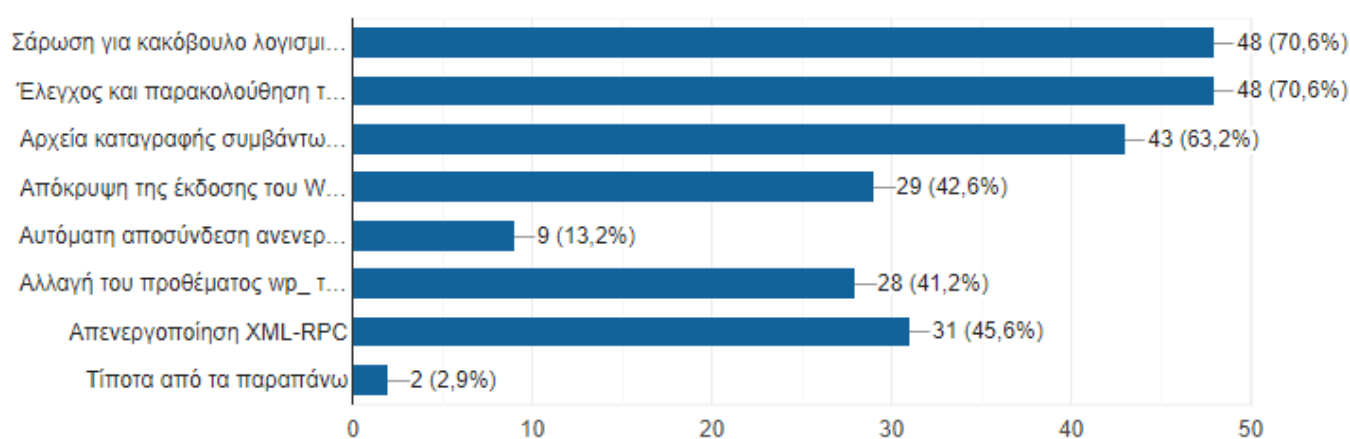
Διάγραμμα 13: Ποια από τις παρακάτω ενέργειες για την ασφάλεια σύνδεσης των διαχειριστών ή/και των χρηστών εκτελείτε;

Επίσης υπάρχουν πρακτικές που αφορούν την ασφάλεια των αρχείων και την αποτροπή πρόσβασης σε αυτά των κακόβουλων χρηστών. Όπως φάνηκε από την έρευνα οι περισσότεροι διαχειριστές εκτελούν αυτές τις ενέργειες, με πιο δημοφιλή την απενεργοποίηση εμφάνισης καταλόγου αρχείων (directory listing) σε ποσοστό 66,2%. Η απενεργοποίηση επεξεργασίας αρχείων είναι μια πρακτική που επίσης χρησιμοποιείται σε ποσοστό 60,3%, ενώ ακολουθεί η απόκρυψη των αρχείων wp-config και .htaccess σε ποσοστό 58,8%. Άλλη μια πρακτική που χρησιμοποιείται σε ποσοστό 57,4% είναι η απενεργοποίηση εκτέλεσης της PHP σε συγκεκριμένους φακέλους (πχ /wp-includes, /wp-content/uploads). Τέλος, ένα μικρό ποσοστό των συμμετεχόντων, το 8,8% απάντησε ότι δεν χρησιμοποιεί καμία από τις παραπάνω πρακτικές.



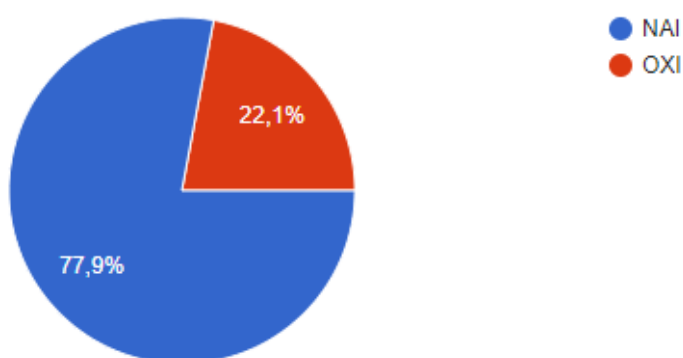
Διάγραμμα 14: Ποια από τις παρακάτω πρακτικές εφαρμόζετε για την ασφάλεια των αρχείων;

Στην επόμενη ερώτηση αναφέρονται ακόμα κάποιες σημαντικές πρακτικές ασφάλειας με τις πιο δημοφιλείς σε χρήση να είναι η σάρωση για κακόβουλο λογισμικό και ο έλεγχος και η παρακολούθηση της ιστοσελίδας (monitoring) με ποσοστό 70,6%. ακολουθούν τα αρχεία καταγραφής συμβάντων με ποσοστό 63,2% και η απενεργοποίηση XML-RPC με ποσοστό 45,6%. Ακόμα δύο καλές πρακτικές ασφάλειας που χρησιμοποιούν σε μικρότερο ποσοστό οι διαχειριστές είναι η απόκρυψη της έκδοσης του WordPress (42,6%) και η αλλαγή του προθέματος wp_ της βάσης δεδομένων (41,2%). Το μικρότερο ποσοστό (13,2%) συγκέντρωσε η λειτουργία της αυτόματης αποσύνδεσης ανενεργών χρηστών. Τέλος το 2,9% των συμμετεχόντων απάντησαν ότι δεν χρησιμοποιούν καμία από τις παραπάνω πρακτικές.



Διάγραμμα 15: Ποια από τις παρακάτω πρακτικές ασφάλειας εφαρμόζετε;

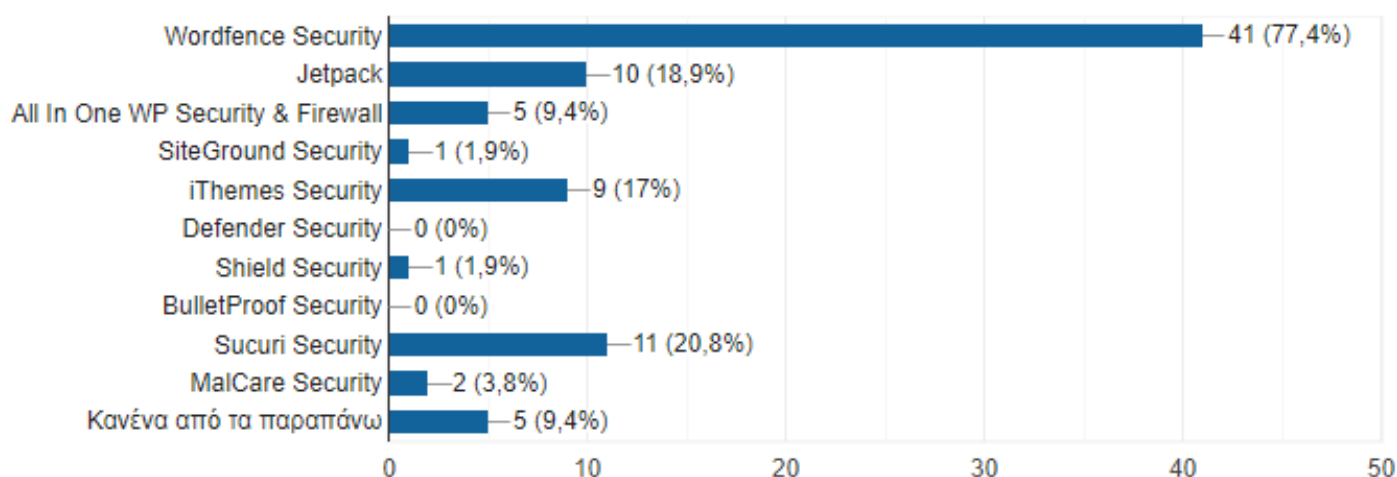
Στην τελευταία ερώτηση της τρίτης ενότητας οι συμμετέχοντες στην έρευνα έπρεπε να απαντήσουν αν έχουν εγκαταστήσει στην ιστοσελίδα στους κάποιο plugin ασφάλειας. Για όσους απάντησαν «Όχι» το ερωτηματολόγιο ήταν έτοιμο για υποβολή. Όσοι απάντησαν «Ναι» προχώρησαν και στην τελευταία και τέταρτη ενότητα του ερωτηματολογίου η οποία αφορά την χρήση των plugins. Όπως φαίνεται και στο διάγραμμα που ακολουθεί το 77,9% (53 άτομα) απάντησαν ότι χρησιμοποιούν κάποιο plugin ασφάλειας, ενώ το 22,1% (15 άτομα) δεν χρησιμοποιεί.



Διάγραμμα 16: Χρησιμοποιείτε κάποιο plugin ασφάλειας

4^η Ενότητα: Plugin Ασφάλειας

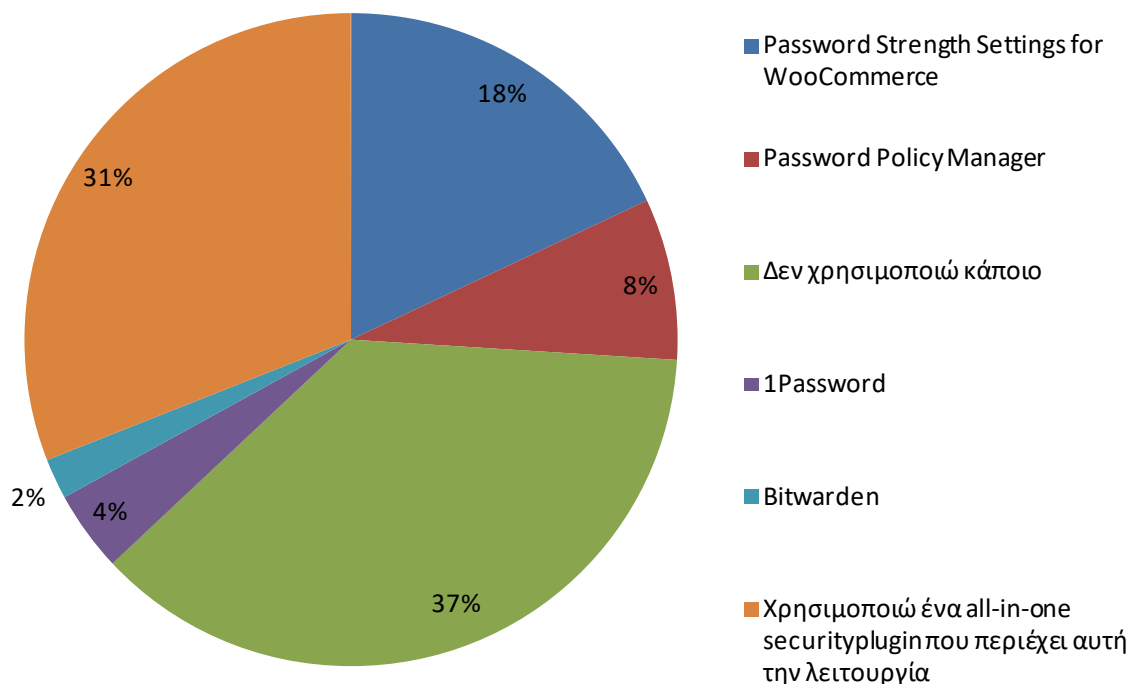
Αρχικά οι συμμετέχοντες κλήθηκαν να απαντήσουν αν χρησιμοποιούν κάποιο από τα plugins ασφάλειας που αναγράφονται στο διάγραμμα 17. Το πιο δημοφιλές πρόσθετο ασφάλειας που χρησιμοποιεί το 77,4% των διαχειριστών είναι το Wordfence Security. Ακολουθεί το Sucuri Security (20,8%), το Jetpack (18,9%) και το iThemes Security (17%).



Διάγραμμα 17: Ποιο ή ποια από τα παρακάτω plugins ασφάλειας χρησιμοποιείτε;

Η επόμενη ερώτηση αφορά τα πρόσθετα διαχείρισης ασφαλών κωδικών πρόσβασης. Το μεγαλύτερο ποσοστό (37% - 21 άτομα) των συμμετεχόντων απάντησαν ότι δεν χρησιμοποιούν κάποιο, ενώ το 31% (16 άτομα) απάντησε ότι χρησιμοποιεί ένα all-in-one plugin που περιέχει αυτή την λειτουργία. Επόμενο σε χρήση εργαλείο είναι το Password Strength Settings for WooCommerce με ποσοστό 18% (9 άτομα) και το Password Policy Manager με ποσοστό 8% (4 άτομα). Τέλος κάποιοι συμμετέχοντες έδωσαν κάποιες επιπλέον απαντήσεις, δύο εξ αυτών απάντησαν ότι χρησιμοποιούν το 1Password και ένας απάντησε ότι χρησιμοποιεί το Bitwarden.

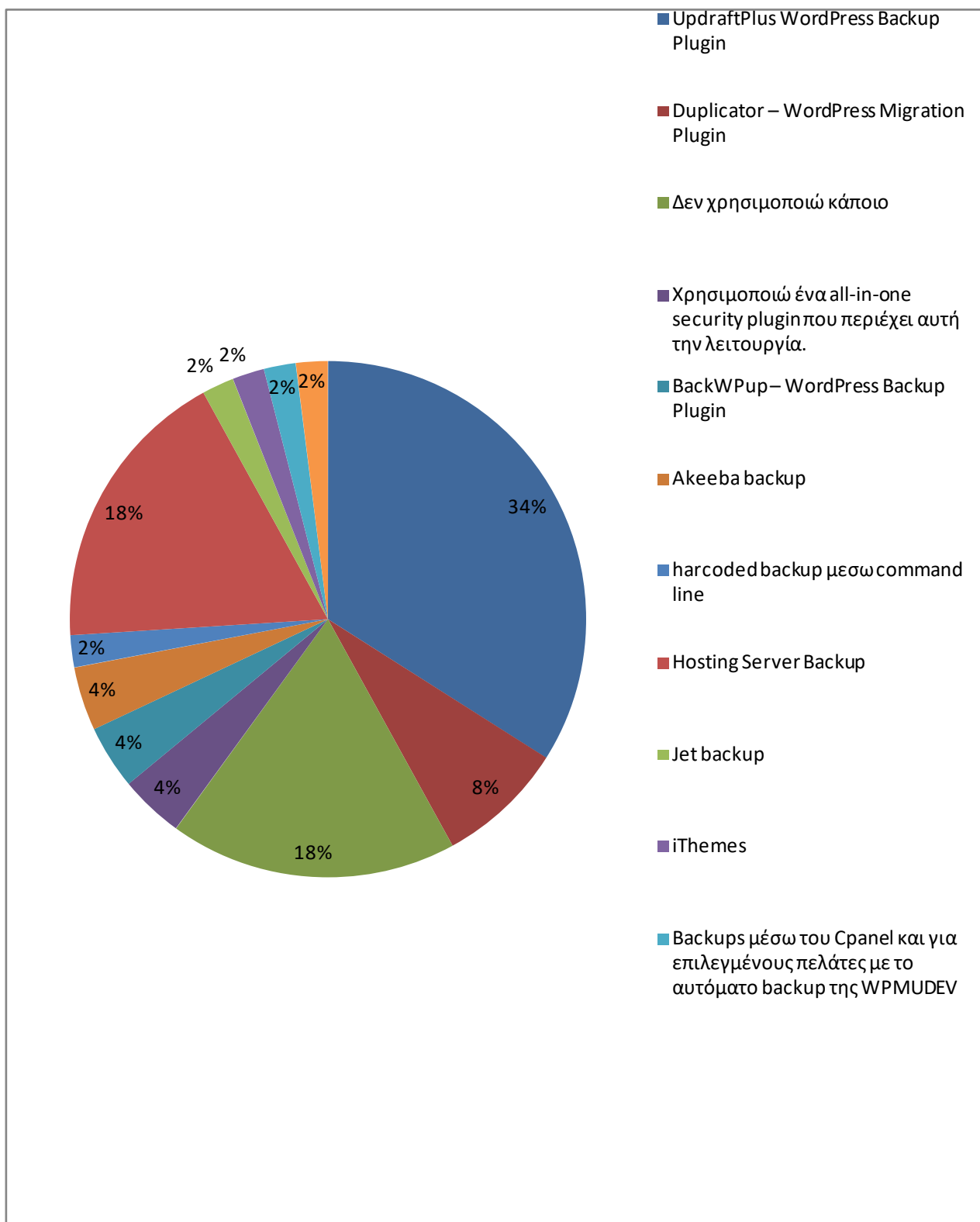
Ποιο από τα παρακάτω plugins χρησιμοποιείτε για διαχείριση ασφαλών κωδικών πρόσβασης;



Διάγραμμα 18: Ποιο plugin χρησιμοποιείτε για διαχείριση ασφαλών κωδικών πρόσβασης;

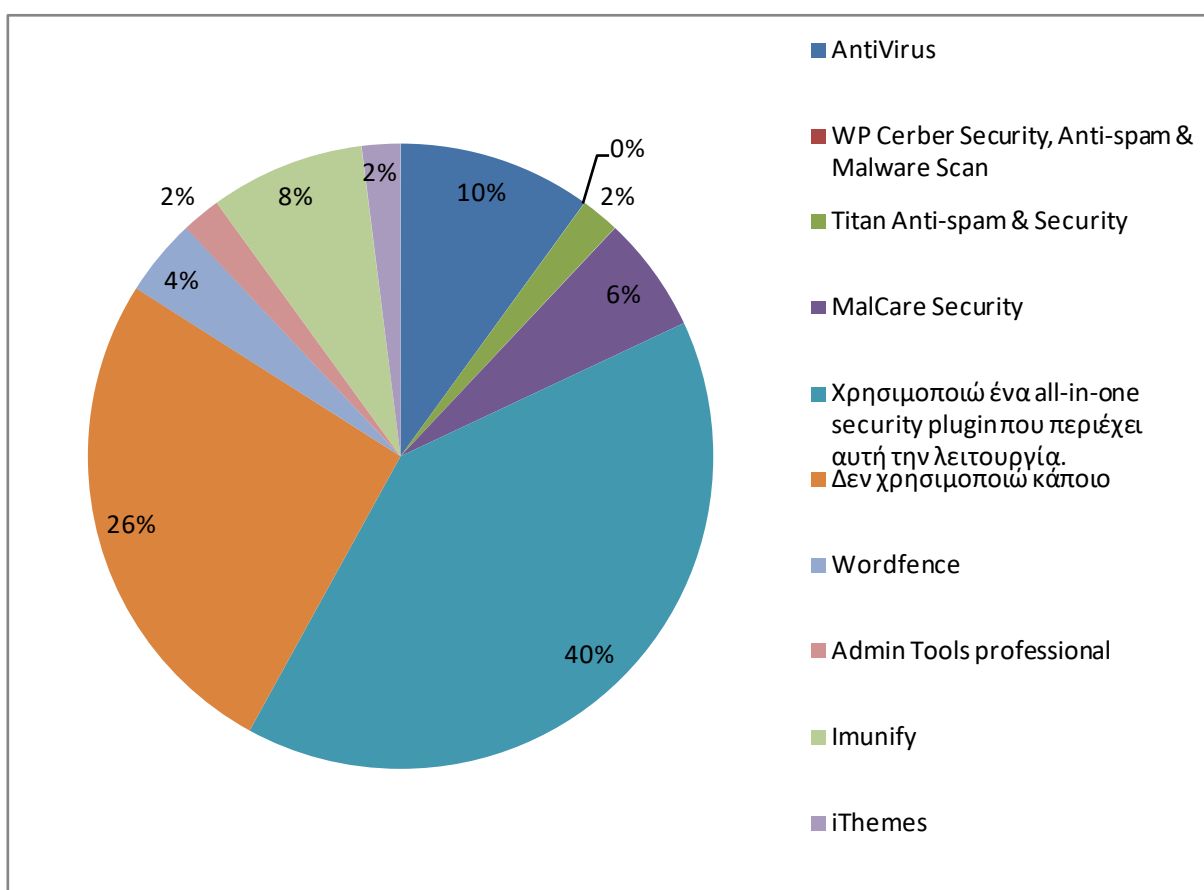
Στην συνέχεια οι συμμετέχοντες ρωτήθηκαν για τα πρόσθετα που χρησιμοποιούν για την δημιουργία και διατήρηση αντιγράφων ασφάλειας. Το μεγαλύτερο ποσοστό (34%) των συμμετεχόντων απάντησαν ότι χρησιμοποιούν το «UpdraftPlus WordPress Backup Plugin». Αρκετοί ήταν αυτοί που απάντησαν ότι δεν χρησιμοποιούν κάποιο σε ποσοστό 18%. Επίσης, σε ποσοστό 18% απάντησαν ότι χρησιμοποιούν το «Hosting Server Backup», δηλαδή την custom λύση που προτείνει ο hosting provider του καθενός. Επόμενο σε σειρά έρχεται το «Duplicator – WordPress Migration Plugin» με ποσοστό 8%, ενώ ακολουθεί με ποσοστό 4% το «BackWPup – WordPress Backup Plugin» και το «Akeeba backup» με το ίδιο ποσοστό. Επίσης το 4% των διαχειριστών απάντησαν ότι χρησιμοποιούν ένα all-in-one security plugin που περιέχει αυτή την λειτουργία. Τέλος πήραμε ακόμα πέντε απαντήσεις με ποσοστό 2% η κάθε μία, οι οποίες έχουν ως εξής:

- ✓ Hardcored backup μέσω command line
- ✓ Jet backup
- ✓ iThemes
- ✓ Backups μέσω του Cpanel και για επιλεγμένους πελάτες με το αυτόματο backup της WPMUDEV
- ✓ BackupPC σε τρίτο server αποκλειστικά για backups, και ένα custom wp-cli script για τα backup της βάσης.



Διάγραμμα 19: Ποιο plugin χρησιμοποιείτε για την διατήρηση αντιγράφων ασφαλείας

Η επόμενη ερώτηση αφορά τα plugins που χρησιμοποιούνται για σάρωση για κακόβουλο λογισμικό, ιούς και ευπάθειες. Όπως φαίνεται και στο διάγραμμα το μεγαλύτερο ποσοστό (40% - 20 άτομα) απάντησε ότι χρησιμοποιεί ένα all-in-one security plugin που περιέχει αυτή την λειτουργία. Ενώ το 26% (13 άτομα) απάντησε ότι δεν χρησιμοποιεί κάποιο plugin για αυτή την λειτουργία. Το 10% (5 άτομα) των συμμετεχόντων απάντησε ότι χρησιμοποιεί το «AntiVirus», ενώ το 8% (4 άτομα) το «Imunify». Ακόμα το 6% (3 άτομα) έχει εγκαταστήσει το plugin «MalCare Security», ενώ το 4% (2 άτομα) το «Wordfence». Τέλος σε ποσοστό 2% χρησιμοποιούνται τα plugins «Admin Tools professional», «Titan Anti-spam & Security» και «iThemes Security» αντίστοιχα.



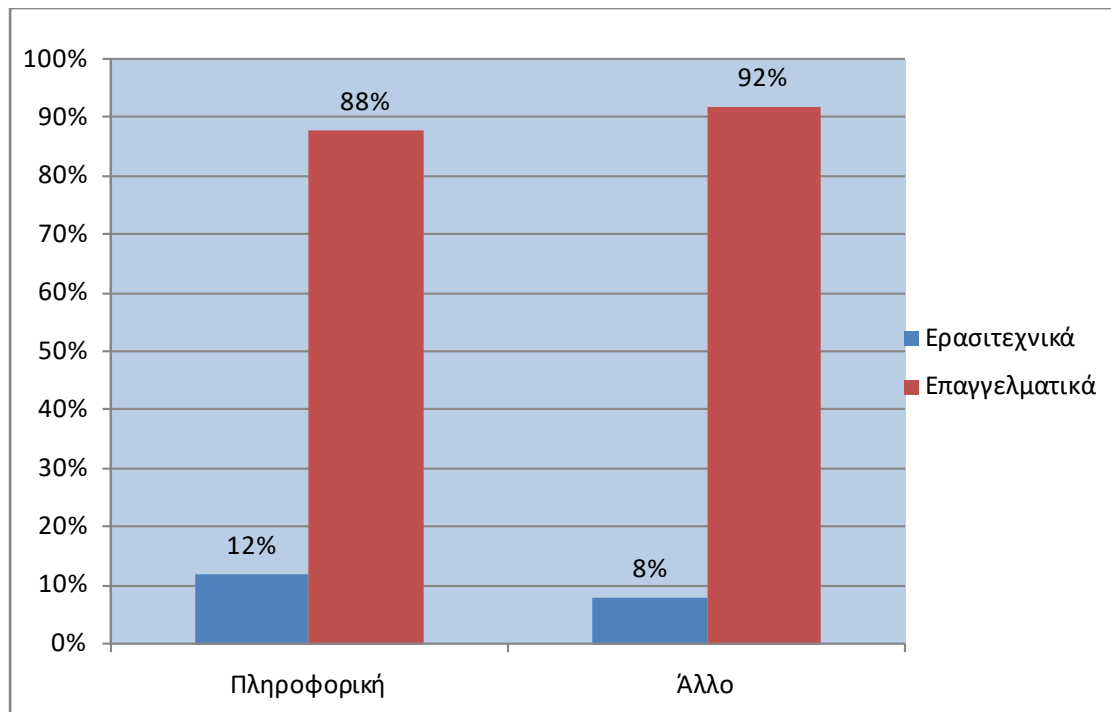
Διάγραμμα 20: Ποιο plugin χρησιμοποιείτε για σάρωση για κακόβουλο λογισμικό, ιούς και ευπάθειες;

Στην τελευταία ερώτηση του ερωτηματολογίου ζητήσαμε από τους συμμετέχοντες να μας αναφέρουν πιο plugin ασφάλειας χρησιμοποιούν το οποίο δεν αναφέρθηκε σε όλες τις προηγούμενες ερωτήσεις. Οι απαντήσεις που λάβαμε έχουν ως εξής:

- ✓ Akeeba Admin Tools
- ✓ WPMUDEV Defender Pro
- ✓ Ninja Firewall
- ✓ ImmunifyAV
- ✓ Limit Login Attempts
- ✓ Ninja

Και ακόμα μερικά αποτελέσματα...

Όπως βλέπουμε στο παρακάτω διάγραμμα από τους 68 συμμετέχοντες στην έρευνα, οι 38 έχουν αντικείμενο σπουδών την πληροφορική και ασχολούνται επαγγελματικά με την δημιουργία και διαχείριση ιστοσελίδων, ενώ οι 23 έχουν άλλο αντικείμενο σπουδών αλλά ασχολούνται επαγγελματικά και αυτοί.

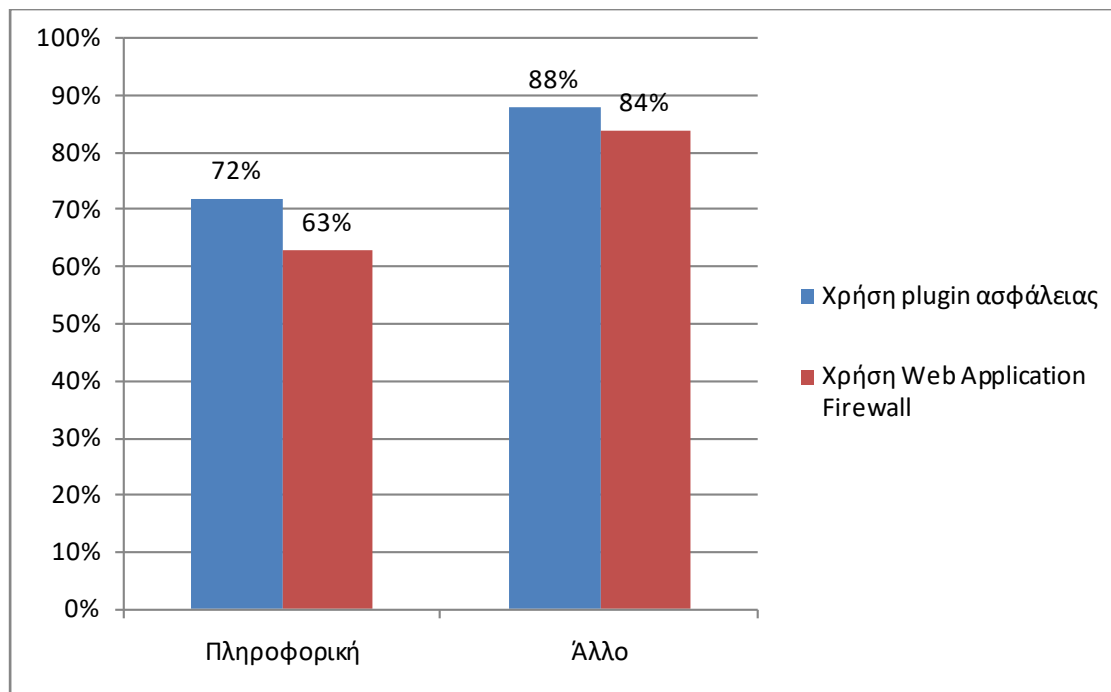


Διάγραμμα 21: Αντικείμενο σπουδών σε σχέση με το είδος ενασχόλησης

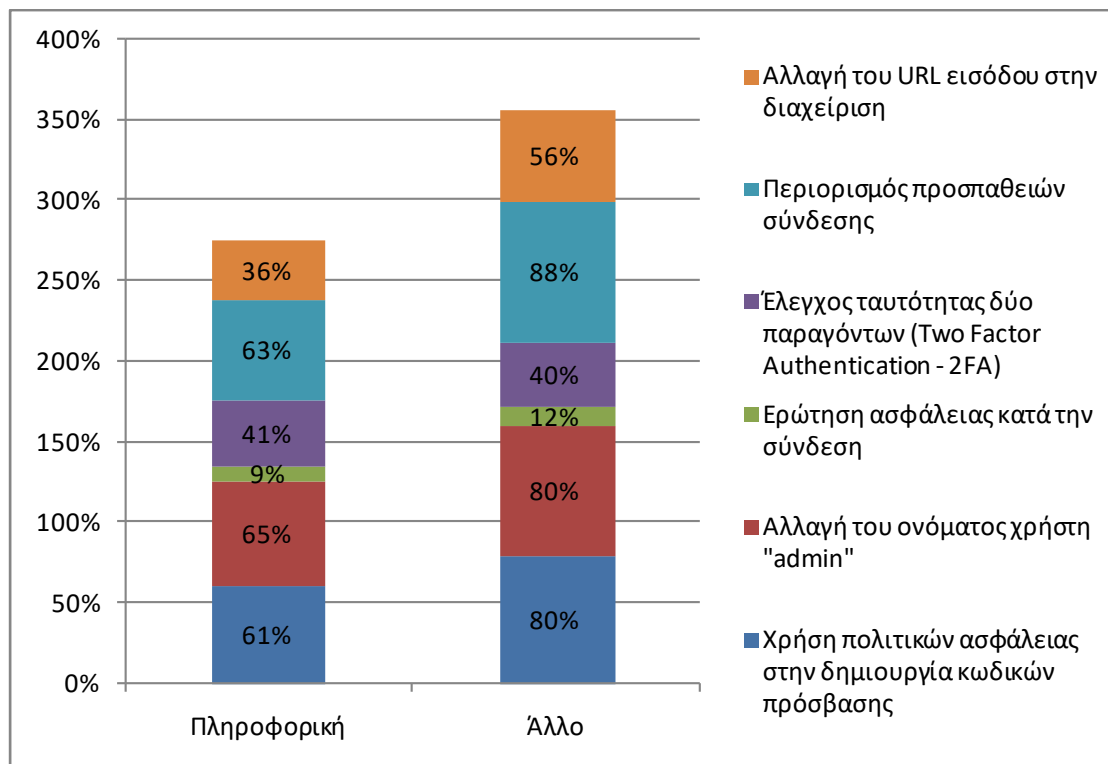
Όσον αφορά το «security awareness» των συμμετεχόντων σε σχέση με το αντικείμενο σπουδών, όπως θα δούμε και στα διαγράμματα που ακολουθούν, όσοι δήλωσαν ότι το αντικείμενο σπουδών τους είναι άλλο από αυτό της πληροφορικής, έχουν μεγαλύτερη ευαισθητοποίηση για την ασφάλεια σε σχέση με όσους δήλωσαν ότι το αντικείμενο σπουδών τους είναι η πληροφορική. Όπως φαίνεται στο διάγραμμα 22, το 88% όσων απάντησαν ότι έχουν άλλο αντικείμενο σπουδών, χρησιμοποιεί plugin ασφάλειας. Ενώ το ποσοστό όσων απάντησαν ότι έχουν αντικείμενο σπουδών την πληροφορική, είναι 72%.

Επίσης οι έχοντες αντικείμενο σπουδών «Άλλο» χρησιμοποιούν Web Application Firewall σε ποσοστό 84%, ενώ το αντίστοιχο ποσοστό όσων έχουν αντικείμενο σπουδών «Πληροφορική» είναι 63%.

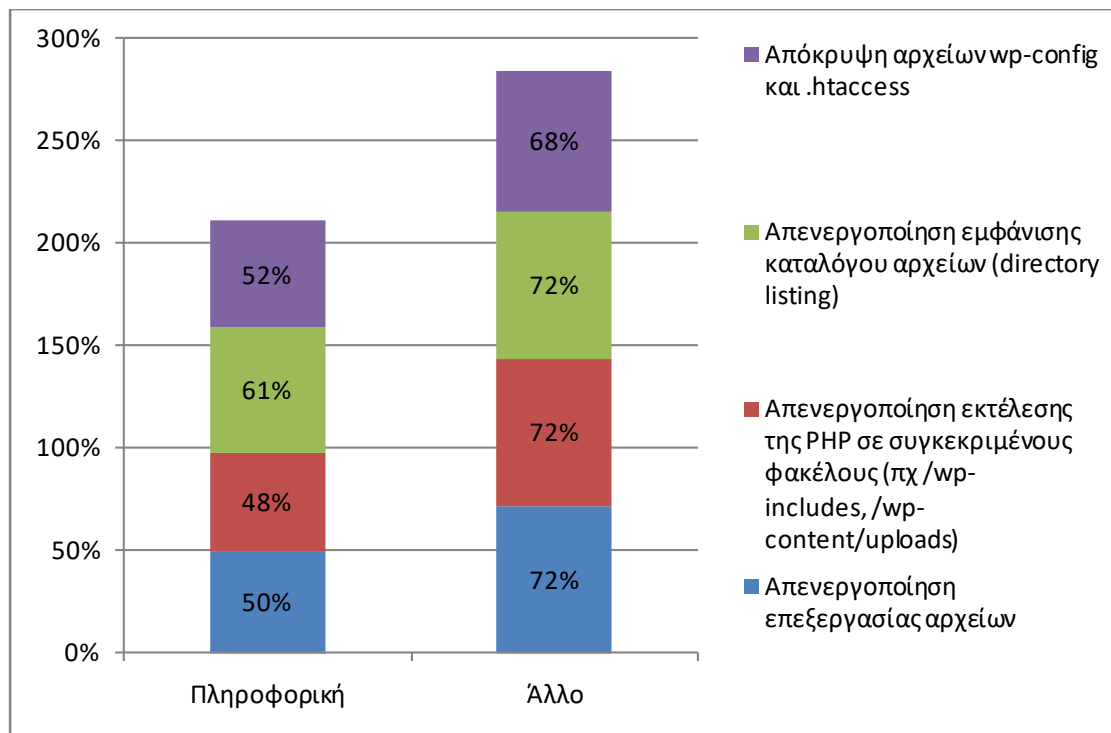
Αντίστοιχα και στα επόμενα διαγράμματα 23, 24, 25, βλέπουμε ότι το όσοι απάντησαν ότι έχουν άλλο αντικείμενο σπουδών χρησιμοποιούν περισσότερες πρακτικές ασφάλειας (hardening techniques) από όσους απάντησαν ότι έχουν αντικείμενο σπουδών την Πληροφορική.



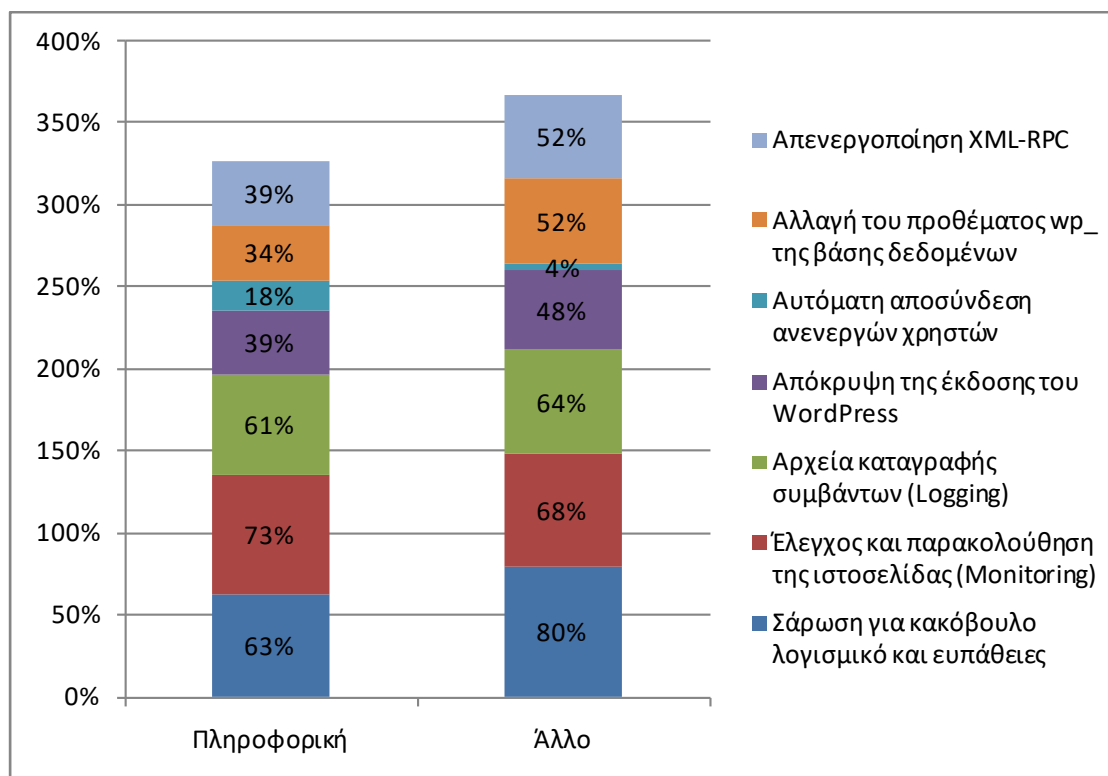
Διάγραμμα 22: Αντικείμενο σπουδών σε σχέση με την χρήση WAF και plugin ασφάλειας



Διάγραμμα 23: Αντικείμενο σπουδών σε σχέση με την εκτέλεση ενεργειών για ασφάλεια κατά την σύνδεση

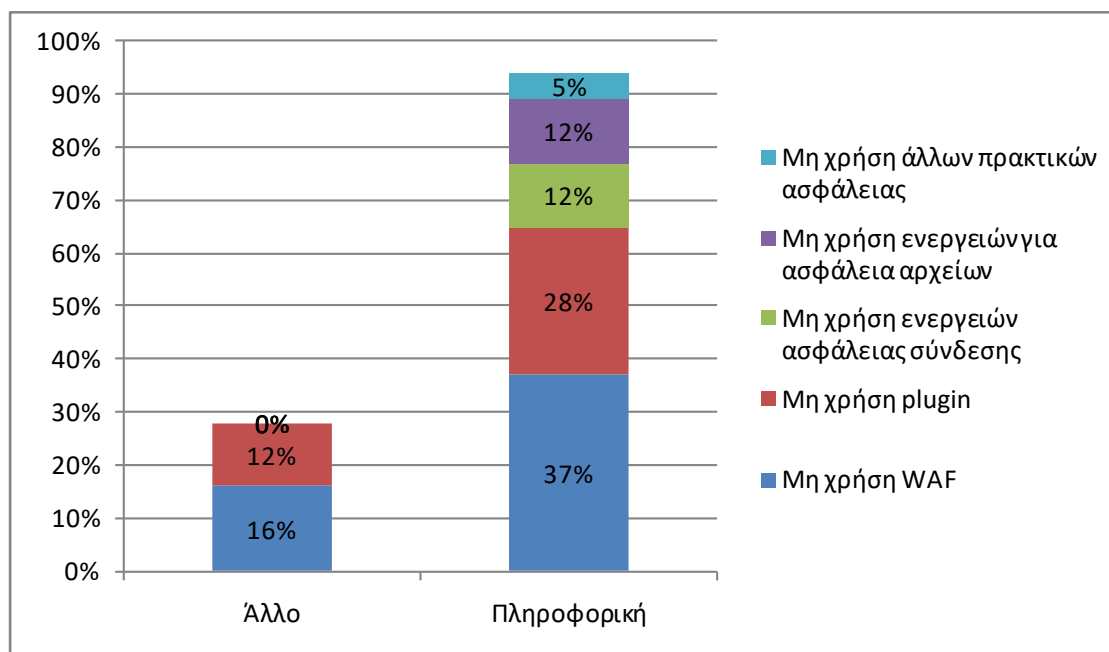


Διάγραμμα 24: Αντικείμενο σπουδών σε σχέση με την εκτέλεση ενεργειών για ασφάλεια των αρχείων



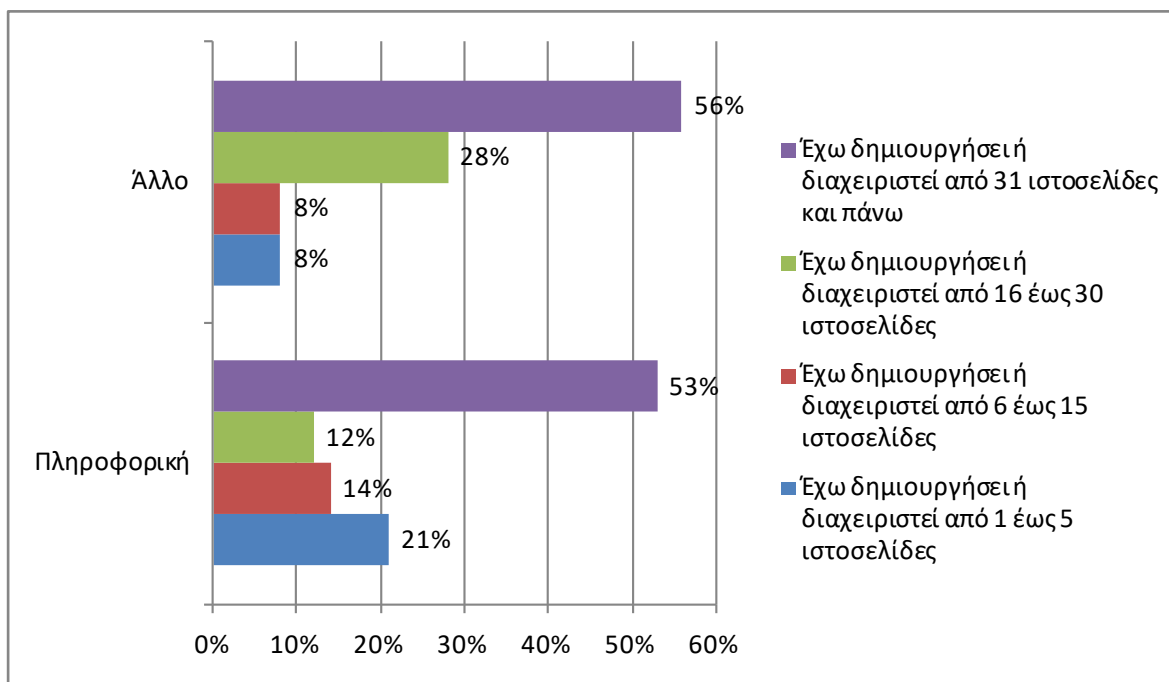
Διάγραμμα 25: Αντικείμενο σπουδών σε σχέση με την χρήση πρακτικών ασφάλειας

Στο επόμενο διάγραμμα 26, βλέπουμε αντίστοιχα τα ποσοστά όσων απάντησαν ότι δεν χρησιμοποιούν καθόλου hardening techniques σε σχέση με το αντικείμενο σπουδών τους. Οι έχοντες αντικείμενο σπουδών την πληροφορική έχουν υψηλότερα ποσοστά.



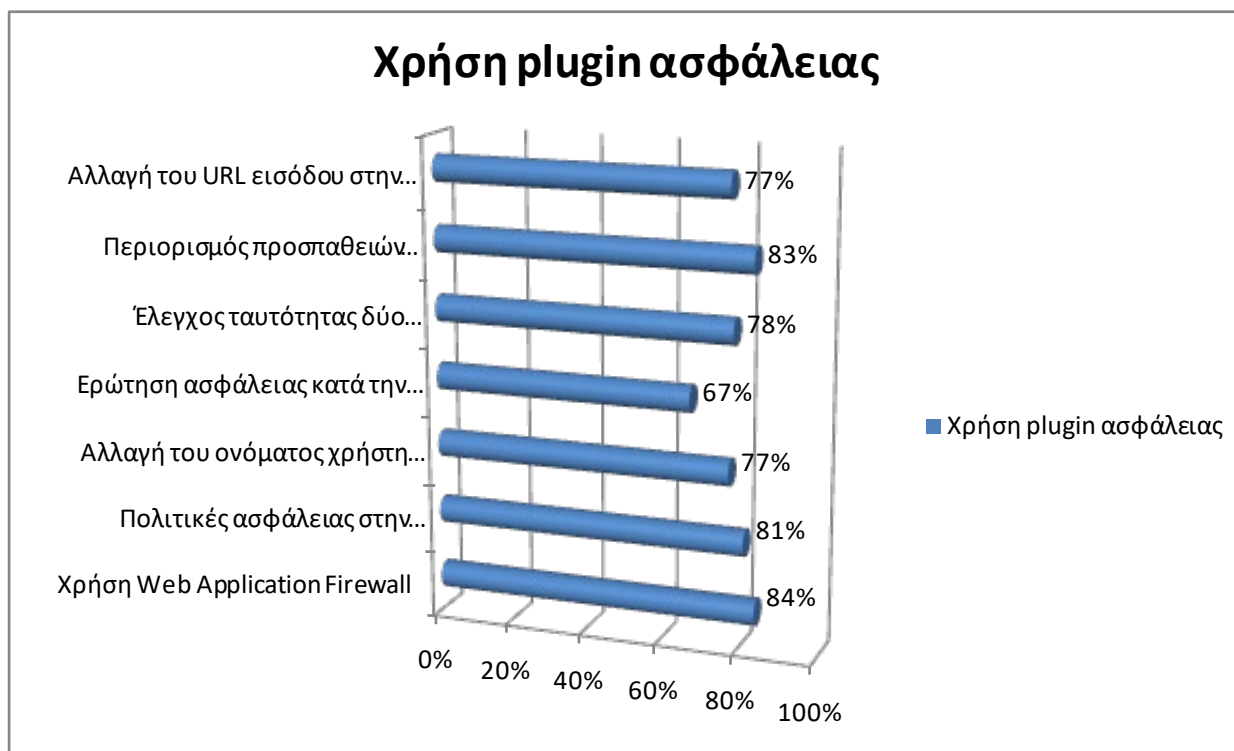
Διάγραμμα 26: Αντικείμενο σπουδών σε σχέση με την μη χρήση hardening techniques

Τα παραπάνω αποτελέσματα ίσως να οφείλονται στο γεγονός ότι όσοι από τους συμμετέχοντες απάντησαν ότι έχουν άλλο αντικείμενο σπουδών έχουν και μεγάλη εμπειρία στην διαχείριση ιστοσελίδων, όπως φαίνεται στο παρακάτω διάγραμμα.

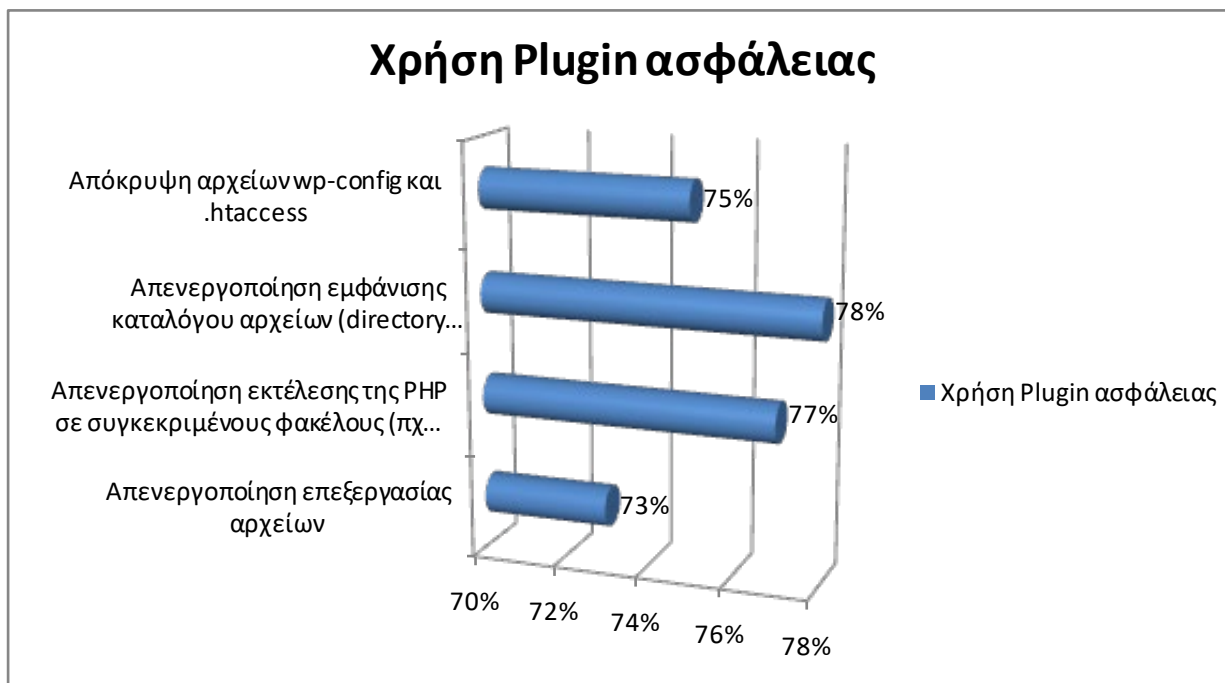


Διάγραμμα 27: Αντικείμενο σπουδών σε σχέση με την εμπειρία

Στην συνέχεια θα δούμε το κατά πόσο όσοι χρησιμοποιούν πρακτικές ασφάλειας, χρησιμοποιούν και plugin ασφάλειας. Στα επόμενα διαγράμματα 28, 29 και 30 φαίνονται τα ποσοστά, τα οποία μας δίνουν συγκεντρωτικά έναν μέσο όρο 75%. Δηλαδή περίπου το 75% όσων κάνουν hardening χρησιμοποιούν και plugin ασφάλειας.

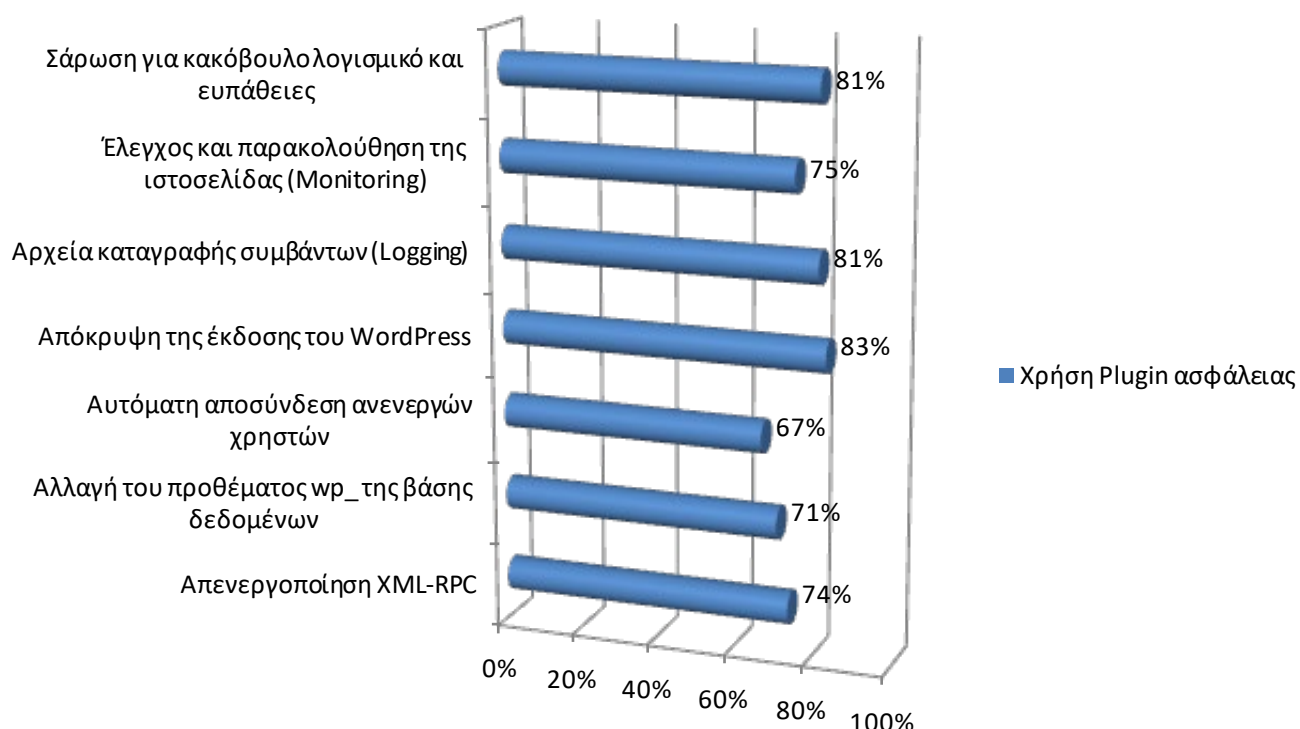


Διάγραμμα 28: Χρήση hardening techniques σε σχέση με την χρήση plugin ασφάλειας



Διάγραμμα 29: Χρήση hardening techniques σε σχέση με την χρήση plugin ασφάλειας

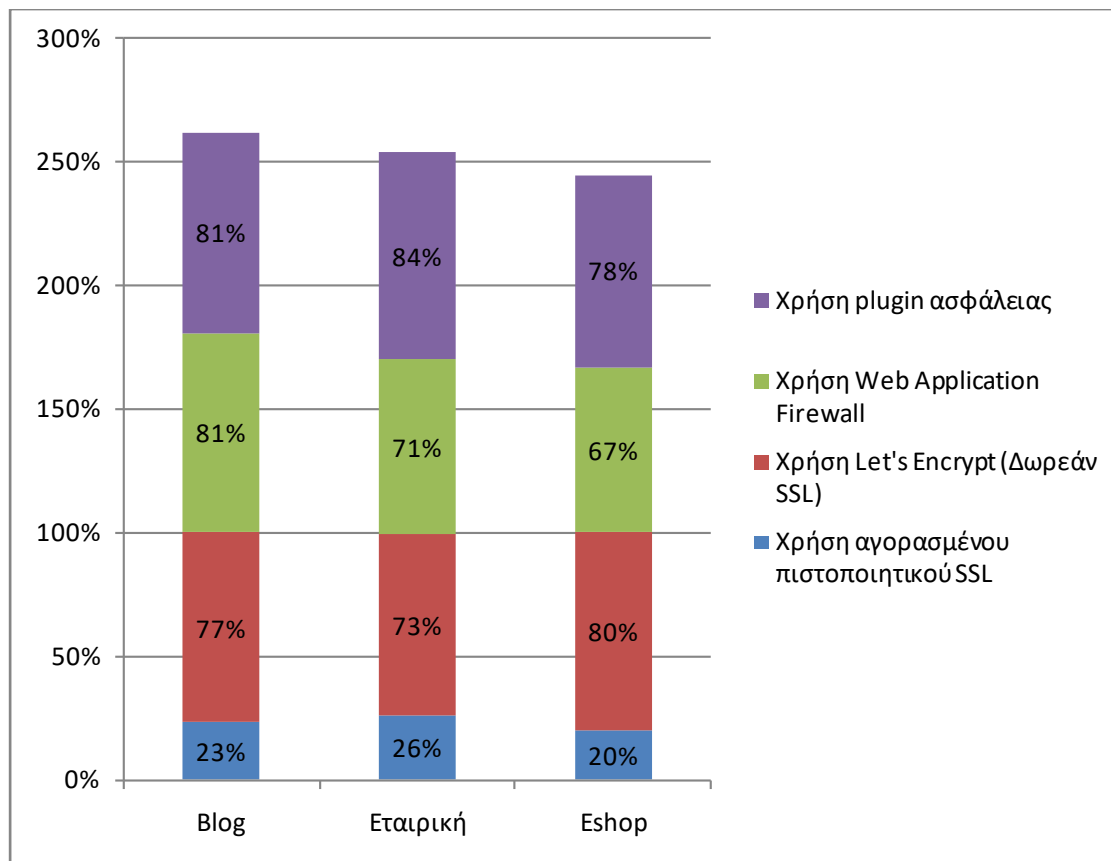
Χρήση Plugin ασφάλειας



Διάγραμμα 30: Χρήση hardening techniques σε σχέση με την χρήση plugin ασφάλειας

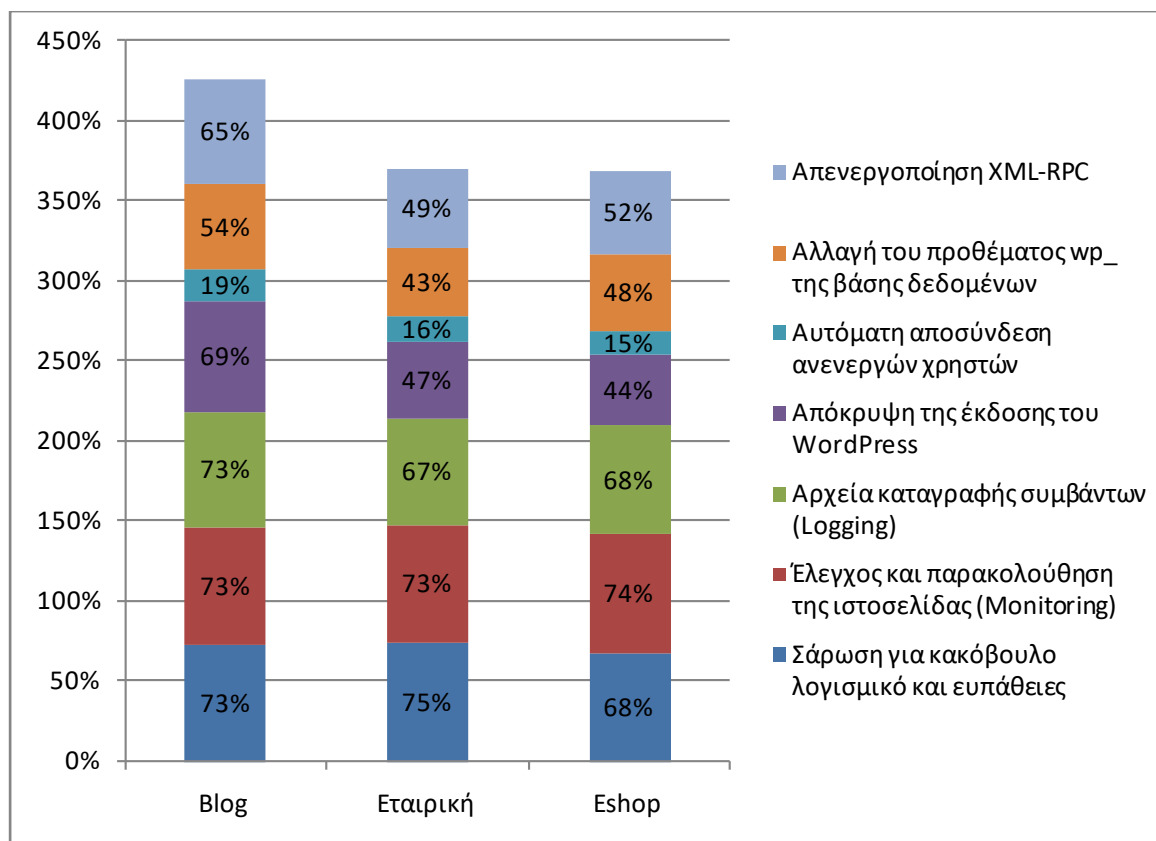
Στο παρακάτω διάγραμμα 31, βλέπουμε το είδος της ιστοσελίδας σε σχέση με την χρήση πιστοποιητικού SSL, Web Application Firewall και plugin ασφάλειας. Οι διαχειριστές που κάνουν χρήση αγορασμένου πιστοποιητικού SSL διαχειρίζονται σε μεγαλύτερο ποσοστό εταιρικές ιστοσελίδες, ενώ όσοι κάνουν χρήση του δωρεάν πιστοποιητικού Let's Encrypt διαχειρίζονται σε μεγαλύτερο ποσοστό Eshop. Αυτό που παρατηρούμε είναι ότι και για τα τρία είδη ιστοσελίδων, οι διαχειριστές χρησιμοποιούν περισσότερο το δωρεάν πιστοποιητικό SSL "Let's Encrypt".

Επίσης το μεγαλύτερο ποσοστό χρήσης WAF έχουν όσοι διαχειρίζονται blog. Ενώ όσοι χρησιμοποιούν plugin ασφάλειας διαχειρίζονται σε μεγαλύτερο ποσοστό εταιρικές ιστοσελίδες, με μικρή διαφορά από τις άλλες.

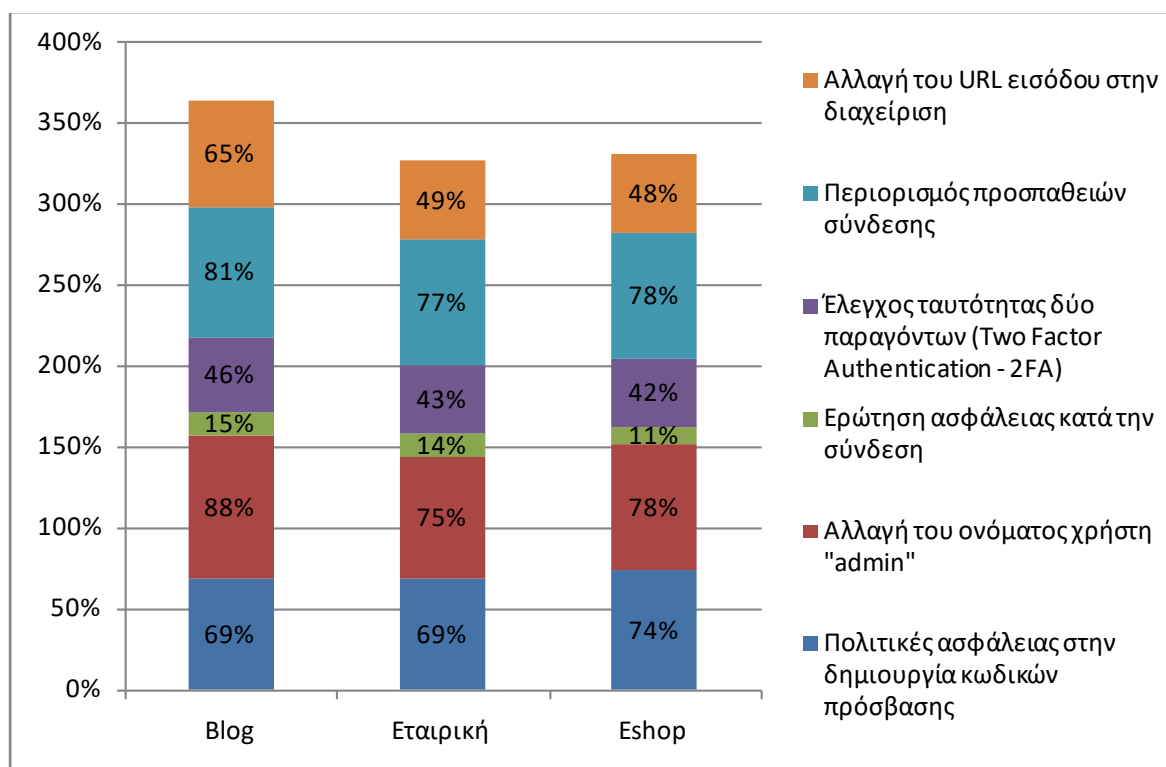


Διάγραμμα 31: Είδος ιστοσελίδας σε σχέση με τη χρήση Hardening techniques

Στα παρακάτω δύο διαγράμματα 32 και 33 φαίνεται ανάλογα με το είδος της ιστοσελίδας που διαχειρίζονται οι προγραμματιστές κατά πόσο χρησιμοποιούν πρακτικές ασφάλειας. Η έρευνα έδειξε ότι μεγαλύτερη χρήση πρακτικών ασφάλειας γίνεται στις ιστοσελίδες blog.

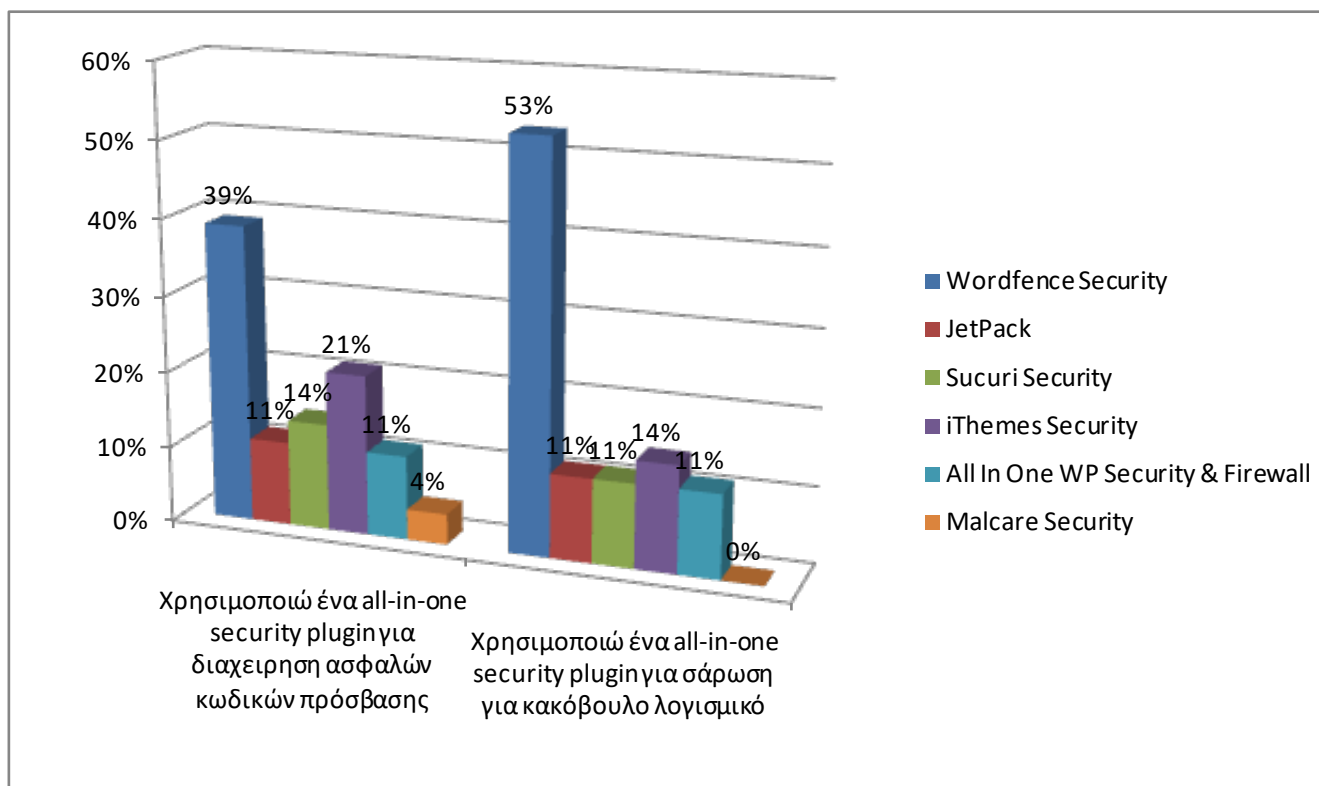


Διάγραμμα 32: Είδος ιστοσελίδας σε σχέση με τη χρήση Hardening techniques



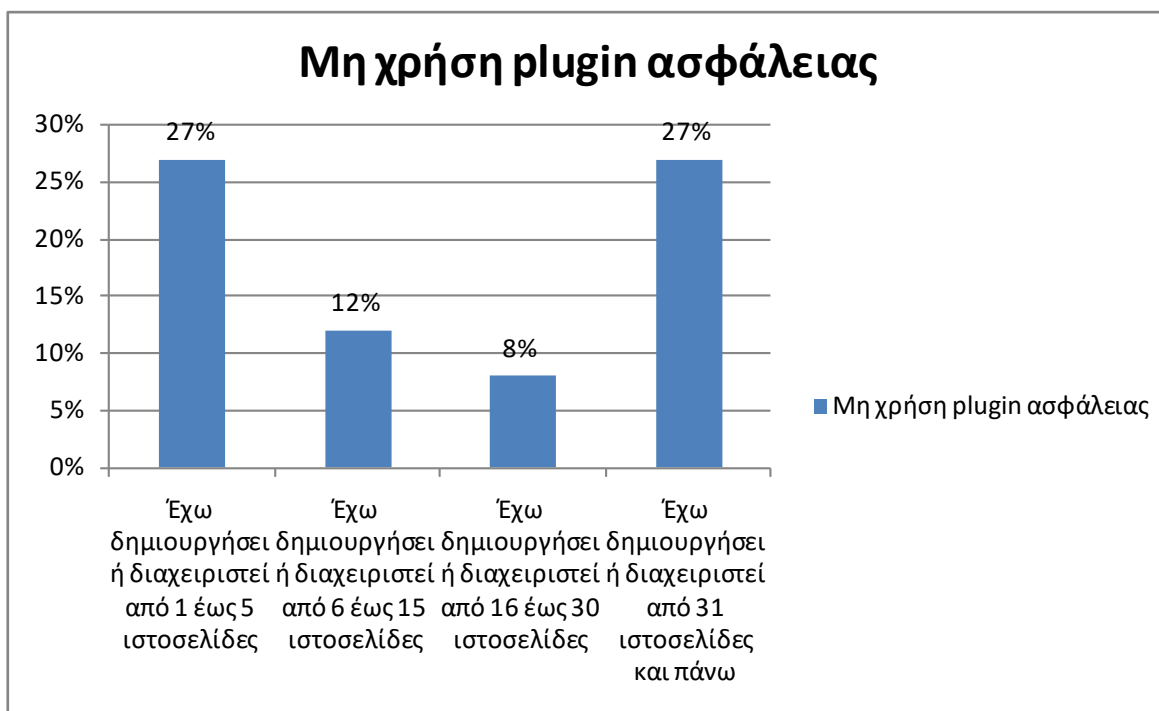
Διάγραμμα 33: Είδος ιστοσελίδας σε σχέση με τη χρήση Hardening techniques

Στο επόμενο διάγραμμα 34, φαίνονται τα plugins που χρησιμοποιούν όσοι απάντησαν ότι χρησιμοποιούν ένα all-in-one security plugin για διαχείριση ασφαλών κωδικών πρόσβασης και για σάρωση για κακόβουλο λογισμικό. Και για τις δύο ενέργειες πρώτο σε χρήση έρχεται το Wordfence Security και ακολουθεί το iThemes Security.



Διάγραμμα 34: Χρήση all-in-one security plugin

Στην συνέχεια θα δούμε ποιοί είναι αυτοί που χρησιμοποιούν λιγότερο plugin ασφάλειας σε σχέση με την εμπειρία τους. Όπως φαίνεται στο διάγραμμα 35, τα μεγαλύτερα ποσοστά όσων δεν χρησιμοποιούν plugin ασφάλειας εμφανίζουν όσοι έχουν πολύ μικρή εμπειρία (1-5 ιστοσελίδες) σε ποσοστό 27% και όσοι έχουν πολύ μεγάλη εμπειρία (30 και πάνω ιστοσελίδες) σε ποσοστό 27%. Ενώ αυτοί που χρησιμοποιούν περισσότερο plugin ασφάλειας είναι όσοι έχουν διαχειριστεί από 16 έως 30 ιστοσελίδες, σε ποσοστό 92%.



Διάγραμμα 35: Εμπειρία σε σχέση με την μη χρήση plugin ασφάλειας

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην συγκεκριμένη εργασία έγινε ανάλυση των ευπαθειών που παρουσιάζουν οι διαδικτυακές εφαρμογές, των επιθέσεων που αυτές συχνά δέχονται καθώς και των πρακτικών ασφάλειας που θα πρέπει να εκτελούν οι διαχειριστές των ιστοσελίδων WordPress προκειμένου να ελαχιστοποιούν τις ευπάθειες και τις επιθέσεις. Στην συνέχεια προσπαθήσαμε να αναλύσουμε την χρήση λογισμικού και plugin ασφάλειας στις ιστοσελίδες WordPress μέσα από έρευνα με ερωτηματολόγιο.

Σκοπός της έρευνας ήταν να κατανοήσουμε την ευαισθητοποίηση που δείχνουν οι διαχειριστές σε θέματα ασφάλειας. Κατά πόσο δηλαδή θεωρούν σημαντική την ασφάλεια του ιστοτόπου τους, αν χρησιμοποιούν πρακτικές για να ενισχύσουν την ασφάλεια αυτού, καθώς και αν εγκαθιστούν plugin ασφάλειας. Το τελικό συμπέρασμα είναι ότι όντως είναι αρκετά ευαισθητοποιημένοι όσον αφορά την ασφάλεια και εκτελούν αρκετές ενέργειες προκειμένου να εξασφαλίσουν την ασφάλεια του ιστοτόπου και των χρηστών του. Πιο συγκεκριμένα τα συμπεράσματα που προέκυψαν από την έρευνα έχουν ως εξής:

- ✚ Οι διαχειριστές των ιστοσελίδων WordPress θεωρούν, σε ποσοστό 76,5% ότι η ενίσχυση της ασφάλειας της ιστοσελίδας τους είναι πολύ σημαντική και αυτό επιβεβαιώνεται από τις απαντήσεις τους σχετικά με τις τεχνικές που ακολουθούν για να το πετύχουν. Πιο συγκεκριμένα ένα μεγάλο ποσοστό 75% ανανεώνουν τις ενημερωμένες εκδόσεις του WordPress, των plugins και των themes αμέσως μόλις εκδοθούν ή λίγες μέρες μετά. Επίσης το 63,2% των διαχειριστών δημιουργούν και αποθηκεύουν αντίγραφα ασφάλειας καθημερινά! Ακόμα το 100% των συμμετεχόντων στην έρευνα απάντησαν ότι χρησιμοποιούν πιστοποιητικό SSL, ενώ το 70% χρησιμοποιεί Web Application Firewall. Τέλος, το 77,9% χρησιμοποιούν plugin ασφάλειας.
- ✚ Η πιο δημοφιλής από τις πρακτικές ασφάλειας που χρησιμοποιούν είναι ο περιορισμός των αποτυχημένων προσπαθειών σύνδεσης, με ποσοστό 73,5% και ακολουθεί η αλλαγή του ονόματος χρήστη «admin» με ποσοστό 72,1%.
- ✚ Το δημοφιλέστερο σε χρήση plugin είναι το Wordfence Security με ποσοστό 77,4%, ενώ ακολουθεί το Sucuri Security με ποσοστό 20,8%.
- ✚ Ένα επόμενο συμπέρασμα είναι ότι οι συμμετέχοντες που απάντησαν ότι έχουν άλλο αντικείμενο σπουδών, έχουν μεγαλύτερο security awareness, χρησιμοποιούν δηλαδή σε μεγαλύτερο ποσοστό τις πρακτικές ασφάλειας σε σχέση με αυτούς που απάντησαν ότι έχουν αντικείμενο σπουδών την πληροφορική, όπως φαίνεται στα διαγράμματα 22, 23, 24, 25. Αν λάβουμε υπόψη ότι το 92% όσων έχουν άλλο αντικείμενο σπουδών, ασχολούνται επαγγελματικά με την δημιουργία διαχείριση ιστοσελίδων (διάγραμμα 21), και σε ποσοστό 84% έχουν διαχειριστεί πάνω από 16 ιστοσελίδες, άρα είναι αρκετά έμπειροι, σε σχέση με το αντίστοιχο 65% όσων έχουν αντικείμενο σπουδών την πληροφορική (διάγραμμα 27), καταλαβαίνουμε γιατί μπορεί να έχουμε αυτό το αποτέλεσμα. Παρόλα αυτά, επειδή αυτό το αποτέλεσμα δεν θα λέγαμε ότι είναι το αναμενόμενο, ίσως χρειάζεται περεταίρω διερεύνηση.
- ✚ Σύμφωνα με τα διαγράμματα 32 και 33, όσοι διαχειρίζονται blog, χρησιμοποιούν σε μεγαλύτερο ποσοστό πρακτικές ασφάλειας σε σχέση με

όσους διαχειρίζονται εταιρικές ιστοσελίδες και eshop. Οι πρακτικές που χρησιμοποιούν σε μεγαλύτερο ποσοστό είναι, η απόκρυψη της έκδοσης του WordPress σε ποσοστό 69%, η απενεργοποίηση XML-RPC με ποσοστό 65%, η αλλαγή του URL εισόδου στην διαχείριση με ποσοστό 65% και η αλλαγή του ονόματος χρήστη «admin» σε ποσοστό 88%, σε σχέση με όσους διαχειρίζονται εταιρικές ιστοσελίδες και eshop, όπου το ποσοστό χρήσης αυτών των πρακτικών είναι αρκετά μικρότερο. Επομένως καταλήγουμε στο συμπέρασμα ότι όσοι διαχειρίζονται blog έχουν μεγαλύτερο security awareness σε σχέση με όσους διαχειρίζονται εταιρικές ιστοσελίδες και eshop.

✚ Όσον αφορά το πιστοποιητικό SSL, οι διαχειριστές χρησιμοποιούν περισσότερο το δωρεάν πιστοποιητικό SSL “Let’s Encrypt” και για τα τρία είδη ιστοσελίδων (blog 77%, εταιρική 73%, eshop 80%). Η Let’s Encrypt εκδίδει μόνο Domain Validation (DV) SSL πιστοποιητικά. Τα DV SSL είναι ιδανικά για όσους αναζητούν βασική προστασία για το προσωπικό τους domain/ site ή forum, που χρειάζεται βασική κρυπτογράφηση για τα login ή τις φόρμες του. Με λίγα λόγια, δεν μπορούν να καλύψουν τις απαιτήσεις που έχουν μεγαλύτερα sites ή eShops. Αυτή τη “δουλειά” κάνουν τα Organization Validation (OV) και Extended Validation (EV) SSL. Συγκεκριμένα, τα OV πιστοποιούν domain και στοιχεία μιας επιχείρησης. Προτείνονται για εταιρικά site που έχουν ελάχιστη έως καθόλου διαχείριση ευαίσθητων προσωπικών δεδομένων των επισκεπτών. Τα EV είναι τα υψηλότερων προδιαγραφών SSL και είναι ιδανικά για μεγάλες επιχειρήσεις με online και e-commerce υπηρεσίες, που επιθυμούν να προβάλλουν ότι έχουν περάσει από τον αυστηρότερο έλεγχο αξιολόγησης, ώστε να κερδίσουν άμεσα την εμπιστοσύνη του πελάτη. Με ένα EV διατηρούν την ανταγωνιστικότητά τους και γνωστοποιούν ότι έχουν διαμορφώσει μια ασφαλή σελίδα, όπου τα προσωπικά στοιχεία και οι συναλλαγές του πελάτη προστατεύονται. [34] Επομένως, η χρήση του δωρεάν πιστοποιητικού SSL Let’s Encrypt σε ποσοστό 80% για όσους διαχειρίζονται eshop, θα μπορούσαμε να πούμε ότι δεν είναι η πιο συνετή πρακτική (Διάγραμμα 31).

✚ Ένα μεγάλο ποσοστό, κατά μέσο όρο 75%, όσων χρησιμοποιούν hardening techniques χρησιμοποιούν και plugin ασφάλειας. Το μεγαλύτερο ποσοστό (84%) χρήσης plugin ασφάλειας συγκεντρώνουν όσοι χρησιμοποιούν και Web Application Firewall (Διαγράμματα 28, 29, 30).

Συμπερασματικά, με αυτή την έρευνα παρουσιάσαμε όλη την ιδέα της χρήσης λογισμικού και plugin ασφάλειας στις ιστοσελίδες WordPress. Παρότι υπάρχει σχετικά μεγάλη ευαισθητοποίηση στο θέμα της ασφάλειας από τους προγραμματιστές, υπάρχει ακόμα κάποιο ποσοστό ατόμων που θα μπορούσε να κάνει περισσότερες ενέργειες προκειμένου να ενισχύσει την ασφάλεια της ιστοσελίδας και των χρηστών της.

7. ΑΝΑΦΟΡΕΣ

Ελληνόγλωσση Βιβλιογραφία:

- 1) Γκριτζαλης Σ., Κάτσικας Σ. και Γκριτζαλης Δ. (2003). «Ασφάλεια Δικτύων Υπολογιστών» Εκδόσεις Παπασωτηρίου, Αθήνα.

Ηλεκτρονικές αναφορές:

- 2) ΒΙΚΙΠΑΙΔΕΙΑ, Ασφάλεια Πληροφοριακών Συστημάτων [online] <https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CF%8E%CE%BD%CF%83%CF%85%CF%83%CF%84%CE%B7%CE%BC%CE%AC%CF%84%CF%89%CE%BD> (Πρόσβαση 10/12/2021)
- 3) OWASP. owasp.org [online] <https://owasp.org/> (Πρόσβαση 15/12/2021)
- 4) OWASP TOP 10: A01:2021 – Broken Access Control [online] [A01 Broken Access Control - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 5) OWASP TOP 10: A02:2021 – Cryptographic Failures [online] [A02 Cryptographic Failures - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 6) OWASP TOP 10: A03:2021 – Injection [online] [A03 Injection - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 7) OWASP TOP 10: A04:2021 – Insecure Design [online] [A04 Insecure Design - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 8) OWASP TOP 10: A05:2021 – Security Misconfiguration [online] [A05 Security Misconfiguration - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 9) OWASP TOP 10: A06:2021 – Vulnerable and Outdated Components [online] [A06 Vulnerable and Outdated Components - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 10) OWASP TOP 10: A07:2021 – Identification and Authentication Failures [online] [A07 Identification and Authentication Failures - OWASP Top 10 OWASP TOP 10::2021](#) (Πρόσβαση 15/12/2021)
- 11) OWASP TOP 10: A08:2021 – Software and Data Integrity Failures [online] [A08 Software and Data Integrity Failures - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 12) OWASP TOP 10: A09:2021 – Security Logging and Monitoring Failures [online] [A09 Security Logging and Monitoring Failures - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 13) OWASP TOP 10: A10:2021 – Server-Side Request Forgery (SSRF) [online] [A10 Server Side Request Forgery \(SSRF\) - OWASP Top 10:2021](#) (Πρόσβαση 15/12/2021)
- 14) WordPress.org, Brute force attacks [online] <https://wordpress.org/support/article/brute-force-attacks/> (Πρόσβαση 20/12/2021)
- 15) ΒΙΚΙΠΑΙΔΕΙΑ, Επιθέσεις άρνησης υπηρεσιών [online] <https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%B9%CE%B8%CE%AD%CF%83%CE%B5%CE%B9%CF%82%CE%AC%CF%81%CE%BD%CE%B7%CF%83%CE%B7%CF%82%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%B9%CF%8E%CE%BD> (Πρόσβαση 20/12/2021)

- 16) ΒΙΚΙΠΑΙΔΕΙΑ, Χάκερ: Μέθοδοι επιθέσεων. [online] <https://el.wikipedia.org/wiki/%CE%A7%CE%AC%CE%BA%CE%B5%CF%81> (Πρόσβαση 20/12/2021)
- 17) Malcare.com. (2021) How to Implement Cross-Site Scripting Prevention? [online] <https://www.malcare.com/blog/cross-site-scripting-xss-attacks-what-how-prevent-them/> (Τελευταία πρόσβαση 20/12/2021)
- 18) KirstenS. Cross Site Scripting (XSS) [online] <https://owasp.org/www-community/attacks/xss/> (Πρόσβαση 23/12/2021)
- 19) Malcare.com. (2021) How To Prevent SQL Injections? [online] <https://www.malcare.com/blog/preventing-sql-injections/> (Πρόσβαση 23/12/2021)
- 20) Malcare.com (2021) How to Scan Backdoors of Your Hacked WordPress Site? [online] <https://www.malcare.com/blog/how-to-scan-malware-and-backdoors-of-your-wordpress-site/> (Πρόσβαση 27/12/2021)
- 21) WordPress.org. About. [online] <https://wordpress.org/about/> (Πρόσβαση 05/01/2022)
- 22) W3Techs-Web Technology Surveys. w3techs.com. [online] [Usage Statistics and Market Share of Content Management Systems, February 2022 \(w3techs.com\)](https://w3techs.com/usage-statistics-and-market-share/content-management-systems-february-2022/) (Πρόσβαση 10/01/2022)
- 23) Builtwith. CMS Usage Distribution on the Entire Internet. [online] [CMS technologies Web Usage Distribution on the Entire Internet \(builtwith.com\)](https://builtwith.com/cms-technologies/web-usage-distribution-on-the-entire-internet/) (Πρόσβαση 10/01/2022)
- 24) Builtwith. WordPress Usage Statistics. [online] [WordPress Usage Statistics \(builtwith.com\)](https://builtwith.com/wordpress-usage-statistics/) (Πρόσβαση 10/01/2022)
- 25) W3Techs-Web Technology Surveys. w3techs.com. [online] [Historical yearly trends in the usage statistics of content management systems, February 2022 \(w3techs.com\)](https://w3techs.com/usage-statistics/content-management-systems-february-2022/) (Πρόσβαση 10/01/2022)
- 26) Sara Rosso. (2015) WordPress Security. [online] [Security | WordPress.org](https://security.wordpress.org/) (Πρόσβαση 15/01/2022)
- 27) Malcare. (2021) How do Web Hosts Affect Website Security. [online] [Web Host Security - How Do Web Hosts Affect Website Security? \(malcare.com\)](https://malcare.com/web-host-security-how-do-web-hosts-affect-website-security/) (Πρόσβαση 12/01/2022)
- 28) Wordpress.org. Hardening WordPress. [online] <https://wordpress.org/support/article/hardening-wordpress/#database-security> (Πρόσβαση 12/01/2022)
- 29) Ilias Kypraios. TopHost. (2020) 15 βήματα για να αυξήσεις την ασφάλεια ενός WordPress site. [online] [15 βήματα για να αυξήσεις την ασφάλεια ενός WordPress site - Top.Host Blog](https://tophostblog.com/15-bhmatata-για-na-avxihsis-tin-asfalεια-enos-wordpress-site/) (Πρόσβαση 12/01/2022)
- 30) Sucuri (2020) WordPress Security. [WordPress Security: How to Secure & Protect WordPress | Sucuri](https://sucuri.net/wordpress-security-how-to-secure-protect-wordpress/) (Πρόσβαση 12/01/2022)
- 31) WPBEGINNER (2022) The Ultimate WordPress Security Guide. [online] <https://www.wpbeginner.com/wordpress-security/> (Πρόσβαση 12/01/2022)
- 32) Samsoft (2019) Ασφάλεια ενός WordPress site – Χρήσιμες συμβουλές και ενέργειες. [online] [Ασφάλεια WordPress - Χρήσιμες συμβουλές - Samsoft](https://samsoft.gr/asfalεια-wordpress-chrisimes-symvoulis-kenergies/) (Πρόσβαση 12/01/2022)

- 33) Oliver Sild. (2021) Security vulnerabilities of WordPress ecosystem in 2020. [online] <https://patchstack.com/wp-content/uploads/2021/04/Security-vulnerabilities-of-WordPress-ecosystem-in-2020-Patchstack-1.pdf> (Πρόσβαση 10/01/2022)
- 34) Marieta Christopoulou (2019). Γιατί να αγοράσω SSL όταν μπορώ να βρω δωρεάν; [online] <https://www.papaki.com/blog/2018/09/04/free-ssl-vs-paid-ssl/> (Πρόσβαση 20/01/2022)