



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ &
ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Αξιολόγηση ασφάλειας ιστοσελίδων Wordpress μέσω ερωτηματολογίου

Υποψήφια: Λασοπούλου Βαλέρια, Π 2017062

Επιβλέπων: Νταντογιάν Χριστόφορος (Ιδιότητα)

Κέρκυρα
2022

Αξιολόγηση ασφάλειας ιστοσελίδων Wordpress μέσω ερωτηματολογίου

Η πτυχιακή εργασία εγκρίθηκε από:

- 1. Νταντογιάν Χριστόφορο, Επιβλέπων**
- 2. Τσώχου Αγγελική, μέλος της επιτροπής**
- 3. Μάγκος Εμμανουήλ, μέλος της επιτροπής**

Υπεύθυνη Δήλωση

Με το παρόν κείμενο βεβαιώνω ότι η κάτωθι υπογράφουσα είμαι συγγραφέας της παρούσας πτυχιακής εργασίας, η οποία εκπονήθηκε στο πλαίσιο των απαιτήσεων του προγράμματος σπουδών του Τμήματος Πληροφορικής του Ιονίου Πανεπιστημίου και η οποία παραδόθηκε, μετά από έγκριση του επιβλέποντας καθηγητή μου, σε έντυπη και ψηφιακή μορφή στη Γραμματεία του Τμήματος. Επίσης δηλώνω πως κάθε πηγή που χρησιμοποίησα (βιβλιογραφία, αρθρογραφία, δικτυογραφία), για την υποστήριξη των υποθέσεων της μελέτης και της έρευνάς μου, είναι πλήρως συμβατή με τα ακολουθούμενα επιστημονικά πρότυπα και, επιπλέον, αναφέρεται ρητά, υπό μορφή αναφοράς-παραπομπής, σε όλο το φάσμα κειμένων της παρούσας εργασίας. Το αυτό ισχύει για τη χρήση δευτερογενών δεδομένων (πινάκων, διαγραμμάτων και εικόνων), ιδεών και λέξεων, τα οποία και αναφέρονται είτε ακριβώς όπως υπάρχουν στις πηγές είτε μεθερμηνεύονται από εμένα.

Όνομα	Βαλέρια
Επώνυμο	Λασοπούλου
Αριθμός Μητρώου	Π2017062
Ημερομηνία	10/09/2022
Υπογραφή	

“Security culture can achieve more than prohibition posture.”

~ Stephane Nappo

Περίληψη

Παρόλο που οι περισσότεροι χρήστες του διαδικτύου αισθάνονται ασφαλείς όταν “σερφάρουν” στον παγκόσμιο ιστό, τα τελευταία χρόνια έχει παρατηρηθεί μία αύξηση στον κόσμο του κυβερνοεγκλήματος που φαίνεται να γίνεται όλο και σπουδαιότερη με το πέρασμα του χρόνου.

Σύμφωνα με στατιστικές έρευνες, το 43% των κυβερνοεπιθέσεων στοχεύουν μικρές επιχειρήσεις εξαιτίας της εκτεθειμένης ασφάλειας τόσο των ιδίων, αλλά και του συστήματος των υπολογιστών που χρησιμοποιούν.^[1] Οι επιτιθέμενοι επιλέγοντας τέτοιου είδους “εύκολους στόχους” έχουν αβίαστη πρόσβαση σε πληροφορίες και οικονομικούς πόρους. Ιδιαίτερα ανησυχητικό είναι πως ένα σημαντικό 70% των μικρών επιχειρήσεων δεν είναι σε θέση να αντιμετωπίσει κυβερνοεπιθέσεις διαφόρων ειδών.^{[1][2][3]}

Γνωρίζοντας τα παραπάνω, ποιά είναι πραγματικά η θέση των προγραμματιστών όσον αφορά την θωράκιση των ιστοσελίδων τους; Είναι η ασφάλεια μιας ιστοσελίδας η κύρια προτεραιότητα τους;

Η έρευνα αυτή έρχεται να απαντήσει τα παραπάνω ερωτήματα και να ξεκαθαρίσει ποιά πραγματικά είναι η κατάσταση όσον αφορά την ασφάλεια των ιστοσελίδων που έχουν σχεδιαστεί με τη χρήση της ιδιαίτερα δημοφιλούς πλατφόρμας Content Management System Wordpress.

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

Abstract

Although most internet users feel safe while “surfing” the world wide web, an increase of cases in the world of cybercrime has been noticed in the last couple of years that seems to be getting more and more prevalent with the passage of time.

According to statistical surveys, 43% of cyberattacks target small businesses due to the lack of security of both themselves and the web servers they run on.^[1] By selecting these easy targets, the attackers have access to user information, financial resources and all different types of data. Of particular concern is that a significant 70% of small businesses are unable to deal with cyber-attacks of various kinds due to lack of cybersecurity knowledge.^{[1][2][3]}

Knowing the above, some questions arise; where do developers really stand when it comes to customizing their websites? Is the security of the websites they create their top priority?

This research comes to answer these questions and to clarify what the situation really is in terms of the security of websites designed with the use of the popular Content Management System platform Wordpress.

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

Πίνακας Περιεχομένων

Περίληψη

Abstract

Πίνακας Περιεχομένων

Εισαγωγή

1. Σκοπός της εργασίας
2. Μεθοδολογία της εργασίας
3. Διάρθρωση εργασίας

Κεφάλαιο 1: Web Content Management Systems

- 1.1 Τί είναι οι CMS πλατφόρμες;
- 1.2 Διαφορετικοί τύποι πλατφόρμων CMS
 - 1.2.1 Open source CMS
 - 1.2.2 Proprietary CMS
 - 1.2.3 Software as a Service (SaaS) CMS
- 1.3 Πώς επιλέγεις την καλύτερη CMS πλατφόρμα για την ιστοσελίδα σου;
 - 1.3.1 CMS ή website builder;
 - 1.3.2 Κριτήρια επιλογής CMS
 - 1.3.2.1 Ευκολία χρήσης
 - 1.3.2.2 Εξατομίκευση
 - 1.3.2.3 Ασφάλεια
 - 1.3.2.4 Τιμή
 - 1.3.2.5 Μεταφορά δεδομένων
 - 1.3.2.6 Επικράτηση στην αγορά
- 1.4 Οι πιο δημοφιλείς CMS πλατφόρμες
 - 1.4.1 CMS Hub
 - 1.4.2 WordPress
 - 1.4.3 Drupal
 - 1.4.4 Joomla
 - 1.4.5 Shopify
 - 1.4.6 Magento

1.4.7 Magnolia

1.4.8 TYPO3

1.4.9 Prestashop

1.4.10 Concrete5

1.5 Επιλέγουν οι προγραμματιστές ιστοσελίδων να δουλέψουν με CMS πλατφόρμες;

Κεφάλαιο 2: WordPress

2.1 Μια αναλυτική περιγραφή του WordPress

2.1.1 WordPress Themes

2.1.2 Wordpress Plugins

2.1.3 Επιπλέον γνωρίσματα

2.2 Ασφάλεια στο WordPress

2.2.1 Θέματα ασφαλείας και ευπάθειες

2.2.1.1 *Outdated Core Software*

2.2.1.2 *Outdated Θέματα και Plugins*

2.2.1.3 *Malware*

2.2.1.4 *Μη Εξουσιοδοτημένα Logins*

2.2.1.5 *Μη Καθορισμένοι Ρόλοι Χρήστη*

2.2.2 Κυριότερες επιθέσεις στην πλατφόρμα

2.2.2.1 *Structured Query Language (SQL) Injections*

2.2.2.2 *Search Engine Optimization (SEO) Spam*

2.2.2.3 *Skimming Πιστωτικών Καρτών*

2.2.2.4 *Brute Force Attack*

2.2.2.5 *Cross-Site Scripting (XSS)*

2.2.2.6 *Denial of Service Attack (DoS)*

2.2.2.7 *Phishing*

2.2.3 Τρόποι ενίσχυσης ασφαλείας

2.2.3.1 *Χρήση ασφαλούς παρόχου φιλοξενίας (Web Hosting)*

2.2.3.2 *Συνεχής ενημέρωση της πλατφόρμας WordPress*

2.2.3.3 *Παρακολούθηση του Dashboard της πλατφόρμας*

2.2.3.4 *Ελεγχόμενη χρήση plugin και θεμάτων*

2.2.3.5 *Ενίσχυση του “πυρήνα της πλατφόρμας” (WordPress Core)*

2.2.3.6 *TLS (SSL)*

2.2.3.7 Επιπλέον βήματα ενίσχυσης της ασφάλειας

2.3 Δημοφιλή Security Plugins

Κεφάλαιο 3: Μεθοδολογία Έρευνας

3.1 Ερευνητικά Ερωτήματα

3.2 Σχεδιασμός Ερωτηματολογίου

3.3 Δείγμα Έρευνας

3.4 Ερωτηματολόγιο

Κεφάλαιο 4: Αποτελέσματα Έρευνας και Συμπεράσματα

4.1 Ενότητα 1: Μέτρα Ασφαλείας

4.2 Ενότητα 2: Ενίσχυση Ασφαλείας των WordPress Ιστοσελίδων

4.3 Ενότητα 3: Security Plugins

4.4 Ενότητα 4: Εγγραφή Χρηστών

4.5 Ενότητα 5: Ασφάλεια Ιστοσελίδων που επιτρέπουν την είσοδο χρηστών

4.6 Ενότητα 6: Γενικές Ερωτήσεις Ασφαλείας

4.7 Ενότητα 7: Προσωπικά Δεδομένα

4.8 Συνδυαστικά συμπεράσματα

4.8.1 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Τρόπος λήψης πρόσθετων.

4.8.2 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν τί είναι η επίθεση XSS.

4.8.3 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν αν οι HTTPS ιστοσελίδες τους χρησιμοποιούν TLS 1.2 ή TLS 1.3.

4.8.4 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο εφαρμόζουν κατάλληλα μέτρα για να εξασφαλίσουν την συμμόρφωση με το GDPR.

4.8.5 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν το default WordPress hashing scheme των αποθηκευμένων κωδικών πρόσβασης των χρηστών τους.

4.8.6 Κατά πόσο οι προγραμματιστές χρησιμοποιούν κάποιο all-in-one plugin / Κατά πόσο χρησιμοποιούν κάποιο malware scanner plugin.

4.8.7 Συγκεντρωτικά συμπεράσματα

Σχετικές Έρευνες

Βιβλιογραφία

Εισαγωγή

Σκοπός της εργασίας

Με τη ραγδαία ανάπτυξη του διαδικτύου και κατά κανόνα των επιχειρήσεων που θέλουν να έχουν μια θέση στην εικονική αγορά, παράγονται όλο και περισσότερες ιστοσελίδες με τη χρήση πλατφορμών CMS. Το WordPress αποτελεί τη πιο δημοφιλή πλατφόρμα συστήματος διαχείρισης περιεχομένου και χρησιμοποιείται σε καθημερινή βάση από επαγγελματίες web developers και μη για τη δημιουργία ιστοσελίδων και ιστοτόπων.

Μιας και οι άνθρωποι χρησιμοποιούν το διαδίκτυο σε καθημερινή βάση για να πραγματοποιήσουν τις διεργασίες που επιθυμούν, μπορούμε να συμπεράνουμε πως η κάθε ιστοσελίδα περιλαμβάνει μια πληθώρα δεδομένων που μπορούν να υποκλαπούν από κακόβουλους χρήστες. Πέρα από την παραβίαση της εμπιστευτικότητας, υπάρχει και κίνδυνος έκθεσης της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Ο σκοπός αυτής της εργασίας είναι να εξετάσει κατά πόσο οι επαγγελματίες χρήστες της πλατφόρμας WordPress λαμβάνουν υπόψη τους τις απειλές που αντιμετωπίζουν οι ιστοσελίδες της σύγχρονης εποχής και ποιές μεθόδους χρησιμοποιούν για να εξασφαλίσουν την πλήρη ασφάλεια τόσο των δημιουργημάτων τους όσο και των χρηστών που “εισέρχονται” σε αυτά.

Μεθοδολογία της εργασίας

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

Διάρθρωση της εργασίας

Η παρούσα εργασία αποτελείται από πέντε κεφάλαια, συμπεριλαμβανομένης της εισαγωγής. Σε κάθε ένα από αυτά, παρουσιάζονται και αναλύονται με τη σειρά, τα διάφορα θέματα που κλήθηκε να μελετήσει η συγκεκριμένη έρευνα. Τα κεφάλαια 1, 2 και 3 αναλύουν με τη σειρά που αναφέρονται: τί είναι οι πλατφόρμες CMS, τί ακριβώς είναι η πλατφόρμα WordPress και ποιά είναι τα διάφορα είδη επιθέσεων που αντιμετωπίζουν οι ιστοσελίδες που δημιουργήθηκαν με αυτή, και τέλος, ποιά είναι η μεθοδολογία που ακολουθήθηκε για την εκπόνηση αυτής της εργασίας. Η μεγάλη και αναλυτική αυτή “εισαγωγή” συγγράφηκε προκειμένου να μπορούν αναγνώστες κάθε ιδιότητας να αναγνωρίζουν και να κατανοούν σε ικανοποιητικό βαθμό τις έννοιες που αναφέρονται στο 4ο και τελευταίο κεφάλαιο της έρευνας. Με αυτόν τον τρόπο θα μπορέσουν τελικά να αξιοποιήσουν τις γνώσεις που

αφομοίωσαν για να αντλήσουν τα δικά τους συμπεράσματα βάση των αποτελεσμάτων που συγκεντρώθηκαν. Στο τελευταίο κεφάλαιο, παρουσιάζεται εξ ολοκλήρου το ερωτηματολόγιο που δημιουργήθηκε και στη συνέχεια αναλύονται με τη σειρά τα ερωτήματα που συμπεριλαμβάνει. Τέλος, εξετάζονται ορισμένα ενδιαφέροντα συγκεντρωτικά συμπεράσματα που προκύπτουν από το συνδυασμό ορισμένων ερωτήσεων.

Κεφάλαιο 1: Web Content Management Systems

1.1 Τί είναι οι CMS πλατφόρμες;

Μια πλατφόρμα CMS (πλατφόρμα συστήματος διαχείρισης περιεχομένου) είναι ένα κομμάτι λογισμικού που επιτρέπει στους χρήστες να διαχειρίζονται εύκολα περιεχόμενο και να δημιουργούν ιστοτόπους της αρεσκείας τους.[4]

Κανονικά, οι ιστοσελίδες είναι γραμμένες σε γλώσσες προγραμματισμού όπως η HTML, η JavaScript και η CSS. Εάν κάποιος θελήσει να δημιουργήσει έναν ιστότοπο χωρίς πλατφόρμα CMS, τότε θα πρέπει να μάθει αυτές τις γλώσσες ως ένα αρκετά μεγάλο βαθμό και να γράψει ένα σημαντικό κομμάτι κώδικα.[4]

Οι πλατφόρμες CMS λύνουν αυτό το πρόβλημα επιτρέποντας σε άτομα χωρίς εξειδικευμένες γνώσεις να δημιουργήσουν έναν ιστότοπο χωρίς να γράψουν κώδικα ή να μάθουν προγραμματισμό. Ωστόσο, αυτό δε σημαίνει πως οι προγραμματιστές δε μπορούν να επωφεληθούν από τέτοιου είδους πλατφόρμες καθώς η χρήση τους καθιστά την διαχείριση ιστοσελίδων πολύ πιο προσιτή και βολική. Επιπρόσθετα, αν κάποιος επιθυμεί να εμπλουτίσει την ιστοσελίδα του με επιπρόσθετο κώδικα, υπάρχουν CMS που παρέχουν αυτή τη δυνατότητα.[4]

1.2 Διαφορετικοί τύπου πλατφορμών CMS

Όταν κάποιος καλείται να επιλέξει ένα σύστημα διαχείρισης περιεχομένου (CMS) για την επιχείρησή του, βοηθάει να έχει κατανοήσει τις διαφορές μεταξύ των διαφόρων τύπων, των χαρακτηριστικών και των λειτουργιών τους καθώς και τα μοντέλα τιμολόγησης. Υπάρχουν τρεις μεγάλες κατηγορίες λογισμικού CMS: open source, proprietary και Software-as-a-Service CMS, συμπεριλαμβανομένων και των cloud-based solutions. [5]

1.2.1 Open Source CMS

Τα λογισμικά ανοιχτού κώδικα (open source) CMS μπορούν να εγκατασταθούν χωρίς αρχικό κόστος. Δεν υπάρχουν τέλη άδειας ή αναβάθμισης ή συμβόλαια. Ωστόσο, με το CMS ανοιχτού κώδικα μπορεί να χρειαστεί κάποιος να πληρώσει για: [5]

- τεχνική βοήθεια κατά την εγκατάσταση και το set up
- προσαρμογή για επέκταση του λογισμικού πέρα από την κύρια προσφορά
- συμβατά πρότυπα, add-ons και plugins (αν και μπορεί να είναι διαθέσιμες δωρεάν εκδόσεις)
- εκπαίδευση προσωπικού
- υποστήριξη, συμπεριλαμβανομένης της τακτικής ενημέρωσης του λογισμικού

Παραδείγματα των πιο ευρέως χρησιμοποιούμενων πλατφορμών ανοιχτού κώδικα CMS περιλαμβάνουν:

- WordPress
- Joomla
- Drupal

- Magento (ηλεκτρονικό εμπόριο)
- PrestaShop (ηλεκτρονικό εμπόριο)

Οι CMS ανοιχτού κώδικα μπορούν να εγκατασταθούν και να ρυθμιστούν σε έναν διακομιστή web. Ενώ οι περισσότερες λύσεις (solutions) λειτουργούν απροσδόκητα, διατίθενται αμέτρητες προσαρμογές για την κάλυψη των διαφορετικών επιχειρηματικών αναγκών, όπως plugins για ιστότοπους ηλεκτρονικού εμπορίου (e-commerce), tools που θα σας βοηθήσουν να βελτιστοποιήσετε το περιεχόμενο για τις μηχανές αναζήτησης ή να προσαρμόσετε τα σχεδιασμένα θέματα και τα layouts σας.^[5]

1.2.2 Proprietary CMS

Το ιδιόκτητο ή εμπορικό λογισμικό CMS δημιουργείται και είναι διαχειρίσιμο από μία μόνο εταιρεία. Η χρήση τέτοιου CMS περιλαμβάνει γενικά: ^[5]

- αγορά ενός τέλους άδειας χρήσης του λογισμικού
- μηνιαίες ή ετήσιες χρεώσεις για ενημερώσεις ή υποστήριξη

Μπορεί επίσης να χρειαστεί να πληρωθεί κάποιο επιπλέον κόστος για προσαρμογή και αναβαθμίσεις, καθώς και για εκπαίδευση και συνεχή τεχνική υποστήριξη ή υποστήριξη χρηστών.

Μερικά παραδείγματα δημοφιλών CMS solutions:

- Kentico
- Microsoft SharePoint
- IBM Enterprise Content Management
- Pulse CMS
- Sitecore
- Shopify

Ο χρήστης μπορεί συνήθως να προσαρμόσει στο ιδιόκτητο CMS ενσωματωμένες λειτουργίες, αν και αυτό μπορεί να έχει επιπλέον κόστος. Εάν είναι δυνατόν, ένας ενδιαφερόμενος θα ήταν καλύτερο να αναζητήσει μια λύση CMS που να ικανοποιεί όλες τις απαιτήσεις του από την αρχή. Εάν ένα ιδιόκτητο CMS εφαρμοστεί με έναν υπάρχοντα ιστότοπο ή ένα σύστημα back-end, μπορεί να χρειαστεί εκτεταμένη εργασία ανάπτυξης.

Αν κάποιος ψάχνει ένα CMS για έναν ολοκαίνουργιο ιστότοπο, είναι καλύτερο να επιλέξει μια λύση που έχει όλες τις σημαντικές δυνατότητες και λειτουργίες για να καλύψει τις τρέχουσες και μελλοντικές επιχειρηματικές του ανάγκες.^[5]

1.2.3 Software as a Service (SaaS) CMS

Οι λύσεις (solutions) SaaS CMS περιλαμβάνουν συνήθως λογισμικό διαχείρισης περιεχομένου ιστού, web hosting και τεχνική υποστήριξη με έναν μόνο προμηθευτή. Πρόκειται για εικονικά solutions που φιλοξενούνται στο cloud και βασίζονται σε ένα μοντέλο συνδρομής, συνήθως ανά χρήστη ή ανά τοποθεσία. Η τιμολόγηση συνήθως περιλαμβάνει:

- ποσότητα μεταφοράς δεδομένων (π.χ. εύρος ζώνης προς και από τον ιστότοπο του χρήστη)
- αποθηκευτικό χώρο για το περιεχόμενο και τα δεδομένα του χρήστη
- συνεχή υποστήριξη

Υπάρχουν δύο τύποι συστημάτων διαχείρισης περιεχομένου cloud:

- Το CMS «Fully cloud» έρχεται συχνά ως μέρος ενός πακέτου ή υπηρεσίας. Συνήθως, αυτά είναι ιδιόκτητα συστήματα υπό τον έλεγχο του προμηθευτή, επομένως δεν είναι πάντα δυνατό να προσαρμοστεί ή να τροποποιηθεί η λειτουργικότητά τους ανάλογα με τις ανάγκες των χρηστών.
- Το CMS «μερικού νέφους» βρίσκεται στον διακομιστή web cloud του χρήστη. Παρέχει μεγαλύτερη ευελιξία, καθώς μπορεί να τροποποιηθεί η λειτουργικότητα, είτε με πρόσθετες μονάδες είτε αλλάζοντας τον πηγαίο κώδικα.

Το Cloud CMS προσφέρει ορισμένα σημαντικά οφέλη στις μικρές και μεσαίες επιχειρήσεις. Για παράδειγμα:

- Το κόστος είναι γενικά χαμηλό - μια μικρή χρέωση εγκατάστασης συνήθως καλύπτει μια βασική υλοποίηση.
- Ο προμηθευτής SaaS ασχολείται με αναβαθμίσεις, συντήρηση και τεχνικά ζητήματα.
- Το λογισμικό είναι προσβάσιμο από οποιονδήποτε υπολογιστή, φορητό υπολογιστή ή κινητό με σύνδεση στο διαδίκτυο.
- Ενημερώσεις λογισμικού και λειτουργιών είναι διαθέσιμες σε πραγματικό χρόνο.
- Τα πακέτα είναι εύκολα επεκτάσιμα - μπορείτε να προσθέσετε περισσότερους ιστότοπους ή χρήστες καθώς αλλάζουν οι ανάγκες σας.

1.3 Πώς επιλέγεις την καλύτερη CMS πλατφόρμα για την ιστοσελίδα σου;

Πολλοί ελεύθεροι επαγγελματίες και επιχειρήσεις δεν γνωρίζουν ή δεν έχουν το χρόνο να μάθουν αρκετή HTML, CSS και JavaScript για να δημιουργήσουν έναν ιστότοπο από την αρχή. Ευτυχώς, με τα κατάλληλα εργαλεία, μπορούμε εύκολα και γρήγορα να δημιουργήσουμε έναν προσαρμοσμένο ιστότοπο που παρέχει απρόσκοπτες εμπειρίες τόσο στους επισκέπτες όσο και στους χρήστες. Αυτά τα εργαλεία εμπίπτουν σε δύο μεγάλες κατηγορίες: πλατφόρμες CMS και website builders. [\[11\]](#)

Ενώ και οι δύο προσφέρουν ενσωματωμένες δυνατότητες, προσχεδιασμένα πρότυπα και επεκτάσεις για τη δημιουργία προσαρμοσμένου ιστότοπου με ή χωρίς κωδικοποίηση, παρουσιάζουν δύο πολύ διαφορετικές προσεγγίσεις για τη δημιουργία και τη διαχείριση ενός ιστότοπου. [\[11\]](#)

1.3.1 CMS ή Website Builder

Αν κάποιος ψάχνει για εργαλεία δημιουργίας ιστοτόπων και web hosting σε ένα μέρος, τα προγράμματα δημιουργίας ιστοτόπων (website builder) είναι η καλύτερη επιλογή. Ο ενδιαφερόμενος μπορεί να αγοράσει ένα custom domain, να προσαρμόσει την εμφάνιση του ιστότοπού του και να δημιουργήσει πλούσιες σελίδες πολυμέσων με προηγμένα στοιχεία όπως κινούμενα σχέδια και εφέ κύλισης. Ενώ ο χρήστης εστιάζει στο σχεδιασμό και το

περιεχόμενο, η πλατφόρμα φιλοξενίας θα φροντίζει για τη συντήρηση, την ασφάλεια, τη δημιουργία αντιγράφων ασφαλείας και πολλά άλλα.[11]

Ωστόσο, ως αντάλλαγμα για αυτήν την ευκολία χρήσης, πρέπει να εγκαταλειφθεί κάποια ευελιξία. Οι κατασκευαστές ιστοτόπων δεν διαθέτουν τις δυνατότητες διαχείρισης περιεχομένου, τις προηγμένες λειτουργίες και τις επιλογές προσαρμογής που θα βρείτε στις πλατφόρμες CMS. Για αυτόν τον λόγο, τα προγράμματα δημιουργίας ιστοτόπων είναι ιδανικά για πρακτορεία, καλλιτέχνες, εστιατόρια και άλλους τύπους χρηστών που θέλουν να δημιουργήσουν γρήγορα ιστοτόπους πλούσιους σε εικόνες.[11]

Για πιο προηγμένες δυνατότητες και επιλογές προσαρμογής, χρησιμοποιήστε ένα CMS. Με ένα CMS, μπορείτε να ελέγξετε πλήρως τη σχεδίαση του ιστότοπού σας, να προσθέσετε πολυμέσα στις αναρτήσεις σας, να οργανώσετε το περιεχόμενό σας ανά ετικέτες και κατηγορίες, να διαχειριστείτε πολλούς χρήστες, να επεξεργαστείτε τον υποκείμενο κώδικα του ιστότοπού σας και πολλά άλλα. Η διαδικασία εγκατάστασης και εκκίνησης του ιστότοπού σας θα είναι μεγαλύτερη, αλλά, στο τέλος, θα μπορείτε να δημιουργήσετε και να διαχειριστείτε έναν μεγαλύτερο και πιο περίπλοκο ιστότοπο που μπορεί να αναπτυχθεί με την πάροδο του χρόνου.[11]

1.3.2 Κριτήρια επιλογής CMS

Η κατάλληλη πλατφόρμα CMS για την κάθε επιχείρησή πρέπει να συμβαδίζει με τις ανάγκες και τους στόχους του εν λόγω ιστότοπού. Μερικοί από τους πιο σημαντικούς παράγοντες που πρέπει να ληφθούν υπόψη είναι η ευκολία χρήσης, η δυνατότητα προσαρμογής, η ασφάλεια, η τιμολόγηση και η επικράτηση στην αγορά.[18]

Εάν μια πλατφόρμα προσφέρει την ακριβή λειτουργικότητα που αναζητά ο χρήστης, αλλά είναι εκτός του οικονομικού του προϋπολογισμού, τότε δεν είναι η καλύτερη επιλογή. Από την άλλη πλευρά, μια φθηνή πλατφόρμα που θα απαιτεί πολλή συντήρηση και επεκτάσεις για να καλύψει τις ανάγκες του δεν είναι επίσης ιδανική.[11]

Ας ρίξουμε μια πιο προσεκτική ματιά σε καθένα από αυτά τα κριτήρια παρακάτω.

1.3.2.1 Ευκολία χρήσης [11][17]

Η ευκολία χρήσης είναι ένας ουσιαστικός παράγοντας που πρέπει να ληφθεί υπόψη κατά την επιλογή ενός CMS καθώς επηρεάζει σε μεγάλο βαθμό το ποσοστό υιοθέτησης και τις ροές εργασίας του εργατικού δυναμικού. Μια ιδανική πλατφόρμα θα είναι εύκολη στη χρήση για όλα τα ενδιαφερόμενα μέρη της ομάδας σας.

Ας πούμε ότι όλοι, από επαγγελματίες του μάρκετινγκ περιεχομένου έως προγραμματιστές, εργάζονται στο backend του CMS. Σε αυτήν την περίπτωση, χρειάζονται λειτουργίες CMS που διευκολύνουν κάθε ένα από αυτά τα μέλη της ομάδας να εκτελεί τις καθημερινές του εργασίες. Η σελίδα χρειάζεται μια πλατφόρμα που προσφέρει ένα πρόγραμμα επεξεργασίας WYSIWYG ώστε τα μέλη σύνταξης να δημιουργούν και να επεξεργάζονται γρήγορα περιεχόμενο και λειτουργικές μονάδες για να προστίθεται γρήγορα προσαρμοσμένος κώδικας από τους προγραμματιστές.

1.3.2.2 Εξατομίκευση [11]

Ενώ μπορεί να δίνεται προτεραιότητα στην ευκολία χρήσης έναντι της δυνατότητας προσαρμογής, ιδανικά θα θέλαμε μια λύση που να προσφέρει και τα δύο. Για παράδειγμα ένα CMS με πολλές επιλογές προσαρμογής και ευελιξία, όπως το CMS Hub, μπορεί να κλιμακώνεται καθώς αναπτύσσεται η επιχείρησή του χρήστη.

Κατά την αξιολόγηση ενός CMS, είναι απαραίτητο να δούμε ποιες επιλογές προσαρμογής είναι ενσωματωμένες στον πίνακα εργαλείων, πόσες επεκτάσεις είναι διαθέσιμες και αν μπορούμε να επεξεργαστούμε τον πηγαίο κώδικα. Εάν θέλουμε να δημιουργήσουμε έναν ιστότοπο με ελάχιστους πόρους ανάπτυξης, οι περισσότερες πλατφόρμες CMS επιτρέπουν την επιλογή προσχεδιασμένων θεμάτων και την προσαρμογή της σελίδας γύρω από την επιθυμητή επωνυμία. Ωστόσο, σε περίπτωση που κάποιος θέλει να προσλάβει έναν προγραμματιστή, πολλές πλατφόρμες CMS επιτρέπουν επίσης επιλογές κωδικοποίησης, ώστε να προστεθούν πιο προηγμένες λειτουργίες στον εν λόγω ιστότοπο.

1.3.2.3 Ασφάλεια [\[1\]](#)

Είναι αναγκαίο η πλατφόρμα που θα επιλέξουμε να κρατά ασφαλή το περιεχόμενό της σελίδας, τους χρήστες και τους επισκέπτες του front-end μας. Κατά την αξιολόγηση διαφορετικών προοπτικών, πρέπει να αποφασίσουμε ποιό ρόλο θα αναλαμβάνει η πλατφόρμα και ποιον ρόλο θα πρέπει να αναλάβουμε εμείς στην προστασία του ιστότοπου. Θα χρειαστεί να δημιουργήσουμε μη αυτόματα αντίγραφα ασφαλείας του ιστότοπου μας; Ενημέρωση του λογισμικού; Εγκατάσταση πρόσθετων ασφαλείας; Αγορά πιστοποιητικού SSL;

Αυτές είναι μόνο μερικές ερωτήσεις που πρέπει να θέσουμε όταν εξετάζουμε διαφορετικά συστήματα CMS. Ένας γενικός εμπειρικός κανόνας είναι πως εάν δεν έχετε τον χρόνο ή δεν είστε εξοικειωμένοι με τις βέλτιστες πρακτικές για την ασφάλεια του ιστότοπού σας, τότε χρειάζεστε μια πλατφόρμα με ισχυρά πρωτόκολλα ασφαλείας, δυνατότητες και ομάδες για να διατηρήσετε τον ιστότοπό σας ασφαλή.

1.3.2.4 Τιμή [\[1\]](#)

Ο προϋπολογισμός παίζει σημαντικό ρόλο σχεδόν σε κάθε απόφαση που παίρνουμε για την επιχείρησή μας. Όταν πρόκειται για το δικό μας CMS, θέλουμε μια λύση που να ανταποκρίνεται στις ανάγκες μας, τις προσδοκίες των επισκεπτών μας και τον προϋπολογισμό μας. Ευτυχώς, πολλές πλατφόρμες προσφέρουν διαφορετικές βαθμίδες προγραμμάτων με πόρους που κλιμακώνονται για κάθε τιμή, όπως το δωρεάν CMS του HubSpot. Όπως και οι επιλογές εξατομίκευσης, αυτές οι επιλογές αναβάθμισης υποδεικνύουν ότι το CMS θα μπορεί να αναπτύσσεται καθώς αναπτύσσεται η επιχείρησή σας.

1.3.2.5 Μεταφορά δεδομένων [\[1\]](#)

Μια εξαιρετική πλατφόρμα CMS θα πρέπει να διαθέτει εργαλεία για να μπορούμε να εξαγάγουμε εύκολα δεδομένα και να τα μετακινούμε αλλού. Για παράδειγμα, μπορεί αργότερα

να αποφασίσουμε να επιλέξουμε διαφορετική πλατφόρμα ή διαφορετική εταιρεία φιλοξενίας. Η φορητότητα δεδομένων μας διευκολύνει να μετακινηθούμε με απόλυτη ελευθερία.

1.3.2.6 Επικράτηση στην αγορά [11]

Ένας πολύ καλός τρόπος για να περιορίσουμε τις επιλογές των συστημάτων CMS είναι κοιτάζοντας την τρέχουσα λίστα του κάθε συστήματος και τους επιτυχημένους πελάτες του, όπως μεγάλες μάρκες ή ανταγωνιστές. Εάν αξιόπιστες επωνυμίες σε κλάδους παρόμοιους με τους δικούς μας χρησιμοποιούν ένα συγκεκριμένο CMS, αυτό θα μπορούσε να σημαίνει ότι οι δυνατότητες της πλατφόρμας είναι πολύτιμες και μπορούν να επεκταθούν σε μια αναπτυσσόμενη εταιρεία. Ακόμα κι αν εργάζεστε ήδη με ένα CMS, μπορεί να αισθάνεστε ότι το τρέχον εργαλείο δεν εκπληρώνει τους στόχους σας ή ίσως θέλετε να συμβαδίσετε με τις στρατηγικές CMS άλλων επιτυχημένων επωνυμιών.

Επιπλέον, το να παρακολουθήσετε πλατφόρμες CMS και ιστότοπους που χρησιμοποιούνται από επωνυμίες στον κλάδο σας μπορεί να σας δώσει έμπνευση για τη δική σας στρατηγική περιεχομένου.

Αυτά τα κριτήρια μπορεί να ταξινομούνται διαφορετικά ανάλογα με τη δική σας διαδικασία επιλογής, ωστόσο το καθένα είναι σημαντικό για την επιλογή ενός CMS που μπορεί να υποστηρίξει και να αναπτυχθεί μαζί με την επιχείρησή σας.

1.4 Οι πιο δημοφιλείς CMS πλατφόρμες

Όπως αναφέρθηκε παραπάνω μια πλατφόρμα CMS (πλατφόρμα συστήματος διαχείρισης περιεχομένου) είναι ένα κομμάτι λογισμικού που μας επιτρέπει να διαχειριζόμαστε εύκολα περιεχόμενο και να δημιουργούμε ιστότοπους. Μερικές από τις πιο δημοφιλείς πλατφόρμες CMS είναι αυτές που θα αναφερθούν παρακάτω.

1.4.1 CMS Hub [19]

Το HubSpot CMS είναι μία από τις κορυφαίες επιλογές CMS για τη δημιουργία ιστότοπου χωρίς την ανάγκη συνεχών ενημερώσεων και τροποποιήσεων. Είναι ιδανικό και για αρχάριους, καθώς τα φιλικά προς τον χρήστη εργαλεία αυτής της πλατφόρμας μπορούν να βοηθήσουν στη δημοσίευση ενός ιστότοπου χωρίς τεχνικές γνώσεις. Τα εξαιρετικά ενσωματωμένα εργαλεία πωλήσεων και μάρκετινγκ συμβάλλουν επίσης στην αύξηση της απήχησης και της ενεργής συμμετοχής.

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:

- Αύξημένη συμμετοχή με τη χρήση εργαλείων ηλεκτρονικού ταχυδρομείου και των κοινωνικών μέσων.
- Παρέχεται μια αποκλειστική ομάδα για την παρακολούθηση της πλατφόρμας 24/7 για να ελέγχει για επιθέσεις και να χειρίζεται τακτικές σαρώσεις ιών.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:

- Περιορισμένη συλλογή από προσθήκες και θέματα.
- Δεν παρέχεται άμεση τεχνική υποστήριξη.

Τα προγράμματα τιμολόγησης του CMS Hub είναι:

- Το πρόγραμμα εκκίνησης, κοστίζει 23 \$/μήνα.
- Το επαγγελματικό σχέδιο, κοστίζει 360 \$/μήνα.
- Το επιχειρηματικό σχέδιο, κοστίζει 1.200 \$/μήνα.

Μερικές από τις επιχειρήσεις που χρησιμοποιούν το CMS Hub είναι οι:

- Trello
- The Chopping Block

1.4.2 WordPress

Το WordPress, κυκλοφόρησε αρχικά ως λογισμικό blogging, και στην συνέχεια εξελίχθηκε στην πιο δημοφιλή πλατφόρμα CMS που δημιουργήθηκε ποτέ. Λόγω της φύσης αυτής της πλατφόρμας ανοιχτού κώδικα, η οποία δίνει έμφαση στα χαρακτηριστικά σύνταξης όπως τη δημοσίευση άρθρων και ιστολογίων, χρησιμοποιείται τακτικά σε εκδόσεις και σε βιομηχανίες φιλικές προς το blogging. Επειδή η διεπαφή και τα θέματα του ιστότοπού του είναι αρκετά απλά στη χρήση, είναι ιδιαίτερα χρήσιμο για μικρότερες επιχειρήσεις που απλώς αναπτύσσουν τη στρατηγική τους στον ιστό ή έχουν λιγότερη εμπειρία με το σχεδιασμό.

Εάν κάποιος επεξεργαστής ιστού ή προγραμματιστής με γνώσεις τεχνολογίας θέλει να προσθέσει προσαρμογές στον ιστότοπό του, το WordPress επιτρέπει μια σειρά από προσθήκες και άλλες ευκαιρίες εξατομίκευσης.^[11]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: ^{[4][6]}

- Το WordPress σας προσφέρει την ευελιξία και την ελευθερία να δημιουργήσετε οποιοδήποτε είδος ιστότοπου (διαδικτυακό κατάστημα, ιστότοπο δημοπρασιών, ιστότοπο συνδρομής κ.λπ.).
- Δεν απαιτεί τεχνικές δεξιότητες ή γνώσεις κωδικοποίησης. Το πρόγραμμα επεξεργασίας μπλοκ WordPress διευκολύνει πραγματικά τη δημιουργία σελίδων εξαιρετικής εμφάνισης στον ιστότοπό σας.
- Έχετε απόλυτη ελευθερία να κερδίσετε χρήματα online από τον ιστότοπό σας με όποιον τρόπο θέλετε.
- Υπάρχουν χιλιάδες θέματα και WordPress plugins διαθέσιμα, τόσο επί πληρωμή όσο και δωρεάν. Αυτά σας επιτρέπουν να προσθέτετε κάθε είδους χρήσιμα πρόσθετα στον ιστότοπό σας, όπως φόρμες επικοινωνίας, γκαλερί φωτογραφιών και πολλά άλλα.
- Το WordPress είναι πραγματικά καλά σχεδιασμένο για τη βελτιστοποίηση μηχανών αναζήτησης (SEO). Είναι εύκολο να δημιουργήσετε διευθύνσεις URL, κατηγορίες και ετικέτες φιλικές προς το SEO για τις αναρτήσεις σας. Μπορείτε επίσης να επιλέξετε από πολλές προσθήκες SEO για να σας βοηθήσουν να κάνετε περισσότερα.
- Υπάρχει μια τεράστια και υποστηρικτική κοινότητα γύρω από το WordPress, καθώς είναι ένα CMS ανοιχτού κώδικα. Μπορείτε να εγγραφείτε σε ομάδες όπως το WPBeginner Engage στο Facebook για να λάβετε βοήθεια για τυχόν προβλήματα που αντιμετωπίζετε.
- Το WordPress προσφέρει μεγάλη επεκτασιμότητα, κάτι που το καθιστά ιδανική πλατφόρμα CMS τόσο για αρχάριους όσο και για προγραμματιστές.
- Το WordPress σας επιτρέπει να κατεβάζετε όλο το περιεχόμενό σας σε μορφή XML, καθιστώντας εύκολη τη μετάβαση σε διαφορετικό σύστημα στο μέλλον, εάν το επιλέξετε.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:[4][8]

- Οι χρήστες χρειάζεται να ρυθμίσουν μόνοι τους το hosting και το domain name τους και είναι υπεύθυνοι για τη διαχείριση πραγμάτων όπως η ασφάλεια και τα αντίγραφα ασφαλείας.
- Επειδή το WordPress προσφέρει τόσες πολλές επιλογές και τόση ευελιξία, μπορεί μερικές φορές να φαίνεται λίγο τρομακτικό στους αρχάριους. Αυτός είναι ο λόγος για τον οποίο πολλοί αρχάριοι χρησιμοποιούν πρόσθετα δημιουργίας σελίδων μεταφοράς και απόθεσης για το WordPress.

Ως λογισμικό ανοιχτού κώδικα, το WordPress είναι δωρεάν για λήψη. Ωστόσο, πρέπει να πληρώσετε για ένα domain name, το hosting και τυχόν premium plugins ή θέματα που θέλετε να εγκαταστήσετε. Αν και αυτό σημαίνει ότι το κόστος κατασκευής και διαχείρισης ιστότοπων WordPress μπορεί να κυμαίνεται δραματικά, το μέσο κόστος είναι σχετικά μέτριο. Σύμφωνα με το Website Builder Expert, η δημιουργία ενός ιστότοπου WordPress θα σας κοστίσει μια εφάπαξ χρέωση 200 \$ και η διαχείρισή του θα κοστίσει μεταξύ 11 και 40 \$ το μήνα.[11]

Μερικές από τις επιχειρήσεις που χρησιμοποιούν το WordPress είναι οι: [11]

- TechCrunch
- IKEA

1.4.3 Drupal

Το Drupal είναι μια άλλη πλατφόρμα CMS ανοιχτού κώδικα. Είναι το CMS πάνω στο οποίο έχουν χτιστεί ορισμένοι σημαντικοί ιστότοποι, συμπεριλαμβανομένου του The Economist και ορισμένων ιστοτόπων πανεπιστημίων.[4]

Η συγκεκριμένη πλατφόρμα είναι μια καλή επιλογή για προγραμματιστές ή για άτομα που μπορούν να προσλάβουν έναν προγραμματιστή. Είναι ιδιαίτερα καλό αν σκοπεύετε να δημιουργήσετε έναν εξαιρετικά προσαρμοσμένο ιστότοπο που χρειάζεται να χειρίζεται πολλά δεδομένα.[4]

Ένας ιστότοπος Drupal μπορεί να φιλοξενηθεί στο SiteGround. Το SiteGround προσφέρει δωρεάν εγκατάσταση και μπορεί ακόμη και να μας βοηθήσει να μεταφέρουμε μια υπάρχουσα τοποθεσία Drupal.[4]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:[4]

- Είναι εύκολο να προστεθεί περιεχόμενο. Οι προσαρμοσμένοι τύποι περιεχομένου είναι ευέλικτοι και προσφέρουν πολλές επιλογές.
- Υπάρχουν πολλές διαφορετικές ενότητες διαθέσιμες που μπορούν να προστεθούν στον ιστότοπο μας (αυτές λειτουργούν σαν πρόσθετα WordPress).
- Η υποστήριξη είναι διαθέσιμη μέσω επιλογών υποστήριξης κοινότητας παρόμοιες με άλλες δημοφιλείς πλατφόρμες όπως το Joomla και το WordPress
- Η διαχείριση χρηστών είναι εύκολη, με ένα ενσωματωμένο σύστημα όπου μπορούν να δημιουργηθούν νέοι ρόλοι με καθορισμένα δικαιώματά.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:[4]

- Ορισμένες φορές είναι δύσκολο στους χρήστες να καταλάβουν πώς να αλλάξουν την εμφάνιση του ιστότοπού τους ή να προσθέσουν πρόσθετα. Σίγουρα δεν είναι τόσο φιλικό για αρχάριους όσο το WordPress.

- Οι περισσότεροι ιστότοποι του Drupal έχουν ένα ιδιαίτερα προσαρμοσμένο θέμα που δημιουργήθηκε από έναν προγραμματιστή, το οποίο μπορεί να είναι αρκετά ακριβό.

Μερικές από τις επιχειρήσεις που χρησιμοποιούν το Drupal είναι οι:[11]

- Unicef
- Pinterest

1.4.4 Joomla

Το Joomla είναι μια άλλη δημοφιλής δωρεάν πλατφόρμα CMS ανοιχτού κώδικα που συνοδεύεται από πολλά διαφορετικά πρότυπα και επεκτάσεις. Είναι δωρεάν στη χρήση, αλλά θα χρειάζεται φιλοξενία και ένα domain name.[4]

Κυκλοφόρησε για πρώτη φορά το 2005, έτσι όπως το WordPress, και λειτουργεί εδώ και χρόνια. Το Joomla είναι γεμάτο με δυνατότητες και πολλοί οικοδεσπότες ιστού προσφέρουν εγκατάσταση με ένα κλικ. Είναι πραγματικά μια ιδανική πλατφόρμα CMS για προγραμματιστές και έμπειρους δημιουργούς ιστότοπων, επομένως δεν είναι τόσο καλή επιλογή για αρχάριους.[4]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:[4]

- Το Joomla προσφέρει μεγάλη ευελιξία και πολλές επιλογές. Είναι μια καλή επιλογή εάν χτίζουμε κάτι περίπλοκο ή κατά παραγγελία.
- Αν και το Joomla είναι ιδιαίτερα χρήσιμο για προγραμματιστές, μπορεί να χρησιμοποιηθεί ακόμα κι αν δεν θέλουμε να αγγίζουμε ούτε μια γραμμή κώδικα καθώς είναι εύκολη η επεξεργασία περιεχομένου.
- Όπως το WordPress, το Joomla είναι πλατφόρμα ανοιχτού κώδικα και υπάρχει διαθέσιμη πολλή υποστήριξη κοινότητας εάν κολλήσουμε κάπου.
- Μπορεί να χρησιμοποιηθεί για να δημιουργήσουμε καταστήματα ηλεκτρονικού εμπορίου, καθώς υπάρχουν διαθέσιμες επεκτάσεις και για αυτό.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:[4]

- Ακόμη και οι θαυμαστές του Joomla θα παραδεχτούν ότι μπορεί να είναι αρκετά περίπλοκο. Ανάλογα με το τι θέλουμε να κάνουμε, ίσως χρειαστεί να προσλάβουμε έναν προγραμματιστή για να μας βοηθήσει.
- Δεν υπάρχουν τόσες πολλές επιλογές για πρόσθετες επεκτάσεις. Εάν έχετε συνηθίσει σε ένα CMS όπως το WordPress, το οποίο έχει χιλιάδες διαθέσιμα θέματα και πρόσθετα που επεκτείνουν τη βασική λειτουργικότητα, μπορεί να απογοητευτείτε από το Joomla.
- Μπορεί να υπάρχουν ορισμένα προβλήματα συμβατότητας εάν εγκαταστήσουμε πολλές διαφορετικές επεκτάσεις και λειτουργικές μονάδες.

Το Joomla είναι δωρεάν, αν και θα χρειαστεί να πληρώσετε για όνομα τομέα και φιλοξενία ιστού που υποστηρίζει Joomla. Το SiteGround είναι μια καλή επιλογή εδώ, καθώς έχουν συγκεκριμένα προγράμματα φιλοξενίας Joomla με πολλές εύχρηστες δυνατότητες.

Μπορεί να χρειαστεί να πληρώσετε για ορισμένες επεκτάσεις για να προσθέσετε περισσότερη λειτουργικότητα στον ιστότοπό σας. Ίσως θελήσετε ακόμη και να βάλετε προϋπολογισμό για να λάβετε βοήθεια από έναν προγραμματιστή, ανάλογα με το τι προσπαθείτε να επιτύχετε. Συνολικά, τα δεδομένα από το CMS2CMS δείχνουν ότι η λειτουργία ενός ιστότοπου στο Joomla θα κοστίζει 700 έως 6.500 \$ κατά μέσο όρο.[4]

Ορισμένες επιχειρήσεις που χρησιμοποιούν το Joomla είναι οι εξής: [\[11\]](#)

- Ariel Investments
- Nintendo Nordic

1.4.5 Shopify

Το Shopify είναι μια άλλη πλατφόρμα CMS που φιλοξενείται all-in-one. Δεν θα χρειαστεί να αγοράσετε φιλοξενία, να εγκαταστήσετε οποιοδήποτε λογισμικό ή να διαχειριστείτε πράγματα όπως ενημερώσεις και αντίγραφα ασφαλείας. Έχει μια απλή διεπαφή μεταφοράς και απόθεσης. Υποστηρίζει πωλήσεις εντός καταστήματος, κάτι που είναι εξαιρετικό αν έχετε φυσικό κατάστημα καθώς και διαδικτυακό.[\[4\]](#)

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [\[4\]](#)

- Η πλατφόρμα αποδέχεται πιστωτικές και χρεωστικές κάρτες μέσω της ολοκληρωμένης λύσης πληρωμής του Shopify, Shopify Payments. Το PayPal περιλαμβάνεται επίσης ως ένας από τους προεπιλεγμένους παρόχους πληρωμών του Shopify.
- Υπάρχουν πολλές επεκτάσεις και θέματα διαθέσιμα για το Shopify. Μπορείτε να αγοράσετε εφαρμογές Shopify τρίτων που σας επιτρέπουν να προσθέτετε κάθε είδους δυνατότητες στο ηλεκτρονικό σας κατάστημα.
- Δεν χρειάζεται να κάνετε αναβάθμιση εάν κάνετε πωλήσεις πάνω από ένα συγκεκριμένο ποσό σε δολάρια, όπως κάνετε με το BigCommerce.
- Το Shopify έχει υποστήριξη 24/7 μέσω ζωντανής συνομιλίας, email, τηλεφώνου, ακόμη και Twitter. Υπάρχει επίσης πολλή διαθέσιμη τεκμηρίωση (συμπεριλαμβανομένων γραπτών οδηγιών και εκπαιδευτικών βίντεο) καθώς και διαδικτυακά φόρουμ.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [\[4\]](#)

- Το κόστος μπορεί να καταλήξει αρκετά υψηλό, ειδικά αν θέλουμε να προσθέσουμε πολλές εφαρμογές τρίτων στο κατάστημά μας.
- Μπορεί να διαπιστώσετε ότι θέλετε να προσθέσετε λειτουργίες που απλά δεν είναι διαθέσιμες: οι εφαρμογές του Shopify είναι πιο περιορισμένες από πράγματα όπως τα πρόσθετα του WordPress.

Το Shopify είναι μια ιδιόκτητη πλατφόρμα που προσφέρει τρία προγράμματα επί πληρωμή. Ξεκινώντας από 29 \$ ανά μήνα, τα προγράμματα Shopify περιλαμβάνουν φιλοξενία ιστού, πιστοποίηση SSL και υποτομέα Shopify (yourname.shopify.com). Εάν θέλετε έναν προσαρμοσμένο τομέα, αυτό θα είναι ένα επιπλέον κόστος. Για επιπλέον θέσεις και άλλες προηγμένες λειτουργίες, όπως δωροκάρτες και περισσότερες αναφορές, μπορείτε να κάνετε αναβάθμιση σε "Shopify" με 79 \$ το μήνα. Καθώς συνεχίζετε να αναπτύσσετε, μπορείτε να κάνετε αναβάθμιση στο "Advanced Shopify" για 299 \$ το μήνα για ακόμη περισσότερες θέσεις, αναλυτικά στοιχεία και εκπτώσεις στις χρεώσεις διεκπεραίωσης πληρωμών. [\[11\]](#)

Ορισμένες επιχειρήσεις που χρησιμοποιούν το Shopify είναι οι εξής: [\[11\]](#)

- Briogeo
- Pipcorn

1.4.6 Magento

Το Magento είναι μια ισχυρή πλατφόρμα ηλεκτρονικού εμπορίου ανοιχτού κώδικα από την τεράστια εταιρεία λογισμικού Adobe. Υπάρχει μια δωρεάν έκδοση που μπορείτε να κατεβάσετε και να εγκαταστήσετε στον δικό σας λογαριασμό web hosting, που ονομάζεται Magento Open Source. Εάν θέλετε να χρησιμοποιήσετε αυτή την πλατφόρμα, τότε η φιλοξενία SiteGround Magento θα ήταν ο ευκολότερος τρόπος για να ξεκινήσετε. Εάν προτιμάτε, τότε μπορείτε να πληρώσετε για το Magento Commerce. Αυτό παρέχεται με πλήρη υποστήριξη και δικό του hosting, αλλά είναι αρκετά ακριβό.^[4]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: ^[4]

- Το Magento είναι εξαιρετικά προσαρμόσιμο, με πολλές διαθέσιμες επεκτάσεις τρίτων που μπορείτε να χρησιμοποιήσετε για να προσθέσετε επιπλέον λειτουργίες.
- Με το Magento, μπορείτε να χειριστείτε πολλά προϊόντα και πελάτες. Επιτρέπει στην επιχείρησή σας να αναπτυχθεί εύκολα, χωρίς να επιβραδύνεται ο ιστότοπός σας. (Πιθανότατα ωστόσο θα χρειαστεί να αναβαθμίσετε το πρόγραμμα φιλοξενίας σας.)
- Υπάρχουν μερικές πολύ μεγάλες επωνυμίες που χρησιμοποιούν το Magento, συμπεριλαμβανομένων των Nike, Ford και Coca Cola.
- Μπορείτε να συνδέσετε διαφορετικές πύλες πληρωμής στο Magento. Έρχεται επίσης με ορισμένες επιλογές, όπως το PayPal, την αντικαταβολή και την τραπεζική μεταφορά που έχει ήδη ενσωματωθεί.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: ^[4]

- Εάν μόλις ξεκινάτε στο ηλεκτρονικό εμπόριο, το Magento μπορεί να φαίνεται συντριπτικό.
- Μπορεί να είναι δύσκολο να βρείτε καλούς προγραμματιστές για έργα Magento και μπορεί να είναι πολύ ακριβό να τους προσλάβετε.
- Η διαθέσιμη υποστήριξη μπορεί να ποικίλλει, ιδιαίτερα εάν χρησιμοποιείτε το Magento Open Source και βασίζεστε σε διαδικτυακά φόρουμ για βοήθεια.

Το Magento Commerce δεν είναι φθηνό. Στην πραγματικότητα, είναι τόσο ακριβό που ο ιστότοπος του Magento δεν σας λέει καν πόσο κοστίζει. Οι τιμές ξεκινούν από περίπου 22.000 \$/έτος, γεγονός που το βάζει εκτός του προϋπολογισμού πολλών νέων επιχειρήσεων. Ωστόσο, εάν θέλετε μια ισχυρή πλατφόρμα CMS ηλεκτρονικού εμπορίου για μια καθιερωμένη επιχείρηση, θα μπορούσε να είναι μια επιλογή που πρέπει να εξετάσετε. Πολλά μεγαλύτερα καταστήματα μεταναστεύουν είτε στο WooCommerce, στο Shopify ή στο BigCommerce.^[4]

Ορισμένες επιχειρήσεις που χρησιμοποιούν το Magento πέρα από αυτές που αναφέρθηκαν παραπάνω είναι οι εξής: ^[11]

- Yakima
- Boodles

1.4.7 Magnolia

Το Magnolia είναι ένα ακέφαλο, όλα-σε-ένα σύστημα που έχει δημιουργηθεί για τη διαχείριση ψηφιακών εμπειριών πολλών τοποθεσιών, πολλών γλωσσών και πολλών καναλιών. Οι αγοραστές έχουν δύο επιλογές για να διαλέξουν: υπηρεσία cloud ή εξυπηρέτηση πελατών. Η υπηρεσία που βασίζεται στο cloud επιτρέπει στις εταιρείες να

ξεκινούν έργα γρήγορα χωρίς να χρειάζονται devops ή βοήθεια IT, ενώ η επιλογή φιλοξενίας πελάτη επιτρέπει στις εταιρείες να έχουν προσαρμοσμένη ανάπτυξη και ενσωμάτωση Java στη δική τους υποδομή.[11]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [10]

- Περιλαμβάνει εύχρηστες αναρτήσεις και επιλογές διαχείρισης περιεχομένου.
- Παρέχει ένα ισχυρό πρόγραμμα επεξεργασίας που μας επιτρέπει να μορφοποιούμε το περιεχόμενό μας με ευκολία.
- Είναι εξαιρετικά προσαρμόσιμο, χάρη στα χιλιάδες πρόσθετα και θέματα.
- Έχει μια ισχυρή και πολύ ενεργή κοινότητα.
- Περιλαμβάνει υποστήριξη για πολύγλωσσους ιστότοπους.
- Μας επιτρέπει να διαχειριζόμαστε πολλαπλούς ιστότοπους από μία εγκατάσταση.
- Καθιστά δυνατή την κοινή χρήση δεδομένων και εργαλείων μεταξύ των ιστότοπων μας.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [10]

- Εστιάζει περισσότερο σε χρήστες με εμπειρία στην ανάπτυξη ιστοσελίδων και στον σχεδιασμό σύνθετων ιστοσελίδων.
- Υψηλή καμπύλη μάθησης.
- Το πρόβλημα της μεταφόρτωσης και δημοσίευσης αρχείων που είναι τεράστια/μεγάλα γίνεται αισθητό στη Magnolia.

Η Magnolia λειτουργεί βάσει ενός μοντέλου τιμολόγησης προσφοράς που βασίζεται στις ατομικές επιχειρηματικές σας ανάγκες. Θα χρειαστεί να επικοινωνήσετε απευθείας μαζί τους για διαβούλευση για να λάβετε μια εξατομικευμένη προσφορά.[11]

Ορισμένες επιχειρήσεις που χρησιμοποιούν το Magnolia είναι οι εξής: [11]

- BMW
- Atlassian

1.4.8 TYPO3

Το TYPO3 είναι μια δωρεάν, ανοιχτού κώδικα πλατφόρμα CMS που κυκλοφόρησε αρχικά το 1998. Είναι ένα εταιρικό CMS, που σημαίνει ότι είναι χρήσιμο για τοποθεσίες intranet (εσωτερικές εταιρικές τοποθεσίες) καθώς και για ιστότοπους. Υπάρχει ένας αριθμός διαθέσιμων επεκτάσεων για το TYPO3 που προσφέρουν επιπλέον λειτουργικότητα.[4]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [4]

- Το TYPO3 μπορεί να χειριστεί πραγματικά μεγάλους ιστότοπους, συμπεριλαμβανομένων αυτών που έχουν πολλούς ιστότοπους σε διαφορετικές γλώσσες. Είναι μια καλή επιλογή για μεγάλες διεθνείς εταιρείες.
- Επειδή είναι ανοιχτού κώδικα, το TYPO3 μπορεί να επεκταθεί όπως θέλετε, εάν θέλετε μπορείτε να προσλάβετε ακόμα και έναν προγραμματιστή για να εργαστεί για εσάς.
- Μπορείτε εύκολα να τροποποιήσετε τα δικαιώματα πρόσβασης διαφορετικών ατόμων και ομάδων που εργάζονται στον ιστότοπό σας.
- Υπάρχουν περισσότερες από 6.000 επεκτάσεις και εφαρμογές που μπορείτε να προσθέσετε στον ιστότοπό TYPO3 σας για να συμπεριλάβετε νέες δυνατότητες.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής: [4]

- Δεν υπάρχουν τόσα πολλά διαθέσιμα θέματα, επομένως πιθανότατα θα πρέπει να προσλάβετε κάποιον για να δημιουργήσει ένα για εσάς.
- Θα χρειαστείτε αρκετά υψηλό βαθμό τεχνικής εξειδίκευσης για να θέσετε σε λειτουργία το TYPO3 και να το διατηρήσετε.

Εκτός από το μέσο κόστος των 15 \$ ετησίως για την εγγραφή τομέα, η φιλοξενία ενός ιστότοπου TYPO3 κυμαίνεται από 6 έως 69 \$ ανά μήνα. Το μέσο κόστος των premium προτύπων και επεκτάσεων TYPO3 είναι 49 \$. Το μεγαλύτερο κόστος δημιουργίας και διαχείρισης ενός ιστότοπου TYPO3 είναι η πρόσληψη ενός προγραμματιστή ή μιας εταιρείας για να βοηθήσει στη διαδικασία. Τα καλά νέα είναι ότι μπορείτε να βρείτε πιστοποιημένη βοήθεια απευθείας στον ιστότοπο του TYPO3. Τα κακά νέα είναι ότι η τιμή μπορεί να κυμαίνεται από μερικές εκατοντάδες έως μερικές χιλιάδες δολάρια, ανάλογα με τη διάρκεια και το εύρος του έργου web.^[11]

Μία επιχείρηση που χρησιμοποιεί το TYPO3 είναι η: ^[11]

- Pearson

1.4.9 Prestashop

Το PrestaShop είναι μια πλατφόρμα CMS ηλεκτρονικού εμπορίου ανοιχτού κώδικα. Χρειάζεται να το φιλοξενήσετε μόνοι σας, ώστε να μπορέσετε να το εγκαταστήσετε σε οποιοδήποτε web host που το υποστηρίζει. Συνιστάται η χρήση της φιλοξενίας PrestaShop του SiteGround.^[4]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:^[4]

- Υπάρχει μεγάλη κοινότητα στο PrestaShop. Αυτό περιλαμβάνει ένα επίσημο φόρουμ όπου μοιράζονται συμβουλές και σεμινάρια, καθώς και πολλές άλλες ομάδες.
- Δεν θα χρειαστεί να πληρώσετε επιπλέον καθώς το κατάστημά σας μεγαλώνει (εκτός αν χρειαστεί να αναβαθμίσετε το πρόγραμμα φιλοξενίας σας).
- Υπάρχουν πολλές μονάδες PrestaShop, ώστε να μπορείτε να προσθέτετε εύκολα νέες δυνατότητες.
- Δεν κοστίζει πολύ για να ξεκινήσετε με το PrestaShop, ειδικά αν βρίσκεστε σε ένα φτηνό πρόγραμμα κοινόχρηστης φιλοξενίας.

Τα μειονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:^[4]

- Το PrestaShop μπορεί να έχει μια αρκετά απότομη καμπύλη εκμάθησης για αρχή.
- Υπάρχουν πολλά θέματα (σχέδια) διαθέσιμα από το PrestaShop, αλλά πολλά από αυτά δεν είναι πολύ καλά. Ίσως χρειαστεί να αφιερώσετε πολύ χρόνο να τα ψάχνετε για να βρείτε κάτι που θα λειτουργήσει για το ηλεκτρονικό σας κατάστημα.

Το PrestaShop είναι δωρεάν, αν και θα χρειαστεί να πληρώσετε για τη φιλοξενία ιστού και ένα όνομα τομέα. Ωστόσο, οι ενότητες και τα θέματα που διατίθενται μέσω του PrestaShop Addons Marketplace θα μπορούσαν να κοστίσουν αρκετά. Τα περισσότερα ξεκινούν από 59,99 \$.^[4]

Μία επιχείρηση που χρησιμοποιεί το TYPO3 είναι η: ^[11]

- Freshly Cosmetics

1.4.10 Concrete5

Το Concrete είναι ένα CMS ανοιχτού κώδικα που έχει σχεδιαστεί για να καλύψει ένα κενό στην αγορά. Το Concrete5 δεν είναι ένα περίπλοκο ή τρομακτικό CMS που έχει σχεδιαστεί από προγραμματιστές για προγραμματιστές — και δεν είναι ένα υπερβολικά απλοποιημένο CMS τύπου "κάντο μόνος σου". Έχει σχεδιαστεί για να προσφέρει τις καλύτερες πλευρές και των δύο κόσμων.^[11]

Τα πλεονεκτήματα της συγκεκριμένης πλατφόρμας είναι τα εξής:^[12]

- Δεδομένου ότι το Concrete5 είναι ανοιχτού κώδικα, θα έχετε τη δυνατότητα να τροποποιείτε και να διανέμετε ελεύθερα τον κώδικα χωρίς να ανησυχείτε για τα τέλη αδειοδότησης.
- Το Concrete5 προσφέρει τη μοναδική δυνατότητα μεταφοράς και απόθεσης μπλοκ περιεχομένου μέσα σε ένα πρότυπο, προσφέροντας εκπληκτικές οργανωτικές ικανότητες και εύκολη επεξεργασία.
- Είναι εύκολο στη χρήση και την εγκατάσταση για άτομα με μικρή εμπειρία στο web development ή στον κώδικα.
- Το Concrete5 προσφέρει πολλά εργαλεία SEO για την προσθήκη Meta Descriptions ενώ ταυτόχρονα συμβάλλει στο να διασφαλιστεί ότι ο ιστότοπός σας θα είναι εύκολα ανιχνεύσιμος από την Google.
- Με το Concrete5 έχετε τη δυνατότητα να εκχωρήσετε διάφορα δικαιώματα βάσει διαφορετικών επιπέδων διαχείρισης, ελέγχοντας τι μπορούν και τι δεν μπορούν να επεξεργαστούν διάφορα άτομα στον ιστότοπο.

Το μειονέκτημα της συγκεκριμένης πλατφόρμας είναι:^[12]

- Το Concrete5 έχει πολύ μικρότερη κοινότητα που σημαίνει ότι η εύρεση απαντήσεων στις ερωτήσεις σας και η βοήθεια με τα προβλήματά σας είναι πιο δύσκολη από ό,τι με άλλα συστήματα διαχείρισης περιεχομένου.

Δεδομένου ότι το ConcreteCMS είναι ανοιχτού κώδικα, πρέπει απλώς να εξετάσετε πόσο θα κοστίσει η εγγραφή στον domain, η φιλοξενία, τα premium modules και τα θέματα. Η εγγραφή στο domain και η φιλοξενία είναι παρόμοιες με άλλες πλατφόρμες ανοιχτού κώδικα. Η πλατφόρμα κοστίζει περίπου 15 \$ ετησίως για ένα domain και από \$3 έως \$60 το μήνα για τη φιλοξενία. Το μέσο κόστος μιας μονάδας premium είναι \$25 και το μέσο κόστος ενός premium θέματος είναι \$40. Αυτό τοποθετεί το σύνολο μεταξύ \$50 και \$800 ετησίως για μια ιστοσελίδα Concrete5. ^[11]

1.5 Επιλέγουν οι προγραμματιστές ιστοσελίδων να δουλέψουν με CMS πλατφόρμες;

Ορισμένοι προγραμματιστές ιστού μάλλον θα υποστήριζαν ότι ένα σύστημα διαχείρισης περιεχομένου (CMS) είναι χτισμένο με τέτοιο τρόπο ώστε να εξαλείφει την ανάγκη για κωδικοποίηση, επομένως περικλύπτει πλήρως ένα μεγάλο μέρος μιας εργασίας προγραμματιστή ιστού. Ωστόσο, μπορούμε να πούμε με ασφάλεια, πως η χρήση ενός CMS εξακολουθεί να παρέχει πολλά οφέλη όσον αφορά τη διαδικασία δημιουργίας και συντήρησης μιας ιστοσελίδας.^[20]

Όπως αναφέρθηκε και παραπάνω, ο κύριος στόχος ενός CMS είναι να παρέχει ένα έξυπνο περιβάλλον χρήστη για τη δημιουργία και τη διαχείριση του περιεχομένου των ιστοσελίδων. Με την προσθήκη ενός εύχρηστου εργαλείου δημοσίευσης ιστού, δίνει στις εταιρείες την

ευκαιρία να διαχειρίζονται τον δικό τους ιστότοπο, κάτι που πολλές φορές είναι μια εργασία που οι περισσότερες επιχειρήσεις και οι εργαζόμενοι δεν θα είχαν τη δυνατότητα ή την πρόσβαση να κάνουν.[20]

Ας επικεντρωθούμε στο κεντρικό ερώτημα αυτού του κεφαλαίου που είναι “Είναι σοφό ένας προγραμματιστής ιστού να χρησιμοποιεί πλατφόρμες CMS;”. Ανεξάρτητα από το γεγονός ότι ένα σύστημα διαχείρισης περιεχομένου μπορεί να εξαλείψει την ανάγκη χρήσης μεγάλου κομματιού κώδικα κατά την κατασκευή ενός ιστότοπου και μπορεί να θεωρηθεί ως η ψηφιακή έκδοση ενός Lego για έναν προγραμματιστή ιστού, τα CMS φαίνεται πως ήρθαν για να μείνουν. [20]

Παρόλο που τα πράγματα μοιάζουν λίγο μονοδιάστατα, ένας προγραμματιστής ιστού έχει ακόμα πολλά εργαλεία στη διάθεσή του προκειμένου να επεκτείνει και να τροποποιήσει έναν ιστότοπο μέσω μιας μεγάλης γκάμα διαθέσιμων προτύπων και προσθηκών που παρέχονται από τα συστήματα διαχείρισης περιεχομένου. Ένας συντάκτης περιεχομένου δεν θα έχει ποτέ τον πλήρη έλεγχο του σχεδιασμού και της δομής ενός ιστότοπου, πράγμα που σημαίνει ότι η προσαρμοσμένη εργασία θα απαιτεί την τεχνογνωσία ενός προγραμματιστή ιστού.[20]

Οι προγραμματιστές που χρησιμοποιούν CMS πλατφόρμες απολαμβάνουν αρκετά προνόμια όπως:

- Η πραγματοποίηση αλλαγών όσον αφορά την συντήρηση ενός ιστότοπου και η ενημέρωση λογισμικού είναι ευκολότερη, καθώς οι αλλαγές σε ολόκληρο τον ιστότοπο είναι πολύ πιο γρήγορες.
- Οι αλλαγές όσον αφορά το σχεδιασμό της ιστοσελίδας είναι επίσης πολύ πιο εύκολο να εφαρμοστούν λόγω του μεγάλου εύρους template και plugin που διατίθενται.
- Τα συστήματα διαχείρισης περιεχομένου μειώνουν τον χρόνο που αφιερώνεται στον σχεδιασμό και την συγγραφή ενός μόνο website, δίνοντας στον προγραμματιστή περισσότερο χρόνο για να επικεντρωθεί σε πολλούς πελάτες ταυτόχρονα.

Συνοψίζοντας, είναι εμφανές ότι η απόφαση όσον αφορά τη χρήση ενός συστήματος διαχείρισης περιεχομένου εξαρτάται από τις ανάγκες και τις επιθυμίες του πελάτη για τον ιστότοπό του. Εάν ο πελάτης επιθυμεί να έχει τον έλεγχο της δημιουργίας περιεχομένου, θέλει να έχει τόσο δημόσια όσο και ιδιωτικά τμήματα στον ιστότοπό του, όπως για παράδειγμα login χρηστών και θέλει επίσης οι επισκέπτες να αλληλεπιδρούν με το περιεχόμενό τους, τότε το CMS είναι η καλύτερη επιλογή για τη φιλοξενία και την κατασκευή του ιστοτόπου.[20]

Κεφάλαιο 2: WordPress

2.1 Μια αναλυτική περιγραφή του WordPress

Το WordPress ξεκίνησε το 2003 ως ένα κομμάτι δωρεάν λογισμικού blogging που δημιουργήθηκε από τους Mike Little και Mike Mullenweg, οι οποίοι συνεχίζουν να τρέχουν το WordPress.org, την εταιρεία που κάνει το WordPress διαθέσιμο σε όποιον θέλει να δημιουργήσει έναν ιστότοπο ή ένα ιστολόγιο. Αναπτύσσοντας το WordPress και καθιστώντας το δωρεάν καθόλη τη διάρκεια της ύπαρξης σου, οι δημιουργοί του ήλπιζαν να «εκδημοκρατίσουν τη δημοσίευση» σχεδιάζοντας ένα πρόγραμμα δημιουργίας ιστότοπου που θα μπορούσε να επιτρέψει σε οποιονδήποτε να έχει φωνή και παρουσία στο διαδίκτυο.^[21]

Τα χαρακτηριστικά που έκαναν το WordPress τόσο ελκυστικό στους bloggers και σε άλλα είδη εκδοτών Διαδικτύου απήχθησαν επίσης σε ένα πολύ ευρύτερο κοινό, συμπεριλαμβανομένων ορισμένων από τις πιο εξέχουσες εταιρείες στις ΗΠΑ και σε όλο τον κόσμο. Τώρα, το WordPress είναι η πλατφόρμα επιλογής για μια μακρά λίστα γνωστών ονομάτων, συμπεριλαμβανομένων των Sony Music, Variety, Time, Inc. και της Disney Company, μαζί με εκατομμύρια μικρότερες επιχειρήσεις και προσωπικά ιστολόγια. Η πιο πρόσφατη έκδοση της πλατφόρμας έχει ληφθεί πάνω από 22 εκατομμύρια φορές μέχρι στιγμής και νέες εκδόσεις συνεχίζουν να αναπτύσσονται από τη μεγάλη κοινότητα χρηστών του WordPress.^[21]

Το WordPress είναι ένα ανοιχτού κώδικα, δωρεάν εργαλείο δημιουργίας ιστότοπου γραμμένο στη γλώσσα προγραμματισμού PHP. Αδειοδοτείται βάσει General Public License, η οποία επιτρέπει σε οποιονδήποτε όχι μόνο να χρησιμοποιεί το λογισμικό, αλλά και να το τροποποιεί ώστε να ταιριάζει με τις ατομικές ανάγκες και να μοιράζεται αυτές τις τροποποιήσεις με άλλους. Το λογισμικό «ανοιχτού κώδικα» είναι δημόσια διαθέσιμο και πάντα δωρεάν, έτσι ώστε το WordPress να μπορεί να ληφθεί ανά πάσα στιγμή ή να εγκατασταθεί ως μέρος κάποιου πακέτου web hosting.^[21]

Επειδή το WordPress προσκαλεί τροποποιήσεις και βελτιώσεις, έχει την υποστήριξη μιας μεγάλης και αυξανόμενης κοινότητας σχεδιαστών, προγραμματιστών και λάτρων του λογισμικού. Αυτά τα μέλη της κοινότητας του WordPress εργάζονται συνεχώς πάνω στον βασικό κώδικα του WordPress, καθώς και οργανώνουν εκδηλώσεις και «στρατόπεδα WordPress» για να βοηθήσουν τους ανθρώπους να μάθουν για το WordPress και να λύσουν προβλήματα με τη χρήση του. Οι χρήστες του WordPress όλων των επιπέδων εμπειρίας καλούνται να ενταχθούν στην κοινότητα του WordPress και να συνεισφέρουν με όποιον τρόπο μπορούν για την υποστήριξη άλλων χρηστών αλλά και για να διατηρούν το πρόγραμμα σταθερό και ενημερωμένο.^[21]

Το να ξεκινήσει κανείς με έναν ιστότοπο WordPress είναι ιδιαίτερα εύκολο. Αρκεί να κάνετε λήψη ενός αντιγράφου από το WordPress.org και να το εγκαταστήσετε σε μια πλατφόρμα φιλοξενίας ή να εγκαταστήσετε το WordPress με το πάτημα ενός κουμπιού καθώς η πλατφόρμα προσφέρεται από τους περισσότερους παρόχους φιλοξενίας ιστού. Ανεξάρτητα από το πώς αποκτάται ή εγκατασταθεί, το WordPress είναι εντελώς δωρεάν.^[21]

2.1.1 WordPress Themes

Οι χρήστες του WordPress μπορούν να εγκαταστήσουν και να κάνουν εναλλαγή μεταξύ πολλών διαφορετικών θεμάτων. Τα θέματα επιτρέπουν στους χρήστες να αλλάξουν την εμφάνιση και τη λειτουργικότητα ενός ιστότοπου WordPress χωρίς να αλλάξουν τον βασικό κώδικα ή το περιεχόμενο του ιστότοπου. Κάθε ιστότοπος WordPress απαιτεί τουλάχιστον ένα θέμα για να υπάρχει. Τα θέματα μπορούν να εγκατασταθούν απευθείας χρησιμοποιώντας το εργαλείο διαχείρισης "Εμφάνιση" του WordPress στον πίνακα εργαλείων ή οι φάκελοι θεμάτων μπορούν να αντιγραφούν απευθείας στον κατάλογο θεμάτων.[\[22\]](#) Τα θέματα του WordPress ταξινομούνται γενικά σε δύο κατηγορίες: δωρεάν και premium. Πολλά δωρεάν θέματα παρατίθενται στον κατάλογο θεμάτων του WordPress (γνωστό και ως αποθετήριο) και τα premium θέματα είναι διαθέσιμα για αγορά από αγορές και μεμονωμένους προγραμματιστές WordPress. Οι χρήστες του WordPress μπορούν επίσης να δημιουργήσουν και να αναπτύξουν τα δικά τους προσαρμοσμένα θέματα.[\[23\]](#)

2.1.2 WordPress Plugins

Η αρχιτεκτονική των plugins του WordPress επιτρέπει στους χρήστες να επεκτείνουν τις δυνατότητες και τη λειτουργικότητα ενός ιστότοπου ή ενός ιστολογίου. Από τον Δεκέμβριο του 2021, το WordPress.org έχει διαθέσιμες 59.756 προσθήκες,[\[24\]](#) καθεμία από τις οποίες προσφέρει προσαρμοσμένες λειτουργίες και δυνατότητες που επιτρέπουν στους χρήστες να προσαρμόσουν τους ιστότοπούς τους στις συγκεκριμένες ανάγκες τους. Ωστόσο, αυτό δεν περιλαμβάνει τα premium πρόσθετα που είναι διαθέσιμα (περίπου 1.500+), τα οποία ενδέχεται να μην αναφέρονται στο αποθετήριο WordPress.org. Αυτές οι προσαρμογές κυμαίνονται από τη βελτιστοποίηση μηχανών αναζήτησης (SEO), σε πύλες πελατών που χρησιμοποιούνται για την εμφάνιση προσωπικών πληροφοριών σε συνδεδεμένους χρήστες, σε συστήματα διαχείρισης περιεχομένου, έως λειτουργίες προβολής περιεχομένου, όπως η προσθήκη γραφικών στοιχείων και γραμμών πλοήγησης. Δεν είναι πάντα ενήμερες όλες οι διαθέσιμες προσθήκες με τις αναβαθμίσεις και ως εκ τούτου ενδέχεται να μην λειτουργούν σωστά ή να μην λειτουργούν καθόλου. Τα περισσότερα plugins είναι διαθέσιμα μέσω του ίδιου του WordPress, είτε μέσω λήψης τους και εγκατάστασης των αρχείων με μη αυτόματο τρόπο μέσω FTP είτε μέσω του dashboard του WordPress. Ωστόσο, πολλοί τρίτοι προσφέρουν plugins μέσω των δικών τους ιστοσελίδων, πολλά από τα οποία είναι πακέτα επί πληρωμή.[\[25\]](#)

Οι web developers που επιθυμούν να αναπτύξουν plugins πρέπει να μάθουν το σύστημα hook του WordPress το οποίο αποτελείται από περισσότερα από 2.000 hook (από την έκδοση 5.7 το 2021)[\[26\]](#) χωρισμένα σε δύο κατηγορίες: hook δράσης και hook φίλτρων.

Τα plugins αντιπροσωπεύουν επίσης μια στρατηγική ανάπτυξης που μπορεί να μετατρέψει το WordPress σε κάθε λογής σύστημα λογισμικού και εφαρμογή. Οι δυνατότητες του περιορίζονται μόνο από τη φαντασία και τη δημιουργικότητα των προγραμματιστών.

Ωστόσο, μην ξεχνάμε πως τα plugins θα μπορούσαν να χρησιμοποιηθούν από χάκερ που στοχεύουν έναν ιστότοπο που χρησιμοποιεί το WordPress, καθώς οι εισβολείς θα μπορούσαν να εκμεταλλευτούν τα σφάλματα στις προσθήκες του WordPress αντί να εκμεταλλευτούν τα σφάλματα στο ίδιο το WordPress.

2.1.3 Επιπλέον γνωρίσματα

Το WordPress διαθέτει επίσης ενσωματωμένη διαχείριση συνδέσμων, μια φιλική προς τις μηχανές αναζήτησης, καθαρή δομή μόνιμου συνδέσμου, τη δυνατότητα αντιστοίχισης πολλαπλών κατηγοριών σε αναρτήσεις καθώς και υποστήριξη για προσθήκη ετικετών σε αναρτήσεις. Περιλαμβάνονται επίσης αυτόματα φίλτρα, τα οποία παρέχουν τυποποιημένη μορφοποίηση και στυλ κειμένου σε αναρτήσεις (για παράδειγμα, μετατροπή κανονικών εισαγωγικών σε έξυπνα εισαγωγικά). Το WordPress υποστηρίζει επίσης τα πρότυπα Trackback και Pingback για την εμφάνιση συνδέσμων προς άλλους ιστότοπους που έχουν συνδεθεί με μια ανάρτηση ή ένα άρθρο. Οι αναρτήσεις του WordPress μπορούν να υποβληθούν σε επεξεργασία HTML, χρησιμοποιώντας το οπτικό πρόγραμμα επεξεργασίας ή χρησιμοποιώντας ένα από τα διάφορα πρόσθετα που επιτρέπουν μια ποικιλία προσαρμοσμένων λειτουργιών επεξεργασίας.[25]

2.2 Ασφάλεια στο WordPress

Πολλά ζητήματα ασφαλείας[27] έχουν αποκαλυφθεί στο λογισμικό, ιδιαίτερα το 2007, το 2008 και το 2015. Σύμφωνα με τη Secunia, το WordPress τον Απρίλιο του 2009 είχε επτά μη επιδιορθωμένες συμβουλές ασφαλείας (από 32 συνολικά), με μέγιστη βαθμολογία "Less Critical". Η Secunia διατηρεί μια ενημερωμένη λίστα ευπαθειών του WordPress.[28]

Τον Ιανουάριο του 2007, πολλά ιστολόγια βελτιστοποίησης μηχανών αναζήτησης (SEO) υψηλού προφίλ, καθώς και πολλά εμπορικά ιστολόγια χαμηλού προφίλ που διέθεταν το AdSense, στοχοποιήθηκαν και έπεσαν θύματα επιθέσεων λόγω της εκμετάλλευσης των ευπαθειών του WordPress.[29] Μια ξεχωριστή ευπάθεια σε έναν από τους server του project site επέτρεψε σε έναν εισβολέα να εισάγει εκμεταλλεύσιμο κώδικα με τη μορφή πίσω πόρτας σε ορισμένες λήψεις του WordPress 2.1.1. Η έκδοση 2.1.2 ήρθε για να αντιμετωπίσει αυτό το ζήτημα, και η συμβουλευτική που κυκλοφόρησε εκείνη την εποχή προέτρεψε όλους τους χρήστες να αναβαθμίσουν αμέσως.[30]

Τον Μάιο του 2007, μια μελέτη αποκάλυψε ότι το 98% των ιστολογίων WordPress που εκτελούνταν ήταν εκμεταλλεύσιμα επειδή εκτελούσαν παλιές και μη υποστηριζόμενες εκδόσεις του λογισμικού.[31] Εν μέρει για να μετριάσει αυτό το πρόβλημα, το WordPress έκανε την ενημέρωση του λογισμικού μια πολύ πιο εύκολη, αυτοματοποιημένη διαδικασία με "ένα κλικ" στην έκδοση 2.7 (κυκλοφόρησε τον Δεκέμβριο του 2008).[32] Ωστόσο, οι ρυθμίσεις ασφαλείας του συστήματος αρχείων που απαιτούνταν για την ενεργοποίηση της διαδικασίας ενημέρωσης μπορούσαν να αποτελέσουν πρόσθετο κίνδυνο.[33]

Σε μια συνέντευξη που πραγματοποιήθηκε τον Ιούνιο του 2007, ο Stefan Esser, ο ιδρυτής της ομάδας PHP Security Response, μίλησε επικριτικά για το ιστορικό ασφάλειας του WordPress, αναφέροντας προβλήματα με την αρχιτεκτονική της εφαρμογής που καθιστούσαν αδικαιολόγητα δύσκολη τη σύνταξη κώδικα που είναι ασφαλής από ευπάθειες SQL injection, καθώς και κάποια άλλα προβλήματα.[34]

Τον Ιούνιο του 2013, διαπιστώθηκε ότι μερικά από τα 50 plugin του WordPress με τις περισσότερες λήψεις ήταν ευάλωτα σε κοινές επιθέσεις ιστού, όπως η SQL injection και η

XSS. Μια ξεχωριστή επιθεώρηση των 10 κορυφαίων plugins που χρησιμοποιούνταν από ιστοσελίδες ηλεκτρονικού εμπορίου έδειξε ότι επτά από αυτά ήταν ευάλωτα.[35]

Σε μια προσπάθεια να προωθηθεί καλύτερη ασφάλεια και να εξορθολογιστεί η εμπειρία ενημέρωσης συνολικά, εισήχθησαν αυτόματες ενημερώσεις παρασκηνίου στο WordPress 3.7.[36]

Οι μεμονωμένες εγκαταστάσεις του WordPress μπορούν να προστατεύονται με plugin ασφαλείας που εμποδίζουν την απαρίθμηση των χρηστών, την απόκρυψη πόρων και την αποτροπή διερεύνησης. Οι χρήστες μπορούν επίσης να προστατεύσουν τη δική τους εγκατάσταση του WordPress κάνοντας βήματα όπως η ενημέρωση όλων των εγκαταστάσεων, των θεμάτων και των plugin του WordPress, χρησιμοποιώντας μόνο αξιόπιστα θέματα και προσθήκες,[37] και επεξεργάζοντας το αρχείο διαμόρφωσης .htaccess του ιστότοπου, εάν αυτό υποστηρίζεται από τον διακομιστή ιστού, για να αποτρέψουν πολλούς τύπους επιθέσεων SQL injection και να αποκλείσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα αρχεία. Το να διατηρούνται ενημερωμένα τα plugin είναι ιδιαίτερα σημαντικό καθώς οι επίδοξοι χάκερ μπορούν εύκολα να απαριθμήσουν όλα τα πρόσθετα που χρησιμοποιεί ένας ιστότοπος και στη συνέχεια να εκτελέσουν σαρώσεις αναζητώντας τυχόν ευπάθειες σε αυτά τα πρόσθετα. Εάν εντοπιστούν ευπάθειες, ενδέχεται να χρησιμοποιηθούν για να επιτραπεί στους χάκερ να ανεβάσουν, για παράδειγμα, τα δικά τους αρχεία (όπως ένα web shell) που συλλέγουν ευαίσθητες πληροφορίες.

Οι προγραμματιστές μπορούν επίσης να χρησιμοποιήσουν εργαλεία για την ανάλυση πιθανών τρωτών σημείων, συμπεριλαμβανομένων των WPScan, WordPress Auditor και WordPress Sploit Framework που αναπτύχθηκαν από την 0p0deFR. Αυτοί οι τύποι εργαλείων ερευνούν για γνωστές ευπάθειες, όπως CSRF, LFI, RFI, XSS, SQL injection και user enumeration. Ωστόσο, δεν είναι δυνατόν να εντοπίσουμε όλα τα τρωτά σημεία με τη χρήση εργαλείων, επομένως συνιστάται ο έλεγχος του κώδικα των plugin, των θεμάτων και άλλων πρόσθετων από άλλους προγραμματιστές.

Τον Μάρτιο του 2015, αναφέρθηκε ότι το πρόσθετο Yoast SEO ήταν ευάλωτο στην SQL injection, επιτρέποντας στους εισβολείς να εκτελούν δυνητικά αυθαίρετες εντολές SQL.[38][39] Το πρόβλημα επιδιορθώθηκε στην έκδοση 1.7.4 της προσθήκης.[40]

Τον Ιανουάριο του 2017, οι ελεγκτές ασφαλείας στο Sucuri εντόπισαν μια ευπάθεια στο WordPress REST API που θα επέτρεπε σε οποιονδήποτε μη πιστοποιημένο χρήστη να τροποποιήσει οποιαδήποτε ανάρτηση ή σελίδα σε έναν ιστότοπο που εκτελεί WordPress 4.7 ή νεότερη έκδοση. Οι ελεγκτές ειδοποίησαν αθόρυβα τους προγραμματιστές του WordPress και μέσα σε έξι ημέρες το WordPress κυκλοφόρησε μια ενημέρωση κώδικα υψηλής προτεραιότητας στην έκδοση 4.7.2, η οποία αντιμετώπισε το πρόβλημα.[41][42]

Το WordPress 5.2, έχει ως ελάχιστη απαίτηση έκδοσης PHP την PHP 5.6,[43] η οποία κυκλοφόρησε στις 28 Αυγούστου 2014[44] και η οποία δεν υποστηρίζεται από την ομάδα PHP και δεν έχει λάβει ενημερώσεις κώδικα ασφαλείας από τις 31 Δεκεμβρίου 2018. [44] Επομένως, το WordPress συνιστά τη χρήση PHP έκδοσης 7.3 ή νεότερης.[43]

Ελλείψει συγκεκριμένων αλλαγών στον προεπιλεγμένο κώδικα μορφοποίησής τους, οι ιστότοποι που βασίζονται στο WordPress χρησιμοποιούν το canvas element για να εντοπίσουν εάν το πρόγραμμα περιήγησης μπορεί να αποδώσει σωστά τα emoji. Επειδή το Tor Browser προς το παρόν δεν κάνει διακρίσεις μεταξύ αυτής της νόμιμης χρήσης του

Canvas API και μιας προσπάθειας για την εκτέλεση δακτυλικών αποτυπωμάτων σε canvas, προειδοποιεί ότι ο ιστότοπος επιχειρεί «εξαγωγή δεδομένων εικόνας canvas HTML5».[45]

2.2.1 Θέματα ασφαλείας και ευπάθειες

Όπως αναφέρθηκε παραπάνω, το WordPress είναι το πιο δημοφιλές CMS στο Διαδίκτυο, επομένως και το πιο χακαρισμένο. Το 2020, το Wordfence ανέφερε περισσότερες από 2.800 επιθέσεις ανά δευτερόλεπτο με στόχο το WordPress.

Οι κυβερνοεπιθέσεις σπαταλούν χρόνο, ενέργεια και χρήματα και μπορούν να απειλήσουν την εξουσία και τη φήμη μιας επιχείρησης, ειδικά εάν οι επισκέπτες του ιστότοπού-θύματος επηρεάζονται από τις επιθέσεις. Αν και είναι αδύνατο να ποσοτικοποιηθεί ο αριθμός των καθημερινών απειλών που μπορεί να αντιμετωπίζει ένας ιστότοπος, είναι σημαντικό οι χρήστες να αναγνωρίζουν και να κατανοούν συγκεκριμένα ζητήματα του WordPress που μπορούν να οδηγήσουν τις ιστοσελίδες τους σε ευκολότερες παραβιάσεις από εισβολείς.

Τα σημαντικότερα θέματα ασφαλείας που εμφανίζει η πλατφόρμα WordPress αναφέρονται παρακάτω.

2.2.1.1 Outdated Core Software

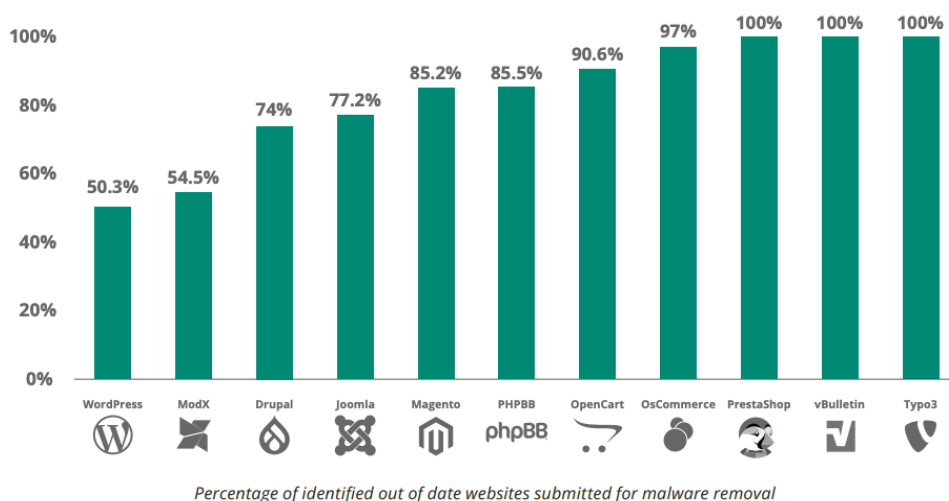
Ένα πλεονέκτημα που προκύπτει από τη χρήση μιας πλατφόρμας δημιουργίας ιστότοπου αντί της δημιουργίας ενός ιστότοπου από την αρχή είναι ότι οι προγραμματιστές της πλατφόρμας βελτιώνουν συνεχώς τη λειτουργικότητα και την ασφάλεια της για να παρέχουν μια απρόσκοπτη εμπειρία χρήστη.

Οι προγραμματιστές του WordPress κυκλοφορούν ενημερώσεις κάθε τρεις μήνες περίπου. Συνιστάται ανεπιφύλακτα σε όλους τους χρήστες του WordPress να κάνουν λήψη αυτών των ενημερώσεων όταν γίνουν διαθέσιμες είτε με μη αυτόματο τρόπο είτε ενεργοποιώντας τις αυτόματες ενημερώσεις. Κάθε μία από αυτές τις εκδόσεις περιλαμβάνει συνήθως βελτιώσεις, διορθώσεις σφαλμάτων και διορθώσεις στα πιο κρίσιμα τρωτά σημεία ασφαλείας. Έτσι, με την ενημέρωση των βασικών αρχείων τους οι χρήστες μπορούν να συμβάλλουν και στη βελτίωση της λειτουργικότητας, της απόδοσης και της συμβατότητας του ιστότοπού τους εκτός από την ασφάλεια.

Παρά τη δυνατότητα αυτόματης ενημέρωσης, σύμφωνα με τη βάση δεδομένων της Sucuri, «το 50,3% των μολυσμένων ιστοσελίδων WordPress ήταν outdated».

Αυτό το ποσοστό φαίνεται καλύτερο από τα άλλα CMS, όπως το PrestaShop, το vBulletin και το TYPO3, όπου το 100% των μολυσμένων ιστότοπων εκτελούνταν σε απαρχαιωμένο λογισμικό. Ωστόσο, είναι σημαντικό να σημειωθεί ότι το 50% του WordPress είναι περισσότεροι ιστότοποι από το 100% του TYPO3 και άλλων πλατφορμών. Επομένως, εξακολουθεί να υπάρχει σημαντικό μέρος των ιστότοπων WordPress που εκτελούνται με απαρχαιωμένο λογισμικό.[46]

Out-of-date CMS Distribution - 2021



Εικόνα 1

2.2.1.2 Outdated Θέματα και Plugins

Ένα από τα σημαντικότερα πλεονεκτήματα του WordPress είναι η προσαρμοστικότητα του. Οι προγραμματιστές δημιουργούν εκατοντάδες μοναδικά θέματα και προσθήκες που μπορούν να χρησιμοποιήσουν οι ιδιοκτήτες ιστότοπων WordPress για να προσαρμόσουν τους ιστότοπούς τους.

Αυτές οι επεκτάσεις απαιτούν από τους κατόχους ιστοτόπων να λαμβάνουν τις κατάλληλες προφυλάξεις ασφαλείας. Όπως αναφέρθηκε παραπάνω, το μη ενημερωμένο βασικό λογισμικό μπορεί να εκθέσει τον ιστότοπό σας σε κινδύνους για την ασφάλεια. Το ίδιο ακριβώς συμβαίνει και με τη χρήση παλιών θεμάτων και plugin.

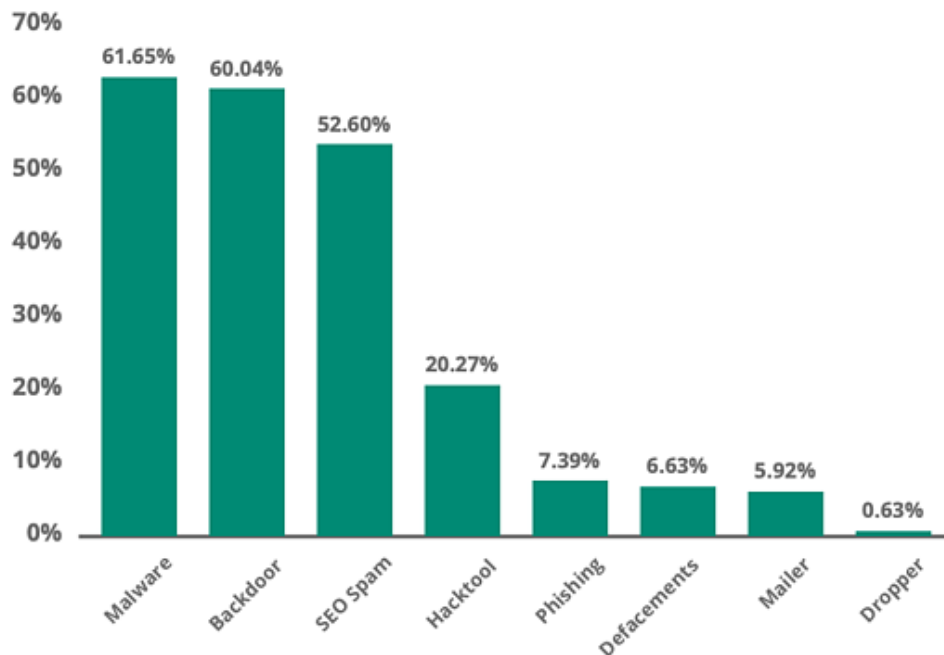
Στην πραγματικότητα, σύμφωνα με δεδομένα από το WPScan, περίπου το 97% των τρωτών σημείων στη βάση δεδομένων τους είναι plugins και θέματα και μόνο το 4% είναι βασικό λογισμικό.[\[46\]](#)

2.2.1.3 Malware

Το malware είναι ένας ευρύς όρος που περιλαμβάνει οποιοδήποτε κακόβουλο λογισμικό (επομένως, "mal-ware"). Οι χάκερ μπορούν να τοποθετήσουν αρχεία κακόβουλου λογισμικού σε νόμιμα αρχεία ιστότοπου ή να εγκαθιστούν κώδικα σε υπάρχοντα αρχεία για να κλέψουν από ιστότοπους και τους επισκέπτες τους. Το κακόβουλο λογισμικό θα μπορούσε επίσης να επιχειρήσει μια μη εξουσιοδοτημένη σύνδεση μέσω αρχείων "backdoor" ή να προκαλέσει γενικό όλεθρο.

Το 2021, το 61,65% των διορθωμένων ιστότοπων στη βάση δεδομένων Sucuri είχαν μολυνθεί από κακόβουλο λογισμικό.

Malware Family Distribution - 2021



ε

Εικόνα 2

Τα κακόβουλα λογισμικά εισέρχονται συνήθως σε ιστότοπους WordPress μέσω μη εξουσιοδοτημένων και ξεπερασμένων θεμάτων και προσθηκών. Οι χάκερ εκμεταλλεύονται προβλήματα ασφάλειας σε plugins και θέματα, μιμούνται τα υπάρχοντα ή ακόμη και δημιουργούν εντελώς νέα plugins με μοναδικό σκοπό την τοποθέτηση επιβλαβούς κώδικα στον ιστότοπό σας. [\[46\]](#)

2.2.1.4 Μη Εξουσιοδοτημένα Logins

Οι μη εξουσιοδοτημένες συνδέσεις εκτελούνται συνήθως με "brute-force". Σε ένα brute-force login, ο εισβολέας χρησιμοποιεί ένα bot για να εκτελέσει γρήγορα δισεκατομμύρια πιθανούς συνδυασμούς ονόματος χρήστη-κωδικού πρόσβασης. Εάν είναι τυχερός, θα μαντέψει τελικά τα σωστά διαπιστευτήρια και θα αποκτήσει πρόσβαση στις προστατευμένες πληροφορίες.

Υπάρχουν δύο βασικοί λόγοι για τους οποίους αυτές οι επιθέσεις συμβαίνουν με επιτυχία σε ιστότοπους WordPress. Πρώτον, η default backend σελίδα σύνδεσης για κάθε δεδομένο ιστότοπο WordPress είναι σχετικά εύκολο να βρεθεί. Οποιοσδήποτε μπορεί απλώς να πάρει την κύρια διεύθυνση URL του ιστότοπου, να προσθέσει /wp-admin ή /wp-login.php στο τέλος και θα αποκτήσει πρόσβαση στη σελίδα σύνδεσης. Εάν δεν εξατομικεύσετε την προεπιλεγμένη σελίδα σύνδεσης, οι εισβολείς μπορούν εύκολα να αποκτήσουν πρόσβαση και να επιχειρήσουν μια brute force entry. [\[46\]](#)

2.2.1.5 Μη Καθορισμένοι Ρόλοι Χρήστη

Όταν δημιουργείται ένας ιστότοπο WordPress, υπάρχουν έξι διαφορετικοί ρόλοι χρήστη για να διαλέξετε, όπως για παράδειγμα Συνδρομητής ή Διαχειριστής. Κάθε ρόλος συνοδεύεται από εγγενή δικαιώματα που επιτρέπουν ή περιορίζουν τους χρήστες από το να προβούν σε συγκεκριμένες ενέργειες στον ιστότοπό, όπως η τροποποίηση προσθηκών και η δημοσίευση περιεχομένου. Ο προεπιλεγμένος ρόλος χρήστη είναι “Διαχειριστής” και αυτός ο ρόλος έχει τον μεγαλύτερο έλεγχο σε οποιονδήποτε δεδομένο ιστότοπο WordPress.

Εάν μια ιστοσελίδα έχει πολλούς χρήστες και δεν τροποποιηθούν οι προεπιλεγμένες ρυθμίσεις, όλοι είναι διαχειριστές, κάτι που θα μπορούσε να αποτελέσει πρόβλημα. Αυτό δεν σημαίνει απαραίτητα ότι τα άτομα με τα οποία δημιουργείτε έναν ιστότοπο θα σας βλάψουν, αλλά σημαίνει ότι ένας χάκερ που αποκτά πρόσβαση στον ιστότοπό σας θα μπορεί να κάνει αλλαγές ως διαχειριστής.

Οι κακώς καθορισμένοι ρόλοι διαχειριστή εκθέτουν τον ιστότοπό σας σε αυξημένο κίνδυνο εάν οι επιθέσεις brute force είναι επιτυχείς, καθώς ο ρόλος διαχειριστή μπορεί να δώσει στον χάκερ τον πλήρη έλεγχο του ιστότοπού σας. Επιπλέον, το cross-site scripting παρέχει στους χάκερ πρόσβαση σε δυνατότητες front-end με αποτέλεσμα να μπορούν να λάβουν πρόσθετες πληροφορίες από τους επισκέπτες του ιστότοπού σας. [46]

2.2.2 Κυριότερες επιθέσεις στην πλατφόρμα

2.2.2.1 Structured Query Language (SQL) Injections

Η SQL είναι μια γλώσσα προγραμματισμού που χρησιμοποιείται για γρήγορη πρόσβαση σε αποθηκευμένα δεδομένα σε μια συγκεκριμένη ιστοσελίδα. Είναι η προτιμώμενη γλώσσα στο WordPress για τη διαχείριση της βάσης δεδομένων και, ενώ είναι κάπως ασφαλής, τα κακόβουλα μέρη μπορούν να τη χρησιμοποιήσουν για να επωφεληθούν από τον ιστότοπό σας.[9][46]

Κατά τη διάρκεια μιας SQL injection, ένας χάκερ αποκτά τη δυνατότητα να προβάλλει και να τροποποιεί απευθείας τη βάση δεδομένων του ιστότοπού σας. Οι εισβολείς μπορούν να χρησιμοποιήσουν την SQL για να δημιουργήσουν νέους λογαριασμούς στον ιστότοπό σας, να προσθέσουν μη εξουσιοδοτημένους συνδέσμους και περιεχόμενο και να διαρρεύσουν, να επεξεργαστούν και να διαγράψουν δεδομένα.[46]

Οι ιστότοποι WordPress είναι ευάλωτοι σε αυτού του είδους τις επιθέσεις, επειδή οι περισσότεροι έχουν σχεδιαστεί για να καλλιεργούν την αίσθηση της κοινότητας. Οι εισβολείς χρησιμοποιούν συνήθως ενέσεις SQL μέσω φορμών υποβολής που αναφέρονται σε επισκέπτες, όπως φόρμες επικοινωνίας, πεδία πληροφοριών πληρωμής και φόρμες δυνητικού πελάτη. Όταν οι χάκερ εισάγουν πληροφορίες σε αυτές τις φόρμες, δεν ελπίζουν να χρησιμοποιήσουν το περιεχόμενο που προσφέρεται στην ιστοσελίδα — υποβάλλουν κώδικα που θα εκτελείται και θα κάνει αλλαγές από μέσα.[46]

Ο καλύτερος τρόπος άμυνας απέναντι σε αυτή την επίθεση είναι να είμαστε σκεπτικοί ως προς τη συμβολή των χρηστών. Οποιαδήποτε υποβολή φόρμας στον ιστότοπό μας είναι μια ευκαιρία για επισκέπτες με κακόβουλη πρόθεση να υποβάλουν πληροφορίες απευθείας στη βάση δεδομένων SQL.[9][46]

Ο περιορισμός της υποβολής ειδικών χαρακτήρων στις υποβολές επισκεπτών είναι ένα επιπλέον μέτρο που προτείνεται. Χωρίς σύμβολα, μια σειρά κακόβουλου κώδικα μειώνεται σε αβλαβή ασυναρτησία. Μπορεί επίσης να χρησιμοποιηθεί ένα plugin φόρμας WordPress ή/και ένα plugin ασφαλείας WordPress προκειμένου να γίνει αυτόματα η διαδικασία. Ως επιπλέον μέτρο άμυνας, μπορεί να γίνει χρήση ενός captcha στο τελευταίο βήμα της διαδικασίας υποβολής προκειμένου να αποτραπούν τα bots από το να κάνουν προσπάθειες ένεσης.^[46]

2.2.2.2 Search Engine Optimization (SEO) Spam

Αυτά τα spammy hacks είναι παρόμοια με την SQL injection, αλλά στοχεύουν αυτό που εκτιμά περισσότερο ο κάθε ιδιοκτήτης ιστότοπου: SEO. Αυτά τα hacks εκμεταλλεύονται τις σελίδες με την κορυφαία κατάταξη, τις γεμίζουν με ανεπιθύμητες λέξεις-κλειδιά και αναδυόμενες διαφημίσεις και πωλούν αντικείμενα ή πλαστά εμπορεύματα.

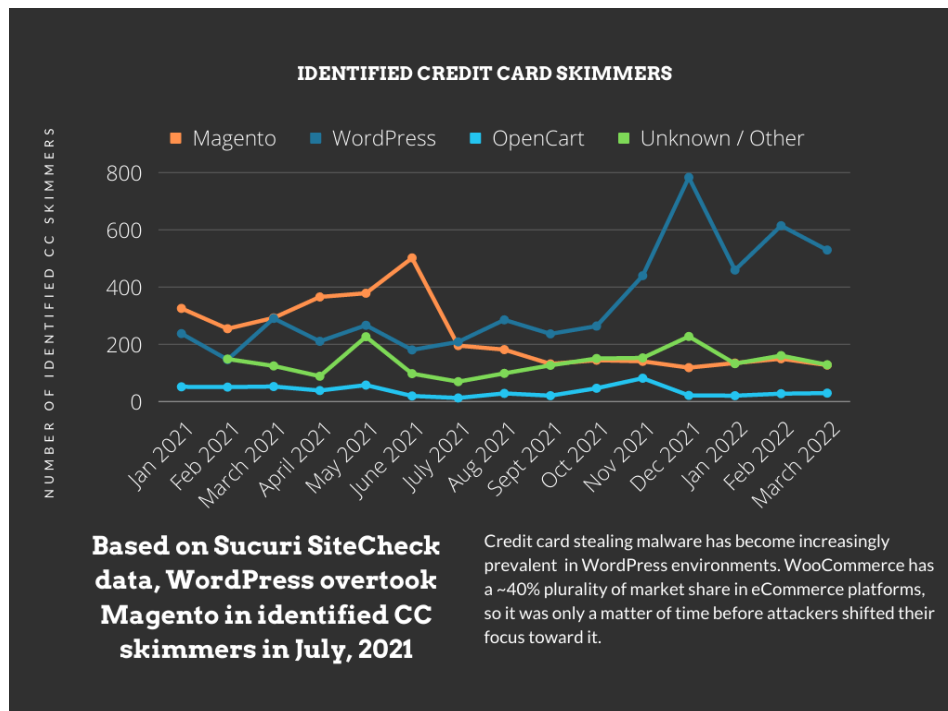
Οι ιστότοποι WordPress είναι ευάλωτοι σε αυτές τις επιθέσεις με τον ίδιο τρόπο που είναι και τα υπόλοιπα ζητήματα ασφαλείας σε αυτήν τη λίστα: ξεπερασμένα plugins, θέματα και βασικό λογισμικό. Οι επιτυχείς brute επιθέσεις και οι απροσδιόριστοι ρόλοι χρηστών μπορούν επίσης να κάνουν τον ιστότοπό σας ευάλωτο. Αυτές οι επιθέσεις είναι επίσης πιο δύσκολο να εντοπιστούν, γεγονός που τις καθιστά ακόμη πιο επικίνδυνες. Οι χάκερ αποκτούν συχνά πρόσβαση στην ιστοσελίδα, αλλά περιμένουν πριν κάνουν οποιοσδήποτε αλλαγές για να μην εγείρουν άμεση υποψία. Αυτό σημαίνει ότι η SEO spam είναι πιο αισθητή στους SEO crawlers, καθώς θα ευρετηριάσουν τον ιστότοπό σας για τις λέξεις-κλειδιά ανεπιθύμητης αλληλογραφίας.^[46]

Το πρώτο πράγμα που πρέπει κάποιος να κάνει για να αμυνθεί είναι να ακολουθήσει τα προαναφερθέντα μέτρα ασφαλείας, όπως η έγκαιρη ενημέρωση και ο καθορισμός ρόλων χρηστών. Μπορεί επίσης να χρησιμοποιήσει μια προσθήκη ασφαλείας WordPress που μπορεί να εκτελέσει σαρώσεις κακόβουλου λογισμικού.

2.2.2.3 Skimming Πιστωτικών Καρτών

Το skimming πιστωτικών καρτών είναι ένας τύπος κακόβουλου λογισμικού που έχει σχεδιαστεί για να κλέβει τα στοιχεία της πιστωτικής κάρτας των πελατών μιας ιστοσελίδας. Οι περισσότεροι skimmers πιστωτικών καρτών εισάγουν JavaScript για να κλέψουν τα στοιχεία πληρωμής που έχουν καταχωρηθεί στις φόρμες πληρωμής των σελίδων ολοκλήρωσης αγοράς και είναι καλά κρυμμένα για να αποφευχθεί ο εντοπισμός τους.

Σύμφωνα με το CMS, το WordPress καταλαμβάνει το μεγαλύτερο μέρος των μολύνσεων skimmer, με 34,5% το 2021. ^[46]



Εικόνα 3

Η λύση απέναντι σε αυτές τις επιθέσεις είναι ένα εργαλείο παρακολούθησης όπως το Sucuri SiteCheck, το οποίο σαρώνει τον ιστότοπό σας για γνωστό κακόβουλο περιεχόμενο και ενέσεις κακόβουλου λογισμικού και μας επιτρέπει να δούμε για ποιο σκοπό θέλουν οι εισβολείς τις πληροφορίες.

2.2.2.4 Brute Force Attack

Η Brute Force Attack περιλαμβάνει μια προσέγγιση πολλαπλών δοκιμών και σφαλμάτων που χρησιμοποιεί εκατοντάδες συνδυασμούς για να μαντέψει το σωστό όνομα χρήστη ή κωδικό πρόσβασης. Αυτό γίνεται χρησιμοποιώντας ισχυρούς αλγόριθμους και dictionaries που μαντεύουν τον κωδικό πρόσβασης χρησιμοποιώντας κάποιου είδους συμφραζόμενα.^[47]

Αυτό το είδος επίθεσης είναι δύσκολο να εκτελεστεί, αλλά εξακολουθεί να είναι μια από τις δημοφιλείς επιθέσεις που εκτελούνται σε ιστότοπους WordPress. Από προεπιλογή, το WordPress δεν εμποδίζει έναν χρήστη να δοκιμάσει πολλαπλές προσπάθειες αποτυχίας που επιτρέπουν σε έναν άνθρωπο ή ένα bot να δοκιμάσει χιλιάδες συνδυασμούς ανά δευτερόλεπτο.^[47] Ένα κοινό σημείο επίθεσης στο WordPress είναι το αρχείο wp-login.php στο οποίο ο επιτιθέμενος χτυπά ξανά και ξανά μέχρι να εισχωρήσει ή να πέσει ο server.^[48]

Η αποφυγή της συγκεκριμένης επίθεσης είναι αρκετά απλή. Το μόνο που έχει να κάνει ο χρήστης είναι να δημιουργήσει έναν ισχυρό κωδικό πρόσβασης που περιλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες. Κάθε χαρακτήρας έχει διαφορετικές τιμές ASCII οπότε είναι δύσκολο για κάποιον να μαντέψει έναν μακρύ και πολύπλοκο κωδικό πρόσβασης.^[47]

2.2.2.5 Cross-Site Scripting

Το Cross-Site Scripting (XSS) συμβαίνει όταν ένας εισβολέας τοποθετεί κακόβουλο κώδικα στον κώδικα παρασκηνίου του επιλεγμένου ιστότοπου. Οι επιθέσεις XSS είναι παρόμοιες με τις database injections, καθώς οι εισβολείς προσπαθούν να εγκαταστήσουν κώδικα που εκτελείται μέσα στα αρχεία σας, ωστόσο το XSS στοχεύει κυρίως στη λειτουργικότητα της ιστοσελίδας. Μόλις αποκτηθεί πρόσβαση στην οθόνη διεπαφής, οι χάκερ μπορεί να προσπαθήσουν να βλάψουν τους επισκέπτες, για παράδειγμα, δημοσιεύοντας έναν συγκαλυμμένο σύνδεσμο σε έναν ελαττωματικό ιστότοπο ή εμφανίζοντας μια ψεύτικη φόρμα επικοινωνίας για να κλέψουν πληροφορίες χρήστη.[47]

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.[49]

Για άλλη μια φορά τα plugins και τα θέματα του WordPress είναι οι ένοχοι. Εάν ένας εισβολέας βρει ένα outdated ή κακοσυντηρημένο plugin στην ιστοσελίδα σας, μπορεί να το εκμεταλλευτεί για πρόσβαση σε αρχεία που υπαγορεύουν τη διεπαφή του ιστότοπού σας. Το ίδιο ισχύει και με outdated θέματα της πλατφόρμας.[47]

Όπως καταλαβαίνουμε, ο πιο αποτελεσματικός τρόπος άμυνας είναι η συνεχής και στην ώρα της ενημέρωση του πυρήνα του WordPress, των θεμάτων και των plugin του.[47]

2.2.2.6 Denial of Service Attack (DoS)

Μια επίθεση Denial-of-Service (DoS) στοχεύει να εμποδίσει τους διαχειριστές και τους επισκέπτες του ιστότοπου να έχουν πρόσβαση σε έναν ιστότοπο. Αυτό γίνεται στέλνοντας τόση πολλή κίνηση σε έναν στοχευμένο διακομιστή που κρασάρει, κατεβάζοντας όλους τους ιστότοπους που φιλοξενούνται σε αυτόν. Τελικά, ο διακομιστής και οι ιστοσελίδες που

φιλοξενούνται αποκαθίστανται, αλλά η φήμη των ιστοτόπων που έχουν προσβληθεί ενδέχεται να είναι δύσκολο να επανέλθει.[47]

Αυτές οι επιθέσεις πραγματοποιούνται συχνά από πολλαπλούς μηχανισμούς ταυτόχρονα (δημιουργώντας ένα botnet), το οποίο κρύβει την αρχική πηγή της επισκεψιμότητας και συνδυάζει τον όγκο των spam. Η συγκεκριμένη μορφή της επίθεσης είναι γνωστή ως καταναμημένη επίθεση άρνησης υπηρεσίας (DDoS) και είναι πολύ πιο επικίνδυνη.

Το WordPress είναι ευάλωτο σε αυτού του τύπου της επιθέσεις εξαιτίας των διακομιστών φιλοξενίας με περιορισμένη ασφάλεια. Μην βασίζεστε μόνο σε προσθήκες για την άμυνα ενάντια σε αυτήν την επίθεση. Ο καλύτερος τρόπος προστασίας ενάντια στις επιθέσεις DoS/DDoS είναι το ασφαλές hosting των σελίδων WordPress. Οι χρήστες θα χρειαστεί να στραφούν σε έναν αξιόπιστο πάροχο φιλοξενίας που να ταιριάζει στις ανάγκες της επιχείρησής τους και να διατηρεί τη φήμη ότι λαμβάνει σοβαρά υπόψη την ασφάλεια των ιστοσελίδων που φιλοξενεί.[47]

2.2.2.7 Phishing

Το phishing πήρε το όνομά του από το πραγματικό ψάρεμα (fishing), όπου οι άνθρωποι πετούν δολώματα το ένα μετά το άλλο ελπίζοντας ότι κάτι θα τσιμπήσει. Κατά το ηλεκτρονικό ψάρεμα, οι χάκερ στέλνουν τεράστιες ποσότητες συνδέσμων ανεπιθύμητης αλληλογραφίας ελπίζοντας ότι τουλάχιστον ένα άτομο θα κάνει κλικ σε έναν από αυτούς με αποτέλεσμα να παραβιαστούν οι πληροφορίες του. [47]

Όπως και άλλα ζητήματα ασφαλείας σε αυτήν τη λίστα, οι ιστότοποι του WordPress γίνονται ευάλωτοι σε απόπειρες ηλεκτρονικού ψαρέματος μέσω απαρχαιωμένων προσθηκών, θεμάτων, λογισμικού ή έλλειψης ελέγχων ασφαλείας για φόρμες υποβολής και σχολίων.

Η προστασία από το ηλεκτρονικό ψάρεμα περιλαμβάνει τα συνήθη βήματα: να πραγματοποιείτε τακτικές ενημερώσεις, να παρακολουθείτε τη δραστηριότητα του ιστότοπου και να χρησιμοποιείτε ασφαλείς κωδικούς πρόσβασης. Θα πρέπει επίσης να κατεβάσετε πρόσθετα μέτρα ασφαλείας για τον ιστότοπό σας, όπως το ReCAPTCHA, για προστασία από spammy bots phishing. Το ReCAPTCHA χρησιμοποιεί μηχανική εκμάθηση για την κατανόηση των μοτίβων περιήγησης για τη διάκριση μεταξύ ανθρώπων και ρομπότ.[47]

2.2.3 Τρόποι Ενίσχυσης Ασφάλειας

Η ασφάλεια των ιστοτόπων, και κατ' επέκταση η ασφάλεια του ιστότοπου WordPress, καταλήγει στην τήρηση ενός συνόλου βέλτιστων πρακτικών. Ορισμένες από αυτές ισχύουν γενικότερα για όλους τους ιστότοπους (π.χ. χρήση ισχυρών κωδικών πρόσβασης και έλεγχος ταυτότητας δύο παραγόντων, SSL και τείχη προστασίας), ενώ άλλες ισχύουν ειδικά για ιστότοπους WordPress (π.χ. χρήση ασφαλών προσθηκών και θεμάτων WordPress).

Για να διατηρήσει ένας χρήστης τον ιστότοπο του ασφαλή, συνιστάται να τηρηθούν όσο το δυνατόν περισσότερες από τις βέλτιστες πρακτικές. Παρακάτω θα αναφερθούν οι κυριότεροι τρόποι εξασφάλισης της ασφάλειας, καθώς και κάποιες επιπρόσθετες ενέργειες που μπορεί να ακολουθήσει κάποιος εάν ο ιστότοπος του κινδυνεύει ιδιαίτερα ή εάν θέλει να εξασφαλίσει τη μέγιστη προστασία του.

2.2.3.1 Χρήση ασφαλούς παρόχου φιλοξενίας (Web Hosting)

Ένα πρώτο μέρος της ασφάλειας του ιστότοπου, 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.[49]

Το πού και το πώς θα επιλέξετε να φιλοξενήσετε τον ιστότοπό σας στο WordPress θα εξαρτηθεί σε μεγάλο βαθμό από τις απαιτήσεις σας. Παρόλο που οι χρήστες μπορούν να φιλοξενούν ή να διαχειρίζονται την ιστοσελίδα τους χωρίς κάποια βοήθεια, εάν κάποιος δε διαθέτει τις τεχνικές γνώσεις ή θέλει να βεβαιωθεί ότι πληροί τις περισσότερες προϋποθέσεις των βασικών αρχών ασφαλείας του WordPress χωρίς να κάνει πολλές ενέργειες χειροκίνητα, μπορεί να επιλέξει ένα διαχειριζόμενο πάροχο φιλοξενίας του WordPress, όπως το Kinsta ή το WP Engine.[50]

2.2.3.2 Συνεχής ενημέρωση της πλατφόρμας WordPress

Ακριβώς όπως πρέπει να διατηρούνται ενημερωμένα τα πρόσθετα και τα θέματά, θα πρέπει επίσης να διατηρείτε ενημερωμένη η έκδοση του WordPress που χρησιμοποιείται. Ευτυχώς, αυτό είναι πλέον πολύ πιο εύκολο από ό,τι στο παρελθόν, με τις κρίσιμες ενημερώσεις ασφαλείας να πραγματοποιούνται αυτόματα. Αυτό, εκτός και αν απενεργοποιήσετε ρητά αυτή τη λειτουργία.

Εκτός από νέες δυνατότητες, βελτιώσεις και διορθώσεις σφαλμάτων, οι βασικές ενημερώσεις του WordPress περιέχουν επίσης διορθώσεις ασφαλείας που ενδέχεται να σας προστατεύσουν από εισβολείς που εκμεταλλεύονται τον ιστότοπό σας στο WordPress και τον χρησιμοποιούν για παράνομα κέρδη.[51]

2.2.3.3 Παρακολούθηση του Dashboard της πλατφόρμας[52]

Το dashboard του WordPress ιστοτόπου σας είναι ένα μέρος όπου δεν θέλετε να παραμονεύει κανένας μη εξουσιοδοτημένος. Ενώ υπάρχουν ορισμένοι ιστότοποι που έχουν νόμιμους λόγους για να επιτρέπουν στους δημόσιους χρήστες να συνδεθούν χρησιμοποιώντας το dashboard του WordPress, αυτός είναι ένας τεράστιος κίνδυνος ασφαλείας και πρέπει να εξεταστεί πολύ προσεκτικά.

Ευτυχώς, οι περισσότεροι ιστότοποι WordPress δεν έχουν αυτήν την απαίτηση και ως εκ τούτου θα πρέπει να εμποδίζουν την πρόσβαση στον πίνακα ελέγχου του WordPress. Υπάρχουν διάφοροι τρόποι για να πραγματοποιηθεί αυτό και θα πρέπει ο κάθε χρήστης να επιλέξει αυτό που λειτουργεί καλύτερα για τον ίδιο.

Μια κοινή μέθοδος που αποτρέπει την είσοδο μη εξουσιοδοτημένων χρηστών είναι ο περιορισμός της πρόσβασης με χρήση κωδικού πρόσβασης με σκοπό την προστασία των

WordPress Admin (wp-admin) σελίδων. Μια άλλη λύση αποτελεί η δυνατότητα πρόσβασης στο /wp-admin μόνο από έναν αριθμό επιλεγμένων διευθύνσεων IP.

Μερικοί από τους τρόπους ενάντια σε απειλές τέτοιου είδους είναι οι εξής:

- **Απενεργοποίηση της εγγραφής χρηστών:** Από προεπιλογή, το WordPress δεν επιτρέπει στους δημόσιους χρήστες να εγγραφούν στον ιστότοπό σας στο WordPress.
- **Διαπιστευτήρια:** Όπως κάθε άλλος ιστότοπος, η δυνατότητα πρόσβαση στο WordPress dashboard σας είναι τόσο ισχυρή όσο και τα διαπιστευτήριά σας. Η επιβολή κωδικών ισχυρής ασφάλειας είναι κρίσιμη για κάθε σύστημα και το WordPress δεν αποτελεί εξαίρεση. Το WordPress δεν έχει κανέναν τρόπο να ορίσει μια πολιτική ανάθεσης κωδικού πρόσβασης, ωστόσο plugin όπως το WPassword είναι απαραίτητα για την επιβολή των απαιτήσεων της ισχύος του κωδικού πρόσβασης στους χρήστες που έχουν πρόσβαση στον πίνακα ελέγχου του WordPress.
- **Two-Factor Authentication (2FA):** Ένας άλλος βασικός έλεγχος ασφαλείας για το dashboard του WordPress σας είναι να απαιτείται έλεγχος ταυτότητας δύο παραγόντων. Ο έλεγχος ταυτότητας δύο παραγόντων (2FA) καθιστά σημαντικά πιο δύσκολο για έναν εισβολέα να αποκτήσει πρόσβαση στον πίνακα ελέγχου του WordPress ακόμα και εάν αυτός καταφέρει να υποκλέψει τον κωδικό πρόσβασης ενός χρήστη (π.χ. ένας εισβολέας μπορεί να αποκτήσει τον κωδικό πρόσβασης ενός χρήστη από data breach). Ευτυχώς, είναι πολύ εύκολο να ρυθμίσετε τον έλεγχο ταυτότητας δύο παραγόντων στο WordPress. Υπάρχουν πολλά πρόσθετα υψηλής ποιότητας που μπορείτε να χρησιμοποιήσετε για να προσθέσετε αυτήν τη λειτουργία.

2.2.3.4 Ελεγχόμενη χρήση plugin και θεμάτων^[52]

Το νούμερο ένα ζήτημα που υπονομεύει την ασφάλεια του WordPress είναι επίσης αυτό που το κάνει απίστευτα δημοφιλές. Τα πρόσθετα και τα θέματα του WordPress ποικίλλουν σε μεγάλο βαθμό ως προς την ποιότητα και την ασφάλεια. Ενώ έχει γίνει πολλή δουλειά από την ομάδα του WordPress για να βοηθήσει τους προγραμματιστές να δημιουργήσουν πιο ασφαλή πρόσθετα και θέματα, εξακολουθούν να παραμένουν ένας εφιάλτης για την ασφάλεια. Αυτό μπορεί να γίνει αντιληπτό αν κάποιος χρησιμοποιήσει κακώς συντηρημένες προσθήκες ή προσθήκες που λαμβάνονται από μια πρόχειρη πηγή.

Μερικοί τρόποι για να αποφύγετε εισβολές που προέρχονται από εύαλωτα plugin και θέματα είναι οι εξής:

- **Αποφυγή εκτέλεσης περιττού λογισμικού:** Παρόλο που μπορεί να έχετε κάνει όλη την απαραίτητη έρευνα για μια προσθήκη που σας ενδιαφέρει, αυτή μπορεί ακόμα και τότε, να αποτελεί απειλή για την ασφάλεια της ιστοσελίδας σας. Ένας από τους τρόπους άμυνας έναντι τέτοιων περιστάσεων, είναι η εκτέλεση μόνο του απαραίτητου λογισμικού που είναι αναγκαίο και εμπεριστατωμένα, πλήρως ασφαλές. Πριν γίνει η εγκατάσταση ενός νέου προσθέτου WordPress, είναι αναγκαίο ο χρήστης να αναρωτηθεί αν η εγκατάσταση του είναι πραγματικά απαραίτητη. Εάν έχετε πραγματική ανάγκη να εκτελέσετε μια προσθήκη, βεβαιωθείτε ότι διατηρείται ενεργά και ενημερώνεται τακτικά. Κατά κανόνα, το γεγονός ότι ένα θέμα ή μία προσθήκη έχουν μεγάλο αριθμό λήψεων και πρόσφατων ενημερώσεων υποδηλώνει ότι χρησιμοποιούνται ευρέως και διατηρούνται ενεργά από τους δημιουργούς τους. Αυτό

δεν σημαίνει ότι τέτοιου τύπου πρόσθετα για παράδειγμα δεν θα έχουν ποτέ ευπάθειες. Ωστόσο, εάν εντοπιστεί μια ευπάθεια, ο προγραμματιστής θα ενεργήσει γρήγορα και θα εκδώσει γρήγορα μια επιδιόρθωση. Συμβουλεύεται η αποφυγή προσθέτων που δεν έχουν πολλές λήψεις και μεγάλη ενεργή κοινότητα που συμβάλλει στις τακτικές ενημερώσεις. Εάν κάτι δεν έχει λάβει ενημέρωση εντός ενός έτους, είναι γενικά αποφευκτέο.

- **Παρακολούθηση της αρχής των ελαχίστων προνομίων:** Το WordPress δεν χρειάζεται να χρησιμοποιήσει τον χρήστη root της MySQL για να συνδεθεί στη βάση δεδομένων του. Επίσης δε χρειάζεται ο κάθε χρήστης του WordPress να έχει ρόλο διαχειριστή. Γενικότερα, η εκτέλεση προγραμμάτων με τα δικαιώματα προνομιούχου χρήστη δεν είναι καλή ιδέα εκτός αν υπάρχει κάποιος συγκεκριμένος λόγος. Οι βέλτιστες πρακτικές ασφαλείας υπαγορεύουν πάντα στις εφαρμογές να παρέχουν πάντα τα λιγότερα δυνατά προνόμια που επιτρέπουν την ορθή λειτουργία τους, με τυχόν επιπλέον προνόμια απενεργοποιημένα. Αυτή η πρακτική αναφέρεται συνήθως ως η αρχή του ελάχιστου προνομίου (principle of least privilege). Η εκτέλεση λογισμικού με δικαιώματα διαχειριστή ή η παροχή στους χρήστες περισσότερων δικαιωμάτων πρόσβασης από ό,τι χρειάζεται είναι πρόβλημα. Αντιβαίνει στη δοκιμασμένη αρχή των ελαχίστων προνομίων, καθώς επιτρέπει σε έναν εισβολέα να προκαλέσει μεγαλύτερη ζημιά σε περίπτωση παραβίασης της ασφάλειας. Το καλό με το WordPress είναι ότι έχει έναν αριθμό ενσωματωμένων ρόλων, τους οποίους μπορείτε να χρησιμοποιήσετε για να εκχωρήσετε διαφορετικά προνόμια σε διαφορετικούς χρήστες, ανάλογα με τις απαιτήσεις τους.
- **Συχνές ενημερώσεις των θεμάτων και των προσθέτων της πλατφόρμας:** Οι ενημερώσεις των προσθηκών και των θεμάτων του WordPress είναι σημαντικές όχι μόνο για να επωφεληθείτε από νέες λειτουργικότητες και διορθώσεις σφαλμάτων, αλλά και για να επιδιορθώσετε ευπάθειες ασφαλείας. Τόσο τα πρόσθετα όσο και τα θέματα ενημερώνονται εύκολα στη διεπαφή του WordPress.
- **Αποφυγή της χρήσης “nulled” θεμάτων και plugin της πλατφόρμας:** Το WordPress κάνει χρήση της άδειας GPL1. Η άδεια αυτή επιτρέπει σε οποιονδήποτε να διανέμει ελεύθερα λογισμικό που διαθέτει επίσης την ίδια άδεια. Αυτό όπως καταλαβαίνουμε, περιλαμβάνει και εμπορικά/premium θέματα και προσθήκες WordPress με άδεια χρήσης GPL. Επομένως, μπορεί να μην είναι ακριβώς παράνομο να κατεβάσουμε ένα τροποποιημένο, που συνήθως αναφέρεται ως nulled, premium θέμα ή προσθήκη και να το χρησιμοποιήσουμε δωρεάν. Ωστόσο, όπως ίσως έχετε ήδη μαντέψει, εκτός από το ότι κατά αυτό τον τρόπο δεν υποστηρίζεται ο προγραμματιστής του συγκεκριμένου plugin, είναι πολύ απίθανο να λαμβάνετε ενημερώσεις για nulled προσθήκες. Επιπλέον, δεν υπάρχει τρόπος να γνωρίζουμε εάν η πηγή αυτής της προσθήκης έχει υποστεί κάποιου είδους τροποποίηση για να κάνει κάτι μοχθηρό.

2.2.3.5 Ενίσχυση του “πυρήνα της πλατφόρμας” (WordPress Core)^[52]

Παρόλο που ο πυρήνας του WordPress αποτελεί ένα ασφαλές κομμάτι λογισμικού, αυτό δεν σημαίνει ότι δεν μπορούμε να το ενισχύσουμε περαιτέρω. Παρακάτω αναφέρονται ορισμένες

στρατηγικές σκλήρυνσης που μπορείτε να ακολουθήσετε όσον αφορά τον πυρήνα του WordPress:

- **Βεβαιωθείτε ότι το debug login είναι απενεργοποιημένο:** Το WordPress επιτρέπει στους προγραμματιστές να καταγράφουν τα μηνύματα εντοπισμού σφαλμάτων σε ένα αρχείο (αυτό είναι το `/wp-content/debug.log` από προεπιλογή). Αν και αυτό είναι απολύτως αποδεκτό όταν πρόκειται για ένα περιβάλλον ανάπτυξης, πρέπει να ληφθεί υπόψη ότι αυτό το αρχείο μπορεί να είναι εύκολα προσβάσιμο σε έναν εισβολέα, εάν το ίδιο ή/και οι ρυθμίσεις φτάσουν στην παραγωγή. Γενικότερα ο εντοπισμός σφαλμάτων του WordPress είναι απενεργοποιημένος από προεπιλογή παρόλα αυτά συμβουλευτείτε να γίνεται ένας έλεγχος για παν ενδεχόμενο.
- **Απενεργοποιήστε το XML-RPC:** Η προδιαγραφή XML-RPC του WordPress σχεδιάστηκε για να επιτρέπει την επικοινωνία μεταξύ διαφορετικών συστημάτων. Πρακτικά, αυτό σημαίνει ότι σχεδόν οποιαδήποτε εφαρμογή μπορεί να αλληλεπιδράσει με το WordPress. Η προδιαγραφή WordPress XML-RPC είναι ιστορικά σημαντική για το WordPress καθώς του επιτρέπει να αλληλεπιδρά και να ενσωματώνεται με άλλα συστήματα και λογισμικό. Το καλό είναι ότι το XML-RPC έχει πλέον αντικατασταθεί από το WordPress REST API. Μία ανησυχία όσον αφορά την ασφάλεια του XML-RPC είναι πως η διεπαφή του είναι έχει αποτελέσει την πηγή πολλών ευπαθειών όλα αυτά τα χρόνια. Επιπρόσθετα μέσω XML-RPC pingbacks οι εισβολείς μπορούν να αποπειραθούν απαρίθμηση ονομάτων χρήστη, ωμή επιβολή κωδικού πρόσβασης, ή επιθέσεις άρνησης υπηρεσίας (DoS). Επομένως, εκτός και εάν χρησιμοποιείτε ενεργά το XML-RPC και έχετε τα κατάλληλα στοιχεία ελέγχου ασφαλείας, είναι σοφό να το απενεργοποιήσετε.
- **Περιορίστε το WordPress REST API:** Στο ίδιο πνεύμα με το XML-RPC, το WordPress API είναι ο σύγχρονος τρόπος για εφαρμογές τρίτων να επικοινωνούν με το WordPress. Αν και είναι ασφαλές στη χρήση, συνιστάται να περιορίσετε ορισμένες λειτουργίες του για να αποτρέψετε την απαρίθμηση χρηστών και άλλες πιθανές ευπάθειες. Σε αντίθεση με το XML-RPC, το WordPress δεν παρέχει έναν απλό, εγγενή τρόπο για να απενεργοποιήσετε πλήρως το REST API, ωστόσο, είναι δυνατός ο περιορισμός του.
- **Αποτρέψτε την δυνατότητα αποκάλυψη της έκδοσης του WordPress:** Όπως πολλές άλλες εφαρμογές Ιστού, από προεπιλογή, το WordPress αποκαλύπτει την έκδοσή του σε διάφορα σημεία. Η αποκάλυψη έκδοσης δεν είναι ακριβώς μια ευπάθεια ασφαλείας, ωστόσο αυτές οι πληροφορίες είναι πολύ χρήσιμες για έναν εισβολέα όταν σχεδιάζει μια επίθεση. Ως αποτέλεσμα, η απενεργοποίηση της λειτουργίας αποκάλυψης έκδοσης του WordPress μπορεί να κάνει μια επίθεση λίγο πιο δύσκολη.
- **Αποτρέψτε τη απαρίθμηση των χρηστών του WordPress:** Το WordPress είναι ευάλωτο σε μια σειρά επιθέσεων απαρίθμησης χρηστών. Τέτοιες επιθέσεις επιτρέπουν σε έναν εισβολέα να καταλάβει ποιοι χρήστες υπάρχουν σε ένα site και του επιβεβαιώνουν την ύπαρξη ή μη κάποιου χρήστη. Αν και αυτό μπορεί να φαίνεται ακίνδυνο, να έχετε κατά νου ότι οι εισβολείς ενδέχεται να χρησιμοποιήσουν αυτές τις πληροφορίες ως μέρος μιας μεγαλύτερης επίθεσης.

- **Απενεργοποιήστε τον file editor του WordPress:** Ένα από τα πιο επικίνδυνα χαρακτηριστικά του WordPress είναι η δυνατότητα επεξεργασίας αρχείων μέσω του πίνακα ελέγχου του. Δεν υπάρχει νόμιμος λόγος για τον οποίο οποιοσδήποτε χρήστης πρέπει να κάνει επεξεργασία τέτοιου είδους, και σίγουρα όχι στον πυρήνα του WordPress. Αν μη τι άλλο, είναι αναγκαίο να βεβαιωθείτε ότι γνωρίζετε ακριβώς ποια αρχεία αλλάζουν στην ιστοσελίδα σας χρησιμοποιώντας πρόσθετα ασφαλείας υψηλής ποιότητας παρακολούθησης ακεραιότητας αρχείων (FIM).
- **Απενεργοποιήστε τη διαχείριση θεμάτων και προσθηκών:** Μια καλή βέλτιστη πρακτική για την ασφάλεια του WordPress είναι η απενεργοποίηση της διαχείρισης προσθηκών και θεμάτων από τον πίνακα ελέγχου του WordPress. Αντιθέτως, οι ενέργειες αυτές συμβουλεύεται να εκτελούνται με τη χρήση γραμμής εντολών όπως το wp-cli. Απενεργοποιώντας τις αλλαγές θέματος και προσθηκών, μειώνεται δραστικά η δυνατότητα επίθεσης του ιστότοπού σας. Έχοντας κάνει τις παραπάνω ενέργειες, ακόμα κι αν ένας εισβολέας παραβιάσει με επιτυχία έναν λογαριασμό διαχειριστή, δεν θα είναι σε θέση να ανεβάσει μια κακόβουλη προσθήκη για να κλιμακώσει την επίθεση πέρα από την πρόσβαση στον πίνακα ελέγχου του WordPress.

2.2.3.6 TLS (SSL)

Το Transport Layer Security (TLS) είναι απολύτως απαραίτητο για την ασφάλεια του WordPress, και είναι δωρεάν και εύκολο στη ρύθμιση. (Σημείωση: Το TLS είναι το πρωτόκολλο που αντικατέστησε το Secure Socket Layer, SSL.) Ωστόσο, δεδομένου ότι ο όρος SSL είναι πολύ δημοφιλής, πολλοί εξακολουθούν να αναφέρονται στο TLS ως SSL.

Όταν επισκέπτεστε τον ιστότοπό σας μέσω HTTPS (HTTP μέσω TLS), τα αιτήματα και οι απαντήσεις HTTP δεν μπορούν να υποκλαπούν και να κατασκοπευτούν ή χειρότερα να τροποποιηθούν από έναν εισβολέα.

Ενώ το TLS σχετίζεται περισσότερο με τον διακομιστή ιστού σας ή το Δίκτυο παράδοσης περιεχομένου (CDN) παρά με την εγκατάσταση του WordPress, μία από τις πιο σημαντικές πτυχές του TLS (WordPress HTTPS) είναι η επιβολή του.

2.2.3.7 Επιπλέον βήματα ενίσχυσης της ασφάλειας

Ορισμένοι επιπλέον τρόποι ενίσχυσης της ιστοσελίδας σας είναι:

- **Ενίσχυση της PHP:** Δεδομένου ότι η PHP είναι ένα βασικό συστατικό οποιουδήποτε ιστότοπου WordPress, η ενίσχυση της είναι ένα από τα λογικά επόμενα βήματα.
- **Χρήση αξιόπιστων προσθηκών ασφαλείας:** Τα ποιοτικά πρόσθετα ασφαλείας προσφέρουν προηγμένες λειτουργίες ασφαλείας που δεν περιλαμβάνονται εγγενώς στο WordPress. Υπάρχει ένας τεράστιος αριθμός προσθηκών ασφαλείας WordPress εκεί έξω. Ωστόσο, φροντίστε να επιλέξετε προσθήκες με καλή φήμη και, ιδανικά,

εκείνες όπου διατίθεται premium ή εμπορική υποστήριξη, όπως οι προσθήκες ασφαλείας υψηλής ποιότητας για το WordPress.

- **Πραγματοποίηση ελέγχου των δικαιωμάτων των αρχείων:** Για ιστότοπους WordPress που εκτελούνται σε Linux, τα εσφαλμένα δικαιώματα αρχείων ενδέχεται να επιτρέψουν σε μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση σε δυνητικά ευαίσθητα αρχεία.
- **Πραγματοποίηση ελέγχου των αντιγράφων ασφαλείας (backup files):** Τα αρχεία αντιγράφων ασφαλείας που αφέθηκαν κατά λάθος προσβάσιμα ενδέχεται να διαρρεύσουν ευαίσθητες πληροφορίες. Αυτό περιλαμβάνει configuration που περιέχει μυστικά που μπορεί να επιτρέψουν στους εισβολείς να αποκτήσουν τον έλεγχο ολόκληρης της εγκατάστασης του WordPress.
- **Χρήση WordPress Firewall:** ένα τείχος προστασίας WordPress μπορεί να προστατεύσει τον ιστότοπό σας στο WordPress από κακόβουλες γνωστές επιθέσεις hack
- **Χρήση αρχείου καταγραφής δραστηριοτήτων WordPress:** Μπορεί να βοηθήσει πολύ – κρατώντας ένα αρχείο όλων των αλλαγών που συμβαίνουν στον ιστότοπό σας, μπορείτε να βελτιώσετε τη λογοδοσία των χρηστών, να ξέρετε τι θέλει ο κάθε χρήστης και επίσης να παρακολουθείτε όλες τις δραστηριότητες.
- **Χρήση εργαλείων όπως το WPScan:** Τα εργαλεία αυτά μπορούν να σας βοηθήσουν να δοκιμάσετε τη στάση ασφαλείας του ιστότοπού σας στο WordPress
- **Χρήση Security Plugins του WordPress**
- **Ενίσχυση του διακομιστή ιστού σας**
- **Ενίσχυση της MySQL**
- **Προσθήκη των απαραίτητων HTTP κεφαλίδων ασφαλείας**
- **Λειτουργικό σύστημα δημιουργίας αντιγράφων ασφαλείας WordPress.**
- **Χρήση μιας υπηρεσίας προστασίας DDoS**
- **Εφαρμογή μιας Πολιτικής Ασφάλειας Περιεχομένου**

2.3 Δημοφιλή Security Plugins

Το Διαδίκτυο είναι ένα καταπληκτικό μέρος. Ωστόσο μπορεί να είναι και ιδιαίτερα τρομακτικό, καθώς εκατοντάδες χιλιάδες ιστότοποι παραβιάζονται κάθε μέρα. Οι εγκληματίες του κυβερνοχώρου δεν προβλέπεται να φύγουν σύντομα — ακόμα κι αν τους το ζητήσουμε ευγενικά. Για να προστατεύσετε τον ιστότοπό σας λοιπόν, χρειάζεστε τα καλύτερα πρόσθετα ασφαλείας του WordPress.^[54]

Αυτά τα πρόσθετα ασφαλείας έχουν δημιουργηθεί για να αμύνονται από κυβερνοεπιθέσεις που στοχεύουν το WordPress. Περιλαμβάνουν μια πληθώρα ικανοτήτων όπως τη σάρωση ιστοτόπων και τείχη προστασίας εφαρμογών ιστού (WAF). Οι προσθήκες ασφαλείας του WordPress μπορούν να είναι δωρεάν ή να πληρώνονται μηνιαία. Οι εκδόσεις επί πληρωμή

θεωρούνται συχνά ότι αξίζουν τα επαναλαμβανόμενα έξοδα για να αποφευχθεί η επίπτωση μιας επίθεσης.[54]

Η ειρωνεία είναι, πως ένα λάθος πρόσθετο μπορεί να αυξήσει τις πιθανότητες για ένα επιτυχημένο hack στον ιστότοπό σας, γι' αυτό είναι σημαντικό να επιλέγετε προσθήκες με καλή κριτική και καλή συντήρηση από τη βιβλιοθήκη προσθηκών του WordPress.[54]

Ορισμένα από τα πιο δημοφιλή Security Plugins του WordPress είναι τα εξής:

- **Wordfence Security:** Με πάνω από 4 εκατομμύρια λήψεις μέχρι σήμερα, το Wordfence είναι ένα κορυφαίο πρόσθετο ασφαλείας. Το κορυφαίο δωρεάν εργαλείο σάρωσης του ελέγχει τα βασικά αρχεία, τα αρχεία προσθηκών, τα αρχεία θεμάτων, τις αναρτήσεις και τα σχόλια για ύποπτους κώδικα, λανθασμένες διευθύνσεις URL και ανεπιθύμητα μηνύματα. Το Wordfence εκτελεί αυτές τις σαρώσεις τακτικά και αυτόματα και σας ειδοποιεί εάν εντοπίσει απειλή, ευπάθεια ή κατεστραμμένο αρχείο. Αν και δεν προσφέρει επιλογές επαναφοράς για το τελευταίο, θα σας πει πώς έχει αλλάξει το αρχείο, ώστε να μπορείτε να το επιδιορθώσετε πιο γρήγορα. Η δωρεάν έκδοση περιλαμβάνει ένα τείχος προστασίας ιστότοπου για τη διατήρηση των bot εκτός του ιστότοπού σας — σε αντίθεση με τα περισσότερα πρόσθετα ασφαλείας, τα οποία προσφέρουν μόνο τείχος προστασίας στην premium έκδοση τους. Η δωρεάν έκδοση του Wordfence περιλαμβάνει επίσης όρια προσπαθειών σύνδεσης για τη διακοπή επιθέσεων brute force και ζωντανή παρακολούθηση της κυκλοφορίας που παρακολουθεί ποιος επισκέπτεται τον ιστότοπό σας (άνθρωποι, καλά bot ή κακά bot) και αναφέρει απόπειρες κακόβουλης εισβολής σε πραγματικό χρόνο. Το Wordfence Security προσφέρει μια premium έκδοση που περιλαμβάνει φίλτρα ανεπιθύμητων σχολίων, country blocking, απομακρυσμένη σάρωση, έλεγχο ταυτότητας δύο παραγόντων και premium υποστήριξη πελατών.
- **iThemes Security:** Το iThemes Security έχει περισσότερους από 1 εκατομμύριο χρήστες παγκοσμίως και προσφέρει τόσο δωρεάν όσο και επί πληρωμή έκδοση. Η δωρεάν έκδοση πραγματοποιεί σαρώσεις κακόβουλου λογισμικού που υποστηρίζονται από το Sucuri SiteCheck και παρέχει συμβουλές για την αντιμετώπιση τυχόν ευπαθειών που εντοπίστηκαν. Ορίζει επίσης διάφορες απαιτήσεις ασφαλείας σε ολόκληρο τον ιστότοπό σας. Για παράδειγμα, επιβάλλει ισχυρούς κωδικούς πρόσβασης και SSL σε όλες τις σελίδες και εμποδίζει τον διαχειριστή να επεξεργάζεται αρχεία εάν κάποιος εισβολέας αποκτήσει ποτέ πρόσβαση στα προσωπικά σας διαπιστευτήρια. Το iThemes σας επιτρέπει επίσης να αλλάξετε το πρόθεμα πίνακα βάσης δεδομένων του WordPress και τη διαδρομή wp-content, απαγορεύει τα ενοχλητικά bots και spiders, αποτρέπει επιθέσεις brute force και δημιουργεί αντίγραφα ασφαλείας της βάσης δεδομένων σας. Για διαδικτυακές συγκρίσεις αρχείων, θα πρέπει να κάνετε αναβάθμιση στην έκδοση premium. Όταν εντοπιστεί μια αλλαγή αρχείου, η προσθήκη θα σαρώσει την προέλευση των αρχείων για να προσδιορίσει εάν η αλλαγή ήταν κακόβουλη ή όχι. Προς το παρόν, λειτουργεί μόνο για βασικά αρχεία WordPress — όχι για προσθήκες και θέματα. Ξεκινώντας από 80 \$ ετησίως, το iThemes Security Pro προσφέρει πιο προηγμένες λειτουργίες: GeoIP, έλεγχο ταυτότητας δύο παραγόντων, αυτοματοποιημένη καθημερινή σάρωση κακόβουλου λογισμικού, λήξη κωδικού πρόσβασης και captchas Google, για να αναφέρουμε μερικά. Η δωρεάν έκδοση είναι μια εξαιρετική επιλογή για αρχάριους,

αλλά η premium έκδοση είναι όπου το iThemes λάμπει. Και οι δύο εκδόσεις του iThemes έχουν κατασκευαστεί για να συνδυάζονται με τη διεπαφή διαχειριστή του WordPress και η βιβλιοθήκη τεκμηρίωσης και τα εκπαιδευτικά βίντεο βοηθούν στη μείωση της καμπύλης εκμάθησης.[54]

- **Sucuri Security:** Η Sucuri είναι δημοφιλής μεταξύ των προγραμματιστών ιστού και των διαδικτυακών επιχειρήσεων για τα εξαιρετικά προϊόντα και τις υπηρεσίες της στον κυβερνοχώρο. Το δωρεάν πρόσθετο ασφαλείας WordPress της Sucuri, το οποίο δίνει εκτεταμένο έλεγχο στον ιστότοπό σας και μια ολοκληρωμένη επισκόπηση των πτυχών που σχετίζονται με την ασφάλεια, είναι μεταξύ αυτών των προσφορών. Εκτός από πόρους όπως ειδοποιήσεις ηλεκτρονικού ταχυδρομείου, ελέγχους ακεραιότητας πυρήνα του WordPress και οδηγούς για ένα σενάριο μετά την εισβολή, η προσθήκη του Sucuri περιέχει έναν σαρωτή που εντοπίζει κακόβουλο λογισμικό, σφάλματα, παλιό κώδικα και την κατάσταση της μαύρης λίστας. Ένας περιορισμός του σαρωτή της Sucuri είναι ότι είναι ένα απομακρυσμένο εργαλείο, επομένως μπορεί να βρει τρωτά σημεία μόνο στις σελίδες του ιστότοπού σας στο WordPress. Δεν μπορεί να σαρώσει τα βασικά αρχεία που ελέγχουν το back end του ιστότοπού σας. Επιπλέον, για να ξεκλειδώσετε τα πλεονεκτήματα της εικονικής επιδιόρθωσης και σκλήρυνσης, της προστασίας DDoS, της βελτιστοποίησης απόδοσης CDN, του εντοπισμού υπογραφών και του αποκλεισμού bot, θα πρέπει να πληρώσετε για την υπηρεσία τείχους προστασίας εφαρμογών ιστού της Sucuri.[54]
- **WP fail2ban:** Το fail2ban είναι ένα από τα πιο απλά και αποτελεσματικά μέτρα ασφαλείας που μπορείτε να εφαρμόσετε για να αποτρέψετε επιθέσεις ωμής βίας. Το WP fail2ban καταγράφει όλες τις προσπάθειες σύνδεσης – συμπεριλαμβανομένου του XML-RPC, είτε επιτυχές είτε όχι, στο σύστημα καταγραφής χρησιμοποιώντας το LOG_AUTH. Το WPf2b διαθέτει τρία φίλτρα fail2ban: wordpress-hard.conf, wordpress-soft.conf και wordpress-extra.conf. Αυτά έχουν σχεδιαστεί για να επιτρέπουν τη διάκριση μεταξύ της άμεσης απαγόρευσης (σκληρή) και της παραδοσιακής πιο χαριτωμένης προσέγγισης (μαλακή), με επιπλέον κανόνες για προσαρμοσμένες διαμορφώσεις.[55]
- **All in One WP Security & Firewall:** Το All In One WP Security & Firewall είναι μια δωρεάν, δημοφιλής και ευέλικτη προσθήκη ασφαλείας. Αυτό το πρόσθετο μπορεί να υπερηφανεύεται για ένα ευρύ φάσμα δυνατοτήτων που προσφέρονται παρά την έλλειψη χρέωσης, όπως την σάρωση κακόβουλου λογισμικού και ευπάθειας, την προστασία σύνδεσης, την προστασία από ανεπιθύμητα σχόλια, την παρακολούθηση χρηστών, τη δημιουργία αντιγράφων ασφαλείας βάσης δεδομένων, το τείχος προστασίας και άλλους τρόπους για να ενισχύσετε τον ιστότοπό σας. Όλα αυτά συνδέονται με μια διαισθητική, καινοτόμο διεπαφή — η προσθήκη παρουσιάζει τα ευρήματά της με ένα σύστημα βαθμολόγησης, διευκολύνοντας τους αρχάριους ιδιοκτήτες ιστοτόπων να κατανοήσουν και να βελτιώσουν την ασφάλεια του ιστότοπού τους. Μια όχι και τόσο φιλική προς τους αρχάριους πτυχή αυτής της προσθήκης ωστόσο είναι ότι ενώ ένας χρήστης μπορεί να ενεργοποιήσει τη βασική προστασία τείχους προστασίας επιλέγοντας ένα πλαίσιο στον πίνακα εργαλείων του WordPress, θα πρέπει να προσθέσει τους ενδιάμεσους και προχωρημένους κανόνες τείχους προστασίας της προσθήκης μέσω του αρχείου .htaccess. Αυτό μπορεί

ενδεχομένως να διακόψει κάποια λειτουργικότητα άλλων προσθηκών που είναι εγκατεστημένα στον ιστότοπό, επομένως ενδέχεται να υπάρξουν δοκιμές και σφάλματα κατά την εφαρμογή των πιο προηγμένων κανόνων του τείχους προστασίας.[\[54\]](#)

- **Jetpack:** Το Jetpack, (κατασκευασμένο από την Automattic) είναι ένα εργαλείο πολλαπλών χρήσεων που είναι καλό (σχεδόν) σε όλα. Βοηθά με το μάρκετινγκ, το σχεδιασμό και την ασφάλεια. Μεταξύ των διαφόρων δυνατοτήτων του, κάποιος μπορεί να βρει αναλυτικά στοιχεία ιστότοπου, αυτοματοποιημένη ανάρτηση στα μέσα κοινωνικής δικτύωσης, πολλαπλά θέματα WordPress, φιλτράρισμα ανεπιθύμητων μηνυμάτων, παρακολούθηση downtime, σάρωση κακόβουλου λογισμικού, ασφάλεια όσον αφορά την σύνδεση, αργή φόρτωση εικόνων, CDN και πολλά άλλα. Το Jetpack διατίθεται σε ένα δωρεάν και τρία προγράμματα επί πληρωμή, επομένως δεν είναι όλες οι λειτουργίες του δωρεάν. Το πρόσθετο είναι κατάλληλο για προσωπικά ιστολόγια και τόσο για νεοσύστατες όσο και για εταιρικές επιχειρήσεις. Καλύπτει όλες τις βασικές ανάγκες και όλους τους προϋπολογισμούς.[\[53\]](#)
- **SecuPress:** Εάν είστε προληπτικοί, η δωρεάν έκδοση αυτού του πρόσθετου ασφαλείας WordPress είναι μια εξαιρετική επιλογή! Δεν υπάρχει χρόνος για ενεργοποίηση εβδομαδιαίων σαρώσεων; Τότε το SecuPress pro είναι η καλύτερη επιλογή. Αυτό το πρόσθετο φροντίζει τα πάντα με αυτοματοποιημένες εργασίες. Μερικές από τις δυνατότητες που παρέχει είναι: [\[56\]](#)
 - Anti Brute Force login
 - Blocked IPs
 - Firewall
 - Security alerts
 - Malware Scan
 - Block country by geolocation
 - Protection of Security Keys
 - Block visits from Bad Bots
 - Vulnerable Plugins & Themes detection
 - Security Reports in PDF format
- **BulletProof Security:** Το BulletProof Security είναι μια κατάλληλη επιλογή εάν αναζητάτε ένα πιο προηγμένο, πρακτικό πρόσθετο ασφαλείας. Αυτό το πρόσθετο εκτελεί τις εργασίες του μέσω του κύριου αρχείου .htaccess και τα κύρια χαρακτηριστικά του βελτιώνουν την ασφάλεια της βάσης δεδομένων, την ασφάλεια του τείχους προστασίας και τη σκλήρυνση σύνδεσης. Το BulletProof περιλαμβάνει επίσης μη αυτόματα και προγραμματισμένα αντίγραφα ασφαλείας της βάσης δεδομένων, καταγραφή ασφαλείας και καταγραφή σφαλμάτων HTTP, καθώς και την επιλογή ενεργοποίησης της λειτουργίας συντήρησης, ώστε να μπορείτε να εισάγετε πιθανότητες χωρίς να εκθέτετε πιθανά προβλήματα απόδοσης στους επισκέπτες σας. Η δωρεάν έκδοση του BulletProof Security είναι αρκετά ικανή από μόνη της και η pro έκδοση σχεδόν διπλασιάζει τον αριθμό των χαρακτηριστικών. Θα πρέπει να κάνετε αναβάθμιση σε αυτήν την έκδοση για να ξεκλειδώσετε το τείχος προστασίας της — το οποίο προσφέρουν ορισμένα πρόσθετα δωρεάν — αλλά θα έχετε προηγμένη λειτουργικότητα που καμία άλλη προσθήκη ασφαλείας δεν παρέχει. Το

AutoRestore Intrusion Detection & Prevention System είναι ένα μόνο παράδειγμα. Αυτό το σύστημα παρακολουθεί όλα τα αρχεία του ιστότοπού σας για αλλαγές. Εάν εντοπιστούν αλλαγές αρχείων ή αν ανεβαίνουν νέα αρχεία στον ιστότοπό σας, τότε αυτά τα αρχεία είτε αποκαθίστανται αυτόματα είτε τίθενται σε καραντίνα για έλεγχο πιθανής κακόβουλης δραστηριότητας. Η προσθήκη Bulletproof Security μπορεί να πάρει λίγο περισσότερο χρόνο για να μάθουν οι αρχάριοι, αλλά ο οδηγός εγκατάστασης και η ολοκληρωμένη τεκμηρίωση υπάρχουν για να κάνουν τα πράγματα λίγο πιο απλά.^[54]

- **WPScan - Wordpress Security Scanner:** Το πρόσθετο ασφαλείας WPScan WordPress είναι μοναδικό καθώς χρησιμοποιεί τη δική του, μη αυτόματα επιμελημένη βάση δεδομένων ευπάθειας WPScan WordPress. Η βάση δεδομένων ευπάθειας υπάρχει από το 2014 και ενημερώνεται σε καθημερινή βάση από αφοσιωμένους ειδικούς ασφαλείας του WordPress και την κοινότητα γενικότερα. Η βάση δεδομένων περιλαμβάνει περισσότερα από 21.000 γνωστά τρωτά σημεία ασφαλείας. Το πρόσθετο χρησιμοποιεί αυτήν τη βάση δεδομένων για τη σάρωση ευπαθειών του WordPress, τρωτών σημείων προσθηκών και ευπαθειών θεμάτων και έχει τις επιλογές να προγραμματίζει αυτοματοποιημένες καθημερινές σαρώσεις και να στέλνει ειδοποιήσεις μέσω email. Το WPScan έχει ένα δωρεάν πρόγραμμα API που θα πρέπει να είναι κατάλληλο για τους περισσότερους ιστότοπους WordPress, ωστόσο, έχει επίσης προγράμματα επί πληρωμή για χρήστες που μπορεί να χρειαστούν περισσότερα API calls. Για να χρησιμοποιήσετε το WPScan WordPress Security Plugin θα χρειαστεί να χρησιμοποιήσετε ένα δωρεάν διακριτικό API.^[57]
- **VaultPress:** Το VaultPress είναι μια υπηρεσία σάρωσης backup και ασφάλειας που λειτουργεί σε πραγματικό χρόνο. Σχεδιάστηκε και κατασκευάστηκε από την Automattic, την ίδια εταιρεία που διαχειρίζεται (και δημιουργεί αντίγραφα ασφαλείας!) εκατομμυρίων τοποθεσιών στο WordPress.com. Το VaultPress υποστηρίζεται πλέον από το Jetpack και δημιουργεί χωρίς κόπο αντίγραφα ασφαλείας κάθε ανάρτησης, σχολίου, αρχείου πολυμέσων, αναθεώρησης και ρύθμισης πίνακα εργαλείων του ιστοτόπου σας και τα αποστέλλει στους διακομιστές του. Το VaultPress προστατεύει τους χρήστες του από χάκερ, κακόβουλο λογισμικό, τυχαία ζημιά και διακοπές λειτουργίας κεντρικού υπολογιστή. ^[58]
- **Google Authenticator -Two Factor Authentication:** Το plugin Google Authenticator του WordPress παρέχει έλεγχο ταυτότητας δύο παραγόντων χρησιμοποιώντας την εφαρμογή Google Authenticator για Android, iPhone ή Blackberry. Εάν γνωρίζετε τα περί της ασφάλειας, μπορεί να έχετε ήδη εγκατεστημένη την εφαρμογή Google Authenticator στο smartphone σας, και αν τη χρησιμοποιείτε για τον έλεγχο ταυτότητας δύο παραγόντων στο Gmail, Dropbox, Lastpass, Amazon κ.λπ. Η απαίτηση ελέγχου ταυτότητας δύο παραγόντων μπορεί να ενεργοποιηθεί ανά χρήστη. Μπορεί να ενεργοποιηθεί για τον λογαριασμό διαχειριστή της ιστοσελίδας, χωρίς ωστόσο να είναι αναγκαίο να αλλάξει ο τρόπος σύνδεσης των λιγότερων προνομιούχων λογαριασμών. Εάν πρέπει να διατηρήσετε το ιστολόγιό σας χρησιμοποιώντας μια εφαρμογή Android, iPhone ή οποιοδήποτε άλλο λογισμικό που χρησιμοποιεί τη διεπαφή XMLRPC, μπορείτε να ενεργοποιήσετε τη λειτουργία κωδικού πρόσβασης εφαρμογή, ωστόσο είναι απαραίτητο να σημειωθεί ότι η

ενεργοποίηση το App password feature θα κάνει το ιστολόγιό σας λιγότερο ασφαλές.
[\[59\]](#)

- **Security Ninja:** Για έλεγχο ευπάθειας που είναι ολοκληρωμένος και φιλικός προς το χρήστη, δοκιμάστε την προσθήκη Security Ninja. Αυτό το εργαλείο εκτελεί περισσότερους από 50 ελέγχους ασφαλείας στα βασικά αρχεία, τα θέματα, τις προσθήκες και την ισχύ του κωδικού πρόσβασης και, στη συνέχεια, αναφέρει την κατάσταση ασφαλείας του ιστότοπού σας στον πίνακα ελέγχου. Η δωρεάν έκδοση του Security Ninja αναφέρει μόνο προβλήματα και δεν αλλάζει τον ιστότοπό σας με κανέναν τρόπο. Επομένως, αν διστάζετε να κάνετε σημαντικές αλλαγές αυτή τη στιγμή, δοκιμάστε την! Από την άλλη πλευρά, εάν χρειάζεστε ένα πρόσθετο που εφαρμόζει διορθώσεις σε αυτά τα ζητήματα για εσάς, σκεφτείτε μια εναλλακτική λύση ή αναβαθμίστε το Security Ninja Pro για 39,99 \$ ετησίως. Εκτός από αυτόματο πρόγραμμα επιδιόρθωσης, η επαγγελματική έκδοση περιλαμβάνει τείχος προστασίας, σαρωτή κακόβουλου λογισμικού, καταγραφικό συμβάντων και προγραμματισμένες σαρώσεις.[\[54\]](#)
- **Defender:** Το Defender είναι μια νέα αλλά πολλά υποσχόμενη λύση ασφαλείας για το WordPress που έχει ήδη ληφθεί πάνω από ένα εκατομμύριο φορές. Αφού εγκαταστήσετε και ρυθμίσετε τις παραμέτρους του εργαλείου με μερικά κλικ, αυτό ξεκινάει αμέσως να προστατεύει τον ιστότοπό σας. Το Defender προσφέρει μια εντυπωσιακή γκάμα χαρακτηριστικών ασφαλείας χωρίς κόστος. Όπως το Wordfence, παρέχει ένα τείχος προστασίας με δωρεάν αποκλεισμό IP ενεργοποιημένο. Επιπλέον, η δωρεάν έκδοσή του περιλαμβάνει σαρώσεις κακόβουλου λογισμικού, προστασία σύνδεσης με brute force, ειδοποιήσεις από απειλές και έλεγχο ταυτότητας δύο παραγόντων μέσω της Google. Η αναβάθμιση σε Defender Pro για 49 \$ / μήνα επιτρέπει τον προγραμματισμό αυτοματοποιημένων σαρώσεων, πιο εμπεριστατωμένη αναφορά προβλημάτων ασφαλείας και βελτιωμένη υποστήριξη. Η συνδρομή παρέχει επίσης πρόσβαση σε όλα τα άλλα premium πρόσθετα WordPress που δημιουργήθηκαν από την WPMU Dev.[\[54\]](#)
- **Astra Web Security:** Με το Astra, δεν χρειάζεται να ανησυχείτε για κακόβουλο λογισμικό, παραβίαση πιστωτικής κάρτας, SQLi, XSS, SEO Spam, ανεπιθύμητα σχόλια, brute force attacks και 100+ είδη απειλών. Αυτό σημαίνει ότι μπορείτε να απαλλαγείτε από άλλα πρόσθετα ασφαλείας και να αφήσετε το Astra να τα φροντίσει όλα. Το Astra εγκαθίσταται ως επέκταση ακολουθώντας βήματα αυτοεξυπηρέτησης και εύκολης εκτέλεσης (διαρκεί λιγότερο από 5 λεπτά). Αυτό σημαίνει ότι δε χρειάζεται να γίνουν αλλαγές στις ρυθμίσεις του DNS, σε αντίθεση με άλλα πρόσθετα ασφαλείας. Επιπλέον, αυτή η προσθήκη προσφέρει Web Application Firewall για την προστασία του ιστότοπού σας σε πραγματικό χρόνο, on-demand σαρωτή κακόβουλου λογισμικού που υποστηρίζεται από μηχανική εκμάθηση, άμεση εκκαθάριση κακόβουλου λογισμικού, αξιολόγηση ασφάλειας και ευπάθειας κοινότητας και δοκιμή διείσδυσης (VAPT) για την εύρεση όλων των πιθανών ελαττωμάτων και σφαλμάτων επιχειρηματικής λογικής.[\[60\]](#)
- **Shield Security:** Το Shield Security είναι ένα από τα πρόσθετα ασφαλείας με την υψηλότερη βαθμολογία και τις περισσότερες λήψεις στον κατάλογο του WordPress. Αρχίζει να λειτουργεί αμέσως μόλις ενεργοποιηθεί, επομένως ο ιστότοπός σας

προστατεύεται ακόμη και όταν διαμορφώνετε τις ρυθμίσεις του. Η δωρεάν έκδοση προσφέρει ένα τείχος προστασίας application-layer και έγκαιρη αναγνώριση και αυτόματο αποκλεισμό κακόβουλων ρομπότ. Το Shield Security είναι επίσης το μόνο πρόσθετο ασφαλείας του WordPress που προσφέρει πλήρη και ακριβή ανίχνευση τροποποιήσεων αρχείων για προσθήκες και θέματα — όχι μόνο βασικά αρχεία. Αυτό συμβαίνει επειδή ενώ άλλες προσθήκες βασίζονται αποκλειστικά στα βασικά αρχεία δακτυλικών αποτυπωμάτων που παρέχει το WordPress, η Shield Security δημιουργεί τα δακτυλικά αποτυπώματα των αρχείων της. Για να προστατεύσετε premium πρόσθετα και θέματα και να αποκτήσετε πρόσβαση σε μεμονωμένη, αποκλειστική τεχνική υποστήριξη, θα χρειαστεί να κάνετε αναβάθμιση στο ShieldPRO.^[54]

- **WebARX:** Το WebARX λαμβάνει συγκεκριμένα δεδομένα σχετικά με τους επισκέπτες του ιστότοπού του όταν αυτές οι πληροφορίες παρέχονται οικειοθελώς, όπως όταν οι επισκέπτες μας ζητούν πληροφορίες, αγοράζουν ή εγγράφονται για Υπηρεσίες, υποβάλλουν αίτημα υποστήριξης πελατών, παρέχουν πληροφορίες για ευκαιρίες απασχόλησης ή στέλνουν email με προσωπικά στοιχεία. Ορισμένες από αυτές τις δραστηριότητες απαιτούν οι χρήστες να δώσουν πληροφορίες, όπως για παράδειγμα όταν κάνουν μια αγορά, υποβάλλουν το βιογραφικό του ή ζητούν συγκεκριμένους τύπους πληροφοριών.^[61]
- **Security & Malware Scan by Clean Talk:** Η cloud εταιρεία υπηρεσιών ασφάλειας, CleanTalk, σχεδίασε την προσθήκη Security & Malware Scan για να προστατεύει τους ιστότοπους του WordPress από όλες τις διαδικτυακές απειλές. Εκτός από τον περιορισμό των προσπαθειών σύνδεσης και την προσωρινή απαγόρευση διευθύνσεων IP με 10+ προσπάθειες σύνδεσης, το CleanTalk Security μπορεί να διαμορφωθεί ώστε να αποκλείει διευθύνσεις IP που έχουν υπερβεί έναν καθορισμένο αριθμό αιτημάτων HTTP ανά ώρα, διευθύνσεις IP από μια συγκεκριμένη κομητεία ή ολόκληρα δίκτυα IP. Το τείχος προστασίας εφαρμογών ιστού του ελέγχει όλα τα αιτήματα HTTP για SQL Injection, Cross-Site Scripting (XSS), μεταφορτωμένα αρχεία από μη εξουσιοδοτημένους χρήστες, κατασκευές/κώδικες PHP και κακόβουλο κώδικα. Τυχόν αποκλεισμένα αιτήματα θα καταγράφονται και θα μπορούν να προβληθούν στον πίνακα ελέγχου σας. Το CleanTalk Security θα σαρώσει επίσης όλα τα αρχεία του WordPress — συμπεριλαμβανομένων των αρχείων προσθηκών και θεμάτων, όχι μόνο του πυρήνα — και θα επισημάνει τυχόν αρχεία με ύποπτο κώδικα στον πίνακα ελέγχου σας. Μπορείτε να δείτε τον κωδικό εκεί καθώς και άλλα λεπτομερή στατιστικά ασφαλείας. Ενώ η προσθήκη είναι δωρεάν, απαιτεί συνδρομή στην υπηρεσία ασφάλειας cloud του CleanTalk. Όταν εγγραφείτε για πρώτη φορά στον λογαριασμό σας, θα λάβετε μια δωρεάν δοκιμή. Μόλις λήξει η δωρεάν δοκιμή, μπορείτε να ανανεώσετε τη συνδρομή ξεκινώντας από 8 \$ ετησίως ή να απενεργοποιήσετε την προσθήκη.^[54]
- **MalCare Security:** Έχουμε μιλήσει για πολλές επιλογές όσον αφορά την αποτροπή κυβερνοεπιθέσεων, αλλά οι περισσότεροι άνθρωποι δεν θέλουν ούτε να σκεφτούν τι θα έκαναν μετά από μια επιτυχημένη απόπειρα hacking. Εδώ μπαίνει το MalCare Security. Αυτή η προσθήκη ειδικεύεται στην εκκαθάριση κακόβουλου λογισμικού μετά την επίθεση, προσφέροντας αφαίρεση με ένα κλικ με την έκδοση premium (ξεκινώντας από 99 \$ ετησίως). Το MalCare free είναι μια σταθερή προσθήκη από

μόνη της — συνοδεύεται από εργαλεία για βαθιά σάρωση κακόβουλου λογισμικού των αρχείων του ιστότοπού σας και της βάσης δεδομένων WordPress, προστασία σύνδεσης και bot και ένα τείχος προστασίας εφαρμογών ιστού. Ωστόσο, θα χρειαστεί να κάνετε αναβάθμιση για να επωφεληθείτε από τις αυτόματες και απεριόριστες εκκαθαρίσεις μετά την εισβολή.[54]

- **miniOrange's Google Authenticator:** Παραδόξως, ο έλεγχος ταυτότητας δύο παραγόντων δεν είναι δεδομένος για τα περισσότερα δωρεάν πρόσθετα ασφαλείας του WordPress. Ωστόσο, εάν θέλετε να ενσωματώσετε ένα δωρεάν πρόσθετο ασφαλείας ή έχετε πιο περιορισμένο προϋπολογισμό και δεν μπορείτε να αντέξετε οικονομικά μια premium λύση που προσφέρει τείχος προστασίας, αποκλεισμό IP, αφαίρεση κακόβουλου λογισμικού και άλλες δυνατότητες ασφαλείας, το MiniOrange είναι μία δωρεάν, απλή λύση για να αποκτήσετε επιπλέον προστασία σύνδεσης. Με αυτήν την προσθήκη, μπορείτε να προσθέσετε το Google 2FA στις οθόνες σύνδεσής σας για χρήστες σε όλα τα επίπεδα πρόσβασης, καθώς και στις φόρμες σας και σε άλλα πεδία υποβολής χρηστών. Επιπλέον, το Google Authenticator ενσωματώνεται με άλλες δημοφιλείς προσθήκες περιορισμού περιεχομένου, όπως το BuddyPress και το Ultimate Member και σας επιτρέπει ακόμη και να επιλέξετε την προτιμώμενη δευτερεύουσα μέθοδο ελέγχου ταυτότητας.[54]
- **Cerber Security, Anti-spam & Security:** Το Cerber Security είναι ένα άλλο πρόσθετο ασφαλείας πέντε αστέρων που είναι αποτελεσματικό έναντι επιθέσεων χάκερ, scammers, trojans και κακόβουλου λογισμικού. Η δωρεάν έκδοση του Cerber Security προσφέρει εξελιγμένη προστασία από ανεπιθύμητα μηνύματα και άλλες κακόβουλες δραστηριότητες — αλλά δεν είναι τόσο πλούσια σε δυνατότητες όσο άλλες δωρεάν εκδόσεις προσθηκών σε αυτήν τη λίστα. Η αναβάθμιση στην έκδοση premium θα ξεκλειδώσει περισσότερες λειτουργίες, συμπεριλαμβανομένης της πολυεπίπεδης προστασίας από ανεπιθύμητα μηνύματα και αυτοματοποιημένους ελέγχους ακεραιότητας. Επιπλέον, με το Cerber Security Pro, μπορείτε να προγραμματίσετε αυτοματοποιημένες σαρώσεις ιστοτόπων και ανάκτηση αρχείων ωριαία ή καθημερινά. Το Cerber Security θα αφαιρέσει το κακόβουλο λογισμικό και θα ανακτήσει τα κατεστραμμένα αρχεία σας εάν εντοπίσει κακόβουλο λογισμικό ή τυχόν τροποποιημένα ή μολυσμένα αρχεία.[54]
- **NinjaFirewall (WP Edition):** Το NinjaFirewall είναι ένα από τα πιο ισχυρά πρόσθετα ασφαλείας που διατίθενται σε δωρεάν και premium έκδοση. Σε αντίθεση με άλλα πρόσθετα, το NinjaFirewall «στέκεται» μπροστά από το WordPress. Αυτό σημαίνει ότι επεξεργάζεται όλα τα εισερχόμενα αιτήματα HTTP προτού φτάσουν στον ιστότοπό σας ή σε οποιαδήποτε από τις εγκατεστημένες προσθήκες του. Αυτό καθιστά το NinjaFirewall το μόνο πρόσθετο WordPress που μπορεί να προστατεύσει έναν ιστότοπο από μαζικές επιθέσεις ωμής βίας, συμπεριλαμβανομένων κατανεμημένων επιθέσεων που προέρχονται από πολλές χιλιάδες IP. Παρέχει επίσης μια ισχυρή μηχανή φιλτραρίσματος που μπορεί να απολυμαίνει, να ομαλοποιεί, να μετασχηματίζει, να αποκωδικοποιεί και να αποσυμφορεί δεδομένα από εισερχόμενα αιτήματα HTTP. Αυτό του επιτρέπει να ανιχνεύει τυχόν WAF evasion τεχνικές και obfuscation τακτικές που χρησιμοποιούνται από χάκερ οι οποίες μπορεί να έχουν περάσει απαρατήρητες από άλλα τείχη προστασίας πρόσθετων. Επιπλέον, το

NinjaFirewall προσφέρει παρακολούθηση ακεραιότητας αρχείων και ανίχνευση σε πραγματικό χρόνο. Όχι μόνο ελέγχει την ακεραιότητα του αρχείου σας όταν σαρώνει τον ιστότοπό σας κάθε ώρα, δύο φορές την ημέρα ή καθημερινά (ανάλογα με τον τρόπο διαμόρφωσης των ρυθμίσεων της προσθήκης) — μπορεί επίσης να εντοπίσει οποιαδήποτε πρόσβαση σε ένα αρχείο PHP που τροποποιήθηκε ή δημιουργήθηκε πρόσφατα και να σας στείλει ειδοποίηση σε πραγματικό χρόνο. Αυτή η ειδοποίηση θα περιέχει όλες τις λεπτομέρειες που χρειάζεστε — όνομα σεναρίου, διεύθυνση IP, αίτημα, ημερομηνία και ώρα — για να προσδιορίσετε εάν επρόκειτο για κακόβουλη δραστηριότητα. Για περισσότερες δυνατότητες, όπως περιορισμός ρυθμού, anti-spam για σχόλια και φόρμες εγγραφής και άλλα στοιχεία ελέγχου μεταφόρτωσης και πρόσβασης αρχείων, μπορείτε να κάνετε αναβάθμιση σε NinjaFirewall WP+ Edition. Είναι σημαντικό να σημειωθεί ότι το NinjaFirewall απαιτεί έκδοση PHP 5.5 ή μεταγενέστερη και επέκταση MySQLi. Είναι επίσης συμβατό μόνο με λειτουργικά συστήματα Linux και BSD. Αυτό σημαίνει ότι οι ιδιοκτήτες ιστότοπων WordPress που χρησιμοποιούν Microsoft Windows θα πρέπει να χρησιμοποιήσουν μια εναλλακτική λύση.[\[54\]](#)

Κεφάλαιο 3: Μεθοδολογία Έρευνας

3.1 Ερευνητικά Ερωτήματα

Για τον σχεδιασμό του ερωτηματολογίου βασιστήκαμε κυρίως στα ερευνητικά ερωτήματα που θέλαμε να απαντηθούν προκειμένου να καλύψουμε το κενό που υπάρχει στην επιστημονική κοινότητα όσον αφορά την ποιότητα της ασφάλειας των ιστοσελίδων που δημιουργούνται από επαγγελματίες με τη χρήση WordPress. Προκειμένου να δημιουργήσουμε μια συνολική εικόνα τόσο για το εκπαιδευτικό επίπεδο των ερωτηθέντων όσο και για τις μεθόδους που ακολουθούν για να ασφαλίσουν τις ιστοσελίδες τους ρωτήσαμε τα εξής:

- Πώς ασφαλίζουν τα WordPress sites τους;
- Χρησιμοποιούν κάποιο plugin ασφάλειας; Αν ναι ποιό χρησιμοποιούν και πως το εγκαθιστούν;
- Προσωπικές πληροφορίες που αφορούν τους προγραμματιστές/διαχειριστές των ιστοσελίδων
- Ποιά είναι η εμπειρία τους όσον αφορά τη δημιουργία ιστοσελίδων;
- Ποιό είναι το είδος των ιστοσελίδων που διαχειρίζονται;
- Πόσο σημαντική θεωρούν την ασφάλεια των ιστοσελίδων που δημιουργούν;
- Ποιές πρακτικές χρησιμοποιούν για να διατηρήσουν τον ιστότοπό τους ασφαλή;

3.2 Σχεδιασμός Ερωτηματολογίου

Το ερωτηματολόγιο το οποίο παρουσιάζεται στην συνέχεια χωρίστηκε σε επτά βασικές ενότητες (στις ενότητες αυτές δεν περιλαμβάνεται η ενότητα που περιγράφει το ποιόν του ερωτηματολογίου και η τελευταία ενότητα στην οποία παρατίθενται οι ευχαριστίες) ως εξής:

- Η πρώτη ενότητα απαρτίζεται από μία μονάχα ερώτηση η οποία μας ενημερώνει αν ο χρήστης χρησιμοποιεί κάποιο all-in-one security plugin.
- Η δεύτερη ενότητα απαρτίζεται από μία μονάχα ερώτηση που αφορά τους τρόπους με τους οποίους οι χρήστες επιλέγουν να ασφαλίσουν τις ιστοσελίδες τους.
- Η τρίτη ενότητα απαρτίζεται από έξι ερωτήσεις που αφορούν τη χρήση των plugin, πώς οι χρήστες επιλέγουν να τα εγκαταστήσουν κτλ.
- Η τέταρτη ενότητα περιλαμβάνει μόνο μία ερώτηση που επιθυμεί να χωρίσει τους χρήστες σε δύο κατηγορίες: α) σε αυτούς που δημιουργούν ιστοσελίδες που δέχονται την εγγραφή χρηστών και β) σε αυτούς που δημιουργούν ιστοσελίδες χωρίς αυτή τη δυνατότητα.
- Η πέμπτη ενότητα αναφέρεται μονάχα στους χρήστες της α) κατηγορίας και τους ρωτά κάποιες περαιτέρω ερωτήσεις όσον αφορά το user registration.
- Η έκτη ενότητα αναφέρεται σε όλους τους χρήστες και περιλαμβάνει ορισμένες γενικές ερωτήσεις που αφορούν την ασφάλεια.
- Η έβδομη ενότητα περιλαμβάνει ερωτήσεις όσον αφορά τις προσωπικές πληροφορίες των χρηστών.

3.3 Δείγμα Έρευνας

Το δείγμα της έρευνας προέρχεται από τις ομάδες του Facebook a) [WordPress Greek Community](#), b) [WordPress Developers](#), c) [Wordpress Experts](#), d) [WordPress Developers and Freelancers](#) και e) [WordPress Developer](#). Από τις ομάδες του LinkedIn a) [Freelancer Wordpress Developer](#), b) [Professional Web Designer and Developer or WordPress Expert Service](#), και c) [Web Developers, Magento, Wordpress, PHP, Frontend/Backend developer](#) και από προσωπικά post της ερευνήτριας στο Twitter που αναφέρονταν σε επαγγελματίες developers. Συνολικά συγκεντρώθηκαν απαντήσεις 56 επαγγελματιών.

3.4 Ερωτηματολόγιο

Ενότητα 1: Εισαγωγή

WordPress Security Assessment

Thank you for taking the time to participate in this study conducted by the Ionian University located in Corfu, Greece. Dr. Christoforos Dadoyan (dadoyan@ionio.gr), Assistant Professor of the Department of Informatics of the Ionian University is the head investigator in this research.

This typescript describes the purposes of this study and provides you with a description of your involvement as a participant. Please read it carefully.

This questionnaire was developed to gather feedback from developers who create websites using the CMS WordPress. The answers gathered will be used to draw conclusions about the level of security and quality of said websites so your honest and detailed answers will be highly appreciated. The questionnaire consists of 20 questions at most and its completion should take about 5 minutes. There are no right or wrong answers.

There will be no immediate or financial benefits from your participation in this research. However, through your participation you will significantly contribute to the analysis of how CMS WordPress developers secure their websites and how safe said websites are.

We inform you that your data will receive the proper and statutory protection. To achieve this:

- 1) We will collect and use the data of your answers only for the aforementioned purposes of the research. The storage-registration and the statistical processing of the data will be done according to the current legislation.
- 2) Your anonymity is preserved, as none of the stages of this investigation will ask for your name or email address.
- 3) The data of your answers will be accessible only by the research coordinator and the members of the research team.
- 4) Your participation in this research is completely voluntary. You can choose not to participate or if you choose to participate, you can stop and withdraw from the survey at any time you decide.

Thank you for your time and contribution.

Εικόνα 4

Ενότητα 2: Μέτρα Ασφαλείας

WordPress Security Assessment

 **walerilas@gmail.com** (δεν κοινοποιήθηκε)
[Εναλλαγή λογαριασμού](#)

* Απαιτείται

Security measures

Do you use an all-in-one Security plugin (e.g., Wordfence Security, Defender, iThemes Security, Sucuri, All In One WP Security and Firewall, Jetpack)? *

☐ Yes

☐ Not really, but i use a WAF from a Content Delivery Network (CDN) such as Cloudflare.

☐ No

[Πίσω](#)[Επόμενο](#)

Σελίδα 2 από 9

[Εκκαθάριση φόρμας](#)

Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

Αυτό το περιεχόμενο δεν έχει δημιουργηθεί και δεν έχει εγκριθεί από την Google. [Αναφορά κακής χρήσης - Όροι Παροχής Υπηρεσιών - Πολιτική απορρήτου](#)

Google Φόρμες

Εικόνα 5

Ενότητα 3: Ενίσχυση Ασφαλείας των WordPress Ιστοσελίδων

WordPress Security Assessment

 **walerilas@gmail.com** (δεν κοινοποιήθηκε)
Εναλλαγή λογαριασμού



* Απαιτείται

WordPress Security Hardening

Please choose which of the security measures mentioned below you use to secure your WordPress sites? *

- ☐ Keep regular backups
- ☐ Change Database Prefix (eg wp_admin, wp_login)
- ☐ Hide the WordPress or its version you are using (e.g., using Hide my WP plugin)
- ☐ Secure the wp-config file
- ☐ Disable Directory Indexing and Browsing
- ☐ Disable XMLRPC
- ☐ Relocate or rename administrator login page (e.g., <https://wordpress.org/plugins/wps-hide-login/>)
- ☐ Secure administrator login (e.g. use of CAPTCHA such as <https://wordpress.org/plugins/captchinoa-captcha-for-login-form-protection/>, or additional security questions).

Πίσω

Επόμενο

Σελίδα 3 από 9

Εκκαθάριση
φόρμας

Εικόνα 6

Ενότητα 4: Plugin Ασφαλείας

Security Plugins

Please choose which WordPress security plugins you use, if you use any.

- ☐ Wordfence Security
- ☐ iThemes Security
- ☐ Sucuri Security
- ☐ WP fail2ban
- ☐ All in One WP Security & Firewall
- ☐ Jetpack
- ☐ SecuPress
- ☐ BulletProof Security
- ☐ WPScan - Wordpress Security Scanner
- ☐ VaultPress
- ☐ Google Authenticator -Two Factor Authentication
- ☐ Security Ninja
- ☐ Defender
- ☐ Astra Web Security
- ☐ Shield Security
- ☐ WebARX
- ☐ Security & Malware Scan by Clean Talk
- ☐ MalCare Security
- ☐ miniOrange's Google Authenticator
- ☐ Cerber Security, Anti-spam & Security
- ☐ NinjaFirewall (WP Edition)

Εικόνα 7

When you want to install a WordPress plugin... *

- ☐ I simply install the plugin that has the functionality i am looking for.
- ☐ I check the ratings and number of downloads but almost always i install the plugin, regardless of the ratings.
- ☐ I check the ratings and number of downloads and if they are not satisfactory (i.e., very few number of downloads), i avoid installing it.
- ☐ I never install plugins

Please mention any additional security plugins you use that are missing from the list above.

Η απάντησή σας

Do you use a malware scanner plugin? *

- ☐ Yes
- ☐ No

Εικόνα 8

Ενότητα 5: Εγγραφή Χρηστών

WordPress Security Assessment

 **walerilas@gmail.com** (δεν κοινοποιήθηκε)
Εναλλαγή λογαριασμού 

* Απαιτείται

User registration

Do your WordPress websites (some or all) allow user registration creating their own passwords to login (e.g., an ecommerce website)? *

☐ Yes

☐ No

Πίσω

Επόμενο

Σελίδα 5 από 9

Εκκαθάριση
φόρμας

Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

Αυτό το περιεχόμενο δεν έχει δημιουργηθεί και δεν έχει εγκριθεί από την Google. [Αναφορά κακής χρήσης](#) - [Όροι Παροχής Υπηρεσιών](#) - [Πολιτική απορρήτου](#)

Google Φόρμες

Εικόνα 9

Ενότητα 6: Ασφάλεια Ιστοσελίδων που επιτρέπουν την είσοδο χρηστών (Απαντούν μόνο οι χρήστες που επέλεξαν “Ναι” στην προηγούμενη ενότητα.)

Registration website security

Please choose which of the security measures below you use to secure your user *
registration websites (e.g., an ecommerce website)?

☐ Allow two-factor authentication (2FA) (e.g., <https://wordpress.org/plugins/wp-2fa/>)

☐ Use of password policies for strong passwords creation for your users

☐ Limit the number of simultaneous login sessions per user.

☐ Limit the rate of login attempts (e.g., <https://wordpress.org/plugins/wps-limit-login/>)

☐ Blocklist / Blacklisting IP addresses.

Do you know the default WordPress hashing scheme of your users stored *
passwords?

☐ Yes and I have also changed the default passwords' hashing scheme to a stronger one.

☐ Yes and I have kept the default hashing scheme.

☐ No idea, I've never heard about it!

Πίσω

Επόμενο

Σελίδα 6 από 9

Εκκαθάριση
φόρμας

Εικόνα 10

Ενότητα 7: Γενικές Ερωτήσεις Ασφαλείας

Εικόνα 11

Generic Security Questions

Do you know whether your HTTPS WordPress websites use TLS 1.2 or TLS 1.3? *

☐ Yes

☐ No

☐ I do not use HTTPS for my WordPress websites (no use of certificates).

Do you know what is an XSS attack? *

☐ Yes

☐ No

How important do you think the security of your websites is? *

☐ Very important.

☐ So and so.

☐ Not so important.

Do you update your WordPress websites plugins regularly? *

☐ I skip the updates in general or install them in a future date

☐ I skip the updates in general, except for security updates which i install them immediately

☐ I install all updates (both functional and security), only when I find the time to test them and ensure that they do not break my website.

☐ I install all updates automatically without testing them.

[Πίσω](#)

[Επόμενο](#)

Σελίδα 7 από 9

[Εκκαθάριση
φόρμας](#)

Ενότητα 8: Προσωπικά Δεδομένα

Εικόνα 12

Personal Info

What is your gender (optional)?

☐ Male

☐ Female

☐ Non-binary

How old are you (optional)?

☐ Under 18 years old

☐ 18 - 29 years old

☐ 30 - 40 years old

☐ 41 - 50 years old

☐ Over 50 years old

You live in...(optional)

☐ Africa

☐ Asia

☐ Australia

☐ Europe

☐ USA

What is your relationship with IT? *

☐ I am majoring or I have a degree or a job in computer science, computer engineering, information technology or a related field.

☐ I work as web/software developer.

☐ I am just really interested in building websites using WordPress (self-taught).

What is your cyber security level of expertise? *

- ☐ I am majoring or I have a degree or a job as computer security/cybersecurity specialist.
- ☐ I have no prior security/cybersecurity related knowledge/experience.

Πίσω

Επόμενο

Σελίδα 8 από 9

Εκκαθάριση
φόρμας

Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

Αυτό το περιεχόμενο δεν έχει δημιουργηθεί και δεν έχει εγκριθεί από την Google. [Αναφορά κακής χρήσης](#) - [Όροι Παροχής Υπηρεσιών](#) - [Πολιτική απορρήτου](#)

Google Φόρμες

Ενότητα 9: Τέλος

WordPress Security Assessment

 **walerilas@gmail.com** (δεν κοινοποιήθηκε)
[Εναλλαγή λογαριασμού](#)

The End!

Thank you for your contribution!

Πίσω

Υποβολή

Σελίδα 9 από 9

Εκκαθάριση
φόρμας

Μην υποβάλετε ποτέ κωδικούς πρόσβασης μέσω των Φορμών Google.

Αυτό το περιεχόμενο δεν έχει δημιουργηθεί και δεν έχει εγκριθεί από την Google. [Αναφορά κακής χρήσης](#) - [Όροι Παροχής Υπηρεσιών](#) - [Πολιτική απορρήτου](#)

Google Φόρμες

Εικόνα 13

Κεφάλαιο 4: Αποτελέσματα Έρευνας και Συμπεράσματα

Σε αυτό το κεφάλαιο θα παρουσιαστούν τα αποτελέσματα που συγκεντρώθηκαν με τη χρήση ερωτηματολογίου με περιγραφική στατιστική.

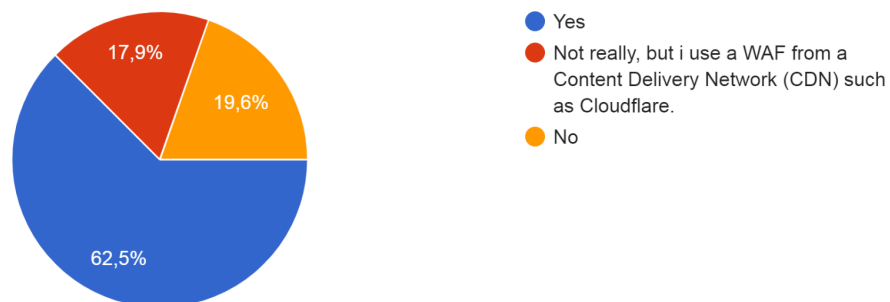
4.1 Ενότητα 1: Μέτρα Ασφαλείας

Χρησιμοποιείτε κάποιο all-in-one Security Plugin (WordFence Security, Defender, iThemes Security, Sucuri, All In One WP Security and Firewall, Jetpack);

Ξεκινώντας με τα μέτρα ασφαλείας, οι χρήστες ερωτήθηκαν αν προτιμούν να χρησιμοποιούν κάποιο plugin ασφαλείας που καλύπτει όλες τις πτυχές της ασφάλειας μιας ιστοσελίδας. Από τις τρεις διαθέσιμες απαντήσεις η πλειοψηφία των ερωτηθέντων με ποσοστό 62.5% απάντησε πως χρησιμοποιεί ένα plugin τέτοιου είδους. Ένα ποσοστό 19.6% απάντησε πως δε χρησιμοποιεί κάτι τέτοιο ενώ οι υπόλοιποι 17.9% απάντησαν ότι χρησιμοποιούν ένα WAF από ένα CDN όπως το Cloudflare.

Do you use an all-in-one Security plugin (e.g., Wordfence Security, Defender, iThemes Security, Sucuri, All In One WP Security and Firewall, Jetpack)?

56 απαντήσεις



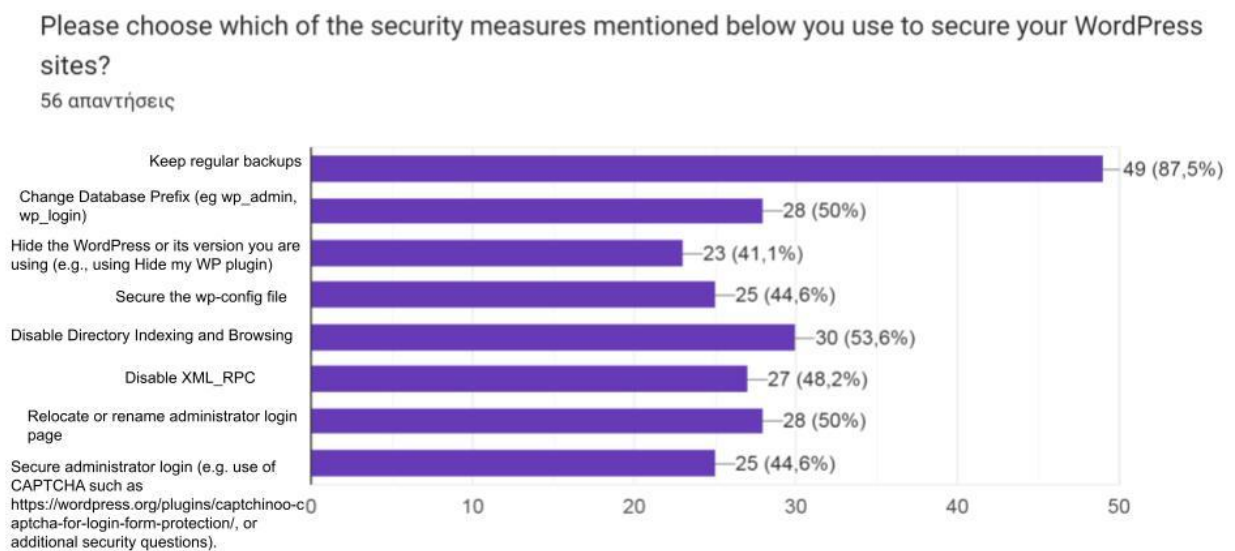
Εικόνα 14

Συμπέρασμα: Όπως βλέπουμε παραπάνω, η πλειοψηφία των προγραμματιστών του WordPress προτιμά να χρησιμοποιεί plugin ασφαλείας που καλύπτουν όλες τις πτυχές της ασφάλειας μιας ιστοσελίδας. Αυτή η ερώτηση δε μας μαρτυρά κάτι για το ποιόν των χρηστών καθώς η χρήση τέτοιου είδους plugin είναι επαρκής για την ασφάλεια των ιστοσελίδων. Σαφώς, τα site μπορούν να θωρακιστούν χειροκίνητα καθώς και με την εγκατάσταση πολλαπλών plugin που ασφαλίζουν διαφορετικούς τομείς των ιστοσελίδων ωστόσο κάτι τέτοιο φαίνεται πως δεν προτιμάται από τους χρήστες.

4.2 Ενότητα 2: Ενίσχυση Ασφαλείας των Ιστοσελίδων WordPress

Παρακαλώ επιλέξτε ποιά από τα μέτρα ασφαλείας που αναφέρονται παρακάτω χρησιμοποιείτε για να ασφαλίσετε τις ιστοσελίδες σας;

Η δεύτερη ενότητα απαρτίζεται από μία μονάχα ερώτηση που αφορά τους τρόπους με τους οποίους οι χρήστες επιλέγουν να ασφαλίσουν τις WordPress ιστοσελίδες τους. Πρώτη επιλογή για τους περισσότερους ερωτηθέντες με συγκέντρωση 49 ψήφων φαίνεται να έχει η χρήση regular backups, με την απενεργοποίηση της ευρετηρίασης και της περιήγησης καταλόγου να έρχεται στη δεύτερη θέση με 30 ψήφους. Στη συνέχεια με ισοβαθμία 28 ψήφων έχουμε την αλλαγή του database prefix και την μεταφορά και την μετονομασία της login σελίδας. 27 χρήστες επέλεξαν και την απενεργοποίηση του XML_RPC για την ενίσχυση της ασφάλειας της ιστοσελίδας τους και 25 χρήστες επέλεξαν να ασφαλίσουν το wp-config file και τον τρόπο σύνδεσης του διαχειριστή. Τέλος, 23 χρήστες επέλεξαν την απόκρυψη του ίδιου του WordPress ή της έκδοσης του που χρησιμοποιεί η ιστοσελίδα τους.



Εικόνα 15

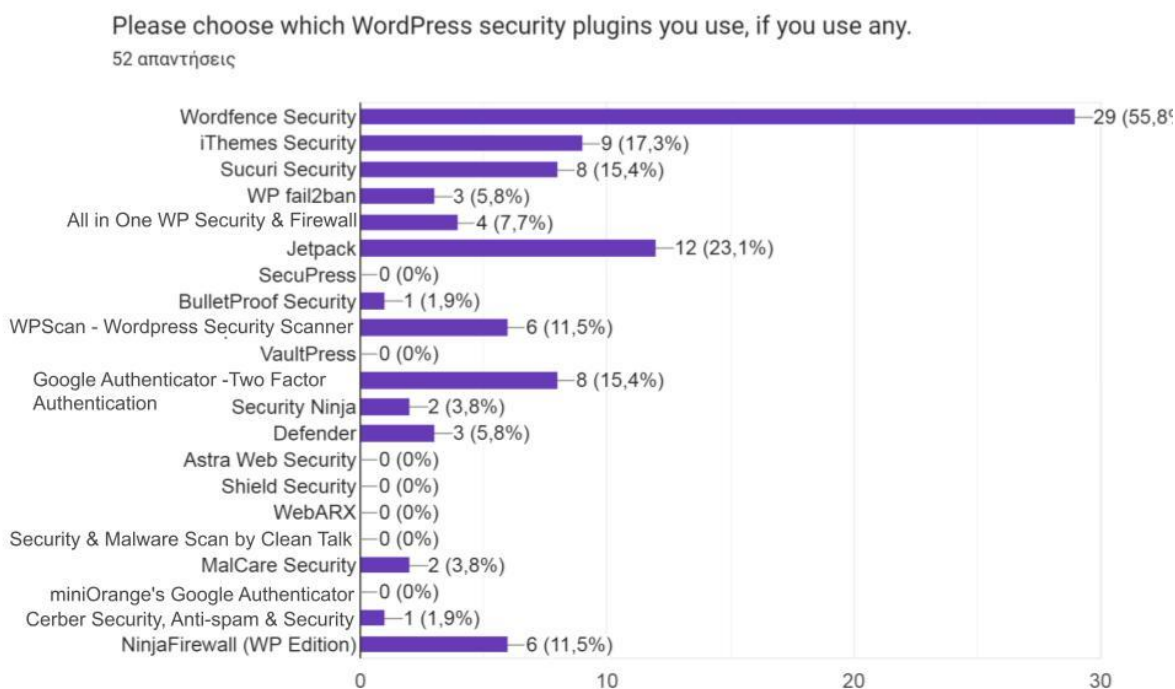
Συμπέρασμα: Σύμφωνα με τα αποτελέσματα που συγκεντρώθηκαν από την έρευνα, το πιο δημοφιλές μέτρο ασφαλείας είναι η χρήση των regular backups. Η δημοσιότητα αυτού του μέτρου ενδέχεται να οφείλεται στην απλότητα της εφαρμογή του, που τις περισσότερες φορές δεν απαιτεί καν τεχνικές γνώσεις ασφαλείας. Από την άλλη, οι μέθοδοι που συγκεντρώσαν τις λιγότερες ψήφους μπορούμε να υποθέσουμε πως απλά είναι λιγότερο διαδεδομένες στην προγραμματιστική κοινότητα. Πολλοί προγραμματιστές για παράδειγμα, όπως μπορούμε να δούμε και παραπάνω, φαίνεται πως δεν γνωρίζουν ότι η απόκρυψη της έκδοσης του site τους βοηθά στην διατήρηση της ασφάλειας του.

4.3 Ενότητα 3: Security Plugins

Σε αυτή την ενότητα οι συμμετέχοντες κλήθηκαν να απαντήσουν ερωτήσεις σχετικά με τα plugin ασφαλείας που χρησιμοποιούν.

Ερώτηση 1 : Παρακαλώ επιλέξτε ποιά από τα παρακάτω Security Plugin χρησιμοποιείτε, αν όντως χρησιμοποιείτε κάποιο από αυτά.

Αρχικά οι συμμετέχοντες ερωτήθηκαν ποιά από τα παρακάτω plugin επιλέγουν για να ασφαλίσουν τις ιστοσελίδες τους. Το πιο δημοφιλές πρόσθετο φαίνεται πως είναι το Wordfence Security το οποίο συγκέντρωσε 29 ψήφους με ποσοστό χρηστών 55.89%. Ακολουθείτε από το Jetpack με 12 ψήφους και ποσοστό 23.1%, το iThemes Security με 9 ψήφους και ποσοστό 17.3%, το Sucuri Security και το Google Authenticator με 8 ψήφους έκαστο και ποσοστό 15.4%, το NinjaFirewall με 6 ψήφους και ποσοστό 11.5%, το All in One WP Security & Firewall με 4 ψήφους και ποσοστό 7.7%, τα WP fail2ban και Defender με 3 ψήφους έκαστο και ποσοστό 5.8%, τα Security Ninja και MalCare Security με 2 ψήφους έκαστο και ποσοστό 3.8% και τέλος τα BulletProof Security και Cerber Security με 1 ψήφο έκαστο και ποσοστό 1.9%. Τα Security plugins που δεν έλαβαν καθόλου ψήφους στην έρευνα είναι τα: SucuPress, VaultPress, Astra Web Security, Shield Security, WebARX, Security & Malware Scan by Clean talk και το miniOranges's Google Authenticator.



Εικόνα 16

Συμπέρασμα: Όπως ήταν αναμενόμενο, το Wordfence Security συγκέντρωσε τις περισσότερες ψήφους στην συγκεκριμένη ερώτηση. Το συγκεκριμένο plugin είναι ιδιαίτερα δημοφιλές στα πλαίσια της προγραμματιστικής κοινότητας καθώς συγκεντρώνει περίπου 4 εκατομμύρια χρήστες και το σημαντικότερο, παρέχει τα περισσότερα χαρακτηριστικά του δωρεάν.^[65] Αρκετές ψήφους συγκέντρωσε και το Jetpack, που συγκεντρώνει περισσότερα από 5 εκατομμύρια downloads παγκοσμίως.^[66] Ωστόσο, το συγκεκριμένο plugin διαθέτει μόνο τη βασική προστασία των ιστοσελίδων δωρεάν, γεγονός που ενδεχομένως μαρτυρά το λόγο που λιγότεροι χρήστες το επέλεξαν. Περίεργο είναι το γεγονός πως το Shield Security

δεν συγκέντρωσε κανέναν ψήφο μιας και είναι αρκετά δημοφιλές στην WordPress κοινότητα και επιπρόσθετα διατίθεται δωρεάν[67].

Ερώτηση 2: Παρακαλώ αναφέρετε επιπλέον Security Plugins που χρησιμοποιείτε τα οποία λείπουν από την παραπάνω λίστα.

Προκειμένου να δημιουργήσουμε μια γενική εικόνα της χρήσης των προσθέτων ασφαλείας προστέθηκε μία ερώτηση που προέτρεπε τους χρήστες να προσθέσουν επιπλέον plugin που χρησιμοποιούν αλλά δεν υπάρχουν στη λίστα που δημιουργήθηκε. Από την ερώτηση αυτή συγκεντρώσαμε τα plugin WPMEUDEV, UpdraftPlus και Akeeba Admin Tools με 1 ψήφο έκαστο. Επίσης, είχαμε έναν χρήστη που χρησιμοποιεί custom WAF, modsecurity και VPN για τον administrator, έναν που απάντησε πως όλα τα sites που δημιουργούνται από την ομάδα του έχουν τα δικά τους dedicated servers με ένα ποσοστό μικρότερο του 5% να φιλοξενούνται κάπου αλλού και τέλος έναν που απάντησε πως δε χρησιμοποιεί plugins για να ασφαλίσει τα site του και αν αμυνθεί από malware και πρόσθεσε πως η ασφάλεια πρέπει να εφαρμόζεται στο web server layer.

Απάντηση
All our sites are on our own dedicated servers (I would say less than 5% are hosted somewhere else)
WPMEUDEV
UpdraftPlus
Not using plugins for security / malware, security should be applied on the web server layer
custom WAF, modsecurity, VPN for administrator
Akeeba Admin Tools

Εικόνα 17

Ερώτηση 3: Όταν θέλετε να εγκαταστήσετε ένα WordPress plugin...

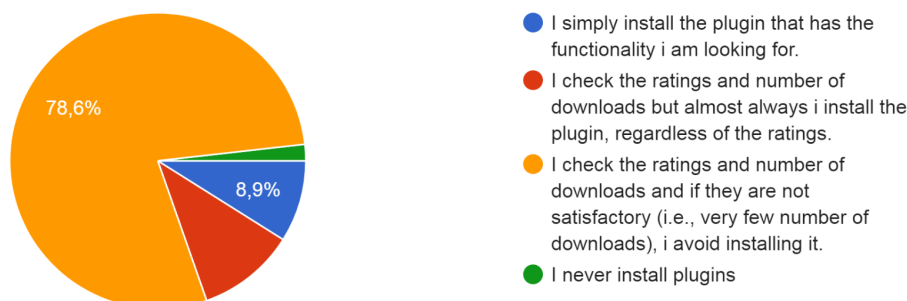
Στο δεύτερο διάγραμμα αυτής της ενότητας οι ερωτηθέντες κλήθηκαν να επιλέξουν τον τρόπο που προτιμούν να εγκαθιστούν τα WordPress plugins τους. Υπήρχαν τέσσερις πιθανές απαντήσεις από τις οποίες οι περισσότεροι, 44 άτομα με ποσοστό 78.6%, επέλεξαν την εγκατάσταση αφοτου πρώτα έχουν ελέγξει τις βαθμολογίες και τις λήψεις των προσθέτων και αποφεύγουν να τα κατεβάσουν αν αυτές δεν είναι ικανοποιητικές. 6 άτομα, δηλαδή ένα ποσοστό 10.7%, απάντησαν πως ελέγχουν τις βαθμολογίες και τις λήψεις των προσθέτων που θέλουν να εγκαταστήσουν ωστόσο κάνουν τη λήψη ανεξαρτήτως του αποτελέσματος και 5 άτομα, δηλαδή ποσοστό 8.9% απάντησαν πως απλά εγκαθιστούν το πρόσθετο που παρέχει

τη λειτουργικότητα που επιζητούν. Τέλος, ένα μόνο άτομο απάντησε πως ποτέ δεν εγκαθιστά plugin.

Εικόνα 18

When you want to install a WordPress plugin...

56 απαντήσεις



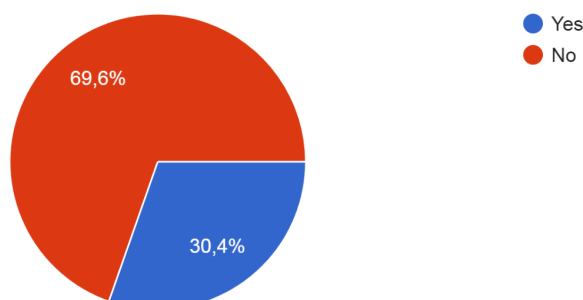
Συμπέρασμα: Ελπιδοφόρο είναι το γεγονός πως ένα ποσοστό των χρηστών του WordPress που πλησιάζει το 80% εγκαθιστούν τα πρόσθετα που τους ενδιαφέρουν αφού πρώτα έχουν ελέγξει τις βαθμολογίες και τις λήψεις τους και αποφεύγουν να τα κατεβάσουν αν αυτές δεν είναι ικανοποιητικές. Ένα μικρό ποσοστό, 8.9%, των χρηστών απάντησαν πως απλά εγκαθιστούν το πρόσθετο που παρέχει τη λειτουργικότητα που επιζητούν, μία τακτική που όπως καταλαβαίνουμε είναι ιδιαίτερα επικίνδυνη για οποιονδήποτε διαχειρίζεται μια ιστοσελίδα. Όπως έχει αναφερθεί και παραπάνω, τα plugin που δεν έχουν ελεγχθεί και δεν παρέχονται από αξιόπιστους φορείς μπορούν να αποτελέσουν κίνδυνο για την ασφάλεια των site μας.

Ερώτηση 4: Χρησιμοποιείτε κάποιο malware scanner plugin;

Η επόμενη ερώτηση αυτής της ενότητας ρωτά τους developers αν χρησιμοποιούν κάποιο malware scanner plugin. 39 άτομα με ποσοστό 69.6% απάντησαν πως δε χρησιμοποιούν κάτι τέτοιο ενώ τα υπόλοιπα 17 με ποσοστό 30.4% απάντησαν πως χρησιμοποιούν.

Do you use a malware scanner plugin?

56 απαντήσεις



Εικόνα 19

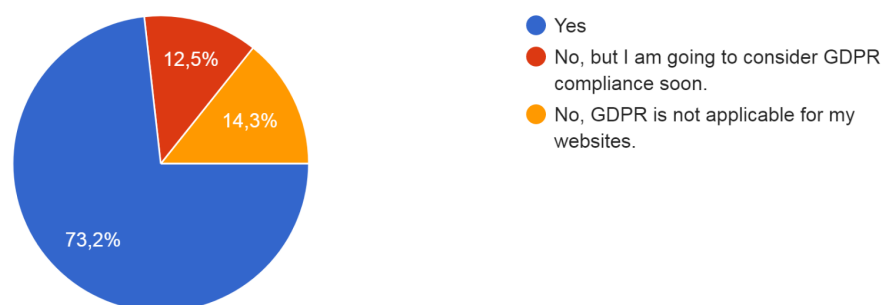
Συμπέρασμα: Το τόσο μεγάλο ποσοστό προγραμματιστών που απάντησαν όχι σε αυτήν την ερώτηση εξηγείται με δύο πιθανούς τρόπους. Αρχικά, υπάρχει το ενδεχόμενο κακής πρακτικής. Με λίγα λόγια οι χρήστες θα έπρεπε να χρησιμοποιούν κάποιο malware scanner plugin και απλώς δεν το κάνουν. Ωστόσο, κάτι τέτοιο αντιτίθεται στις απαντήσεις που συγκεντρώσαμε στην πρώτη ερώτηση του ερωτηματολογίου όπου ένα ποσοστό που πλησιάζει το 63% απάντησε πως χρησιμοποιεί κάποιο all-in-one plugin. Τα plugin αυτού του είδους, όπως μπορούμε να υποθέσουμε, πολλές φορές περιλαμβάνουν εξ αρχής ενσωματωμένα malware scanner οπότε αρκετοί από τους χρήστες που απάντησαν πως δεν χρησιμοποιούν κάτι τέτοιο, στην πραγματικότητα το κάνουν εν άγνοια τους.

Ερώτηση 5: Έχετε λάβει κατάλληλα μέτρα προκειμένου να εξασφαλίσετε την συμμόρφωση με το GDPR (χρησιμοποιώντας π.χ. ένα plugin όπως το GDPR Cookie Compliance);

Στη συνέχεια οι προγραμματιστές ερωτήθηκαν αν παίρνουν τα κατάλληλα μέτρα για να εξασφαλίσουν την συμμόρφωση με το GDPR (χρησιμοποιώντας π.χ. ένα plugin όπως το GDPR Cookie Compliance). 41 άτομα με ποσοστό 73.2% απάντησαν πως χρησιμοποιούν κάτι τέτοιο, 7 άτομα με ποσοστό 12.5% απάντησαν πως δεν παίρνουν τέτοιου είδους μέτρα ωστόσο σκέφτονται σοβαρά την συμμόρφωση με το GDPR στο μέλλον ενώ 8 άτομα με ποσοστό 14.3% απάντησαν πως το GDPR δεν είναι εφαρμόσιμο στα site τους.

Do you take appropriate measures to ensure GDPR compliance (e.g., through a plugin such as <https://wordpress.org/plugins/gdpr-cookie-compliance/>)?

56 απαντήσεις



Εικόνα 20

Συμπέρασμα: Από ότι φαίνεται τα περισσότερα site που δημιουργούνται την σήμερα κατανοούν την σημασία του GDPR και την σπουδαιότητα του να συμμορφώνονται βάση αυτού. Σύμφωνα με την έρευνα μας ακόμα και άτομα που ακόμα δεν έχουν συμμορφωθεί καταγγίζουν πως αργά ή γρήγορα η εφαρμογή του είναι αναπόφευκτη. Παρόλα αυτά, είναι σημαντικό να αναφέρουμε πως το 14.3% που αρνείται ακόμα και να σκεφτεί να συμμορφωθεί βάση του πρωτοκόλλου είναι ένα αρκετά μεγάλο ποσοστό και αποτελεί

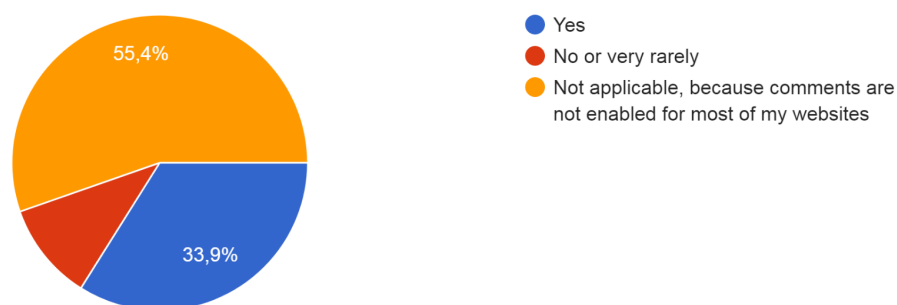
κίνδυνο για την προστασία των δεδομένων των χρηστών.

Ερώτηση 6: Αν τα σχόλια είναι ενεργοποιημένα στην ιστοσελίδα σας, χρησιμοποιείτε κάποιο plugin για να εμποδίσετε τα spam;

Η τελευταία ερώτηση αυτής της ενότητας αφορά την χρήση των comments στις ιστοσελίδες των προγραμματιστών. Οι ερωτηθέντες κλήθηκαν να απαντήσουν αν έχουν ενεργά τα σχόλια στις ιστοσελίδες τους, και αν ναι, αν χρησιμοποιούν πρόσθετα για να εμποδίσουν τα spam που λαμβάνουν τα sites. 31 άτομα με ποσοστό 55.4% απάντησαν πως κάτι τέτοιο δεν είναι εφαρμόσιμο στα sites τους καθώς τα σχόλια είναι απενεργοποιημένα για τις περισσότερες ιστοσελίδες που δημιουργούν. 19 άτομα με ποσοστό 33.9% απάντησαν πως χρησιμοποιούν τέτοιου είδους plugin ενώ 6 άτομα με ποσοστό 10.7% απάντησαν πως δε χρησιμοποιούν κάτι τέτοιο και αν ναι τότε χρησιμοποιούν τα πρόσθετα πολύ σπάνια.

If comments are enabled on your websites, do you use plugins to block spam?

56 απαντήσεις



Εικόνα 21

Συμπέρασμα: Με μια πρώτη ματιά το ποσοστό 55.4% των χρηστών που απάντησαν πως δε χρησιμοποιούν κάποιο plugin για να αποτρέψουν τα σπαμ καθώς η ιστοσελίδα τους δεν επιτρέπει το σχολιασμό, μπορεί να φαίνεται αρκετά θετικό όσον αφορά την ασφάλεια των site. Ωστόσο, αυτό δεν σημαίνει πως οι προγραμματιστές που εφαρμόζουν κάτι τέτοιο γνωρίζουν τους κινδύνους που επιφέρει η δυνατότητα σχολιασμού. Με λίγα λόγια, τα σχόλια τις περισσότερες φορές είναι απενεργοποιημένα επειδή δε χρειάζονται και όχι για κάποιο λόγο που σχετίζεται με την ασφάλεια. Από την άλλη, έχουμε ένα ποσοστό που πλησιάζει το 34% που επιτρέπει το σχολιασμό των ιστοσελίδων του και χρησιμοποιεί τέτοιου είδους πρόσθετα ασφαλείας. Μπορεί το ποσοστό αυτό να φαίνεται επαρκές μιας και η πλειοψηφία των προγραμματιστών που συμμετείχαν σε αυτή την έρευνα δεν επιτρέπουν την ύπαρξη των σχολίων στις σελίδες τους παρόλα αυτά, ιδανικά, θα θέλαμε περισσότερα άτομα να απαντήσουν “Ναι” σε αυτό το ερώτημα.

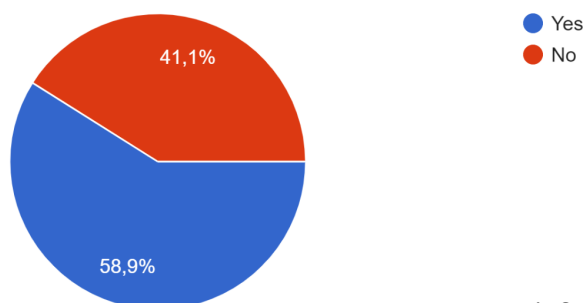
4.4. Ενότητα 4: Εγγραφή Χρηστών

Επιτρέπουν τα WordPress sites σας (μερικά ή όλα) την εγγραφή χρηστών με τη δημιουργία δικών τους κωδικών ασφαλείας προκειμένου να συνδεθούν στην ιστοσελίδα τους (για παράδειγμα ένα e-commerce site);

Η συγκεκριμένη ενότητα περιλαμβάνει μόνο μία ερώτηση η οποία διαχωρίζει τους ερωτηθέντες σε δύο κατηγορίες, αυτούς που δημιουργούν ιστοσελίδες που επιτρέπουν την εγγραφή χρηστών, και αυτούς που δεν επιτρέπουν την είσοδο χρηστών στα sites τους. Ο διαχωρισμός αυτός μας επέτρεψε να ρωτήσουμε πιο εξειδικευμένες ερωτήσεις τους χρήστες που επιτρέπουν το login. Από τα 56 άτομα, 23, με ποσοστό 41.1% απάντησαν ότι δεν επιτρέπουν την είσοδο χρηστών στις ιστοσελίδες που κατασκευάζουν ενώ οι υπόλοιποι 33, με ποσοστό 58.9% απάντησαν πως υπάρχει δυνατότητα login στα site τους.

Do your WordPress websites (some or all) allow user registration creating their own passwords to login (e.g., an ecommerce website)?

56 απαντήσεις



Εικόνα 22

Συμπέρασμα: Όπως παρατηρούμε παραπάνω οι ιστοσελίδες που επιτρέπουν την εγγραφή χρηστών είναι πιο δημοφιλείς από αυτές που δεν επιτρέπουν κάτι τέτοιο ανάμεσα στους προγραμματιστές του WordPress.

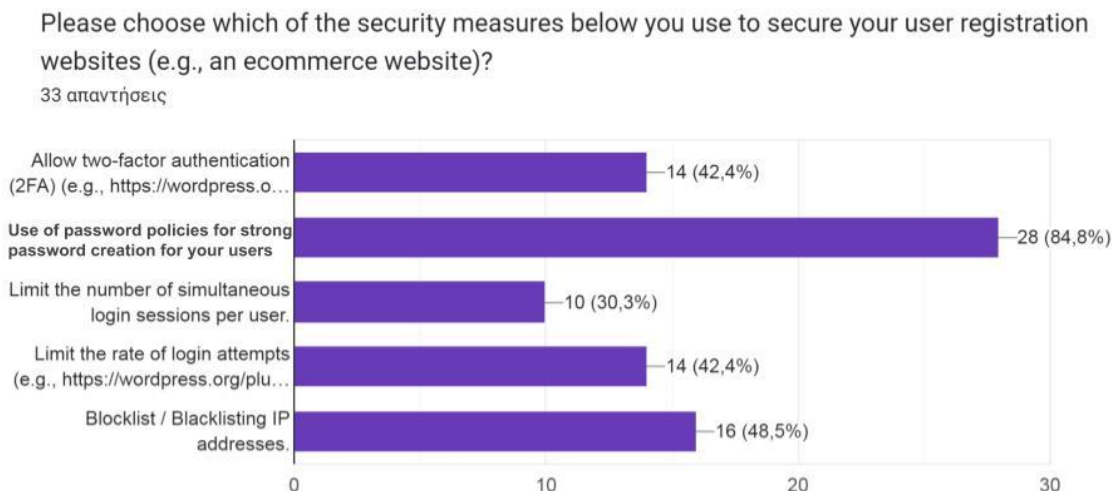
4.5 Ενότητα 5: Ασφάλεια Ιστοσελίδων που επιτρέπουν την είσοδο χρηστών

Η ενότητα αυτή απευθύνεται μόνο στους 33 προγραμματιστές που απάντησαν πως επιτρέπουν την σύνδεση χρηστών στις ιστοσελίδες τους και περιέχει δύο ερωτήσεις.

Ερώτηση 1: Παρακαλώ επιλέξτε ποιά από τα μέτρα ασφαλείας παρακάτω χρησιμοποιείτε για να ασφαλίσετε τις ιστοσελίδες σας που επιτρέπουν την εγγραφή και είσοδο των χρηστών.

Η πρώτη ερώτηση αφορά τους τρόπους ασφάλισης των ιστοσελίδων που επιτρέπουν την εγγραφή χρηστών (π.χ. τις ιστοσελίδες ecommerce). Η χρήση πολιτικών για την εξασφάλιση ισχυρών κωδικών πρόσβασης των χρηστών φαίνεται να είναι ο πιο δημοφιλής τρόπος ασφάλισης με 28 χρήστες σε ποσοστό 84.8% να τον επιλέγουν. Στη δεύτερη θέση είναι το blocklisting ή blacklisting συγκεκριμένων διευθύνσεων IP με 16 χρήστες σε ποσοστό 48.5% να το επιλέγουν. Στην συνέχεια, ακολουθούν η χρήση του two-factor authentication και ο περιορισμός των προσπαθειών login των χρηστών με 14 χρήστες να τα επιλέγουν με

ποσοστό 42.4%. Τέλος, 10 χρήστες με ποσοστό 30.3% επέλεξαν και τον περιορισμό του αριθμού των ταυτόχρονων συνδέσεων από τον ίδιο χρήστη.



Εικόνα 23

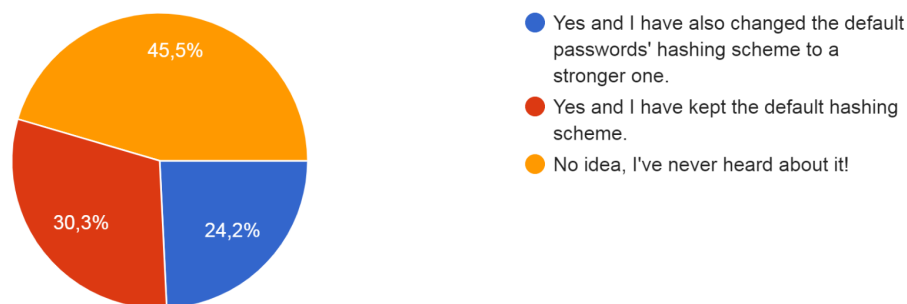
Συμπέρασμα: Όπως μπορούμε να δούμε από τα αποτελέσματα της έρευνας το πιο δημοφιλές μέτρο ασφαλείας ανάμεσα στους προγραμματιστές του WordPress, με ποσοστό που πλησιάζει το 85% είναι η χρήση πολιτικών για την εξασφάλιση ισχυρών κωδικών πρόσβασης των χρηστών. Η δημοτικότητα αυτού του μέτρου πιθανότητα να οφείλεται στην εύκολη εφαρμογή του καθώς και στην ενημέρωση που υπάρχει την σήμερα όσον αφορά την σπουδαιότητα των ισχυρών κωδικών ασφαλείας. Μπορούμε να πούμε ότι οι επόμενοι τρεις τρόποι ασφάλισης αυτού του είδους των ιστοσελίδων είναι εξίσου δημοφιλείς μιας και συγκεντρώνουν περίπου το ίδιο αριθμό ψήφων. Το λιγότερο δημοφιλές μέτρο με μόνο 10 ψήφους φαίνεται πως είναι ο περιορισμός του αριθμού των ταυτόχρονων συνδέσεων από τον ίδιο χρήστη.

Ερώτηση 2: Γνωρίζετε ποιά είναι το προεπιλεγμένο WordPress hashing scheme των αποθηκευμένων κωδικών των χρηστών σας;

Η δεύτερη ερώτηση αφορά το hashing scheme των κωδικών πρόσβασης των χρηστών των ιστοσελίδων. Στην ερώτηση αν οι ίδιοι οι προγραμματιστές γνωρίζουν το default hashing scheme των χρηστών των ιστοσελίδων τους, 15 άτομα με ένα ποσοστό 45.5% απάντησαν πως δεν έχουν ιδέα και δεν έχουν ακούσει ποτέ κάτι παρόμοιο, 10 άτομα με ποσοστό 30.3% απάντησαν πως ξέρουν το hashing scheme καθώς έχουν επιλέξει το default και τέλος, 8 άτομα με ποσοστό 24.2% απάντησαν πως το γνωρίζουν και έχουν αλλάξει το default hashing scheme σε κάτι πιο ισχυρό.

Do you know the default WordPress hashing scheme of your users stored passwords?

33 απαντήσεις



Εικόνα 24

Συμπέρασμα: Τα αποτελέσματα που συγκεντρώσαμε σε αυτήν την ερώτηση μαρτυρούν ότι περίπου οι μισοί προγραμματιστές διαδικτύου που συμμετείχαν στην έρευνα μας δε γνωρίζουν καν την ύπαρξη του hashing scheme ως ευρύτερη έννοια. Σαφώς, κάτι τέτοιο είναι ιδιαίτερα ανησυχητικό μιας και άτομα που ασχολούνται με τη δημιουργία ιστοσελίδων είναι σημαντικό να είναι ενήμερα για οποιονδήποτε όρο σχετίζεται με το κλάδο. Το 30.3% που απάντησε πως γνωρίζει την ύπαρξη της έννοιας αλλά δεν έχει αλλάξει το default hashing scheme μπορεί να μοιάζει αρκετά ενημερωμένο ωστόσο κάτι τέτοιο δεν υφίσταται. Γενικότερα, προτιμάται η αλλαγή του hashing scheme για την εξασφάλιση της απόλυτης ασφάλειας. Το 24.2% των χρηστών που απάντησαν πως ακολουθούν μια τέτοια τακτική λοιπόν, είναι αυτό που είναι επαρκώς ενημερωμένο για την κατάσταση ασφαλείας όσον αφορά τα hash.

4.6 Ενότητα 6: Γενικές Ερωτήσεις Ασφαλείας

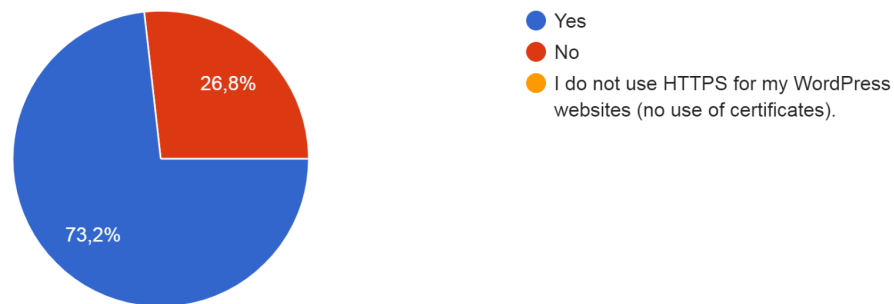
Η ενότητα αυτή περιλαμβάνει 4 γενικές ερωτήσεις ασφαλείας που αφορούν και τους 56 προγραμματιστές που πήραν μέρος στην έρευνα.

Ερώτηση 1: Γνωρίζετε αν η HTTPS WordPress ιστοσελίδα σας χρησιμοποιεί TLS 1.2 ή TLS 1.3;

Αρχικά, οι συμμετέχοντες ερωτήθηκαν αν το HTTPS WordPress site τους χρησιμοποιεί TLS 1.2 ή TLS 1.3. 41 χρήστες με ποσοστό 73.2% απάντησαν πως χρησιμοποιούν κάποιο από αυτά τα δύο ενώ 15 άτομα, με ποσοστό 26.8% απάντησαν πως δεν χρησιμοποιούν κανένα από τα δύο. Η επιλογή της μη χρήσης HTTPS για τις Wordpress ιστοσελίδες τους δεν συγκέντρωσε κανέναν ψήφο.

Do you know whether your HTTPS WordPress websites use TLS 1.2 or TLS 1.3?

56 απαντήσεις



Εικόνα 25

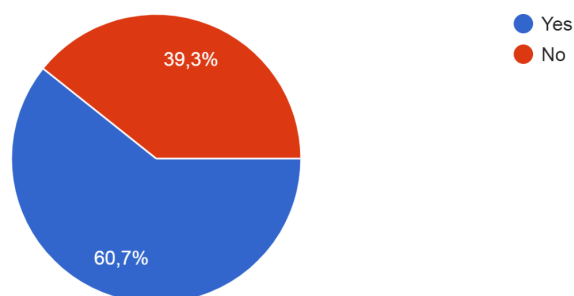
Συμπέρασμα: Θετικό είναι το γεγονός πως ένα ποσοστό που πλησιάζει το 73.2% γνωρίζει αν οι HTTPS ιστοσελίδες του χρησιμοποιούν TLS 1.2 ή TLS 1.3. Γενικότερα, η χρήση του συγκεκριμένου πρωτοκόλλου προτιμάται στην προγραμματιστική κοινότητα επομένως οι χρήστες που απάντησαν πως δε γνωρίζουν ποιο TLS χρησιμοποιεί θα ήταν σοφό να ενημερωθούν για τη λειτουργία του.

Ερώτηση 2: Γνωρίζετε τι είναι μια επίθεση XSS;

Η δεύτερη ερώτηση καλεί τους προγραμματιστές να απαντήσουν αν γνωρίζουν τι είναι μία επίθεση XSS. 34 από αυτούς, με ποσοστό 60.7%, απάντησαν πως γνωρίζουν για την επίθεση ενώ οι υπόλοιποι 22, με ποσοστό 39.3%, απάντησαν πως δε γνωρίζουν τι προϋποθέτει μια τέτοια επίθεση.

Do you know what is an XSS attack?

56 απαντήσεις



Εικόνα 26

Συμπέρασμα: Το αποτέλεσμα που συγκεντρώσαμε είναι οριακά ανησυχητικό καθώς ένα ποσοστό που πλησιάζει το 40% δε γνωρίζει την ύπαρξη των επιθέσεων XSS. Όπως αναφέρθηκε και παραπάνω, οι επιθέσεις XSS είναι ο πιο συνηθισμένος τρόπος να

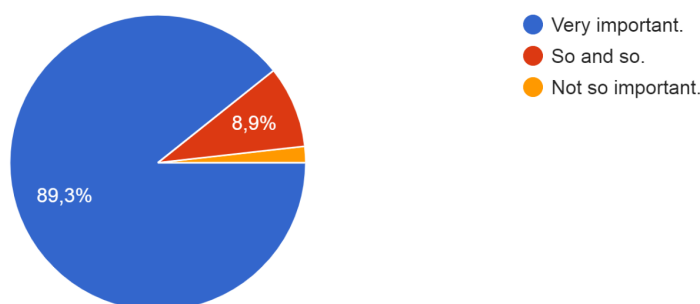
παραβιαστούν οι WordPress ιστοσελίδες καθώς πολλά plugin της πλατφόρμας περιέχουν τέτοιου είδους ευπάθειες. Επομένως, η άγνοια ενός τόσο μεγάλου ποσοστού των προγραμματιστών αποτελεί σοβαρό κίνδυνο.

Ερώτηση 3: Πόσο σημαντική θεωρείτε πως είναι η ασφάλεια της ιστοσελίδας σας;

Σε αυτήν την ερώτηση οι συμμετέχοντες καλούνται να απαντήσουν πόσο σημαντική θεωρούν πως είναι η ασφάλεια των ιστοσελίδων τους. 50 άτομα, με ποσοστό 89.3% απάντησαν πως η ασφάλεια των site τους είναι πολύ σημαντική, 5 απάντησαν πως είναι έτσι και έτσι, ενώ, ένα άτομο απάντησε πως δεν είναι σημαντική.

How important do you think the security of your websites is?

56 απαντήσεις



Εικόνα 27

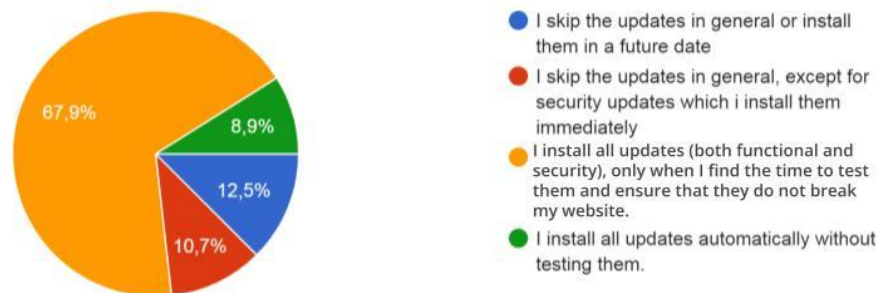
Συμπέρασμα: Είναι ιδιαίτερα ελπιδοφόρο το γεγονός πως ένα ποσοστό που πλησιάζει το 90% θεωρεί πως η ασφάλεια των ιστοσελίδων είναι ιδιαίτερα σημαντική. Αυτό μας δείχνει πως όλο και περισσότεροι προγραμματιστές ιστοσελίδων ξεκινούν να συνειδητοποιούν πως η ασφάλεια των ιστοσελίδων είναι υψίστης σημασίας με αποτέλεσμα να κινητοποιηθούν για να την εξασφαλίσουν.

Ερώτηση 4: Πόσο συχνά ενημερώνετε τα WordPress plugin σας;

Τέλος, οι προγραμματιστές καλούνται να απαντήσουν αν ενημερώνουν τα plugin της ιστοσελίδας τους αρκετά συχνά. 38 άτομα, με ποσοστό 67.9%, απάντησαν πως εγκαθιστούν όλες τις αναβαθμίσεις είτε για ασφάλεια είτε για λειτουργικότητα μόνο όταν βρίσκουν χρόνο να τις δοκιμάσουν για να μην πέσει η ιστοσελίδα τους. 7 άτομα, με ποσοστό 12.5% απάντησαν πως αποφεύγουν τα updates γενικότερα και τα εγκαθιστούν κάποια άλλη στιγμή και 6 άτομα, με ποσοστό 10.7%, απάντησαν πως αποφεύγουν τις ενημερώσεις γενικότερα, εκτός αν πρόκειται για ενημερώσεις ασφαλείας τις οποίες και πραγματοποιούν απευθείας. Τέλος, 5 άτομα με ποσοστό 8.9% απάντησαν πως εγκαθιστούν όλες τις ενημερώσεις αυτόματα χωρίς να τις δοκιμάσουν.

Do you update your WordPress websites plugins regularly?

56 απαντήσεις



Εικόνα 28

Συμπέρασμα: Είναι ιδιαίτερα ελπιδοφόρο το γεγονός πως ένα ποσοστό προγραμματιστών που πλησιάζει το 70% δεν εγκαθιστά τις ενημερώσεις των plugin τους πριν τις τεστάρει προκειμένου να προστατεύσει τις ιστοσελίδες του. Το ποσοστό 12.5% που αποφεύγει τις ενημερώσεις ή τις εγκαθιστά κάποια στιγμή στο μέλλον καθώς και το ποσοστό 8.9% που εγκαθιστά τα πάντα χωρίς να τα τεστάρει βρίσκονται στις δύο άκρες τις κλίμακας. Η αποφυγή ή μεγάλη καθυστέρηση εγκατάστασης των ενημερώσεων των προσθέτων ασφαλείας αποτελεί μεγάλο κίνδυνο καθώς τα plugin πολλές φορές περιέχουν ευπάθειες τις οποίες εκμεταλλεύονται οι επιτιθέμενοι. Οι ενημερώσεις περιέχουν τις περισσότερες φορές λύσεις σε αυτά τα προβλήματα που θωρακίζουν ακόμα περισσότερο τις ιστοσελίδες των χρηστών. Από την άλλη, η άλογη εγκατάσταση ενημερώσεων των προσθέτων χωρίς καμία απολύτως δοκιμή αποτελεί μια εξίσου σημαντική απειλή καθώς υπάρχει περίπτωση η νέα έκδοση τους να περιέχει κακόβουλο κώδικα. Ο κίνδυνος αυτός γίνεται ακόμα πιο αισθητός όταν τα plugin που χρησιμοποιούνται στην ιστοσελίδα δεν παρέχονται από αξιόπιστους φορείς. Το 10.7% που εγκαθιστά αμέσως αναβαθμίσεις μόνο όταν πρόκειται για security plugin ενώ αποφεύγει τις υπόλοιπες φαίνεται πως δε γνωρίζει ότι τα πιο επικίνδυνα plugins δεν είναι απαραίτητα αυτά που ασχολούνται με την ασφάλεια των ιστοσελίδων. Αντιθέτως, πρόσθετα όπως το Yoast SEO, το Woocommerce και το SEOPress που δεν είναι σχετικά με την ασφάλεια των ιστοσελίδων βρίσκονται συχνά στο στόχαστρο επιθέσεων λόγω της δημοτικότητας τους. Τις περισσότερες φορές, οι ευπάθειες που εμφανίζονται σε όλων των ειδών τα plugin εντοπίζονται από τους δημιουργούς τους, με αποτέλεσμα να αντιμετωπίζονται εν τέλει με μία απλή ενημέρωση. Όπως καταλαβαίνουμε λοιπόν, η αναβάθμιση μόνο των προσθέτων ασφαλείας δεν είναι μία σοφή λύση για την εξασφάλιση της ασφάλειας της ιστοσελίδας μας.

4.7 Ενότητα 7: Προσωπικά Δεδομένα

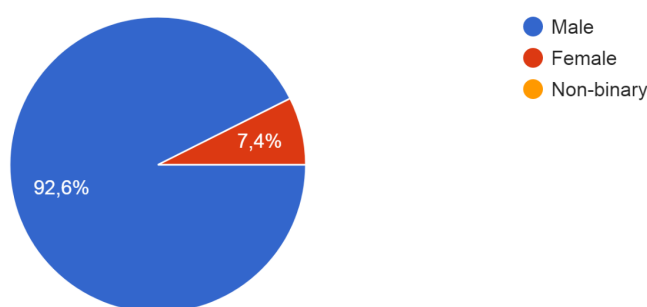
Η τελευταία ενότητα της έρευνας που περιέχει ερωτήματα (η πρώτη και τελευταία ενότητα της φόρμας περιέχουν την εισαγωγή και ευχαριστίες), αφορά την συμπλήρωση των προσωπικών δεδομένων όλων των συμμετεχόντων της έρευνας.

Ερώτηση 1: Ποιό είναι το φύλο σας;

Η πρώτη ερώτηση αφορά το γένος των ερωτηθέντων. Η ερώτηση αυτή δεν ήταν υποχρεωτική επομένως 54 από τα 56 άτομα την απάντησαν. Από τους 54, 50 συμμετέχοντες, με ποσοστό 92.6%, απάντησαν πως είναι άντρες ενώ οι υπόλοιποι 4 απάντησαν πως ανήκουν στο γυναικείο φύλο. Η τρίτη επιλογή που προστέθηκε, το μη-δυναδικό φύλο, δεν συγκέντρωσε κανέναν ψήφο.

What is your gender (optional)?

54 απαντήσεις



Εικόνα 29

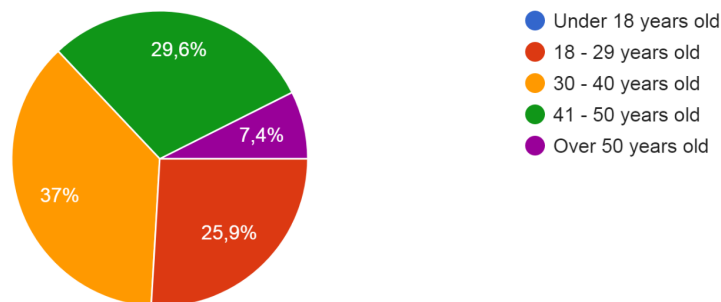
Συμπέρασμα: Όπως ήταν αναμενόμενο η πλειονότητα των προγραμματιστών ανήκουν στο ανδρικό φύλο, με ποσοστό που ξεπερνά το 90%. Σύμφωνα με έρευνες, φαίνεται ότι 26.7% των θέσεων πληροφορικής είναι κατειλημμένες από γυναίκες [62] ωστόσο όπως καταλαβαίνουμε η συγκεκριμένη έρευνα δεν επιβεβαιώνει κάτι τέτοιο.

Ερώτηση 2: Σε ποιά ηλικιακή ομάδα ανήκετε (προαιρετική ερώτηση);

Η δεύτερη ερώτηση αφορά την ηλικία των συμμετεχόντων. Η ερώτηση αυτή είναι προαιρετική επομένως από τους 56 χρήστες απάντησαν οι 54. 20 προγραμματιστές, με ποσοστό 37% απάντησαν πως είναι μεταξύ 30 με 40 χρονών, 16 άτομα, με ποσοστό 29.6% απάντησαν πως είναι μεταξύ 41-50 ενώ 14 άτομα με ποσοστό 25.9% απάντησαν πως η ηλικία τους κυμαίνεται μεταξύ 18 και 29 ετών. Τα τελευταία 4 άτομα, με ποσοστό 7.4% απάντησαν πως είναι άνω των 50 ετών.

How old are you (optional)?

54 απαντήσεις



Εικόνα 30

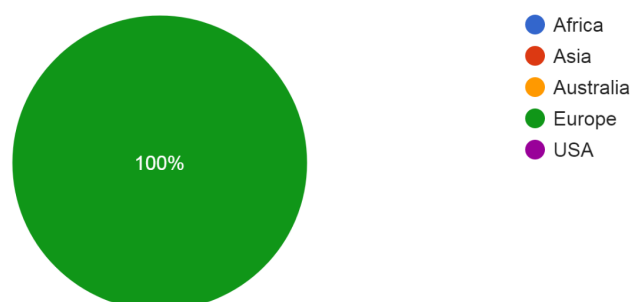
Συμπέρασμα: Σύμφωνα με έρευνα της ZIPPIA την πλειοψηφία των θέσεων πληροφορικής καταλαμβάνουν άτομα ηλικίας άνω των 40 ετών με ποσοστό 54% και άτομα που κυμαίνονται από 30 έως 40 ετών με ποσοστό 30%^[63]. Η έρευνα μας επιβεβαιώνει αυτά τα αποτελέσματα καθώς όπως φαίνεται τα μεγαλύτερα ποσοστά εργασίας προγραμματιστών WordPress συγκεντρώνουν οι ηλικιακές ομάδες που κυμαίνονται από 30-40 ετών με ποσοστό 37% και από 41-50 ετών με ποσοστό 29.6%. Βάση της ίδιας έρευνας, τα νεότερα άτομα που κυμαίνονται ηλικιακά από τα 20 έως τα 30 χρόνια καταλαμβάνουν θέσεις πληροφορικής σε ποσοστό 16%, η δική μας έρευνα ωστόσο συγκέντρωσε ένα ποσοστό 25.9% νέων ατόμων που εργάζονται ως προγραμματιστές WordPress.

Ερώτηση 3: Κατοικείτε στην...

Η τρίτη ερώτηση αφορά την εθνικότητα των συμμετεχόντων και είναι επίσης προαιρετική. Από τους συνολικά 56 προγραμματιστές που συνέβαλαν στην έρευνα απάντησαν οι 53. Από τις 5 επιλογές που είχαν προστεθεί: Αφρική, Ασία, Αυστραλία, Ευρώπη και Ηνωμένες Πολιτείες της Αμερικής και οι 53 προγραμματιστές δήλωσαν πως διαμένουν στην Ευρώπη.

You live in...(optional)

53 απαντήσεις



Εικόνα 31

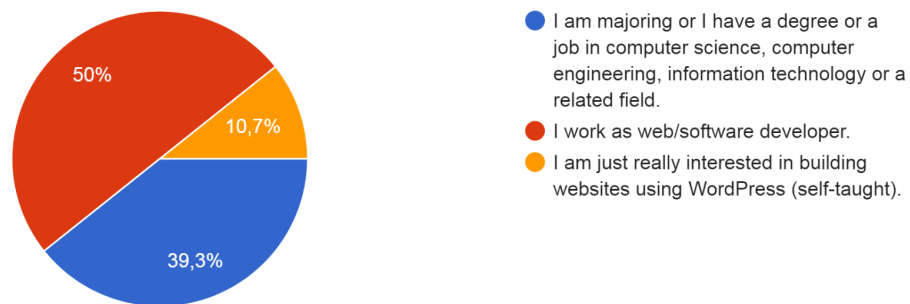
Συμπέρασμα: Μιας και 100% των προγραμματιστών δήλωσαν ότι κατοικούν στην Ευρώπη δε μπορούμε να αντλήσουμε επαρκή συμπεράσματα από την συγκεκριμένη ερώτηση.

Ερώτηση 4: Ποιά είναι η σχέση σας με τις επιστήμες της πληροφορικής;

Στην συνέχεια οι συμμετέχοντες ερωτήθηκαν ποιά είναι η σχέση τους με το κλάδο της πληροφορικής. Από τα 56 συνολικά άτομα τα 28, με ποσοστό 50%, απάντησαν πως δουλεύουν ως προγραμματιστές ιστού ή λογισμικού ενώ 22 άτομα, με ποσοστό 39.3% απάντησαν πως σπουδάζουν, έχουν πτυχίο ή δουλειά σε κάποιον κλάδο σχετικό της πληροφορικής. Τέλος, 6 άτομα με ποσοστό 10.7% απάντησαν πως απλά τους ενδιαφέρει ιδιαίτερα η δημιουργία ιστοσελίδων με τη χρήση WordPress (αυτοδίδακτοι).

What is your relationship with IT?

56 απαντήσεις



Εικόνα 32

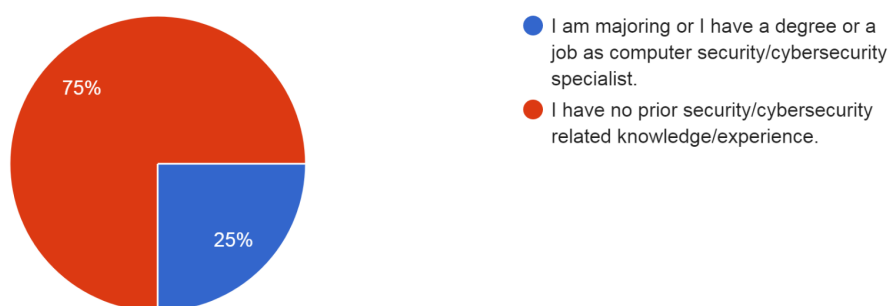
Συμπέρασμα: Από ότι φαίνεται από τα αποτελέσματα που συγκεντρώσαμε οι μισοί προγραμματιστές που δημιουργούν ιστοσελίδες με τη χρήση του WordPress δουλεύουν ως web ή software developers ενώ ένα ποσοστό που πλησιάζει το 40% σπουδάζει ή έχει πτυχίο σε κάποιον κλάδο που σχετίζεται με τις επιστήμες της πληροφορικής. Μόνο ένα ποσοστό 10.7% των προγραμματιστών που συμπλήρωσαν το ερωτηματολόγιο είναι αυτοδίδακτοι. Σύμφωνα με έρευνα που πραγματοποιήθηκε από το Stack Overflow το 2016 περίπου 13% των προγραμματιστών διαδικτύου είναι αυτοδίδακτοι επομένως οι απαντήσεις που δόθηκαν σε αυτή την ερώτηση επιβεβαιώνουν τα νούμερα^[64]. Παρόλο που αξίζει να σημειωθεί πως οποιοσδήποτε με χρόνο και διάθεση μπορεί να μάθει να προγραμματίζει είναι προφανές πως η επαφή με το χώρο της πληροφορικής καθιστά κάτι τέτοιο πιο προσιτό και δίνει τη δυνατότητα στους σπουδαστές ή τους πτυχιούχους να έρθουν σε επαφή με διαφορετικούς τομείς του κλάδου που δε θα συναντούσαν εύκολα στην καθημερινότητα τους.

Ερώτηση 5: Ποιό είναι το επίπεδο των γνώσεων σας στον τομέα της κυβερνοασφάλειας;

Η τελευταία ερώτηση της ενότητας αφορά το επίπεδο τεχνογνωσίας των χρηστών όσον αφορά την ασφάλεια στον κυβερνοχώρο. 42 άτομα από τα 56 που απάντησαν συνολικά, με ποσοστό 75% απάντησαν πως δεν κατέχουν καμία προϋπάρχουσα γνώση ή εμπειρία σχετικά με τους τομείς της ασφάλειας ή κυβερνοασφάλειας ενώ 14, με ποσοστό 25% απάντησαν πως σπουδάζουν ή έχουν πτυχίο ή δουλειά σε κάποιον κλάδο σχετικό της πληροφορικής.

What is your cyber security level of expertise?

56 απαντήσεις



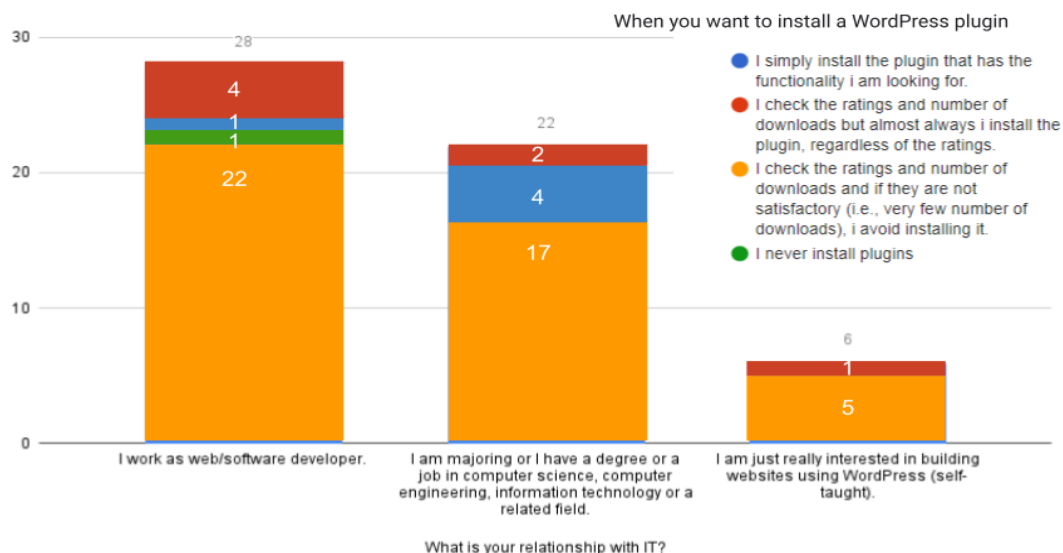
Εικόνα 33

Συμπέρασμα: Τα αποτελέσματα της τελευταίας ερώτησης της έρευνας ήταν και τα πιο ανησυχητικά όσον αφορά την ασφάλεια των ιστοσελίδων που δημιουργούνται. 75% των συμμετεχόντων απάντησαν ότι δεν κατέχουν καμία προϋπάρχουσα γνώση ή εμπειρία σχετικά με τους τομείς της ασφάλειας ή κυβερνοασφάλειας γεγονός που είναι ανεπίτρεπτο για άτομα που ασχολούνται με τη δημιουργία ιστοσελίδων την σήμερον ημέρα. Όπως αναφέρθηκε και παραπάνω, οι μικρές επιχειρήσεις είναι οι πιο συνηθισμένοι στόχοι των κυβερνοεπιθέσεων συγκεντρώνοντας ένα ποσοστό 43% επομένως η ενίσχυση της ασφάλειας τους θα πρέπει να λαμβάνεται πολύ σοβαρά από τους δημιουργούς τους.^[1] Παρόλο που δεν είναι αναγκαίο κάποιος προγραμματιστής ιστοσελίδων να έχει σπουδάσει κάτι σχετικό με το cybersecurity θα πρέπει να είναι πάντα ενημερωμένος για τους νέους κινδύνους και τις επιθέσεις που απειλούν τις ιστοσελίδες του και να εξασφαλίζει την εφαρμογή μέτρων που θα τις αποτρέψουν.

4.8 Συνδυαστικά Συμπεράσματα

Παρόλο που τα συμπεράσματα που συγκεντρώθηκαν παραπάνω καλύπτουν ένα σημαντικό μέρος των ερωτημάτων που θέσαμε πριν την έναρξη της συγκεκριμένης έρευνας είναι σημαντικό να εξερευνήσουμε και ορισμένες άλλες πτυχές των απαντήσεων. Ο τρόπος προσέγγισης των επιπλέον συμπερασμάτων που εκμαιεύτηκαν προέρχεται από το συνδυασμό διαφορετικών ερωτήσεων προκειμένου να αντλήσουμε συμπεράσματα για τη συμπεριφορά των χρηστών κυρίως ανάλογα με το προγραμματιστικό τους υπόβαθρο.

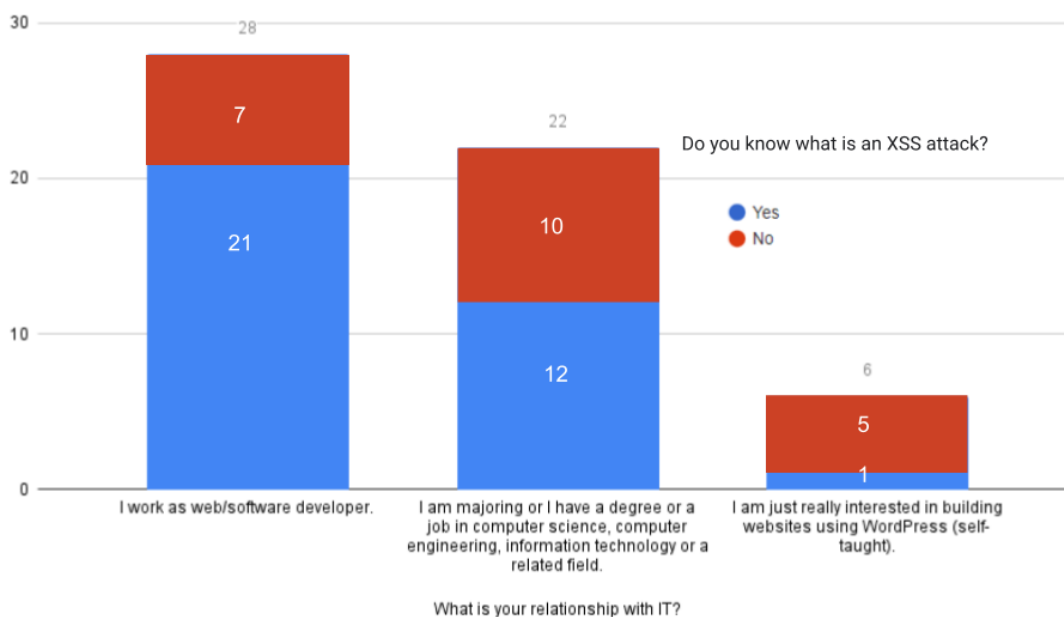
4.8.1 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Τρόπος λήψης πρόσθετων.



Εικόνα 34

Όπως βλέπουμε στο παραπάνω συνδυαστικό γράφημα, τα αποτελέσματα όσον αφορά τον τρόπο λήψης προσθέτων μας δείχνουν πως όλοι οι συμμετέχοντες της έρευνας, ανεξάρτητα από το εκπαιδευτικό τους υπόβαθρο, απάντησαν πως επιλέγουν την εγκατάσταση αφότου πρώτα έχουν ελέγξει τις βαθμολογίες και τις λήψεις των προσθέτων και αποφεύγουν να τα κατεβάσουν αν αυτές δεν είναι ικανοποιητικές.

4.8.2 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν τί είναι η επίθεση XSS.

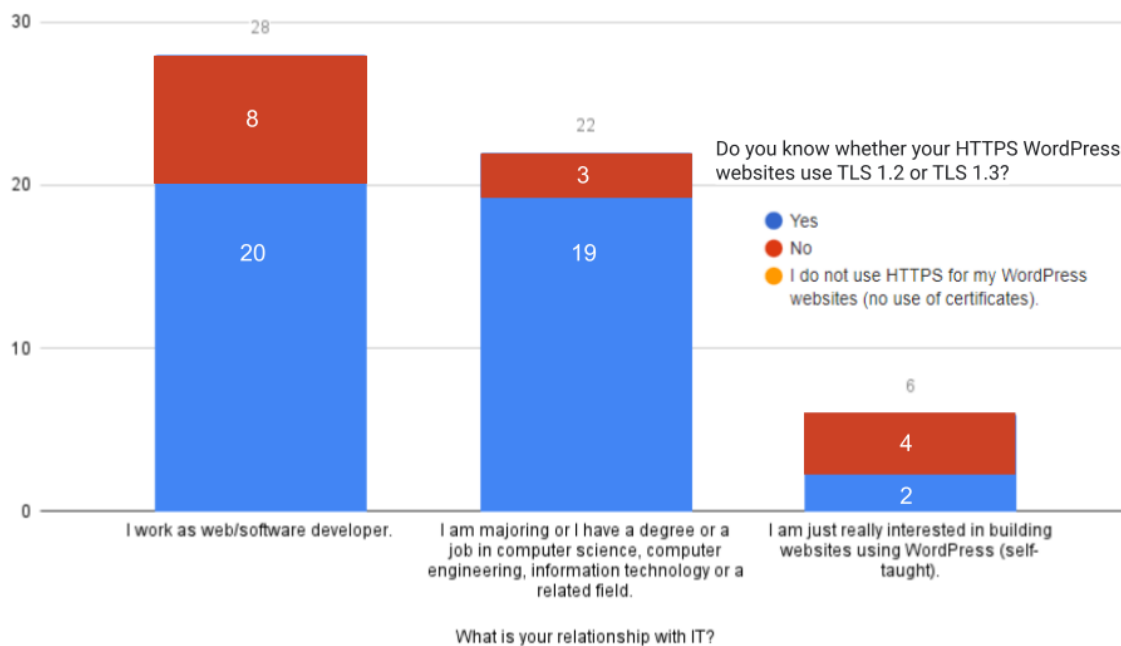


Εικόνα 35

Όπως βλέπουμε σε αυτό το συνδυαστικό γράφημα η γνώση των συμμετεχόντων αναφορικά με τις επιθέσεις XSS σχετίζεται άμεσα με το εκπαιδευτικό τους υπόβαθρο. Παρόλο που οι προγραμματιστές που δουλεύουν ή σπουδάζουν σε κάτι σχετικό με τον κλάδο της πληροφορικής γνώριζαν κατά κανόνα τι είναι μια τέτοια επίθεση, οι αυτοδίδακτοι developers δεν ήταν ενήμεροι για κάτι τέτοιο.

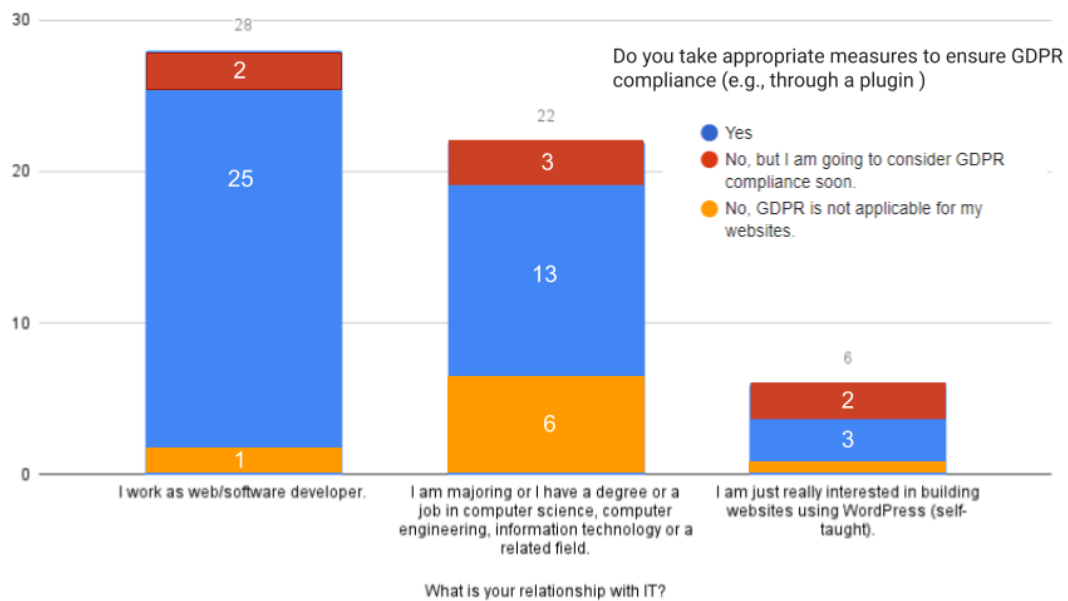
4.8.3 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν αν οι HTTPS ιστοσελίδες τους χρησιμοποιούν TLS 1.2 ή TLS 1.3.

Εικόνα 36



Όπως βλέπουμε στο παραπάνω συνδυαστικό γράφημα και εδώ η γνώση όσον αφορά το πρωτόκολλο HTTPS εξαρτάται από το εκπαιδευτικό υπόβαθρο των προγραμματιστών διαδικτύου. Το ποσοστό που γνωρίζει τι εστί το HTTPS πρωτόκολλο και κατά κανόνα τι είναι τα TLS 1.2 και 1.3 φαίνεται πως είναι παραπάνω από το 70% στα άτομα που έχουν σπουδάσει ή δουλεύουν σε κλάδο που σχετίζεται με την πληροφορική. Από την άλλη, τα άτομα που είναι αυτοδίδακτα όσον αφορά τη δημιουργία ιστοσελίδων, δε γνωρίζουν τι χρησιμοποιούν οι HTTPS ιστοσελίδες τους σε ποσοστό που πλησιάζει το 70%.

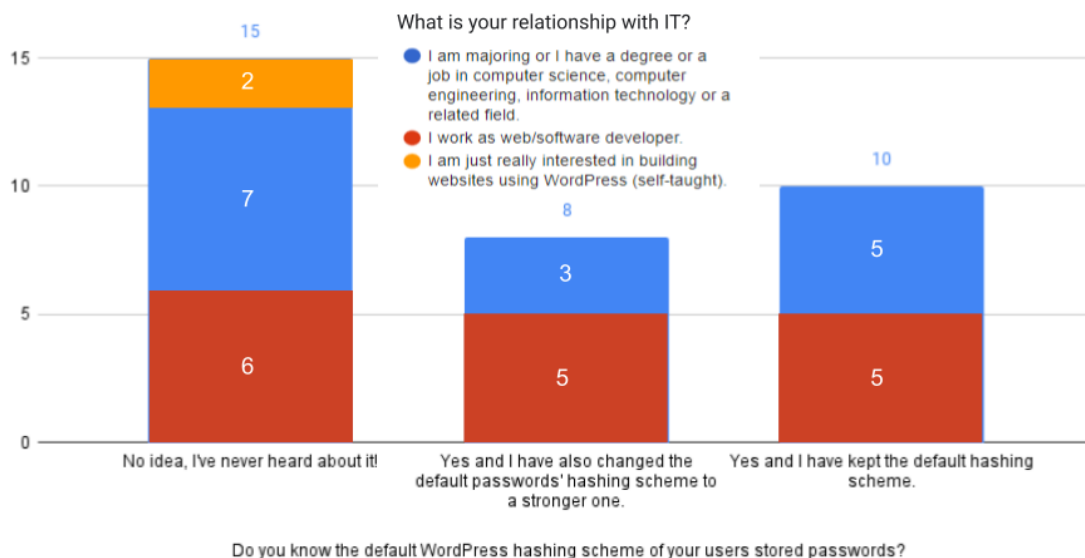
4.8.4 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο εφαρμόζουν κατάλληλα μέτρα για να εξασφαλίσουν την συμμόρφωση με το GDPR.



Εικόνα 37

Όπως βλέπουμε στο συνδυαστικό γράφημα παραπάνω, το εκπαιδευτικό υπόβαθρο δεν παίζει ιδιαίτερα σημαντικό ρόλο στην εφαρμογή του GDPR από τους προγραμματιστές. Ωστόσο, μπορούμε να παρατηρήσουμε πως τα άτομα που εργάζονται ως web ή software developers νοιάζονται περισσότερο για την εξασφάλιση της συμμόρφωσης με το GDPR, πιθανότατα γιατί κάτι τέτοιο απαιτείται από το χώρο εργασίας τους.

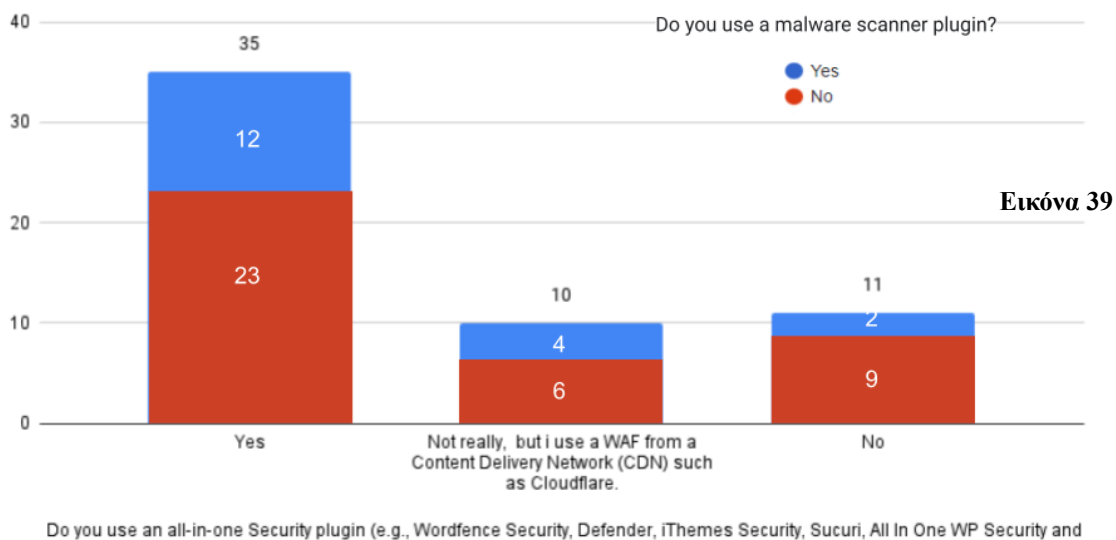
4.8.5 Σχέση ερωτηθέντων με το κλάδο της πληροφορικής / Κατά πόσο γνωρίζουν το default WordPress hashing scheme των αποθηκευμένων κωδικών πρόσβασης των χρηστών τους.



Εικόνα 38

Αυτή η ερώτηση απευθύνεται μόνο στους 33 χρήστες που απάντησαν πως οι ιστοσελίδες τους επιτρέπουν την εγγραφή και είσοδο χρηστών. Όπως μπορούμε να δούμε στο παραπάνω γράφημα μόνο δύο αυτοδίδακτοι προγραμματιστές απάντησαν αυτή την ερώτηση και πρόσθεσαν πως δε γνώριζαν πως υπάρχει κάτι τέτοιο πριν έρθουν σε επαφή με αυτή την έρευνα. Ωστόσο, και το μεγαλύτερο ποσοστό των ατόμων που εργάζονται σε κάποιον κλάδο της πληροφορικής ή σπουδάζουν κάτι σχετικό απάντησε το ίδιο. Όπως μπορούμε ήδη να υποθέσουμε, δε μπορούμε να βγάλουμε ξεκάθαρα συμπεράσματα από την συγκεκριμένη ερώτηση όσον αφορά την συσχέτιση του εκπαιδευτικού υπόβαθρου των συμμετεχόντων και της γνώσης τους όσον αφορά το hashing scheme. Το μόνο που μπορεί να ειπωθεί είναι πως τα άτομα που εργάζονται σε κάποιον κλάδο της πληροφορικής φαίνεται να γνωρίζουν περισσότερα πράγματα όσον αφορά την συγκεκριμένη έννοια.

4.8.6 Κατά πόσο οι προγραμματιστές χρησιμοποιούν κάποιο all-in-one plugin / Κατά πόσο χρησιμοποιούν κάποιο malware scanner plugin.



Εικόνα 39

Όπως είχαμε υποθέσει στα συμπεράσματα που συγγράφηκαν παραπάνω οι περισσότεροι χρήστες που απάντησαν πως δε χρησιμοποιούν κάποιο malware scanner plugin χρησιμοποιούν κάποιο all-in-one plugin πράγμα που σημαίνει πως στην πραγματικότητα το χρησιμοποιούν εν άγνοια τους. Από την άλλη υπάρχουν 9 χρήστες που δε χρησιμοποιούν κανέναν από τους δύο αυτούς τρόπους ασφαλείας πράγμα αρκετά επικίνδυνο.

4.8.7 Συγκεντρωτικά συμπεράσματα

Ένα από τα κύρια πράγματα που παρατηρήσαμε μελετώντας τα συμπεράσματα που συγκεντρώσαμε παραπάνω είναι πως τα άτομα που ασχολούνται με τη δημιουργία ιστοσελίδων WordPress χωρίς να έχουν κάποια σχέση με το κλάδο της πληροφορικής υστερούν όσον αφορά την ενημέρωση στους θεωρητικούς και κάπως εξειδικευμένους τομείς της δημιουργίας ενός site. Για παράδειγμα, τα άτομα που σπουδάζουν ή εργάζονται σε κάτι σχετικό με την συγκεκριμένη επιστήμη έχουν έρθει σε επαφή με διάφορου είδους επιθέσεις

που απειλούν τους σημερινούς ιστοτόπους με αποτέλεσμα να είναι ενήμεροι για τους κινδύνους ώστε να προσπαθήσουν να τους περιορίσουν. Παρομοίως, το ίδιο συμβαίνει και με τα πρωτόκολλα δικτύου όπως το HTTPS. Σαφώς, τα άτομα με κάποιο πληροφοριακό υπόβαθρο έχουν έρθει σε επαφή με αυτό το πρωτόκολλο και γνωρίζουν τους τρόπους λειτουργίας τους.

Παρόλο που τα γεγονότα που συγκεντρώθηκαν δεν αλλάζουν, αυτό δεν σημαίνει πως κάποιος αυτοδίδακτος προγραμματιστής του WordPress δε μπορεί να μάθει όλα τα παραπάνω. Με την κατάλληλη ενημέρωση και την εκβάθυνση στον κλάδο της πληροφορικής όλες αυτές οι πληροφορίες μπορούν να αφομοιωθούν.

Σχετικές Έρευνες

- [1] Hannes Trunde, Edgar Weippl, [“WordPress security: an analysis based on publicly available exploits”](#), IEEE, December 11, 2015
- [2] Ar Kar Kyaw, Franco Sioquim, Justin Joseph, [”Dictionary attack on Wordpress: Security and forensic analysis”](#), IEEE, 21 March, 2016
- [3] Teemu Koskinen, Petri Ihanola, Ville Karavirta, [“Quality of WordPress Plug-Ins: An Overview of Security and User Ratings”](#), IEEE, January 10, 2013
- [4] Ionut Cernica, Nirvana Popescu, Bogdan țigănoaia, [”Security Evaluation of Wordpress Backup Plugins”](#), IEEE, June 27, 2019

Βιβλιογραφία - Δικτυογραφία

- [1] Purplesec, [“Cyber Security StatisticsThe Ultimate List Of Stats Data, & Trends For 2022”](#), 2022
- [2] Edward Segal, [“Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report”](#), Forbes, March 16, 2022
- [3] Robert Johnson, III, [“60 Percent Of Small Companies Close Within 6 Months Of Being Hacked”](#), Cyber Security Ventures, January 2, 2019
- [4] Editorial Staff, [“15 Best and Most Popular CMS Platforms in 2022 \(Compared\)”](#), wpBegginner, last updated January 1st, 2022
- [5] Nibusiness info, [“Contact management systems”](#), Nibusiness
- [6] ArcStone Staff, [“The Pros and Cons of Choosing WordPress for your Website CMS”](#), January 2020
- [7] Δρ.Α.Κουμπαρέλης, [“Πρότυπο Πτυχιακής εργασίας”](#), Αργοστόλι, Κεφαλονιά, 2018
- [8] Kandace Cortez, [“The Disadvantages of WordPress”](#), doctorlogic
- [9] Μπεκιάρη Κωνσταντίνα, [“Ασφάλεια διαδικτυακών εφαρμογών: Σχεδιαστικές λύσεις και αξιολόγηση της ασφάλειας”](#), Πανεπιστήμιο Δυτικής Αττικής, Σχολή Διοικητικών,Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Αρχαιονομίας, Βιβλιοθηκονομίας και Συστημάτων Πληροφόρησης, Μάρτιος 2021
- [10] Manuel Alejandro Lupion Jimenez, [“Magnolia”](#), Trustradius, January 12, 2022
- [11] Anna Fitzgerald, [“The 16 Best CMS Systems Today & How to Choose”](#), Hubspot, January 04, updated August 11, 2022
- [12] Informatics Article, [“The Pros and Cons of a Concrete5 Content Management System”](#), Informatics, November 4, 2014
- [13] Γκέσσας Ιωάννης, [“Η πολιτική της κυβερνοασφάλειας και η ενσωμάτωση της οδηγίας για την κυβερνοασφάλεια \(cybersecurity directive\)”](#), Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφορικής και επικοινωνιακών Συστημάτων, 22 Σεπτεμβρίου, 2021
- [14] Βλυσσίδης Κωνσταντίνος, [“Ασφάλεια δικτύων υπολογιστών και ανάλυση αδυναμιών”](#), Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Πληροφορικής, 2012
- [15] Μπίλης Ευστράτιος, [“Έλεγχος Ευπαθειών με Χρήση του Πλαισίου Metasploit”](#), Πανεπιστήμιο Μακεδονίας, Τμήμα Εφαρμοσμένης Πληροφορικής, Σεπτέμβριος, 2012
- [16] Ρουπάκας Παρασκευάς Σωτήριος, [“To CyberSecurity στις ελληνικές τράπεζες, κίνδυνοι δικλείδες ασφαλείας και μέθοδοι ελέγχου”](#), Hellanicus, 2020
- [17] Jeff Dance, [“How to Choose a CMS? 10 Factors to Keep in Mind”](#), Freshconsulting, February 8, 2019
- [18] Sitecore staff, [“How to choose the right CMS”](#), Sitecore
- [19] Will Morris, [“15 Best CMS Platforms to Start a Website in 2022”](#), Hostinger Tutorials, May 10, 2022
- [20] Noel Greene, [“Should a developer use a content management system?”](#), evolve
- [21] Desiree Johnson, [“What Is WordPress & What is It Used For?”](#), bluehost, September 03, 2018
- [22] [“Using Themes”](#). *WordPress.org*. Retrieved July 17, 2022
- [23] Chandler, Jeff (April 3, 2014). "Introduction To Underscores: A WordPress Starter Theme With Konstantin Obenland". Archived from the original on August 19, 2016. Retrieved July 31, 2016.
- [24] ["WordPress Plugins"](#). *WordPress.org*. Retrieved June 18, 2022.
- [25] Wikipedia Users, [WordPress](#), Wikipedia the Free Encyclopedia, last edited September 4, 2022
- [26] Adam R, Brown, [WordPress Hooks Database](#), Adam R. Brown website
- [27] ["David Kierznowski"](#). Blogsecurity.net. June 28, 2007. Archived from the original on March 9, 2012. Retrieved February 17, 2016.

- [28] "[Secunia WordPress Vulnerability Report](#)". Secunia.com. [Archived](#) from the original on July 23, 2017. Retrieved September 13, 2013.
- [29] "[WordPress Exploit Nails Big Name Seo Bloggers](#)". Threadwatch.org. [Archived](#) from the original on October 6, 2018. Retrieved December 18, 2011.
- [30] "[WordPress 2.1.1 dangerous, Upgrade to 2.1.2](#)". WordPress.org. March 2, 2007. [Archived](#) from the original on March 4, 2007. Retrieved March 4, 2007.
- [31] "[Survey Finds Most WordPress Blogs Vulnerable](#)". Blog Security. May 23, 2007. [Archived](#) from the original on March 15, 2012. Retrieved June 15, 2010
- [32] "[Updating WordPress](#)". WordPress Codex. [Archived](#) from the original on October 11, 2012. Retrieved September 25, 2012.
- [33] "[Yet another WordPress release](#)". August 13, 2009. [Archived](#) from the original on October 30, 2012. Retrieved September 24, 2012.
- [34] "[Interview with Stefan Esser](#)". BlogSecurity. June 28, 2007. [Archived](#) from the original on October 13, 2012. Retrieved June 15, 2010.
- [35] Westervelt, Robert (June 18, 2013). "[Popular WordPress E-Commerce Plugins Riddled With Security Flaws – Page: 1](#)". CRN. [Archived](#) from the original on March 20, 2015. Retrieved March 11, 2015.
- [36] "[Configuring Automatic Background Updates « WordPress Codex](#)". Codex.wordpress.org. [Archived](#) from the original on June 28, 2014. Retrieved June 30, 2014.
- [37] Ward, Simon (July 9, 2012). "[Original Free WordPress Security Infographic by Pingable](#)". Pingable. [Archived](#) from the original on October 25, 2012. Retrieved October 28, 2012.
- [38] [CVE-2015-2292 "Archived copy"](#). [Archived](#) from the original on June 14, 2017. Retrieved July 7, 2017., Retrieved on July 7, 2017
- [39] Common Vulnerabilities and Exposures [CVE-2015-2293"Archived copy"](#). [Archived](#) from the original on June 15, 2017. Retrieved July 7, 2017., Retrieved on July 7, 2017
- [40] Barry Schwartz "[Yoast WordPress SEO Plugin Vulnerable To Hackers](#)" [Archived](#) February 11, 2016, at the [Wayback Machine](#), Retrieved on February 13, 2016.
- [41] "[Disclosure of Additional Security Fix in WordPress 4.7.2](#)". *Make WordPress Core*. February 1, 2017. [Archived](#) from the original on February 16, 2017. Retrieved February 16, 2017.
- [42] "[Content Injection Vulnerability in WordPress 4.7 and 4.7.1](#)". *Sucuri Blog*. February 1, 2017. [Archived](#) from the original on February 16, 2017. Retrieved February 16, 2017.
- [43] "[WordPress » About » Requirements](#)". *wordpress.org*. March 28, 2018. [Archived](#) from the original on May 21, 2019. Retrieved May 21, 2019.
- [44] "[Unsupported Branches](#)". *php.net*. [Archived](#) from the original on May 15, 2019. Retrieved May 21, 2019.
- [45] "[Bug report #42428: wp-emoji pops up privacy hanger in Firefox with privacy.resistFingerprinting turned on](#)". *Make WordPress Core*. Retrieved February 4, 2020.
- [46] Jamie Juviler, "[14 WordPress Security Issues & Vulnerabilities You Should Know About \[New Research from WCEU 2022\]](#)", Hubspot, updated June 23, 2022
- [47] Ibad Rehman, WSR Team, "[Top 6 Most Common WordPress Vulnerabilities \(and How To Fix Them\)](#)", Website Rating, June 16, 2022
- [48] "[Brute Force Attacks](#)". *WordPress.org*. Retrieved July 17, 2022.
- [49] Ραμπαβίλα Αρτεμης, "Ανάλυση της χρήσης λογισμικού και plugin ασφαλείας του WordPress", Ιόνιο Πανεπιστήμιο, Κέρκυρα, Μάρτιος, 2022
- [50] Mark Grima, "[WordPress Security & Hardening, the Definitive Guide](#)", WP White Security, last updated June 15, 2022
- [51] Mark Grima, "[WordPress Security & Hardening, the Definitive Guide-Update](#)", WP White Security, last updated June 15, 2022

- [52] Mark Grima, [“WordPress Security & Hardening, the Definitive Guide-Security”](#), WP White Security, last updated June 15, 2022
- [53] Adalina Tuca, [“Here Are the Most Popular WordPress Plugins of All Time \(Based on Data\)”](#), Themeisle, April 19, 2022
- [54] Jamie Juviler, [“16 WordPress Security Plugins To Protect Your Blog”](#), Hubspot, updated March 25, 2022
- [55] Charles Lecklider, [“WP fail2ban”](#), WordPress, last updated 2 months ago
- [56] SucuPress, [“SucuPress Free - WordPress Security”](#), WordPress, last updated 4 weeks ago
- [57] WPScan Team, [“WPScan - WordPress Security Scanner”](#), WordPress, last updated 2 months ago
- [58] Automattic, [“VaultPress”](#), WordPress, last updated 2 months ago
- [59] Ivan Kruckhoff, [“Google Authenticator”](#), WordPress, last updated 2 months ago
- [60] Astra Security, [“Astra Security Suite - Firewall & Malware Scan”](#), WordPress, last updated 1 year ago
- [61] WebArxSecurity, [“Privacy Policy”](#), WebARX, last update October 29, 2019
- [62] Josh Howarth, [“74+ Shocking Women In Tech Statistics \(2022\)”](#), Exploding Topics, August 15, 2022
- [63] Zippia Team, [“Information Technology Professional Demographics and Statistics In the US”](#), updated April 18, 2022
- [64] Karen Turner, [“Lots of coder are self-taught according to developer survey”](#), March 30, 2016
- [65] Wordfence, [“Wordfence Security - Firewall & Malware Scan”](#), WordPress, updated 1 month ago
- [66] Jetpack, [“Jetpack”](#)
- [67] Getshieldsecurity, [“Shield Security”](#), ShieldFREE, 2022