Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Ασφάλεια σε περιβάλλον ιστολόγιου, με χρήση Wordpress Security in blogging environment, using Wordpress
Ονοματεπώνυμο Φοιτητή	Σπυρίδων Λόης
Πατρώνυμο	Σωκράτης
Αριθμός Μητρώου	ΜΠΠΛ/ 12029
Επιβλέπων	Παναγιώτης Κοτζανικολάου, Λέκτορας

Τριμελής Εξεταστική Επιτροπή

Ψαράκης Μιχαήλ	Κοτζανικολάου Παναγιώτης	Πατσάκης Κωνσταντίνος
Επίκουρος Καθηγητής	Λέκτορας	Λέκτορας

ΠΕΡΙΛΗΨΗ

Στην εργασία που ακολουθεί εξετάζονται τα θέματα ασφαλείας και ιδιωτικότητας στα συστήματα ιστολογίων (web logs η blogs).Τα συστήματα αυτά είναι πληροφοριακά συστήματα που υποστηρίζουν δημοσίευση πληροφοριών, και αποτελούν μία μορφή δημοσιογραφίας που επηρεάζει τη δημοκρατία, έξω από τα μέσα μαζικής ενημέρωσης και τα παραδοσιακό πολιτικά κόμματα. Ιστολόγια με θέμα τη τεχνολογία, (shlashdot.org) και τη πολιτική έχουν χιλιάδες αναγνώστες την ημέρα. Σαν πληροφοριακό σύστημα, το σύστημα του ιστολογίου είναι εκτεθειμένο, και οι αδυναμίες του μπορούν να γίνουν αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες. Σκοπός της εργασίας αυτής είναι να μελετήσει τους τρόπους εξασφάλισης ασφάλειας των ιστολογίων, και η δημιουργία ενός ασφαλούς ιστολόγιου με βάση το XAMPP και το Wordpress, σε περιβάλλον Windows.

του
ΣΠΥΡΙΔΩΝ ΛΟΗΣ ΜΠΠΛ12029
ΠΜΣ: «ΠΛΗΡΟΦΟΡΙΚΗ»
Τμήμα Πληροφορικής
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ABSTRACT

This dissertation addresses the security and privacy issues in blog systems (web logs the blogs). Such systems are information systems that support publication of information, and are a form of journalism that affects democracy, out of the media and the traditional political parties. Blogs on technology, (shlashdot.org) and policy have thousands of readers per day. As information system, the blog is exposed, and the weaknesses can be exploited by malicious users. The purpose of this dissertation is to study how to provide security blogs, and creating a safe blog based XAMPP and wordpress, environment.

Spyridon Lois
Department of Informatics
UNIVERSITY OF PIRAEUS

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή και περιγραφή του υπό μελέτη χώρου

Οι νέες τεχνολογίες καλύπτουν ολοένα και μεγαλύτερο μέρος τόσο της εργασιακής όσο και της καθημερινής μας ζωής. Σήμερα έχει αυξηθεί η δυνατότητα πληροφόρησης του ατόμου σε σχέση με τις προηγούμενες γενιές. Με τον όρο διαδίκτυο εννοούμε το μεγαλύτερο δίκτυο υπολογιστών στο πλανήτη. Είναι ένα δίκτυο που αποτελείται από εκατομμύρια ιδιωτικά, δημόσια, ακαδημαϊκά επιχειρηματικά και κυβερνητικά δίκτυα. Οι υπηρεσίες και οι εφαρμογές που βασίζονται σε αυτό είναι αναρίθμητες. Ο ιστός είναι ένα κατανεμημένο σύστημα διασυνδεδεμένων πολυμέσων για την ανάκτηση δικτυακών πληροφοριών, βασισμένο στο δίπολο πελάτη-διακομιστή [1]. Για να έχει πρόσβαση σε διακομιστή κάποιος χρήστης , μέσω σύνδεσης στο internet, πρέπει να χρησιμοποιήσει ένα πρόγραμμα πελάτη, γνωστό ως φυλλομετρητή. Οι περισσότερες υπηρεσίες, όπως ηλεκτρονικά καταστήματα(e-shops), ηλεκτρονική τραπεζική(e-banking), μετάδοση πληροφοριών και ειδήσεων , προσφέρονται μέσα από τον ιστό λόγω της ευκολίας πρόσβασης. Ένα ζήτημα που υπάρχει στις περιπτώσεις αυτές, είναι αυτό της ασφάλειας, καθώς στον ιστό δεν υπάρχει η φυσική παρουσία των μεθόδων ταυτοποίησης όπως η ταυτότητα στο φυσικό περιβάλλον. Επίσης υπάρχουν κίνδυνοι όπως η πλαστογράφηση σελίδων και η υποκλοπή δεδομένων.
Ιστολόγιο (web log ή blog) είναι ένας πληροφοριακός ιστότοπος που εκδίδεται στον παγκόσμιο ιστό και αποτελείται από διαφορετικές αναρτήσεις οι οποίες συνήθως εμφανίζονται σε αντίστροφη χρονολογική σειρά. Μέχρι το 2009 το κάθε ιστολόγιο ήταν δημιουργία ατόμων, μικρών ομάδων και κάλυπταν ένα θέμα. Πιο πρόσφατα ιστολόγια πολλών συγγραφέων έχουν εμφανιστεί, με άρθρα που γράφονται από μεγάλο αριθμό δημιουργών και διαμορφώνονται , με επαγγελματικό τρόπο.

Στο πρακτικό μέρος της εργασίας θα χρησιμοποιηθούν για τη δημιουργία και την ασφάλεια ενός ιστολογίου (blog) το σύνολο προγραμμάτων XAMPP και το σύστημα διαχείρισης περιεχομένου wordpress. Το XAMPP είναι ένα ενοποιημένο σύνολο εφαρμογών λογισμικού ανοιχτού κώδικα που αποτελείται από τον διακομιστή web Apache, τη βαση δεδομένων MySQL, τις γλώσσες PHP και Perl. Η ύπαρξή του είναι αναγκαία για την εγκατάσταση συστημάτων διαχείρισης περιεχομένων, κάποια από τα πιο διαδεδομένα είναι το joomla το wordpress και το drupal.
Το wordpress είναι ένα εργαλείο δημιουργίας ιστολόγιων και διαχείρισης περιεχομένου ανοιχτού κώδικα. Το Wordpress είναι το πιο δημοφιλές εργαλείο για την ανάπτυξη ιστολόγιων. Είναι γραμμένο σε PHP και λειτουργεί σε συνεργασία με τη βάση δεδομένων MySQL.Στην εργασία θα γίνει παραμετροποίηση του wordpress με σκοπό να μελετηθεί η δυνατότητα δημιουργίας ιστολόγιου με βασικές προδιαγραφές ασφαλείας με βάση το XAMPP σε wordpress, σε windows ultimate 7. Θα παρουσιαστεί η διαχείριση χρηστών μέσα από το wordpress για να επιτρέπονται συγκεκριμένοι ρόλοι σε συγκεκριμένα άτομα.
Μέθοδοι που χρησιμοποιούνται για την ασφάλεια των χρηστών και των πληροφοριών είναι η χρησιμοποίηση συνθηματικών, η κρυπτογράφηση και η εφαρμογή της για ασφαλή μεταφορά με πρωτόκολλο SLL και TLS. Η κρυπτογράφηση είναι η εφαρμογή μεθόδων για τη προστασία των πληροφοριών κατά τη μετάδοσή τους. Ακόμα και αν υποκλαπούν δεδομένα, θα είναι ακατανόητα για το παρεμβαλλόμενο μέρος. Στην περίπτωση της ασφάλειας σύνδεσης στον ιστό χρησιμοποιούνται και η συμμετρική και η ασύμμετρη κρυπτογράφηση.

1.2 Ορισμός

. Ιστολόγια είναι ιστότοποι που περιέχουν πληροφορίες, ειδήσεις, συζητήσεις πάνω σε κάποια θεματική ενότητα, ή σε επίκαιρα θέματα. Αποτελούνται από εγγραφές σε αντίστροφη χρονολογική σειρά. Εταιρίες όπως η IBM διατηρούν ιστολόγια στα οποία παρουσιάζουν τις εξελίξεις στο χώρο τους, και τη προοπτική τους για το μέλλον, το εργατικό δυναμικό τους(blog.ibm.jobs). Τεχνολογικά blog παρουσιάζουν εξελίξεις στο τομέα τους, και λειτουργούν ως εφημερίδες, ή online περιοδικά.

1.3 Πλεονεκτήματα και μειονεκτήματα online ιστολόγιων

Τα μειονεκτήματα των ιστολόγιων στο διαδίκτυο είναι ρίσκο που προκύπτει από τα τμήματα κώδικα που υπάρχουν σε αυτό και επιτρέπουν δημιουργία αδυναμιών(vulnerabilities) . Είναι αλήθεια ότι υπάρχουν θέματα ασφαλείας σε κάθε ιστότοπο, το να υπάρχει ένα ιστολόγιο ή ένα σύστημα διαχείρισης περιεχομένου στην ιστοσελίδα του αυξάνει αυτό το ρίσκο. Τέτοιο λογισμικό είναι περίπλοκο με πολλά τμήματα που εκτελούν διαφορετικά καθήκοντα. Είναι πάντα δυνατό να υπάρχει μία τρύπα ασφαλείας για την οποία ο προγραμματιστής να μην είναι ενήμερος. Από τη στιγμή που το λογισμικό υπάρχει στο ιστότοπο είναι εκτεθειμένο, και οποιοσδήποτε βρει ένα κενό ασφαλείας που δεν το γνωρίζει ο προγραμματιστής μπορεί να θέσει σε κίνδυνο το πρόγραμμα και τα δεδομένα. Οι αναβαθμίσεις μπορεί να είναι ένα άλλο πρόβλημα, καθώς κάθε φορά που ανακαλύπτεται μία αδυναμία στην ασφάλεια εκδίδεται και αναβάθμιση λογισμικού για την αντιμετώπισή της και η αναβάθμιση πρέπει να γίνεται για να μην είναι εκτεθειμένη η ιστοσελίδα σε γνωστούς κινδύνους. Το ιστολόγιο μπορεί να μην είναι διαθέσιμο κατά την αναβάθμιση. Άλλο μειονέκτημα είναι η ανάγκη να αντιμετωπιστούν σχόλια spam στο ιστολόγιο. Αν και είναι καλό να αφήνουν σχόλια οι πραγματικοί επισκέπτες , είτε θετικά είτε αρνητικά, μαζί με τους κανονικούς επισκέπτες έρχονται και ανεπιθύμητοι όπως bots και webmasters που αφήνουν διαφημίσεις. Φυσικά μπορούν να διαγραφούν τα σχόλια αλλά αυτό είναι χρονοβόρο. Κάποιες φορές ο λόγος σήματος προς θόρυβο είναι τόσο χαμηλός που οι διαχειριστές απενεργοποιούν τα σχόλια. Αυτό όμως περιορίζει τη λειτουργικότητα του ιστολόγιου και τη δημιουργία κοινότητας.

1.4 1 Είδη ιστολογίων

Ο δημιουργός του ιστολογίου μπορεί να χρησιμοποιήσει μία έτοιμη online πλατφόρμα όπως το blogger της google ή το wordpress.com που υπάρχουν στο διαδίκτυο και προσφέρουν φιλοξενία στο περιεχόμενό του. Μία άλλη επιλογή είναι να κατασκευάσει μόνος του το ιστολόγιό του, χρησιμοποιώντας κάποιο εργαλείο όπως σύστημα διαχείρισης περιεχομένου και να το ανεβάσει σε μία δική του περιοχή (domain)στο internet. Το μειονέκτημα της online πλατφόρμας είναι ότι ένα λάθος στο σχεδιασμό είναι άμεσα φανερό στο κοινό, ενώ ένα ιστολόγιο σε ιδιόκτητο CMS έχει τη

δυνατότητα της δοκιμής και χωρίς σύνδεση, πριν το περιεχόμενο ανεβεί στο διαδίκτυο. Ένα τέτοιο ιστολόγιο απαιτεί κάποιες γνώσεις τεχνολογιών CMS και βάσεων δεδομένων

1.5 Υπηρεσία blogger

Οι υπηρεσία blogger επιτρέπει την άμεση δημιουργία ιστολόγιου σε ιστοσελίδες που φιλοξενούνται από τη Google στον υποτομέα blogspot.com. Στις σελίδες του υποστηρίζονται διάφορες γλώσσες μεταξύ των οποίων και τα ελληνικά. Το blogger επιτρέπει τη χρήση διαφόρων προτύπων (templates) και την προσαρμογή τους. Το πιο καινούριο template βασίζεται σε HTML5, AJAX και CSS3. Υπάρχει HTML editor που επιτρέπει στο εκδότη του ιστολόγιου να επεξεργαστεί το πηγαίο κώδικα της σελίδας.
Ο Δημιουργός του ιστολόγιου δεν αποκαλύπτει τη πραγματική του ταυτότητα παρά μόνο ένα ψευδώνυμο αν το επιθυμεί.. Υπάρχει η δυνατότητα δημιουργίας πολλαπλών ιστολογίων, με διαφορετικό όνομα, με κατάληξη blogspot.com.

1.6 Ιδιωτικότητα και ασφάλεια

Ο σκοπός του ιστολόγιου είναι να δημοσιεύονται πληροφορίες οι οποίες καθώς είναι γενικά διαθέσιμες δεν προστατεύονται, όπως το περιεχόμενο των μηνυμάτων, η υπογραφή και η χρονοσήμανση αν υπάρχει αλλά ταυτόχρονα χρειάζεται να υπάρχει δυνατότητα για προστασία της ακεραιότητας του ιστολογίου και κάποιων ιδιωτικών πληροφοριών επικοινωνίας που χρησιμοποιεί ο δημιουργός του ιστολόγιου. Το πραγματικό του όνομα πρέπει να είναι προστατευμένο, τα στοιχεία πρόσβασης πρέπει να είναι κρυπτογραφημένα όταν γίνεται η σύνδεση για τη μετάδοση των εξωτερικών πληροφοριών της επικοινωνίας, όπως η διεύθυνση IP και αριθμός mac. Η κάθε ιστοσελίδα που συλλέγει στοιχεία από το χρήστη πρέπει να τον προειδοποιεί για αυτό και να μην παρέχει πρόσβαση σε τρίτους ως προς τις ιδιωτικές πληροφορίες του χρήστη. Παρατηρούμε μία αντίφαση στην ανάγκη για ύπαρξη δημοσιοποίησης πληροφοριών και στην ανάγκη προστασίας κάποιων ευαίσθητων πληροφοριών.

1.7 Στόχοι της εργασίας

Στόχος της εργασίας είναι

- Να μελετηθούν τεχνολογίες ασφαλείας σε εφαρμογές ιστού και ιδιαίτερα σε ιστολόγια.
- Να γίνει εγκατάσταση, του συστήματος διαχείρισης περιεχομένου wordpress.
- Να μελετηθεί ο έλεγχος πρόσβασης ειδικά σε περιβάλλον wordpress, οι λειτουργίες ασφαλείας του λειτουργικού συστήματος διακομιστή windows.
- Να προσδιοριστεί η ασφάλεια που παρέχει το wordpress.
- Να παρουσιαστεί η εγκατάσταση των προγραμμάτων που χρειάζεται για την δημιουργία και λειτουργία ενός ιστολόγιου, και
- Να γίνουν ρυθμίσεις για την ύπαρξη ασφάλειας των δεδομένων και προστασίας των χρηστών του ιστολόγιου.
- Να εξαχθεί συμπέρασμα για το πόσο ασφαλές είναι το wordpress.

1.8 Σχεδιασμός εργασίας, πλάνο υλοποίησης

Η ασφάλεια σε ιστολόγιο σχετίζεται με το θέμα της ασφάλειας πληροφοριών σε εφαρμογές ιστού. Οι περισσότερες επιθέσεις στον ιστό γίνονται σε εφαρμογές ιστού. Αδύναμα σημεία σε εφαρμογές ιστού ήταν υπεύθυνα για παραβιάσεις και διαρροή δεδομένων χρηστών

Για το πρώτο μέρος θα παρουσιαστούν οι κίνδυνοι και οι απειλές που πλήττουν ένα ιστολόγιο καθώς και οι τρόποι αντιμετώπισής τους, με πολιτικές ασφαλείας του λειτουργικού συστήματος και των διακομιστών ιστού και βάσης δεδομένων. Θα βρεθούν πληροφορίες για τις συνέπειες που συνεπάγονται οι απειλές για το σύστημα του ιστολόγιου.

Για το δεύτερο μέρος θα παρουσιαστεί το θέμα της ιδιωτικότητας, και της προστασίας των προσωπικών δεδομένων του χρήστη του ιστολόγιου, θα παρουσιαστούν τα θέματα του έλεγχου πρόσβασης χρηστών, και πιο αναλυτικά η ταυτοποίηση και αυθεντικοποίηση χρήστη με συνθηματικό σε πληροφοριακά συστήματα, και ειδικά σε εφαρμογές web. Θα παρουσιαστεί η κρυπτογραφία στο ιστολόγιο.

Στο τρίτο σημείο θα παρουσιαστεί το σύστημα διαχείρισης περιεχομένου wordpress, που είναι η πιο διαδεδομένη πλατφόρμα κατασκευής ιστολόγιου (blog). Παρουσιάζονται οι δυνατότητές του στη διαχείριση χρηστών και στην προστασία από εξωτερικές απειλές.

Στο τέταρτο μέρος Μετά από εγκατάσταση της σειράς προγραμμάτων XAMPP θα γίνει εγκατάσταση του wordpress και θα παρουσιαστούν οι δυνατότητες προστασίας των προσωπικών δεδομένων, και ελέγχου πρόσβασης χρηστών. Θα εφαρμοστούν πρόσθετα που θα προστατεύουν από spam και άλλες απειλές. Εξετάζεται η χρήση του wordress από πλατφόρμες ιστολόγιων. Οι αδυναμίες τους θα αναφερθούν. Θα γίνει έλεγχος ασφάλειας σε ιστολόγιο που θα εγκατασταθεί σε υπολογιστή με λειτουργικό σύστημα windows, και θα παρουσιαστούν τρόποι για την αντιμετώπιση των αδυναμιών.

Στόχος της εργασίας είναι η παρουσίαση διαχείρισης χρηστών στο wordpress, η παρουσίαση των κινδύνων που αντιμετωπίζει ένα σύστημα ιστολόγιου, ο έλεγχος των αδύνατων σημείων του διακομιστή με εργαλείο auditing, η δημιουργία και διαχείριση χρηστών με διαφορετικά δικαιώματα.

Παραδοτέο	Περιγραφή	Ημερομηνία παράδοσης
Π1.1.	Πρόταση εκπόνησης	21/05/2014
Π1.2	1η έκδοση, κεφάλαια Ειαγωγή,1	25/06/2014
Π1.3	2η έκδοση κεφάλαια εισαγωγή,1,2	13/10/2014
Π1.4	3η έκδοση κεφάλαια εισαγωγή,1,2,3	04/11/2014
ΤΕΛΙΚΗ ΕΚΔΟΣΗ	4η έκδοση κεφάλαια εισαγωγή,1,2,3,4,5	13/02/2015

Πίνακας 1. Συγκεντρωτική περιγραφή παραδοτέων εργασίας

1.9 Δομή της εργασίας

Η παρούσα εργασία περιλαμβάνει 5 κεφάλαια.

Στο Κεφάλαιο 1 γίνεται μία εισαγωγή. Το Κεφάλαιο 2 αναφέρεται στην ασφάλεια σε συστήματα ιστολόγιου όπου αναλύονται οι απαιτήσεις ασφαλείας σε ιστολόγιο, οι κίνδυνοι και χαρακτηριστικά ασφαλείας σε ιστολόγια για βελτίωση της ασφάλειας. Γίνεται

αναφορά στη πλατφόρμα blogger.Το κεφάλαιο 3 αναφέρεται σε ιδιωτικότητα σε συστήματα ιστολόγιου κατά πόσο μπορούν να προστατευθούν τα προσωπικά δεδομένα των ατόμων που χειρίζονται τα ιστολόγια. Στο κεφάλαιο 4 γίνεται περιγραφή Εγκατάστασης ιστολόγιου wordpress. Δημιουργία βάσης δεδομένων και χρηστών Δημοσίευση ανάρτησης. Στο κεφάλαιο 5 αναφέρονται συμπεράσματα για το κατά πόσο το Wordpress αποτελεί ασφαλή πλατφόρμα ιστολόγιου. Στο παράρτημα γίνεται παρουσίαση εγκατάστασης των προγραμμάτων της σειράς XAMPP στα οποία βασίζεται το Wordpress.

ΚΕΦΑΛΑΙΟ 2 - Ασφάλεια σε συστήματα ιστολόγιου

Η ασφάλεια πληροφοριών είναι η εφαρμογή της προστασίας των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διανομή, κατάχρηση, καταγραφή, καταστροφή. Η ασφάλεια εφαρμογών ιστού είναι ένας κλάδος της ασφάλειας πληροφοριών που ασχολείται με την ασφάλεια στους ιστότοπους, τις εφαρμογές ιστού και τις υπηρεσίες ιστού.
Το διαδίκτυο έχει γίνει μέσο διάδοσης κακόβουλου λογισμικού. Το έγκλημα στον ιστό περιλαμβάνει κλοπή ταυτότητας, κατασκοπία, απάτη, συγκέντρωση πληροφοριών. Μία στις 10 ιστοσελίδες μπορεί να περιέχει κακόβουλο κώδικα.[2]

Στην εργασία θα αναλυθούν κίνδυνοι στους οποίους είναι εκτεθειμένο ένα ιστολόγιο και οι χρήστες του. Το wordpress καθώς είναι η βάση εκατομμυρίων Blog στο wordpress.com της automatic, και αποτελεί στόχο για ηθελημένες απειλές. Μία επίθεση θα έχει αποτέλεσμα την απώλεια της εμπιστευτικότητας, της εγκυρότητας ή και της διαθεσιμότητας των διαθέσιμων πληροφοριών. Για παράδειγμα υπάρχει ο κίνδυνος των spam μηνυμάτων με διαφημιστικό, ή άσχετο περιεχόμενο σε σχέση με το ιστολόγιο, κάτι που μπορεί να μειώσει τη διαθεσιμότητα των πληροφοριών του ιστολόγιου. Υπάρχει κίνδυνος κλοπής δεδομένων, μέσω της υποκλοπής κωδικού πρόσβασης στον ιστότοπο¨, με πιθανό αποτέλεσμα να ελαττωθεί η εγκυρότητα των πληροφοριών.

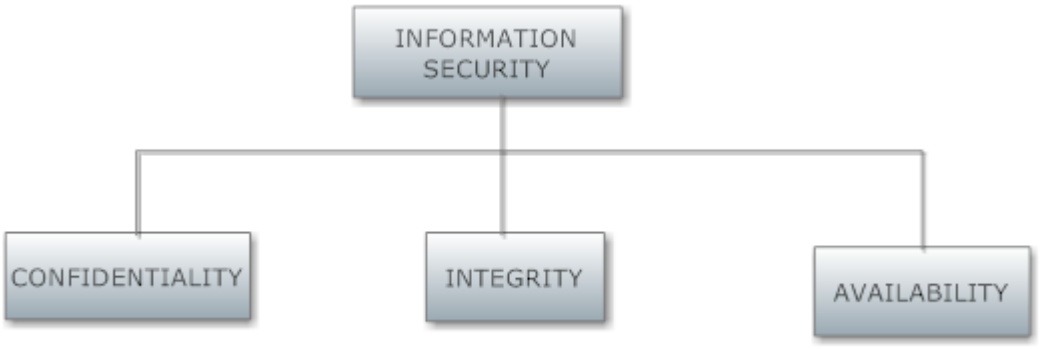
Στην παρούσα εργασία, θα προταθούν μέθοδοι προστασίας του ιστολόγιου από κακόβουλους χρήστες με πρόσθετο του wordpress που εντοπίζει τα μηνύματα spam.

Σύμφωνα με τον κανονισμό 460/2004 του Ευρωπαϊκού Κοινοβουλίου της 10ης Μαρτίου 2004, για τη δημιουργία Ευρωπαϊκού Οργανισμού για την ασφάλεια δικτύων και πληροφοριών, η ασφάλεια ορίζεται ως η δυνατότητα του δικτύου να ανθίσταται, σε συγκεκριμένο επίπεδο εμπιστοσύνης, σε ατυχήματα ή σε παράνομες ή σε κακόβουλες δράσεις οι οποίες θέτουν σε κίνδυνο την αυθεντικότητα την ακεραιότητα τη διαθεσιμότητα και την εμπιστευτικότητα, όσον αφορά τα δεδομένα που έχουν αποθηκευτεί ή μεταδίδονται και τις σχετικές υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω αυτών.
Στα ιστολόγια πραγματοποιείται ανάρτηση δημοσιεύσεων, ώστε να είναι ορατές οι πληροφορίες στο ευρύ κοινό. Έτσι έχουμε επικοινωνία αορίστου αριθμού ατόμων σε κάθε περίπτωση, άρα δεν τίθεται θέμα εμπιστοσύνης γιατί σκοπός του ιστολόγιου είναι η δημοσίευση πληροφοριών. Υπάρχει όμως επικοινωνία που πραγματοποιείται για να γίνει η δημοσίευση του περιεχομένου της σελίδας που πρέπει να είναι προστατευμένη.

2.1 Απαιτήσεις ασφαλείας.

Σε ένα ιστολόγιο υπάρχουν οι απαιτήσεις, να μην μπορεί ο κάθε χρήστης να αλλοιώνει το περιεχόμενο του ιστολόγιου. Κάθε χρήστης του ιστολόγιου μπορεί να δημοσιεύει απαντήσεις σε άλλες αναρτήσεις, χωρίς όμως προσβλητικό ή διαφημιστικό περιεχόμενο. Η ταυτότητα του κάθε blogger προσδιορίζεται από ένα όνομα χρήστη και ένα συνθηματικό, και αποκαλύπτονται δημόσια μόνο τα στοιχεία που επιτρέπει ο ίδιος ο συγγραφέας ιστολογίου. Η απάντηση στην ανάρτηση μπορεί να πρέπει να περιμένει την έγκριση του διαχειριστή. Ο διαχειριστής του ιστολόγιου μπορεί να κάνει παρατηρήσεις και να επιβάλει ποινές αποκλεισμού σε μέλη που παραβαίνουν τους όρους χρήσης του

ιστολόγιου.



Εικόνα 1 Στόχοι της ασφάλειας πληροφοριών

2.1.1 Εμπιστευτικότητα

Η εμπιστευτικότητα (confidentiality) των πληροφοριών προστατεύεται με τη κρυπτογράφηση.

2.1.2 Ακεραιότητα

Η ακεραιότητα (integrity) μπορεί να επιτευχθεί μέσα από τη χρήση αλγορίθμων κατακερματισμού, και ψηφιακών υπογραφών. Ο πίνακας κατακερματισμού είναι ένα σταθερού μήκους αλφαριθμητικό. Υπολογίζεται χρησιμοποιώντας έναν αλγόριθμο κατακερματισμού όπως το MD5. Η τιμή αυτή αποστέλλεται μαζί με τα δεδομένα, όπου ο παραλήπτης μπορεί να υπολογίσει και να συγκρίνει τη τιμή κατακερματισμού με τη τιμή του μηνύματος. Αν οι τιμές διαφέρουν τότε η ακεραιότητα των δεδομένων έχει πληγεί.

2.1.3 Μη αποκήρυξη

Η Μη αποκήρυξη (non repudiation) Είναι μία κατάσταση όπου ο υποτιθέμενος – αναφερόμενος δημιουργός δήλωσης δεν μπορεί να αρνηθεί την ύπαρξη της δήλωσης. Ένας συνδυασμός χρονοσφραγίδας και ψηφιακής υπογραφής θα μπορούσε να χρησιμοποιηθεί για την εξασφάλιση αυτής της δυνατότητας.

2.2 Απειλές

Καθώς τα ιστολόγια είναι εφαρμογές ιστού είναι εκτεθειμένες, θα γίνουν στόχοι ατόμων που θα θελήσουν να έχουν πρόσβαση για διάφορους λόγους. Ένας λόγος είναι να δουν τι μπορούν να βρουν, όπως πληροφορίες για το προσωπικό της επιχείρησης, αριθμούς πιστωτικών καρτών. Ένας δεύτερος λόγος είναι ότι θέλουν να παραποιήσουν πληροφορίες, ή να απορυθμίσουν το σύστημα. Σε αυτή τη περίπτωση ο εισβολέας δεν ενδιαφέρεται να έχει οικονομικό όφελος. Μία άλλη πιθανότητα είναι να θέλει ο εισβολέας να ξεκινήσει επίθεση από τα εκτεθειμένα συστήματα σε άλλα συστήματα ή δίκτυα. Οι υπολογιστές μπορούν να ξεκινήσουν επίθεσης άρνησης υπηρεσίας DOS attacks ή να μεταδώσουν κακοπροαίρετο λογισμικό.
Οι εκτεθειμένες εφαρμογές έχουν να αντιμετωπίσουν απειλές, όπως

2.2.1 Επίθεση Spoofing

Spoofing (εξαπάτηση) είναι η κατάσταση στην οποία το επιτιθέμενο μέρος υποδύεται ένα αξιόπιστο μέρος για να λάβει κάποιο προνόμιο. Κάποια από τα πρωτόκολλα του TCP/IP δεν απαιτούν αυθεντικοποίηση για να επαληθεύουν τον αποστολέα ή το παραλήπτη και έτσι είναι εκτεθειμένα σε επιθέσεις όταν το πρόγραμμα δεν λαμβάνει επιπλέον μέτρα για να επαληθευθεί η ταυτότητα του αποστολέα ή του παραλήπτη διακομιστή. Ασυνεπή στοιχεία σε πακέτα, όπως διεύθυνση αποστολέα και στοιχεία συνόδου μπορεί να είναι ένδειξη τυχαίου ελέγχου scanning στο δίκτυο. Η αντιγραφή στοιχείων ενός αξιόπιστου χρήστη όπως η IP είναι το αντικείμενο της πλαστογράφησης. [4]

2.2.2 SQL injection

Η SQL injection είναι μία μέθοδος που εκμεταλλεύεται αδυναμίες σε διακομιστές ιστού που υποστηρίζονται από βάση δεδομένων. Οι αδυναμίες εμφανίζονται όταν τα δεδομένα που εισάγει ο χρήστης στην ιστοσελίδα δεν φιλτράρονται από χαρακτήρες διαφυγής κατάλληλα, κάτι που μπορεί να επιτρέψει στον επιτιθέμενο να δημιουργήσει προτάσεις που θα ερμηνευτούν ως ενσωματωμένη SQL από το σύστημα, και έτσι να χειραγωγήσει την εφαρμογή που τρέχει στη βάση δεδομένων. Το 2012 η εταιρία ασφαλείας imperva ανακοίνωσε ότι οι εφαρμογές ιστού δέχονται κατά μέσο όρο τέσσερις επιθέσεις το μήνα, με τις περισσότερες να γίνονται στο τομέα των λιανικών πωλήσεων.[7]
Το Μάρτιο του 2014 το πανεπιστήμιο Johns Hopkins ανακοίνωσε επίθεση SQL injection που είχε σαν αποτέλεσμα να εκτεθούν οι πληροφορίες εκατοντάδων φοιτητών και προσωπικού σε ένα εργαστήριό του.

2.2.3 XSS scripting (cross-site scripting)

Η τεχνική cross site scripting εκμεταλλεύεται την δυνατότητα εφαρμογής να δέχεται δεδομένα και κώδικα από τρίτους χρήστες. Ο κώδικας αυτός θα εκτελείται όποτε κάποιος φορτώνει αυτή τη σελίδα. Μία αδυναμία cross site scripting μπορεί να χρησιμοποιηθεί για να παρακάμψει πολιτικές ασφαλείας πρόσβασης όπως τη πολιτική ιδίας προέλευσης

Εικόνα 2 Το σύστημα ασφαλείας του Blogger προειδοποιεί για πιθανή απειλή στη περίπτωση ανάρτησης μέσω άλλου ιστότοπου.

Τα προβλήματα που μπορεί να προκύψουν από αυτή τον τρόπο επίθεσης είναι κλοπή στοιχείων χρηστών μέσω της παραβίασης της συνεδρίας του φυλλομετρητή του χρήστη, παραβίαση της ιδιωτικότητας του θύματος μέσω της παρακολούθησης του ιστορικού περιήγησης του.[3]

2.3 Phising

Το Phising(ψάρεμα) είναι μία προσπάθεια να υποκλαπούν ευαίσθητες πληροφορίες όπως το όνομα το συνθηματικό, αριθμός κάρτας, με την μεταμφίεση σε μία αξιόπιστη οντότητα στην ηλεκτρονική επικοινωνία. Σελίδες που υποδύονται ότι προέρχονται από δημοφιλείς ιστοσελίδες, ιστότοπους δημοπρασιών, τράπεζες, χρησιμοποιούνται για να παγιδέψουν ανυποψίαστο κοινό.

2.4 Επίθεση άρνησης παροχής υπηρεσίας(DoS)

Η άρνηση παροχής υπηρεσίας είναι μία μορφή επίθεσης που στοχεύει στο να σταματήσει η διαθεσιμότητα μίας υπηρεσίας δικτύου ή πόρου στο δίκτυο προς τους χρήστες Οι δράστες των επιθέσεων αυτών στοχεύουν σε ιστοτόπους οργανισμών σε γνωστούς διακομιστές. Μια κοινή μέθοδος επίθεσης είναι ο κορεσμός των γραμμών με requests για επικοινωνία σε τέτοιο βαθμό που να γίνει αδύνατη η εξυπηρέτηση πραγματικής επικοινωνίας, ή να είναι τόσο αργή που να είναι ουσιαστικά αδύνατη.

2.5 Ασφάλεια επικοινωνίας πελάτη διακομιστή

Η ασφάλεια στην επικοινωνία μεταξύ του προγράμματος του πελάτη –client του ιστολόγιου και του διακομιστή είναι σημαντική γιατί μέσω της επικοινωνίας αυτής μεταφέρονται όχι μόνο οι προς δημοσίευση πληροφορίες αλλά και ευαίσθητα δεδομένα όπως η διεύθυνση IP του αποστολέα και η ταυτότητά του. Ο διαχειριστής, και τα μέλη του ιστολόγιου πρέπει να μπορούν να προστατέψουν την ταυτότητά τους όταν το επιθυμούν.
Η σύνδεση στο ιστολόγιο πρέπει να γίνεται από σύνδεση με TLS ή SSL κρυπτογραφικά πρωτόκολλα τα οποία στην ιεραρχία του TCP/IP βρίσκεται στο επίπεδο της εφαρμογής. Τα πρωτόκολλα αυτά βασίζονται σε πιστοποιητικά προτύπου X,509 που υλοποιεί μία ιεραρχική δομή Αρχών πιστοποίησης (Certification Authorities). Έτσι, χρησιμοποιούν αρχικά ασύμμετρη κρυπτογραφία για να αυθεντικοποιήσουν το μέλος με το οποίο επικοινωνούν και να ανταλλάξουν ένα συμμετρικό κλειδί. Η επικοινωνία συνεχίζεται κρυπτογραφημένη με το κλειδί συνόδου.

2.6 Ασφαλές λογισμικό πελάτη διακομιστή

Η πρόσβαση στο διακομιστή γίνεται με φυλλομετρητές(browser) , προγράμματα τα οποία υποστηρίζουν τα πρωτόκολλα ασφαλείας και πρέπει να είναι ενημερωμένα στη τελευταία τους έκδοση ώστε να υποστηρίζουν τις τελευταίες εκδόσεις αυτών. Ο φυλομετρητής παρουσιάζει πληροφορίες για την ασφάλεια της σελίδας που επισκέπτεται, όπως τρόπο κρυπτογράφησης το πιστοποιητικό , από ποια αρχή προέρχεται. Κάποια site χρησιμοποιούν πιστοποιητικά για να ταυτοποιούνται. Αυτή η πληροφορία απαιτείται πρίν το site αρχίσει να κρυπτογραφεί πληροφορίες που μεταδίδονται από και προς τον υπολογιστή του χρήστη, ώστε κανείς να μην μπορεί να διαβάσει τα δεδομένα που στέλνονται. Αν το URL της σελίδας αρχίζει με https:// η σελίδα χρησιμοποιεί πιστοποιητικό .Αν το πιστοποιητικό έχει εκδοθεί από αρχή πιστοποίησης που ο διαχειριστής πιστοποιητικών του υπολογιστή δεν γνωρίζει, ο χρήστης θα ερωτηθεί αν θέλει να δεχθεί το πιστοποιητικό της ιστοσελίδας. Αν ο χρήστης δεχθεί το πιστοποιητικό μιας καινούριας σελίδας, το προσθέτει στη λίστα με τα πιστοποιητικά των ιστοσελίδων.

2.7 Αποδοχή ευθυνών

Οι αναρτήσεις φέρουν το όνομα-ψευδώνυμο που είναι μοναδικό για το κάθε μέλος του ιστολόγιου. Για τους λογαριασμούς των χρηστών πρέπει ο κάθε χρήστης να μην επιτρέπει σε άλλους χρήστες να χρησιμοποιεί τον λογαριασμό του, και πρέπει να υπάρχει μία πολιτική που το επιβάλει αυτό.

2.8 Έλεγχος πρόσβασης στο ιστολόγιο

Η πρόσβαση του χρήστη του διαχειριστή και των μελών του ιστολογίου ελέγχεται από το σύστημα. Σκοπός του ελέγχου είναι να προσδιοριστούν οι πόροι στους οποίους πρέπει να έχει πρόσβαση ο χρήστης του υπολογιστικού συστήματος και ειδικά του ιστολογίου.

Η διαδικασία προσπέλασης περιλαμβάνει τις παρακάτω απαιτήσεις:
Την **ταυτοποίηση (identification)** όπου ο χρήστης αναφέρει την ταυτότητά του και το σύστημα ελέγχου προσπέλασης αναζητεί το χρήστη με αυτή τη ταυτότητα. Απαιτείται να δοθεί από το χρήστη ένα όνομα, ή ένας ταυτοποιητής (user identifier). Τα ονόματα των χρηστών βρίσκονται σε ένα αρχείο της βάσης δεδομένων που χρησιμοποιεί το σύστημα ιστολόγιου.
Την **Αυθεντικοποίηση (authentication)** όπου ο χρήστης επιβεβαιώνει ότι είναι αυτός που ισχυρίσθηκε και το σύστημα ελέγχου προσπέλασης ελέγχει την ορθότητα της επιβεβαίωσης.
Την **εξουσιοδότηση (authorization)** όπου ο χρήστης του ιστολόγιου αποκτά τα δικαιώματα που έχουν προβλεφθεί για αυτόν και το σύστημα ελέγχου επιτηρεί την νομιμότητα των ενεργειών του.
Μέτρα κατά τη διαδικασία προσπέλασης
Κατά την αυθεντικοποίηση υπάρχουν τέσσερις μέθοδοι για να αποδείξει κάποιος την ταυτότητά του. Για να το κάνει αυτό χρησιμοποιεί κάτι που ξέρει, είτε κάτι που έχει, είτε κάτι που αποτελεί μοναδικό ατομικό χαρακτηριστικό του.
Η πρώτη μέθοδος, η χρήση καποιας πληροφορίας που γνωρίζει ο χρήστης, είναι ίσως και η ευκολότερη για χρήση όταν στη διαδικασία αυθεντικοποίησης εμπλέκονται μηχανές. Παραδείγματα σχετικών μέσων αυθεντικοποίησης είναι τα συνθηματικά, τα PINs (Personal Identification Numbers), οι συνθηματικές φράσεις και πληροφορίες σχετικές με το άτομο ή την οικογένεια κάποιου που δεν είναι ευρέως γνωστές.
Τα πλεονεκτήματα της μεθόδου αυτής είναι
Το μέσο αυθεντικοποίησης είναι πάντα στην κατοχή του χρήστη.
Το μέσο αυθεντικοποίησης μπορεί να αλλάξει εύκολα
Η προστασία του μέσου αυθεντικοποίησης είναι σχετικά εύκολη
Το μέσο αυθεντικοποίησης εισάγεται εύκολα στο μηχανισμό αυθεντικοποίησης μέσω πληκτρολογίου χωρίς να υπάρχει ανάγκη προσθήκης εξειδικευμένου υλικού.
Ωστόσο, η μέθοδος έχει και μειονεκτήματα. Το κυριότερο είναι ότι ο αυθεντικοποιημένος χρήστης του συστήματος γνωρίζει κάτι που εύκολα μπορεί να ξεχαστεί, να αντιγραφεί, ή ακόμη και να εικαστεί από κάποιον άλλο μη εξουσιοδοτημένο να το κάνει.. Σε πολλές περιπτώσεις τέτοιου μηχανισμού δεν είναι ιδιαίτερα δύσκολο για κάποιο επιτιθέμενο να μάθει το μέσο αυθεντικοποίησης, απλώς παρακολουθώντας τον εξουσιοδοτημένο χρήστη να το εισάγει στο σύστημα. Επιπλέον δεν απαιτούνται ειδικά εργαλεία, γνώσεις ή μέθοδοι για να αντιγράψει κανείς το μέσο αυθεντικοποίησης. Παρ' όλο που η μέθοδος αυτή είναι σε ευρύτατη χρήση σήμερα σε υπολογιστές, αυτόματες ταπεζικές μηχανές, τηλεφωνικές κάρτες, κτλ., εκτιμάται ως ατελής.
Αφού δώσουμε το όνομα χρήστη και το συνθηματικό μας, ο υπολογιστής θα το συγκρίνει με τις εγγραφές ενός αρχείου χρηστών και συνθηματικών στη βάση δεδομένων. Η σύνδεση θα πετύχει αν δοθεί ένα έγκυρο όνομα χρήστη και το αντίστοιχο επίσης έγκυρο συνθηματικό. Αν όμως το όνομα χρήστη ή το συνθηματικό είναι λαθεμένα η απόπειρα σύνδεσης θα αποτύχει. Συνήθως σε μία τέτοια περίπτωση θα μας ζητηθεί να ξαναπροσπαθήσουμε. Κάποια συστήματα μετρούν τις αποτυχημένες προσπάθειες σύνδεσης για κάθε χρήστη και κλειδώνουν τον αντίστοιχο λογαριασμό όταν το πλήθος

των αποτυχημένων προσπαθειών ξεπεράσει κάποιο καθορισμένο όριο. Στο ιστολόγιο η πρόσβαση κάθε χρήστη γίνεται με χρήση συνθηματικού, που δίνεται από τον διαχειριστή ή από την υπηρεσία βοήθειας- helpdesk.
Εναλλακτικά, μπορούν να εφαρμοστούν μέθοδοι κατοχής αντικειμένου όπως έξυπνη ή μαγνητική κάρτα, ένα κλειδί, ή μία γεννήτρια πρόκλησης απάντησης. Τρίτη μέθοδος είναι η αναγνώριση και επαλήθευση ατομικών χαρακτηριστικών (δακτυλικό αποτύπωμα, ίριδα) [6]

2.9 Πολιτικές ελέγχου προσπέλασης σε ιστολόγιο

Η πολιτική ελέγχου προσπέλασης βασίζεται στην ευαισθησία της πληροφορίας που περιέχεται στο ιστολόγιο και στο βαθμό εμπιστοσύνης που έχουμε στους άλλους χρήστες. Η απόφαση χορήγησης άδειας προσπέλασης, βασίζεται στην σύγκριση του βαθμού εμπιστοσύνης που έχουμε στον χρήστη και της ευαισθησία της πληροφορίας. Η πολιτική αυτή είναι υποχρεωτική για όλους τους χρήστες του συστήματος.
Σε επίπεδο λειτουργικού συστήματος στο διακομιστή, καλό είναι να υπάρχουν διαφορετικοί λογαριασμοί για κάθε χρήστη. Η δυνατότητα ελέγχου λογαριασμού χρήστη UAC των windows 7 επιτρέπει στους διαχειριστές να εισέρχονται στο σύστημα με περιορισμένα δικαιώματα (standard rights) και όταν μια σημαντική αλλαγή πραγματοποιείται όπως εγκατάσταση λογισμικού, απαιτείται επιβεβαίωση και προσωρινά τα δικαιώματα ανεβαίνουν στα δικαιώματα του διαχειριστή. Αν είναι απενεργοποιημένο το UAC μπορεί να δημιουργηθεί ένα δεύτερο account χωρίς πλεονεκτήματα διαχειριστή, για τις μη σημαντικές εργασίες.
Στη δημιουργία χρηστών στο wordpress υπάρχουν κατηγορίες/ρόλοι όπου μπορεί να ενταχθεί ο νέος χρήστης και καθορίζουν πώς μπορεί να αλληλεπιδρά ο χρήστης με το σύστημα, οι κατηγορίες είναι Συνδρομητής, Συνεργάτης Συντάκτης, Αρχισυντάκτης, Διαχειριστής.

- Διαχειριστής (Administrator)- Δεν έχει περιορισμούς έχει πρόσβαση σε όλα τα χαρακτηριστικά διαχείρισης της σελίδας και τα υπόλοιπα χαρακτηριστικά.
- Αρχισυντάκτης (Editor): Μπορεί να διαχειριστεί και να κοινοποιήσει άρθρα δικά του και άλλων.
- Συντάκτης (Author):μπορεί να διαχειριστεί και να κοινοποιήσει δικά του άρθρα.
- Συνεργάτης (Contributor): Κάποιος που μπορεί να γράψει άρθρα αλλά δεν μπορεί να τα δημοσιεύσει.
- Συνδρομητής (Subscriber) : Κάποιος που μπορεί να διαχειριστεί μόνο το δικό του προφίλ και να διαβάσει αναρτημένα μυνήματα..

2.9.1 Διαχειριστής

Ο διαχειριστής είναι η ανώτερη βαθμίδα χρήστη, Οι δυνατότητες του διαχειριστή περιλαμβάνουν όλες τις δυνατότητες και επιπλέον

Διαχείριση του δικτύου,

Διαχείριση των ιστότοπων,

Διαχείριση των χρηστών,

Διαχειριστεί τα πρόσθετα(plug-ins) των ιστότοπων,

Διαχείριση των θεμάτων (themes) του ιστότοπου,

Διαχείριση τις επιλογές του δικτύου.

2.9.2 Αρχισυντάκτης

Οι σημαντικότερες δυνατότητες του αρχισυντάκτη περιλαμβάνουν :

Ενεργοποίηση προσθέτων,

Διαγραφή αναρτήσεων ιδιωτικών και δημοσιευμένων,

Επεξεργασία αναρτήσεων, σελίδων άλλων χρηστών

Ανάγνωση ιδιωτικών άρθρων,

Διαχείριση κατηγοριών,

Αναβάθμιση χρηστών.

Δημοσίευση σελίδων και αναρτήσεων

2.9.3 Συντάκτης

Οι δυνατότητες του συντάκτη του επιτρέπουν:

Διαγραφή σελίδων άλλων

Διαγραφή άρθρων, σελίδων, αναρτημένων ή μη αναρτημένων

Συντάσσει και να επεξεργάζεται σελίδες και άρθρα, δημοσιευμένα ή μη δημοσιευμένα

Διαβάζει και δημοσιοποιεί άρθρα,

Γράφει HTML σε σολίδες και σχόλια,

Ανεβάζει αρχεία.

2.9.4 Συγγραφέας

Διαγράφει, επεξεργάζεται άρθρα, δημοσιευμένα ή μη δημοσιευμένα.

Ανάγνωση των αναρτήσεων.

Ανεβάζει αρχεία.

2.9.5 Συνδρομητής

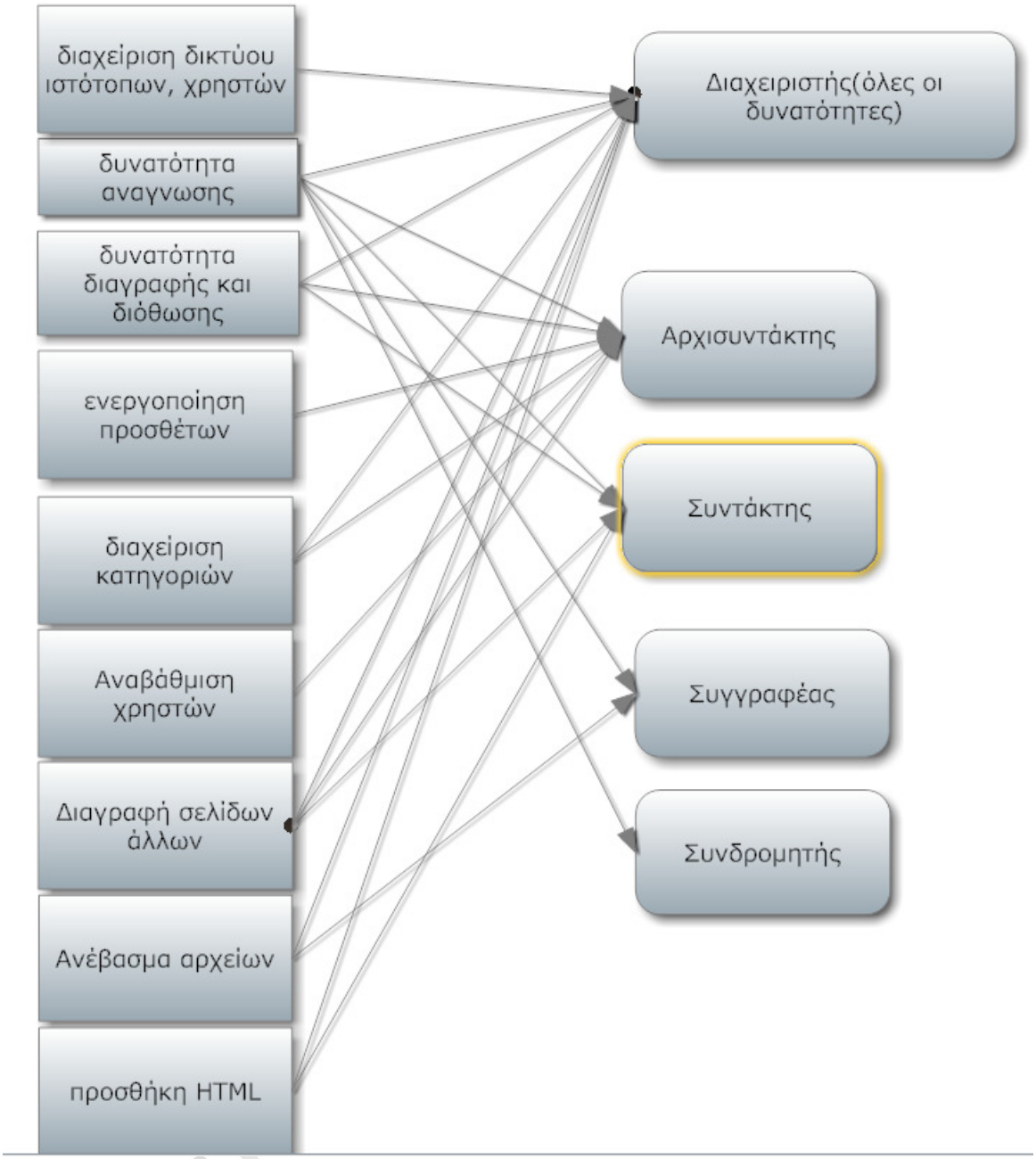
Ο συνδρομητής έχει δυνατότητα να κάνει

Ανάγνωση των αναρτήσεων.

[5]

Κάθε επίπεδο ενσωματώνει τα δικαιώματα των κατωτέρων επιπέδων και χαρακτηρίζεται από νέα δικαιώματα. Ο νέος χρήστης ξεκινάει από το κατώτερο επίπεδο και μπορεί να αναβαθμιστεί στη συνέχεια από το διαχειριστή.

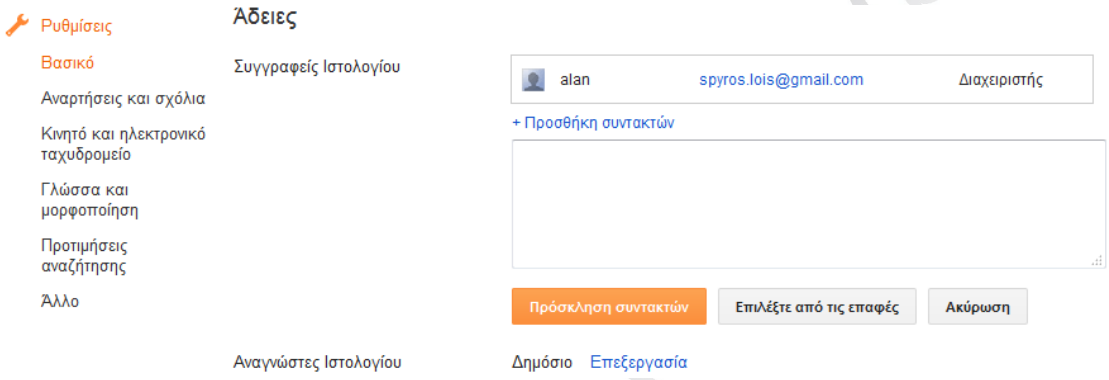
Συνοπτικά τα δικαιώματα των ρόλων εμφανίζονται ατην παρακάτω εικόνα



Εικόνα 2 α δικαιώματα ρόλων σε ιστολόγιο.

2.10 Ελεγχος πρόσβασης στο blogger.

Στο blogger, τη πλατφόρμα ιστολόγιων της google, κάθε χρήστης που έχει λογαριασμό google έχει δικαίωμα να δημιουργήσει ιστολόγιο στο οποίο θα είναι διαχειριστής και να ξεκινήσει να δημοσιοποιεί μηνύματα ιστολόγιου και σελίδες. Το ιστολόγιο θα έχει κατάληξη .blogspot.com. Επίσης έχει δικαίωμα να γράφει σχόλια σε αναρτήσεις άλλων ιστολόγιων στην ίδια πλατφόρμα. Ο ιδιοκτήτης του ιστολόγιου είναι ο διαχειριστής και έχει δικαίωμα να καλέσει άλλα άτομα της εμπιστοσύνης του για να γίνουν συντάκτες στο δικό του ιστολόγιο.



Εικόνα 2β οι άδειες στο blogger ορίζονται από το μενού ρυθμίσεις, επιλογή βασικό.

Με τον έλεγχο πρόσβασης το σύστημα ιστολόγιου προστατεύεται από προσπάθειες πρόσβασης μη εξουσιοδοτούμενων ατόμων, ή από χρήστες του ιστολογίου που προσπαθούν να αποκτήσουν προνόμια που δεν τους έχουν εκχωρηθεί. Η αδυναμία σε αυτό το σημείο είναι οι επιθέσεις ωμής δύναμης (brute force attack) που μπορούν να γίνουν με αυτοματοποιημένο τρόπο και να δοκιμάζουν πολλά συνθηματικά και ονόματα. Τρόποι προστασίας είναι η χρησιμοποίηση περίπλοκων συνθηματικών και η χρήση χρονικού περιορισμού στην διαδικασία πρόσβασης

ΚΕΦΑΛΑΙΟ 3 - ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΕ ΣΥΣΤΗΜΑΤΑ ΙΣΤΟΛΟΓΙΟΥ

3.1 Ορισμός ιδιωτικότητας

Ιδιωτικότητα είναι η προστασία του ατόμου από την αναρμόδια κοινοποίηση πληροφοριών που τον αφορούν. Ο νόμος προστατεύει το πολίτη από προσβολή της προσωπικότητάς του.
Το 2011 η Επιτροπή για την Αντιμετώπιση του Ηλεκτρονικού Εγκλήματος του υπουργείου Δικαιοσύνης πρότεινε κατά πλειοψηφία τη προώθηση διατάξεων σε υπό κατάθεση νομοσχέδιο για άρση του απορρήτου για όλα τα κακουργήματα, αλλά και για τα πλημμελήματα για τα οποία ο νόμος προβλέπει ποινή φυλάκισης τουλάχιστον τριών μηνών.

Στο επίκεντρο του προβληματισμού πάντως και του υπουργείου Δικαιοσύνης είναι επί της ουσίας ο κατάλογος των εγκλημάτων για τα οποία θα επιτρέπεται η άρση του απορρήτου των επικοινωνιών και η ταυτοποίηση των διαχειριστών των blogs στις περιπτώσεις που οι αρμόδιοι διαπιστώνουν, με απτά στοιχεία και πέρα από κάθε αμφιβολία, ότι διαπράττεται συγκεκριμένο αδίκημα το οποίο διώκεται από το Ποινικό μας Δίκαιο.

3.2 Πολιτική ιδιωτικότητας στα συστήματα ιστολόγιου

Ο χρήστης του ιστολόγιου αποδέχεται τη πολιτική του ιστολόγιου που περιγράφονται σε ξεχωριστή σελίδα του ιστολόγιου, με λεπτομέρειες για το πώς η υπηρεσία που έχει το ιστολόγιο θα συλλέγει , θα μεταδίδει και θα χρησιμοποιεί τη προσωπική πληροφορία:
Πριν ή κατά τη διάρκεια της συλλογής προσωπικών πληροφοριών το ιστολόγιο θα ταυτοποιεί τους σκοπούς για τους οποίους η πληροφορία θα συλλέγεται.
Θα συλλέγουμε και θα χρησιμοποιούμε πληροφορίες μόνο με σκοπό να εκπληρώσουμε τους σκοπούς που περιγράφονται από εμάς ή από άλλους συμβατούς σκοπούς, εκτός αν αποκτήσουμε τη συγκατάθεση του ενδιαφερόμενου ατόμου, όπως ορίζει ο νόμος.
Θα παρακρατήσουμε προσωπικές πληροφορίες μόνο για όσο χρονικό διάστημα χρειάζεται για την εκπλήρωση αυτών των σκοπών.
Θα συλλέγουμε προσωπικές πληροφορίες με νόμιμα και δίκαια μέσα και όπου είναι εφικτό με την συγκατάθεση του ενδιαφερόμενου.
Η χρήση της υπηρεσίας ιστολόγιων υπόκειται στους Ελληνικούς και Διεθνείς νόμους, στους εθιμικούς κανόνες του Διαδικτύου, καθώς επίσης και στα χρηστά ήθη.
Το ιστολόγιο ουδεμία ευθύνη, άμεση ή έμμεση, φέρει για τυχόν (θετική ή αποθετική) ζημία του επισκέπτη από τη χρήση της υπηρεσίας ή/και των στοιχείων που περιέχονται σ" αυτήν.
Το ιστολόγιο δεν ευθύνεται για τυχόν ζημία που μπορεί να προκληθεί από τη χρήση συνδέσμων (links) προς άλλους δικτυακούς τόπους καθώς και για τις πληροφορίες που μπορεί να περιλαμβάνονται στις δικτυακές σελίδες της υπηρεσίας Εκπαιδευτικών Κοινοτήτων και ιστολόγιων. Επίσης, το Πανελλήνιο Σχολικό Δίκτυο δεν φέρει καμία ευθύνη για το περιεχόμενο των σελίδων προς τις οποίες διατηρεί συνδέσμους, ούτε είναι υπεύθυνο για την πολιτική ασφαλείας άλλων κόμβων, καθώς και για τον τρόπο διαχείρισης των ηλεκτρονικών επισκεπτών τους.
Τα άρθρα που φιλοξενούνται στο ιστολόγιο εκφράζουν αποκλειστικά και μόνο την άποψη των δημιουργών τους.
το μέλος του ιστολογίου πρέπει να φροντίσει ώστε:- Τα στοιχεία και το περιεχόμενο των άρθρων και των σχολίων που αναρτά στην υπηρεσία να μην προσβάλλουν, δυσφημούν ή υβρίζουν άλλα μέλη του Πανελλήνιου Σχολικού Δικτύου, άλλους επισκέπτες του

δικτυακού τόπου και του Διαδικτύου γενικότερα, καθώς επίσης να ακολουθούν τους νόμους τα χρηστά ήθη και τα ήθη χρήσης του Διαδικτύου.
Να έχει καταβάλει επαρκείς προσπάθειες απομάκρυνσης ιών (viruses) ή άλλων κακόβουλων στοιχείων που μπορούν να βλάψουν τον δικτυακό τόπο της υπηρεσίας ή άλλους χρήστες του Διαδικτύου.
Τα στοιχεία να μην είναι αλλοιωμένα από το μέλος που κάνει την δημοσίευση ή εν γνώσει του από άλλους.

3.3 Άρση απορρήτου στις επικοινωνίες

Το σύνταγμα ορίζει ότι η άρση του απορρήτου της επικοινωνίας είναι θεμιτή για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαιτέρως σοβαρών εγκλημάτων.

3.4 Άρση απορρήτου στο διαδίκτυο και στα ιστολόγια

Στην συγκεκριμένη περίπτωση το απόρρητο επικοινωνίας δεν καλύπτει το περιεχόμενο του μηνύματος διότι αυτό είναι ήδη δημοσιευμένο, αλλά τα εξωτερικά στοιχεία επικοινωνίας. Στην έννοια των εξωτερικών στοιχείων επικοινωνίας περιλαμβάνονται οι διευθύνσεις IP, τα ηλεκτρονικά ίχνη που βοηθούν στην ταυτοποίηση του χρήστη με τον εξοπλισμό του, όπως είναι το Mac Address του modem/router. Τα στοιχεία αυτά πρέπει να διατηρούνται υποχρεωτικά. Αυτό σημαίνει ότι η διάθεση των στοιχείων για την ταυτοποίηση των bloggers επιτρέπεται .
Συχνά παρατηρείται bloggers να έχουν δυσφημήσει/ απειλήσει κάποιον τρίτο. Σε αυτήν την περίπτωση μπορεί να ζητηθεί από την εταιρία που φιλοξενεί το blog να αφαιρέσει τα σχόλια ή τις δημοσιεύσεις με δυσφημιστικό/ απειλητικό περιεχόμενο.
Σύμφωνα με τη γνωμοδότηση του εισαγγελέα του Αρείου Πάγου για την επικοινωνία μέσω Internet «δεν συντρέχει δικαιολογητικός λόγος προστασίας του απορρήτου» στις περιπτώσεις που αναρτούν υβριστικά, απειλητικά ή εκβιαστικά δημοσιεύματα. Ο πάροχος υπηρεσιών διαδικτύου ο οποίος διαθέτει εγκαταστάσεις διαδικτύου υποχρεούται να έχει τα πλήρη στοιχεία ταυτότητας των χρηστών πελατών του(ονοματεπώνυμο, διεύθυνση, ιστοσελίδα) καθώς και τον τρόπο πρόσβασής τους.
Κάθε πρόσβαση του χρήστη στο διαδίκτυο καταγράφεται στις εγκαταστάσεις του ISP στο επίπεδο του δικτύου (πακέτα IP).Με τη διάταξη μπορεί να επιτραπεί η εξέταση του περιεχομένου των πακέτων προκειμένου να αποκαλυφθούν χρήσιμες πληροφορίες σχετικά με τις ενέργειες του χρήστη στο διαδίκτυο όπως.
-επισκεπτόμενες διευθύνσεις
-χρησιμοποιούμενες υπηρεσίες
-περιήγηση σε ιστοσελίδες και βάσεις πληροφοριών

3.4.1 Απειλές για την ιδιωτικότητα

Τα cookies είναι δεδομένα που στέλνονται από την ιστοσελίδα και αποθηκεύονται στο φυλλομετρητή του χρήστη ενώ αυτός επισκέπτεται την ιστοσελίδα. Κάθε φορά που ο χρήστης επισκέπτεται την ιστοσελίδα, ο φυλλομετρητής αποστέλλει το cookie στην ιστοσελίδα για να ενημερώσει για την δραστηριότητα του χρήστη.
Τα cookies είναι σχεδιασμένα να αποθηκεύουν πληροφορίες για το χρήστη όπως τα αντικείμενα σε ένα καλάθι αγορών, ή να καταγράφουν το ιστορικό φυλλομετρητή, και στοιχεία σύνδεσης όνομα χρήστη και συνθηματικά δυνατότητα tracking cookie να συλλέγουν δεδομένα, ώθησε ευρωπαίους και αμερικανούς νομοθέτες να δράσουν το 2011. Από το 2012 και μετά, ο ιστότοπος που χρησιμοποιεί cookies πρέπει να πάρει την συγκατάθεσή του χρήστη για να αποθηκεύσει αρχεία cookies στον υπολογιστή του. Ο χρήστης πρέπει να μπορεί να αρνηθεί τη χρήση cookies. Στην δήλωση ιδιωτικότητας πρέπει να περιγράφεται τι πληροφορίες αποθηκεύονται σε cookies και για ποιο λόγο.
[5]
Web crawlers Οι μηχανές αναζήτησης διαθέτουν software που τους επιτρέπει να ανανεώνουν τα περιεχόμενα που έχουν από τις σελίδες στο internet. Ο web crawler

μπορεί να αντιγράψει το περιεχόμενο της κάθε ιστοσελίδας και να το κατηγοριοποιήσει ώστε η αναζητήσεις να γίνονται πολύ γρήγορα. Οι web crawlers των μεγάλων μηχανών αναζήτησης αποθηκεύουν μεγάλο μέρος των ιστοσελίδων, και αυτό δημιουργεί θέματα ως προς την προστασία της ιδιωτικότητας των ανθρώπων στους οποίους αφορούν τα δεδομένα. Οι δημιουργοί περιεχομένου έχουν την απαίτηση να μην αποθηκεύονται τα δεδομένα τους για μεγάλο χρονικό διάστημα κάπου που δεν έχουν δώσει συγκατάθεση, να μην γίνεται μεγάλης κλίμακας ψάξιμο στις σελίδες τους και να μην συνδέονται τα δεδομένα τους με βάσεις δεδομένων. Έτσι πρέπει να υπάρχει ένας περιορισμός, στις ιστοσελίδες που να θέτει κανόνες στις μηχανές αναζήτησης και να τις εμποδίζει να λάβουν δεδομένα από την κάθε ιστοσελίδα αν ο δημιουργός της το επιθυμεί. Το αρχείο robots.txt είναι το αρχείο που η μηχανή αναζήτησης διαβάζει για να βρει τους κανόνες και τους περιορισμούς που επιβάλλονται από τον ιστότοπο για τις μηχανές αναζήτησης. [9]

Για παράδειγμα το
User-agent: Googlebot-Image
Disallow: /
Θα εμποδίσει το crawler της google που ψάχνει εικόνες να έχει πρόσβαση στον ιστότοπο.
Το επόμενο παράδειγμα εμποδίζει μηχανές να έχουν πρόσβαση σε επιλεγμένες θέσεις του ιστότοπου.

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /privatedir/
Disallow: /tutorials/blank.htm
```

[10]

3.4.2 Προστασία ιδιωτικότητας με χρήση διακομιστή proxy

Ο ανώνυμος διακομιστής proxy είναι ένα εργαλείο με το οποίο η δραστηριότητα στο διαδίκτυο γίνεται μυστική. Ένας ενδιάμεσος υπολογιστής χρησιμοποιείται για να προστατέψει τα στοιχεία πρόσβασης μεταξύ του υπολογιστή πελάτη και του διαδικτύου. Πραγματοποιεί πρόσβαση στο διαδίκτυο για λογαριασμό του χρήστη προστατεύοντας προσωπικές πληροφορίες, κρύβοντας τα στοιχεία πρόσβασης του υπολογιστή πελάτη, το IP και το MAC.Ο ανώνυμος διακομιστής proxy μπορεί να χρησιμοποιηθεί για την προστασία της ταυτότητας, ή για τη προστασία του ιστορικού αναζήτησης από δημόσια αποκάλυψη.

Η εταιρία anonymizer είναι μία ιδιωτική εταιρία ασφαλείας που ιδρύθηκε το 1995 από τον Lance Cottrell.. Ο anonymizer δημιουργεί μία VPN σύνδεση μεταξύ των διακομιστών και του υπολογιστή του χρήστη, δημιουργώντας μία τυχαία διεύθυνση IP αντί για τη πραγματική που χρησιμοποιείται. Αυτό μπορεί να χρησιμοποιηθεί για να διατυπωθεί ανώνυμα μία καταγγελία, να αποφευχθεί η λήψη διαφημιστικού ή προσβλητικών μηνυμάτων να αποφευχθεί η λογοκρισία στο διαδίκτυο και να κρατηθεί μυστική η ταυτότητα του χρήστη. Δεν υπάρχει ανθρώπινη παρέμβαση στη λειτουργία του anonymizer, δεν τηρούνται αρχεία καταγραφής και έτσι η χρήση είναι ανώνυμη.

3.5 Νομικό πλαίσιο προστασίας δεδομένων στα ιστολόγια

Όσον αφορά τα blogs, η ΑΔΑΕ (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών) αναφέρεται στην υπάρχουσα ελληνική νομολογία η οποία έχει αποδεχθεί ότι το ιστολόγιο είναι μέσο επικοινωνίας αορίστου αριθμού προσώπων και το γεγονός ότι ο κάτοχος-

διαχειριστής του ιστολόγιου δεν υποχρεούται να χρησιμοποιεί τα αληθινά στοιχεία του αλλά δύναται να εμφανίζεται στους αναγνώστες του χρησιμοποιώντας ψευδώνυμο

Ειδικά για την περίπτωση των ιστοσελίδων ή των ιστολόγιων επισημαίνεται ότι δεν πρέπει να συγχέεται η δημοσιοποίηση του περιεχομένου τους στο ευρύ κοινό που χαίρει της προστασίας του άρθρου 14 του Συντάγματος με την επικοινωνία που πραγματοποιείται ώστε να δημοσιευθεί το περιεχόμενο της ιστοσελίδας ή να πραγματοποιηθεί η πρόσβαση τρίτων σε αυτήν. Αυτή η επικοινωνία προστατεύεται από το απόρρητο των επικοινωνιών σύμφωνα με το άρθρο 19.

[11]

Οι γνωμοδοτήσεις καταλήγουν συμπερασματικά ότι «οι αρμόδιες δικαστικές αρχές μπορούν να ζητούν από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να τους γνωρίσουν τα στοιχεία εντοπισμού των προσώπων που τελούν διάφορα εγκλήματα (εκβίαση, δυσφήμηση, απειλή, εξύβριση κ.τ.λ.) με κακόβουλες κλήσεις ή μηνύματα ή μέσω Διαδικτύου, χωρίς να τηρούν την προβλεπόμενη διαδικασία άρσεως του απορρήτου».[17]

Επομένως μπορούμε να πούμε ότι δεν υπάρχει προστασία απορρήτου στα ιστολόγια καθώς ο πάροχος υποχρεώνεται στην αποκάλυψη των στοιχείων του δημιουργού του ιστολόγιου.

3.6 Ένα μοντέλο για την ασφαλή διατήρηση της επικοινωνίας

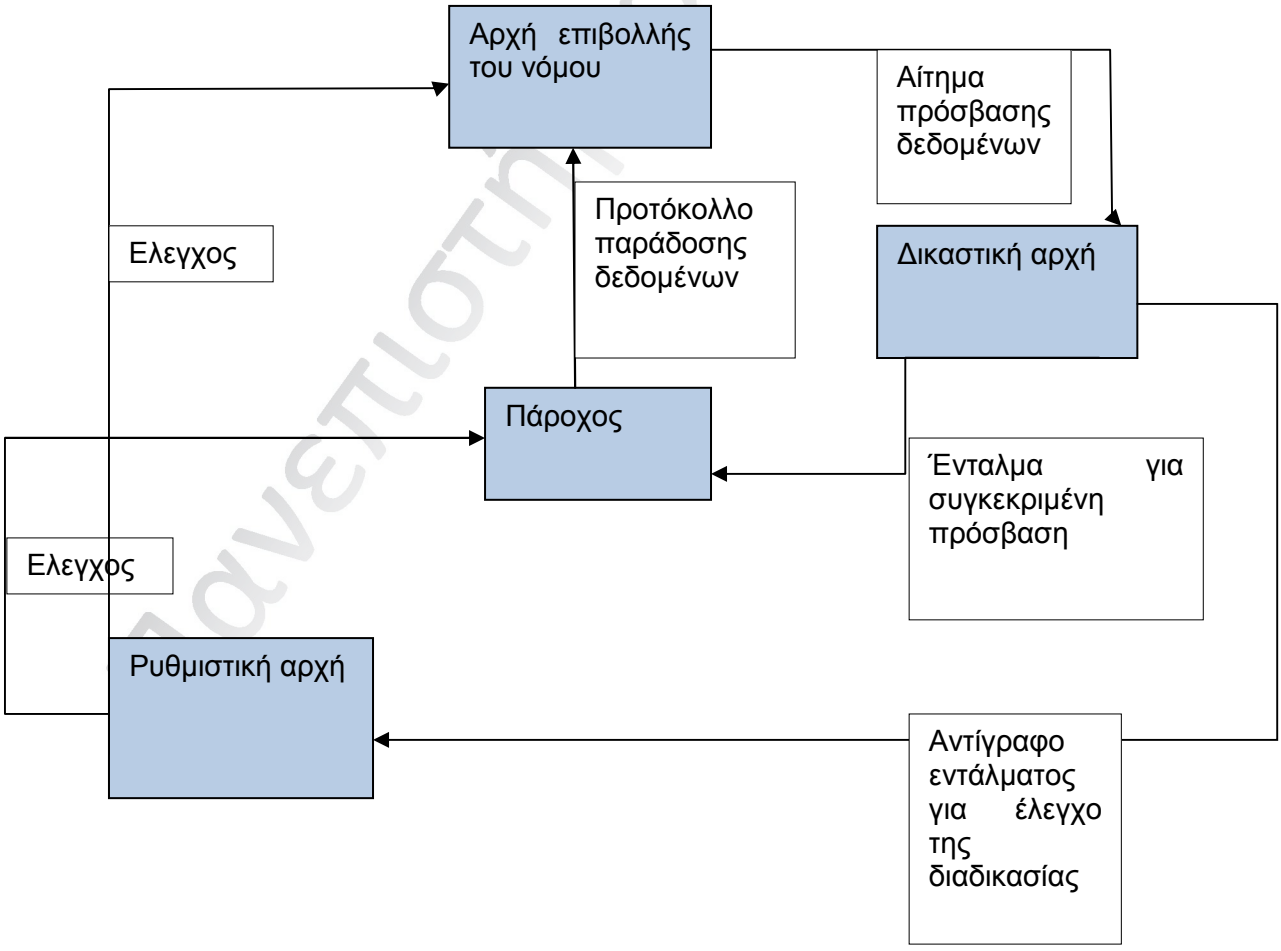
Το σχήμα που προτείνεται αποτελείται από

1)Τον πάροχο, είτε πρόκειται για πάροχο υπηρεσίας internet είτε το πάροχο του server στο οποίο βρίσκεται η εφαρμογή. Ο πάροχος πρέπει να φροντίζει για την ασφαλή διατήρηση των δεδομένων, και την εφαρμογή των πρωτοκόλλων ασφαλείας στις επικοινωνίες που χρησιμοποιούν οι συνδρομητές του.

2)Αρχή επιβολής νόμου που λαμβάνει καταγγελίες να τις αξιολογεί διεξάγει έρευνα για εντοπισμό παράνομης και εγκληματικής δράσης, και να κάνει το αίτημα για άρση απορρήτου προς τη δικαστική αρχή όταν αυτό κρίνεται απαραίτητο.

3)Τη δικαστική αρχή που δέχεται αίτημα από αστυνομική στρατιωτική ή πολιτική αρχή, το αξιολογεί με βάση το νόμο και εκδίδει ένταλμα για να αρθεί το απόρρητο των επικοινωνιών.

4)Την ρυθμιστική αρχή που επιβλέπει και ελέγχει για τη σωστή λειτουργία των διαδικασιών για την άρση του απορρήτου.[12]



ΚΕΦΑΛΑΙΟ 4 - ΕΓΚΑΤΑΣΤΑΣΗ ΛΕΙΤΟΥΡΓΙΑ WORDPRESS

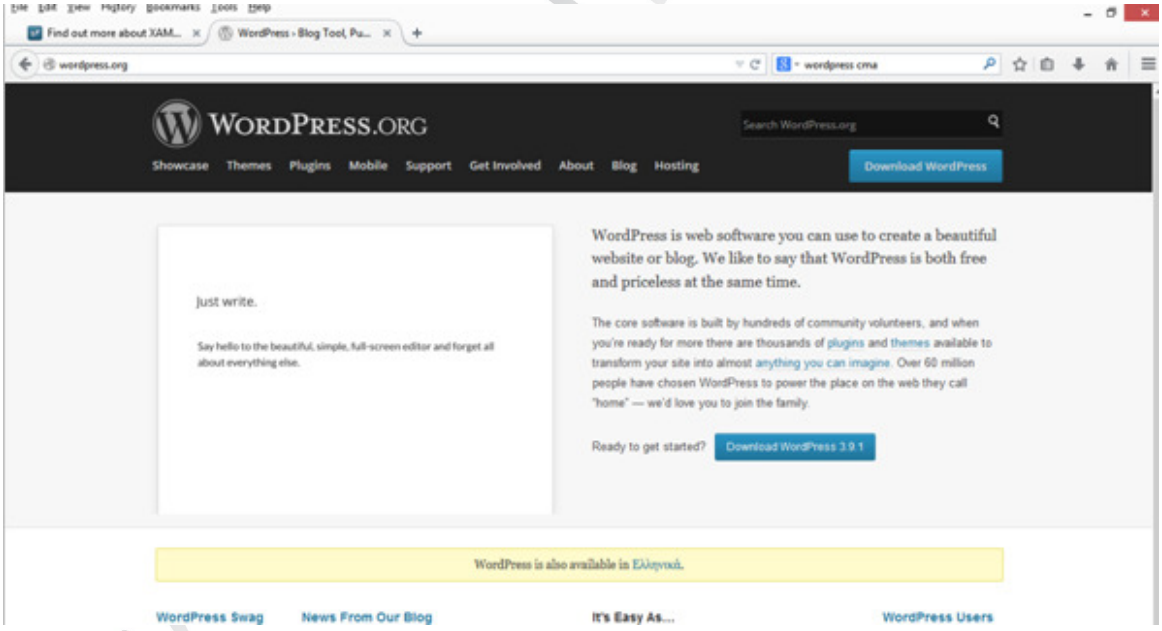
4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εγκαταστήσω ένα Wordpress ιστολόγιο με θέμα τη τεχνολογία και θα δημιουργήσω έναν επιπλέον χρήστη. Ο κάθε χρήστης έχει τα δικαιώματά του. Ο διαχειριστής δημιουργείται κατά την εγκατάσταση και έχει γενική πρόσβαση .Ο νέος χρήστης είναι συνδρομητής, μπορεί να συνδέεται στο ιστολόγιο και να διαβάζει. Οι δύο χρήστες έχουν ξεχωριστό κωδικό και δεν έχει ο ένας πρόσβαση στο λογαριασμό του άλλου. Ο εξωτερικός αναγνώστης μπορεί να δει τα στοιχεία ταυτότητας που ο κάθε χρήστης έχει επιλέξει να φαίνονται.

4.2 Εγκατάσταση Wordpress

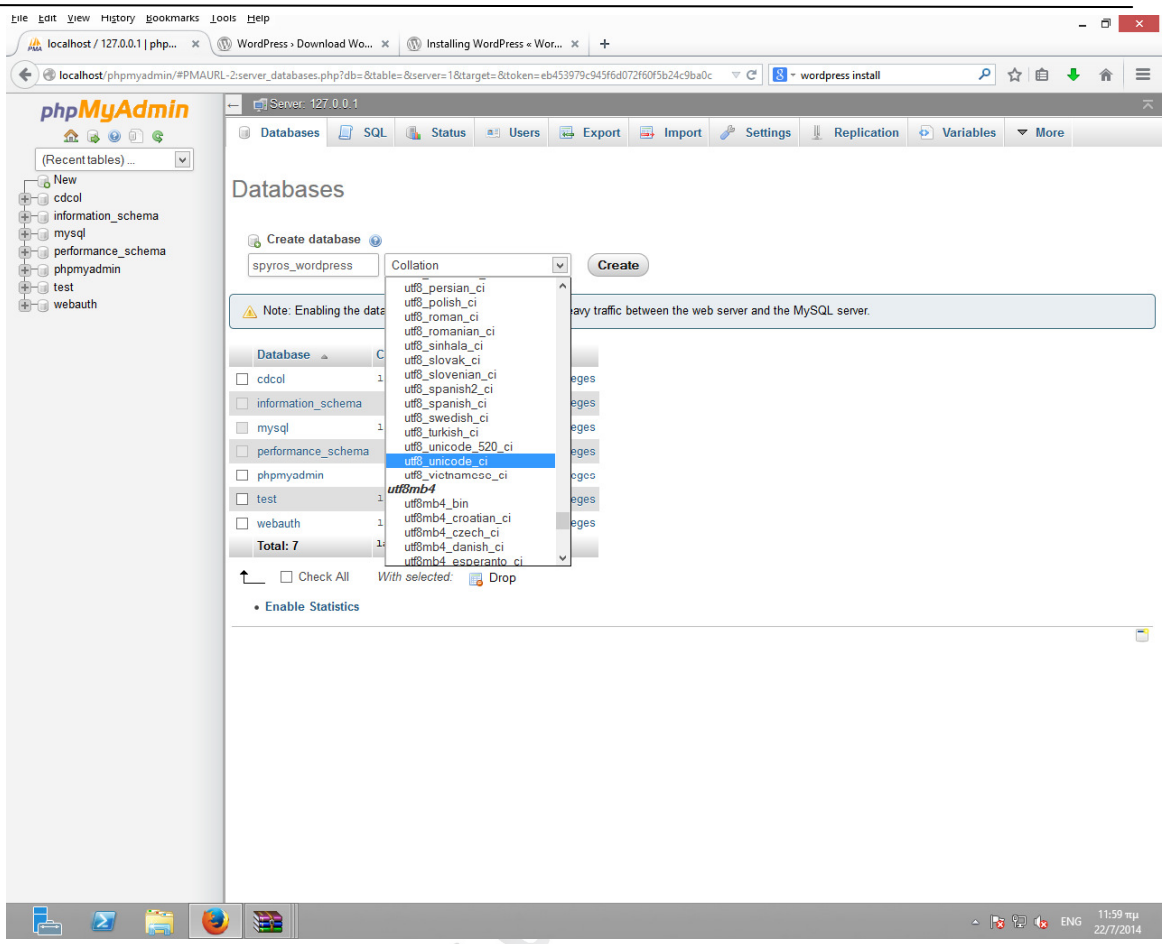
Έχοντας ήδη εγκαταστήσει τη στοίβα προγραμμάτων XAMPP (με τη διαδικασία που βρίσκεται στο παράρτημα) προχωράμε στην εγκατάσταση του Wordpress

Από το ιστότοπο της πλατφόρμας κατεβάζουμε τη τελευταία διαθέσιμη σταθερή έκδοση[14]



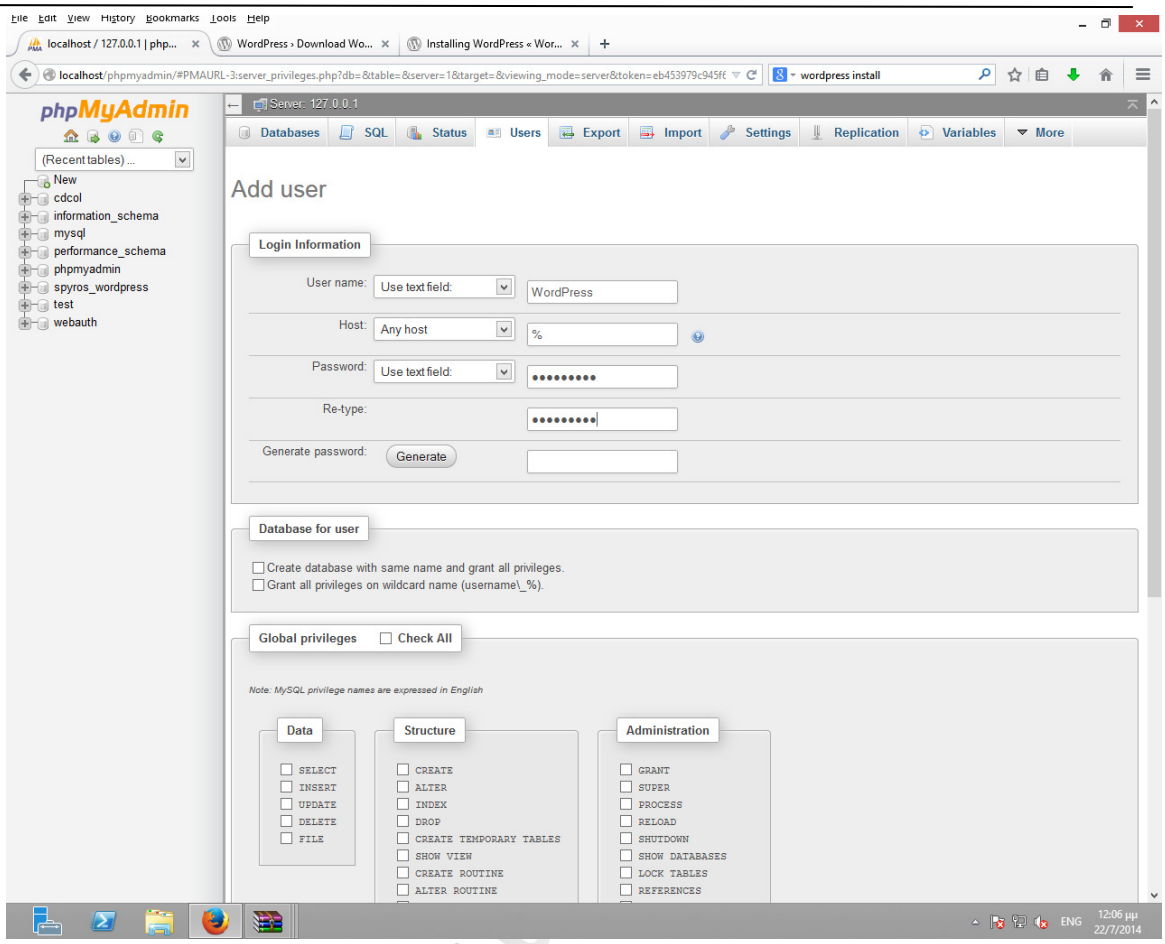
Εικόνα 1 wordpress.org

Αποσυμπιέζουμε το αρχείο στο κατάλογο htdocs του XAMPP και μέσω του phpMyAdmin κατασκευάζουμε τη βάση δεδομένων που θα χρησιμοποιηθεί.



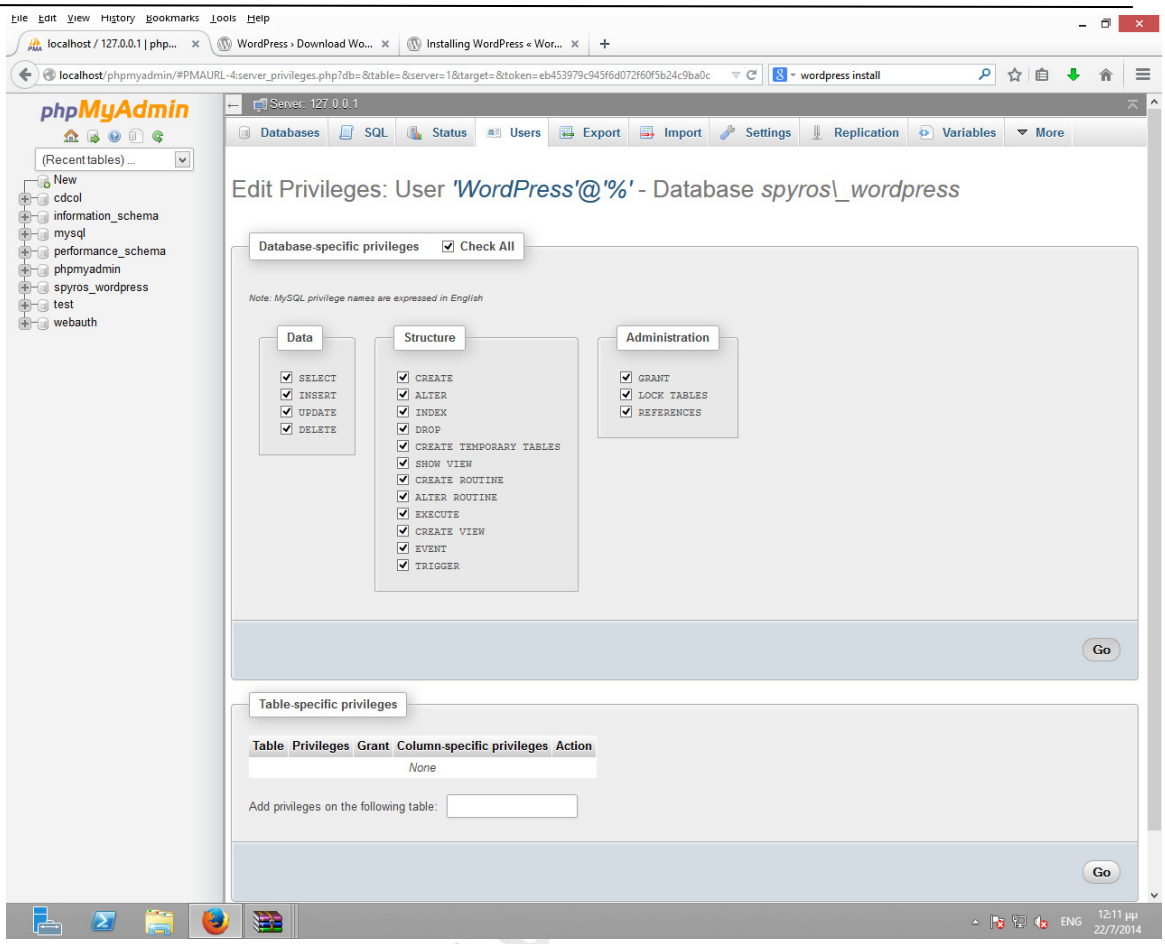
Εικόνα 2 Δημιουργία βάσης δεδομένων για το ιστολόγιο

Δημιουργούμε χρήστη για τη διαχείριση του ιστολόγιου, επιλέγουμε συνθηματικό και αφήνουμε τις προεπιλεγμένες ρυθμίσεις.



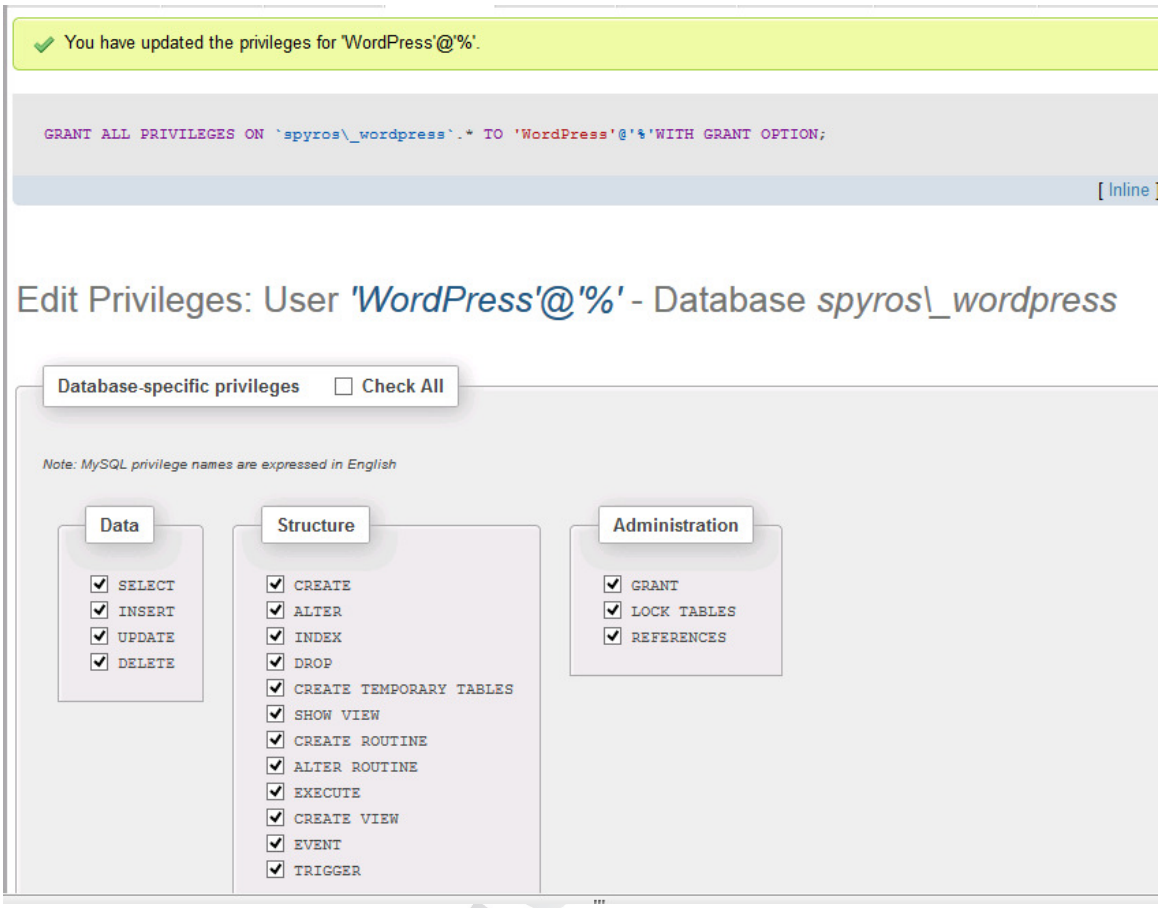
Εικόνα 3 Δημιουργία χρήστη/Διαχειριστή

Στην οθόνη χρηστών επιλέγουμε το χρήστη που δημιουργήσαμε και με την επιλογή add privileges και στην οθόνη add privileges επιλέγουμε τη βάση που φτιάξαμε και όλα τα προνόμια.

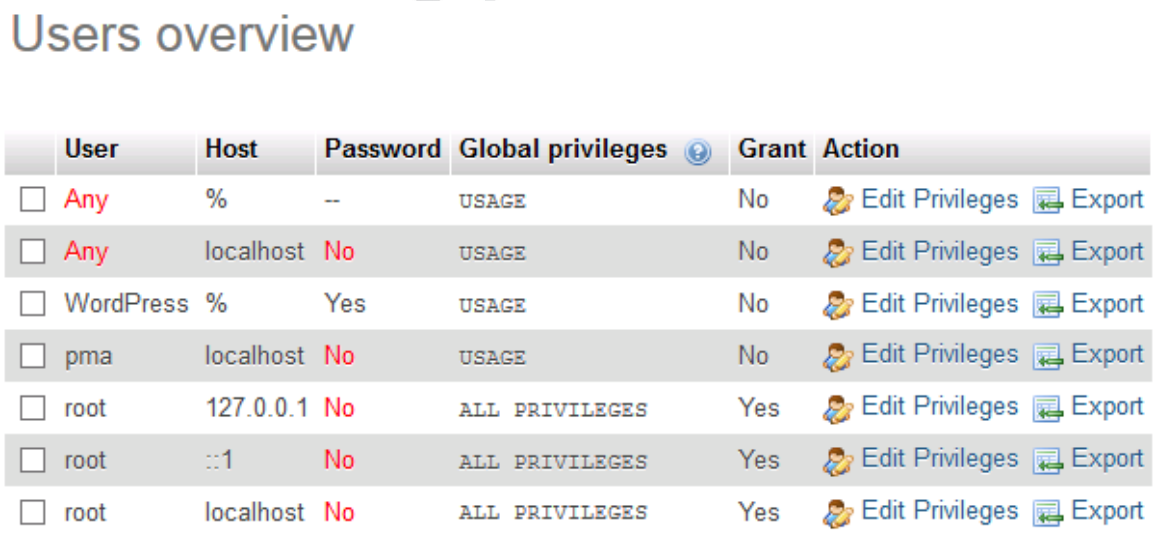


Εικόνα 4 Επιλέγοντας go θα ολοκληρωθεί η εκχώρηση των δικαιωμάτων στο χρήστη WordPress.

Ο χρήστης WordPress θα είναι διαχειριστής και επιπλέον θα έχει δικαιώματα στην βάση δεδομένων του ιστολόγιου.



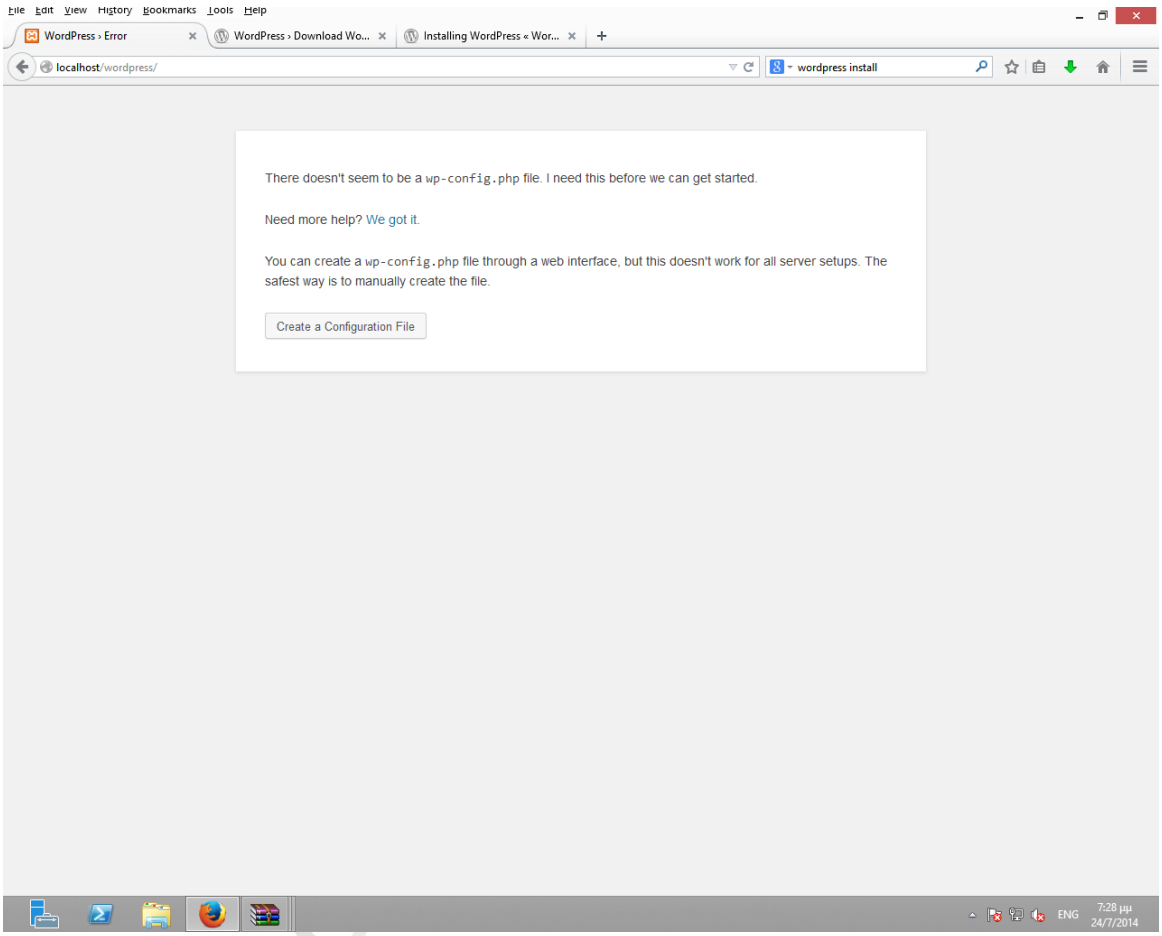
Εικόνα 5 Εκχώρηση δικαιωμάτων στον διαχειριστή



Εικόνα 6 χρήστης βρίσκεται στη σύνοψη χρηστών

Βλέπουμε ότι δημιουργήθηκε ο χρήστης και βρίσκεται στη σύνοψη χρηστών – users overview.

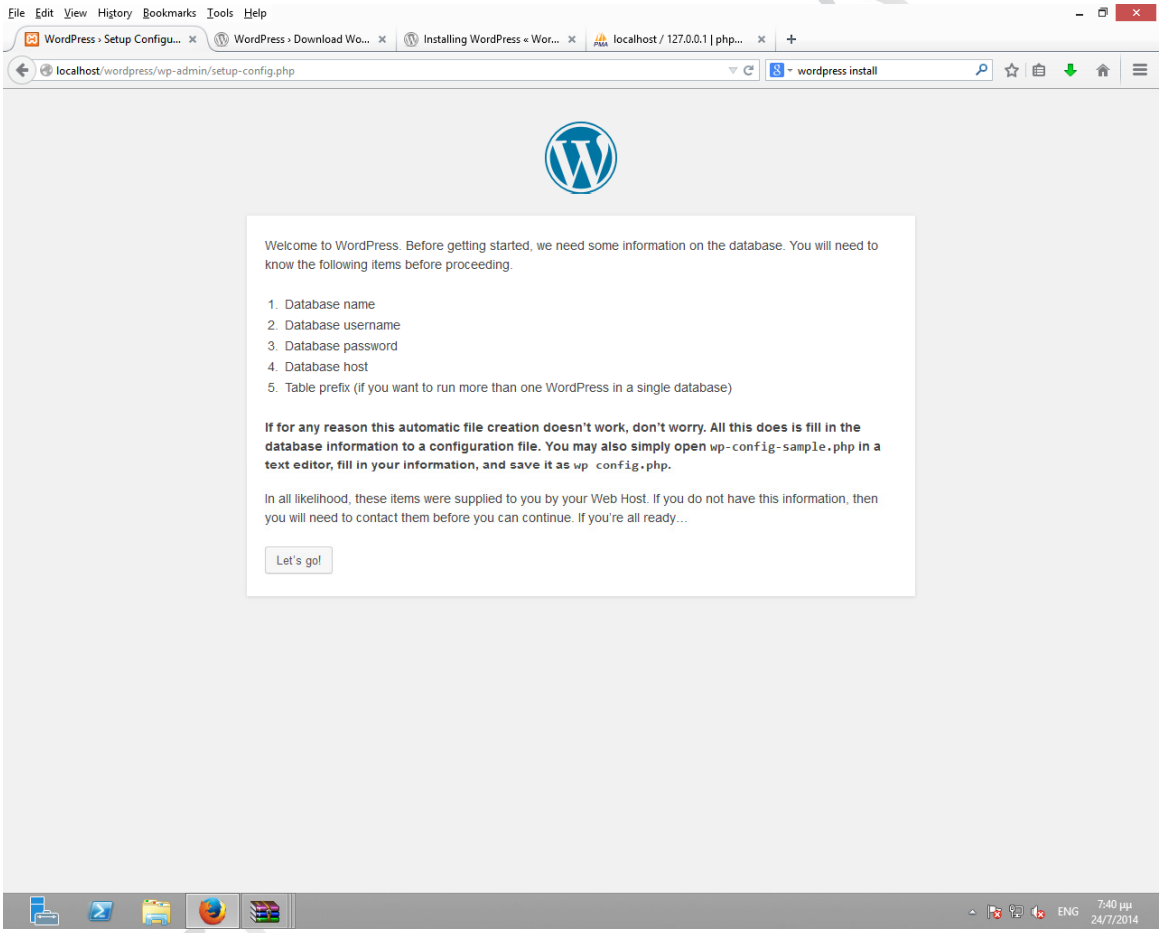
Για να ξεκινήσουμε την εγκατάσταση του Wordpress κατευθύνουμε το φυλλομετρητή στη διεύθυνση όπου αποσυμπιέσαμε το αρχείο του wordpress



Εικόνα 7 Ειδοποιούμαστε ότι πρέπει να δημιουργηθεί configuration file

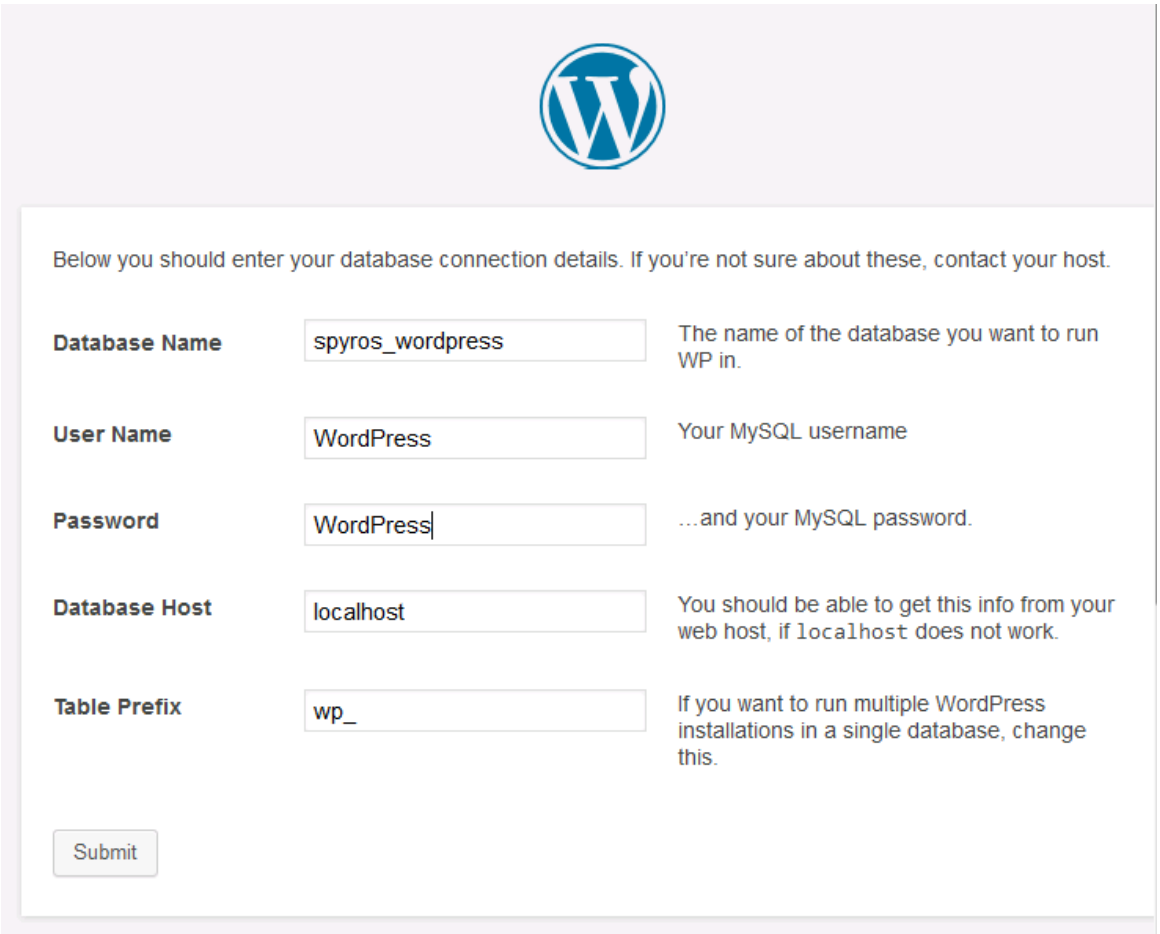
Ειδοποιούμαστε ότι πρέπει να δημιουργηθεί configuration file. Επιλέγουμε create a configuration file.

Ειδοποιούμαστε ότι θα χρειαστούμε τα στοιχεία της βάσης δεδομένων .

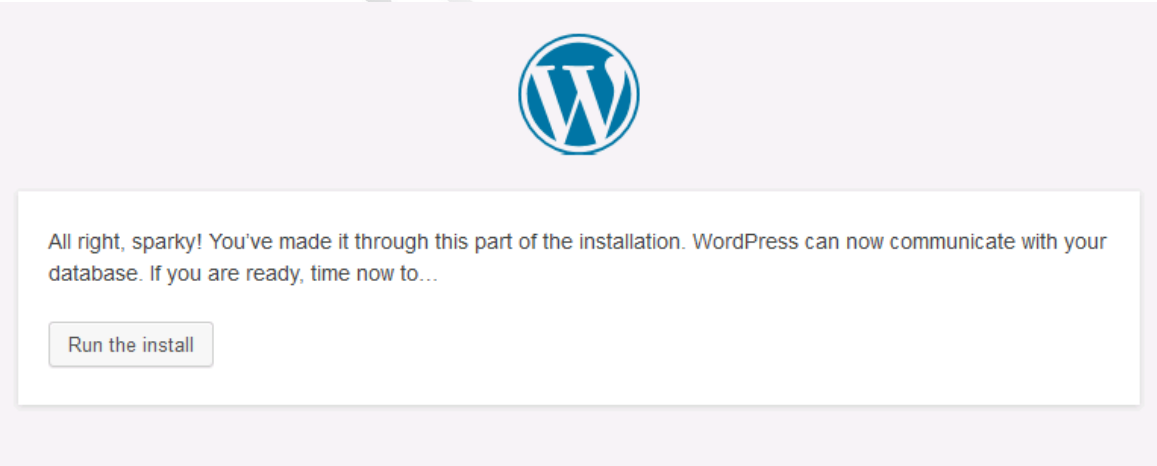


Εικόνα 8 Μετά την εγκατάσταση της βάσης δεδομένων, το wordpress θα ζητήσει ορισμένα στοιχεία

.

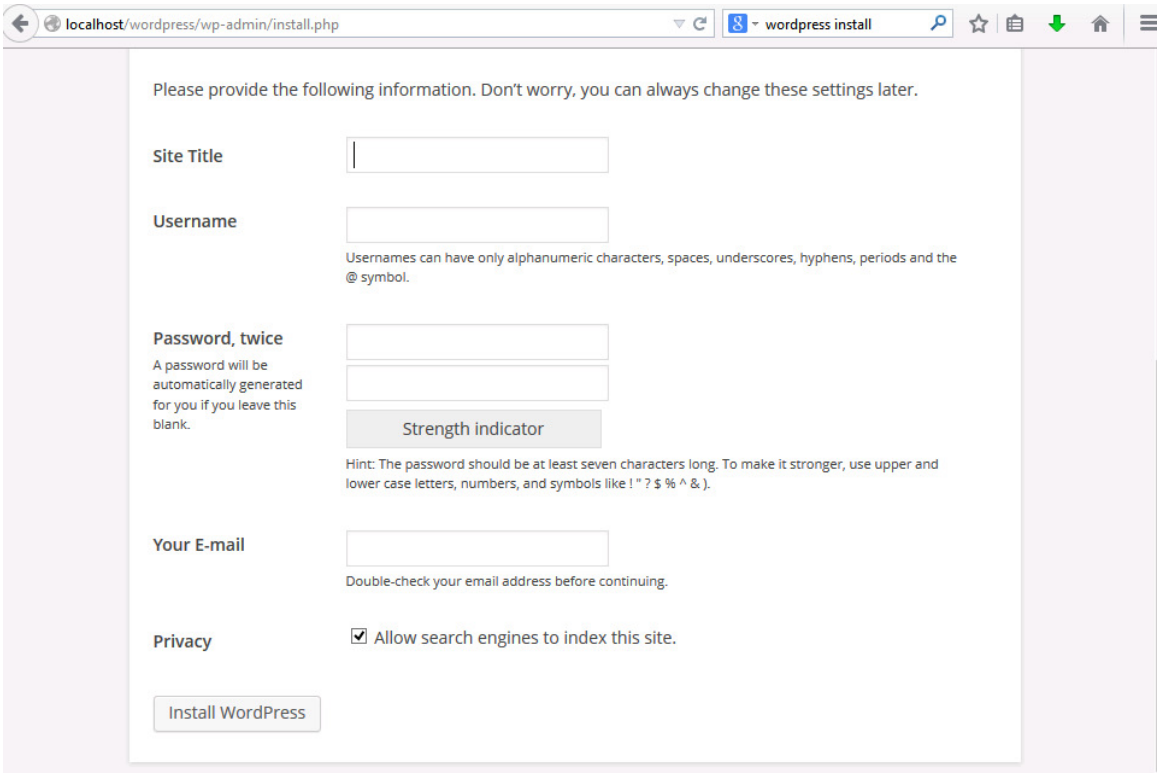


Εικόνα 9 Υποβάλουμε τα στοιχεία που είχαμε ορίσει στα προηγούμενα βήματα



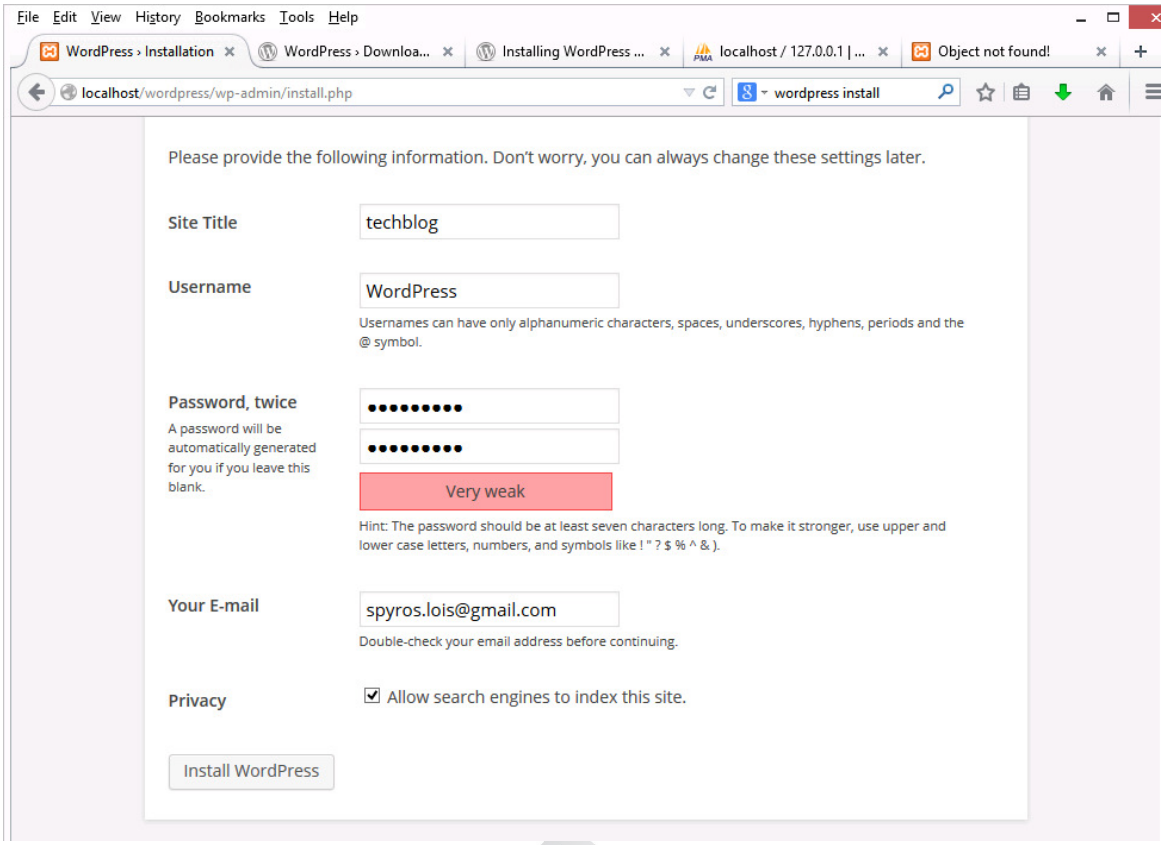
Εικόνα 10 Ειδοποιούμαστε ότι ξεκινάει η εγκατάσταση

Στην εγκατάσταση θα μας ζητηθεί να δώσουμε στοιχεία για το όνομα του ιστότοπου
Το όνομα το συνθηματικό και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή του ιστότοπου



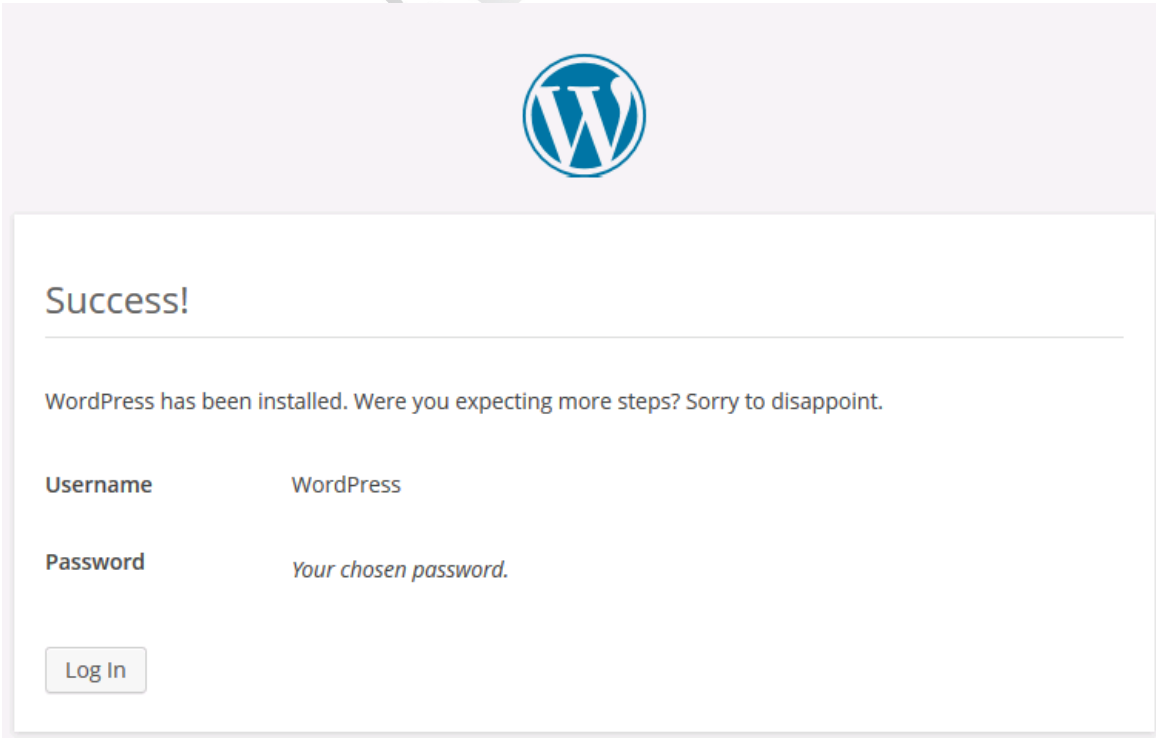
Εικόνα 11 Πληροφορίες για το ιστολόγιο θα ζητηθούν μετά την εγκατάσταση.

Η επιλογή σχετικά με την ιδιωτικότητα έχει να κάνει με το αν θέλουμε να επιτρέπουμε στις μηχανές αναζήτησης να δημιουργήσουν ευρετήριο για το ιστότοπό μας. Αυτό μπορεί να σημαίνει ότι το περιεχόμενο του ιστολόγιου θα αποθηκευτεί για κάποιο χρονικό διάστημα στην μνήμη της μηχανής αναζήτησης και μπορεί να είναι διαθέσιμο από εκεί. Αν δεν θέλουμε να υπάρχει αυτή η δυνατότητα, αποεπιλέγουμε την επιλογή «Allow search engines to index this site».Την αφήνουμε επιλεγμένη αν θέλουμε να ανεβάσουμε το ιστότοπο σε διακομιστή στο internet και να εμφανίζονται τα περιεχόμενα του ιστολόγιου στα αποτελέσματα των μηχανών αναζήτησης. Το συνθηματικό πρέπει να είναι τουλάχιστον 7 χαρακτήρων και μπορεί να περιέχει μικρά/κεφαλαία γράμματα ή και σύμβολα. Η χρωματιστή ένδειξη δείχνει πόσο ισχυρό είναι το συνθηματικό. Αν είναι κόκκινη σημαίνει ότι το συνθηματικό είναι αδύναμο, δηλαδή απλό και θα μπορούσε να παραβιαστεί εύκολα.



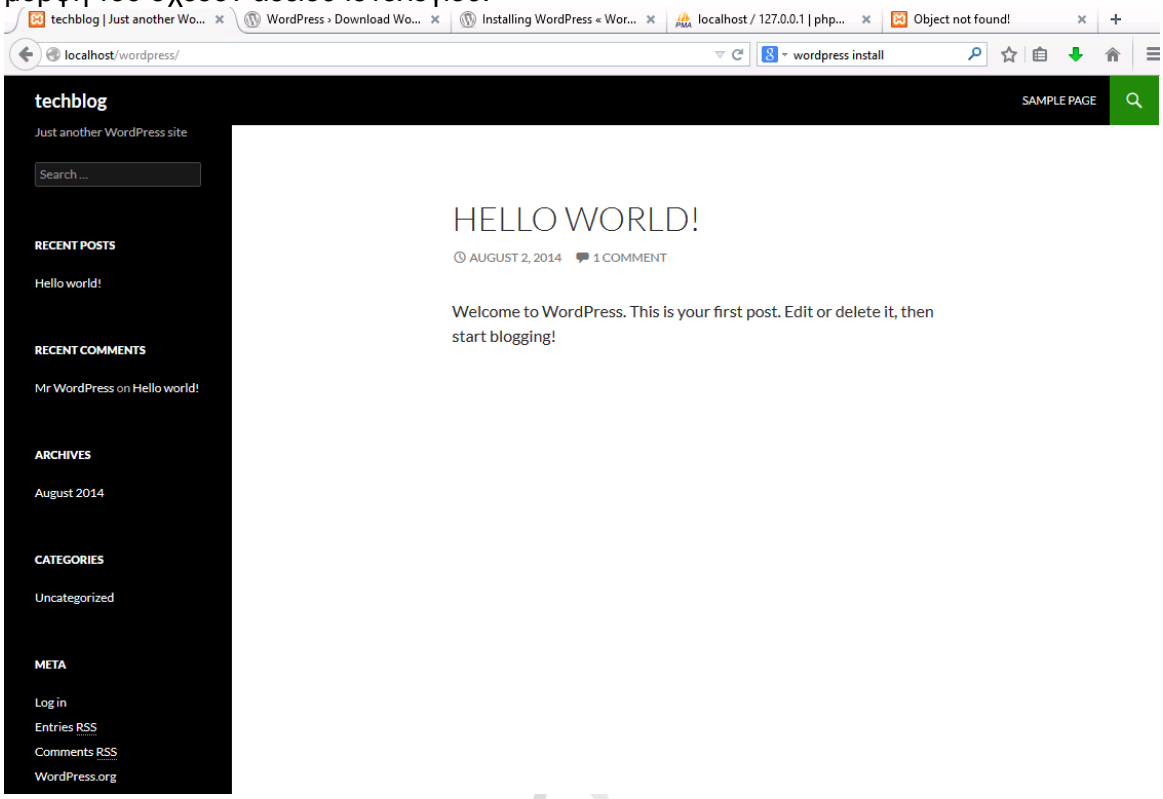
Εικόνα 12 συμπληρώνουμε τα στοιχεία

Αφού συμπληρώσουμε τα στοιχεία που ζητούνται επιλέγουμε εγκατάσταση και περιμένουμε λίγα δευτερόλεπτα για να ολοκληρωθεί η εγκατάσταση και διαμόρφωση του ιστότοπου..



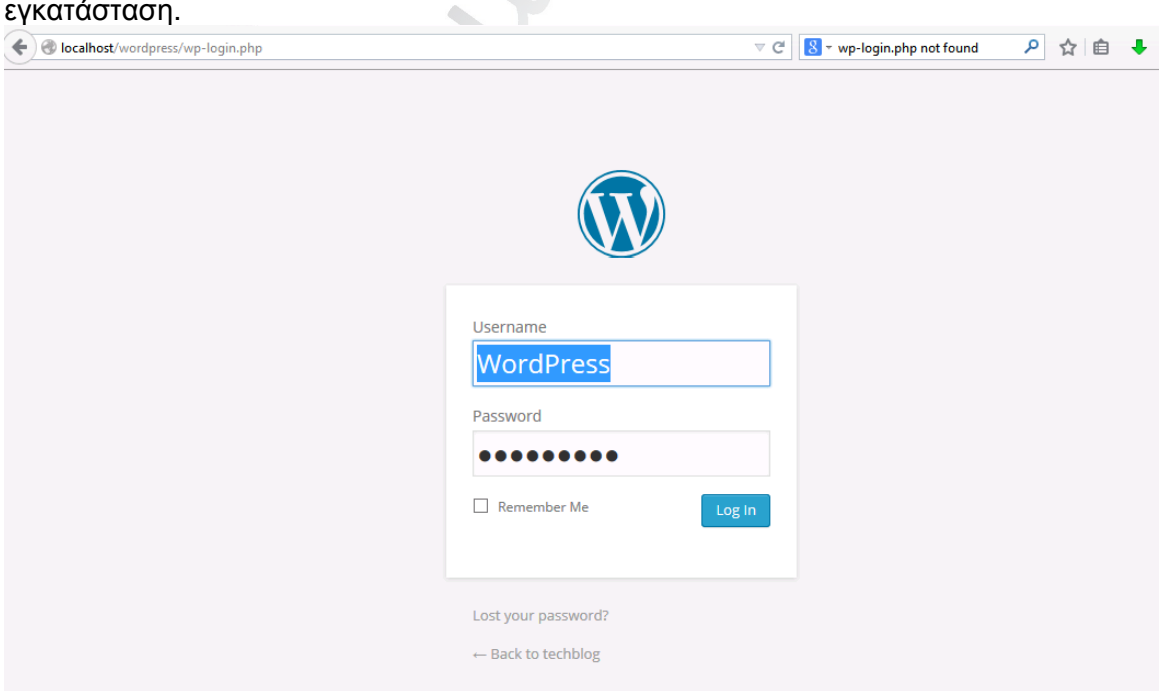
Εικόνα 13 Ειδοποιούμαστε με μήνυμα για την επιτυχή εγκατάσταση

Μπορούμε πια να μεταβούμε στη διεύθυνση localhost/wordpress. Θα δούμε την αρχική μορφή του σχεδόν άδειου ιστολόγιου.



Εικόνα 14 Το πρώτο μήνυμα του ιστολόγιου

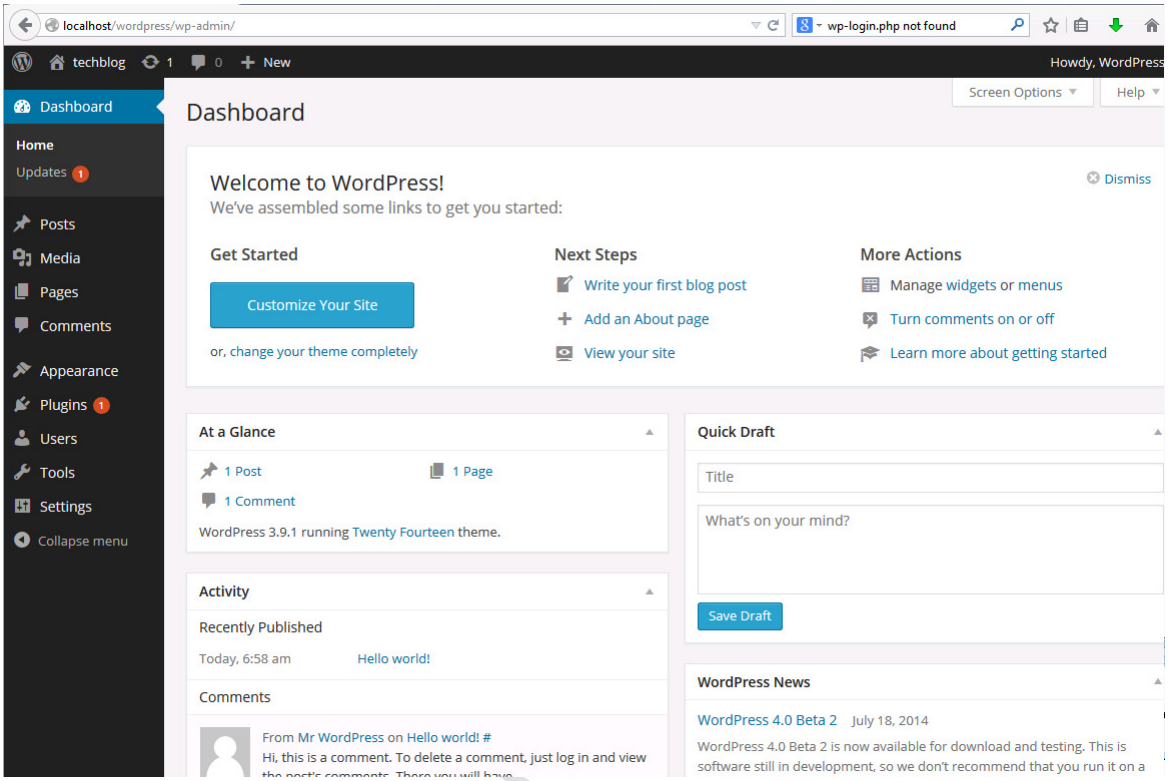
Μπορούμε να κάνουμε είσοδο στο ιστολόγιο με τα στοιχεία που δώσαμε κατά την εγκατάσταση.



Εικόνα 15 Είσοδος χρήστη στο ιστολόγιο

Στη διεύθυνση localhost/wordpress/wp-login.php (αν δεν βρίσκεται το αρχείο wp-login.php μετονομάζουμε το wp-login-sample.php σε wp-login.php) γράφουμε όνομα

χρήστη και συνθηματικό και επιλέγουμε log in.Θα μεταφερθούμε στο πίνακα ελέγχου Dashboard του Wordpress.

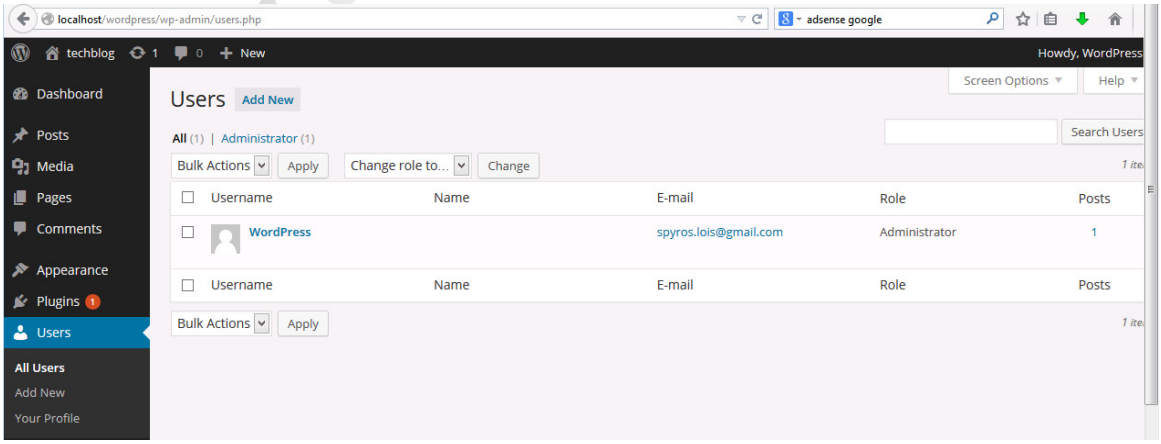


Εικόνα 16 ο πίνακας ελέγχου του wordpress

Αναγνωρίζει το χρήστη WordPress του οποίου δηλώσαμε τα στοιχεία. Υπάρχει μόνο ένα αναρτημένο μήνυμα το hello world. Υπάρχει ειδοποίηση για τη καινούρια έκδοση του Wordpress.

4.3 Διαχείριση χρηστών στο WordPress

Με την επιλογή Users μεταφερόμαστε στην οθόνη διαχείρισης χρηστών στο Wordpress.

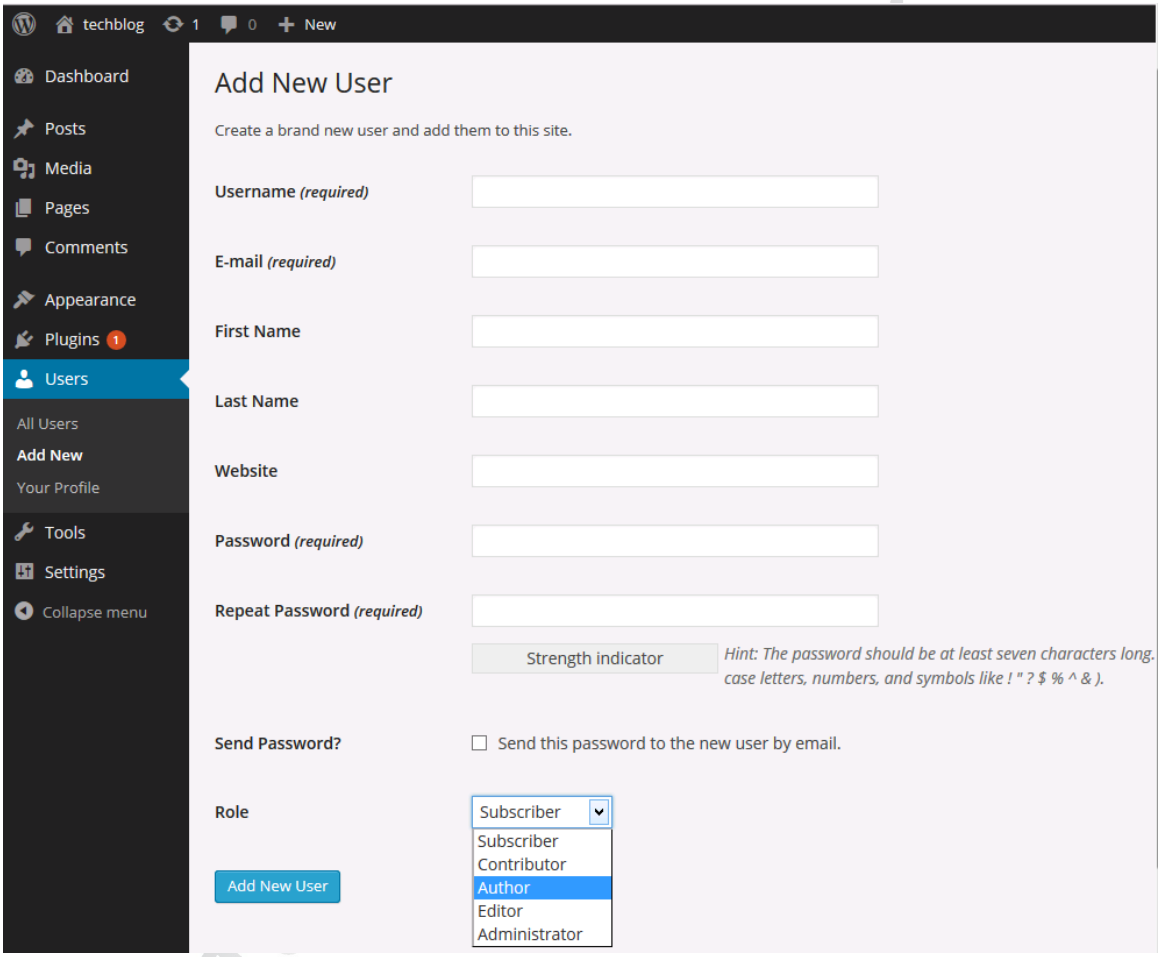


Εικόνα 17 οι χρήστες στο wordpress.

Βλέπουμε ότι υπάρχει μόνο ένας χρήστης ο WordPress, και ένα δημοσιευμένο μήνυμα από αυτόν τον χρήστη.

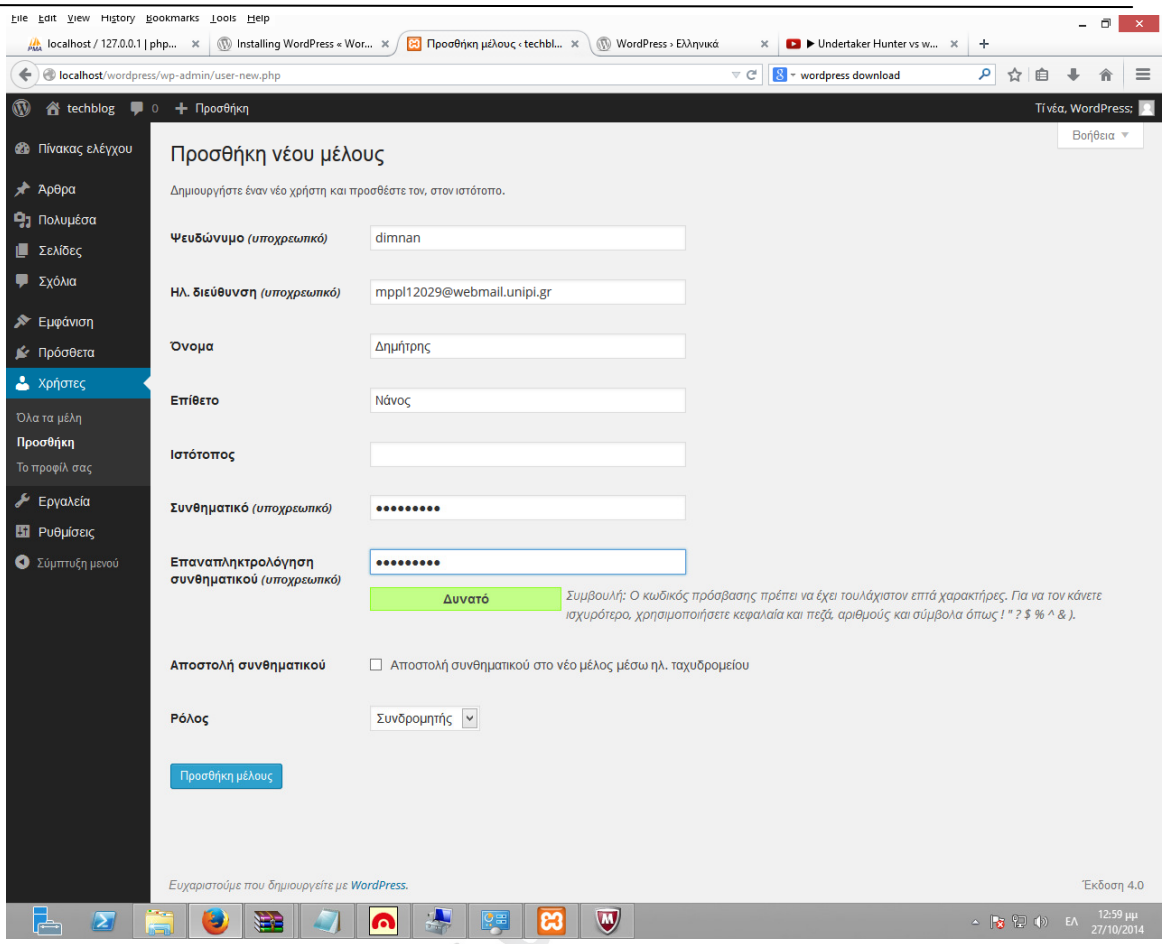
4.3.1 Προσθήκη χρήστη

Επιλέγοντας Add New εμφανίζεται η σελίδα στην οποία θα καταχωρηθούν τα στοιχεία του νέου χρήστη.



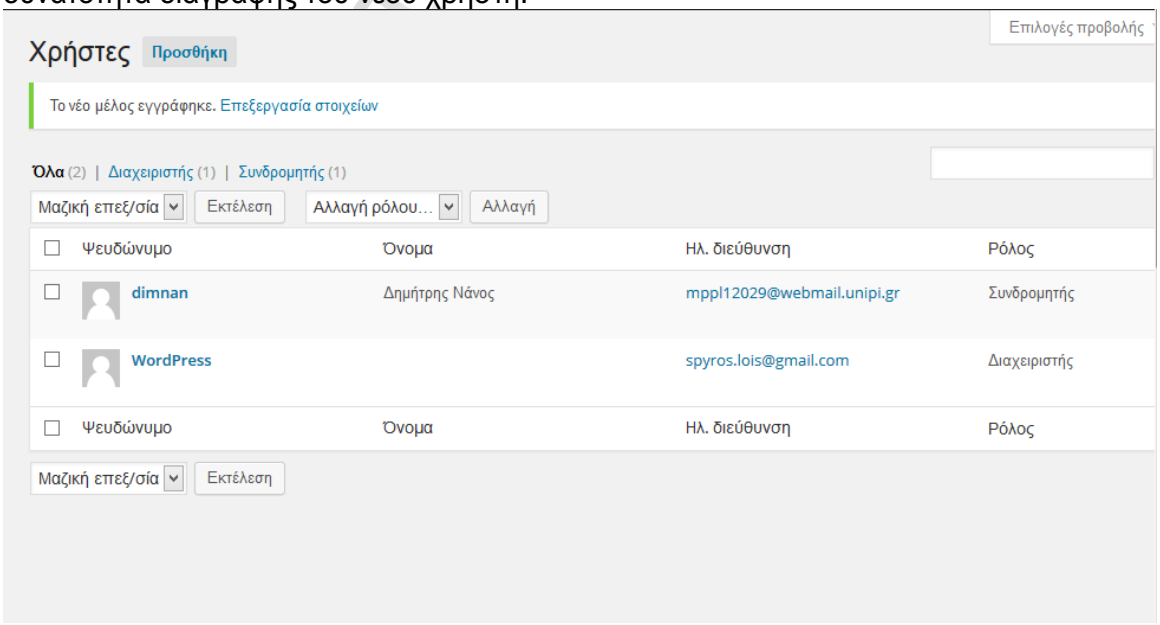
Εικόνα 18 προσθήκη επιπλέον χρήστη/χειριστή του ιστολόγιου

Αφού συμπληρώσουμε τα στοιχεία του χρήστη και επιλέξουμε ρόλο, μεταξύ συνδρομητή, συνεργάτη, συγγραφέα, συντάκτη και διαχειριστή θα του αποσταλεί ένα μήνυμα στη διεύθυνση ηλεκτρονικού ταχυδρομείου με την επιλογή να αποδεχτεί το ρόλο του. Όταν ο χρήστης λάβει το μήνυμα θα το επιλέξει το σύνδεσμο και θα αποκτήσει πρόσβαση στο συγκεκριμένο ρόλο.

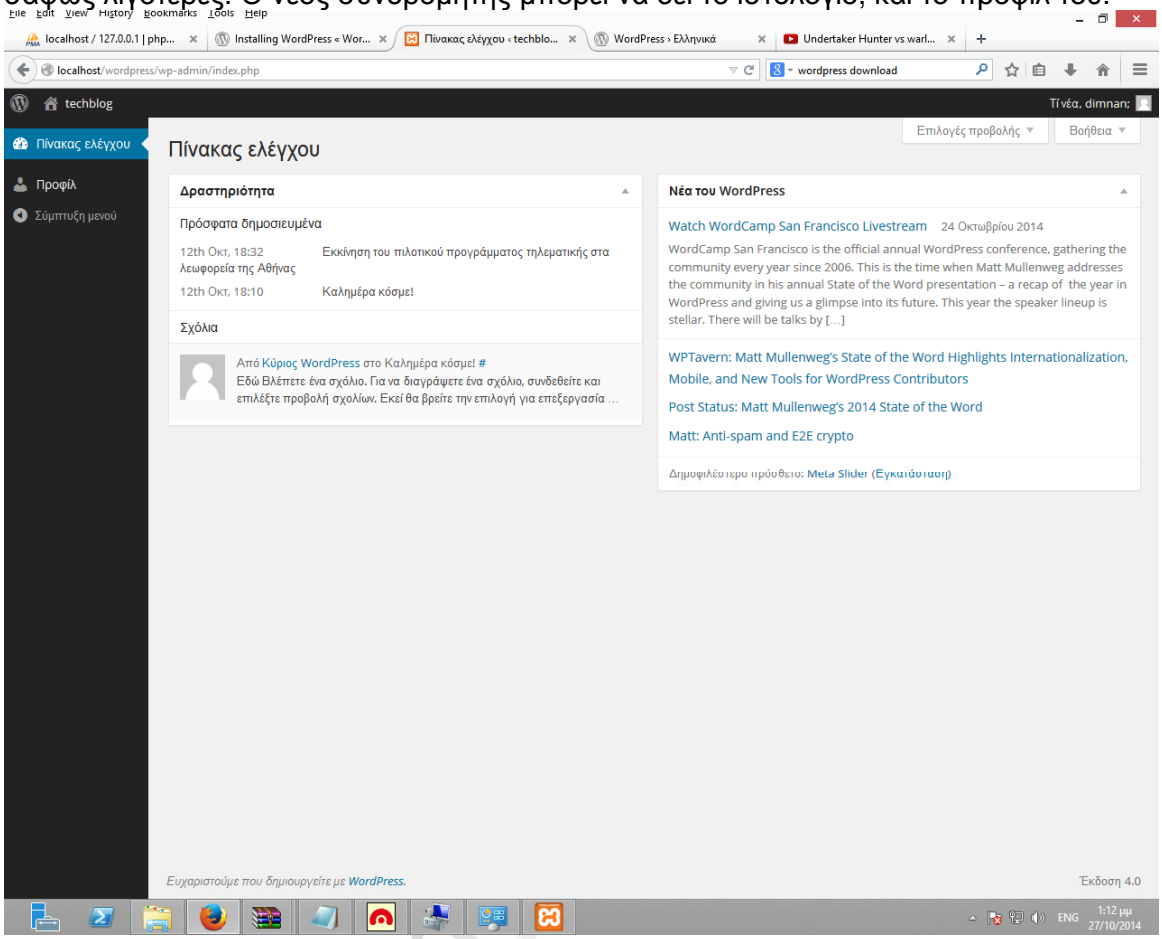


Εικόνα 29 Συμπληρώνουμε τα στοιχεία του χρήστη που θέλουμε να προσθέσουμε

Συμπληρώνοντας τα στοιχεία βλέπουμε τη προσθήκη του νέου συνδρομητή στο ιστολόγιο. Παρατηρούμε τη δυνατότητα αλλαγής ομάδας του κάθε χρήστη και τη δυνατότητα διαγραφής του νέου χρήστη.



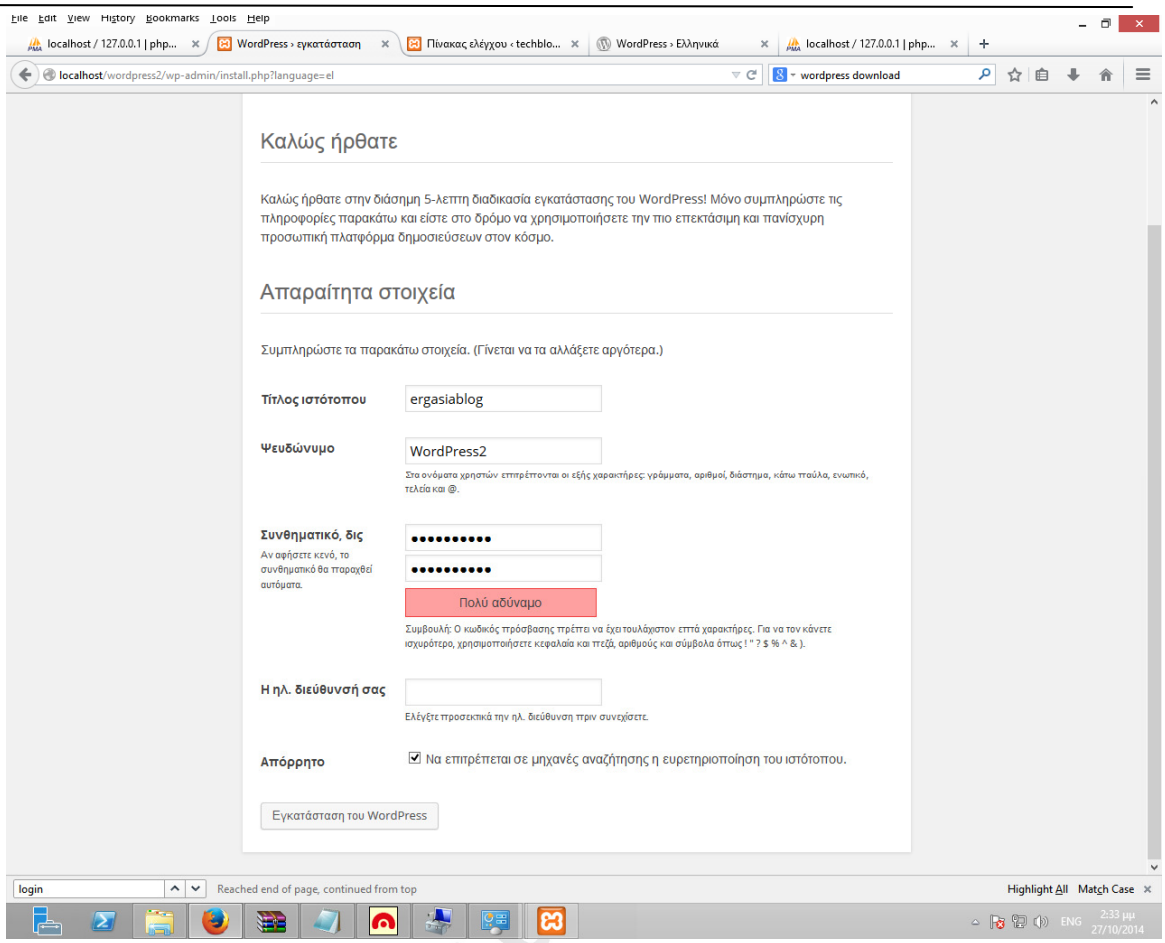
Κάνοντας είσοδο σαν χρήστης dimnan μπορούμε να δούμε ότι οι επιλογές μας είναι σαφώς λιγότερες. Ο νέος συνδρομητής μπορεί να δει το ιστολόγιο, και το προφίλ του.



Στην επιλογή View profile βλέπουμε τα στοιχεία του προφίλ μας και μπορούμε να προσθέσουμε επιπλέον στοιχεία όπως το βιογραφικό μας, ονοματεπώνυμο, και επιλογές εμφάνισης του περιβάλλοντος του Wordpress.

4.4 Πολλαπλά ιστολόγια στο ίδιο διακομιστή

Αν θέλουμε δεύτερη εγκατάσταση ιστολόγιου στο διακομιστή ένας τρόπος είναι να εκτελούμε την διαδικασία εγκατάστασης του Wordpress ξανά, αποσυμπιέζοντας το περιεχόμενο του wordpress σε φάκελο με διαφορετικό όνομα, όπως wordpress2 . Φτιάχνουμε δεύτερη βάση δεδομένων wordpress2 και αρχίζουμε την εγκατάσταση από το localhost/wordpress2.



Η πρόσβαση και η σύνδεση γίνεται από το localhost/wordpress2

4.4.1 Λειτουργία σε περιβάλλον Πολλαπλών χρηστών

Από τη Τρίτη έκδοση του το WordPress έχει τη δυνατότητα δημιουργίας πολλαπλών ιστοτόπων που μοιράζονται την ίδια εγκατάσταση WordPress. Όταν ενεργοποιηθεί η δυνατότητα πολλαπλών ιστοτόπων ο αρχικός ιστότοπος μπορεί να μετατραπεί για να υποστηρίξει ένα δίκτυο ιστοτόπων. Ένα δίκτυο πολλαπλών ιστοτόπων είναι πολύ παρόμοιο με την έκδοση του wordpress.com. Οι χρήστες μπορούν να δημιουργήσουν δικούς τους ιστότοπους κατά παραγγελία. Αν δεν χρειάζεται η δυνατότητα αυτή, μπορεί να δημιουργηθεί ένα δίκτυο πολλαπλών ιστοτόπων όπου μόνο ο διαχειριστής θα μπορεί να έχει τη δυνατότητα να προσθέτει νέους ιστοτόπους.

Ένα δίκτυο πολλαπλών ιστοτόπων είναι ένα σύνολο ιστοτόπων που μοιράζονται την ίδια εγκατάσταση wordpress.Μπορούν επίσης να μοιράζονται ίδια πρόσθετα και θέματα. Οι ξεχωριστοί ιστότοποι στο δίκτυο είναι εικονικοί ιστότοποι με την έννοια ότι δεν έχουν δικούς τους καταλόγους στο διακομιστή, αν και έχουν ξεχωριστούς καταλόγους για περιεχόμενο που θα ανέβει στο διακομιστή και έχουν ξεχωριστούς πίνακες στη βάση δεδομένων.

Σε σχέση με μια τυπική εγκατάσταση wordpress μια εγκατάσταση δικτύου έχει περισσότερες λεπτομέρειες. Πρέπει να αποφασιστεί αν θα περιλαμβάνονται ξεχωριστές περιοχές και καταλόγους και πώς πρέπει να γίνει η διαχείριση τους [19]

Αφού απενεργοποιηθούν τα πρόσθετα ανοίγουμε το wp-config.php και προσθέτουμε την γραμμή

```
/* Multisite */
define( 'WP_ALLOW_MULTISITE', true );
```

πάνω από τη γραμμή /* That's all, stop editing! Happy blogging. */.

Ανανεώνουμε το φυλλομετρητή για να ενεργοποιηθούν οι αλλαγές

Τώρα ενεργοποιείται η επιλογή network setup στο μενού tools. Χρησιμοποιούμε αυτή την επιλογή για να πάμε στη οθόνη create a network of wordpress sites/

4.4.2 Πριν τη δημιουργία δικτύου

Οι ιστότοποι σε ένα δίκτυο πολλαπλών ιστότοπων είναι ξεχωριστά, όπως τα ξεχωριστά ιστολόγια στο wordpress.com. Δεν είναι αλληλοσυνδεόμενα, αν και μπορούν να δημιουργηθούν διάφορες συνδέσεις μεταξύ των ιστοτόπων. Αν σκοπεύετε να δημιουργήσετε ιστοτόπους στενά συνδεδεμένους, μοιράζονται χρήστες ή δεδομένα, ή χρήστες, το δίκτυο πολλαπλών ιστότοπων ίσως να μην είναι η καλύτερη λύση.

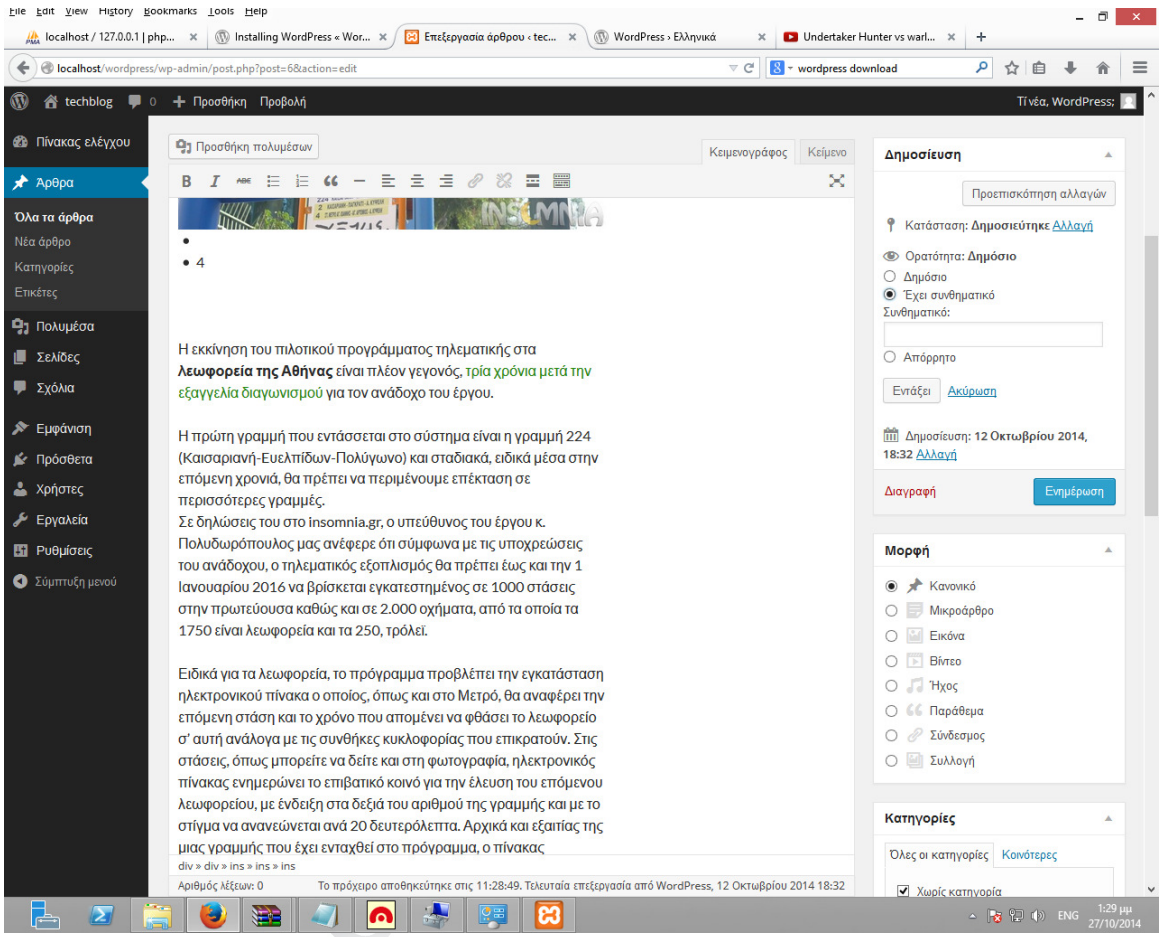
Για παράδειγμα αν θέλουμε για διαφορετικές συλλογές απλώς να φαίνονται διαφορετικά τότε πιθανό να μπορούμε να πετύχουμε αυτό σε ένα ιστότοπο χρησιμοποιώντας ένα πρόσθετο για να αλλάζουμε πρότυπα, θέματα ή stylesheet.[20]

4.5 Επιπλέον ασφάλεια στο Wordpress

Στην ενότητα αυτή παρουσιάζονται ρυθμίσεις για την ενίσχυση της προστασίας του ιστολόγιου.

4.5.1 Χρήση κωδικών ασφαλείας - Ρυθμίσεις ορατότητας ανάρτησης

Ανάλογα με τη πολιτική ιδιωτικότητας του ιστολογίου κάποιες αναρτήσεις θέλουμε να μην είναι φανερές από όλους τους χρήστες ή να είναι ορατές από κάποιους συγκεκριμένους χρήστες, Στις επιλογές Δημοσίευσης μπορούμε να επιλέξουμε μεταξύ *δημόσιο*, έχει *οριστεί συνθηματικό* (μπορούμε να θέσουμε συνθηματικό για τη πρόσβαση στο άρθρο) και *απόρρητο* όπου μόνο ο συγγραφέας θα έχει πρόσβαση στο άρθρο.



Εικόνα 30 Ορατότητα άρθρου

4.5.2 Προστασία της περιοχής διαχειριστή στο Wordpress

Είναι σημαντικό να περιορίζεται η πρόσβαση στη περιοχή διαχειριστή σε άτομα που πραγματικά χρειάζονται πρόσβαση σε αυτή. Οι επισκέπτες δεν θα πρέπει να έχουν πρόσβαση στη θέση /**wp-admin**/ ή στο αρχείο **wp-login.php**. Ένας τρόπος για να γίνει αυτό είναι να βρούμε τη ip διεύθυνση μας και να εισάγουμε αυτές τις γραμμές στο αρχείο *.htaccess* στο φάκελο διαχειριστή

```
<Files wp-login.php>
order deny,allow
Deny from all
Allow from xx.xxx.xxx.xxx
</Files>
```

4.5.3 Αποφυγή του ονόματος admin

Η απλή αποφυγή του ονόματος διαχειριστή Admin μπορεί να προστατέψει το ιστολόγιο από επιθέσεις brute force,

[15]

4.5.4 Αναβάθμιση θεμάτων και προτύπων

Η αναβάθμιση του ιστολόγιου εξασφαλίζει την ασφάλειά του. Η εγκατάσταση της νέας έκδοσης όχι μόνο προσθέτει νέες δυνατότητες αλλά κλείνει τρύπες/κενα ασφαλείας που υπάρχουν σε προηγούμενες εκδόσεις του Wordpress.

4.5.5 Δικαιώματα πρόσβασης σε αρχεία του διακομιστή

Τα δικαιώματα χρήστη στα αρχεία του διακομιστή πρέπει να είναι τέτοια που να απαγορεύουν τη πρόσβαση σε άλλους χρήστες. Σε συστήματα Unix τα δικαιώματα στο αρχείο wp-config.php να είναι «750»

4.5.6 Παρεμπόδιση πρόσβασης στους καταλόγους του ιστότοπου.

Ένας εισβολέας μπορεί να αποκτήσει πρόσβαση σε καταλόγους προσθέτων χρησιμοποιώντας ένα φυλλομετρητή και κατευθύνοντάς τον στο www.yoursite.com/wp-content-plugins. Μπορεί να περιοριστεί αυτή η πρόσβαση είτε με αλλαγές στο αρχείο htaccess ή ανεβάζοντας ένα κενό index.html σε αυτό το κατάλογο.

4.5.7 Λήψη αντιγράφων ασφαλείας για το ιστολόγιο και τη βάση δεδομένων

Η αντιγραφή των αρχείων του ιστολόγιου σε διαφορετικό κατάλογο, ή σκληρό δίσκο, ή σε υπηρεσία cloud όπως το dropbox, επιτρέπει την επαναφορά του ιστολόγιου μετά από προβλήματα και έκτακτα συμβάντα που μπορεί να προκαλέσουν ζημιά στη λειτουργία του.

4.5.8 Κρυπτογράφηση κατά τη πρόσβαση – Login Encrypt

Η ύπαρξη προσθέτου Login Encrypt Επιτρέπει την κρυπτογραφημένη χρήση συνθηματικού χρησιμοποιώντας κρυπτοσύστημα RSA και DES(Data encryption Standard), χωρίς SSL.

Ένα πρόγραμμα javascript προστίθεται στο wp-loginπαράγει κάθε φορά που ο χρήστης συνδέεται ένα μοναδικό κλειδί DES. Χρησιμοποιώντας αυτό το κλειδί το συνθηματικό του χρήστη κρυπτογραφείται. Το πρόγραμμα javascript κρυπτογραφεί αυτό το μοναδικό κλειδί χρησιμοποιώντας το RSA δημόσιο κλειδί (παράγεται όταν το πρόσθετο ενεργοποιείται). Το κρυπτογραφημένο συνθηματικό και το κρυπτογραφημένο DES μοναδικό κλειδί στέλνονται στο διακομιστή. Ο διακομιστής ελέγχει αν ληφθεί ένα κρυπτογραφημένο DES κλειδί. Αν ληφθεί το αποκρυπτογραφεί χρησιμοποιώντας το ασφαλές RSA ιδιωτικό κλειδί. Τότε το αποκρυπτογραφεί χρησιμοποιώντας το ασφαλές RSA ιδιωτικό κλειδί, και αποκρυπτογραφεί το συνθηματικό χρησιμοποιώντας το μοναδικό DES κλειδί.

ΚΕΦΑΛΑΙΟ 5 - Συμπεράσματα

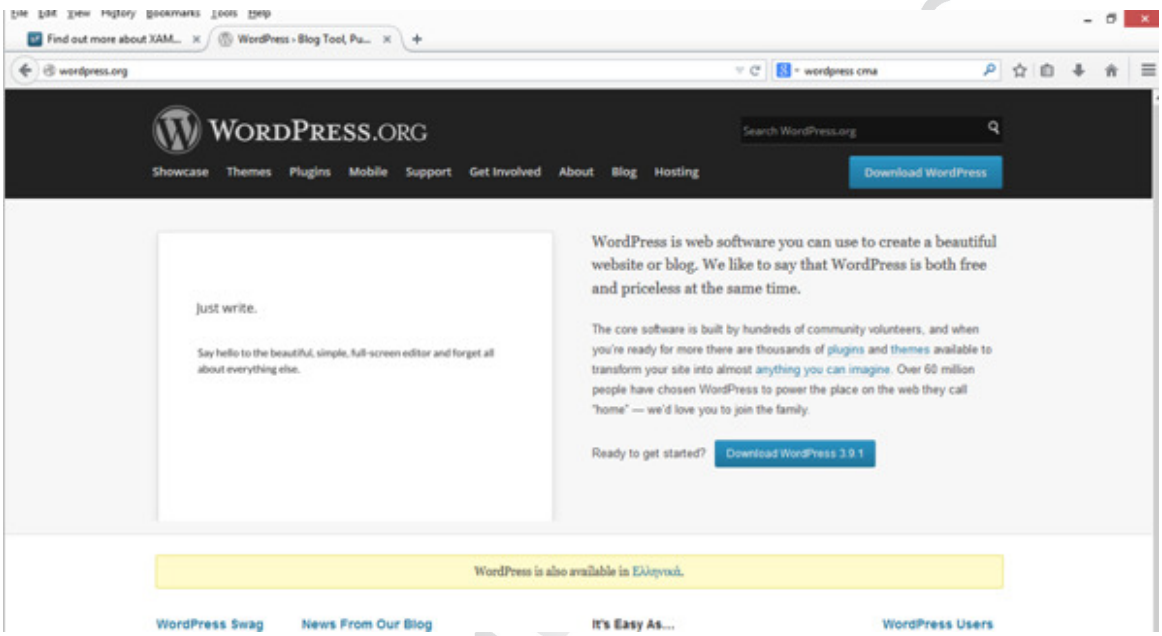
Η ασφάλεια στα ιστολόγια εξασφαλίζει ότι θα προβάλλονται οι πληροφορίες που επιλέγει ο διαχειριστής τους χωρίς να εκτίθενται σε κινδύνους τα ιστολόγια και τα δεδομένα τους.

Μπορούμε να πούμε ότι είναι δυνατό να κατασκευαστεί ένα ιστολόγιο με τρόπο ασφαλή για το πληροφοριακό σύστημα και για τα επιπλέον μέρη του. Η βάση δεδομένων είναι προστατευμένη καθώς δημιουργήθηκε χρήστης από το ίδιο το σύστημα και η πρόσβαση είναι ελεγχόμενη. Μόνο άτομα με εξουσιοδότηση μπορούν να μεταβάλουν τα περιεχόμενα της βάσης δεδομένων και επομένως του ιστολόγιου. Οι τεχνολογίες πιστοποίησης που εφαρμόζονται έχουν στόχο να επιτρέπουν στο χρήστη να αποκαλύπτει μόνο τα στοιχεία της ταυτότητας που χρειάζονται. Στη περίπτωση του blogger (του δημιουργού ιστολόγιου) μπορεί να μοιραστεί μόνο το όνομα που έχει επιλέξει, και να μην αποκαλύψει άλλη πληροφορία. Σε περίπτωση που ζητηθούν στοιχεία πρόσβασης ιστολόγιου λόγω παράβασης θα παραχωρηθούν. Η απόκρυψη ευαίσθητων πληροφοριών έχει συντελέσει ώστε το διαδίκτυο να είναι ένα πολύ ισχυρό εργαλείο το οποίο χρησιμοποιείται για να εκφράζονται απόψεις,. Τέλος βλέπουμε ότι με τη διαχείριση χρηστών του wordpress μπορούμε να εξουσιοδοτούμε επιπλέον άτομα για να χρησιμοποιήσουν το ιστολόγιο και να δημοσιεύουν τα δικά τους άρθρα. Σαν πληροφοριακό σύστημα το wordpress παρέχει καλή ασφάλεια. Κάθε χρήστης μπορεί να έχει πρόσβαση σε ορισμένες λειτουργίες, η δημοσίευση άρθρων είναι δυνατό να γίνει με περιορισμένη ορατότητα. Η πρόσβαση των μελών γίνεται με συνθηματικά, ενώ υπάρχουν πρόσθετα που επιτρέπουν την κρυπτογράφησή τους. Το wordpress εχει αδυναμίες . Στη περίπτωση SQL injection ο εισβολέας μπορεί να ενσωματώσει εντολές στο URL από το φυλλομετρητή και να ενεργοποιήσει κάποια συμπεριφορά στη βάση δεδομένων. Κάτι που θα μπορούσε να προστεθεί σε μία επόμενη εργασία θα ήταν η μέτρηση της ασφάλειας με εξειδικευμένο πρόγραμμα. Δεν υπάρχει 100% ασφαλές λογισμικό αλλά αν ακολουθήσουμε βασικές οδηγίες ασφαλείας, το wordpress θα είναι ενημερωμένο με τις αναγκαίες διορθώσεις για τα κενά ασφαλείας. Για την ασφάλεια της κάθε ιστοσελίδας μόνο ο διαχειριστής της μπορεί να εξασφαλίσει την ασφαλή λειτουργία.

ΠΑΡΑΡΤΗΜΑ

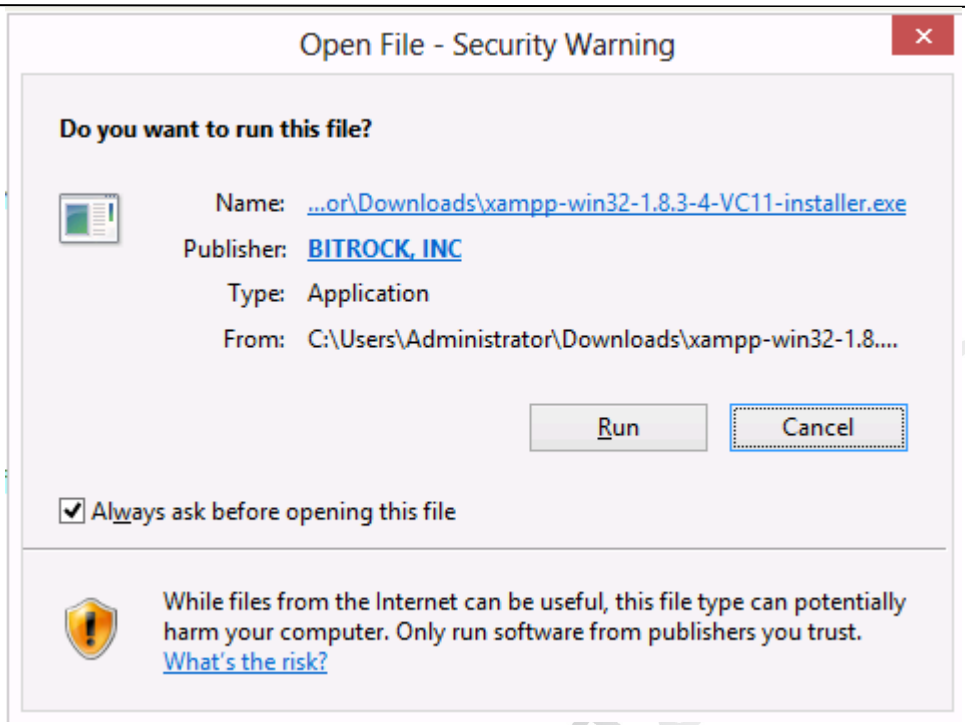
Εγκατάσταση XAMPP

Το πρώτο βήμα είναι να κατεβάσουμε τη τελευταία έκδοση του προγράμματος XAMPP που περιλαμβάνει το διακομιστή Apache, τη βάση δεδομένων MySQL και τις γλώσσες PHP και Perl[12].

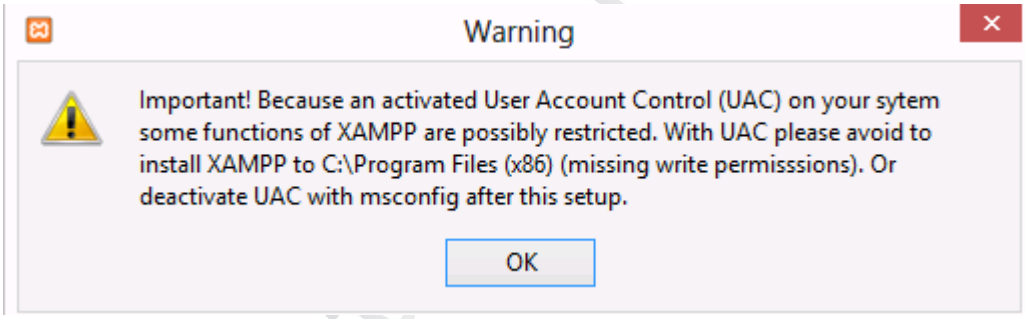


Εικόνα 3 apachefriends.org

Το πρώτο βήμα είναι να κατεβάσουμε από τη σελίδα apachefriends.org το XAMPP. Στη συνέχεια τρέχουμε το Installer.

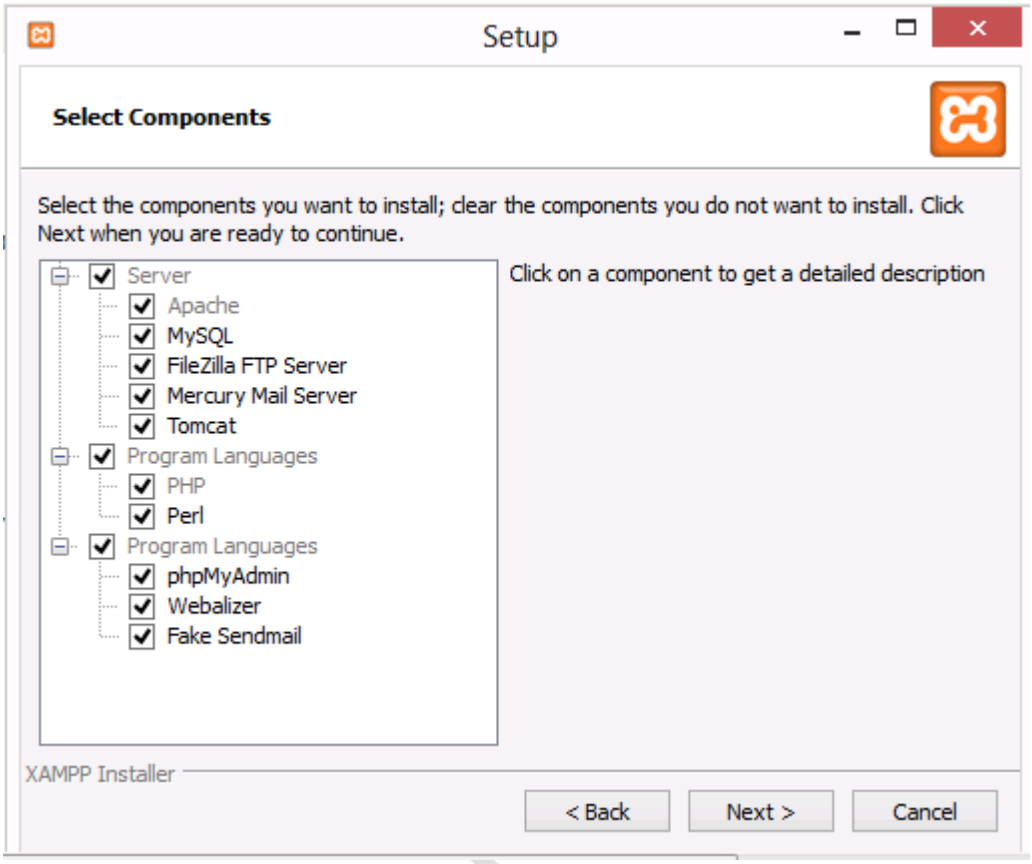


Εικόνα 4 Τρέχουμε το installer του XAMPP

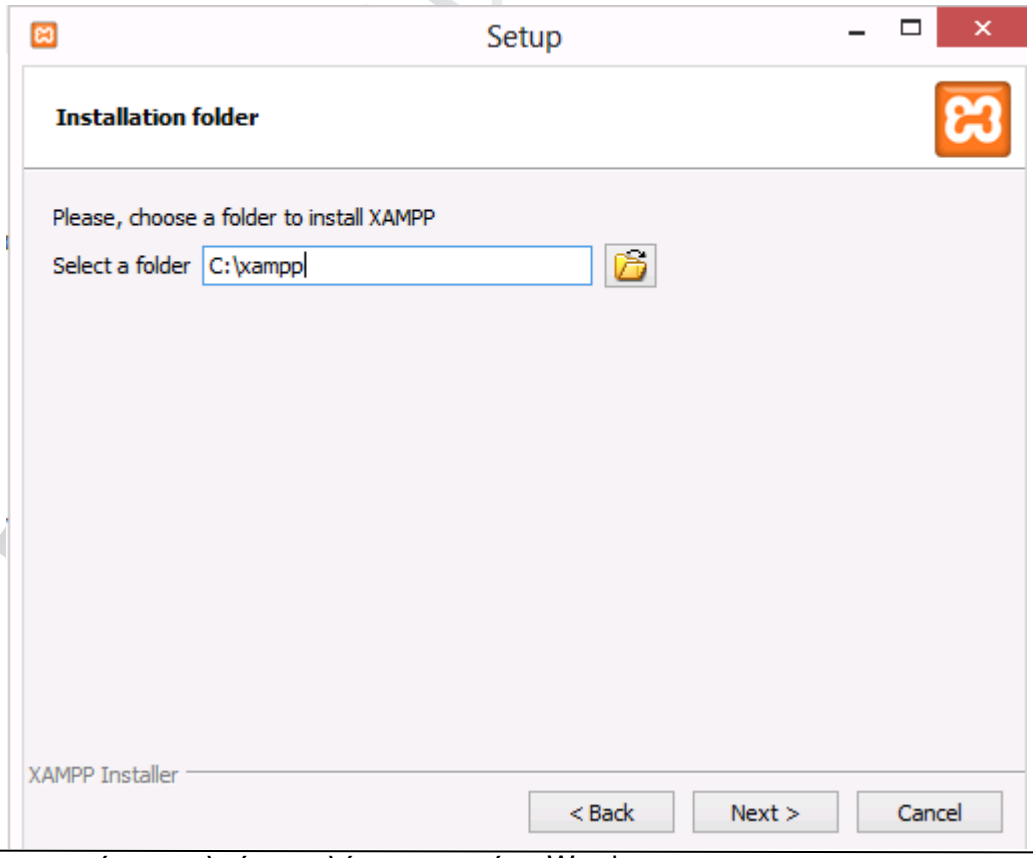


Εικόνα 5 λαμβάνουμε προειδοποίηση σχετικά με το UAC των windows

Εικόνα 19 Βλέπουμε τα εργαλεία που πρόκειται να εγκατασταθούν

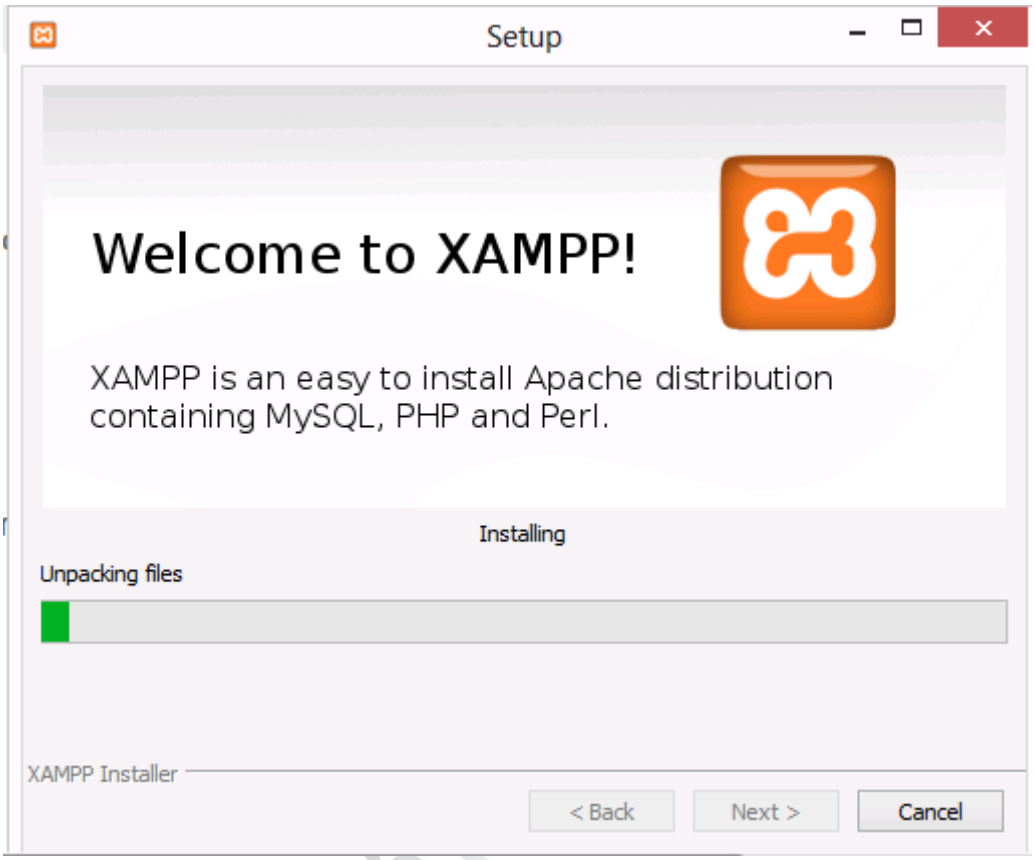


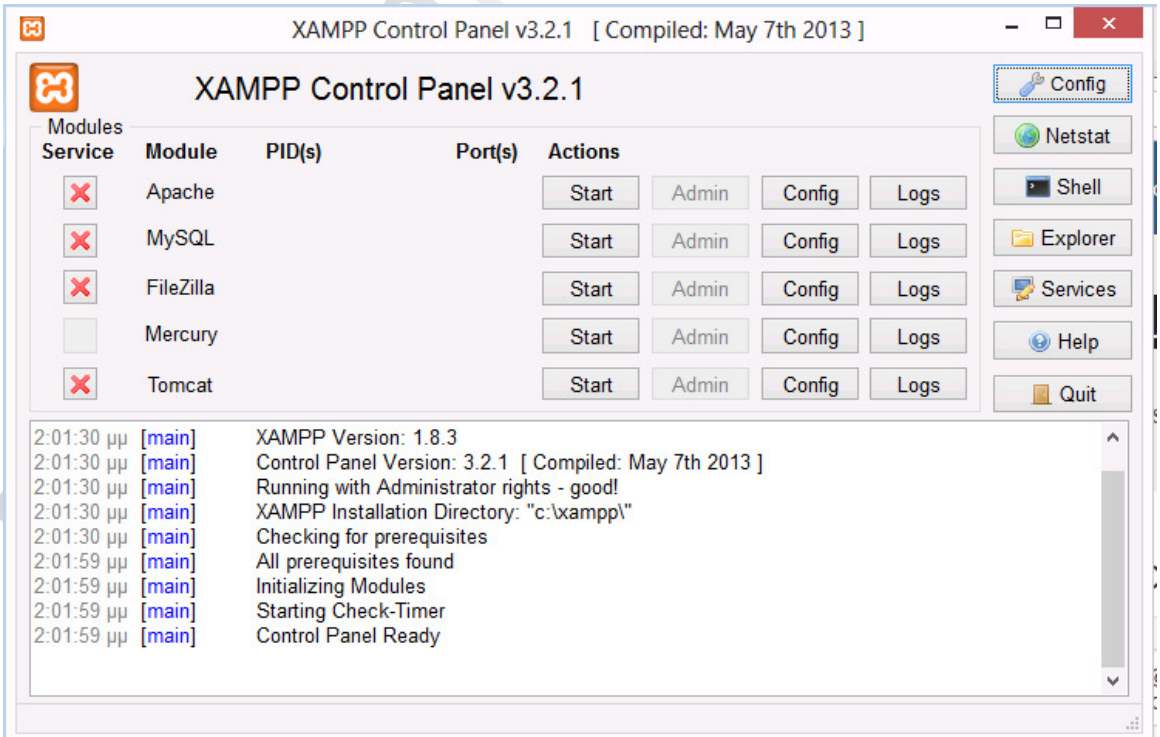
Εικόνα 20 Βλέπουμε τα εργαλεία που πρόκειται να εγκατασταθούν



Εικόνα 21 Δεχόμαστε το προεπιλεγμένο κατάλογο για εγκατάσταση

Επιλέγουμε next για να ξεκινήσει η εγκατάσταση





Εικόνα 22 Μόλις εγκατασταθεί το πρόγραμμα μπορούμε να δούμε το πίνακα ελέγχου

Για τη λειτουργία του Wordpress τοπικά, χρειάζονται ο Apache και η MySQL.Οπότε τα ενεργοποιούμε από τις επιλογές start

Για την αποστολή του ιστολόγιου σε διακομιστή ιστού, χρειάζεται ένα FTP client, για την αποστολή των αρχείων που αποτελούν το ιστότοπο. Στην παρούσα εργασία η εγκατάσταση θα γίνει σε εικονική μηχανή με λειτουργικό σύστημα windows server 2012.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Luciano Fioridi *Εισαγωγή στη φιλοσοφία της πληροφορικής* ,εκδόσεις νήσος 2008

[2] John Viega, Matt Mesler. Pravir Chandra, *Network security with OpenSSL* O'REILLY, 2002

[3] John R. Vacca *computer and information security handbook* , Morgan Kaufmann Series in Computer Security, 2009

[4]en.wikipedia.org

[5] http://codex.wordpress.org/Roles_and_Capabilities

[6]Κάτσικας, *ασφάλεια υπολογιστών* ΕΑΠ, Πάτρα, 2001

[7] http://codex.wordpress.org/Roles_and_Capabilities

[8] theeucookielaw.com

[9] http://33bits.org/2010/12/05/web-crawlers-privacy-reboot-robots-txt/

[10] http://www.javascriptkit.com/howto/robots.shtml

[11] http://www.tovima.gr/society/article/?aid=278725

[12] Στέφανος Γκρίτζαλης, Κ. Λαμπρινουδάκης, Σωκράτης Κάτσικας, Λίλιαν Μήτρου *Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών Νομικά και τεχνικά θέματα*, Παπασωτηρίου 2010. Κεφάλαιο 3 :*Διατήρηση Δεδομένων Επικοινωνίας και διασφάλιση του απορήτου και της ιδιωτικότητας των επικοινωνιών*.

[13] http://www.siteground.com/tutorials/wordpress/wordpress_security.htm#protect_admin

[14] www.apachefriends.org

[15]wordpress.org

[16] http://www.siteground.com/tutorials/wordpress/wordpress_security.htm#protect_admin

[17]http://newpost.gr/post/50297/gnomodotisi-areioy-pagoy-gia-arsi-anonymias-ton-blogs

[18]https://wordpress.org/plugins/login-encryption/

[19] http://codex.wordpress.org/Create_A_Network

[20]http://codex.wordpress.org/Before_You_Create_A_Network