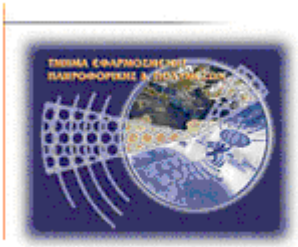
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (Joomla) και η ασφαλής θωράκισή του.

Φωτεινή Ζιώγα (ΑΜ: 1266)
E-mail: fotini_zioga@yahoo.com

Ηράκλειο –18/01/2010

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Υπεύθυνη Δήλωση: *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ζιώγα Φωτεινή, 2010.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου για την αμέριστη υποστήριξη κατά την διάρκεια εκπόνησης της εργασίας αυτής.

Θα ήθελα επίσης να ευχαριστήσω τον καθηγητή κ. Μανιφάβα Χαράλαμπο για την πολύτιμη καθοδήγηση και υποστήριξη του σε όλη τη διάρκεια εκπόνησης της εργασίας αυτής.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Περίληψη

Το θεματικό αντικείμενο της παρούσας πτυχιακής εργασίας είναι η διερεύνηση των ανοιχτών συστημάτων διαχείρισης περιεχομένου (Open Source Content Management Systems – CMS) ως προς την ασφάλεια και τα λοιπά χαρακτηριστικά τους.

Τελικός στόχος είναι η δημιουργία μιας εφαρμογής ηλεκτρονικού καταστήματος χρησιμοποιώντας το ανοιχτού περιεχομένου σύστημα διαχείρισης, Joomla. Ειδικότερα, ο τεχνικός στόχος της εργασίας είναι ο εμπλουτισμός της εφαρμογής με ό,τι μηχανισμούς χρειάζεται έτσι ώστε το ηλεκτρονικό κατάστημα να:

- Γίνει ασφαλές στις συναλλαγές του και να προβάλλει προς τους χρήστες ένα αξιόπιστο προφίλ.
- Έχει εύχρηστο περιβάλλον προς τους όλους τους χρήστες, εξοικειωμένους και μη.
- Προβάλλει με ελκυστικό τρόπο τα διαθέσιμα προϊόντα στους υποψήφιους πελάτες.

Αρχικά, στο θεωρητικό σκέλος της εργασίας μελετήθηκαν θέματα που αφορούν τα συστήματα διαχείρισης περιεχομένου γενικότερα. Έγινε αναφορά σε ορισμούς, στον τρόπο λειτουργίας, στα χαρακτηριστικά και στα πλεονεκτήματά τους. Ερευνήθηκε ο τρόπος που διεξάγονται οι ηλεκτρονικές συναλλαγές. Επίσης, διερευνήθηκαν οι επιθέσεις που μπορεί να δεχτεί ένα ηλεκτρονικό κατάστημα και πως αυτές μπορούν να αντικρουστούν.

Ακολούθως, στο πρακτικό σκέλος της εργασίας έγινε κατασκευή του ηλεκτρονικού καταστήματος με Joomla CMS και εφαρμόστηκαν σε αυτό τεχνικές και components για να εξασφαλίσουν την ασφάλεια του.

Το βασικό component που χρησιμοποιήθηκε για την λειτουργία του ηλεκτρονικού καταστήματος είναι το VirtueMart έκδοση 1.1.3. Γίνεται εκτενή αναφορά των ρυθμίσεων, των δυνατοτήτων και των επιλογών του component αυτού ως προς την ασφάλεια και τα γενικά χαρακτηριστικά του.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Πίνακας Πινάκων

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Το ηλεκτρονικό εμπόριο τα τελευταία χρόνια έχει αρχίσει να αναπτύσσεται και στην χώρα μας, παρόλο που αρχικά αντιμετωπίζοταν με δυσπιστία. Με τον όρο ηλεκτρονικό εμπόριο εννοούμε κάθε είδος εμπορικής συναλλαγής μεταξύ προσώπων (φυσικών και μη) που πραγματοποιείται με ηλεκτρονικά μέσα. Είναι η διάθεση και η αγοραπωλησία προϊόντων ηλεκτρονικά, η διεκπεραίωση εμπορικών λειτουργιών και συναλλαγών χωρίς τη χρήση χαρτιού, συνήθως μέσω δικτύων ηλεκτρονικών υπολογιστών. Πρόκειται για την αγοραπωλησία αγαθών, πληροφοριών και υπηρεσιών μέσα από δίκτυα ηλεκτρονικών υπολογιστών.

1.2 Σκοπός

Η εργασία αυτή επικεντρώνεται στη δημιουργία ενός ασφαλούς ηλεκτρονικού καταστήματος. Το εργαλείο το οποίο θα χρησιμοποιήσουμε είναι το ανοιχτού περιεχομένου σύστημα διαχείρισης, Joomla.

Πιο συγκεκριμένα αναλύονται τα παρακάτω θέματα:

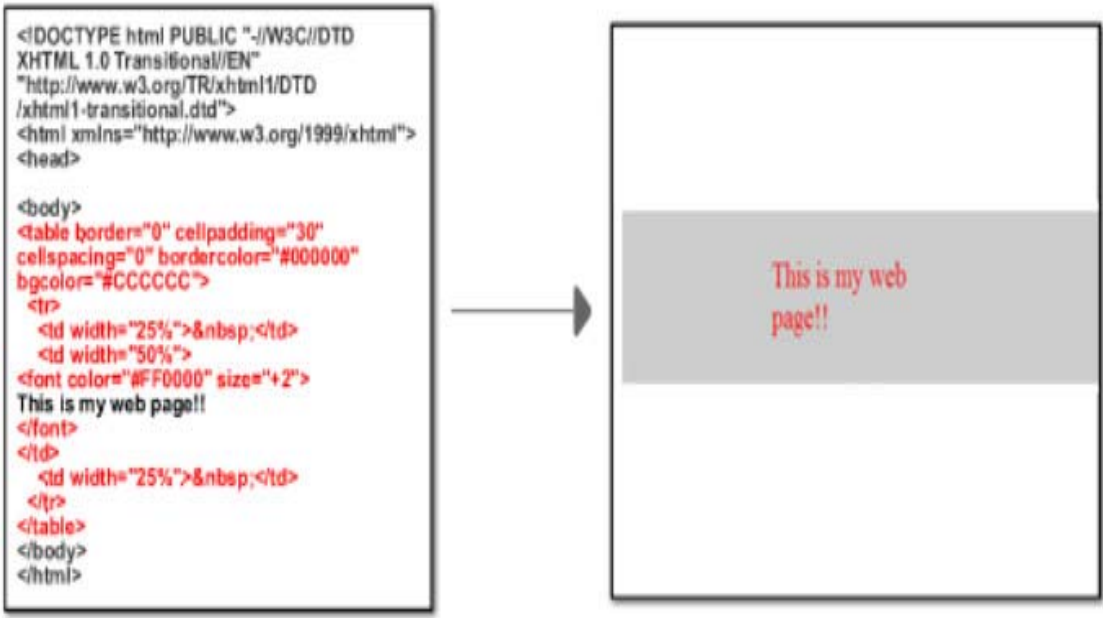
1. Γενικές πληροφορίες για τα Συστήματα Διαχείρισης Περιεχομένου (CMS).
2. Που βασίζεται ένα CMS.
3. Χαρακτηριστικά του Joomla.
4. Προδιαγραφές εγκατάστασης του.
5. Μέθοδοι πληρωμής που υποστηρίζει το εργαλείο που χρησιμοποιούμε.
6. Επικίνδυνα σημεία στην διεξαγωγή του ηλεκτρονικού εμπορίου.
   - DoS attack ή DDoS attack.
   - SQL injections.
   - Social engineering techniques (phishing)
   - Cross site scripting
   - Hidden Manipulation
   - Cross-Site Request Forgery (CSRF)
7. Τεχνικές για την διασφάλιση ενός ηλεκτρονικού καταστήματος όπως:
   - Secure HTTP (S-HTTP).
   - Ψηφιακές υπογραφές.
   - Ψηφιακά πιστοποιητικά.
   - Ηλεκτρονική ανταλλαγή δεδομένων.
   - Επίπεδο ασφαλών συνδέσεων.
8. Τεχνικές διασφάλισης Joomla ηλεκτρονικού καταστήματος.
   - Απόκρουση SQL injections.
   - Απόκρουση Cross-Site-Scripting injection.
   - Αντίγραφο ασφαλείας.
   - File System Premissions.

Κεφάλαιο 2 Συστήματα Διαχείρισης Περιεχομένου (cms)

2.1 Η εξέλιξη της κατασκευής ιστοσελίδων

2.1.1 Κατασκευή ιστοσελίδων στη δεκαετία του '90

Στη δεκαετία του '90 για τη δημιουργία μίας σελίδας θα έπρεπε ο κατασκευαστή της ιστοσελίδας να γράψει τον κώδικα που απαιτούνταν για τη συγκεκριμένη σελίδα. Βλέπουμε πως παρουσιάζεται σχηματικά στην παρακάτω εικόνα.



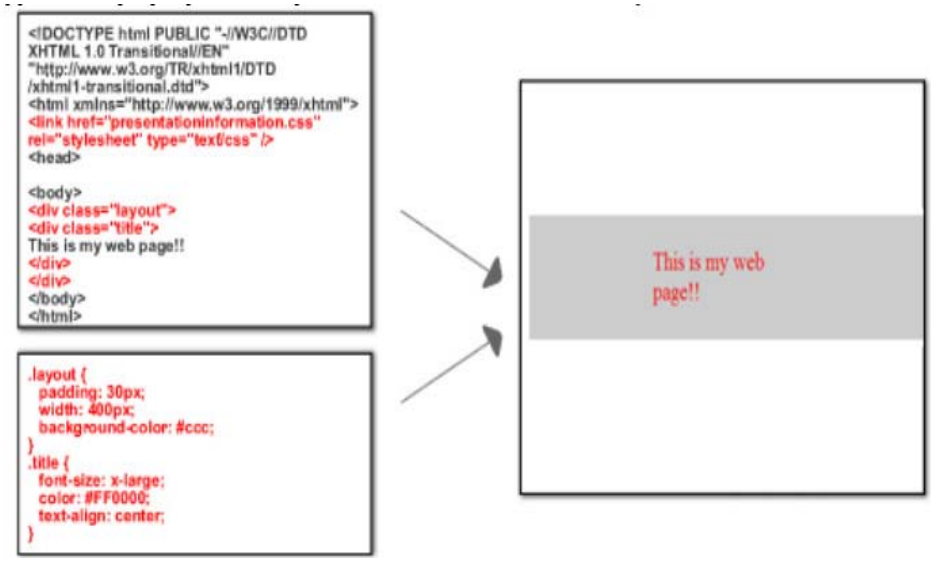
Εικόνα 1: Κατασκευή ιστοσελίδων στη δεκαετία του '90

Γράφουμε τον απαιτούμενο κώδικα αριστερά και η σελίδα μου εμφανίζεται δεξιά.

2.1.2 Κατασκευή ιστοσελίδων σήμερα

Η μορφοποίηση (design) διαχωρίζεται από την html σε ένα CSS αρχείο. Αυτό διευκολύνει τον κατασκευαστή της ιστοσελίδας, αλλά ακόμη απαιτείται η γνώση γραφής κώδικα.

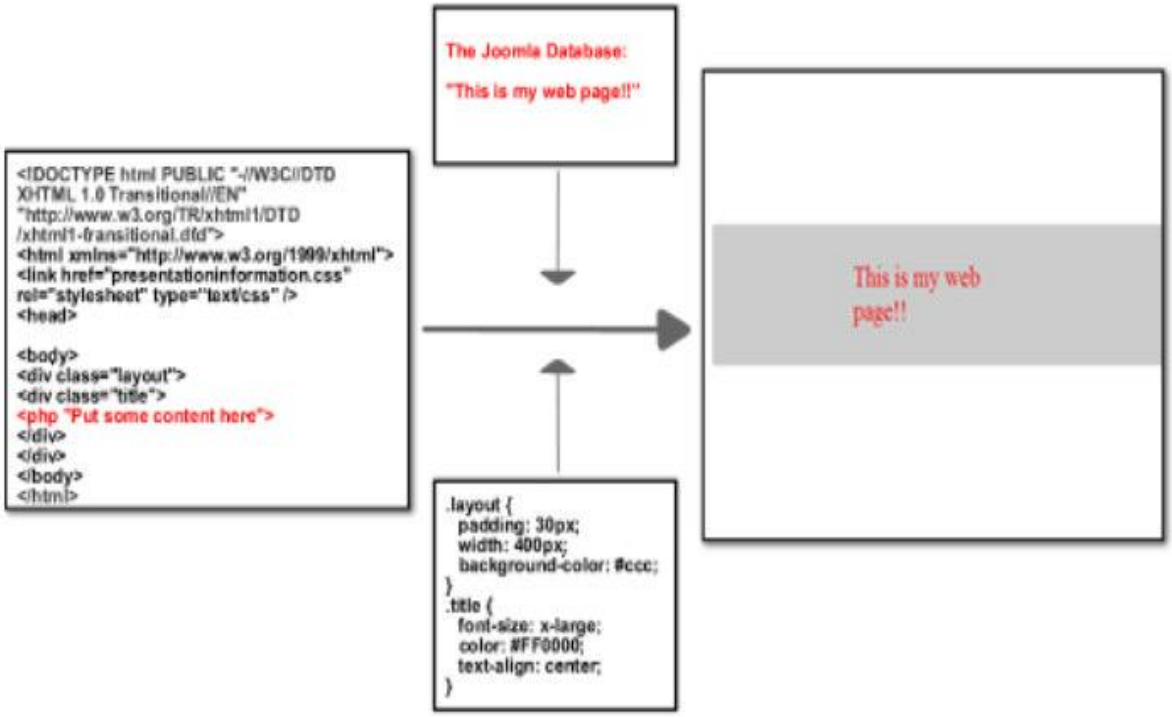
Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



Εικόνα 2: Κατασκευή ιστοσελίδων σήμερα

2.1.3 Κατασκευή ιστοσελίδων με CMS εργαλείο

Χρησιμοποιώντας σήμερα ένα CMS εργαλείο για την κατασκευή μιας ιστοσελίδας, αυτό που πρέπει να γνωρίζει ο κατασκευαστής της ιστοσελίδας είναι πώς να γράψει το κόκκινο κείμενο στο σχήμα της εικόνας που ακολουθεί.



Εικόνα 3: Κατασκευή ιστοσελίδων με CMS εργαλείο

2.2 Ορισμός του CMS

Ένα σύστημα διαχείρισης περιεχομένου (CMS) υποστηρίζει την δημιουργία, την διαχείριση, την διάθεση, την έκδοση και την ανακάλυψη εταιρικών πληροφοριών.

Δηλαδή, αυτό μπορεί να είναι:

- Λογισμικό το οποίο χρησιμοποιείται για την οργάνωση και εξυπηρέτηση συνεργατικής δημιουργίας εγγράφων και άλλου τύπου περιεχομένων.
- Λογισμικό το οποίο χρησιμοποιείται για τη δημιουργία της υποδομής πάνω στην οποία θα στηθεί ένας δυναμικός δικτυακός τόπος.
- Ένα πακέτο λογισμικού σχεδιασμένο για τη διαχείριση ενός ιστότοπου. Διαχειρίζεται ολόκληρο τον κύκλο ζωής μιας σελίδας από τη δημιουργία της μέχρι και την αρχειοθέτησή της.
- Μια λύση για τη δημιουργία custom portals.

Τρείς βασικές κατηγορίες των CMS είναι:

- Enterprise CMS
- Web CMS
- Component CMS

2.2.1 Enterprise CMS

Ο όρος Enterprise CMS αναφέρεται στις τεχνολογίες, τις στρατηγικές, τις μεθόδους και τα εργαλεία που χρησιμοποιούνται για την συλλογή, διαχείριση, αποθήκευση, διατήρηση, και παράδοση των περιεχομένων και των εγγράφων που σχετίζονται με έναν οργανισμό και τις διαδικασίες του. Τα Enterprise CMS εργαλεία επιτρέπουν τη διαχείριση των πληροφοριών ενός οργανισμού.

2.2.2 Component CMS

Το Component CMS διαχειρίζεται περιεχόμενα σε ένα σπυρωτό επίπεδο περιεχομένων παρά ένα επίπεδο εγγράφου. Κάθε περιεχόμενο παρουσιάζει ένα μεμονωμένο θέμα, έννοια ή ένα απόκτημα. Τα συστατικά συγκεντρώνονται σε πολλαπλά περιεχόμενα και μπορούν να θεαθούν σαν ψηφιακά ή παραδοσιακά έγγραφα. Κάθε συστατικό έχει το δικό του κύκλο ζωής και μπορεί να εντοπιστεί μεμονωμένα σαν μέρος μιας σύναξης. Το CCMS χρησιμοποιείτε χαρακτηριστικά σε πολλαπλά κανάλια όσον αφόρα την πελατειακή επεξεργασία περιεχομένων.

2.3 Ορισμός του Web-cms

Το σύστημα διαχείρισης περιεχομένου (CMS) είναι μια εφαρμογή που χρησιμοποιείται για να δημιουργήσει, να επεξεργαστεί, να διαχειριστεί και για να δημοσιεύσει ιστοσελίδες στο διαδίκτυο. Τα συστήματα διαχείρισης περιεχομένου (CMS) μπορούν να χρησιμοποιηθούν για να κατασκευάσουν ιστοτόπους όπως:

- Εταιρικούς

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

- Προσωπικούς
- Εκπαιδευτικούς
- Ηλεκτρονικά καταστήματα
- Ενημερωτικούς

Γενικά, σε ιστοτόπους που μπορούν να καλύψουν σχεδόν όλη την γκάμα των ενδιαφερομένων. Το περιεχόμενο που μπορεί να χρησιμοποιηθεί περιλαμβάνει κείμενα, εικόνες, ήχο, video, ηλεκτρονικά αρχεία και γενικά οτιδήποτε μπορεί να διανεμηθεί μέσω του διαδικτύου.

Ένα σύστημα διαχείρισης περιεχομένου (CMS) πρέπει να υποστηρίζει:

- Εύκολη διαχείριση περιεχομένου μέσω ενός browser.
- Διαφορετικούς ρόλους και επίπεδα για τους χρήστες.
- Δυνατότητα δημοσίευσης περιεχομένου από χρήστες έπειτα από την έγκριση του διαχειριστή.
- Δυνατότητα κατηγοριοποίησης του περιεχομένου ώστε να είναι ευκολότερη η διαχείριση του.
- Διαχωρισμός περιεχομένου και εμφάνισης (για παράδειγμα, οποιαδήποτε στιγμή να μπορούμε να αλλάξουμε το φόντο της σελίδας ή το στυλ της γραμματοσειράς μία φόρα και να εφαρμοστεί σε όλες τις σελίδες).

2.3.1 Ελεύθερο λογισμικό

Το ελεύθερο λογισμικό όπως ορίζεται από το Ίδρυμα Ελευθέρου Λογισμικού (Free Software Foundation), είναι λογισμικό που μπορεί να χρησιμοποιηθεί, αντιγραφεί, μελετηθεί, τροποποιηθεί και αναδιανεμηθεί χωρίς περιορισμό. Η ελευθερία από τέτοιους περιορισμούς είναι βασικό στοιχείο στην ιδέα του "ελεύθερου λογισμικού", έτσι ώστε το αντίθετο του ελεύθερου λογισμικού να είναι το ιδιόκτητο λογισμικό και όχι το λογισμικό που πωλείται για κέρδος, όπως το εμπορικό λογισμικό. Το ελεύθερο λογισμικό ορισμένες φορές αναφέρεται και σαν ανοιχτό λογισμικό ή λογισμικό ανοιχτού κώδικα αλλά οι δύο έννοιες δεν είναι ταυτόσημες.

2.3.2 Άδειες ελευθέρου λογισμικού

Εν γένει, σύμφωνα με την ισχύουσα νομοθεσία περί πνευματικής ιδιοκτησίας, η ελεύθερη αντιγραφή, διανομή και τροποποίηση του λογισμικού δεν επιτρέπεται. Για το λόγο αυτό, οι εκδόσεις ελευθέρου λογισμικού κάνουν χρήση ειδικής άδειας (free software license) σύμφωνα με την οποία, παραχωρείται το δικαίωμα αντιγραφής, τροποποίησης και αναδιανομής του λογισμικού στους χρήστες.

Σύμφωνα με το Ίδρυμα Ελευθέρου Λογισμικού, οι άδειες χρήσης ελευθέρου λογισμικού πρέπει να περιλαμβάνουν τις εξής ελευθερίες:

Ελευθερία 0: Ελευθερία χρήσης του προγράμματος για οποιονδήποτε σκοπό.
Ελευθερία 1: Ελευθερία μελέτης και τροποποίησης του προγράμματος.
Ελευθερία 2: Ελευθερία αντιγραφής του προγράμματος.
Ελευθερία 3: Ελευθερία βελτίωσης του προγράμματος και επανέκδοσής του, προς το συμφέρον της κοινότητας των χρηστών.

Οι ελευθερίες 1 και 3 προϋποθέτουν την πρόσβαση των χρηστών στον πηγαίο κώδικα του λογισμικού.

2.3.3 Δυνατότητες, χαρακτηριστικά και πλεονεκτήματα ενός CMS

Επιγραμματικά, μερικές από τις δυνατότητες, τα πλεονεκτήματα και τα χαρακτηριστικά ενός ολοκληρωμένου CMS είναι:

- Παρέχει τη δυνατότητα της διαχείρισης-συντήρησης ενός ιστότοπου από απλούς χειριστές χωρίς την απαίτηση για εμπλοκή ειδικού τεχνικού προσωπικού.
- Παρέχει δηλαδή την ευκαιρία ο διαχειριστής του να επικεντρωθεί στο περιεχόμενο και όχι στην τεχνολογία.
- Αυτό έχει σαν αποτέλεσμα την ταυτόχρονη ενημέρωση από πολλούς χρήστες και διαφορετικούς υπολογιστές, καθώς επίσης και την γρήγορη ενημέρωση, διαχείριση και αρχειοθέτηση του περιεχομένου του δικτυακού τόπου.
- Αυτοματοποιεί εργασίες ρουτίνας π.χ. εφαρμόζει την ίδια μορφοποίηση (layout) σε όλες τις ιστοσελίδες. Οι επιλογές (menus) και γενικότερα η πλοήγηση αναπαράγεται επίσης αυτόματα.
- Παρέχει απλά εργαλεία (επεξεργαστές σαν το Word) για τη δημιουργία του περιεχομένου, τα οποία είναι εύκολα στη χρήση και υπάρχει άμεση γνώση του τελικού αποτελέσματος, όπως γίνεται με τους γνωστούς κειμενογράφους.
- Δυνατότητα αναζήτησης του περιεχομένου που καταχωρείται και αυτόματη δημιουργία αρχείου.
- Ασφάλεια και προστασία του σχεδιασμού του site από λανθασμένες ενέργειες, που θα μπορούσαν να δημιουργήσουν προβλήματα στην εμφάνισή του.
- Διαχωρισμός του περιεχομένου από το σχεδιασμό και την πλοήγηση (navigation) του δικτυακού τόπου.
- Αλλαγή σχεδιασμού ή τρόπου πλοήγησης χωρίς να είναι απαραίτητη η ενημέρωση όλων των σελίδων από τον ίδιο το χρήστη.
- Αυτόματη δημιουργία των συνδέσμων μεταξύ των σελίδων και αποφυγή προβληματικών ανύπαρκτων σελίδων (404 error pages).
- Όλες τις τεχνικές λεπτομέρειες τις χειρίζεται το ίδιο το σύστημα, επιτρέποντας έτσι σε οποιονδήποτε να διαχειριστεί και να ενημερώνει τον ιστότοπο.
- Μικρότερος φόρτος στον εξυπηρετητή (server) και χρήση λιγότερου χώρου, αφού δεν υπάρχουν πολλές επαναλαμβανόμενες στατικές σελίδες, από τη στιγμή που η ανάπτυξη των σελίδων γίνεται δυναμικά.
- Όλο το περιεχόμενο καταχωρείται στην/στις βάσεις δεδομένων, τις οποίες μπορούμε πιο εύκολα και γρήγορα να τις προστατεύσουμε τηρώντας αντίγραφα ασφαλείας.
- Όλα τα δυναμικά χαρακτηριστικά του συστήματος επιτρέπουν στον ιστότοπο να αναπτύσσεται συγχρόνως με την εκάστοτε επιχείρηση.
- Μεγαλύτερη ομοιομορφία και συνοχή στον ιστότοπο.
- Βελτιωμένο σύστημα πλοήγησης.
- Αυξημένη ευελιξία.
- Μειωμένα έξοδα συντήρησης-διαχείρισης.
- Αυξημένη ικανότητα ανάπτυξης.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

- Υποστήριξη των επιχειρηματικών στόχων και στρατηγικών π.χ. ένα CMS μπορεί να βοηθήσει στη βελτίωση-αύξηση των πωλήσεων, στην αύξηση της ικανοποίησης του πελάτη ή στο να βοηθήσει στην επικοινωνία με το κοινό.

2.4 Διαθέσιμα Web-CMS

Τα διαθέσιμα CMS χωρίζονται σε 3 κατηγορίες:

- CMS κλειστού κώδικα.
- CMS ανοιχτού κώδικα.
- Παραμετροποιημένα CMS βασισμένα σε πλαίσια ανοιχτού κώδικα. Η κατηγορία αυτή ουσιαστικά είναι μια μίξη των παραπάνω.

Εικόνα 4: Τα πιο δημοφιλή CMS

2.4.1 CMS κλειστού κώδικα

Τα CMS κλειστού κώδικα έχουν εμπορική υποστήριξη, καθώς και προσδιορισμένες υπηρεσίες. Σε ορισμένες περιπτώσεις μπορεί να είναι καλύτερα τεκμηριωμένα και πιο ασφαλή αλλά έχουν ένα βασικό μειονέκτημα. Αυτό είναι το κόστος. Εκτός από το βασικό κόστος υπάρχει το κόστος παραμετροποίησης καθώς και το κόστος ολοκλήρωσης με υπάρχοντα εταιρικά συστήματα.

2.4.2 Τα πιο δημοφιλή CMS κλειστού κώδικα

Vignette Content Management: Τα προϊόντα της Vignette βοηθούν τις επιχειρήσεις να αποκτήσουν και να διαχειρίζονται τις πληροφορίες που χρειάζονται. Είναι μια έμπειρη εταιρία αποδοτικότητας, η οποία στοχεύει στην αύξηση της παραγωγικότητας, μείωση του κόστους και στην βελτίωση της εμπειρίας του χρήστη. Οι Intranet, extranet και internet λύσεις της συμπεριλαμβάνουν portal, integration,

enterprise content management και δυνατότητες συνεργασίας που μπορούν να αποδώσουν μοναδικά προτερήματα.

IBM Workplace Web Content Management: Το συγκεκριμένο προϊόν παρέχει μία μεγάλη γκάμα λειτουργιών όπως: personalization, το web content management, η διαχείριση εγγράφων και οι λειτουργίες συνεργασίας και παραγωγικότητας στα πλαίσια της επεκτάσιμης υποδομής του WebShere Portal.

Jalios JCMS: Είναι ένα enterprise content management (ECM) που αναπτύχθηκε από την Jalios, μια γαλλική εταιρεία που ιδρύθηκε το 2001 και εδρεύει στο Παρίσι, Γαλλία. Περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα χαρακτηριστικά: διαχείρισης περιεχομένου, διαχείριση εγγράφων, collaboration, workflow και πύλες.

Dynamicweb: Είναι προϊόν της Dynamicweb Software Ltd η οποία εξειδικεύεται στην παροχή web-based λύσεις λογισμικού για την επαγγελματική αγορά. Όλα τα προϊόντα είναι modular και έχουν επεκταθεί εύκολα για να ταιριάζουν στις ανάγκες των πελατών. Η Dynamicweb Software Ltd αναπτύσσει τρία κύρια προϊόντα Synkron Via, Dynamicweb ηλεκτρονικού εμπορίου και Dynamicweb CMS. Το Dynamicweb CMS είναι ένα πολυγλωσσικό και φιλικό Σύστημα Διαχείρισης Περιεχομένου (CMS), το οποίο μπορεί να χρησιμοποιηθεί για τη διαχείριση του περιεχομένου στους δικτυακούς τόπους, extranets και Intranets. Βασίζεται στην τεχνολογία Microsoft .NET και έχει επιλεχθεί σε περισσότερες από 3.000 εταιρίες και Οργανισμούς σε διάφορες χώρες. (Iterating, 2009)

Powerfront CMS: Το PowerFront παρέχει μια ολοκληρωμένη λύση διαχείρισης περιεχομένου που μπορεί να περιλαμβάνει: τη διαχείριση περιεχομένου, τον σχεδιασμό ιστοσελίδων, θέματα ασφάλειας, το ηλεκτρονικό εμπόριο, procurement, reporting options και υποστήριξη. Στόχος της είναι η υποστήριξη ιστοσελίδων των επιχειρήσεων, intranets, extranets ή procurement websites.

2.4.3 CMS ανοικτού κώδικα

Στις εφαρμογές ανοικτού κώδικα επιτρέπεται η πρόσβαση και η αλλαγή του πηγαίου κώδικα. Το κόστος της εφαρμογής μειώνεται δραματικά καθώς στις περισσότερες περιπτώσεις ολόκληρη η εφαρμογή βρίσκεται στο διαδίκτυο και ο ενδιαφερόμενος την κατεβάζει με μηδενικό κόστος παρόλα αυτά, τυπικά απαιτούνται τουλάχιστον κάποιες τεχνικές γνώσεις για να στηθεί η εφαρμογή και να λειτουργήσει. Υποστηρίζονται από μία κοινότητα χρηστών και προγραμματιστών και συχνά συνοδεύονται από πρόσθετα (plug-ins) τα οποία δημιουργεί και προσφέρει η κοινότητα.

2.4.4 Τα πιο δημοφιλή CMS ανοιχτού κώδικα

Joomla: Είναι ένα σύστημα διαχείρισης περιεχομένου (CMS) με αρκετές δυνατότητες, εξαιρετικά ευέλικτο και φιλικό. Η εφαρμογή αυτή χρησιμοποιείται για τη δημοσίευση στο διαδίκτυο μιας προσωπικής ιστοσελίδα, αλλά και ενός εταιρικού δικτυακού τόπου. Είναι προσαρμόσιμο σε περιβάλλοντα επιχειρηματικής κλίμακας όπως τα intranets μεγάλων επιχειρήσεων ή οργανισμών. Οι δυνατότητες επέκτασής του είναι πρακτικά μεγάλες.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Drupal: Είναι ένα αρθρωτό σύστημα διαχείρισης περιεχομένου (CMS), γραμμένο στη γλώσσα προγραμματισμού php. Το Drupal, όπως πολλά σύγχρονα CMS, επιτρέπει στο διαχειριστή συστήματος να οργανώνει το περιεχόμενο, να προσαρμόζει την παρουσίαση, να αυτοματοποιεί διαχειριστικές εργασίες και να διαχειρίζεται τους επισκέπτες του ιστοτόπου και αυτούς που συνεισφέρουν. Παρόλο που υπάρχει μια πολύπλοκη προγραμματιστική διεπαφή, οι περισσότερες εργασίες μπορούν να γίνουν με λίγο ή και καθόλου προγραμματισμό. Το Drupal ορισμένες φορές περιγράφεται ως "υποδομή για εφαρμογές ιστού", καθώς οι δυνατότητές του προχωρούν παραπέρα από τη διαχείριση περιεχομένου, επιτρέποντας ένα μεγάλο εύρος υπηρεσιών και συναλλαγών.

Xoops: Το Xoops χρησιμοποιεί μια σπονδυλωτή αρχιτεκτονική που επιτρέπει στους χρήστες του να προσαρμόσουν, να ενημερώνουν και διαφοροποιήσουν θεματικά τους ιστοχώρους τους. Είναι γραμμένο σε php και κυκλοφορεί υπό τους όρους της GNU Γενικής Δημόσιας Άδειας (GPL).

2.4.5 Πλεονεκτήματα Web-CMS ανοιχτού κώδικα

Τα Web-CMS ανοιχτού κώδικα έχουν αρκετά πλεονεκτήματα. Τα κυριότερα από τα οποία αναφέρονται παρακάτω:

- Αναμφισβήτητα το να έχεις τη δυνατότητα να δημιουργήσεις έναν ιστότοπο από το μηδέν χωρίς εξειδικευμένες τεχνικές γνώσεις σου προσφέρει χαμηλό κόστος.
- Πληρώνεις για την υπηρεσία και την υποστήριξη που σου παρέχεται και όχι για το λογισμικό.
- Ευκολία παραμετροποίησης.
- Υπάρχει υποστήριξη και βοήθεια των χρηστών του Web-CMS από την Κοινότητα του (forums).
- Υπάρχει απεριόριστη ευκολία ολοκλήρωσης με τα υπάρχοντα λογισμικά.

Κεφάλαιο 3 Η αρχιτεκτονική ενός CMS ανοιχτού κώδικα-Joomla

3.1 Η ιστορία του Joomla

3.1.1 Το Joomla μέσα στο χρόνο

Το Joomla δημιουργήθηκε ως αποτέλεσμα της διάσπασης του development team του Mambo στις 17 Αυγούστου 2005. Την εποχή εκείνη, το όνομα Mambo ήταν εμπορικό σήμα της Miro International Pvt Ltd, οι οποίοι αποτελούσαν ένα μη κερδοσκοπικό ίδρυμα με δεδηλωμένο σκοπό τη χρηματοδότηση του έργου και την προστασία από μηνύσεις.

Το development team του Mambo δημιούργησε μια ιστοσελίδα που ονομάστηκε OpenSourceMatters με σκοπό να διανέμουν πληροφορίες στους χρήστες, προγραμματιστές, σχεδιαστές ιστοσελίδων και στην κοινότητα γενικότερα. Ο αρχηγός της ομάδας, Andrew Eddie, γνωστός και ως "Masterchief" έγραψε μια ανοιχτή επιστολή προς την Κοινότητα, η οποία εμφανίστηκε στο τμήμα ανακοινώσεις του δημόσιου φόρουμ στο mamboserver.com.

Χιλιάδες άνθρωποι εντάχθηκαν στην opensourcematters.org ιστοσελίδα μέσα σε μια μέρα οι περισσότεροι για να αποσπάσουν λόγια ενθάρρυνσης και στήριξης. Ωστόσο, η Miro CEO Peter Lamont δημοσίευσε μια απάντηση στο development team, σε άρθρο με τίτλο "Το Mambo Open Source Controversy-20 ερωτήσεις με την Miro". Το γεγονός αυτό δημιούργησε αντιπαραθέσεις εντός της κοινότητας του ελεύθερου λογισμικού για τον ορισμό του "ανοικτού κώδικα".

Δύο εβδομάδες μετά την ανακοίνωση του Andrew Eddie, οι ομάδες αναδιοργανώθηκαν και η κοινότητα εξακολούθησε να αυξάνεται. Ο Eben Moglen και το Software Freedom Law Center (SFLC) βοήθησαν την βασική ομάδα του Joomla που αρχίζει τον Αύγουστο του 2005. Η SFLC συνεχίσει να παρέχει νομική καθοδήγηση για το Joomla.

Στις 18 του Αυγούστου 2005, γίνεται έκκληση για τη συμβολή της Κοινότητας στο να προτείνει ονόματα για το project. Η βασική ομάδα ανέφερε ότι θα λάβει την τελική απόφαση για το όνομα του project με βάση τα στοιχεία της κοινότητας. Η ομάδα πυρήνας τελικά επέλεξε το όνομα να μην είναι από τον κατάλογο των ονομάτων που προτείνονται από την κοινότητα.

Την 1η Σεπτεμβρίου 2005, το νέο όνομα, "Joomla!", ανακοινώθηκε. Το οποίο είναι η αγγλική ορθογραφία του jumla αραβική λέξη που σημαίνει "όλοι μαζί" ή "ως σύνολο", καθώς και "πρόταση".

Το Joomla (Joomla 1.0.0) κυκλοφόρησε στις 16 Σεπτεμβρίου 2005. Ήταν μια νέα εμπορική απελευθέρωση του Mambo 4.5.2.3. Το Joomla δημιουργήθηκε σε συνδυασμό άλλων σφαλμάτων και μέτριων-διορθώσεων σε επίπεδο ασφαλείας. Κέρδισε το Packt Publishing Open Source Content Management System Award το 2006 και το 2007. (http://en.wikipedia.org/wiki/Joomla)

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

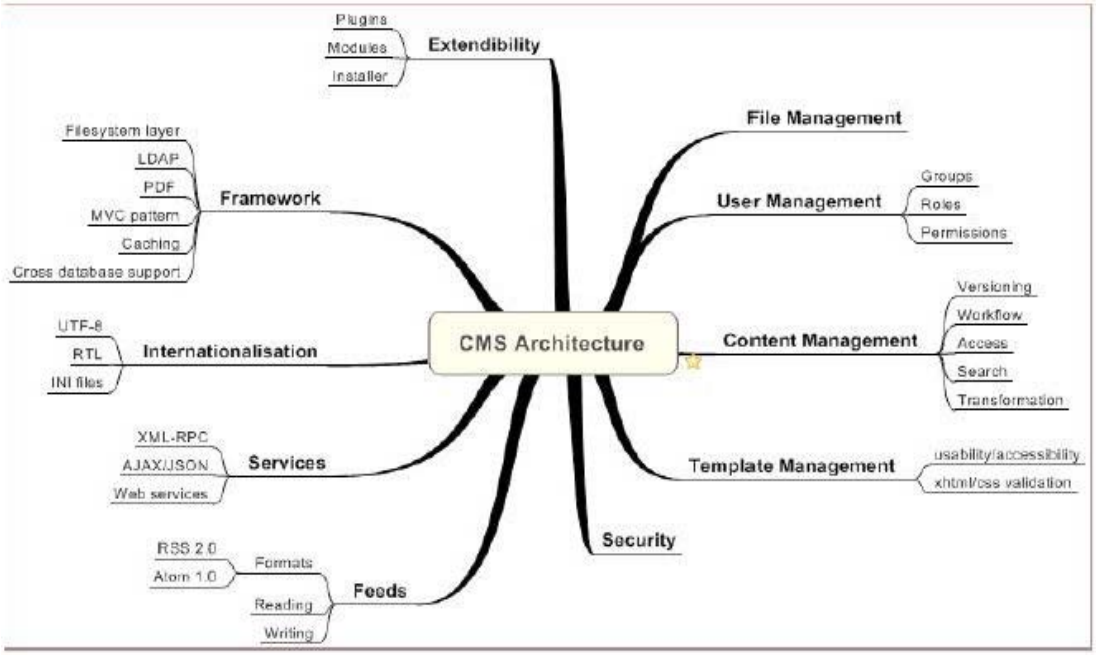
3.2 Χαρακτηριστικά του Joomla

Λαμβάνοντας υπόψη τις παρατηρήσεις των χρηστών του Joomla μπορούμε να πούμε ότι τα πιο σημαντικά χαρακτηριστικά του είναι:

- Χρησιμοποιεί τις καλύτερες διαθέσιμες τεχνολογίες: mysql για τη Βάση Δεδομένων, php για την προγραμματιστική λογική, xml, css2 και δυνατότητα RSS.
- Ο πλήρης μηχανισμός διαχείρισης της βάσης δεδομένων του site.
- Τμήματα για Νέα Προϊόντα ή Υπηρεσίες είναι πλήρως επεξεργάσιμα, διαχωρίσιμα και εύχρηστα.
- Τμήματα με θεματικές ενότητες μπορούν να προστεθούν από διαφορετικούς συντάκτες.
- Πλήρως παραμετροποιημένο περιεχόμενο και περιβάλλον, συμπεριλαμβανομένων των θέσεων του αριστερού, κεντρικού και δεξιού μενού.
- Ευκολία στη χρήση του ακόμα και για αρχάριους χρήστες Η/Υ.
- Είναι πολυγλωσσικό.
- Ανέβασμα φωτογραφιών μέσω του φυλλομετρητή του χρήστη, σε δική του βιβλιοθήκη για χρήση οπουδήποτε στον ιστοχώρο.
- Έχει τη δυνατότητα δημιουργίας πολλών επιπέδων χρηστών.
- Δυναμική υποστήριξη Forum/Ψηφοφορίας για τα επί τόπου αποτελέσματα.
- Υπάρχει ειδικός μηχανισμός για της μηχανές αναζήτησης.
- "Τρέχει" σε Linux, FreeBSD, MacOSX server, Solaris και AIX.

3.3 Η αρχιτεκτονική του Joomla

Το Joomla αποτελείται από πολλά διαφορετικά μέρη, τα οποία επιτρέπουν στις επεκτάσεις να γίνουν εύκολα. Θα μπορούσαμε να το περιγράψουμε ως συναφές και πολύπλοκο σύστημα και όχι ως ένα μπλεγμένο σύνολο από γεγονότα και συσχετίσεις.



Εικόνα 5: Η αρχιτεκτονική ενός CMS

Βάσει των παραπάνω διαχωρίζουμε το CMS σε τρία βασικά υποσυστήματα:

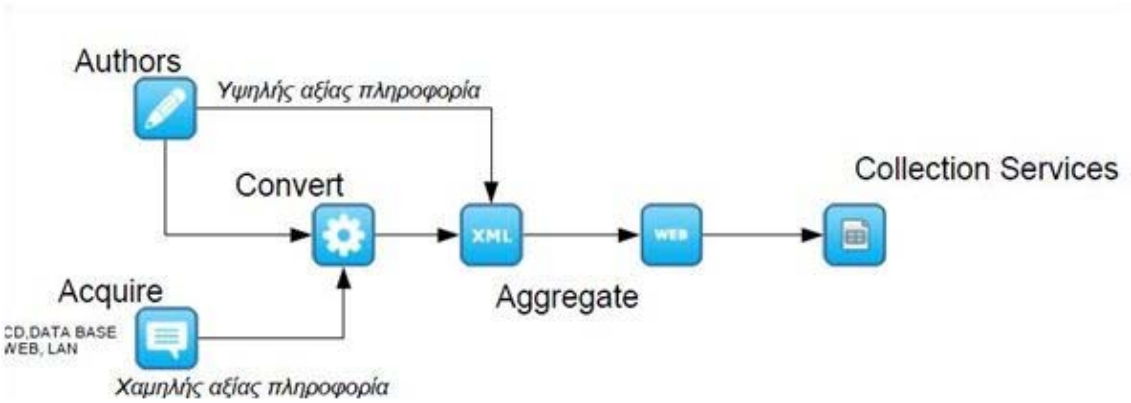
1. Το υποσύστημα συλλογής (Collection System).
2. Το υποσύστημα διαχείρισης (Management System).
3. Το υποσύστημα δημοσίευσης (Publishing System).

3.3.1 Το υποσύστημα συλλογής (Collection System)

Το υποσύστημα συλλογής είναι υπεύθυνο για όλες τις διεργασίες που γίνονται προτού η πληροφορία γίνει έτοιμη για δημοσίευση. Μετατρέπει την ακατέργαστη πληροφορία σε καλά οργανωμένο περιεχόμενο. Στην παρακάτω εικόνα φαίνονται τα στάδια της συλλογής που είναι:

- **Συγγραφή (Authoring)**: Δημιουργείται το περιεχόμενο εξολοκλήρου από την αρχή.
- **Απόκτηση (Acquisition)**: Συλλέγεται το περιεχόμενο από υπάρχουσες πηγές.
- **Μετατροπή (Conversion)**: Εξάγονται οι μη απαραίτητες πληροφορίες από το περιεχόμενο και αν είναι ανάγκη αλλάζει και η μορφή του.
- **Συσσώρευση (Aggregation)**: Επεξεργαζόμαστε το περιεχόμενο, το διαιρούμε σε τμήματα και το προσαυξάνουμε με τα απαραίτητα μεταδεδομένα.
- **Υπηρεσίες Συλλογής (Collection Services)**: Είναι ΣΔΠ, προγράμματα και συναρτήσεις που βοηθούν στη διαδικασία συλλογής. Παραδείγματος χάρη μια υπηρεσία συλλογής είναι οι web forms στις οποίες εισάγουμε περιεχόμενο.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



Εικόνα 6: Σχηματική απεικόνιση των λειτουργιών του υποσυστήματος συλλογής

3.3.2 Το υποσύστημα διαχείρισης (Management System)

Το υποσύστημα διαχείρισης είναι υπεύθυνο για την μακροχρόνια αποθήκευση των συστατικών περιεχομένου καθώς και για κάθε είδους αρχείο που χρησιμοποιείται. Περιέχει την αποθήκη περιεχομένου, το workflow καθώς και δυνατότητες διαχείρισης.

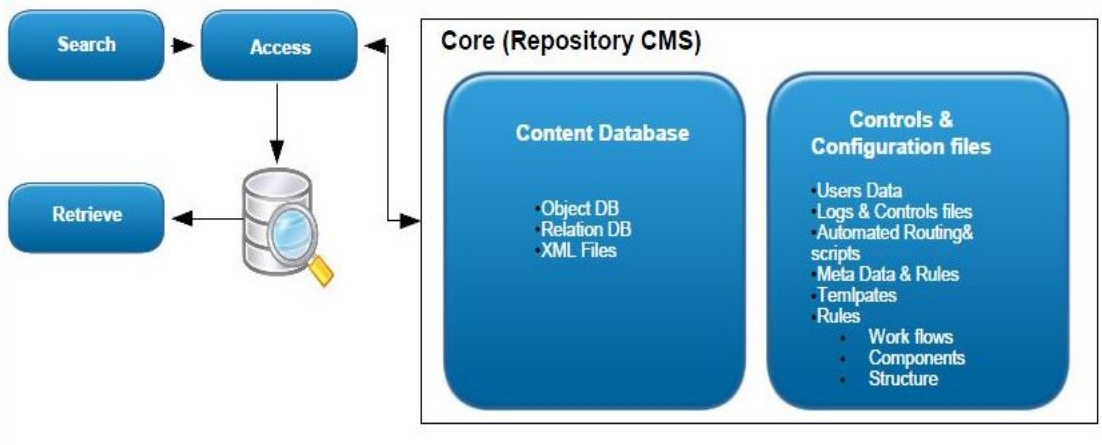
Το CMS πρέπει να είναι ικανό να μας πληροφορεί για τα ακόλουθα:

- Λεπτομέρειες για το περιεχόμενο, δηλαδή τι είδους συστατικά περιεχομένου έχουν συλλεχθεί και σε πιο στάδιο του κύκλου ζωής τους βρίσκονται.
- Πόσο καλά αρχικοποιημένο είναι το υλικό μας και αν μπορεί να δημιουργηθεί συμφόρηση (bottleneck).
- Πως χρησιμοποιούμε τα συστατικά στις δημοσιεύσεις και πιο περιεχόμενο δεν χρησιμοποιείται ή είναι έτοιμο για διαγραφή.
- Ποιος έχει πρόσβαση και πού στο περιεχόμενο και ποιος έχει συνεισφέρει το περισσότερο.

Δηλαδή, πρέπει να βρίσκουμε απαντήσεις στο σύστημα διαχείρισης για οτιδήποτε σχετικά με το περιεχόμενο, τις δημοσιεύσεις και το υποσύστημα συλλογής.

Για να μπορέσει το υποσύστημα διαχείρισης να μας προσφέρει αυτές τις δυνατότητες περιέχει:

- **Αποθηκευτικό χώρο**: Ένα μέρος για την αποθήκευση του περιεχομένου.
- **Διαχείριση**: Ένα σύστημα διαχείρισης για τις ρυθμίσεις του CMS.
- **Workflow**: Καθορισμένα σύνολα βημάτων για την πραγματοποίηση της εργασίας ώστε το περιεχόμενο να γίνει έτοιμο προς δημοσίευση.
- **Συνδέσεις**: Ένα σύνολο συνδέσεων (υλικού και λογισμικού) συνήθως μέσα στον οργανισμό μεταξύ δικτύων, εξυπηρετητών και αποθηκών δεδομένων.



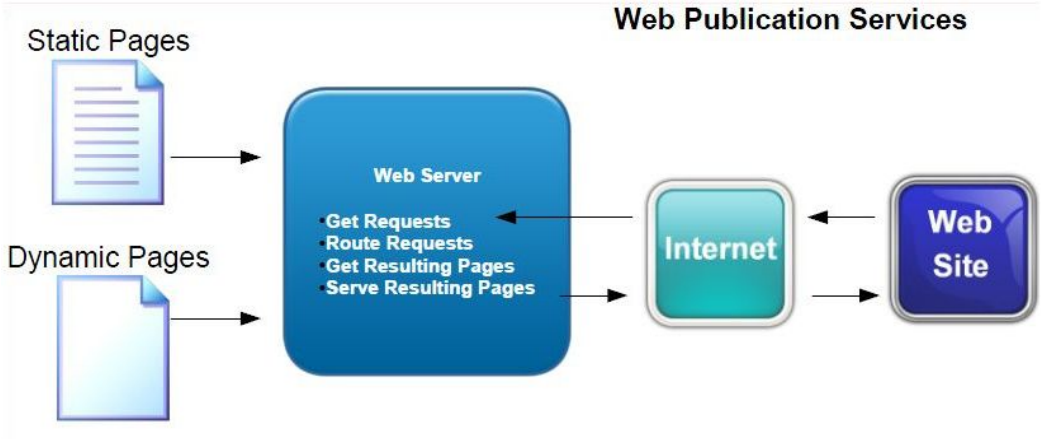
Εικόνα 7: Σχηματική απεικόνιση των λειτουργιών του υποσυστήματος διαχείρισης

3.3.3 Το υποσύστημα δημοσίευσης (Publishing System)

Το υποσύστημα δημοσίευσης είναι υπεύθυνο για την εξαγωγή περιεχομένου από τον αποθηκευτικό χώρο των δεδομένων και την αυτόματη δημιουργία δημοσιεύσεων.

Ένα υποσύστημα δημοσίευσης περιλαμβάνει:

- **Φόρμες δημοσιεύσεων (Publishing Templates)**: Προγράμματα που δημιουργούν δημοσιεύσεις αυτόματα.
- **Υπηρεσίες δημοσιεύσεων**: Ένα σύνολο εργαλείων που ελέγχουν τι έχει δημοσιευτεί και πώς έχει δημοσιευτεί.
- **Συνδέσεις**: Μέθοδοι και εργαλεία που χρησιμοποιούνται για να εισάγουν δεδομένα από συστήματα έξω από το ΣΔΠ.
- **Δημοσιεύσεις ιστού (Web publications)**: Η πιο συνηθισμένη έξοδος για ΣΔΠ.
- **Άλλες δημοσιεύσεις**: Διαφορετικές δημοσιεύσεις από τις δημοσιεύσεις ιστού όπως ηλεκτρονικές δημοσιεύσεις και δημοσιεύσεις εκτύπωσης.



Εικόνα 8: Σχηματική απεικόνιση των λειτουργιών του υποσυστήματος δημοσίευσης

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

3.4 Η δομή του Joomla

3.4.1 Δημόσιο τμήμα και περιοχή διαχείρισης (Front-end και Back-end)

Ένα web cms αποτελείται από ένα Front-end και ένα Back-end. Το δημόσιο τμήμα (Front-end) είναι στην ουσία αυτό που βλέπουν οι επισκέπτες και οι συνδεδεμένοι χρήστες στο site, δηλαδή οι τελικοί χρήστες. Μέσα στο δημόσιο τμήμα βρίσκονται τα άρθρα, τα μενού και γενικά όλα τα στοιχεία που θέλουμε να εμφανίζονται στην ιστοσελίδα μας.

Η περιοχή διαχείρισης θα μπορούσαμε να πούμε ότι είναι το "εργαστήριο" του Joomla. Περιέχει το administration layer του δικτυακού τόπου για τους διαχειριστές. Η διαμόρφωση, η συντήρηση, ο καθαρισμός, η παραγωγή των στατιστικών, καθώς και η δημιουργία νέου περιεχομένου γίνονται όλα στο Back-end από εξουσιοδοτημένα άτομα. Το Back-end βρίσκεται σε διαφορετική διεύθυνση URL από την ιστοσελίδα.

3.4.2 Δικαιώματα πρόσβασης (Access Rights)

Κάθε φορά που μιλάμε για διαχείριση, μιλάμε για την έξυπνη διαχείριση των υφιστάμενων πόρων. Σε web cms, τα ονόματα χρηστών αποδίδονται στα ενδιαφερόμενα άτομα και κάθε ένα από αυτά έχει διαφορετικά δικαιώματα πρόσβασης. Αυτό μπορεί να κυμαίνεται από ένα απλό εγγεγραμμένο χρήστη μέχρι τον «υπέρ-διαχειριστή», ο οποίος έχει τον πλήρη έλεγχο του τομέα. Στη συνέχεια με βάση τα δικαιώματα, η ιστοσελίδα, εμφανίζει διαφορετικό περιεχόμενο. Υπάρχει διαθέσιμη επιλογή για να γίνει επεξεργασία του περιεχομένου απευθείας στο Front-end ή ο χρήστης έχει το δικαίωμα να εργάζονται στο Back-end.

3.4.3 Περιεχόμενο (Content)

Το περιεχόμενο μπορεί να έχει διάφορες μορφές. Στην απλούστερη περίπτωση, είναι κείμενο. Ωστόσο, το περιεχόμενο μπορεί επίσης να είναι μια εικόνα, μια σύνδεση, ένα μουσικό κομμάτι, ένα απόσπασμα από μια εφαρμογή όπως το Google Maps ή ένας συνδυασμός όλων αυτών. Για να δώσουμε μια γενική άποψη της έννοιας περιεχόμενο, μπορεί να ενσωματώνεται σε δομές, για παράδειγμα, τα κείμενα των διαφόρων κατηγοριών αποτελούν περιεχόμενο. Οι κατηγορίες, φυσικά, είναι επίσης περιεχόμενο το οποίο πρέπει να διαχειριστεί.

3.4.4 Επεκτάσεις (Extensions)

Τα συστατικά μέρη, οι ενότητες, τα πρότυπα και τα πρόσθετα (plugins) αναφέρονται όλες ως επεκτάσεις (extensions). Προσφέρουν επιπλέον λειτουργίες οι οποίες δεν περιέχονται στον πυρήνα του Joomla.

3.4.5 Εφαρμογές (Components)

Το Joomla σαν web cms πρέπει να είναι επεκτάσιμο και σε θέση να αναπτυχθεί ανάλογα με τις απαιτήσεις. Οι επεκτάσεις που προσφέρουν επιπλέον λειτουργίες και συνήθως έχουν το δικό τους χώρο στη διαχείριση του Joomla ονομάζονται

εφαρμογές (components). Για παράδειγμα, τυπικές εφαρμογές των τελευταίων ετών είναι για ένα online κατάστημα, για μια gallery φωτογραφιών, καθώς και για e-learning ή forum. Σήμερα τα πράγματα όπως η βελτιστοποίηση μηχανών αναζήτησης, τα δικαιώματα των χρηστών, πολλαπλές μορφές σελίδων και ποικίλες δομές περιεχομένου γίνονται όλο και πιο σημαντικά.

Οι εφαρμογές (components) περιέχουν την επιχειρηματική λογική του site τους και απεικονίζουν το περιεχόμενο στο "κύριο σώμα" της ιστοσελίδας.

3.4.6 Πρότυπα (Templates)

Ένα πρότυπο είναι ένα είδος οπτικής απεικόνισης που τοποθετείται στην κορυφή του περιεχομένου. Καθορίζει χρώματα, γραμματοσειρές, μεγέθη γραμματοσειρών, εικόνες φόντου, αποστάσεις και διαχωρισμό της σελίδας, με άλλα λόγια, ό, τι έχει να κάνει με την εμφάνιση μιας σελίδας. Ένα πρότυπο αποτελείται από τουλάχιστον ένα αρχείο HTML για τη δομή της σελίδας και ένα αρχείο CSS για τον σχεδιασμό. Μπορεί επίσης να έχει μια πολύ πιο εκτεταμένη δομή, ώστε να προετοιμάσει το περιεχόμενο του Joomla για ένα τελείως διαφορετικό σκοπό.

3.4.7 Πρόσθετα (Plug-ins)

Τα προσθετά (plug-ins) είναι ένα κομμάτι κώδικα προγραμματισμού που είναι προσαρτημένα σε ορισμένα σημεία του πλαισίου του Joomla για να αλλάζουν τη λειτουργικότητά του. Ένα plug-in μπορεί, για παράδειγμα, να χρησιμοποιηθεί στο εσωτερικό περιεχόμενο του κειμένου για να φορτώσει το περιεχόμενο ενός ενθέματος (module) στο κείμενο. Τα plugins χρησιμοποιούνται επίσης σε μια ολοκληρωμένη ιστοσελίδα αναζήτησης, προκειμένου να ενσωματώσουν πρόσθετα εφαρμογές (components).

3.4.8 Ενθέματα (Modules)

Τα ενθέματα (modules) μπορούμε να τα παρομοιάσουμε σαν τα "κουτιά" μέσα στα οποία εμφανίζεται το περιεχόμενο, οι εφαρμογές, τα πρόσθετα και γενικά όλα τα αντικείμενα που εμφανίζονται στο δημόσιο τμήμα

3.4.9 Διαμόρφωση Ρυθμίσεων (Configuration Settings)

Οι ρυθμίσεις που ισχύουν για το σύνολο του δικτυακού τόπου προσδιορίζονται χρησιμοποιώντας τη διαμόρφωση ρυθμίσεων. Αυτό περιλαμβάνει το κείμενο τίτλου στο παράθυρο περιήγησης, λέξεις-κλειδιά για τις μηχανές αναζήτησης, διακόπτες που επιτρέπουν ή απαγορεύουν τη σύνδεση στο site ή το διακόπτη που θέτει ολόκληρο το site online ή offline και πολλές άλλες λειτουργίες.

3.4.10 Ροή εργασίας (Workflow)

Η έννοια ροή εργασίας συμπεριλαμβάνει μια ακολουθία εργασιών. Παραδείγματα ροών εργασίας μπορούμε να αντλήσουμε και από την καθημερινότητα, π.χ. μια μαγειρική συνταγή είναι επίσης μια ροή εργασίας.

Δεδομένου ότι πολλά άτομα εργάζονται με κάποιο CMS, καλά οργανωμένες ροές εργασίας είναι μια τεράστια βοήθεια. Μια ροή εργασίας επίσης αναφέρεται και σε

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

μια λίστα διεργασιών που ένας συγκεκριμένος χρήστης έχει να εκτελέσει. Για παράδειγμα, ο συντάκτης (editor) εντοπίζει μια λίστα των μη δημοσιευμένων πακέτων ειδήσεων, τα οποία αυτός ή αυτή πρέπει να εξετάσει την ορθότητά τους. Μετά την εξέταση αυτών, μαρκάρει αυτά τα πακέτα ειδήσεων ως ορθά και έπειτα τα πακέτα περνούν στην λίστα διεργασιών του εκδότη (publisher). Ο εκδότης αποφασίσει τότε αν θα δημοσιεύει κάθε είδηση στην πρώτη σελίδα.

3.4.11 Application Programming Interface (API)

Σήμερα ένα Application Programming Interface (API), πρέπει να συμβαδίζει με την εποχή. Πρέπει να δίνει τη δυνατότητα να υπάρχει πρόσβαση στο Joomla από άλλα προγράμματα. Αυτό ανοίγει εντελώς νέες εφαρμογές που δεν ήταν προηγουμένως εφικτές με Joomla. Ένα API είναι ο πιο σημαντικός σύνδεσμος μεταξύ τρίτων επεκτάσεων και του πυρήνα του Joomla.

3.5 Σύγκριση Joomla με άλλα cms

Το τελευταίο διάστημα διεξάγεται μια μεγάλη "μάχη" ανάμεσα στα συστήματα διαχείρισης περιεχομένου (cms) ανοιχτού κώδικα, με πολλές αξιόλογες προτάσεις. Η επιλογή δεν είναι εύκολη, κάθε εφαρμογή έχει πλεονεκτήματα και μειονεκτήματα, ενώ μεγάλο ρόλο στην τελική απόφαση παίζουν οι απαιτούμενες προδιαγραφές των υπό κατασκευή websites.

Συμφώνα με έρευνες των τελευταίων χρόνων τα τρία συστήματα διαχείρισης περιεχομένου που κυριαρχούν στην αγορά σήμερα είναι: WordPress, Joomla και Drupal. Πράγματι, οι αριθμοί δείχνουν ότι αυτά τα τρία συστήματα διαχείρισης περιεχομένου έχουν παίξει καθοριστικό ρόλο στην διαμόρφωση της αγοράς.

Το Joomla είναι ίσως το καταλληλότερο για αυτούς που αναζητούν ένα ιστότοπο απλό όσο αφόρα την ανάπτυξη, τη διαχείριση αλλά και τη χρήση του, χωρίς αυτό να σημαίνει ότι υστερεί σε ποιότητα και αξιοπιστία.

Αποτελεί ένα από τα πιο ενδιαφέροντα και ισχυρά open source CMS και αυτό οφείλετε τόσο στην αρχιτεκτονική του κώδικά του αλλά κυρίως στην κοινότητα που το περιβάλει και το υποστηρίζει. Το Joomla μπορεί να βρει εφαρμογή από μια προσωπική ιστοσελίδα στην οποία ο πελάτης θέλει να έχει δυναμικά στοιχεία έως μια μεγάλη επιχείρηση με δεκάδες χειριστές να ανανεώνουν το περιεχόμενο του, βάση group policies που ορίζονται από τους διαχειριστές.

Αρχικά, η δομή του δεν είναι περίπλοκη. Έχει αναπτυχθεί για όλους και ο καθένας μπορεί να το αναπτύξει περαιτέρω. Το περιβάλλον διαχείρισης είναι αρκετά διαισθητικό, με αποτέλεσμα να δίνει ξεκάθαρη εικόνα στον διαχειριστή για τις κινήσεις που πρέπει να κάνει. Υπάρχει μεγάλη ποικιλία προτύπων (templates) τα οποία επιτρέπουν στον ιστότοπο να έχει μια καλή εμφάνιση και αρκετά από αυτά είναι δωρεάν. Είναι πολυγλωσσικό, υποστηρίζοντας ακόμα και γλώσσες που γράφονται από δεξιά προς τα αριστερά (π.χ. εβραϊκά ή αραβικά).

Ανάμεσα στα μειονεκτήματα του Joomla βρίσκεται ότι με μία εγκατάσταση σου δίνετε δυνατότητα για ένα μόνο ιστότοπο. Επίσης υπάρχει περιορισμός στη διανομή

των ρόλων των χρηστών και άδειες πρόσβασης που δίνει. Πόλυ σημαντικό είναι ότι τα URLs του δεν είναι αρκετά φιλικά στις μηχανές αναζήτησης, αν και υπάρχει module επί πληρωμής που βοηθάει στην βελτίωση του.

Το Drupal μπορεί εύκολα να δημιουργήσει πολλούς διαφορετικούς τύπους ιστοσελίδων από απλά web blogs μέχρι μεγάλες online κοινότητες. Στο Drupal ο σχεδιασμός του δεν είναι τόσο ζωηρόχρωμος όσο του Joomla, αλλά είναι πολύ εύκολο να προσαρμοστεί. Αυτό που δεν μπορεί να προσαρμοστεί εύκολα είναι η ορολογία του διαχειριστικού περιβάλλοντος που μπορεί να γίνει αρκετά δυσνόητη για μη ειδικευμένους χρήστες. Σε αντίθεση με το Joomla σου δίνει την δυνατότητα με μια εγκατάσταση να δημιουργήσεις και να διαχειριστείς πολλαπλούς ιστότοπους. Επίσης, έχει ενσωματωμένο εργαλείο αναζήτησης και αναζητήσεις-φιλικές προς τις μηχανές URL ως ένα επιπλέον module.

Στον παρακάτω πίνακα βλέπουμε μια ολοκληρωμένη σύγκριση μεταξύ του Joomla και του Drupal.

	Joomla	Drupal
SEO	○ Δεν έχει ισχυρό SEO,ωστόσο το OpenSEF είναι καλό και έχει γρήγορη βελτίωση.	● Τα URLs λειτουργούν καλά και μπορεί να βελτιωθούν με ένα εύκολο addon. Ο κώδικας βελτιστοποιείται εύκολα.
Forums	●	●
SSL Compatible	○	●
Template/Themes	● Έχει πολλές επιλογές από templates, τόσο ελεύθερα όσο και εμπορικά.	○ Επί του παρόντος, έχει ένα πρότυπο για όλες τις σελίδες, αν και αυτό μπορεί να προσαρμοστεί
Shopping Cart Module	● Το Joomla έχει to Virtuemart και την ενσωμάτωση των OSCommerce, είναι αξιόπιστα.	○ Δεν συνιστάται, διότι δεν έχει υπολογισμό φόρων και επιλογές νομίσματος. ωστόσο, η Ubercart φαίνεται πολλά υποσχόμενη.
Trash (Recycle Bin)	●	○
FTP Support (to upload internal content)	●	● Περιορισμένη
Ease-of-use	● Έχει ωραίο graphic interface για τη διαχείριση, ξεχωριστά από τον ιστότοπο.	● Το διαχειριστικό κομμάτι βρίσκεται μαζί με το Front-end του ιστότοπου.
Speed	● Μια default εγκατάσταση της έκδοσης 1.0.11 γίνεται σε 0,90 δευτερόλεπτα, μια default εγκατάσταση της έκδοσης 1.5	● Μια default εγκατάσταση γίνεται σε 1,05 δευτερόλεπτα (από http://sitescore.silktide.com)

	γίνεται σε 1,33 δευτερόλεπτα. (από http://sitescore.silktide.com)	
Site	● Η έκδοση 1.0.11 είναι 16.4 MB και η έκδοσή 1.5 είναι 16.7 MB.	● Η έκδοση 5.0 είναι 2.89 MB

● ναι
○ όχι

Πίνακας 1: Σύγκριση μεταξύ Joomla και Drupal

Όσο αναφορά το WordPress, είναι μία open source blog εφαρμογή γραμμένη σε php. Ενώ το WordPress είναι ευρύτερα γνωστό ως blogging πλατφόρμα, είναι κατά πολλούς τρόπους ένα CMS. Στον πυρήνα του, το σύστημα WordPress επιτρέπει να τη δημιουργία και τη διαχείριση του περιεχομένου που δημιουργείται μέσα στα ιστολόγια (blogs). Το WordPress είναι ο επίσημος διάδοχος μίας άλλης Web εφαρμογής που ονομάζεται b2Cafelog.

Σε γενικές γραμμές το WordPress είναι πιο απλοποιημένο. Σαν interface είναι αρκετά ευκολότερο από ότι το Joomla και το Drupal. Η διαμόρφωση της εμφάνισης (templating), όπως και στο Joomla γίνεται με την επιλογή ενός προτύπου και την επεξεργασία CSS.Το WordPress δεν είναι ένα πλήρες εργαλείο CMS. Πάνω σε αυτό βασίζονται οι πιο πολλές διάφορες με το Joomla και το Drupal.

Είναι βραδύτερο από τα άλλα δύο CMS που εξετάζουμε, αυτό για παράδειγμα μπορεί να διορθωθεί αν βελτιστοποιήσει ο χρήστης χειροκίνητα τα ερωτήματα της βάσης δεδομένων, αποβάλει ορισμένα κομμάτια κώδικα, συμπιέσει τα CSS αρχεία και αν εφαρμοστεί προσωρινή αποθήκευση (caching). Μερικά από αυτά είναι μέρος της αρχιτεκτονικής του Drupal και του Joomla και αυτό είναι που τα κάνει πιο γρήγορα.[1]

Για να αποκτήσουμε περαιτέρω γνώσεις σχετικά με την έκταση και την υποστήριξη από χρήστες που έχει το κάθε CMS που μελετάμε, εξετάσαμε τα βιβλία σε έντυπη μορφή που έχουν εκδοθεί για το καθένα κατά το έτος 2008. Η αναζήτηση αυτή περιορίζεται στα βιβλία γραμμένα στην αγγλική γλώσσα μόνο και δεν περιλαμβάνει μόνο βιβλία ήδη εκτυπωμένα, αλλά και αυτά που αναφέρονται προς δημοσίευση.

[1] http://www.ibm.com

	Titles in print	Published in the last 12 months
Joomla	25	14
Drupal	12	7
Wordpress	11	8

Πίνακας 2: Βιβλία για Joomla, Drupal και Wordpress που έχουν τυπωθεί το 2008

Όσο αναφορά την ανάπτυξη υπηρεσιών τα στατιστικά που αντλούμε από την Elance και την Guru μας δίνουν τον παρακάτω πίνακα. Ουσιαστικά, η Elance είναι ένας διαδικτυακός χώρος εργασίας όπου εργοδότες μπορούν να συνδεθούν με εξειδικευμένους επαγγελματίες για να εκτελέσουν εργασίες από απόσταση. Διατηρώντας το μεγαλύτερο δίκτυο επαγγελματιών που υπάρχει στο διαδίκτυο η Elance βοηθάει τις επιχειρήσεις να ολοκληρώσουν το έργο τους συνδέοντάς τις με τους επαγγελματίες που χρειάζονται**.** Η Guru παρέχει υπηρεσίες παρόμοιες με την Elance αλλά εστιάζει λιγότερο σε επαγγελματίες της τεχνολογίας.

	Elance	**Guru**
Joomla	**2,281**	**785**
Wordpress	**1,844**	**495**
Drupal	**933**	**353**

Πίνακας 3: Ανάπτυξη υπηρεσιών σύμφωνα με Elance και Guru

Τα Google Trends παρέχουν τη δυνατότητα να ελέγχουν τη συχνότητα της εμφάνισης των όρων που υποβάλλονται ως ερωτήματα αναζήτησης του Google. Χρησιμοποιώντας σαν λέξεις κλειδιά στη μηχανή αναζήτησης του Google Trends Labs τα ονόματα των CMS που εξετάζουμε, είχαμε το εξής αποτέλεσμα:

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Εικόνα 9: Η συχνότητα της εμφάνισης των Joomla, Drupal και Wordpress στις google μηχανές αναζήτησης

Συμπερασματικά, το καθένα από τα παραπάνω συστήματα διαχείρισης περιεχομένου που αναλύσαμε (Joomla, Drupal, Wordpress) έχει πλεονεκτήματα και μειονεκτήματα. Οι χρήστες επιλέγοντας το CMS που καλύπτει τις απαιτήσεις τους και είναι ανάλογο των δυνατοτήτων τους θα έχουν τα επιθυμητά αποτελέσματα.[2]

[2] Οι πληροφορίες για την σύγκριση των CMS είναι από "The 2008 *Open Source CMS. Market Share* Report" του Ric Shreves.

Κεφάλαιο 4 Τρόπος εγκατάστασης του Joomla και των απαραίτητων εργαλείων

4.1 Εργαλεία που απαιτούνται

Η δημιουργία μιας εφαρμογής ηλεκτρονικού καταστήματος χρησιμοποιώντας το Joomla CMS προαπαιτεί κάποιες άλλες λειτουργίες. Αρχικά, η εγκατάσταση του ηλεκτρονικού καταστήματος θα γίνει τοπικά οπότε πρέπει να χρησιμοποιηθεί ένας τοπικός server, πάνω στον οποίο θα στηθεί το κατάστημα, σε αυτή την εργασία θα χρησιμοποιηθεί ο Apache HTTP. Ο Apache HTTP γνωστός και απλά σαν Apache είναι ένας εξυπηρετητής του παγκόσμιου ιστού (web). Όταν επισκεπτόμαστε έναν ιστότοπο ο πλοηγός μας επικοινωνεί με έναν διακομιστή HTTP.

Ο Apache είναι ένας από τους δημοφιλέστερους, γιατί λειτουργεί σε διάφορες πλατφόρμες όπως Windows, Linux, Unix και Mac OS X. Παράγεται και διανέμεται δωρεάν από μια κοινότητα ανοιχτού κώδικα με επιτήρηση από το Ίδρυμα Λογισμικού Apache (Apache Software Foundation). Χρησιμοποιείται κυρίως για να εξυπηρετεί στατικό και δυναμικό περιεχόμενο στο web.

Επίσης, πρέπει να έχει εγκατασταθεί στον ηλεκτρονικό υπολογιστή που χρησιμοποιούμε η γλώσσα προγραμματισμού PHP για την διαμόρφωση του site. Όσο αναφορά τη δημιουργία της βάσης δεδομένων στην οποία θα αποθηκεύονται όλες οι πληροφορίες που αφορούν το ηλεκτρονικό κατάστημα θα χρησιμοποιηθεί η MySQL. Η οποία αποτελεί ένα σχεσιακό σύστημα διαχείρισης βάσεων δεδομένων, το οποίο έχει περισσότερα από 6 εκατομμύρια εγκαταστάσεις.

Τα αρχικά MySQL προέρχονται από τις λέξεις My Structured Query Language. Το πρόγραμμα λειτουργεί ως διακομιστής παροχής πρόσβασης πολλών χρηστών σε μια σειρά από βάσεις δεδομένων. Δηλαδή, παρέχει τη δυνατότητα λειτουργίας από πολλαπλούς χρήστες με ασφάλεια αφού μόνο οι κατοχυρωμένοι ως χρήστες έχουν πρόσβαση στα δεδομένα της. Χρησιμοποιεί τη γλώσσα SQL που είναι η πιο διαδεδομένη γλώσσα στις βάσεις δεδομένων.

Ακόμη, θα χρησιμοποιηθεί και το εργαλείο phpMyAdmin, το οποίο είναι ένα δωρεάν λογισμικό γραμμένο σε PHP που προορίζεται για τη διαχείριση του administration της MySQL μέσω του Παγκόσμιου Ιστού. Το εργαλείο phpMyAdmin υποστηρίζει ένα ευρύ φάσμα δράσεων της MySQL.

4.1.1 Εγκατάσταση του XAMPP

Το XAMPP είναι ένα ελεύθερο και ανοικτό cross-platform web server package, που αποτελείται κυρίως από τον Apache HTTP Server, τη MySQL βάση δεδομένων και των διερμηνέων για scripts γραμμένα σε γλώσσες προγραμματισμού PHP και Perl.

Είναι ένα χρήσιμο εργαλείο που μας βοηθάει να μετατρέψουμε τον υπολογιστή μας σε web server. Σε αυτή την εργασία γίνεται εγκατάσταση του XAMPP 1.7.2 σε περιβάλλον Windows Vista.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

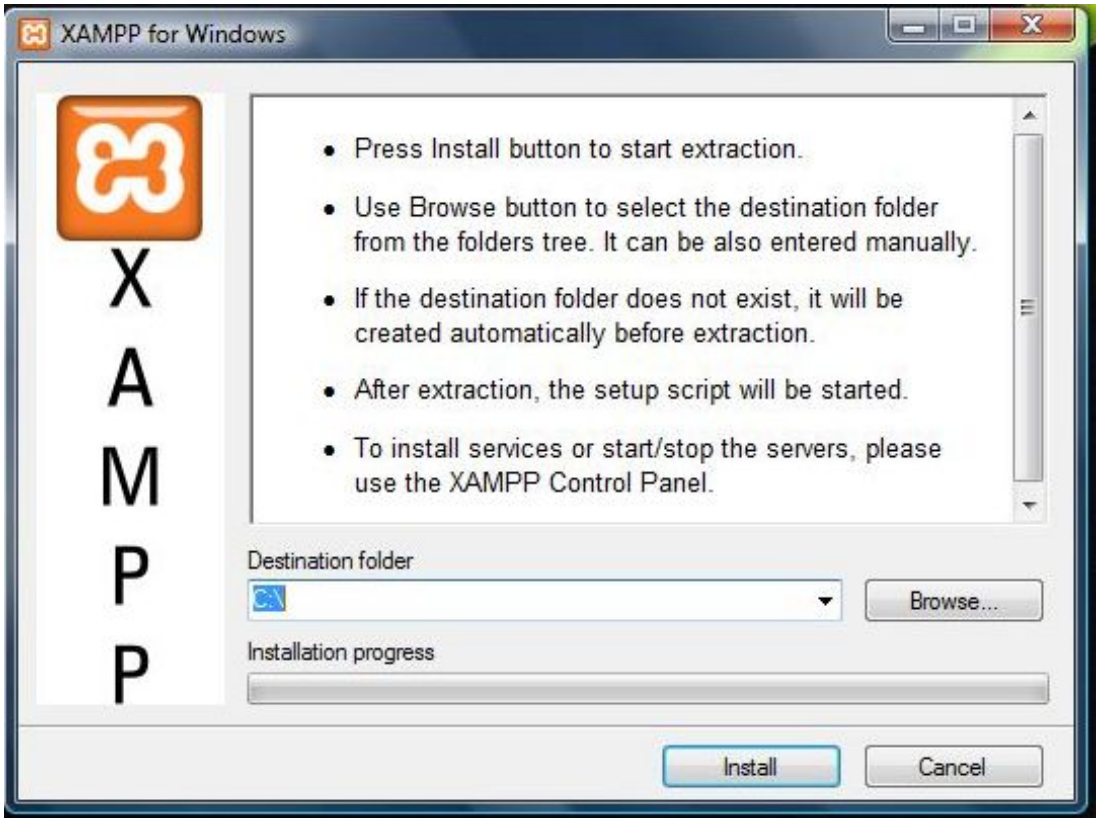
Εικόνα 10: Το λογότυπο του XAMPP

Η έκδοση XAMPP 1.7.2 για Windows περιέχει:

- Apache 2.2.12 (IPv6 enabled) + OpenSSL 0.9.8k
- MySQL 5.1.37 + PBXT engine
- PHP 5.3.0
- phpMyAdmin 3.2.0.1
- Webalizer 2.21-02 + GeoIP lite
- FileZilla FTP Server 0.9.32
- msmtp 1.4.17

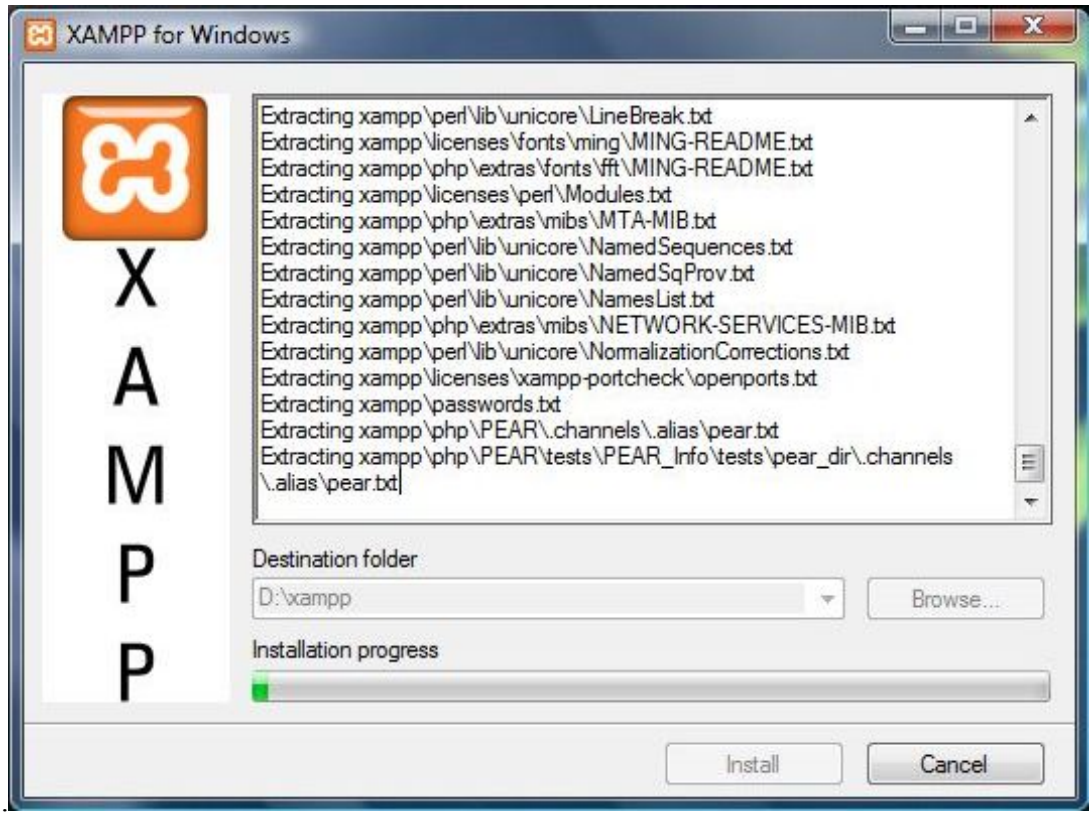
Πρέπει να προσέξουμε σε περίπτωση που χρησιμοποιούμε το messenger Skype στον υπολογιστή μας. Να αποσυνδεθούμε από το Skype πριν αρχίσει η εγκατάσταση του XAMPP, γιατί το Skype δουλεύει στην TCP πόρτα 80 και θα μας δημιουργήσει πρόβλημα στην εγκατάσταση.

Από την ιστοσελίδα http://www.apachefriends.org κατεβάζουμε στον υπολογιστή μας το exe αρχείο xampp-win32-1.7.2. Αφού κατέβει επιτυχώς, τρέχουμε το αρχείο. Μας εμφανίζετε η παρακάτω οθόνη:



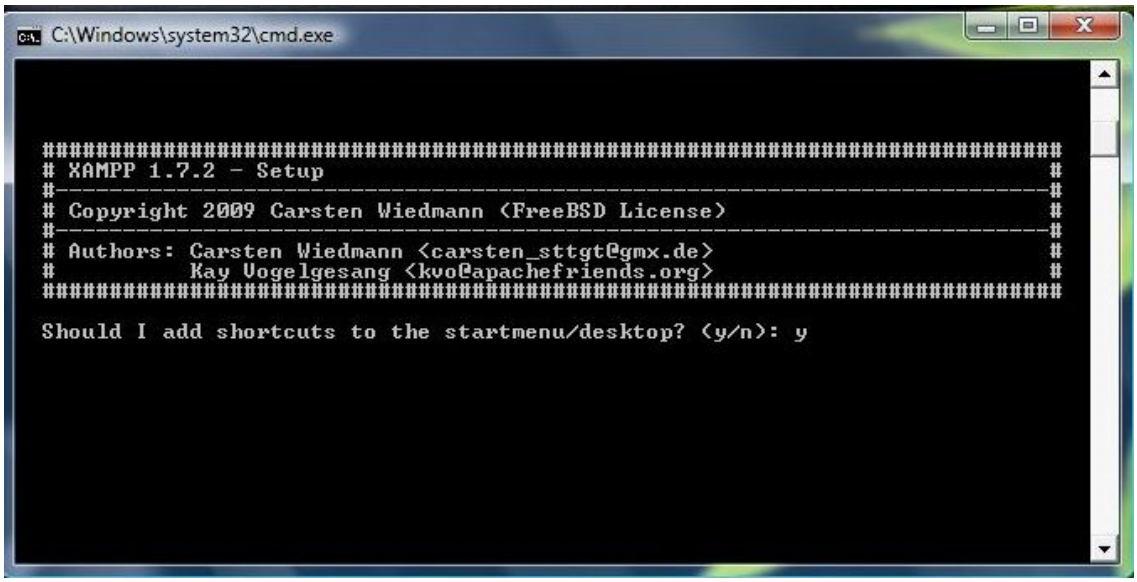
Εικόνα 11: Εγκατάσταση XAMPP. Βήμα 1ο, επιλογή φακέλου εγκατάστασης

Εδώ μας ζητάει να επιλέξουμε το φάκελο στον οποίο θα αποθηκεύσει τα απαραίτητα αρχεία για την λειτουργία του. Επιλέγουμε να τα αποθηκεύσει στον σκληρό δίσκο C και η εγκατάσταση αρχίζει όπως βλέπουμε παρακάτω.



Εικόνα 12: Εγκατάσταση XAMPP. Βήμα 2ο, εξέλειξη εγκατάστασης

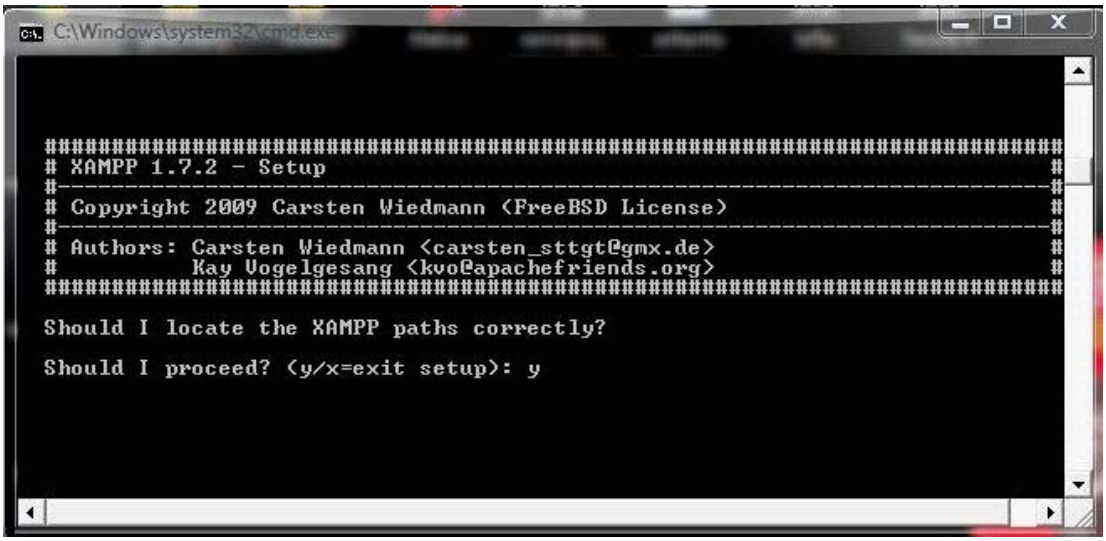
Αφού ολοκληρωθεί η εγκατάσταση μας ρωτάει αν επιθυμούμε τη δημιουργία συντόμευσης στην επιφάνεια εργασίας μας. Αν επιθυμούμε πληκτρολογούμε ‘y’ και έπειτα enter, αν όχι ‘n’ και enter.



Εικόνα 13: Εγκατάσταση XAMPP. Βήμα 3ο, επιλογή δημιουργίας συντόμευσης στην επιφάνεια εργασίας

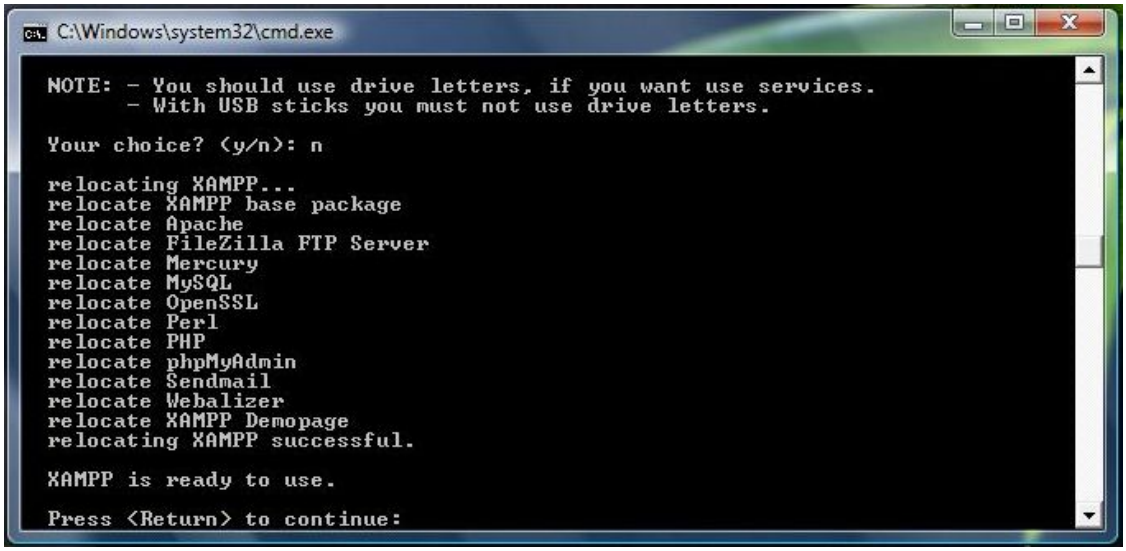
Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Στη συνέχεια, μας ενημερώνει ότι πρέπει να τοποθετήσει σωστά τα XAMPP paths και ζητάει την έγκριση μας για να συνεχίσει. Με τον ίδιο τρόπο, όπως παραπάνω, δίνουμε εντολή για ναι.



Εικόνα 14: Εγκατάσταση XAMPP. Βήμα 4ο, σωστή τοποθέτηση των XAMPP paths, επιλογή για συνέχεια

Έπειτα, επιλέγουμε να μην χρησιμοποιήσει τα drive letters XAMPP επειδή δεν θα χρησιμοποιήσουμε USB sticks. Η εγκατάσταση συνεχίζεται και το XAMPP είναι έτοιμο για χρήση.



Εικόνα 15: Εγκατάσταση XAMPP. Βήμα 5ο, απορρίψη χρησιμοποίησης drive letters

Αφού πληκτρολογήσουμε "Return" για να συνεχίσουμε μας εμφανίζεται η παρακάτω οθόνη, η οποία μας ενημερώνει ότι στα αρχεία "php.ini" και "my.ini" έχει ορίσει την ζώνη ώρας ως "Europe/Helsinki".

Εικόνα 16: Εγκατάσταση XAMPP. Βήμα 6ο, ορισμός ζώνης ώρας

Αυτό δεν ανταποκρίνεται στα δικά μας δεδομένα. Όταν ολοκληρωθεί η εγκατάσταση του XAMPP θα επισκεφτούμε το link:
http://us2.php.net/manual/en/timezones.europe.php

Για να δούμε πως ορίζει τη ζώνη ώρας για την Ελλάδα. Βλέπουμε ότι η ζώνη ώρας αναφέρεται ως Mode/Athens.

Πηγαίνουμε στο **C:\xampp\php\php.ini** να αλλάξουμε το αρχείο "php.ini". Ανοίγουμε το αρχείο με ένα notpad και ψάχνουμε για το σημείο που θα βρούμε τον παρακάτω κώδικα:

Κώδικας

```
[Date]
   ; Defines the default timezone used by the date functions
   ; http://php.net/date.timezone
   date.timezone = "Europe/Helsinki"
```

Αλλάζουμε αυτό το κομμάτι κώδικα συμφωνά με το παρακάτω:

Κώδικας

```
[Date]
  ; Defines the default timezone used by the date functions
  ; http://php.net/date.timezone
  date.timezone = "Europe/Athens"
```

Σώζουμε τις αλλαγές και κάνουμε επανεκκίνηση τον Apache για να αναγνωρίσει τις αλλαγές.

Το ίδιο κάνουμε και για το αρχείο "my.ini". Πηγαίνουμε στο **C:\xampp\mysql\bin\my.ini** που βρίσκεται το συγκεκριμένο αρχείο και το ανοίγουμε με ένα notpad. Βρίσκουμε το σημείο του κώδικα που λέει:

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Κώδικας

```
Default-time-zone = "Europe/Helsinki"
```

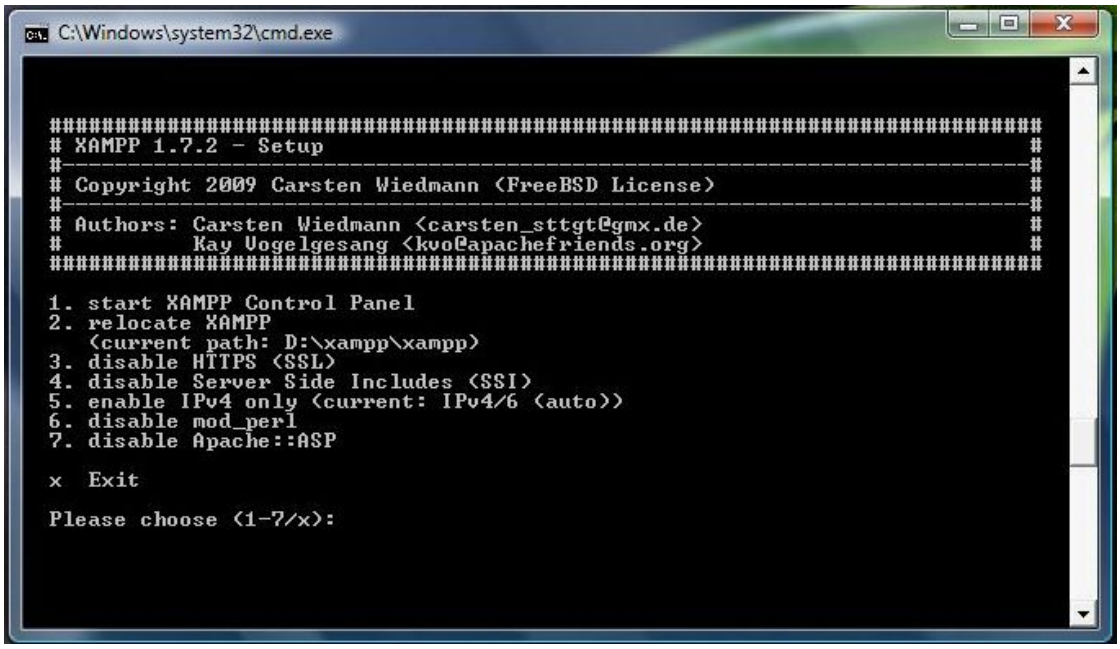
Το αλλάζουμε σύμφωνα με τη δικιά μας ζώνη.

Κώδικας

```
Default-time-zone = "Europe/Athens"
```

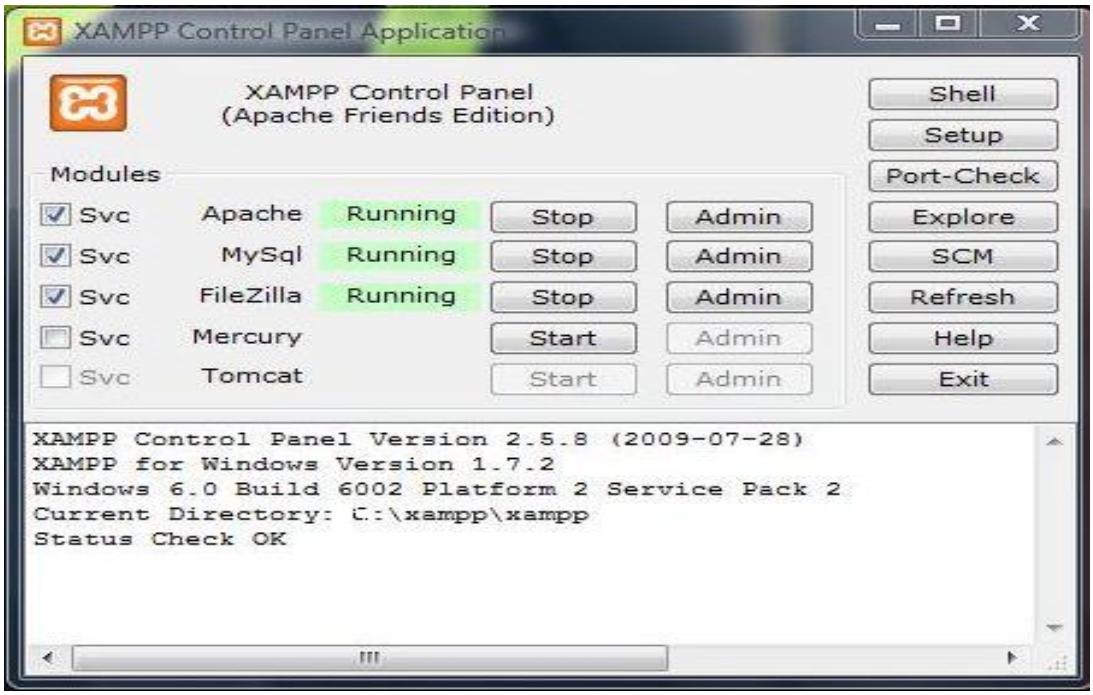
Σώζουμε το αρχείο και κάνουμε επανεκκίνηση της MySQL.

Στη συνέχεια της εγκατάστασης του XAMPP, μας έχει κάποιες επιλογές για το τι θέλουμε να κάνουμε στο συγκεκριμένο σημείο.



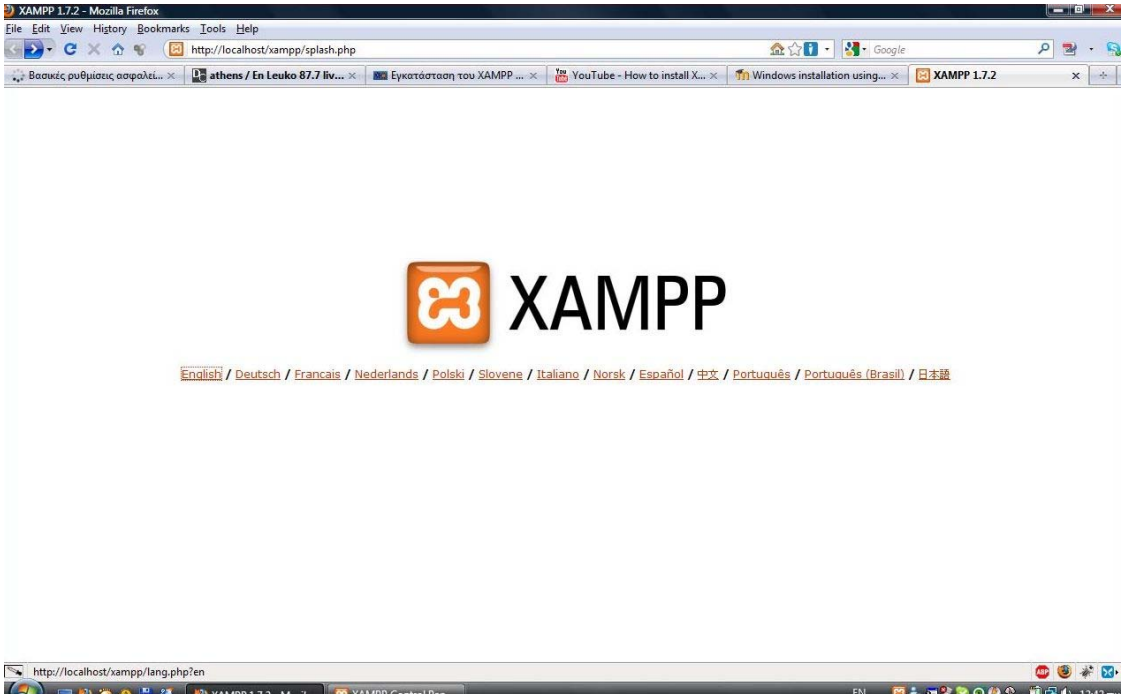
Εικόνα 17: Εγκατάσταση XAMPP. Βήμα 7ο, τέλος εγκατάστασης

Επιλέγουμε start XAMPP Control Panel για να φύγουμε από τις οθόνες εγκατάστασης και να ανοίξει το Control Panel. Στο Control Panel θα εκκινήσουμε τον Apache, την MySql και τον FileZilla.



Εικόνα 18: XAMPP Control Panel

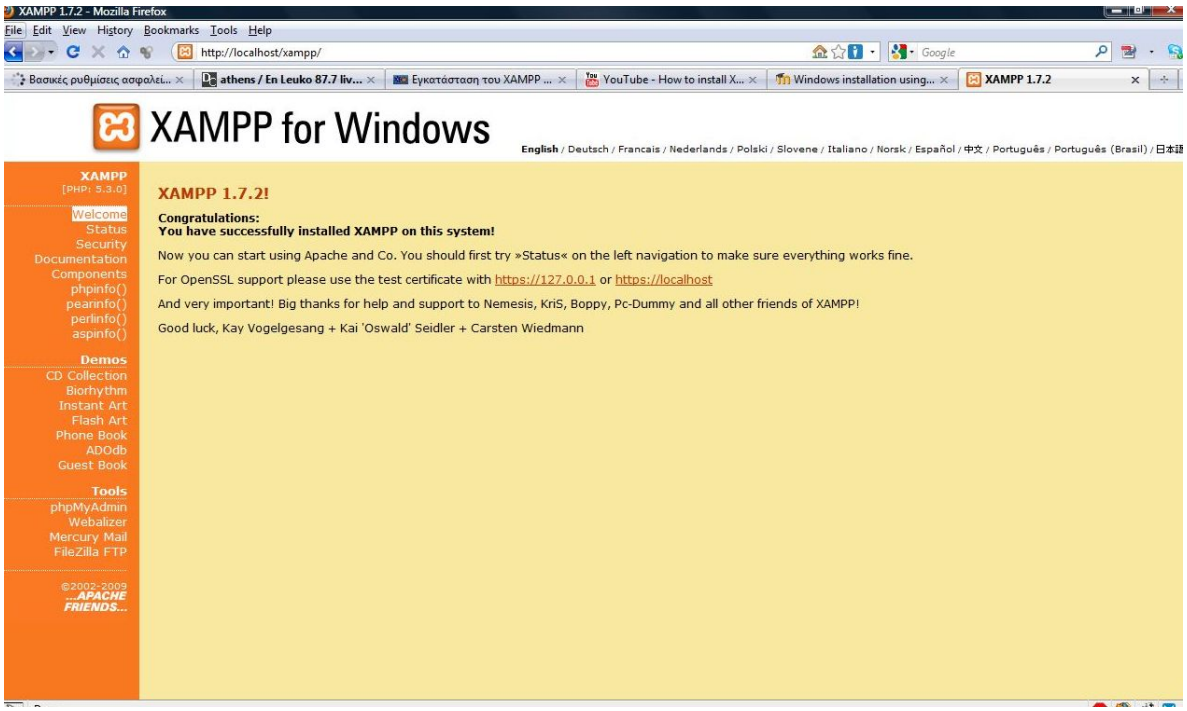
Ανοίγουμε ένα browser της αρεσκείας μας και πληκτρολογούμε http://localhost/ ή http://127.0.0.1/**.** Μας εμφανίζεται η πρώτη σελίδα του XAMPP, θα εξετάσουμε όλα τα παραδείγματα και τα εργαλεία του και θα μας καθοδηγήσει να κάνουμε τις απαραίτητες ρυθμίσεις.



Εικόνα 19: Ρυθμίσεις XAMPP. Επιλογή γλώσσας

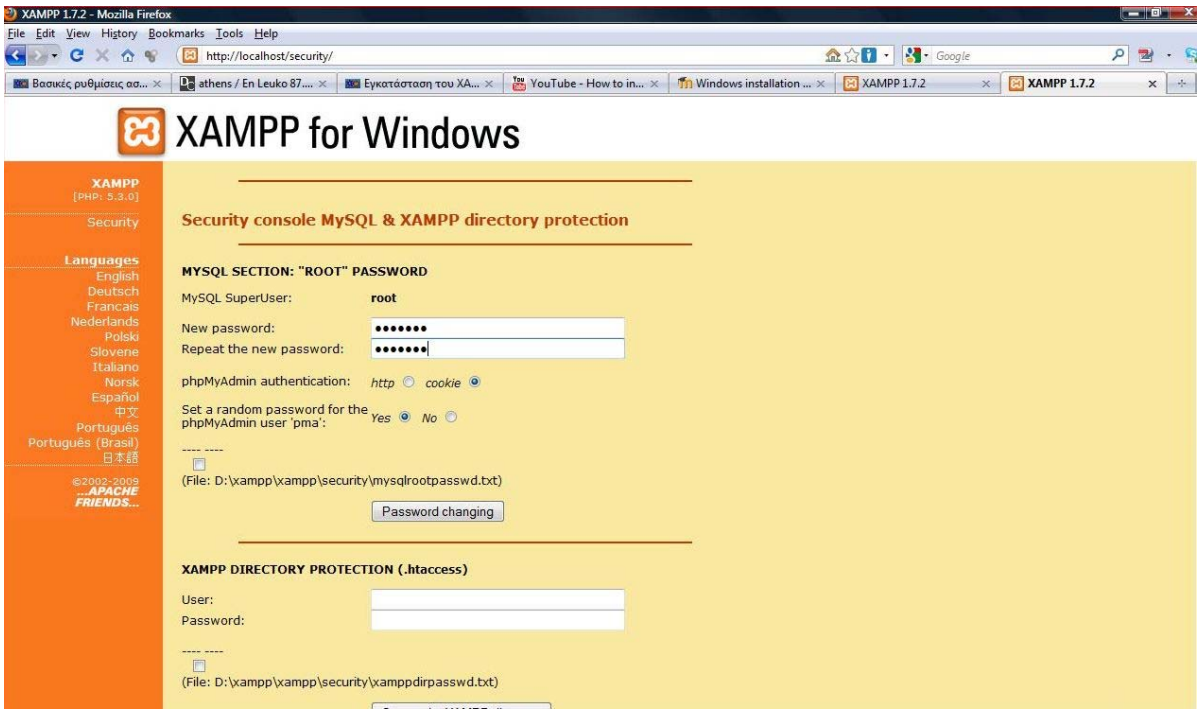
Αρχικά, πρέπει να επιλέξουμε γλώσσα, η ελληνική γλώσσα δεν υπάρχει έτσι επιλέγουμε αγγλικά και συνεχίζουμε.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



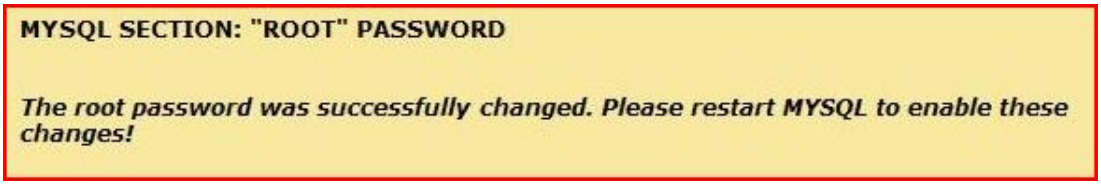
Εικόνα 20: Ρυθμίσεις XAMPP. Μήνυμα καλωσορίσματος

Έχουμε ένα μήνυμα ότι έχουμε εγκαταστήσει επιτυχώς το XAMPP στον υπολογιστή μας και από το αριστερό μενού επιλέγουμε το security για να θέσουμε τους κωδικούς για την MySql και για την προστασία του XAMPP directory.



Εικόνα 21: Ρυθμίσεις XAMPP. Ορισμός κωδικών της MySql και του XAMPP directory

Αφού θέσουμε τους κωδικούς της MySql, εμφανίζεται το παρακάτω μήνυμα.

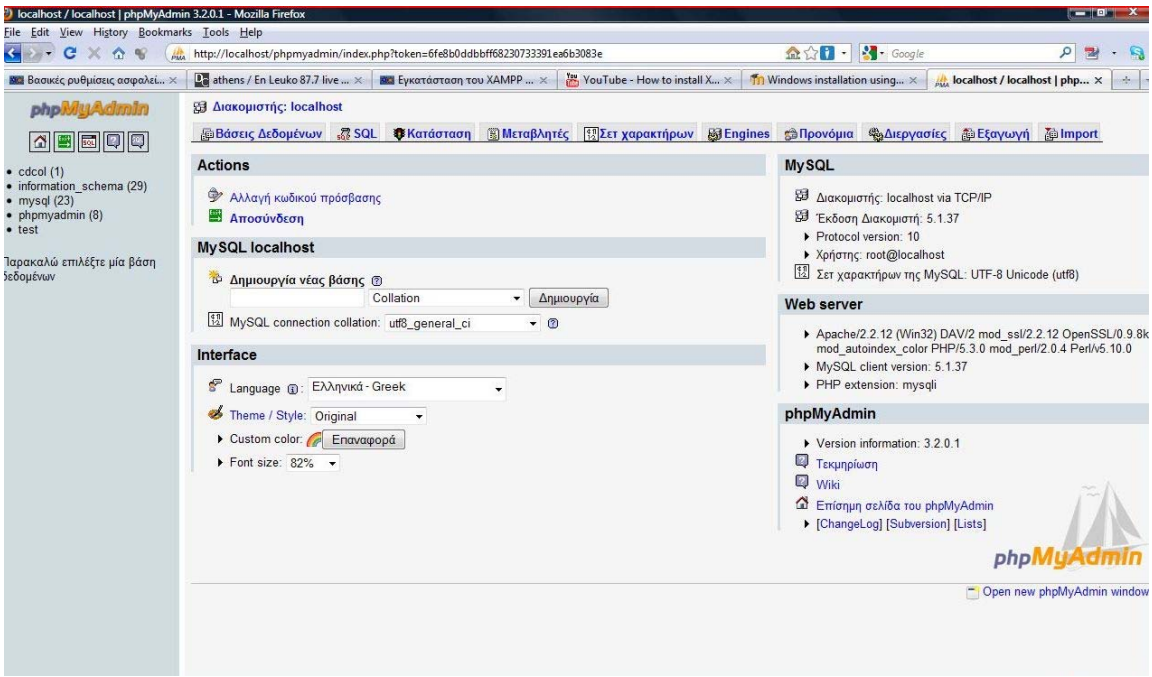


Εικόνα 22: Μήνυμα επιτυχής αλλαγής κωδικού MySql

Αφού θέσουμε όνομα χρήστη και τον κωδικό για την προστασία του XAMPP directory έχουμε το ακόλουθο μήνυμα.

Εικόνα 23: Μήνυμα επιτυχής αποθήκευσης κωδικών του XAMPP directory

Για να δημιουργήσουμε τη βάση δεδομένων από το μενού της αριστερής στήλης του κέντρου διαχείρισης του XAMPP, επιλέγουμε από το phpMyAdmin από την ενότητα Tools. Στο πλαίσιο MySQL localhost, βλέπουμε ότι υπάρχει ο τίτλος "Δημιουργία νέας βάσης". Βάζουμε το όνομα της βάσης μας στο πρώτο πεδίο, στην παρούσα εργασία η βάση που θα δημιουργήσουμε ονομάζεται "joomla". Στο πεδίο "Collation" επιλέγουμε utf8_unicode_ci και κάνουμε κλικ στο κουμπί δημιουργία. Η νέα βάση δεδομένων έχει δημιουργηθεί.



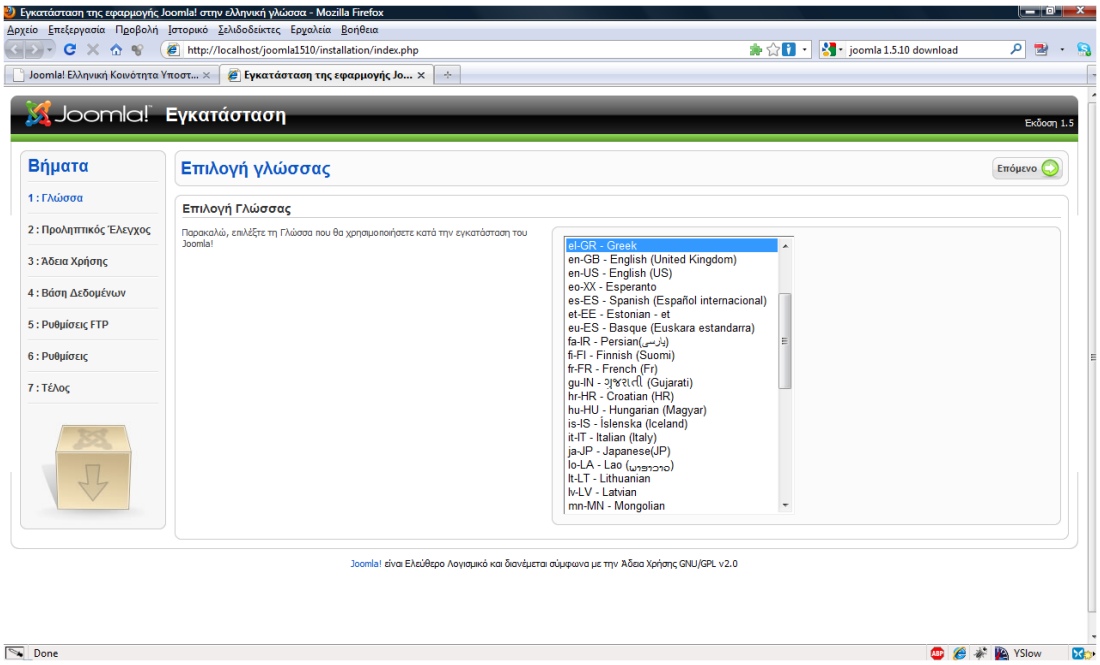
Εικόνα 24: Δημιουργία βάσης δεδομένων μέσω του εργαλείου phpMyAdmin

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

4.1.2 Εγκατάσταση του Joomla

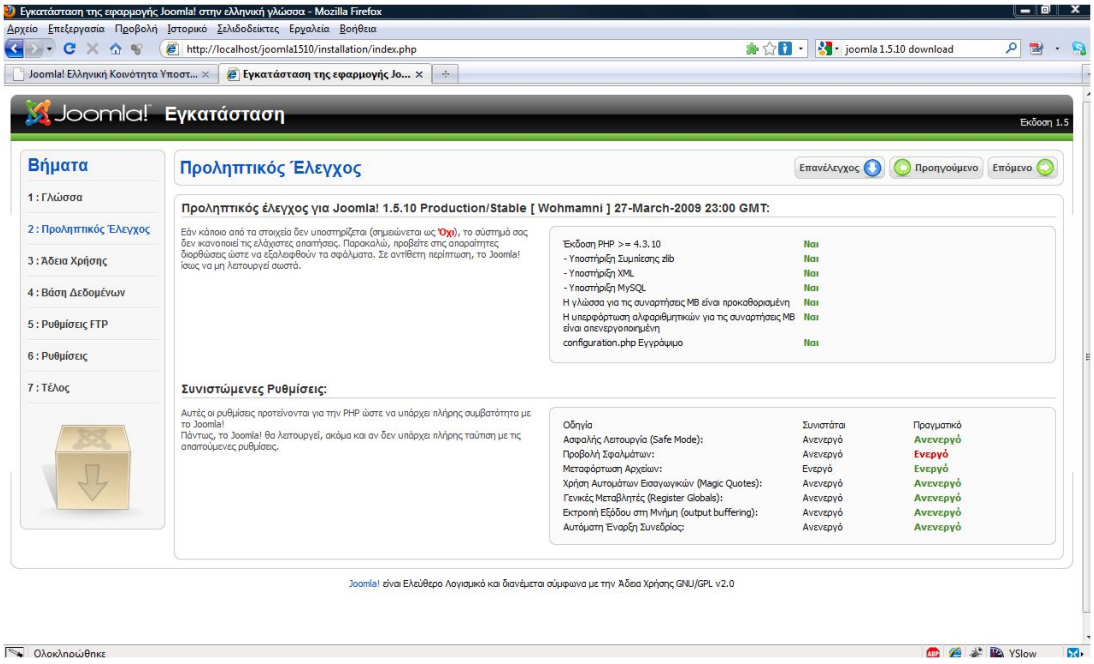
Στην παρούσα εργασία χρησιμοποιείτε η έκδοση 1.5.10 του Joomla. Αρχικά, πρέπει να κατεβάσουμε το αρχείο Joomla_1.5.10-Stable-Full_Package.zip από το http://www.joomla.org/download.html. Αφού έχουμε κατεβάσει το zip αρχείο, πηγαίνουμε στον φάκελο htdocs που βρίσκεται στο **C:\xampp\htdocs** και δημιουργούμε ένα φάκελο στον οποίο θα αποθηκεύσουμε τα αρχεία που περιέχει το zip αρχείο, ονομάζουμε τον φάκελο "joomla1510".

Στη συνέχεια, πηγαίνουμε στο browser και πληκτρολογούμε http://localhost/joomla1510. Η πρώτη οθόνη που εμφανίζεται μας ζητάει να επιλέξουμε γλώσσα που θα χρησιμοποιήσουμε κατά την εγκατάσταση του Joomla.



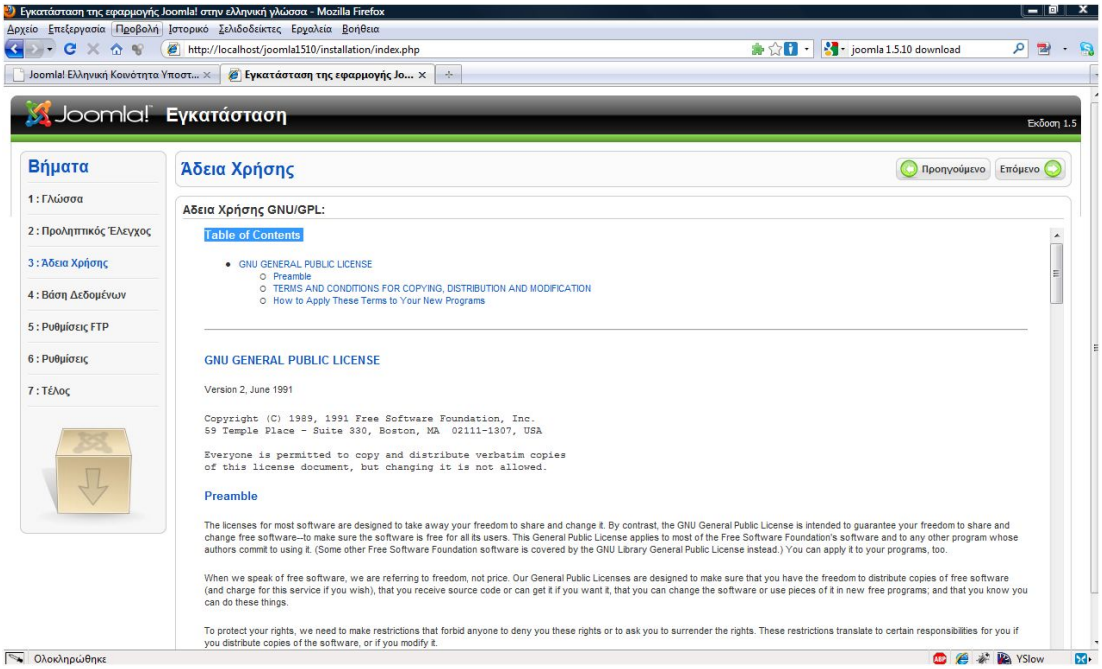
Εικόνα 25: Εγκατάσταση Joomla**.** Βήμα 1ο, επιλογή γλώσσας εγκατάστασης

Επιλέγουμε γλώσσα ελληνικά και συνεχίζουμε κάνοντας κλικ στο κουμπί "Επόμενο". Στην δεύτερη οθόνη εγκατάστασης γίνεται προληπτικός έλεγχος για όλα τα στοιχεία που χρειάζεται το Joomla για την σωστή του λειτουργία (PHP, MySQL, κ.τ.λ.).



Εικόνα 26: Εγκατάσταση Joomla**.** Βήμα 2ο, προληπτικός έλεγχος

Στον έλεγχο που έγινε όλα είναι θετικά και συνεχίζουμε στο επόμενο βήμα. Έπειτα διαβάζουμε την άδεια χρήσης του Joomla και κάνουμε κλικ στο κουμπί "Επόμενο".



Εικόνα 27: Εγκατάσταση Joomla**.** Βήμα 3ο, άδεια χρήσης GNU/GPL

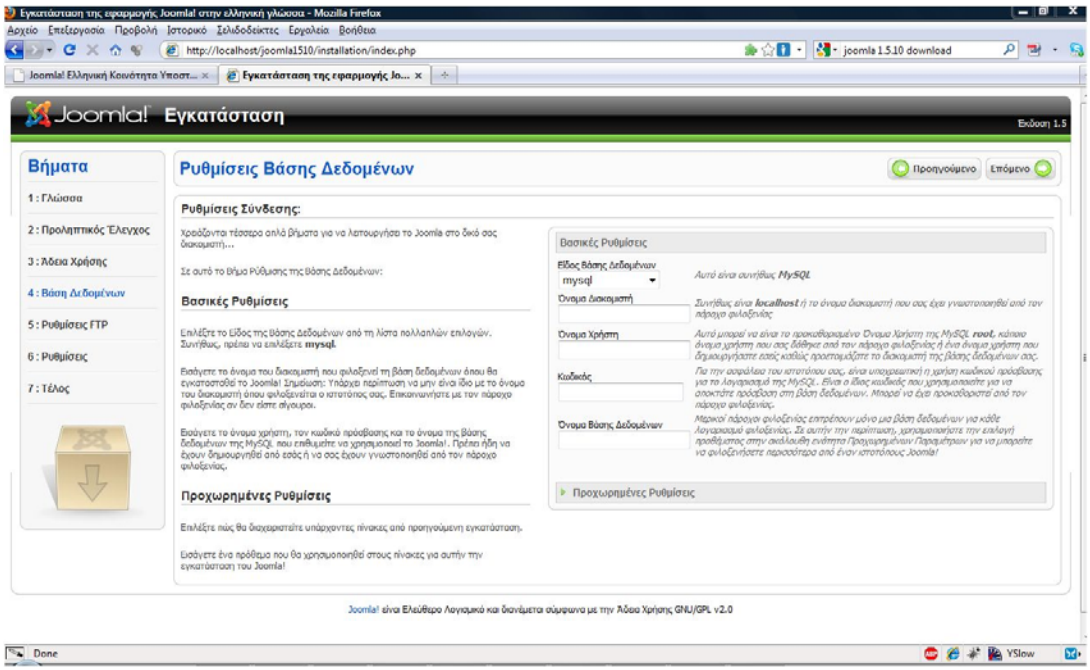
Στο επόμενο βήμα εγκατάστασης πρέπει να ρυθμίσουμε τη βάση δεδομένων. Στις βασικές ρυθμίσεις επιλέγουμε-συμπληρώνουμε:

- **Είδος βάσης δεδομένων**: mysql
- **Όνομα διακομιστή**: localhost

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

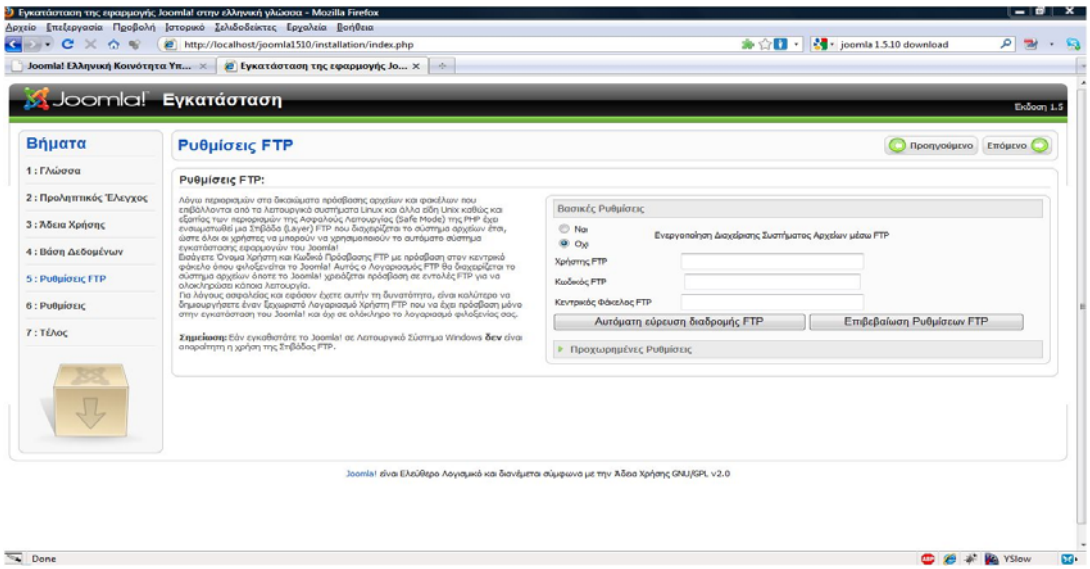
- **Όνομα χρήστη**: root
- **Κωδικός**: βάζουμε τον κωδικό που είχαμε δώσει παραπάνω για την mysql
- **Όνομα βάσης δεδομένων**: joomla

Αφού τα συμπληρώσουμε κάνουμε κλικ στο κουμπί "Επόμενο" και συνεχίζουμε.



Εικόνα 28: Εγκατάσταση Joomla**.** Βήμα 4ο, ρυθμίσεις Βάσης Δεδομένων

Ακολουθούν οι ρυθμίσεις FTP. Εδώ δεν συμπληρώνουμε τίποτα, απλά περνάμε στο επόμενο βήμα.

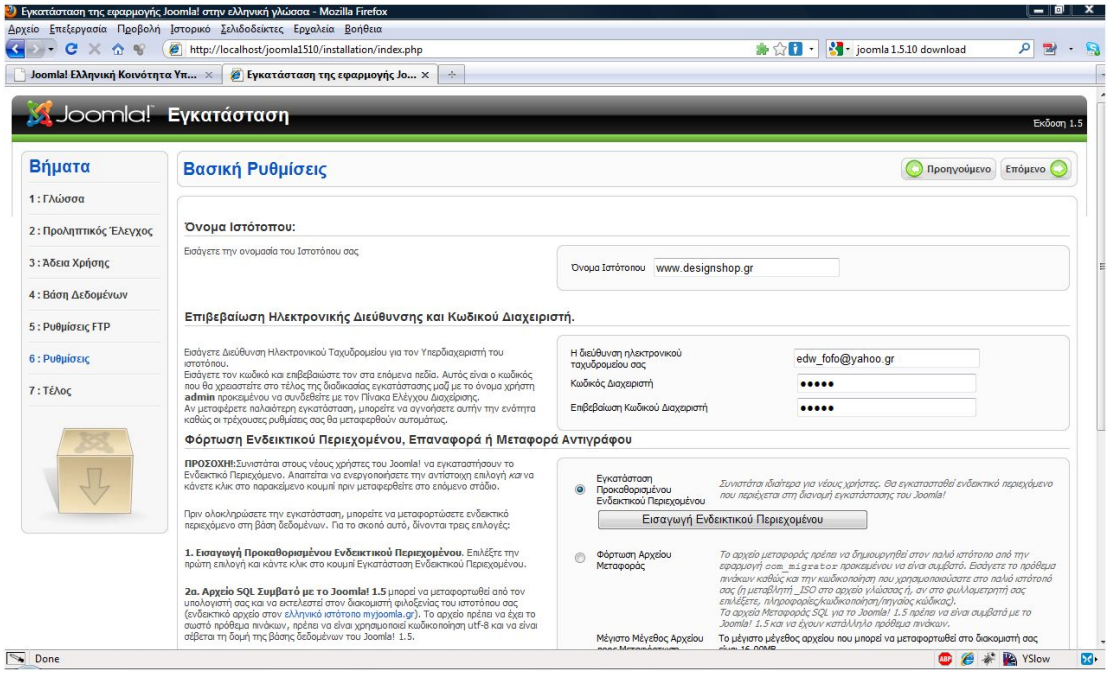


Εικόνα 29: Εγκατάσταση Joomla**.** Βήμα 5ο, ρυθμίσεις FTP

Στο τελευταίο βήμα ορίζουμε τις βασικές ρυθμίσεις του ιστότοπου μας. Συμπληρώνουμε τα πεδία ως εξής:

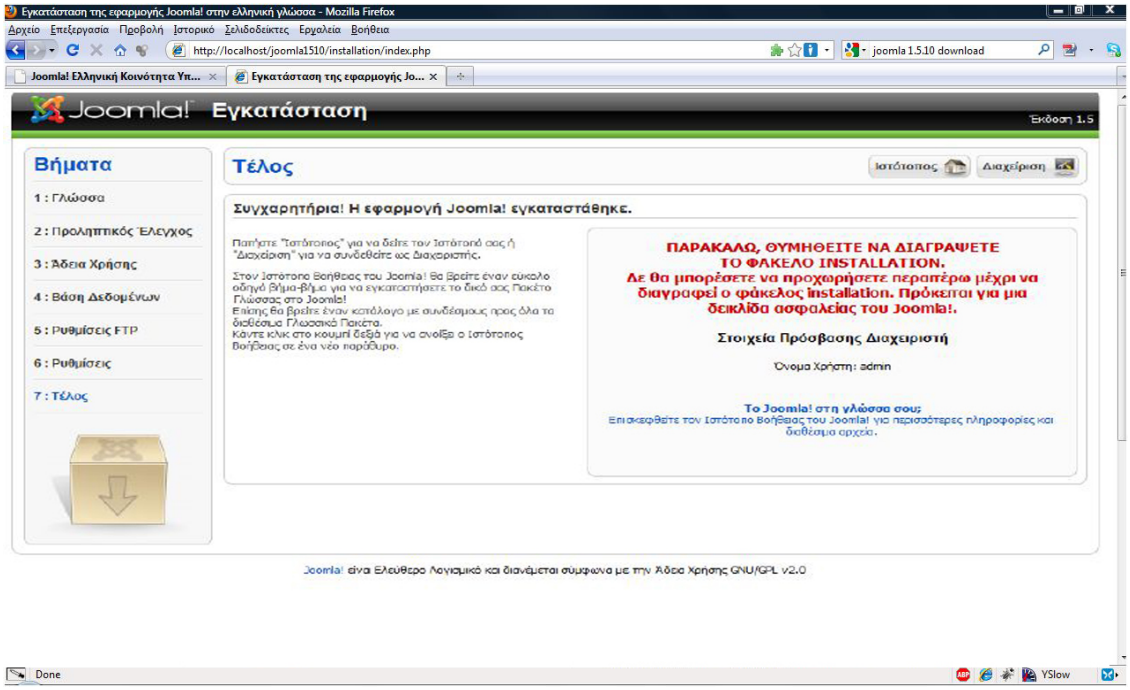
- **Όνομα Ιστοτόπου**: Εισάγουμε την ονομασία του Ιστοτόπου μας, στην δική μας περίπτωση βάζουμε www.mydesignshop.eu.
- **Η διεύθυνση ηλεκτρονικού ταχυδρομείου σας**: Εισάγουμε το ηλεκτρονικό μας ταχυδρομείο αλλά επειδή η εφαρμογή θα χρησιμοποιηθεί τοπικά μπορούμε να βάλουμε και μία τυχαία διεύθυνση.
- **Κωδικός Διαχειριστή**: Βάζουμε τον κωδικό με τον οποίο θα εισερχόμαστε στο διαχειριστικό κομμάτι της ιστοσελίδας μας.
- **Επιβεβαίωση κωδικού διαχειριστή**: Επιβεβαιώνουμε τον κωδικό.

Σε περίπτωση που επιθυμούμε το Joomla να μας φτιάξει μια ενδεικτική αρχική σελίδα, κάνουμε κλικ στο κουμπί "Εισαγωγή Ενδεικτικού Περιεχομένου".



Εικόνα 30: Εγκατάσταση Joomla**.** Βήμα 6ο, βασικές ρυθμίσεις

Η εγκατάστασή μας έχει ολοκληρωθεί, στην τελευταία οθόνη εγκατάστασης μας εμφανίζεται ένα μήνυμα που μας ενημερώνει ότι σε αυτό το σημείο πρέπει να διαγράψουμε τον φάκελο instalation, ο οποίος βρίσκεται στον φάκελο εγκατάστασης του Joomla, με όνομα "joomla1510". Αν παραλείψουμε αυτό το βήμα δεν θα μπορέσουμε να συνεχίσουμε παρακάτω. Μόλις διαγράψουμε τον φάκελο instalation, πατώντας το κουμπί "Ιστότοπος" θα μπορέσουμε να εισέλθουμε στον ιστότοπο μας.



Εικόνα 31: Εγκατάσταση Joomla**.** Βήμα 7ο, τέλος εγκατάστασης

Κεφάλαιο 5 Μελέτη του Component Virtuemart

5.1 Περιγραφή λειτουργίας του Component Virtuemart

5.1.1 Χαρακτηριστικά του Component Virtuemart

Το virtuemart είναι μια shopping cart application βασισμένη σε php για την πώληση αγαθών μέσω του διαδικτύου. Είναι ένα Component (plugin) κατασκευασμένο ειδικά για το Joomla CMS και τον "πρόγονο" του Mambo. Αποτελεί αξιόπιστη e - Commerce λύση για ηλεκτρονικά καταστήματα κατασκευασμένα με Joomla σύμφωνα με τα στατιστικά, αφού χρησιμοποιείται από χιλιάδες ιδιοκτήτες καταστημάτων. Μπορεί να τρέξει σε Store αλλά και Catalog-Mode. Έχει ισχυρό εργαλείο διαχείρισης το οποίο δίνει την δυνατότητα στον διαχειριστή να χειριστεί έναν απεριόριστο αριθμό κατηγοριών, προϊόντων, παραγγελιών, εκπτώσεων, ομάδων Shopper και πελατών. Προορίζεται για χρήση σε μικρές/μεσαίες online επιχειρήσεις και online καταστήματα.[3]

Στη συνέχεια αναφέρονται τα γενικά χαρακτηριστικά, τα χαρακτηριστικά του καταλόγου προϊόντων και τα χαρακτηριστικά της διαχείρισης του Component Virtuemart.

Γενικά χαρακτηριστικά:

- Είναι ικανό να χρησιμοποιήσει Secure Sockets Layer (https) κρυπτογράφηση (128-bit).
- Υποστηρίζει ευέλικτα φορολογικά μοντέλα:
    - Μοντέλο 1: Ζώνη βασισμένη σε φορολογικούς υπολογισμούς (πόλη/πολιτεία και χώρα/περιοχή).
    - Μοντέλο 2: Ιδιοκτησία καταστήματος βασισμένη σε φορολογικούς υπολογισμούς.
    - Μοντέλο 3: EU Mode (ιδιοκτησία καταστήματος βασισμένη σε φορολογικούς υπολογισμούς όταν οι πελάτες προέρχονται από χώρες της Ευρωπαϊκής Ένωσης).
- Οι πελάτες να μπορούν να διαχειρίζονται τα user accounts τους (απαιτείται εγγραφή).
- Ιστορικό παραγγελίας: Ο πελάτης μπορεί να δει όλες τις προηγούμενες παραγγελίες τους (καθώς και τις λεπτομέρειες της παραγγελίας του).
- Δυνατότητα επιβεβαίωσης της παραγγελίας μέσω e-mail, το οποίο αποστέλλεται στον πελάτη και στον ιδιοκτήτη του καταστήματος.
- Χρησιμοποιεί πολλαπλά νομίσματα (επιτρέπει στους πελάτες να αλλάξουν νόμισμα στις συναλλαγές τους και να κάνουν αγορές χρησιμοποιώντας ένα εναλλακτικό νόμισμα).
- Είναι πολυγλωσσικό (με τη χρήση του Component JoomFish).

[3] http://www.authorize.net/

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Τα χαρακτηριστικά του καταλόγου προϊόντων:

- Έχει ισχυρό web-administration interface (Javascript-powered).
- Διαχειρίζεται απεριόριστο αριθμό προϊόντων και κατηγοριών.
- Μπορεί να χρησιμοποιηθεί ως κατάστημα ή απλά ως ένας online-κατάλογος (δυνατότητα απενεργοποίησης εμφάνισης τιμών).
- Δίνει τη δυνατότητα της γρήγορης αναζήτησης ανά προϊόντα, κατηγορίες και κατασκευαστές προϊόντων, φιλτράροντάς τα αναλόγως με τα χαρακτηριστικά τους ή με εκπτωτικά προϊόντα.
- Υπάρχει η επιλογή κάποια προϊόντα, τα οποία είναι σε προσφορά να αναρτηθούν σε μια ειδική κατηγορία με τίτλο "on special".
- Έλεγχος της διαθεσιμότητας ενός προϊόντος: ο πελάτης μπορεί να δει πόσο πρέπει να περιμένει μέχρι την παράδοση του προϊόντος και ποσά "κομμάτια" του συγκεκριμένου προϊόντος είναι διαθέσιμα την ώρα που γίνεται η παραγγελία.

Τα χαρακτηριστικά της διαχείρισης:

- Δυνατότητα πολλαπλών εικόνων και αρχείων (όπως δελτία και flyers) ανά προϊόν.
- Φυσικά χαρακτηριστικά του προϊόντος (όπως το μέγεθος ή χρώμα) μπορούν να προστεθούν σε όλα τα προϊόντα.
- Επιλογή δημιουργίας Shopper Groups (ομάδες καταναλωτών) για τους πελάτες (αυτή η επιλογή επιτρέπει διάφορα επίπεδα τιμών και τρόπους πληρωμής).
- Ευέλικτη εμφάνιση των τιμών προϊόντων (μορφοποίηση αριθμών και νομίσματος συμπεριλαμβανομένου ή όχι του Φ.Π.Α.).
- Περιέχει πινάκα με τα στατιστικά του ηλεκτρονικού καταστήματος και Control Panel με μια περίληψη των νέων πελατών, των νέων παραγγελιών και γενικότερα την εμπορική κίνηση του καταστήματος.
- Δυνατότητα ελέγχου των αποθεμάτων για τα προϊόντα και είδη του καταστήματος.
- Βασική δυνατότητα αναφορών που αναφέρονται στα είδη που έχουν πωληθεί και στα μηνιαία/ετήσια έσοδα.

Τα τελευταία χρόνια το Component Virtuemart έχει αναγνωριστεί από πολλές Gateway πληρωμές. Επειδή το Component VirtueMart προσφέρει ένα API για την εφαρμογή όλων των modules πληρωμής δίνει τη δυνατότητα στο χρήστη να επιλέξει από πολλά διαφορετικά Gateways.

Τα modules πληρωμής μπορούν να διαμορφωθούν ως εξής:

- Ικανά να συμβαδίσουν με Credit Card Processing (Επεξεργασία Πιστωτικών Καρτών).
- Χρησιμοποιούν Gateway πληρωμές όπως: authorize.net®, PayPal, 2Checkout, eWay, Worldpay, PayMate and NoChex.

5.2 Εγκατάσταση του Component Virtuemart

Στην εργασία αυτή χρησιμοποιείται η έκδοση 1.1.3 του component Virtuemart. Η εγκατάσταση αυτού του component δεν απαιτεί κάτι παραπάνω από την απλή εγκατάσταση ενός Joomla component.

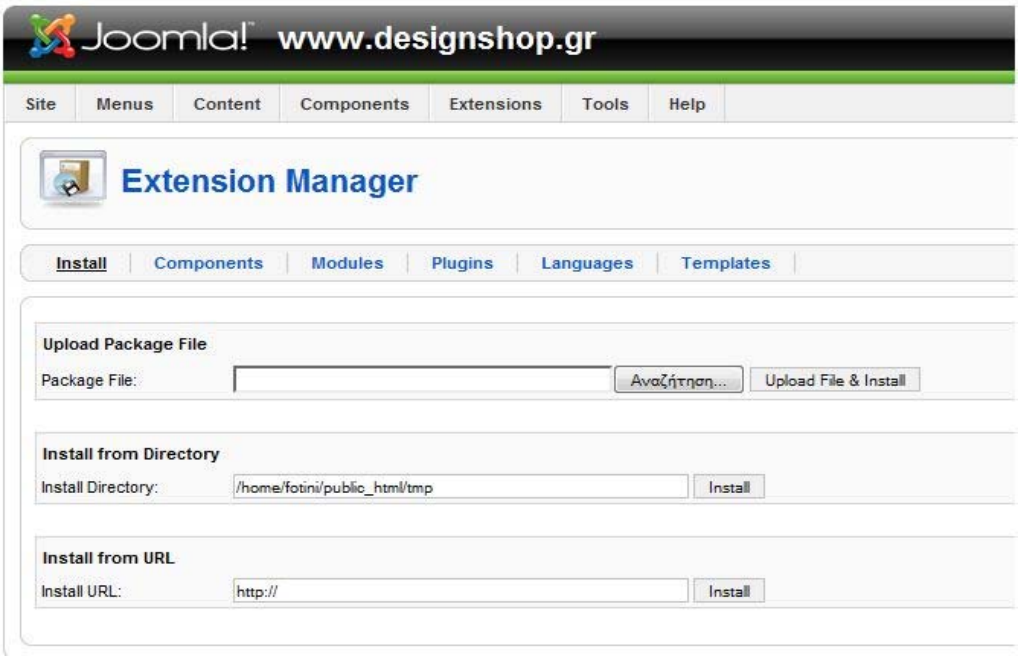
Αρχικά, πρέπει να κατεβάσουμε το Component VirtueMart. Μπορούμε να κατεβάσουμε όλες τις διαθέσιμες εκδόσεις από την επίσημη σελίδα λήψης http://virtuemart.net/ .

Ανάμεσα στα αρχεία που θα βρούμε στα downloads του http://virtuemart.net/, υπάρχει το "VirtueMart Complete Package", πρόκειται για το πλήρες πακέτο που περιέχει ένα αρχείο με όλα όσα χρειαζόμαστε για να εγκαταστήσουμε το VirtueMart σε Joomla, χρησιμοποιούν το αυτόματο σύστημα εγκατάστασης τους. Επιλέγουμε να κατεβάσουμε αυτό το αρχείο, το όποιο θα το βρούμε σε μορφή zip και με την ονομασία **VirtueMart_1.1.x-COMPLETE_PACKAGE.j15.zip.**

Το VirtueMart Complete Package περιέχει:

- Το βασικό component (com_virtuemart_1.1.x.zip).
- Το κυρίως module του VirtueMart (mod_virtuemart_1.1.x.zip).
- Δέκα σχετικά modules.
- Δύο plugins (το search και το content).

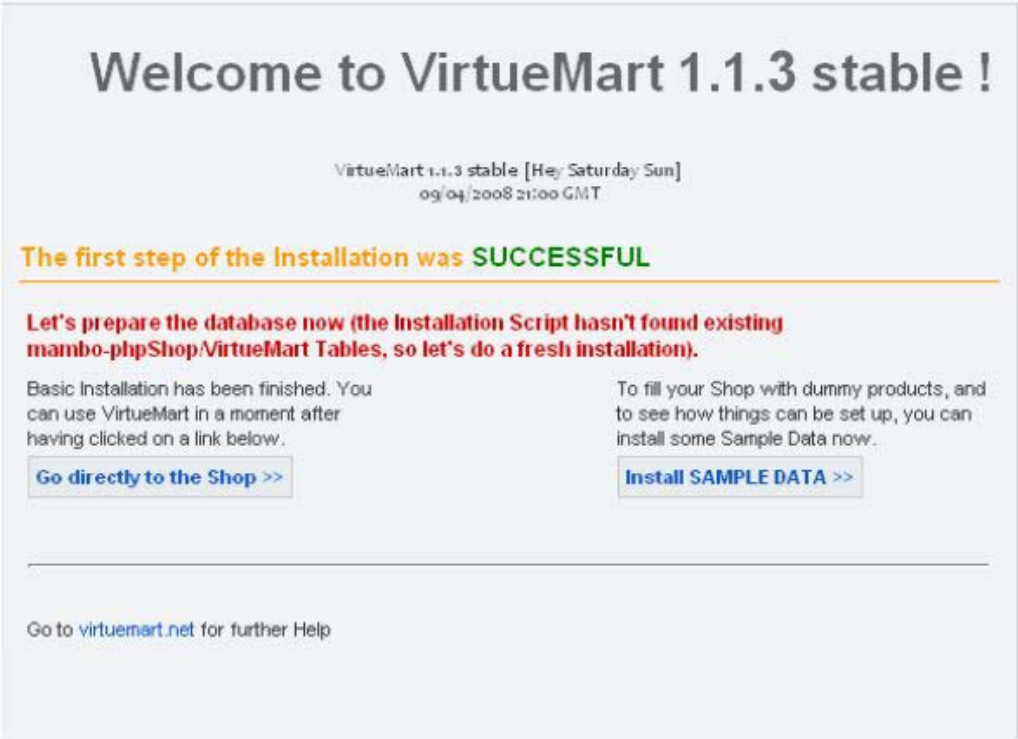
Αποθηκεύουμε το παραπάνω αρχείο στον τοπικό μας directory και κάνουμε log in στο Backend της τοπικής εγκατάστασης του Joomla. Από την επιλογή "Extensions" που βρίσκεται στο top menu επιλεγούμε "Install/Uninstall". Στην περιοχή Upload Package File κάνουμε "αναζήτηση" και επιλέγουμε το αρχείο "com_virtuemart_1.1.x.zip" που θέλουμε να εγκαταστήσουμε και πατάμε το κουμπί "Upload File & Install".



Εικόνα 32: Administrator Back-end Joomla. Οθόνη εγκατάστασης extensions

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Περιμένουμε μερικά δευτερόλεπτα μέχρι να ολοκληρωθεί η εγκατάσταση του component και βλέπουμε στην οθόνη μας ένα μήνυμα που επιβεβαιώνει πως το πρώτο βήμα της εγκατάστασης ήταν επιτυχής.



Εικόνα 33: Administrator Back-end Joomla. Επιτυχής εγκατάσταση του Virtuemart

Σε αυτό το σημείο μπορούμε να επιλέξουμε αν θέλουμε να εγκαταστήσουμε ένα δείγμα δεδομένων (ορισμένα προϊόντα, με χαρακτηριστικά, ταξινομημένα σε κατηγορίες κ.τ.λ.), για να δούμε πώς λειτουργεί το Component Virtuemart ή μπορούμε να επιλέξουμε την επιλογή "πήγαινε κατευθείαν στο κατάστημα" και δεν γίνεται καμία εγκατάσταση δειγμάτων δεδομένων. Επιλέγουμε να μην εγκαταστήσουμε δείγματα δεδομένων.

Στη συνέχεια πρέπει να εγκαταστήσουμε το κυρίως module του Virtuemart. Από την ίδια περιοχή του Extension Manager, επιλέγουμε το αρχείο "mod_virtuemart_1.1.x.zip" και κάνουμε "Upload File & Install". Αφού το εγκαταστήσουμε με επιτυχία, πηγαίνοντας στην επιλογή "Extensions" του top menu επιλεγούμε το "Module Manager" και ενεργοποιούμε το module που μόλις εγκαταστήσαμε. Αν δεν το ενεργοποιήσουμε δεν θα μπορούμε να έχουμε πρόσβαση στο ηλεκτρονικό κατάστημα.

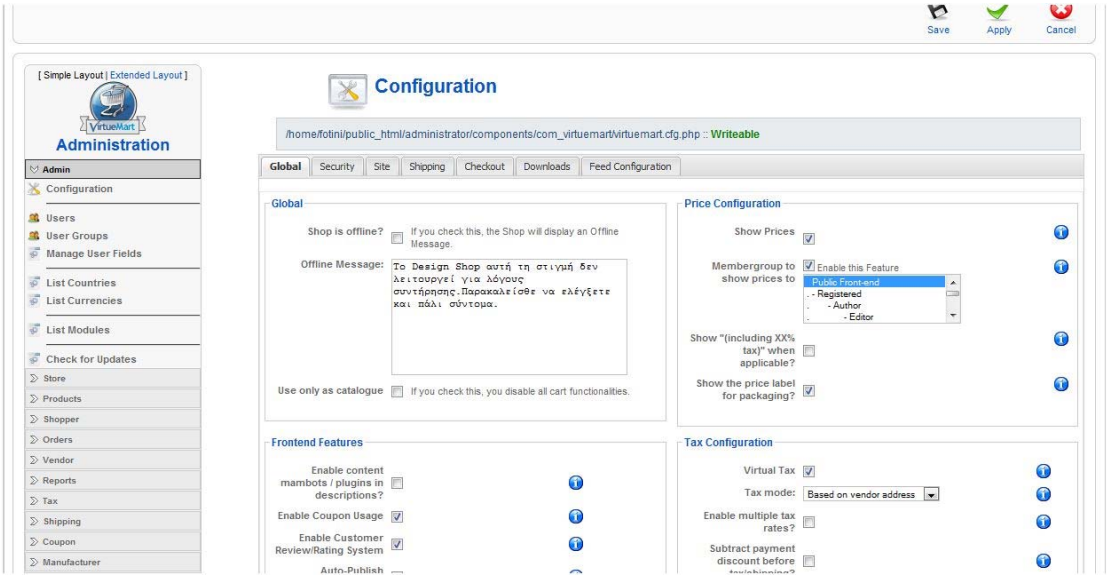
Με τον ίδιο τρόπο εγκαθιστούμε και ενεργοποιούμε και τα υπόλοιπα modules του Virtuemart (search module, frontpage categories module, XHTML product categories module).

5.3 Ρυθμίσεις διαχείρισης του Component Virtuemart

5.3.1 Admin menu

5.3.1.2 Configuration Panel

Αφού έχουν υλοποιηθεί όλα τα βήματα εγκατάστασης, έχουμε πρόσβαση στο Component Virtuemart από το top menu, επιλέγοντας Components/VirtueMart και εμφανίζεται το panel διαμόρφωσης (configuration panel) του component. Το panel διαμόρφωσης είναι το πιο σημαντικό τμήμα του VirtueMart, είναι προσβάσιμο μέσω Admin/Configuration.



Εικόνα 34: Configuration Panel, VirtueMart. Global settings

Όπως βλέπουμε στην παραπάνω εικόνα στο panel διαμόρφωσης υπάρχουν εφτά διαφορετικές καρτέλες (tabs), οι οποίες περιέχουν και τις αντίστοιχες ρυθμίσεις του component. Ονομαστικά οι καρτέλες είναι: Global, Security, Site (Display & Layout), Shipping, Checkout, Downloads.

Στην ενότητα Global έχουμε κάποιες γενικές ρυθμίσεις για το ηλεκτρονικό μας κατάστημα. Στο πρώτο πλαίσιο που ονομάζεται Global υπάρχουν τρείς επιλογές:

- **Shop is offline?:** Αν επιθυμούμε για οποιονδήποτε λόγο να θέσουμε το ηλεκτρονικό κατάστημα offline.
- **Offline Message:** Σε περίπτωση που ενεργοποιήσουμε την παραπάνω επιλογή θα εμφανιστεί αυτό το μήνυμα που θα γράψει ο διαχειριστής του ηλεκτρονικού καταστήματος ενημερώνοντας τους χρήστες για την πορεία του ιστοτόπου.
- **Use only as catalogue:** Αυτή η επιλογή απενεργοποιεί όλες τις λειτουργίες του καλαθιού αγορών και ουσιαστικά το ηλεκτρονικό κατάστημα λειτούργει σαν κατάλογος προϊόντων.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Στο πλαίσιο με όνομα Price Configuration υλοποιούνται γενικές ρυθμίσεις σχετικά με τις τιμές. Βλέπουμε τις παρακάτω επιλογές:

- **Show Prices:** Όταν ενεργοποιηθεί η επιλογή αυτή, εμφανίζονται οι τιμές των προϊόντων (είναι αρκετά χρήσιμο όταν ο ιστότοπος λειτούργει σαν κατάλογος προϊόντων). Σημαντικό είναι το γεγονός ότι δεν μπορεί να παρουσιάσει τιμές μόνο στους εγγεγραμμένους χρήστες και να τις αποκρύψει από τους απλούς επισκέπτες.
- **Membergroup to show prices to:** Η προεπιλεγμένη επιλογή είναι το "Public Frontend". Εδώ μπορούμε να αποφασίσουμε ποιά membergroups του site μας επιτρέπεται να δούν τις τιμές των προϊόντων. Αφήνουμε την προεπιλεγμένη επιλογή.
- **Show"(including XX% tax)"when applicable?:** Όταν ενεργοποιήσουμε αυτή την επιλογή οι χρήστες θα δούν το κείμενο "(συμπεριλαμβανομένων xx% φόρος)", όταν οι τιμές εμφανίζουν φόρο incl (το οποίο εξαρτάται από τις ρυθμίσεις του shopper group). Το αφήνουμε απενεργοποιημένο.
- **Show the price label for packaging?:** Ενεργοποιούμε αυτή την επιλογή, η οποία μας δίνει τη δυνατότητα να παρουσιάζεται η τιμή για πακέτα προϊόντων.

Στο πλαίσιο Frontend Features έχουμε ρυθμίσεις για τα χαρακτηριστικά του Frontend του Component Virtuemart. Έχουμε τις παρακάτω ρυθμίσεις:

- **Enable content mambots/plugins in descriptions?:** Αν ενεργοποιηθεί αυτή η επιλογή μπορούμε να χρησιμοποιήσουμε τα plugins για δυναμικό περιεχόμενο στο προϊόν ή στην περιγραφή της κατηγορίας. Το αφήνουμε απενεργοποιημένο.
- **Enable Coupon Usage:** Ενεργοποιούμε αυτή την επιλογή γιατί επιτρέπει στους πελάτες να συμπληρώσουν το κουπόνι και να κερδίσουν εκπτώσεις στις αγορές τους.
- **Enable Customer Review/Rating System:** Ενεργοποιώντας αυτή την επιλογή επιτρέπουμε στους πελάτες να γίνουν κριτές των προϊόντων, να τα βαθμολογήσουν και να γράψουν σχόλια για αυτά. Το ενεργοποιούμε.
- **Auto-Publish Reviews?:** Με αυτή την επιλογή οι κριτικές των πελατών δημοσιεύονται κατευθείαν χωρίς την έγκριση του διαχειριστή. Δεν το ενεργοποιούμε γιατί καλό θα ήταν πρώτα να ελέγχουμε τις κριτικές και μετά να δημοσιεύονται.
- **Comment Minimum/Maximum Length:** Εδώ ορίζουμε το μέγιστο και τον ελάχιστο αριθμό χαρακτήρων που πρέπει να έχει μια κριτική προϊόντος. Ορίζουμε 100 και 2000 αντίστοιχα.

Στο επόμενο πλαίσιο, Tax Configuration, έχουμε ρυθμίσεις για τους φόρους που προστήθεντε στα προϊόντα.

- **Virtual Tax:** Αυτή η επιλογή καθορίζει αν τα προϊόντα με μηδενικό βάρος θα έχουν επιπλέον φόρους ή όχι. Ενεργοποιούμε την επιλογή αυτή.
- **Tax mode:** Καθορίζει τον φορολογικό συντελεστή που λαμβάνεται για τον υπολογισμό των φόρων. Μπορεί να είναι είτε ο φορολογικός συντελεστής της διεύθυνσης αποστολής του πελάτη, είτε ο φορολογικός συντελεστής του

καταστήματος/τοποθεσία του πωλητή ή το Europian Union Mode, που αποτελεί τον φορολογικό συντελεστή της χώρας στην οποία βρίσκεται το κατάστημα ασχέτως αν των εμπορευμάτων που αποστέλλονται. Επιλέγουμε το Europian Union Mode.

- **Enable multiple tax rates?:** Ενεργοποιούμε αυτή την επιλογή αν θέλουμε να έχουμε προϊόντα με διαφορετικούς φορολογικούς συντελεστές (π.χ. 7% για τα βιβλία και τα τρόφιμα, 16% για άλλα πράγματα). Δεν μας ενδιαφέρει κάτι τέτοιο έτσι απενεργοποιούμε την επιλογή.

Στη συνέχεια, το πλαίσιο User Registration Settings ορίζουμε τις ρυθμίσεις εγγραφής των χρηστών του ηλεκτρονικού καταστήματος.

- **User Registration Type:** Επιλέγουμε τον τύπο λογαριασμού που θέλουμε να δημιουργούν οι χρήστες. Υπάρχουν τέσσερεις επιλογές:

  - Κανονική Δημιουργία Λογαριασμού (Normal Account Creation): Αυτό το είδος της εγγραφής ζητεί από κάθε πελάτη ένα όνομα χρήστη, κωδικό πρόσβασης καθώς και τις υπόλοιπες λεπτομέρειες εγγραφής.

  - Σιωπηλή Δημιουργία Λογαριασμού (Silent Account Creation): Με αυτόν τον τρόπο, οι χρήστες δεν χρειάζεται να συμπληρώσουν ένα όνομα χρήστη και ένα κωδικό πρόσβασης για τη δημιουργία νέου λογαριασμού. Αντ 'αυτού η διεύθυνση ηλεκτρονικού ταχυδρομείου χρησιμοποιείται για το νέο λογαριασμό και ένας τυχαίος κωδικός πρόσβασης δημιουργείται. Οι λεπτομέρειες εγγραφής αποστέλλονται στον πελάτη.

  - Προαιρετική Δημιουργία Λογαριασμού (Optional Account Creation): Ο πελάτης μπορεί να επιλέξει την δημιουργία ή όχι ενός λογαριασμού. Εάν ο πελάτης επιλέξει να δημιουργήσει έναν λογαριασμό, θα του ζητηθεί ένα όνομα χρήστη και ένας κωδικός πρόσβασης. Αν δεν επιλέξει να δημιουργήσει λογαριασμό, ένας κρυφός λογαριασμός δημιουργείται-έτσι ώστε ο πελάτης μπορεί να κάνει login και check out σιωπηλά.

  - Δεν είναι δυνατόν η Δημιουργία Λογαριασμού (No Account Creation possible): Με αυτόν τον τρόπο ο πελάτης μπορεί να ολοκληρώσει την παραγγελία χωρίς να δημιουργήσει ένα λογαριασμό για να τον χρησιμοποιήσει αργότερα. Κάθε φορά ένας εικονικός λογαριασμός χρήστη δημιουργείται για να διατηρηθεί ανέπαφο η δομή δεδομένων.

  Επιλέγουμε την κανονική δημιουργία λογαριασμού για τους πελάτες του ηλεκτρονικού καταστήματος.

- **Show the "Remember me" checkbox on login?:** Η επιλογή " Remember me " επιτρέπει να ρυθμιστεί ένα cookie στον browser του πελάτη έτσι ώστε να μην χρειάζεται να κάνει login κάθε φορά που επιστρέφει στο site. Αυτό γίνεται από προεπιλογή. Όμως, τέτοιου είδος cookies μπορεί να αποτελέσουν κίνδυνο για την ασφάλεια του ιστοτόπου, ειδικά όταν πολλοί χρήστες μοιράζονται τους ίδιους υπολογιστές σε internet cafes για παράδειγμα. Έτσι,

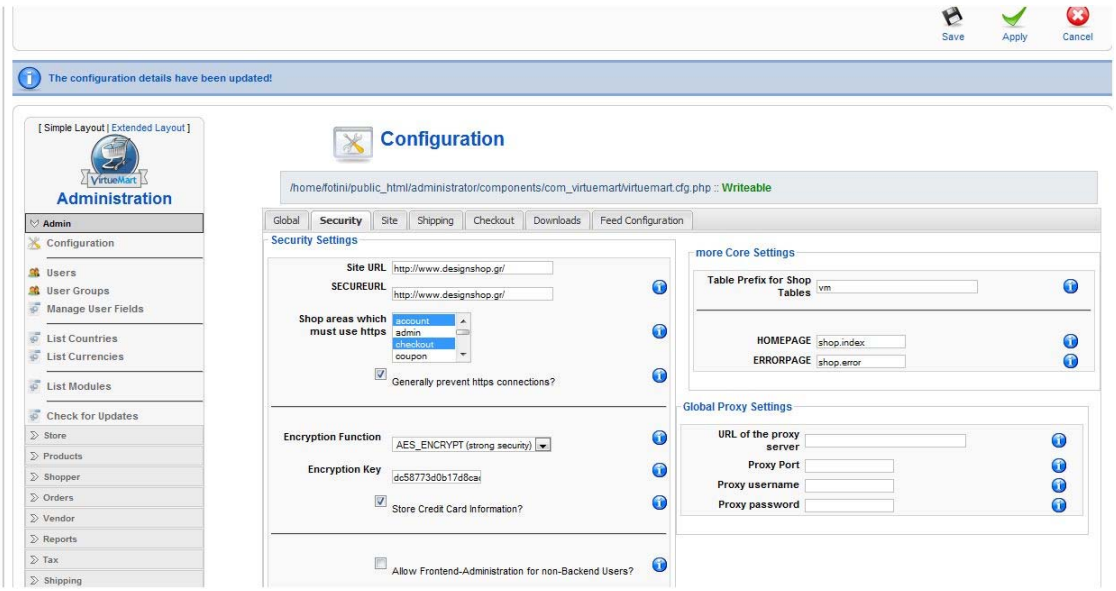
επιλέγουμε αυτή την επιλογή για να επιτρέψουμε στους πελάτες να μην αποθηκεύσουν τα cookies των χρηστών.

- **Must agree to Terms of Service?:** Ενεργοποιούμε την επιλογή αυτή γιατί θέλουμε ο πελάτης να συμφωνήσει με τους "Όρους της υπηρεσίας" πριν την εγγραφή του στο ηλεκτρονικό μας κατάστημα.
- **Show information about "Return Policy" on the order confirmation page?:** Για τους ιδιοκτήτες καταστημάτων, ηλεκτρονικών και μη ,στις περισσότερες ευρωπαϊκές χώρες απαιτείται από το νόμο να ενημερώνουν τους πελάτες τους σχετικά με την πολιτική της επιστροφή και της ακύρωσης παραγγελιών. Έτσι, ενεργοποιούμε την επιλογή αυτή και γραφούμε παρακάτω τους στο πλαίσιο **Legal information text (short version)** τους όρους επιστροφής και ακύρωσης παραγγελίας.

Στη συνέχεια στο πλαίσιο Core Settings ρυθμίζουμε τις επιλογές του component για τα αποθέματα των προϊόντων.

- **Check Stock?:** Ορίζει αν θα ελέγχεται το επίπεδο των αποθεμάτων όταν ένας χρήστης προσθέτει ένα στοιχείο στο καλάθι αγορών. Σε περίπτωση που η επιλογή αυτή είναι ενεργοποιημένη, δεν θα επιτρέπει στο χρήστη να προσθέσει περισσότερα προϊόντα στο καλάθι αγορών του από ό,τι είναι διαθέσιμα στο απόθεμα του συγκεκριμένου προϊόντος. Ενεργοποιούμε την επιλογή.
- **Enable the Cookie Check?:** Σε περίπτωση που ενεργοποιηθεί, το component ελέγχει αν ο browser που χρησιμοποιεί ο χρήστης δέχεται cookies ή όχι. Αυτό είναι φιλικό προς το χρήστη, αλλά μπορεί να έχει αρνητικές συνέπειες για τις μηχανές αναζήτησης του καταστήματος. Το ενεργοποιούμε.
- **Select a currency converter module:** Επιλέγουμε το convertECB.php, το συγκεκριμένο module είναι μετατροπέας νομίσματος.
- **Order-mail format:** Εδώ καθορίζουμε τον τρόπο που έχουν συσταθεί τα μηνύματα επιβεβαίωσης παραγγελιών, επιλέγουμε HTML mail.

Στην δεύτερη ενότητα ρυθμίζουμε την ασφάλεια του component Virtuemart.



Εικόνα 35: Configuration Panel, VirtueMart. Security settings

- **SECUREURL**: Αν έχουμε επιλέξει το ηλεκτρονικό μας κατάστημα να χρησιμοποιήσει SSL πιστοποιητικό ασφαλείας (ανάπτυξη του SSL πιστοποιητικού ασφαλείας γίνεται στην ενότητα 9.4) πληκτρολογούμε το url του ισοτόπου μας αρχίζοντας με https και τελειώνοντας με κάθετος, https://www.mydesignshop.eu/. Πρέπει να είμαστε αρκετά προσεκτικοί σε αυτό το πεδίο γιατί αν η διεύθυνση δεν υπάρχει, οι πελάτες θα στραφούν προς μια διεύθυνση που δεν υπάρχει και θα λάβουν σφάλμα 404!
- **Shop areas which must use https:** Μερικές από τις περιοχές του καταστήματος, όπως το login του χρήστη είναι αναγκασμένες να χρησιμοποιούν SECUREURL σύνδεση. Εδώ επιλέγουμε τις ενότητες που θεωρούμε εμείς ότι πρέπει να χρησιμοποιούν το SECUREURL. Εξ 'ορισμού είναι: "λογαριασμός" (Account Maintenance) και "ταμείο" (το πλήρες Ταμείο).
- **Encryption Function:** Συνιστάται η επιλογή AES_ENCRYPT. Επιλέγουμε την MySQL λειτουργία, η οποία χρησιμοποιείται για να κωδικοποιήσει και να κρυπτογραφήσει σημαντικά στοιχεία στους πίνακες δεδομένων. Η AES κρυπτογράφηση είναι πολύ πιο ασφαλή, διότι στην πραγματικότητα κρυπτογραφεί τα δεδομένα, δεν τα κωδικοποιεί μόνο. Η AES κρυπτογράφηση είναι διαθέσιμη για MySQL > = 4.0.2.
- **Encryption Key:** Το μυστικό κλειδί για την κρυπτογράφηση των δεδομένων του λογαριασμού πληρωμών, όπως αριθμούς πιστωτικών καρτών και την αποθήκευση τους κρυπτογραφημένα στην βάση δεδομένων.
- **Store Credit Card Information?:** Επιτρέπει να απενεργοποιήσετε εντελώς την αποθήκευση των δεδομένων πιστωτικών καρτών, το απενεργοποιούμε.
- **Table Prefix for Shop Tables:** Αυτό είναι ένα πειραματικό χαρακτηριστικό που επιτρέπει πολλαπλά καταστήματα σε μια εγκατάσταση Joomla.
- **HOMEPAGE:** Αυτή είναι η σελίδα που θα φορτωθεί στο frontend από προεπιλογή. Συμπληρώνουμε shop.index.
- **ERRORPAGE:** Αυτή είναι η προεπιλεγμένη σελίδα για την εμφάνιση VirtueMart μηνύματα λάθους. Συμπληρώνουμε shop.error.

Στην τρίτη ενότητα, Site, ορίζουμε τις ρυθμίσεις για το τι επιπλέον θα φαίνεται στον ιστότοπο μας.

- **PDF-Button:** Ενεργοποιούμε την επιλογή για να εμφανιστεί το PDF-Button στο Frontend του καταστήματος.
- **Show the "Print View" link?:** Ενεργοποιούμε την επιλογή για να εμφανιστεί ο σύνδεσμος εκτύπωσης σελίδας στο Frontend του καταστήματος.
- **Show Page Navigation at the Top of the Product Listing?:** Ενεργοποιούμε την οθόνης της σελίδας πλοήγησης στην αρχή της λίστας προϊόντων στο Frontend του καταστήματος.
- **Default product sort order:** Επιλέγουμε Product Name και σύμφωνα με αυτό το κριτήριο τα προϊόντα ταξινομούνται στους καταλόγους προϊόντων.
- **Available "Sort-by" fields:** Επιλέγουμε Product Name, Price, Latest Products τα οποία αποτελούν τα κριτήρια που εμφανίζονται στον πελάτη για να επαναταξινομήσει τη λίστα προϊόντων.

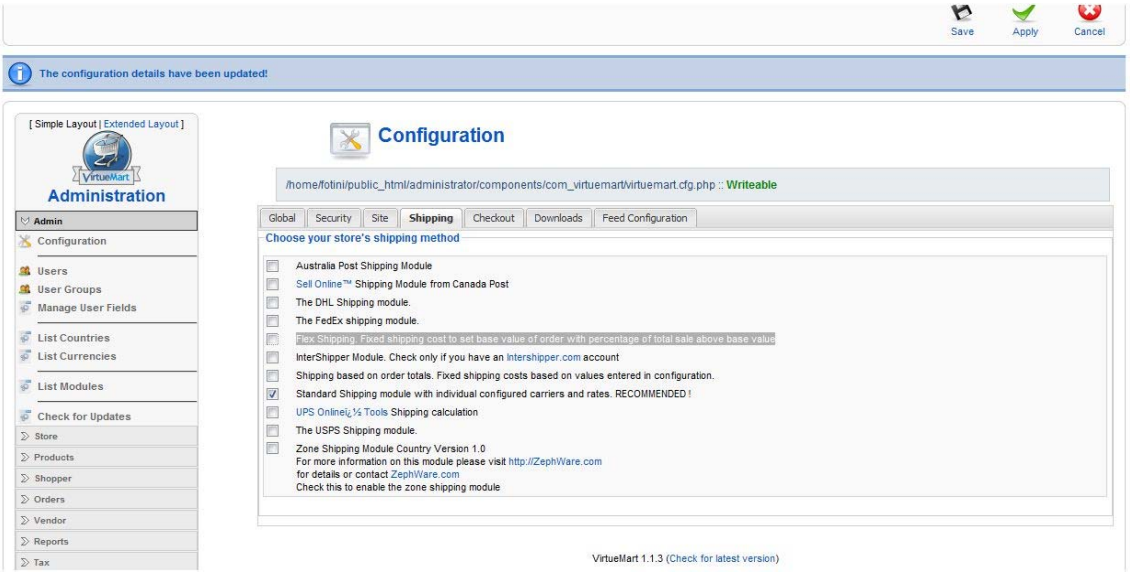
Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

- **"no image" image:** Επιλέγουμε την default εικόνα (**/components/com_virtuemart/themes/default/images/noimage.gif**) που θα προβάλλεται κατά την εικόνα του προϊόντος δεν είναι διαθέσιμο.

Στο πλαίσιο Layout έχουμε ρυθμίσεις για το πως θα είναι το layout του component Virtuemart.

- **Select the theme for your Shop:** Εδώ μπορούμε να επιλέξετε το θέμα το οποίο χρησιμοποιείται για το στυλ του καταστήματος. Αφήνουμε την προεπιλεγμένη επιλογή.
- **Default number of products in a row:** Αυτό καθορίζει τον αριθμό των προϊόντων που προβάλλονται σε μια σειρά. Επιλέγουμε 2 προϊόντα ανά σειρά.
- **FLYPAGE:** Αυτή είναι η σελίδα που χρησιμοποιείται για την εμφάνιση των λεπτομερειών του προϊόντος. Αφήνουμε την default επιλογή flypage.tpl.
- **Enable Dynamic Thumbnail Resizing?:** Επιτρέπει τη δυναμική αλλαγή μεγέθους εικόνας. Αυτό σημαίνει ότι όλες μικρογραφίες αλλάζουν μέγεθος για να ταιριάζουν στα μεγέθη που θα ορίσουμε στη συνέχεια, χρησιμοποιώντας τις λειτουργίες GD2 της PHP.
- **Thumbnail Image Width/Height:** Ορίζουμε το πλάτος και το ύψος της μικρογραφίας της εικόνας. Δίνουμε διαστάσεις 90 και στα δύο.

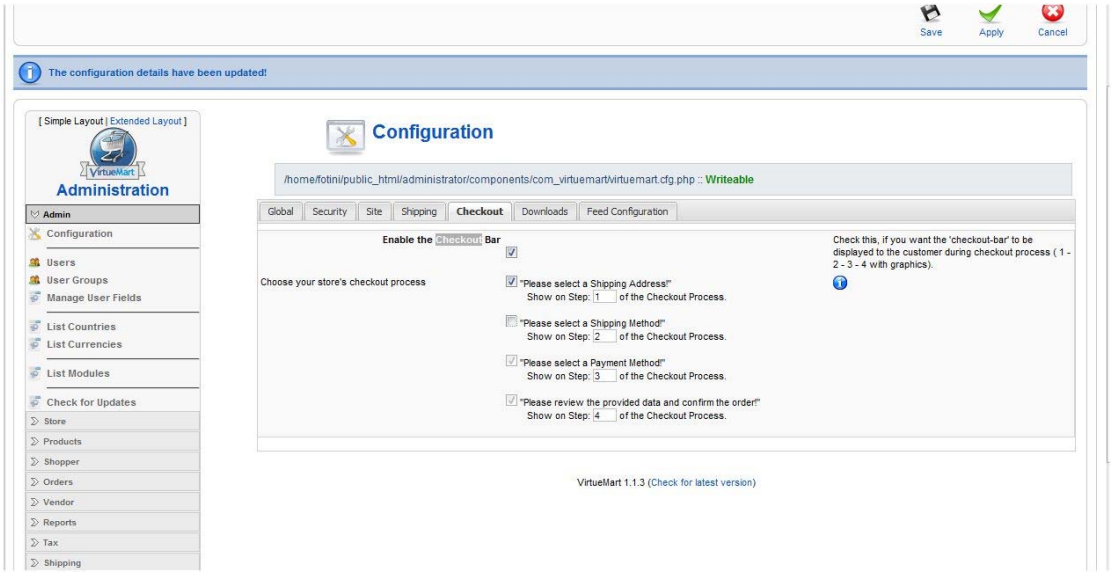
Στην επόμενη ενότητα Shipping μπορούμε να επιλέξουμε ένα ή περισσότερα Shipping Modules. Ουσιαστικά επιλεγούμε τη μέθοδο αποστολής των προϊόντων του καταστήματος μας. Επιλέγουμε το "Standard Shipping module with individual configured carriers and rates. ".



Εικόνα 36: Configuration Panel, VirtueMart. Shipping settings

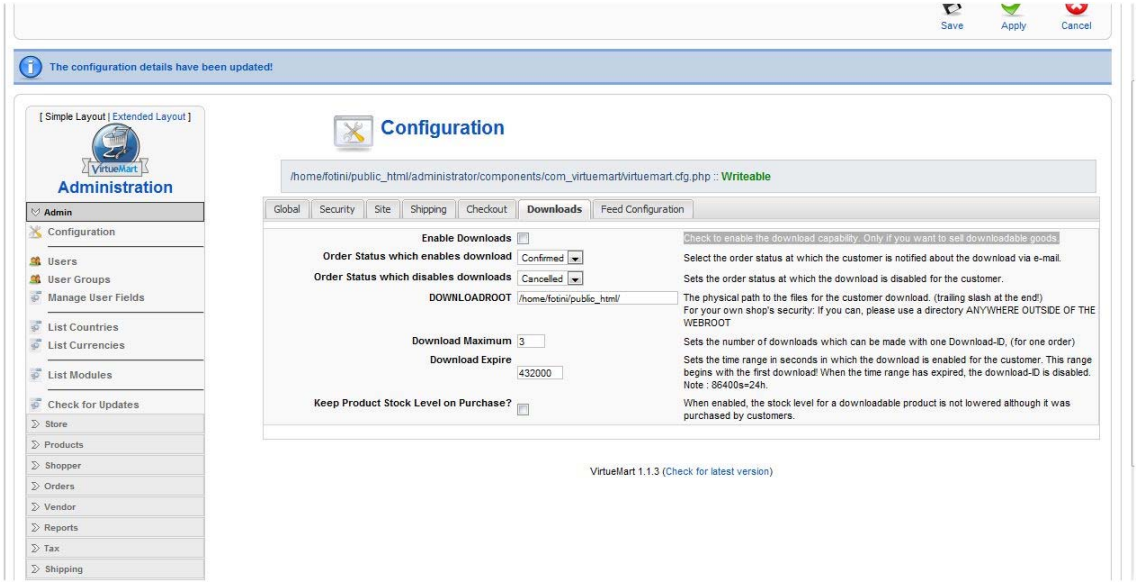
Στην ενότητα Checkout ορίζουμε κάποιες ρυθμίσεις για το πως θα διεξάγεται η διαδικασία πληρωμής του πελάτη στο ταμείο. Ενεργοποιούμε την επιλογή **Enable the Checkout Bar** και αυτό μας δίνει τη δυνατότητα το checkout του χρήστη να

εμφανίζεται με βήματα 1-2-3-4 τα οποία παρουσιάζονται με γραφικά. Από τα βήματα που παρουσιάζονται παρακάτω απενεργοποιούμε το δεύτερο βήμα στο οποίο επιλέγεται η μέθοδος αποστολής.



Εικόνα 37: Configuration Panel, VirtueMart. Checkout settings

Η επόμενη ενότητα ονομάζεται Downloads. Θα ενεργοποιήσουμε τις επιλογές της, αν στο ηλεκτρονικό μας κατάστημα θέλουμε να πουλήσουμε downloadable εμπορεύματα. Δεν μας ενδιαφέρει κάτι τέτοιο, έτσι αφήνουμε την ενότητα απενεργοποιημένη.



Εικόνα 38: Configuration Panel, VirtueMart. Download settings

5.3.1.3 Users, user groups, manage user fields

Στη συνέχεια, στο μενού Admin έχουμε κάποιες ρυθμίσεις για τους χρήστες, για τις ομάδες χρηστών που δημιουργούνται καθώς και για τα πεδία που καλούνται να συμπληρώσουν οι χρήστες κατά την δημιουργία του account τους.

Στο υπομενού users παρουσιάζεται ένας πίνακας με όλους τους εγγεγραμμένους χρήστες του ηλεκτρονικού καταστήματος. Οι πληροφορίες που αντλούμε από τον πίνακα αυτό είναι το username, το full name και το group στο οποίο ανήκει ο κάθε χρήστης. Οι ενέργειες που επιτρέπονται είναι η δημιουργία νέου χρήστη και η διαγραφή κάποιου χρήστη που ήδη υπάρχει.

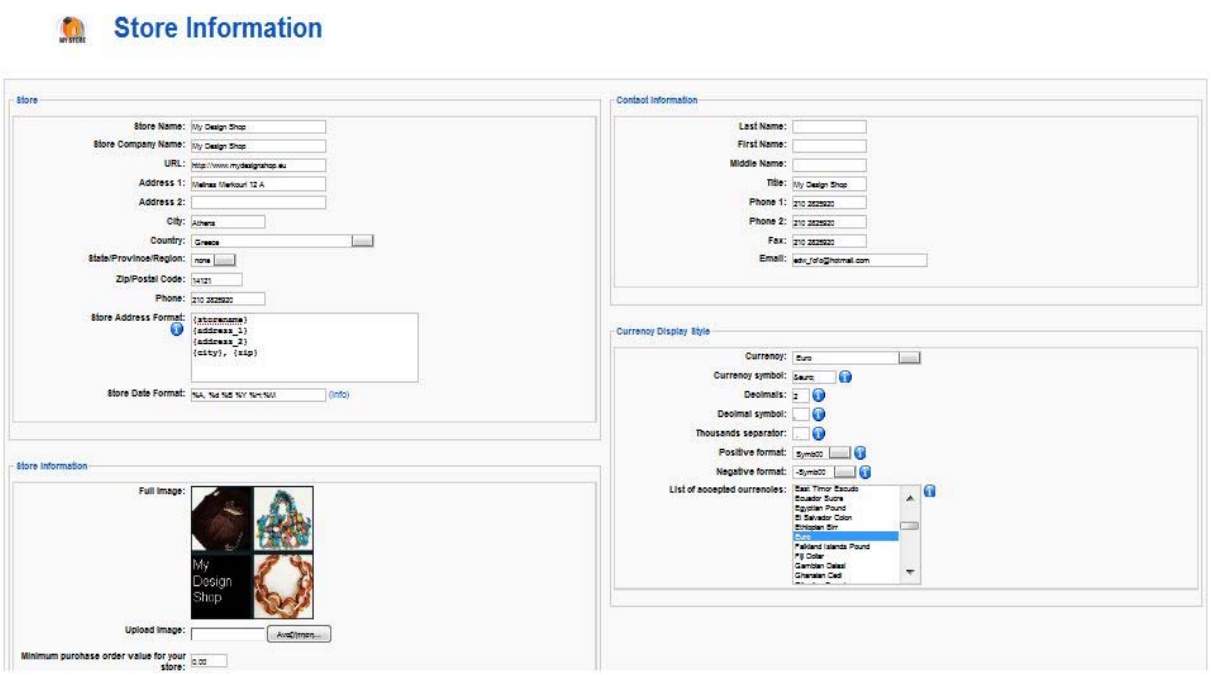
Το υπομενού user groups (ομάδες χρηστών) είναι οι "εξουσιοδοτημένες ομάδες" και χρησιμοποιείται για να περιορίσει την πρόσβαση σε ορισμένα τμήματα και σε ορισμένες λειτουργίες του ηλεκτρονικού καταστήματος. Κάθε εγγεγραμμένος χρήστης έχει ανατεθεί σε μια ομάδα χρηστών. Από προεπιλογή οι εγγεγραμμένοι πελάτες είναι μέλη της ομάδας "shopper".

Αυτός ο διαχωρισμός των χρηστών σε ομάδες είναι χρήσιμος όταν θέλουμε να δίνουμε διαφορετικά premissions στους πελάτες του καταστήματος. Για παράδειγμα, έστω ότι μια ομάδα εγγεγραμμένων χρηστών-πελατών πρέπει να έχει πρόσβαση στον τομέα των αναφορών του συστήματος (report section). Αυτή η αδεία πρόσβασης περιορίζεται μόνο στις ομάδες των admin και stoeradmin. Εάν έχουμε αντιστοιχίσει το χρήστη στην admin ή storeadmin ομάδα, θα είναι επίσης σε θέση να έχει πρόσβαση και σε άλλα τμήματα του καταστήματος όπου θα μπορούσε να αλλάξει ή να διαγράψει σημαντικά δεδομένα. Έτσι, ο διαχωρισμός των χρηστών σε ομάδες μας δίνει τη λύση να προσθέσουμε μια νέα ομάδα χρηστών που ονομάζεται " report ", θα έχει τα ίδια δικαιώματα με την ομάδα των shopper συν την πρόσβαση στις αναφορές του συστήματος.

Το υπομενού manage user fields μας επιτρέπει να τροποποιήσουμε τα ελεύθερα πεδία που εμφανίζονται στην καταχώριση και τη συντήρηση του λογαριασμού των χρηστών. Τα πεδία αυτά είναι για παράδειγμα: Όνομα, Επώνυμο, Τηλέφωνο κ.τ.λ.. Μπορούμε να επιλέξουμε ποιά από αυτά τα πεδία είναι υποχρεωτικά, ποιά θα εμφανίζονται και σε ποιό σημείο.

5.3.2 Ρυθμίσεις πληροφοριών του καταστήματος

Για να ξεκινήσουμε τη λειτουργία του καταστήματος πρέπει να ρυθμίσουμε τις πληροφορίες του.Απο το μενού αριστερά στο περιβάλλον διαχείρισης του VirtueMart component επιλέγουμε "Store|Edit Store".



Εικόνα 39: Edit Store Panel**,** VirtueMart. Store Information

Συμπληρώνουμε τα πεδία στην ενότητα "Store Information", για να εμπλουτίσουμε το κατάστημα μας με τις βασικές πληροφορίες οι οποίες θα εμφανίζονται στους πελάτες κατά τη διεξαγωγή των παραγγελιών.

Στο πλαίσιο Store υπάρχουν οι παρακάτω επιλογές:

- **Store Name/Store Company Name:** Τα πεδία αυτά είναι υποχρεωτικά και συμπληρώνουμε το όνομα του καταστήματος μας και την εταιρία στην οποία ανήκει. Για το συγκεκριμένο κατάστημα η ονομασία είναι My Design Shop και στα δύο πεδία.
- **URL:** Συμπληρώνουμε το url του καταστήματος, http://www.mydesignshop.eu.
- **Address 1/Address 2/City/State/Province/Region/Country/Zip/Postal Code/Phone:** Σε αυτά τα πεδία δίνουμε τα στοιχεία διεύθυνσης, πόλης, περιοχής, χώρας, ταχυδρομικού κώδικα και του τηλεφώνου τα οποία αντιστοιχούν στο κατάστημα μας. Το παρόν κατάστημα είναι εικονικό οπότε τα στοιχεία αυτά δεν ανταποκρίνονται στην πραγματικότητα.

Στη συνέχεια, έχουμε το πλαίσιο Contact Information στο οποίο μας ζητούνται τα στοιχεία του ατόμου που είναι υπεύθυνο για την επικοινωνία με τους πελάτες. Συμπληρώνουμε μονό το πεδίο της ηλεκτρονικής διεύθυνσης.

Στο πλαίσιο Store Information υπάρχουν οι βασικές πληροφορίες ενός ηλεκτρονικού καταστήματος. Συμπληρώνουμε τα παρακάτω πεδία:

- **Full Image:** Το πεδίο αυτό είναι υποχρεωτικό και εμφανίζει τον τρέχον ρυθμισμένο λογότυπο του καταστήματος.
- **Minimum Purchase Order Value/Minimum Amount for Free Shipping:** Σε αυτά τα πεδία συμπληρώνουμε την ελάχιστη αξία της παραγγελίας και το ελάχιστο ποσό παραγγελίας για το οποίο ο πελάτης θα έχει δωρεάν έξοδα

μεταφοράς. Δεν επιθυμούμε να βάλουμε αυτές τις υπηρεσίες στο κατάστημα μας, έτσι αφήνουμε τα πεδία κενά.

Στο επόμενο πλαίσιο, Currency Display Style, ρυθμίζουμε τις βασικές μεταβλητές του βασικού νομίσματος συναλλαγών.

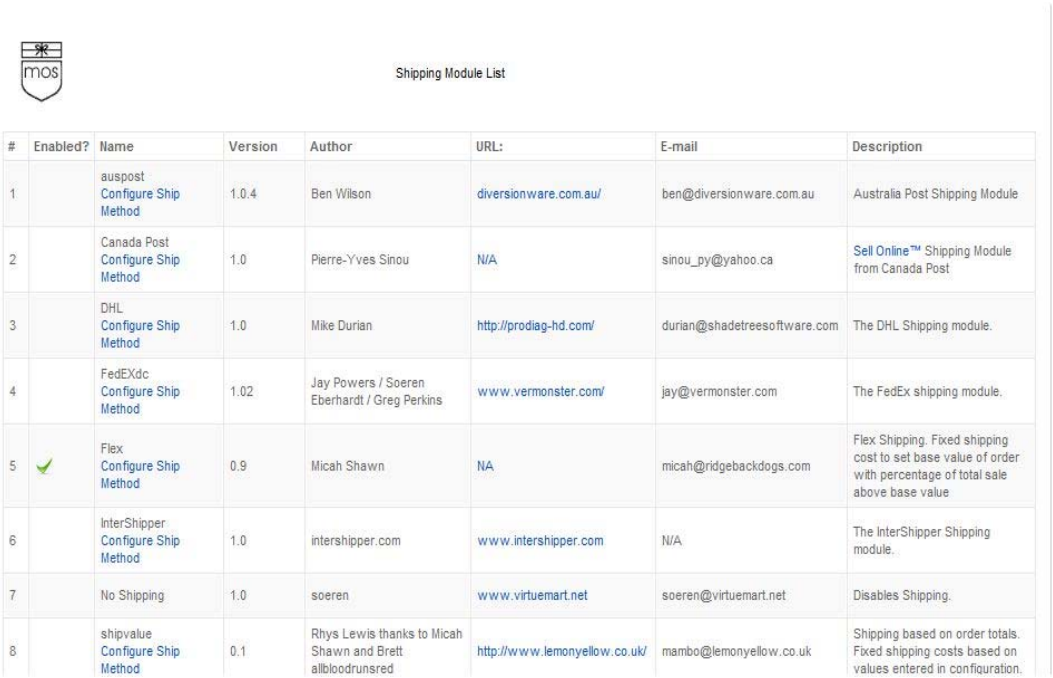
- **Currency:** Εδώ ρυθμίζουμε το default νόμισμα του καταστήματος μας. Στην λίστα επιλογής υπάρχουν σχεδόν όλα τα νομίσματα συναλλαγών ανά τον κόσμο, επιλέγουμε το "euro" και στο αμέσως επόμενο πεδίο, στο **Currency symbol**, συμπληρώνεται αυτόματα το σύμβολο του νομίσματος.
- **Decimals**: Ορίζουμε πόσα δεκαδικά ψηφία θα υπάρχουν στις τιμές των προϊόντων. Του δίνουμε την τιμή δύο.
- **Decimal symbol/Thousands separator:** Σε αυτά τα πεδία ορίζουμε αν θα χρησιμοποιήσουμε "." ή ", " για την διαχώριση των δεκαδικών ψηφίων και των χιλιάδων αντίστοιχα. Επιλέγουμε το σύμβολο "," για τα δεκαδικά ψηφία και το σύμβολο "." για την διαχώριση των χιλιάδων.
- **List of accepted currencies:** Μας εμφανίζεται μια λίστα με διαφορετικά νομίσματα ανά τον κόσμο, μπορούμε να επιλέξουμε ποιά νομίσματα, εκτός από το default νόμισμα που ορίσαμε παραπάνω, θα γίνονται δεκτά στις συναλλαγές του καταστήματος. Δεν θα έχουμε αυτή την επιλογή στο παρόν κατάστημα, έτσι δεν επιλέγεται κάτι από την λίστα.

Στη συνέχεια υπάρχει το πλαίσιο Description στο οποίο μπορούμε να γράψουμε μια περιγραφή του καταστήματος μας. Αυτό είναι η περιγραφή εμφανίζεται στην σελίδα shop.index.

Στο τελευταίο πλαίσιο, Terms of Service, της ενότητας αυτής υπάρχει ένας editor στον οποίο μπορούμε να γράψουμε τους όρους χρήσης των υπηρεσιών του καταστήματος μας.

5.3.3 Shipping Module List

Στο αριστερό μενού "Store" υπάρχει η μια λίστα με τις μεθόδους αποστολής που υποστηρίζει το component Virtuemart. Αρχικά, θα πρέπει πρώτα να σκεφτούμε πώς θα χρεώνονται οι πελάτες για τα ταχυδρομικά τέλη και τις συσκευασίες των προϊόντων. Ο ευκολότερος τρόπος θα ήταν να έχουμε μια σταθερή τιμή για όλες τις αποστολές των προϊόντων μας, αλλά αυτό δεν είναι πάντα η σωστή πρακτική-ειδικά αν τα προϊόντα μας ποικίλλουν σημαντικά σε μέγεθος ή βάρος. Θα πρέπει να σκεφτούμε όχι μόνο για τις χρεώσεις αποστολής αλλά και για της μεθόδους αποστολής.



Shipping Module List

#	Enabled?	Name	Version	Author	URL:	E-mail	Description
1		auspost Configure Ship Method	1.0.4	Ben Wilson	diversionware.com.au/	ben@diversionware.com.au	Australia Post Shipping Module
2		Canada Post Configure Ship Method	1.0	Pierre-Yves Sinou	N/A	sinou_py@yahoo.ca	Sell Online™ Shipping Module from Canada Post
3		DHL Configure Ship Method	1.0	Mike Durian	http://prodiag-hd.com/	durian@shadetreesoftware.com	The DHL Shipping module.
4		FedEXdc Configure Ship Method	1.02	Jay Powers / Soeren Eberhardt / Greg Perkins	www.vermonster.com/	jay@vermonster.com	The FedEx shipping module.
5	✓	Flex Configure Ship Method	0.9	Micah Shawn	NA	micah@ridgebackdogs.com	Flex Shipping. Fixed shipping cost to set base value of order with percentage of total sale above base value
6		InterShipper Configure Ship Method	1.0	intershipper.com	www.intershipper.com	N/A	The InterShipper Shipping module.
7		No Shipping	1.0	soeren	www.virtuemart.net	soeren@virtuemart.net	Disables Shipping.
8		shipvalue Configure Ship Method	0.1	Rhys Lewis thanks to Micah Shawn and Brett allbloodrunsred	http://www.lemonyellow.co.uk/	mambo@lemonyellow.co.uk	Shipping based on order totals. Fixed shipping costs based on values entered in configuration.

Εικόνα 40: Shipping Module List, VirtueMart.

Το component Virtuemart προσφέρει περισσότερες από μία μέθοδο αποστολής-για παράδειγμα παράδοση την επόμενη μέρα. Ακόμη, αν αποφασίσουμε να χρησιμοποιήσουμε μία εταιρεία, η οποία δε υπάρχει στη λίστα, για όλες τις αποστολές προϊόντων, θα πρέπει να ενημερώσουμε το component VirtueMart γι 'αυτό.

Για να δημιουργήσουμε μια νέα μέθοδο αποστολής, επιλέγουμε από το μενού "Shipping|Create Shipper " και μας εμφανίζει τον shipper editor.

Εικόνα 41: Shipper edit/create, VirtueMart. Δημιουργία καινούριας μεθόδου αποστολής προϊόντων

5.3.4 Εισαγωγή νέου προϊόντος

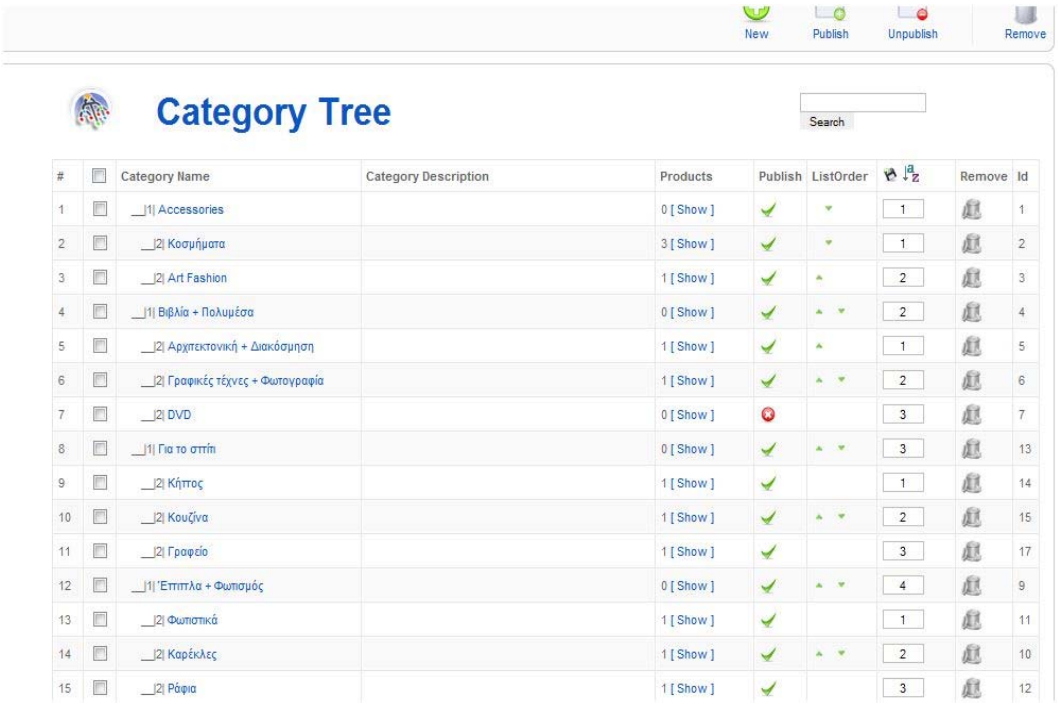
Το component VirtueMart προσφέρει τη δυνατότητα να ταξινομούμε τα προϊόντα όχι μόνο ανά κατασκευαστή, αλλά και ανά κατηγορία προϊόντος. Οι κατηγορίες προϊόντων μπορεί επίσης να περιέχουν υποκατηγορίες επιτρέποντας έτσι στους διαχειριστές του ηλεκτρονικού καταστήματος να διαχειρίζονται τα προϊόντα τους με όσο το δυνατόν περισσότερο λεπτομερή τρόπο.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Στο σημείο αυτό αξίζει να αναφέρουμε ότι επειδή τα προϊόντα και οι κατηγορίες προϊόντων μπορούν να συνδεθούν με ένα συγκεκριμένο vendor (πωλητή), είναι σημαντικό να δημιουργηθούν τα αρχεία του vendor (πωλητή) πριν από τη δημιουργία του προϊόντος και της κατηγορία προϊόντων.

Οι εφαρμογές "vendors" και "vendor categories" αντιπροσωπεύουν την πιο πάνω βαθμίδα του administration του component VirtueMart. Μέσω του vendor administration, ο κάτοχος του καταστήματος είναι σε θέση να διαχειριστεί τα προϊόντα, τους χρήστες, καθώς και τις παραγγελίες του πωλητή ή του προμηθευτή. Ωστόσο, αυτή η εφαρμογή δεν ισχύει για την συγκεκριμένη έκδοση του component VirtueMart που χρησιμοποιούμε, θα είναι διαθέσιμη στο μέλλον.

Η εισαγωγή νέου προϊόντος προϋποθέτει τη δημιουργία κατηγοριών. Από το μενού "Products" οδηγούμαστε στο υπομενού "List Categories" και βλέπουμε τη λίστα με τις κατηγορίες και τις υποκατηγορίες προϊόντων που έχουμε δημιουργήσει.



Εικόνα 42: Category Tree, VirtueMart. Λίστα κατηγοριών και υποκατηγοριών προϊόντων

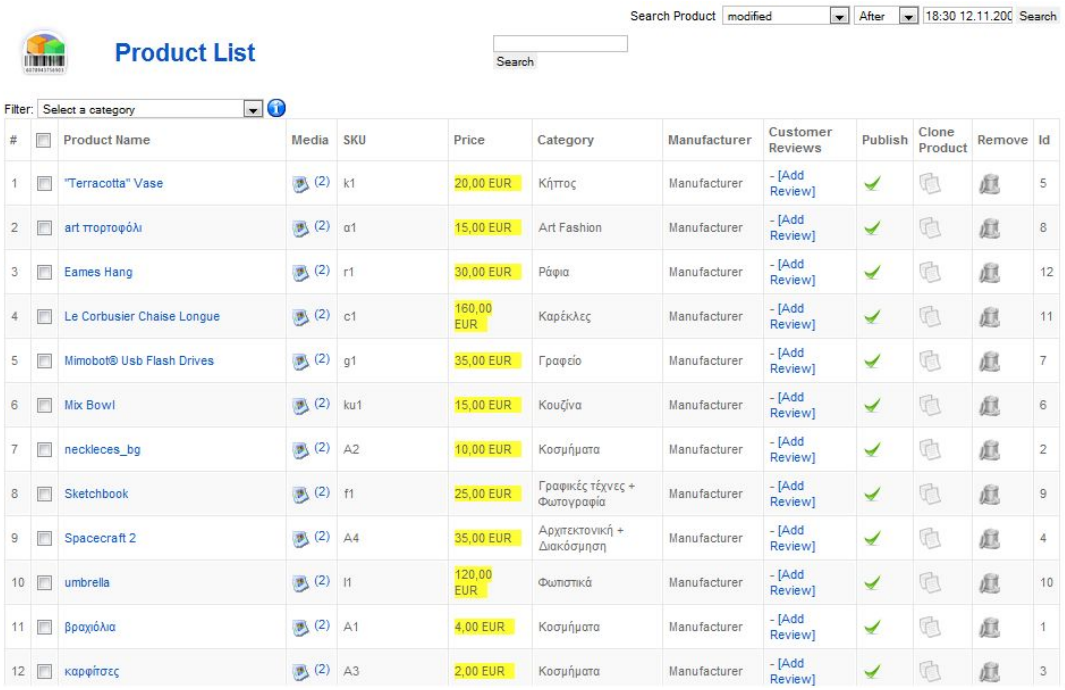
Για την προσθήκη νέας κατηγορίας και υποκατηγορίας κάνουμε κλικ στο κουμπί "Νέο". Μας εμφανίζονται δύο καρτέλες "Category Information" με τα στοιχεία που πρέπει να συμπληρωθούν για την δημιουργία της νέας κατηγορίας. Στην πρώτη καρτέλα έχουμε:

- **Category Name:** Το όνομα της κατηγορίας/υποκατηγορίας, το πεδίο είναι υποχρεωτικό.
- **Category Description:** Μια σύντομη περιγραφή της κατηγορίας/υποκατηγορίας.

- **Parent:** Εδώ γίνεται ο διαχωρισμός ανάμεσα στην δημιουργία κατηγορίας και υποκατηγορίας, ουσιαστικά καλούμαστε να επιλέξουμε την αρχική τους ρίζα. Για την κατηγορία επιλέγουμε την επιλογή "Default-Top Level" και για την υποκατηγορία την αντίστοιχη κατηγορία που ανήκει.

Στην δεύτερη καρτέλα μπορούμε αν θέλουμε να χρησιμοποιήσουμε μια εικόνα για την προβολή της κατηγορίας/υποκατηγορίας.

Τώρα μπορούμε να εισάγουμε νέα προϊόντα στο ηλεκτρονικό κατάστημα. Στο υπομενού "List Products" έχουμε ένα πίνακα με όλα τα προϊόντα του καταστήματος.



#		Product Name	Media	SKU	Price	Category	Manufacturer	Customer Reviews	Publish	Clone Product	Remove	Id
1		"Terracotta" Vase	(2)	k1	20,00 EUR	Κήπος	Manufacturer	- [Add Review]				5
2		art πορτοφόλι	(2)	α1	15,00 EUR	Art Fashion	Manufacturer	- [Add Review]				8
3		Eames Hang	(2)	r1	30,00 EUR	Ράφια	Manufacturer	- [Add Review]				12
4		Le Corbusier Chaise Longue	(2)	c1	160,00 EUR	Καρέκλες	Manufacturer	- [Add Review]				11
5		Mimobot® Usb Flash Drives	(2)	g1	35,00 EUR	Γραφείο	Manufacturer	- [Add Review]				7
6		Mix Bowl	(2)	ku1	15,00 EUR	Κουζίνα	Manufacturer	- [Add Review]				6
7		neckleces_bg	(2)	A2	10,00 EUR	Κοσμήματα	Manufacturer	- [Add Review]				2
8		Sketchbook	(2)	f1	25,00 EUR	Γραφικές τέχνες + Φωτογραφία	Manufacturer	- [Add Review]				9
9		Spacecraft 2	(2)	A4	35,00 EUR	Αρχιτεκτονική + Διακόσμηση	Manufacturer	- [Add Review]				4
10		umbrella	(2)	l1	120,00 EUR	Φωτιστικά	Manufacturer	- [Add Review]				10
11		βραχιόλια	(2)	A1	4,00 EUR	Κοσμήματα	Manufacturer	- [Add Review]				1
12		καρφίτσες	(2)	A3	2,00 EUR	Κοσμήματα	Manufacturer	- [Add Review]				3

Εικόνα 43: Product List, VirtueMart. Πίνακας προϊόντων του καταστήματος

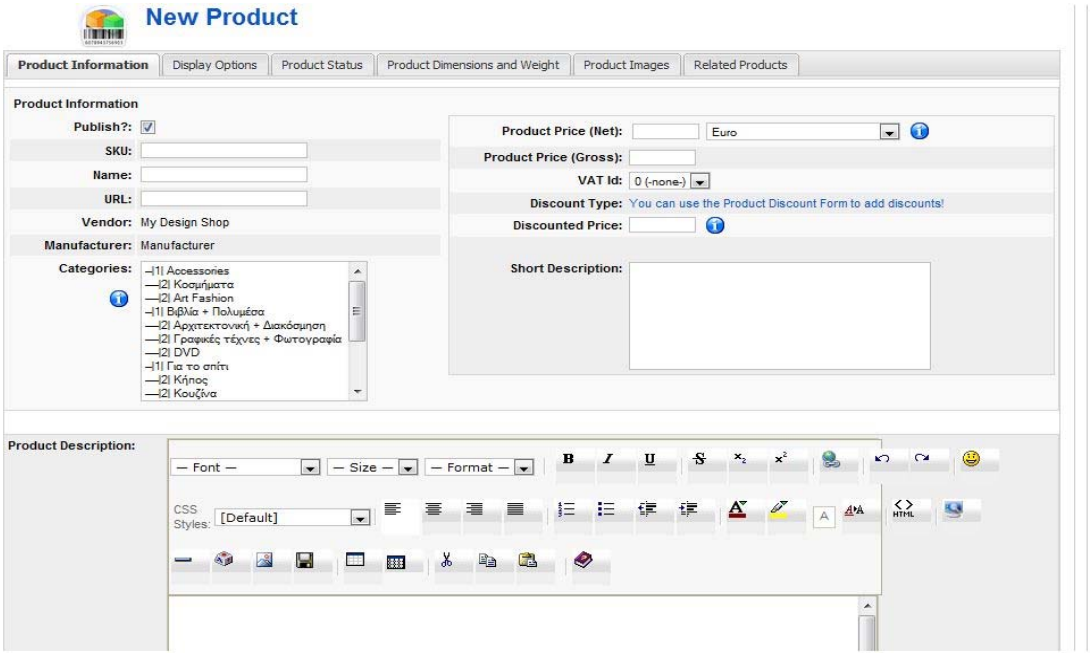
Για να εισάγουμε ένα νέο προϊόν, επιλέγουμε "Add product" από το αριστερό μενού στο οποίο βρισκόμαστε. Μας εμφανίζονται έξι καρτέλες, στις οποίες πρέπει να συμπληρώσουμε τα στοιχεία του νέου προϊόντος.

Αρχικά, έχουμε τις πληροφορίες του προϊόντος. Συμπληρώνουμε τα παρακάτω πεδία ανάλογα με τις απαιτήσεις του προϊόντος μας:

- **Publish?:** Αν θα είναι δημοσιευμένο το προϊόν ή όχι.
- **SKU:** Αποτελεί ακρώνυμο των λέξεων Stock Keeping Unit, είναι συνήθως αλφαριθμητικό των προϊόντων και η τιμή αυτή μας επιτρέπει να παρακολουθούμαι ευκολότερα τα προϊόντα για τους σκοπούς της απογραφής.
- **Name:** Το όνομα που θα χρησιμοποιηθεί για να εντοπιστεί το προϊόν μας.
- **Categories:** Υπάρχει μία selected list με όλες τις κατηγορίες προϊόντων που έχουμε καταχωρήσει παραπάνω, έτσι εδώ επιλέγουμε σε ποία κατηγορία/υποκατηγορία ανήκει το συγκεκριμένο προϊόν (μπορούμε να επιλέξουμε παραπάνω από μια κατηγορίες/υποκατηγορίες).
- **Product Price (Net):** Η τιμή για την προεπιλεγμένη ομάδα Shopper. Συμπληρώνουμε τον δεκαδικό αριθμό και επιλέγουμε το νόμισμα

προϊόντος από την αναπτυσσόμενη λίστα στα δεξιά. Στην δική μας περίπτωση το νόμισμα είναι euro.

- **Product Price (Gross):** Η τιμή συμπεριλαμβανομένων των φόρων (σύμφωνα με την επιλεγμένη τιμή ΦΠΑ) για την προεπιλεγμένη ομάδα Shopper.
- **VAT Id:** Το αναγνωριστικό του φορολογικού συντελεστή (ΦΠΑ) που θα εφαρμοστεί σε αυτό το προϊόν. Εδώ μπορούμε να επιλέξουμε ένα συγκεκριμένο φορολογικό συντελεστή για το προϊόν αυτό. Εάν δεν θέλουμε να φορολογήσουμε αυτό το προϊόν συμπληρώνουμε μηδέν.
- **Discounted Type/Price:** Στο πεδίο Discounted Type μπορούμε αρχικά να επιλέξουμε τον τύπο έκπτωσης που ισχύει για το συγκεκριμένο προϊόν και εάν δεν υπάρχει διαθέσιμος τύπος έκπτωσης να προσθέσουμε ένα νέο τύπο. Το πεδίο Discounted Price αντικαθιστά τον τύπο έκπτωσης του παραπάνω πεδίου και αυτόματα δημιουργεί έκπτωση εγγραφής χρησιμοποιώντας τη διαφορά μεταξύ των ακαθάριστων τιμών και τη μειωμένη τιμή.
- **Short/Product Description:** Δίνουμε μια σύντομη ή εκτεταμένη προγραφή για το συγκεκριμένο προϊόν, η οποία θα εμφανίζεται δίπλα στην εικόνα του προϊόντος.

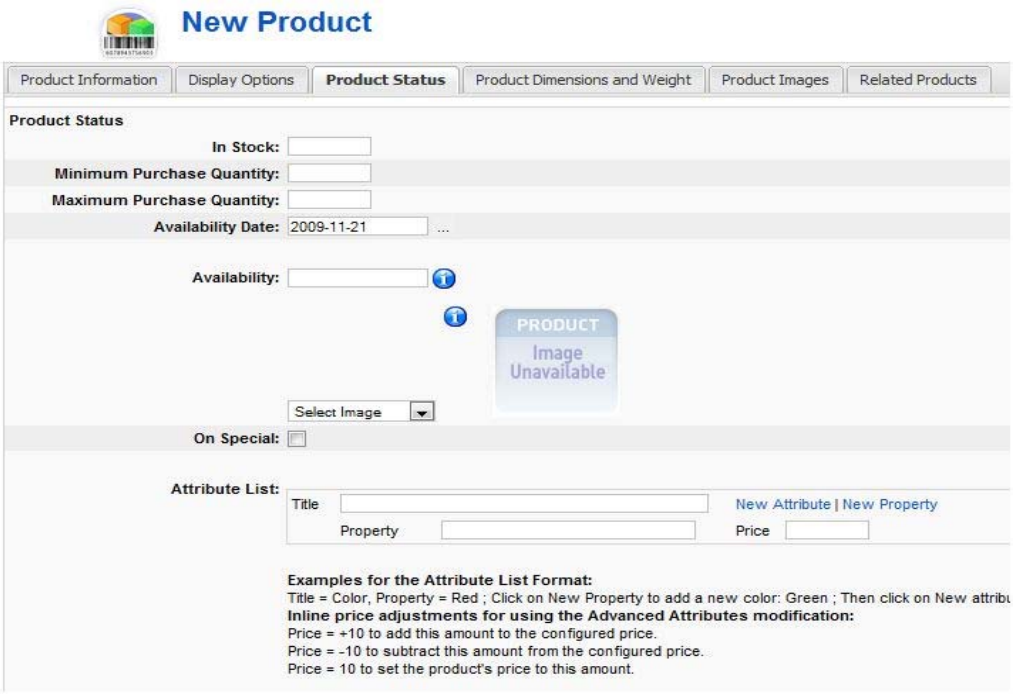


Εικόνα 44: Προσθήκη νέου προϊόντος. Πληροφορίες προϊόντος

Έπειτα, μπορούμε προορατικά να συμπληρώσουμε κάποιες ρυθμίσεις για την κατάσταση προϊόντος (Product Status).

- **Quantity in Stock:** Η τρέχουσα ποσότητα σε απόθεμα για το προϊόν αυτό. Χρησιμοποιείται για ενημέρωση του πελάτη και για να διευκολύνει την απογραφή του ηλεκτρονικού καταστήματος.
- **Minimum/Maxmimum Purchase Quantity:** Ο αριθμός αυτός καθορίζει την ελάχιστη/μεγιστή ποσότητα που μπορούν οι πελάτες να αγοράζουν από αυτό το προϊόν.

- **Availability Date:** Χρησιμοποιείτε για να περιγράψει την ημερομηνία κατά την οποία η τρέχουσα ποσότητα σε απόθεμα είναι διαθέσιμη για διανομή.
- **Availability Text/Image:** Χρησιμοποιείται για να εμφανίσει λεπτομέρειες σχετικά με την παράδοση του προϊόντος π.χ."σε 48 ώρες" ή "κατά την παραγγελία". Μπορούμε να γράψουμε στην text area την περιγραφή της παράδοσης ή να επιλέξουμε μια εικόνα από την αναπτυσσόμενη λίστα.
- **On Special?:** Χρησιμοποιείται για να δηλώσει εάν το προϊόν ανήκει σε κάποιο είδος προσφοράς. Εάν επιλεχθεί αυτή η επιλογή, το προϊόν θα εμφανιστεί στα "Προτεινόμενα Προϊόντα ".



Εικόνα 45: Προσθήκη νέου προϊόντος. Κατάσταση προϊόντος

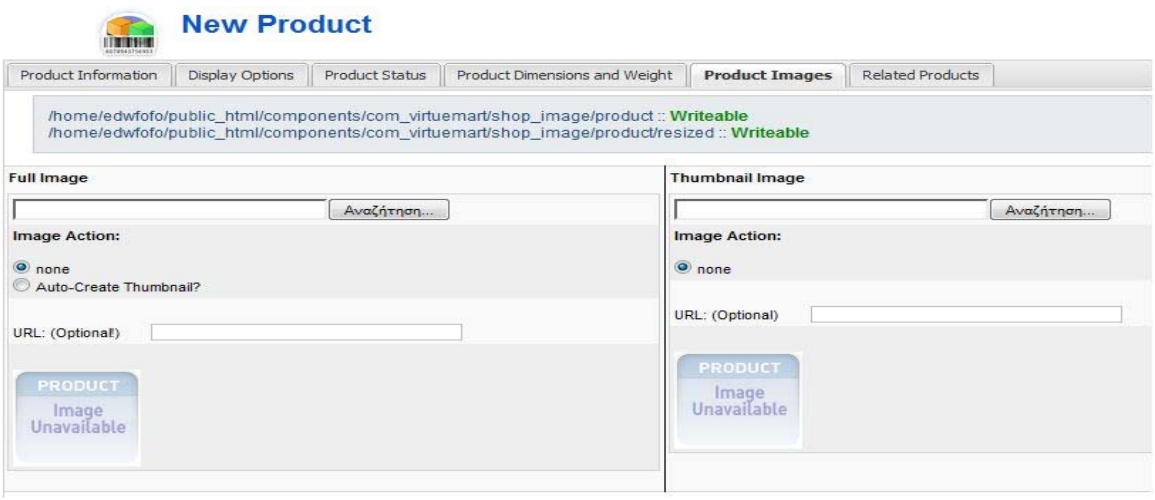
Στην επόμενη καρτέλα (Product Dimensions and Weight) συμπληρώνουμε, προαιρετικά, τις διαστάσεις και το βάρος του συγκεκριμένου προϊόντος. Έτσι οι πελάτες έχουν μια πιο ολοκληρωμένη εικόνα για το προϊόν που πρόκειται να αγοράσουν.

Στην καρτέλα Product Image ανεβάζουμε την βασική εικόνα του προϊόντος, έχουμε τις παρακάτω επιλογές:

- **Thumbnail image:** Μια μικρογραφία της εικόνας που μπορεί να εμφανιστεί μαζί με το προϊόν.
- **Full Image:** Μια μεγαλύτερη εικόνα που μπορεί να εμφανιστεί μαζί με το προϊόν.

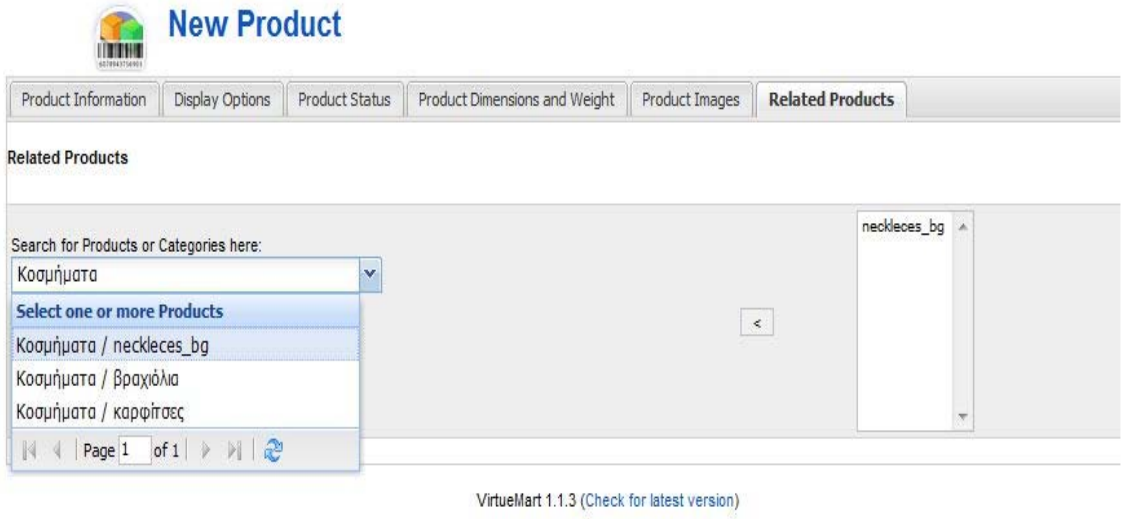
Εδώ θα πρέπει να προσέξουμε ότι εάν έχουμε ενεργοποιημένη την επιλογή "Dynamic Thumbnail Resizing", το thumbnail image εδώ δεν θα δημιουργηθεί αυτόματα από την πλήρης εικόνα.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



Εικόνα 46: Προσθήκη νέου προϊόντος. Καταχώρηση εικόνας του προϊόντος

Η τελευταία καρτέλα (Related Products) αναφέρεται στο αν θέλουμε να συσχετίσουμε το συγκεκριμένο προϊόντων με άλλα σχετικά προϊόντα του ηλεκτρονικού μας καταστήματος σχετικά προϊόντα μπορεί να αξεσουάρ ή άλλος τύπος προϊόντος ή κάποιο παρόμοιο προϊόν.



Εικόνα 47: Προσθήκη νέου προϊόντος. Καταχώρηση σχετικών προϊόντων με το συγκεκριμένο προϊόν

5.4 Μέθοδοι πληρωμής που υποστηρίζει το Component Virtuemart

Στο αριστερό μενού "Store" στο περιβάλλον διαχείρισης του VirtueMart component και επιλέγουμε "Store|Payment Method List " και βλέπουμε τη λίστα με τις μεθόδους πληρωμής που υποστηρίζει το Virtuemart component.

Η ποικιλία των μεθόδων πληρωμής που προσφέρει το component είναι αρκετά μεγάλη έτσι ώστε ο ιδιοκτήτης του καταστήματος να επιλέγει τις μεθόδους πληρωμής που εξυπηρετούν την επιχείρησή του με τον καλύτερο τρόπο.

Ανάμεσα στη λίστα των μεθόδων πληρωμής είναι:

- **2Checkout (2CO):** Είναι ο εξουσιοδοτημένος μεταπωλητής για χιλιάδες υλικά ή ψηφιακά προϊόντα και υπηρεσίες. Ιδρύθηκε το 2000 και έδρα το Columbus, Ohio. Η 2CO προσφέρει ετοιμοπαράδοτες λύσεις ηλεκτρονικού εμπορίου σε χιλιάδες επιχειρήσεις πελάτες σε όλο τον κόσμο.

  Η ιδιόκτητη τεχνολογία 2CO υποστηρίζει λειτουργίες back-office συμπεριλαμβανομένων των οικονομικών εκθέσεων, παρακολούθησης, πρόληψη της απάτης, παρακολούθησης θυγατρικών, εξυπηρέτησης πελατών και παρακολούθησης των πωλήσεων.

  Ο ιδιοκτήτης του ηλεκτρονικού καταστήματος μπορεί να εισάγει τα προϊόντα ή τις υπηρεσίες του στη βάση δεδομένων των προϊόντων της 2CO και να προσθέσει συνδέσεις που δημιουργούνται αυτόματα στο δικτυακό του τόπο. Όταν οι αγοραστές, κάνουν κλικ στους συνδέσμους για να πληρώσουν, η 2CO χειρίζεται την πώληση σε ένα ασφαλές περιβάλλον, δημιουργεί συμβάσεις με τον προμηθευτή (ιδιοκτήτη του ηλεκτρονικού καταστήματος) για να εκπληρώσει την πώληση και καταθέτει το ποσό της πληρωμής για την πώληση στο λογαριασμό του.

  Η 2Checkout δέχεται τους ακόλουθους τύπους πιστωτικών/χρεωστικών καρτών: Visa, Master Card, American Express, Discover, Via Bank Account.

- **eWay:** Προσφέρει μια κορυφαία λύση getaway πληρωμών για την επεξεργασία πληρωμών σε πραγματικό χρόνο.
- **iKobo:** Είναι μία online payment επεξεργασία που υποστηρίζει, επίσης και πιστωτικές κάρτες. Μπορεί επίσης να χρησιμοποιηθεί για την αποστολή χρημάτων πρόσωπο-με-πρόσωπο, με μια προπληρωμένη πιστωτική κάρτα που αποσταλεί στον παραλήπτη. Οι iKobo μεταφορές χρημάτων που χρηματοδοτούνται από μια ηλεκτρονική χρέωση του τραπεζικού λογαριασμού ή της πιστωτικής κάρτας του αποστολέα.[4]
- **iTransact:** Είναι ένα payment getaway και provider εμπορικών λογαριασμών. Οι υπηρεσίες του επιτρέπουν διαδικτυακές αλλά και παραδοσιακές συναλλαγές με τους εμπόρους, οι οποίοι δέχονται πληρωμές με πιστωτικές ή χρεωστικές κάρτες, κάρτες δώρων (gift cards) καθώς και ηλεκτρονικό έλεγχο (και/ή check conversion) με εγγύηση ελέγχου.[5]
- **Noche:** Είναι ένα online payment provider με βάση το Ηνωμένο Βασίλειο που εξειδικεύεται στην παροχή των επιχειρήσεων σε απευθείας σύνδεση με τις υπηρεσίες πληρωμών και στην άμεση μεταφορά χρημάτων μεταξύ ιδιωτών μέσω του Διαδικτύου.[6]
- **Paymate:** Είναι ένας online payments facilitator από την Αυστραλία που άρχισε να λειτουργεί τον Οκτώβριο του 2001. Η υπηρεσία είναι παρόμοια με το PayPal των ΗΠΑ αλλά οι πιστώσεις κεφαλαίων χρεώνονται απευθείας στον τραπεζικό λογαριασμό του δικαιούχου. Το Paymate δίνει τη δυνατότητα

[4] http://en.wikipedia.org/wiki/IKobo
[5] http://en.wikipedia.org/wiki/ITransact
[6] http://en.wikipedia.org/wiki/Noce

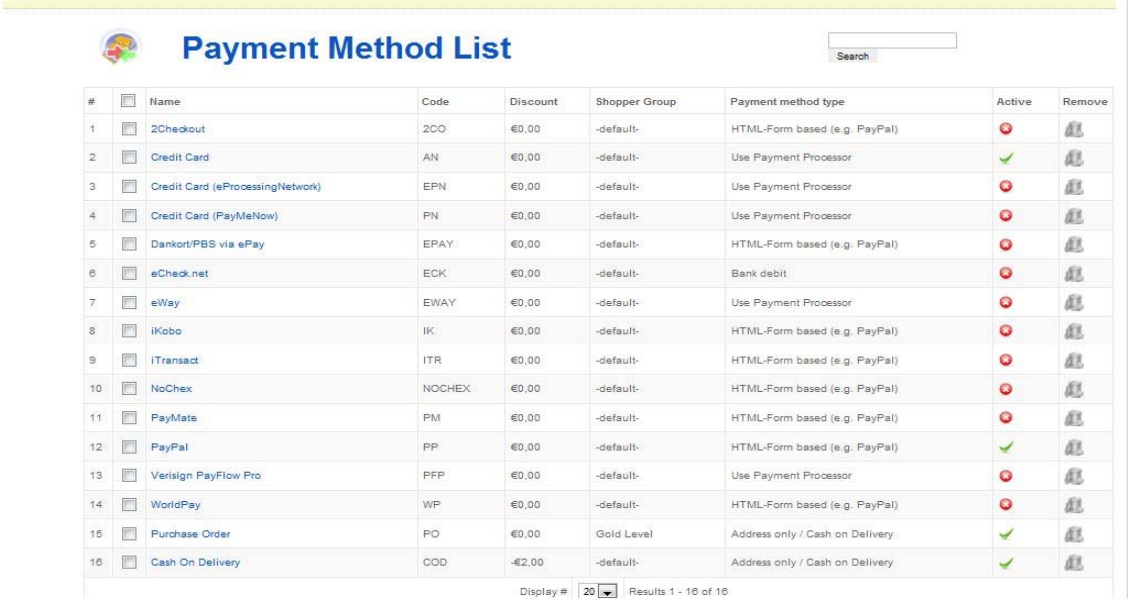
στους πωλητές της Αυστραλίας να δέχονται πληρωμές σε δολάρια Αυστραλίας, δολάρια, λίρες, ευρώ και NZD ενώ οι πωλητές στη Νέα Ζηλανδία μπορεί να δεχθούν πληρωμές σε NZD.

- **PayPal:** Είναι μία on-line υπηρεσία μεταφοράς χρημάτων. Χρησιμοποιείται παγκοσμίως για ασφαλείς συναλλαγές μέσω του Internet. Η εταιρία που το λειτουργεί είναι η ίδια που έχει και το eBay, γι' αυτό εξάλλου οι περισσότερες αγοραπωλησίες στο eBay εξοφλούνται μέσω PayPal.

  Λειτουργεί ακριβώς όπως ένας απλός τραπεζικός λογαριασμός. Οι χρήστες μπορούν να βάλουν σε αυτόν λεφτά από μία κάρτα, να δεχτούν λεφτά από κάποιον ή και να στείλουμε λεφτά σε κάποιον. Αν χρειάζεται να πληρώσουμε κάποιον αλλά δεν θέλουμε να χρησιμοποιήσουμε απευθείας τραπεζικό λογαριασμό, ζητάμε το e-mail που έχει στο PayPal και συμπληρώνουμε στην ειδική κρυπτογραφημένη σελίδα, τα στοιχεία της κάρτας μας και το ποσό. Είναι 100% ασφαλές γιατί ο μόνος που γνωρίζει τα στοιχεία της κάρτας του πελάτη είναι το ίδιο το PayPal. Ο παραλήπτης το μόνο που κάνει είναι να παραλαμβάνει τα χρήματα και όχι αριθμούς καρτών. Δέχεται συναλλαγές σε δολάρια, ευρώ και λίρες.[7]

- **WorldPay:** Είναι ένα τμήμα της Royal Bank of Scotland. Παρέχει υπηρεσίες πληρωμών over mail and order καθώς και διαδικτυακές συναλλαγές. Οι πελάτες είναι κυρίως πολυεθνικές, αλλά και πολλά κανάλια λιανικής πώλησης. Η RBS WorldPay ξεκίνησε ως πάροχος ηλεκτρονικής πληρωμής που ονομάστηκε Streamline το 1989, αλλά έχει επεκταθεί σε Mail Order/Telephone Order, "ανεπιτήρητες" πληρωμές και διακίνηση ασφαλών πληρωμών μέσω του Διαδικτύου, μέσω συγχωνεύσεων και εξαγορών πολλών άλλων εταιρειών.[8]
- **Cash On Delivery:** Ένα είδος της συναλλαγής στην οποία η πληρωμή για ένα προϊόν γίνεται κατά τη στιγμή της παράδοσης. Εάν ο αγοραστής δεν καταβάλει το αντίστοιχο ποσό που αναλογεί στο προϊόν τότε επιστρέφεται στον πωλητή.

[7] http://en.wikipedia.org/wiki/PayPal
[8] http://en.wikipedia.org/wiki/WorldPay



Payment Method List

Search

#		Name	Code	Discount	Shopper Group	Payment method type	Active	Remove
1		2Checkout	2CO	€0,00	-default-	HTML-Form based (e.g. PayPal)		
2		Credit Card	AN	€0,00	-default-	Use Payment Processor		
3		Credit Card (eProcessingNetwork)	EPN	€0,00	-default-	Use Payment Processor		
4		Credit Card (PayMeNow)	PN	€0,00	-default-	Use Payment Processor		
5		Dankort/PBS via ePay	EPAY	€0,00	-default-	HTML-Form based (e.g. PayPal)		
6		eCheck.net	ECK	€0,00	-default-	Bank debit		
7		eWay	EWAY	€0,00	-default-	Use Payment Processor		
8		iKobo	IK	€0,00	-default-	HTML-Form based (e.g. PayPal)		
9		iTransact	ITR	€0,00	-default-	HTML-Form based (e.g. PayPal)		
10		NoChex	NOCHEX	€0,00	-default-	HTML-Form based (e.g. PayPal)		
11		PayMate	PM	€0,00	-default-	HTML-Form based (e.g. PayPal)		
12		PayPal	PP	€0,00	-default-	HTML-Form based (e.g. PayPal)		
13		Verisign PayFlow Pro	PFP	€0,00	-default-	Use Payment Processor		
14		WorldPay	WP	€0,00	-default-	HTML-Form based (e.g. PayPal)		
15		Purchase Order	PO	€0,00	Gold Level	Address only / Cash on Delivery		
16		Cash On Delivery	COD	-€2,00	-default-	Address only / Cash on Delivery		

Display # 20 Results 1 - 16 of 16

Εικόνα 48: Payment Method List, VirtueMart.

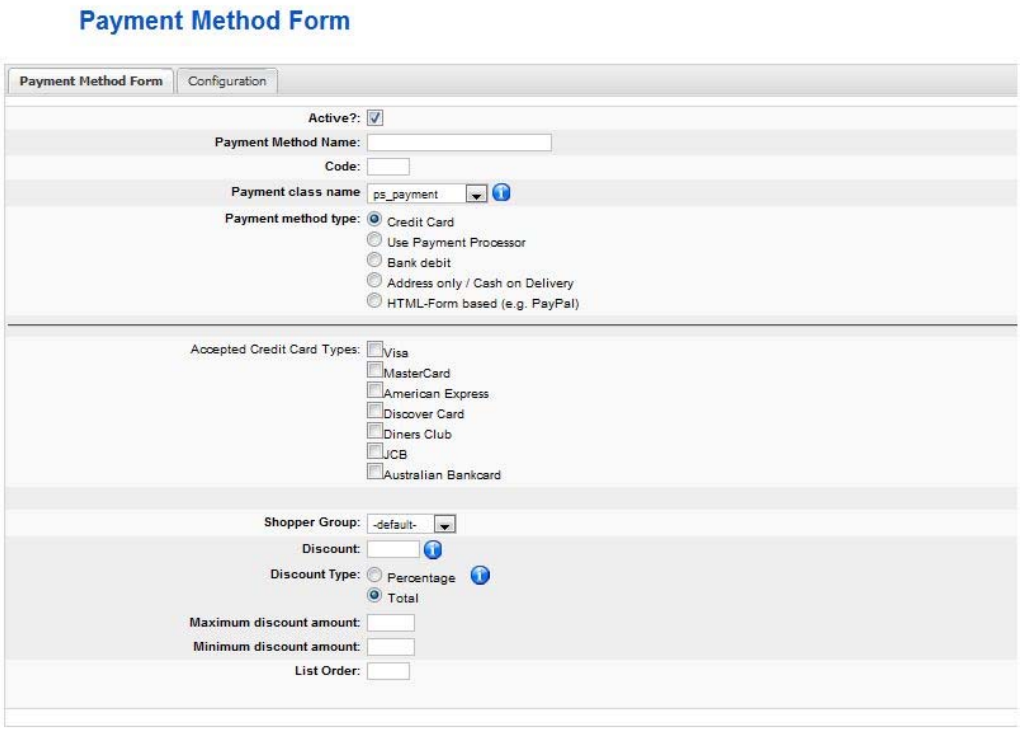
Το Virtuemart Component μας δίνει δύο επιλογές σε αυτό το σημείο. Συμφωνά με την πρώτη, επιλέγοντας κάποια μέθοδο πληρωμής από αυτές αναφέρθηκαν θα πρέπει να συνδεθούμε ατομικά με τους payment processors που αντιστοιχούν στις μεθόδους πληρωμής που επιλέξαμε. Το Virtuemart component δεν παρέχει αυτή την λειτουργία, οπότε είναι καθαρή ενέργεια του διαχειριστή.

Η δεύτερη επιλογή που έχουμε είναι να δημιουργηθεί μια νέα μέθοδο πληρωμής. Για την καταχώρηση της νέας μεθόδου πληρωμής, ο διαχειριστής είναι υπεύθυνος για την εγκατάσταση και την ενεργοποίηση του απαιτούμενου plugin, έτσι ώστε η νέα μέθοδος πληρωμής να λειτουργήσει σωστά και με ασφαλής τρόπο.

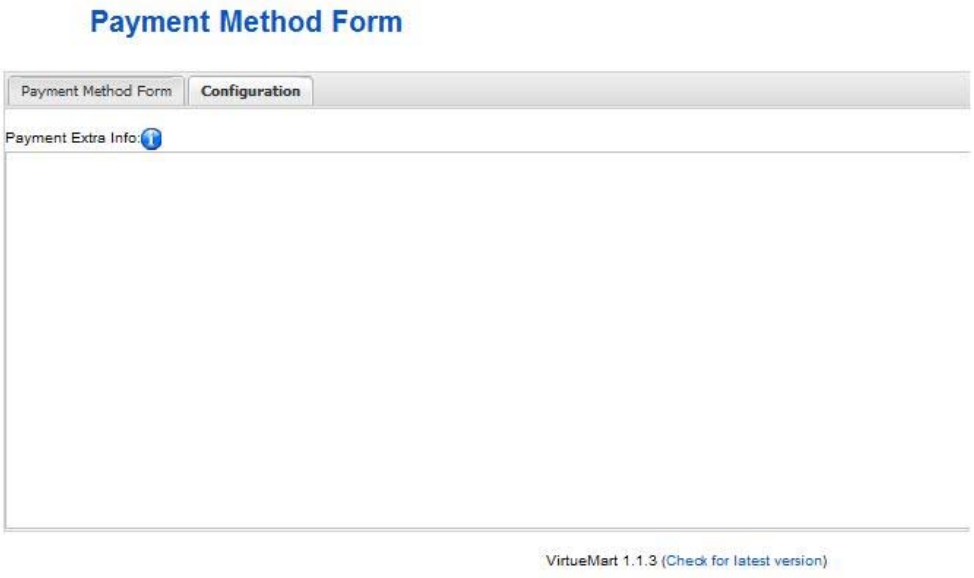
Πάνω δεξιά από την λίστα μεθόδου πληρωμών, υπάρχει ένα κουμπί "Νέο". Με αυτό κάνουμε προσθήκη νέας μεθόδου πληρωμής. Οι επιλογές διαμόρφωσης για κάθε μέθοδο πληρωμής είναι διαφορετικές-ανάλογα με το τι απαιτείται από τον παροχή υπηρεσιών των πληρωμών. Συνήθως, ο φορέας παροχής υπηρεσιών πληρωμών δίνει κάποιο είδος κωδικού ή το όνομα χρήστη που πρέπει να εγγραφεί στο Payment Method Editor.

Ο Payment Method Editor αποτελείται από 2 καρτέλες. Στην πρώτη συμπληρώνονται τα στοιχεία που μας δίνει ο φορέας παροχής υπηρεσιών πληρωμών και στην επόμενη καρτέλα, "Διαμόρφωση", ποικίλλει ανάλογα με τον πάροχο υπηρεσιών πληρωμών.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



Εικόνα 49: Payment Method Form, VirtueMart



Εικόνα 50: Configuration, Extra Payment Info, VirtueMart

Στο κεφάλαιο 6 (υποενότητα 6.2.1) γίνεται δημιουργία μιας νέας μεθόδου πληρωμής, σε συνεργασία με την AlphaBank και παραθέτονται σε αυτή την υποενότητα όλα τα στοιχεία που πρέπει να συμπληρωθούν για την ενεργοποίηση της μεθόδου πληρωμής.

Δίνουμε τη δυνατότητα στο ηλεκτρονικό κατάστημα να υποστηρίζει τρείς τρόπους πληρωμής. Μέσω λογαριασμού paypal, μέσω πιστωτικής κάρτας visa/mastercard και με αντικαταβολή.

Αφού ενεργοποιήσουμε και την νέα μέθοδο πληρωμής επιλέγουμε από τη λίστα τις παρακάτω επιλογές:

- DeltaPay
- PayPal
- Cash On Delivery

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Κεφάλαιο 6 Διεξαγωγή ηλεκτρονικών συναλλαγών

6.1 Ηλεκτρονικές συναλλαγές μέσω τραπεζών

Σύμφωνα με τα τελευταία δεδομένα της έρευνας που έγινε για την παρούσα πτυχιακή εργασία, ικανοποιητικός αριθμός τραπεζών που βρίσκονται στην Ελλάδα παρέχουν υπηρεσίες για τη διεξαγωγή διαδικτυακών συναλλαγών προς τους ιδιοκτήτες ηλεκτρονικών καταστημάτων. Οι πληροφορίες που παρουσιάζονται παρακάτω αναφέρονται στις υπηρεσίες που προσφέρουν η Τράπεζα Πειραιώς και η AlphaBank.

Οι υπηρεσίες που προσφέρουν, απευθύνονται σε όλες τις επιχειρήσεις που διαθέτουν web sites και ηλεκτρονικά καταστήματα. Τα οποία πωλούν προϊόντα-υπηρεσίες μέσω internet ή ενδιαφέρονται να δραστηριοποιηθούν στο χώρο του ηλεκτρονικού εμπορίου. Οι πληρωμές διεκπεραιώνονται αυτόματα μέσω του paycenter της τράπεζας και το ποσό κατατίθεται στον λογαριασμό της επιχείρησης που υπάρχει στην τράπεζα αυτή.

Ανάλογα με την ετοιμότητα του ηλεκτρονικού καταστήματος η Τράπεζα Πειραιώς διαθέτει δύο επιλογές επικοινωνίας με το paycenter της τράπεζας για την ολοκλήρωση της πληρωμής του πελάτη, ενώ η AlphaBank διαθέτει μία. Κατά την πρώτη επιλογή, που υποστηρίζουν και οι δύο τράπεζες, γίνεται redirection του πελάτη στο paycenter και κατά την δεύτερη επιλογή, που υποστηρίζει η Τράπεζα Πειραιώς, υπάρχει web service επικοινωνία του καταστήματος με το paycenter της τράπεζας.

6.1.1 Redirection του πελάτη στο paycenter της τράπεζας

Όταν ένας πελάτης έχει ολοκληρώσει την επιλογή των προϊόντων ή υπηρεσιών που θέλει να αγοράσει μέσω του ηλεκτρονικού καταστήματος και επιλέξει να πληρώσει με χρήση κάρτας στην οθόνη του πελάτη παρουσιάζεται ένα νέο «παράθυρο» (pop - up window), δηλαδή μεταφέρεται σε ειδική ασφαλή ιστοσελίδα της τράπεζας (redirection), όπου εισάγει τα στοιχεία της κάρτας που θέλει να χρεώσει.

Το ηλεκτρονικό κατάστημα, για λόγους ασφαλείας, δεν έχει πρόσβαση στα στοιχεία της κάρτας του πελάτη. Επισημαίνουμε ότι στην ιστοσελίδα εισαγωγής των στοιχείων της κάρτας, εκτός από το λογότυπο της τράπεζας θα εμφανίζεται και το λογότυπο του ηλεκτρονικού καταστήματος.

Μόλις ο πελάτης ολοκληρώσει την καταχώριση των στοιχείων της κάρτας του, η τράπεζα επιχειρεί να χρεώσει την κάρτα με το ποσό που το ηλεκτρονικό κατάστημα ζήτησε να εισπραχθεί. Στη συνέχεια, ανάλογα με το αν η συναλλαγή γίνει αποδεκτή ή όχι, επιστρέφεται θετική ή αρνητική απάντηση στον πελάτη.

6.1.2 Ασφάλεια που παρέχουν οι τράπεζες μέσω redirection

Το υψηλό επίπεδο ασφάλειας των υπηρεσιών ηλεκτρονικών συναλλαγών που προσφέρουν η Τράπεζα Πειραιώς και η AlphaBank εξασφαλίζεται από τα παρακάτω:

- Οι πληροφορίες σχετικά με την κάρτα (αριθμός κάρτας, CVV2, ημερομηνία λήξεως) μεταδίδονται/μεταφέρονται μέσω Διαδικτύου σε κρυπτογραφημένη μορφή (128-bit encryption) και δεν είναι προσβάσιμες από το ηλεκτρονικό μας κατάστημα.
- Τα συστήματα και οι διαδικασίες που χρησιμοποιούνται από τις τράπεζες αποκλείουν σε τρίτους την πρόσβαση στα δεδομένα και τα πληροφοριακά συστήματά της.
- Οι ιστοσελίδες των τραπεζών στις οποίες εισάγει τα στοιχεία της κάρτας του ο πελάτης, φέρει ψηφιακό πιστοποιητικό για να μπορεί ο καθένας να ελέγξει τη γνησιότητάς της, δηλαδή να διαπιστώσει ότι ανήκει πραγματικά στην Υπηρεσία Alpha e-Pay (πρώην delta pay) της Alpha Bank.
- Η διαχείριση των υπηρεσιών ηλεκτρονικού εμπορίου γίνεται από εξουσιοδοτημένα άτομα της επιχειρήσεως, στους οποίους παραδίδονται κωδικοί προσβάσεως (username, password).
- Σε περίπτωση που η εκδότρια τράπεζα υποστηρίζει τη χρήση μυστικού κωδικού για την εκτέλεση on-line πληρωμών με κάρτα και ο κάτοχος της κάρτας έχει παραλάβει τέτοιο κωδικό, οι υπηρεσίες ηλεκτρονικού εμπορίου (Alpha e-Pay) ζητάν αυτόματα από τον πελάτη να πληκτρολογήσει τον μυστικό του κωδικό.
- Ολοκληρώνοντας, η υπηρεσία Alpha e-Pay ακολουθεί τις βέλτιστες διεθνείς πρακτικές στον τομέα των πληρωμών για ηλεκτρονικό εμπόριο και επίσης είναι πλήρως συμβατή με τις προδιαγραφές VbV (Verified by Visa) για ασφαλείς on-line πληρωμές με κάρτα.

Η λύση redirection για την διεκπεραίωση της ηλεκτρονικής πληρωμής συνιστάται σε επιχειρήσεις που δεν επιθυμούν να επενδύσουν σε περαιτέρω ασφάλεια της υποδομής τους και προτιμούν να αξιοποιήσουν απ' ευθείας το κύρος ενός τραπεζικού site.

6.1.3 Web service επικοινωνία με το paycenter της τράπεζας

Με την επιλογή αυτής της μεθόδου που υποστηρίζει η Τράπεζα Πειραιώς ο πελάτης του ηλεκτρονικού καταστήματος, με το πέρας της παραγγελίας του, καθοδηγείται για την εισαγωγή των στοιχείων της κάρτας του από τις σελίδες του ίδιου του ηλεκτρονικού καταστήματος.

Ο web server του ηλεκτρονικού καταστήματος επικοινωνεί με web service (server-to-server επικοινωνία) με το paycenter της τράπεζας για την διεκπεραίωση της πληρωμής του πελάτη. Τα στοιχεία πληρωμής μεταβιβάζονται κρυπτογραφημένα στο paycenter. Απαραίτητη προϋπόθεση είναι η εφαρμογή του ηλεκτρονικού καταστήματος να έχει SSL 128 bit κρυπτογράφηση.

Η χρήση της μεθόδου XML messaging συνιστάται σε web sites και ηλεκτρονικά καταστήματα με ανεπτυγμένη υποδομή ασφάλειας και διαχείρισης της πελατείας τους.

Η τεχνική XML messaging βασίζεται στο XML πρωτόκολλο και στην τεχνική XML-RPC. Το XML πρωτόκολλο (XMLP) προβλέπει απλά πρωτόκολλα που μπορούν να αναπτυχθούν εύκολα και προγραμματίζονται μέσω scripting languages, XML εργαλεία, διαδραστικά Web εργαλεία ανάπτυξης κ.τ.λ.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Ο στόχος του πρωτοκόλλου είναι ένα πολυεπίπεδο σύστημα που θα ικανοποιεί άμεσα τις ανάγκες των εφαρμογών με απλές διεπαφές (π.χ. getStockQuote, validateCreditCard) και το οποίο μπορεί να επεκταθεί σταδιακά να παρέχει την ασφάλεια, την επεκτασιμότητα και την ευρωστία που απαιτούνται για τις πιο περίπλοκες εφαρμογές διασυνδέσεις. [9]

Συγκεκριμένα, το XML Protocol Working Group έχει σχεδιάσει τα ακόλουθα components:

- Ένα "φάκελο" για την ενσωμάτωση των δεδομένων XML, έτσι ώστε να εξασφαλιστεί η μεταφορά των δεδομένων με ένα διαλειτουργικό τρόπο που επιτρέπει τη επεκτασιμότητα.
- Μια σύμβαση για το περιεχόμενο του φακέλου, όταν χρησιμοποιούνται για RPC (Remote Procedure Call) εφαρμογές. Οι πτυχές του πρωτοκόλλου αυτού θα πρέπει να συντονίζονται στενά με το IETF (Internet Engineering Task Force) και προσπαθήσουν να επηρεάσουν κάθε ενέργεια που επιτελούν.
- Ένα μηχανισμό για serializing δεδομένων που αντιπροσωπεύουν ένα μη συντακτικό μοντέλο δεδομένων, όπως γραφήματα αντικειμένων (object graphs) και κατευθυνόμενα γραφήματα με ετικέτες (directed labeled graphs), με βάση τους τύπους δεδομένων της XML Schema.
- Ένα μηχανισμό για τη χρήση HTTP μεταφορών στο πλαίσιο του πρωτοκόλλου XML. Χωρίς αυτό να σημαίνει ότι ο HTTP είναι ο μόνος μηχανισμός μεταφοράς που μπορεί να χρησιμοποιηθεί για την ανάπτυξη των τεχνολογιών, ούτε ότι η στήριξη για τις μεταφορές HTTP είναι υποχρεωτική. Αυτό το component καλύπτει απλώς το γεγονός ότι οι HTTP μεταφορές αναμένεται να χρησιμοποιηθούν ευρέως και έτσι πρέπει να αντιμετωπιστεί από το Working Group. Θα υπάρξει συντονισμός με το Internet Engineering Task Force (IETF).

6.1.2 Εργαλεία διαχείρισης που προσφέρουν οι τράπεζες στους ιδιοκτήτες ηλεκτρονικών καταστημάτων για on-line συναλλαγές

Οι δύο τράπεζες που εξετάζουμε παρέχουν δωρεάν στους ιδιοκτήτες ηλεκτρονικών καταστημάτων εφαρμογές/διαχειριστικά εργαλεία για να διαχειρίζονται on-line κάθε είσπραξη, να αναλογίζονται (cancel, refund) συναλλαγές με ένα απλό τρόπο και να συμφωνούν τις παραγγελίες με τις εισπράξεις τους (reconciliation). Το διαχειριστικό περιβάλλον της Τράπεζας Πειραιώς ονομάζεται paycenter AdminTool και της AlphaBank ονομάζεται e-PAY Merchant Tools.

Στις ασφαλής internet σελίδες των διαχειριστικών εργαλείων των τραπεζών, αρμόδια στελέχη της επιχείρησης (π.χ. λογιστήριο) έχουν ελεγχόμενη πρόσβαση (username/password) ώστε να παρακολουθούν αναλυτικά τις εισπράξεις-συναλλαγές από τους πελάτες σας και να διαχειρίζονται το status κάθε συναλλαγής:

- Αναμονή (pending transactions).

---

[9] http://www.service-architecture.com/

- Έγκριση (approved transactions).
- Ολοκλήρωση (accepted transactions).
- Ακύρωση (cancel transactions).
- Επιστροφή (refund).
- Απόρριψη (void transactions).
- Πακέτο συναλλαγών (batches).
- Παραγωγή στατιστικών στοιχείων.
- Αναλυτικό reporting ανά υπηρεσία είσπραξης, με πολλαπλά κριτήρια αναζήτησης.
- Αποστολή ομάδων συναλλαγών για εκκαθάριση.
- Download των εκτελεσμένων συναλλαγών.

6.2 Payment modules για το VirtueMart

Από τα τμήματα πιστοποιημένων εταιριών τα οποία ασχολούνται με την ανάπτυξη επεκτάσεων ανοικτού κώδικα (Open Source) για δημοφιλείς web εφαρμογές μπορούμε να βρούμε payment plugins για τα πιο γνωστά components των δημοφιλέστερων CMS. Τα payment plugins ουσιαστικά συνδέουν το component πάνω στο οποίο βασίζεται το ηλεκτρονικό μας κατάστημα με τον τύπο πληρωμής της κάθε τράπεζας μέσω των υπηρεσιών που προσφέρει η τράπεζα. Τα συγκεκριμένα payment plugins είναι διαφορετικά για κάθε τράπεζα και για την απόκτηση τους χρειάζεται η καταβολή κάποιου ποσού.

Στη συνέχεια αγοράζουμε το payment module από κάποια πιστοποιημένη εταιρεία. Εγκαθιστούμε το payment module και επικοινωνούμε με την τράπεζα, όπου μας θα μας ζητηθεί να συμπληρώσουμε τις παρακάτω σελίδες: Payment Page, Success Page, Failure Page, Cancel Page σύμφωνα με το δικό μας κατάστημα.

Στην συνέχεια η τράπεζα θα μας αποστείλει τις ρυθμίσεις για το test account, έτσι ώστε να αρχίσουμε να πραγματοποιούμε τις πρώτες δοκιμαστικές συναλλαγές και τους δοκιμαστικούς κωδικούς της πιστωτικής κάρτας. Η διάρκεια αυτών των ρυθμίσεων είναι μερικών ημερών ώστε να υπάρχει αρκετός χρόνος για την πραγματοποίηση των δοκιμών.

Στο payment module που έχουμε αγοράσει υπάρχει η σχετική ρύθμιση για την δοκιμαστική περίοδο, ώστε η συναλλαγή μας να μην ξεπερνά τα 0,5 ευρώ και να μην χρεώνεται μεγάλα ποσά η κάρτα μας.

Εφόσον οι δοκιμαστικές συναλλαγές έχουν ολοκληρωθεί με επιτυχία, επικοινωνούμε με την τράπεζα για να μας αποστείλουν τους κωδικούς του production account και το ηλεκτρονικό κατάστημα είναι έτοιμο να λειτουργήσει.

6.2.1 Εγκατάσταση του payment module

Η εγκατάσταση του payment module για το VirtueMart του Joomla είναι απλή και γίνεται όπως η εγκατάσταση κάθε άλλου module. Αφού γίνει η εγκατάσταση θα πρέπει να προσθέσουμε μια τη νέα μέθοδο πληρωμής που δημιουργήθηκε σε συνεργασία με την τράπεζα που συνεργαζόμαστε.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Από το διαχειριστικό κομμάτι του VirtueMart, πηγαίνουμε στο "Store|Add Payment Method" και συμπληρώνουμε τα παρακάτω στοιχεία (τα στοιχεία αυτά αναφέρονται στην υπηρεσία e-ADeltaPay της AlphaBank):

- Active = Ναι
- Payment Method Name = DeltaPay
- Code = Delta
- Payment Class Name = ps_deltapay
- Payment method type = PayPal (or related)

Στη συνέχεια αποθηκεύουμε και ανοίγουμε την payment μέθοδο που μόλις δημιουργήσαμε και επιλέγουμε το Configuration Tab. Εισάγουμε ή επιλέγουμε τις απαραίτητες ρυθμίσεις, αντιγράφουμε στο text area 'Payment Extra Info' το παρακάτω:

Κώδικας

```
<? php require_once( PAGEPATH.
'checkout.deltapayment_cc_form.php';?>
```

Αποθηκεύουμε και η καινούρια μέθοδος πληρωμής ισχύει.

Κεφάλαιο 7 Επικίνδυνα σημεία στην διεξαγωγή του ηλεκτρονικού εμπορίου

7.1 DoS attack ή DDoS attack

Μια επίθεση DoS (denial-of-service attack) ή επίθεση DDoS (distributed-denial-of-service attack) είναι επιθέσεις που ως στόχο έχουν να αποτρέψουν τη χρήση ενός συστήματος από όλους τους υπόλοιπους χρήστες (δηλαδή τους νόμιμους χρήστες του). Αν και τα μέσα για τη διεξαγωγή της επίθεσης, τα κίνητρα και οι στόχοι μιας επίθεσης DoS μπορεί να ποικίλλουν, αποτελούνται συνήθως από τις συντονισμένες προσπάθειες ενός ατόμου ή ατόμων για να εμποδίσουν μια ιστοσελίδα ή μία υπηρεσία στο διαδίκτυο από την λειτουργία της, προσωρινά ή επ 'αόριστον.

Οι δράστες των επιθέσεων DoS συνήθως στοχεύουν ιστοσελίδες ή υπηρεσίες που φιλοξενούνται σε high-profile web servers, όπως τράπεζες, πύλες πληρωμής με πιστωτική κάρτα ακόμη και root nameservers. Κατά τις επιθέσεις DoS δεν γίνονται προσπάθειες παραβίασης ή κλοπής στοιχείων. Είναι όμως δυνατός ο συνδυασμός τους με άλλες επιθέσεις που γίνονται παράλληλα με σκοπό να "παραπλανήσουν" τα συστήματα ανίχνευσης (Intrusion Detection Systems) και τους διαχειριστές από την πραγματική απειλή.

Μια κοινή μέθοδος επίθεσης συνεπάγεται με τον κορεσμό του στόχου με εξωτερικές αιτήσεις επικοινωνίας, έτσι ώστε να μην μπορεί να ανταποκριθεί στις απαιτήσεις της νόμιμης κυκλοφορίας ή ανταποκρίνεται τόσο αργά ώστε να καταστεί αποδοτικά μη διαθέσιμο.

Σε γενικές γραμμές, οι επιθέσεις DoS υλοποιούνται είτε αναγκάζοντας τους στοχευόμενους υπολογιστές να κάνουν επαναφορά ή να καταναλώσουν τους πόρους τους, έτσι ώστε να μην μπορούν πλέον να παρέχουν τις υπηρεσίες που προορίζονται μεταξύ των χρηστών και των στοχευόμενων υπολογιστών με αποτέλεσμα η επικοινωνία μεταξύ τους να μην είναι πλέον ικανοποιητική.

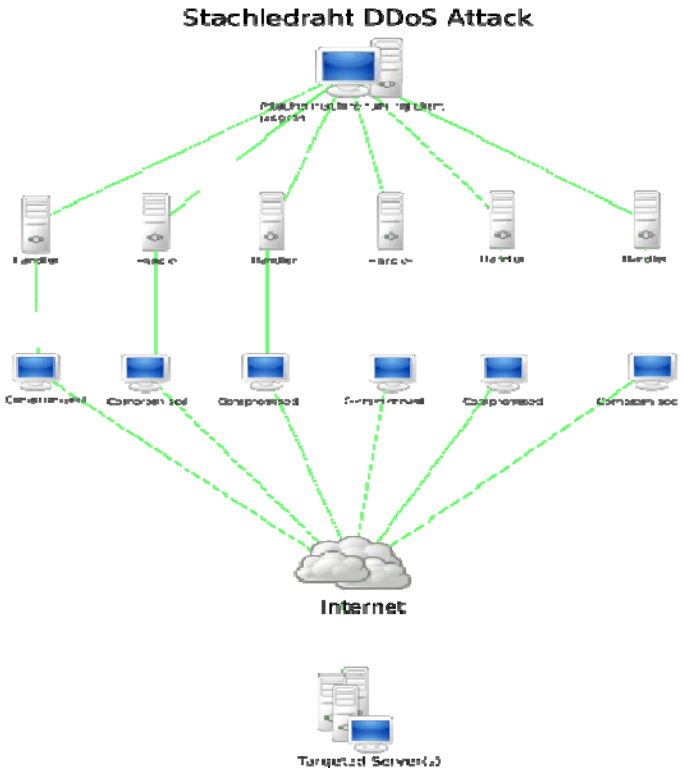
Επιθέσεις DoS μπορούν να απευθύνονται σε οποιαδήποτε συσκευή δικτύου, συμπεριλαμβανομένων των επιθέσεων σε συσκευές δρομολόγησης και διαδίκτυο, ηλεκτρονικό ταχυδρομείο ή Domain Name System διακομιστές.

Μια επίθεση DoS μπορεί να γίνει με διάφορους τρόπους. Οι πέντε βασικοί άξονες της επίθεσης είναι:

- Κατανάλωση των υπολογιστικών πόρων, όπως το εύρος ζώνης, χώρο στο δίσκο ή χρόνου επεξεργασίας
- Η παρεμβολή των πληροφοριών ρύθμισης, όπως πληροφορίες δρομολόγησης.
- Η παρεμβολή των πληροφοριών για την κατάσταση, όπως η αυτόκλητη επαναφορά της συνεδρίας TCP.
- Διατάραξη των φυσικών στοιχείων του δικτύου.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

- Παρεμπόδιση των μέσων επικοινωνίας μεταξύ των χρηστών και του θύματος, έτσι ώστε να μην μπορούν πλέον να επικοινωνούν επαρκώς.[10]



Εικόνα 51: Σχηματική απεικόνισή DDos Attack

7.2 SQL injections

Η SQL injection είναι μια επίθεση κατά την οποία ένα κακόβουλο κομμάτι κώδικα εισάγεται μέσα σε strings τα οποία θα περάσουν αργότερα στον SQL Server για μεταγλώτιση και εκτέλεση. Κάθε διαδικασία που κατασκευάζει SQL statements θα πρέπει να αναθεωρηθεί για τα αδύναμα σημεία της injection γιατί ο SQL Server θα εκτελέσει όλα τα συντακτικά έγκυρα ερωτήματα που λαμβάνει. Ακόμη και παραμετροποιήσιμα δεδομένα μπορεί να αλλοιωθούν από ένα εξειδικευμένο εισβολέα.

Η πρωταρχική μορφή της SQL injection αποτελείται από άμεση εισαγωγή κώδικα σε μεταβλητές εισόδου που συνδέονται αλυσιδωτά με SQL εντολές και εκτελούνται. Μια λιγότερο άμεση επίθεση εισάγει κακόβουλο κώδικα σε strings που προορίζονται για αποθήκευση σε έναν πίνακα ή ως μετά-δεδομένα. Όταν τα αποθηκευμένα strings συνδέονται στη συνέχεια σε μια δυναμική εντολή SQL, ο κακόβουλος κώδικας εκτελείται.

---

[10] http://en.wikipedia.org/wiki/Denial-of-service_attack#Methods_of_attack

Η διαδικασία μίας injection λειτουργεί με το να ολοκληρώσει πρόωρα μια σειρά κειμένων strings και να επισυνάψει μια νέα εντολή. Επειδή η παρενθετική εντολή μπορεί να έχει πρόσθετα strings επισυνημμένα σε αυτήν προτού να εκτελεσθεί, ο επιτιθέμενος ολοκληρώνει το injected string με ένα σημάδι σχολίου "--". Το επόμενο κείμενο αγνοείται στο χρόνο εκτέλεσης.

Το ακόλουθο script παρουσιάζει μια απλή SQL injection. Το script "χτίζει" ένα SQL ερώτημα με τη σύνδεση κωδικοποιημένων strings μαζί με ένα string που εισάγεται από το χρήστη:

Κώδικας

```
var Shipcity;
ShipCity = Request.form ("ShipCity");
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity
+ "'";
```

Ο χρήστης έχει ζητηθεί να πληκτρολογήσει το όνομα μιας πόλης. Αν πληκτρολογήσει "Redmond" το ερώτημα που συναθροίζεται στο script μοιάζει με το ακόλουθο κείμενο:

Κώδικας

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond'
```

Ωστόσο, ας υποθέσουμε ότι ο χρήστης εισάγει τα ακόλουθα:

Κώδικας

```
Redmond'; drop table OrdersTable--
```

Στην περίπτωση αυτή ,το ακόλουθο ερώτημα συναθροίζεται στο παρακάτω script:

Κώδικας

```
SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond'; drop table
OrdersTable--'
```

Το ερωτηματικό ";" υποδηλώνει το τέλος ενός ερωτήματος και την έναρξη ενός άλλου, η διπλή παύλα "--" σημαίνει ότι το υπόλοιπο της τρέχουσας γραμμής είναι σχόλιο και θα πρέπει να αγνοηθεί. Εάν ο τροποποιημένος κώδικας είναι συντακτικά σωστός, θα πρέπει να εκτελεστεί από το διακομιστή. Όταν ο SQL Server επεξεργαστεί αυτή τη δήλωση, θα επιλέξει πρώτα όλα τα αρχεία από τον πίνακα OrdersTable όπου το πεδίο ShipCity είναι Redmond. Στη συνέχεια, ο SQL Server θα φέρει όλο τον πίνακα OrdersTable.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

7.3 Cross-site Scripting (XSS)

Cross site scripting επίθεση (γνωστή και ως XSS) παρουσιάζεται όταν μια web εφαρμογή συγκεντρώνει κακόβουλα δεδομένα από ένα χρήστη. Αυτό που εκμεταλλεύεται μια τέτοιου είδους επίθεση είναι η εμπιστοσύνη που δείχνει ο χρήστης στους ιστοτόπους και στα url που περιέχουν το όνομα του ιστότοπου που έχουν επισκεφτεί.

Τα δεδομένα συγκεντρώνονται συνήθως με τη μορφή μιας υπερ-σύνδεσης που περιέχει κακόβουλο περιεχόμενο μέσα σε αυτήν. Ο χρήστης πιθανότατα θα κάνει κλικ σε αυτό το σύνδεσμο από μια άλλη ιστοσελίδα, από ένα άμεσο μήνυμα ή απλώς από ανάγνωση μηνύματος ηλεκτρονικού ταχυδρομείου. Συνήθως ο εισβολέας θα κωδικοποιήσει το κακόβουλο τμήμα του συνδέσμου στην ιστοσελίδα με HEX (encoding ή άλλες μεθόδους), έτσι ώστε το αίτημα να γίνει λιγότερο καχύποπτο προς τον χρήστη όταν κάνει κλικ επάνω μια σελίδα εξόδου η οποία περιλαμβάνει τα επιβλαβή στοιχεία που έχουν σταλθεί αρχικά. Μετά, τα στοιχεία συλλέγονται από την διαδικτυακή εφαρμογή κατά τρόπο που να εμφανίζεται ως έγκυρο περιεχόμενο από την ιστοσελίδα.

Η εξαπάτηση ενός χρήστη επιτυγχάνεται με την υποβολή web scripting κώδικα (JavaScript, Jscript, VBScript, ActiveX, HTML, Flash κ.τ.λ.) με δυναμική μορφή σε ευάλωτα σημεία της στοχευόμενης ιστοσελίδας. Εάν η ιστοσελίδα δεν κάνει έλεγχο για τον web scripting κώδικα μπορεί να περάσει κατά λέξη στον browser του χρήστη όπου ενδέχεται να προκαλέσει ανεπιθύμητες ενέργειες.

Εξετάζουμε το ακόλουθο url:

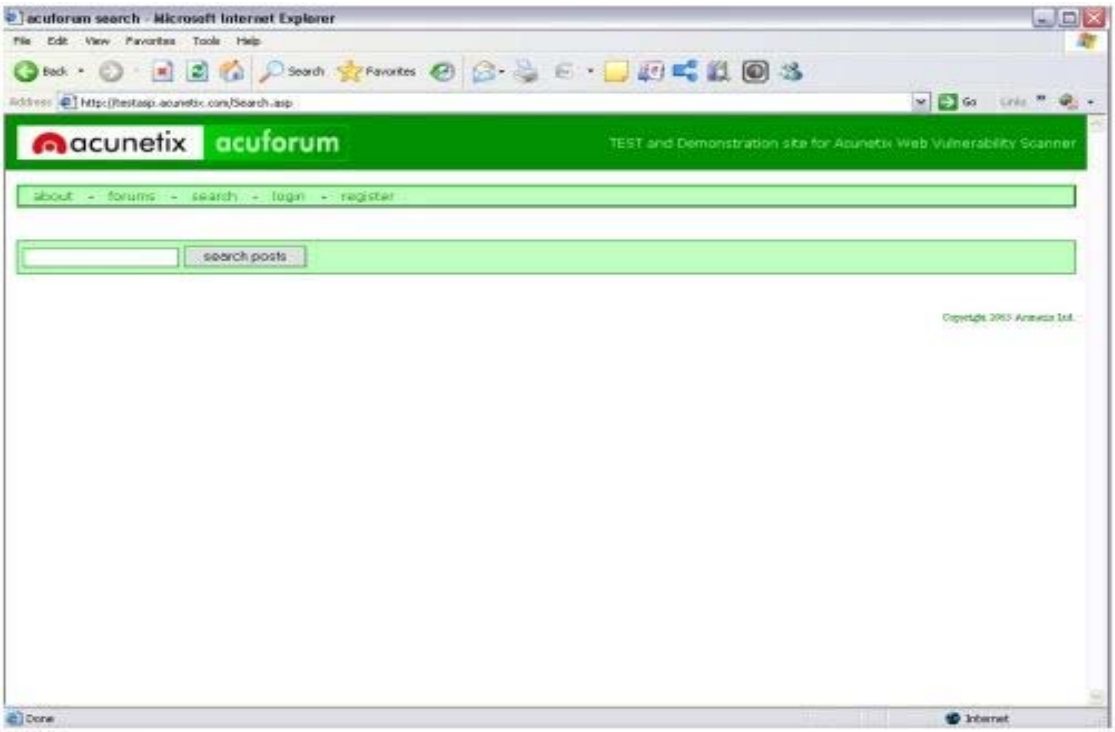
```
http://www.example.com/search.pl?text=<script>alert(document.cookie)
</script>
```

Εάν ένας εισβολέας θα μπορέσει να παραπλανήσει το θύμα έτσι ώστε να επιλέξει μια σύνδεση όπως αυτή και η web εφαρμογή δεν επικυρώνει τα δεδομένα εισόδου, τότε στον browser του θύματος θα αναδυθεί ένα μήνυμα ειδοποιήσεις που θα δείχνει τα τρέχουσα cookies του θύματος. Αυτό το παράδειγμα είναι ακίνδυνο, ένας εισβολέας όμως χρησιμοποιώντας αυτό τον τρόπο μπορεί να κλέψει κωδικούς, να κάνει reset την αρχική σελίδα του θύματος ή να επαναπροσανατολίσει το θύμα στην web τοποθεσία του επιτιθεμένου.

7.3.1 Ένα πρακτικό παράδειγμα XSS επίθεσης σε δοκιμαστικό ιστότοπο Acunetix

Το ακόλουθο παράδειγμα έχει σκοπό να υποδείξει πώς μια XSS επίθεση μπορεί να χρησιμοποιηθεί για να ελέγχει, να τροποποιήσει τη λειτουργικότητα μιας ιστοσελίδας και να επανασχεδιάσει τον τρόπο με τον οποίο η σελίδα επεξεργάζεται τα δεδομένα εισόδου της. Τοποθετούμε τον παρακάτω σύνδεσμο στον browser:
http://testasp.acunetix.com/Search.asp

Παρατηρούμε ότι η σελίδα που εμφανίζεται είναι μια απλή σελίδα με ένα πεδίο εισαγωγής για την εκτέλεση μιας αναζήτησης.[11]



Εικόνα 52: Παράδειγμα XSS επίθεσης σε δοκιμαστικό ιστότοπο Acunetix. Εκτέλεση αναζήτησης

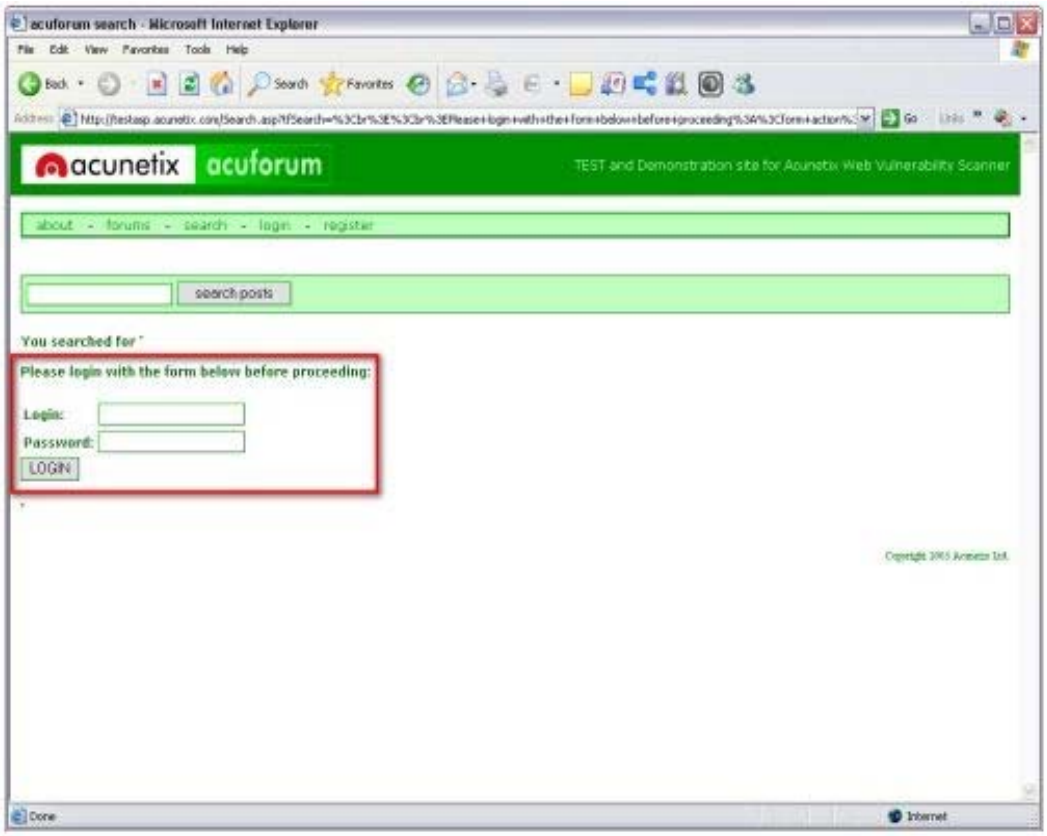
Εισάγουμε τον ακόλουθο κώδικα στο πεδίο αναζήτησης και κάνουμε κλικ στο κουμπί "search posts" και παρατηρούμε πώς εμφανίζεται στη σελίδα μια φόρμα σύνδεσης (login form).

Κώδικας

```
<br><br>Please login with the form below before proceeding:<form
action="destination.asp"><table><tr><td>Login:</td><td><input
type=text length=20
name=login></td></tr><tr><td>Password:</td><td><input type=text
length=20 name=password></td></tr></table><input type=submit
value=LOGIN></form>
```

[11] http://www.acunetix.com/websitesecurity/xss.htm

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.



Εικόνα 53: Παράδειγμα XSS επίθεσης σε δοκιμαστικό ιστότοπο Acunetix. Φόρμα σύνδεσης

Μέσα από XSS στη σελίδα, κατέστη δυνατό να δημιουργήσουμε μια πλαστή φόρμα σύνδεσης που μπορεί να συγκεντρώσει στοιχεία ενός χρήστη. Όπως φαίνεται και στο κομμάτι του κώδικα που εισάγουμε στο πεδίο αναζήτησης περιέχεται ένα τμήμα που αναφέρεται σαν "destination.asp". Σε αυτό το σημείο ένας επιτιθέμενος μπορεί να αποφασίσει εάν η πλαστή φόρμα σύνδεσης θα στείλει τα στοιχεία σύνδεσης του χρήστη λεπτομερώς έτσι ώστε για να μπορούν να ανακτηθούν και να χρησιμοποιηθούν κακόβουλα.

Ένας επιτιθέμενος μπορεί να παρεμβάλει αυτόν τον κώδικα μέσα από τη γραμμή διευθύνσεων του browser έχοντας την εξής μορφή:

http://testasp.acunetix.com/Search.asp?tfSearch=%3Cbr%3E%3Cbr%3EPlease+log in+with+the+form+below+before+proceeding%3A%3Cform+action%3D%22test.a sp%22%3E%3Ctable%3E%3Ctr%3E%3Ctd%3ELogin%3A%3C%2Ftd%3E%3Ctd %3E%3Cinput+type%3Dtext+length%3D20+name%3Dlogin%3E%3C%2Ftd%3E %3C%2Ftr%3E%3Ctr%3E%3Ctd%3EPassword%3A%3C%2Ftd%3E%3Ctd%3E%3Cinput+type%3Dtext+length%3D20+name%3Dpassword%3E%3C%2Ftd%3E%3C%2Ftr%3E%3C%2Ftable%3E%3Cinput+type%3Dsubmit+value%3DLOGIN%3E%3C%2Fform%3E

Αυτό θα δημιουργήσει το ίδιο αποτέλεσμα με πριν, δηλαδή εμφανίζοντας τη σελίδα αναζήτησης. Αποδεικνύεται πώς επιθέσεις XSS μπορεί να χρησιμοποιηθούν με πολλούς διαφορετικούς τρόπους για να επιτευχθεί το ίδιο αποτέλεσμα. Μέτα από αυτή την επίθεση αφού ο επιτιθέμενος αποκτήσει τα προσωπικά στοιχεία σύνδεσης του χρήστη, μπορεί εύκολα να "αναγκάσει" τον browser να εμφανίσει τη σελίδα με

τη μηχανή αναζήτησης όπως ήταν αρχικά και ο χρήστης δεν θα συνειδητοποιήσει ότι μόλις έχει πέσει θύμα εξαπάτησης.

Το παράδειγμα αυτό μπορεί επίσης να βρει χρήση σε όλα τα spam μηνύματα ηλεκτρονικού ταχυδρομείου που όλοι λαμβάνουν. Είναι πολύ κοινό να βρίσκουν οι χρήστες e-mail στα εισερχόμενα μηνύματα που να υποστηρίζει ότι ένας συγκεκριμένος ιστότοπος υποψιάζεται ότι ένα άλλο άτομο έχει εισέλθει με τον λογαριασμό σας κακόβουλα και σας ζητά στη συνέχεια να κάνετε κλικ σε μια σύνδεση για να επικυρώσει την ταυτότητά σας. Πρόκειται για μια παρόμοια μέθοδο που κατευθύνει τον ανυποψίαστο χρήστη σε μια πλαστή έκδοση του ιστοτόπου και αποκτά τα προσωπικά στοιχεία σύνδεσής του. Έπειτα τα εκμεταλλεύεται ο επιτιθέμενος.

7.4 Social engineering techniques (Phishing)

Το Phishing (αμερικανικός νεολογισμός που προκύπτει από την παραφθορά του fishing που σημαίνει ψάρεμα) είναι μια μέθοδος εξαπάτησης των καταναλωτών ενός οργανισμού, συνήθως κερδοσκοπικού και συνίσταται κυρίως στην υποκλοπή των εμπιστευτικών πληροφοριών των καταναλωτών, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κλπ. με σκοπό την παράνομη χρήση τους από τον Phisher για την πρόκληση επιθέσεων.

Με τη βοήθεια κυρίως της απρόσκλητης εμπορικής επικοινωνίας, το γνωστό Spam ή χρησιμοποιώντας bots για την αυτοματοποιημένη στόχευση των υποψήφιων θυμάτων τους ή άλλες παρόμοιες μεθόδους, οι Phishers, εμφανιζόμενοι στο διαδίκτυο ως εκπρόσωποι ενός οργανισμού, τα χαρακτηριστικά του οποίου έχουν αντιγράψει παράνομα, προβαίνουν σε δόλιες πράξεις ή παραλείψεις με τις οποίες πείθουν τα θύματά τους, τα οποία ενδέχεται να μην αντιληφθούν την απάτη, ν' αποκαλύψουν ή να εισάγουν σε σύστημα ηλεκτρονικών υπολογιστών στοιχεία της ταυτότητάς τους και εμπιστευτικές πληροφορίες. Έτσι οι Phishers χρησιμοποιούν αυτές τις πληροφορίες και προσποιούνται την ταυτότητα των θυμάτων. Έχουν πρόσβαση σε όλες τις κινήσεις του χρήστη και ενεργούν εις βάρος του.

7.5 Hidden Manipulation (Παραποίηση Τιμών)

Η παραποίηση τιμών είναι μία από τις πιο κοινές πρακτικές επίθεσης που συμβαίνει σε πολλά e-commerce websites σήμερα. Αυτή η πρακτική επίθεσης συνεπάγεται την χειραγώγηση κρυφών πεδίων και την αλλαγή των δεδομένων που αποθηκεύονται στο πεδίο.

Παραποίηση τιμών γίνεται κατά κανόνα εις βάρος πολλών online καταστημάτων. Κατά τη διάρκεια των ενεργειών του πελάτη, προγραμματιστές με τη βοήθεια των κρυφών πεδίων αποθηκεύουν πληροφορίες που σχετίζονται με τον πελάτη. Τα πεδία, σε γενικές γραμμές, περιλαμβάνουν το ποσοστό των τιμών και τα ποσοστά έκπτωσης. Για παράδειγμα, μια ιστοσελίδα εμπορεύεται κοσμήματα και η τιμή ενός ρολογιού είναι 500€. Το υπάρχον κρυφό πεδίο αναπτύχθηκε από την εφαρμογή για να διευκολυνθεί η ταχεία ανάπτυξη και να αποθηκεύει την αξία του ρολογιού στον συγκεκριμένο πεδίο.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Ο προγραμματιστής που εργάζεται στην εφαρμογή, αναλαμβάνει τη διασφάλιση του κρυφού πεδίου έτσι ώστε να παραμείνει άθικτο. Ωστόσο, ένας επιτιθέμενος μπορεί να τροποποιήσει την αξία του προϊόντος χρησιμοποιώντας ένα κοινό Netscape HTML Editor και να το αλλάξει από 500 € σε 20 €. Έτσι, με την παραποίηση τιμών και τη χρήση του HTML Editor, ο επιτιθέμενος μπορεί να υποβάλει τελικά την ελαφρώς παραλλαγμένη σελίδα HTML και να συνάψει την συναλλαγή του προϊόντος.

Οι περισσότεροι ιδιοκτήτες ιστοχώρων και επιχειρήσεων ανησυχούν ιδιαιτέρως για τέτοιου είδους επιθέσεις.. Για προστασία στο επίπεδο δικτύου τους, χρησιμοποιούν πολλές παραδοσιακές τεχνικές ασφαλείας, όπως η χρησιμοποίηση ηχητικού λογισμικού κατά των ιών, τοίχου προστασίας ή το πιο πρόσφατο λογισμικό εντοπισμού εισβολέων. Στην περίπτωση αυτή, ακόμη και αν τα πεδία είναι κρυφά και υπερβαίνουν τις δυνατότητες των απλών χρηστών, ένας επιτιθέμενος με καλή γνώση προγραμματισμού μπορεί να αποκαλύψει τα πεδία και τα δεδομένα τους και να τα εκμεταλλευτεί. Οι επιθέσεις παραποίησης τιμών μπορούν να παραποιήσουν πληροφορίες ζωτικής σημασίας για την επιχείρηση και το online κατάστημα να αντιμετωπίσει τεράστιες ζημίες. Με μια σειρά από τέτοιες περιπτώσεις, η ιστοσελίδα θα χάσει πιθανώς την αξιοπιστία της στα πρόσωπα των πελατών.[12]

7.6 Λογισμικό με δυνατότητα παρακολούθησης των πακέτων ενός δικτύου (Packet Sniffer)

Packet sniffer ή απλώς sniffer, επίσης αποκαλούμενο network monitor ή network analyzer, είναι ένα λογισμικό με δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Είναι διαθέσιμο για πολλές πλατφόρμες, τόσο εμπορικές όσο open-source παραλλαγές. Μερικά από τα απλούστερα προγράμματα είναι στην πραγματικότητα πολύ εύκολο να υλοποιηθούν σε C ή Perl, χρησιμοποιούν μια γραμμή εντολών και μεταφέρουν τα δεδομένα που έχουν καταγραφεί στην οθόνη. Πιο πολύπλοκα προγράμματα κάνουν χρήση γραφικού περιβάλλοντος, γραφημάτων στατιστικών κυκλοφορίας και προσφέρουν διάφορες δυνατότητες διαμόρφωσης. Όταν γίνει αντιληπτό κάποιο πακέτο, το οποίο ικανοποιεί συγκεκριμένα κριτήρια, καταγράφεται σε ένα αρχείο.

Οι μηχανικοί δικτύων, διαχειριστές συστημάτων και επαγγελματίες στον τομέα της ασφάλειας, αλλά και οι επιτιθέμενοι χρήστες, κάνουν χρήση ανάλογων εργαλείων. Χρησιμοποιούνται νόμιμα από τους πρώτους για καταγραφή και διορθώση στην κίνηση (traffic) του δικτύου και παράνομα από τους επιτιθέμενους για υποκλοπή στοιχείων.

Οι περισσότεροι προσωπικοί υπολογιστές συνδέονται σε ένα LAN (Local Area Network-Τοπικό Δίκτυο), που σημαίνει ότι μοιράζονται μία σύνδεση με άλλους υπολογιστές. Αν το δίκτυο δεν χρησιμοποιεί switch (μεταγωγέας), μεταγωγέας είναι μια συσκευή που φιλτράρει και ξαναστέλνει τα πακέτα ανάμεσα στους τομείς ενός LAN, η κίνηση που προορίζεται για έναν τομέα μεταδίδεται σε κάθε μηχάνημα του δικτύου. Επακόλουθα, κάθε υπολογιστής στην πραγματικότητα βλέπει τα δεδομένα

[12] http://www.hacker4lease.com/hidden-manipulation.html

που προέρχονται από ή προορίζονται για τους γειτονικούς υπολογιστές, αλλά τα αγνοεί.

Το sniffer αναγκάζει τον υπολογιστή, συγκεκριμένα την Network Interface Card (NIC), να αρχίσει να προσέχει και αυτά τα πακέτα, τα οποία προορίζονται για άλλους υπολογιστές. Για να το καταφέρει αυτό θέτει τη NIC σε ειδική λειτουργία, γνωστή ως Promiscuous mode. Όταν η NIC βρίσκεται σε αυτή τη λειτουργία, μια κατάσταση που συνήθως απαιτεί δικαιώματα ανώτερου χρήστη (root), ένα μηχάνημα μπορεί να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του.

Υπάρχουν πολλές δυνατότητες, που καθορίζουν την τύχη των πακέτων:

- Τα πακέτα μετριούνται. Με αυτό τον τρόπο, προσθέτοντας στη συνέχεια το συνολικό μέγεθός τους για μία ορισμένη χρονική περίοδο (συμπεριλαμβάνοντας τις επικεφαλίδες των πακέτων), εξάγεται μια καλή ένδειξη για το πόσο φορτωμένο είναι το δίκτυο. Το πρόγραμμα μπορεί να παρέχει γραφικές απεικονίσεις της σχετικής κίνησης του δικτύου.
- Τα πακέτα μπορούν να εξετασθούν λεπτομερώς. Είναι δυνατόν να γίνει σύλληψη συγκεκριμένων πακέτων, ώστε να διαγνωσθεί και να αντιμετωπιστεί ένα πρόβλημα.[13]

Σε ένα κανονικό LAN υπάρχουν χιλιάδες πακέτα που ανταλλάσσονται με πολλαπλές μηχανές κάθε λεπτό, έτσι ο εισβολέας έχει αρκετό υλικό για να επιτεθεί. Οποιοδήποτε plaintext που διαβιβάζεται μέσω του δικτύου θα είναι ευάλωτο όπως κωδικοί πρόσβασης, ιστοσελίδες, ερωτήσεις βάσεων δεδομένων και μηνύματα. Ένα sniffer μπορεί εύκολα να προσαρμοστεί για να συλλάβει ειδικά πακέτα κυκλοφορίας όπως telnet συνεδρίες ή e-mail. Μόλις κίνηση έχει συλληφθεί και καταγραφεί, οι εισβολείς μπορούν να εξαγάγουν γρήγορα τις πληροφορίες που χρειάζονται-logins, κωδικούς πρόσβασης και κείμενα μηνυμάτων. Οι χρήστες δεν θα υποπτευθούν ποτέ ότι ήταν σε κίνδυνο, τα sniffers δεν προκαλούν βλάβη ή διαταραχή στο περιβάλλον του δικτύου.[14]

7.7 Cross-Site Request Forgery (CSRF)

Το Cross-Site Request Forgery (CSRF) είναι μια επίθεση που αναγκάζει έναν τελικό χρήστη να εκτελέσει τις ανεπιθύμητες ενέργειες σε μια διαδικτυακή εφαρμογή στην οποία έχει πιστοποιηθεί σαν χρήστης. Με τη βοήθεια αποστολής link μέσω μηνυμάτων e-mail και εφαρμογών chat, ένας εισβολέας μπορεί να αναγκάσει τους χρήστες της web εφαρμογής να εκτελέσουν ενέργειες που επιλέγει ο εισβολέας. Μια επιτυχημένη επίθεση CSRF μπορεί να εκμεταλλευτεί τα δεδομένα του τελικού χρήστη και τη λειτουργία σε περίπτωση κανονικής χρήσης. Αν το θύμα, τελικός χρήστης, είναι ο διαχειριστής, αυτό μπορεί να θέσει σε κίνδυνο όλη την web εφαρμογή.

Αναλυτικότερα, είναι μια επίθεση που παγιδεύει το θύμα να φορτώσει μια σελίδα που περιέχει μια κακόβουλη αίτηση. Κακόβουλη αίτηση, υπό την έννοια ότι

---

[13] http://el.wikipedia.org/wiki/Packet_sniffer
[14] http://www.securityfocus.com/infocus/1549

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

κληρονομεί την ταυτότητα και τα προνόμια του θύματος για να εκτελέσει μια ανεπιθύμητη λειτουργία για λογαριασμό του θύματος, όπως η αλλαγή του e-mail του παραλήπτη, της διεύθυνσης κατοικίας ή του κωδικού πρόσβασης, ή η εκτέλεση κάποιας αγοράς. Οι επιθέσεις CSRF γενικά στοχεύουν σε λειτουργίες που προκαλούν αλλαγή της κατάστασης στον server, αλλά μπορεί επίσης να χρησιμοποιηθούν για πρόσβαση σε ευαίσθητα δεδομένα.

Για τους περισσότερες ιστοτόπους, οι browsers περιλαμβάνουν αυτόματα τέτοια αιτήματα κάθε εντολής που σχετίζονται με τον ιστότοπο, όπως cookie συνόδου του χρήστη, βασικά auth διαπιστευτήρια, διεύθυνση IP, διαπιστευτήρια Windows domain κλπ. Επομένως, αν ο χρήστης έχει πιστοποιηθεί στον ιστότοπο, ο ιστότοπος δεν θα έχει κανένα τρόπο να κάνει διάκριση ανάμεσα σε αυτά τα αιτήματα και το νόμιμο αίτημα του χρήστη. Με τον τρόπο αυτό, ο εισβολέας μπορεί να κάνει το θύμα να εκτελεί ενέργειες που δεν είχε την πρόθεση να εκτελέσει, όπως η αποσύνδεση, αγορά προϊόντων, αλλαγή στοιχείων του λογαριασμού του, ανάκτηση στοιχείων του λογαριασμού ή οποιαδήποτε άλλα καθήκοντα που προβλέπονται από τον ευάλωτο δικτυακό τόπο.

Μερικές φορές, είναι δυνατό να αποθηκευτεί η επίθεση CSRF στους ευάλωτους δικτυακούς τόπους. Αυτές οι ευπάθειες ονομάζεται Stored CSRF flaws. Αυτό μπορεί να επιτευχθεί με την απλή αποθήκευση ενός IMG ή IFRAME tag σε ένα πεδίο που δέχεται HTML ή από μία πιο σύνθετη cross-site scripting επίθεση. Αν η επίθεση μπορεί να αποθηκεύσει μια επίθεση CSRF στον ιστότοπο, η σοβαρότητα της επίθεσης είναι αυξημένη. Ειδικότερα, ο κίνδυνος αυξάνεται, επειδή το θύμα είναι πιο πιθανό να επισκεφτεί τη σελίδα που περιέχει την επίθεση παρά να επισκεφτεί κάποια τυχαία σελίδα στο διαδίκτυο. Η πιθανότητα αυτή ενισχύεται, επίσης επειδή το θύμα έχει πιστοποιηθεί στον ιστότοπο ήδη.

Η επίθεση CSRF είναι γνωστή επίσης από μια σειρά ονομάτων όπως XSRF, "Sea Surf", Session Riding, Cross-Site Reference Forgery, Hostile Linking. Η Microsoft αναφέρεται σε αυτό το είδος της επίθεσης ως One-Click επίθεση. [15]

[15] http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

Κεφάλαιο 8 Επικίνδυνα σημεία και τεχνικές διασφαλίσεις Joomla ηλεκτρονικού καταστήματος

Στο διαδίκτυο, η ασφάλεια είναι μια ταχέως εξελισσόμενη και πάντα παρούσα πρόκληση. Δεν υπάρχει ένας συγκεκριμένος τρόπος για να εξασφαλιστεί το δικαίωμα ενός ιστοτόπου, καθώς και όλες οι μέθοδοι ασφαλείας υπόκεινται σε βελτίωση, αναθεώρηση και απαξίωση ανά πάσα στιγμή. Ευτυχώς, υπάρχουν πολλές καλά καθιερωμένες αρχές που μπορούν να βοηθήσουν ένα ιστότοπο να παραμένει ασφαλής. Έχει παρατηρηθεί ότι το Joomla CMS είναι ευάλωτο σε μερικά από τα επικίνδυνα σημεία που αναφέρθηκαν στο κεφάλαιο 7. Παρακάτω περιγράφονται κάποιες βέλτιστες πρακτικές και components που εφαρμόστηκαν στο www.mydesignshop.eu για να ενισχύσουν την ασφάλεια του Joomla ηλεκτρονικού καταστήματος.

8.1 SQL injections σε ιστότοπο Joomla

Οι βάσεις δεδομένων SQL αποτελούν πολύ σημαντικό κομμάτι του Joomla CMS. Η βάση δεδομένων περιέχει το περιεχόμενο, τα id των χρηστών, ρυθμίσεις και πολλά άλλα. Η απόκτηση πρόσβασης σε αυτό το πολύτιμο χώρο είναι ο απώτερος σκοπός των εισβολέων. Η πρόσβαση στην βάση δεδομένων μπορεί να επιτρέψει στον επιτιθέμενο να συγκεντρώσει προσωπικές πληροφορίες όπως ονόματα χρηστών και κωδικούς πρόσβασης.

Όταν γίνεται μια αίτηση από μια σελίδα σε Joomla, αποτελεί ένα "ερώτημα" για τη βάση δεδομένων. Η βάση δεδομένων είναι ανυποψίαστη ότι μπορεί να της έχει ζητηθεί ένα ακατάλληλο αίτημα και θα προσπαθήσει να επεξεργαστεί ό,τι περιέχει το ερώτημα.

.

Συχνά, οι προγραμματιστές δεν κατασκευάζουν τον κώδικα για να παρακολουθήσουν συγκεκριμένα αυτό το είδος της επίθεσης. Στην πραγματικότητα, τον Φεβρουάριο του 2008, είκοσι μία νέα SQL Injection vulnerabilities βρέθηκαν στις εκδόσεις του Joomla.

Για την προστασία των ιστοτόπων από επιθέσεις SQL injections υπάρχουν κάποια πράγματα που μπορεί να κάνει ο διαχειριστής έτσι ώστε να γίνει ο ιστότοπος πιο ασφαλής.

Αρχικά, το πρόθεμα για τους πίνακες του Joomla είναι "jos_". Ωστόσο, αρκετά security exploits[16] βασίζονται σε πίνακες της βάσης δεδομένων που ονομάζονται jos_xxxxxx. Χρησιμοποιώντας ένα διαφορετικό πρόθεμα για την ονομασία των πινάκων του ιστοτόπου μπορεί να προστατευτεί από τα κακόβουλα λογισμικά.

Ο διαχειριστής μπορεί να αλλάξει το πρόθεμα στην ονομασία των πινάκων κατά την εγκατάσταση του νέου Joomla ιστοτόπου, όπου στην σελίδα της εγκατάστασης που συμπληρώνει τις ρυθμίσεις της βάσης δεδομένων, υπάρχει μια περιοχή για "advanced

[16] security exploits: είναι ένα κομμάτι λογισμικού, ένα μεγάλο κομμάτι των δεδομένων ή αριθμός των εντολών που επωφελούνται από ένα σφάλμα,μία βλάβη ή μία ευαισθησία,ώστε να προκαλέσει ανεπιθύμητη ή απρόβλεπτη συμπεριφορά στο λογισμικό του υπολογιστή,

settings" στην οποία προεπιλεγμένο πρόθεμα είναι το "jos_" και απλά αλλάζει το λεκτικό. Θα ήταν προτιμότερο να διατηρηθεί η ίδια μορφή δηλαδή τρία γράμματα και underscore.

Αν έχει ήδη εγκατασταθεί ο ιστότοπος με την προεπιλεγμένη ονομασία πινάκων μπορεί να αλλάξει το πρόθεμα αφού γίνει εξαγωγή της βάσης δεδομένων του ιστότοπου. Στο αρχείο που λαμβάνεται κατά την εξαγωγή της βάσης αντικαθιστάτε το προεπιλεγμένο πρόθεμα με το νέο και με αυτό το αρχείο εκτελείτε ένα νέο SQL ερώτημα που θα δημιουργήσει νέους πινάκες με αυτό το όνομα. Έπειτα διαγράφει ο διαχειριστής πολύ προσεκτικά τους πίνακες με το προεπιλεγμένο πρόθεμα και υπάρχουν πλέον μόνο οι πίνακες με το νέο πρόθεμα που έχει επιλεχτεί.

Επίσης, ο διαχειριστής του ιστοτόπου μπορεί να ακολουθήσει κάποιες μεθόδους έτσι ώστε να γίνει πιο συγκεκριμένος στην διατύπωσή των SQL ερωτημάτων. Όπως για παράδειγμα:

- Οι προγραμματιστές θα πρέπει πάντα να επικυρώνουν την είσοδο του χρήστη, δηλαδή, να γίνεται δοκιμή για τον τύπο, το μήκος, τη μορφή και το φάσμα, και πάντα να υπάρχει η υποψία ότι κακόβουλα δεδομένα εισόδου μπορεί να παραβρίσκονται στα ερωτήματα.
- Θα πρέπει οι διαχειριστές του ιστοτόπου να υποθέσουν διαφορά πιθανά σενάρια επίθεσης και να τα περιορίσουν όπως για παράδειγμα ότι μία περιοχή του ιστότοπου για καταχώρηση εικόνων μπορεί να χρησιμοποιηθούν για κάποιο άλλο σκοπό. Έτσι λοιπόν, πρέπει να περιορίζουν τις καταχωρίσεις δεδομένων σε τύπους αρχείων που πραγματικά θέλουν να αποδεχθούν.
- Ακόμη, δεν θα πρέπει να επιτρέπονται δηλώσεις SQL απευθείας από τα δεδομένα εισόδου του χρήστη.
- Θα πρέπει να επιβληθεί δεδομένη τιμή για το μέγεθος των δεδομένων εισόδου των χρηστών. Αν επιτραπούν μεγαλύτερές εισροές οι χρήστες μπορεί να είναι δυσαρεστημένοι. Εάν το μέγιστο μήκος χαρακτήρων θα πρέπει να είναι οκτώ, δεν επιτρέπονται εισροές πέρα από αυτό. Αυτό θα αποτρέψει μια ζώνη overflow. [17]
- Θα πρέπει να δοκιμαστεί το περιεχόμενο των string μεταβλητών και να αποδέχονται μόνο τις αναμενόμενες τιμές. Να απορρίπτονται καταχωρήσεις που περιέχουν δυαδικά δεδομένα, ακολουθίες διαφυγής, και χαρακτήρες σχολίων. Αυτή είναι μια κοινή τεχνική. Επίσης, αν σε κάποιο σημείο οι χρήστες πρέπει να εισάγουν ένα ακέραιο αριθμό, πρέπει να απαιτηθεί να είναι ακέραιος (ή float). Έτσι, εάν υπάρχει μια μεταβλητή που η τιμή της πρέπει να είναι ακέραιος, αναγκάζεται να έχει ακέραια τιμή δηλαδή:

```
$sql = 'UPDATE #__mytable SET `id` = '. (int) $int;
```

[17] Joomla! Web Security, Tom Canavan

- Η αλληλουχία από strings είναι το πρωταρχικό σημείο εισόδου για script injection. Αν κατά την είσοδο του χρήστη λάβουμε κάποιου είδους μεταβλητής (string) κάλο θα ήταν να αποφύγουμε τη χρήση της[18]:

```
$sql = 'UPDATE #__mytable SET `string` = '. $db->quote ($db-
>getEscaped ($string), false);
```

Παρατηρούμε ότι χρησιμοποιούμε δύο λειτουργίες (functions). Η πρώτη διαφεύγει τη μεταβλητή (string) και η δεύτερη την τυλίγει σε εισαγωγικά. Ακόμη, παρατηρούμε ότι η δεύτερη παράμετρος "$db-> quote ()" είναι ψευδής, αν αφήσουμε αυτή τη συνθήκη εκτός ή την μετατρέψουμε σε αληθής, τότε θα το αποφύγει. Έτσι ώστε έχουμε:

```
$sql = 'UPDATE #__mytable SET `string` = '. $db->quote
($string);
```

Έκτος από τις μεθόδους που περιγράφτηκαν παραπάνω, για τη διασφάλιση του ηλεκτρονικού καταστήματος από SQL injections έχει χρησιμοποιηθεί το jFireWall Litel component, το οποίο είναι ένα δωρεάν επαγγελματικό εργαλείο που προστατεύει τον ιστοχώρο από SQL-Injections. Αντιδρά αμέσως σε κάθε απόπειρα επίθεσης από εισβολείς στην ιστοσελίδα του ηλεκτρονικού καταστήματος και να λαμβάνει αμέσως μέτρα για να κλειδώσουμε τον εισβολέα.

Το συγκεκριμένο component λειτουργεί με βάση ορισμένους κανόνες. Μπορούμε να δημιουργήσετε απεριόριστο αριθμό κανόνων που θεωρούμε ότι θα προστατέψουν των ιστότοπο μας. Για παράδειγμα, μας δίνεται η δυνατότητα να αποκλείσουμε όχι μόνο μία διεύθυνση IP, αλλά και το σύνολο των διευθύνσεων IP της χώρας. Αυτό μας προστατεύει άλλα δεν μπορεί να αποτελέσει ακέραια λύση γιατί υπάρχουν επιθέσεις στις οποίες φαίνεται ότι ο επιτιθέμενος βρίσκεται σε κάποια χώρα και η επίθεση γίνεται από εκεί ενώ στην πραγματικότητα δεν βρίσκεται σε αυτή την χώρα αλλά σε κάποια άλλη.

8.2 Denial of Service Attack σε ιστότοπο Joomla

Επιθέσεις τύπου denial of service, όπως αναφέρεται στο κεφάλαιο 7, είναι αρκετά διαδεδομένες στους διαδικτυακούς τόπους και είναι πολύ πιθανό να συμβούν και σε ιστοτόπους υλοποιημένους με Joomla.

Για την προστασία του ηλεκτρονικού καταστήματος από τις συγκεκριμένες επιθέσεις επιλέξαμε να επισυνάπτουμε τον παρακάτω κώδικα, στον οποίο καθορίζουμε τα requests που μπορεί να δεχτεί ο ιστότοπος ανά λεπτό.

Αρχικά, υπάρχει ένας πίνακας στον οποίο δημιουργούμε τους κανόνες (rules) συμφώνα με τους οποίους θέλουμε να περιορίσουμε τα requests των χρηστών. Συμφώνα με τον πρώτο κανόνα επιτρέπουμε 10 requests σε 10 λεπτά, στον δεύτερο κανόνα επιτρέπουμε 30 requests σε 60 secs κοκ. Έπειτα γίνεται χρήση της συνάρτησης CheckFlood( ), η οποία ελέγχει αν έχουν ξεπεραστεί οι συνθήκες που έχουμε θέσει στον πίνακα των κανόνων (rules), αν ναι θα αποτρέψει τα συνεχόμενα

[18] http://developer.joomla.org/tutorials/181-preventing-sql-injections.html

requests ενημερώνοντας τον εισβολέα ότι δεν μπορεί να συνεχίσει να εκτελεί νέα requests και στέλνοντας ένα e-mail στους διαχειριστές του ιστοτόπου ότι δεχτήκαμε μία επίθεση.

Κώδικας

```
require_once ('class.floodblocker.php');
$flb = new FloodBlocker ( 'tmp/' );

//Δημιουργούμε όσους κανόνες θέλουμε

$flb->rules = array (
 10=>10,                                          // rule 1-maximum
10 requests σε 10 secs
 60=>30,                                          // rule 2-maximum
30 requests σε 60 secs
 300=>50,                                        // rule 3-maximum 50
requests σε 300 secs
 3600=>200                                      // rule 4-maximum 200
requests σε 3600 secs
);

if(!$flb->CheckFlood( ){
 $msg = "There was an hacking attempt by ".$_SERVER['REMOTE_ADDR']."
trying to load ".$_SERVER['REQUEST_URI'];
mail ('info@hellascatalog.gr','HACKING ATTEMPT at
'.$_SERVER['REQUEST_URI'],$msg);
 $html ='<html>
   <head>
   <meta http-equiv="Content-Type" content="text/html; charset=utf-
8"/>
   <title>'.$_SERVER['REMOTE_ADDR'].'</title>
   <style type="text/css">
   <!--
   body{
    background-color: #000000;
    color:#fff;
   }
   -->
   </style>
   </head>
   <body>
     <center>Hey Mr. ' . $_SERVER['REMOTE_ADDR'] . ' oups!!! ;-
)</center>
   </body>
   </html>';
 die ( $html );
}

if (
 ereg('gif\?cmd',$_SERVER['REQUEST_URI']) ||
 ereg('gif&cmd',$_SERVER['REQUEST_URI']) ||
 ereg('jpg\?cmd',$_SERVER['REQUEST_URI']) ||
 ereg('jpg&cmd',$_SERVER['REQUEST_URI']) ||
 ereg('txt?cmd',$_SERVER['REQUEST_URI']) ||
 ereg('txt&cmd',$_SERVER['REQUEST_URI'])
)
{
```

```
 $msg = "There was an hacking attempt by ".$_SERVER['REMOTE_ADDR']."
trying to load ".$_SERVER['REQUEST_URI'];
 mail ('info@hellascatalog.gr','HACKING ATTEMPT at
'.$_SERVER['REQUEST_URI'],$msg);
 die ('Stop hacking!');
}
```

8.3 Προστασία Joomla ιστοτόπου από κακόβουλες επιθέσεις

Κατά την εγκατάσταση του Joomla σε ένα διακομιστή, θα πρέπει να ληφθούν κάποια μέτρα για να αυξηθεί η ασφάλεια και να αποκλειστούν όλα τα σημεία που είναι ευάλωτα σε θέματα ασφαλείας. Εκτός από τα security components και τις τεχνικές που μπορούν να χρησιμοποιήσουν οι διαχειριστές είναι πολύ βασικό η εταιρεία που φιλοξενεί τον ιστότοπο μας στο διαδίκτυο να παρέχει τη μέγιστη ασφάλεια που μπορεί.

8.3.1 Δημιουργία αντιγράφου ασφαλείας

Το Joomla δεν έχει καμία λειτουργία δημιουργίας αντιγράφων ασφαλείας από προεπιλογή. Η δημιουργία αντιγράφων ασφαλείας στο δικτυακό τόπο είναι απαραίτητη γιατί ακόμη και αν ο δικτυακός τόπος δεν αποτελέσει ποτέ στόχο μιας επίθεσης, υπάρχει πάντα η δυνατότητα δημιουργίας κάποιας λάθος ενέργειες από τους ίδιους τους διαχειριστές. Η απλούστερη λύση είναι η δημιουργία αντίγραφών όλων των αρχείων και βάσεων δεδομένων που χρησιμοποιούνται από την ιστοσελίδα σε τοπικό υπολογιστή. Εάν ο ιστότοπος αλλάζει συνεχώς θα χρειαστεί κάποιο είδος αυτόματης δημιουργίας αντιγράφων ασφαλείας. Στις περισσότερες περιπτώσεις, τα πραγματικά αρχεία στο διακομιστή (server) δεν θα αλλάξουν δραματικά, ώστε το μόνο που χρειάζεται είναι ένα αντίγραφο της βάσης δεδομένων.

Στο Joomla υπάρχουν διαφορά components για την δημιουργία αντιγράφων ασφαλείας όπως είναι τα: JoomlaPack, JoomlaCloner, JBackup System Plugin κ.α. Στο www.mydesignshop.eu έχει χρησιμοποιηθεί το JoomlaPack Component για την δημιουργία αντιγράφου ασφαλείας.

8.3.2 Δικαιώματα αρχείων

Κάθε φάκελος και κάθε αρχείο που περιέχει μια ιστοσελίδα διαθέτει ένα σύνολο ιδιοτήτων που ονομάζεται «δικαιώματα». Οι ιδιότητες αυτές καθορίζουν ποιος επιτρέπεται να κάνει οποιαδήποτε ενέργεια με το συγκεκριμένο αρχείο. Σε Unix λειτουργικά συστήματα (συμπεριλαμβανομένου του Linux, FreeBSD, κλπ), υπάρχουν τρείς ενέργειες που μπορούν να πραγματοποιούνται σε ένα αρχείο από κάποιο χρήστη: να διαβάσει, να γράψει και να εκτελέσει. Ομοίως υπάρχουν τρείς κατηγορίες χρηστών που μπορούν να εκτελέσουν αυτές τις ενέργειες. Τα πράγματα είναι λίγο διαφορετικά για τα Windows, αλλά οι περισσότερες Joomla ιστοσελίδες φιλοξενούνται σε διακομιστές (servers) που εκτελούν Unix λειτουργικό σύστημα.

Συνήθως, τα δικαιώματα για ένα αρχείο ορίζονται από ένα τριψήφιο αριθμό. Οι αριθμοί 000 δηλώνουν τον πιο αυστηρό περιορισμό, κανένας χρήστης δεν μπορεί να κάνει καμία ενέργεια. Αντιθέτως, οι αριθμοί 777 δηλώνουν ότι δεν υπάρχει κανένας περιορισμός, ο κάθε χρήστης μπορεί να διαβάσει, να γράψει ή να εκτελέσει το αρχείο.

Το πρώτο ψηφίο αντιπροσωπεύει αυτό που ο «ιδιοκτήτης» του φακέλου (δηλαδή χρήστης που δημιούργησε το αρχείο) επιτρέπεται να κάνει, το δεύτερο ψηφίο διευκρινίζει ποιες ενέργειες μπορούν να κάνουν οι υπόλοιποι εξουσιοδοτημένοι χρήστες και το τρίτο ψηφίο αντιπροσωπεύει τις ενέργειες που επιτρέπονται στους μη εξουσιοδοτημένους χρήστες. Η εντολή που χρησιμοποιείται από το λειτουργικό σύστημα για να ρυθμιστούν τα δικαιώματα ενός αρχείου ονομάζεται «chmod» που σημαίνει «change mode».

Για να υπάρξει ισορροπία μεταξύ ασφάλειας και χρηστικότητας, όλοι οι φάκελοι θα πρέπει να οριστούν σε 755 και όλα τα αρχεία θα πρέπει να οριστεί σε 644 εκτός και αν ένας φάκελος ή ένα αρχείο απαιτεί ρητά μια διαφορετική ρύθμιση, προκειμένου να λειτουργεί σωστά.

Το Joomla έχει τη δυνατότητα να καθορίζει από μόνο του τα εν λόγω δικαιώματα (αναλόγως με τις ρυθμίσεις που έχουν γίνει είτε κατά την εγκατάσταση, είτε μέσω Site|Global Configuration από το διαχειριστικό κομμάτι του Joomla) όταν δημιουργεί νέα αρχεία.

Χρησιμοποιώντας 755 και 644 για τους φακέλους και τα αρχεία, αντίστοιχα, σε γενικές γραμμές σημαίνει ότι τα αρχεία δεν είναι δυνατόν να επεξεργαστούν, ούτε καν από το Joomla (εφόσον δεν έχει εγκατασταθεί suPHP στον server).

Είναι ασφαλέστερο να διατηρούνται τα αρχεία και οι φάκελοι ανεγγράψιμες (δηλαδή. 644) τις περισσότερες φορές, να μετατρέπονται σε εγγράψιμούς μόνο εάν χρειάζεται να γίνουν αλλαγές στις παραμέτρους και να καταστούν ανεγγράψιμες πάλι μόλις τελειώσουν οι αλλαγές. Ειδικά σε σχέση με το αρχείο configuration.php, το οποίο αποθηκεύει τις ρυθμίσεις σας από το Site-> Global Configuration.

Μπορούν να αλλάξουν τα δικαιώματα των αρχείων και των φακέλων χρησιμοποιώντας ένα FTP client ή ένα host πίνακα ελέγχου όπως cPanel ή Plesk.[19]

8.3.3 Διασφάλιση της εισόδου του διαχειριστή

Τα χαρακτηριστικά της σύνδεσης χρήστη στο Joomla, τόσο για το back-end όσο και το front-end της ιστοσελίδας, χρησιμοποιούν μονόδρομη κρυπτογράφηση κωδικού πρόσβασης. Όταν πληκτρολογεί ο χρήστης τον κωδικό πρόσβασης, το Joomla εφαρμόζει ένα "salted hash αλγόριθμο" για να μετατρέψει τον κωδικό πρόσβασης σε ένα ακατάληπτο κείμενο. Ποτέ δεν αποκρυπτογραφεί πραγματικά αυτό το κείμενο, συγκρίνει μόνο την ακατάληπτη εκδοχή του κειμένου του κωδικού πρόσβασης που πληκτρολογείτε με την ακατάληπτη εκδοχή που είναι αποθηκευμένη στη βάση δεδομένων κατά εγγραφή χρήστη για να δεί αν ταιριάζουν.

Προκειμένου να καθοριστεί αν ένας χρήστης είναι συνδεδεμένος ανά πάσα στιγμή, το Joomla χρησιμοποιεί ένα cookie (ένα μικρό αρχείο κειμένου που αποθηκεύεται στον υπολογιστή του χρήστη). Αυτό το cookie δεν περιέχει το όνομα χρήστη και τον κωδικό πρόσβασής, περιέχει μόνο ένα αναγνωριστικό περιόδου (session id) ή τον

[19] http://www.netshinesoftware.com/security/joomla-security.html

αριθμό αναφοράς, τα οποίο το Joomla μπορεί να κοιτάξει μέχρι να μάθουμε ποιος είναι ο χρήστης και εάν έχει εισέλθει. Έτσι ακόμα κι αν κάποιος θα μπορούσε να κλέψει το cookie από τον υπολογιστή του χρήστη, το μόνο που θα πάρει είναι ένας αριθμός αναφοράς και δεν μπορεί να κάνει αρκετά πράγματα με αυτό.

Παρόλα αυτά, οι διαχειριστές πρέπει βεβαιωθούν ότι ο κωδικός πρόσβασης του διαχειριστή δεν είναι εύκολο να τον μαντέψει κάποιος, φυσικά όσο πιο μεγάλος και πολύπλοκος είναι, τόσο πιο λίγες πιθανότητες υπάρχουν να τον μαντέψουν. Κάλο θα ήταν να συμπεριληφθούν στον κωδικό πρόσβασης τόσο αριθμοί όσο και σημεία στίξη για την μέγιστη ασφάλεια.

Επίσης, από προεπιλογή το Joomla θέτει το αναγνωριστικό (id) για τον χρήστη - διαχειριστή ίσον με 62 και αυτό είναι ευρέως γνωστό και μπορεί να χρησιμοποιηθεί από έναν εισβολέα. Για να αποφύγουμε κάτι τέτοιο μπορούμε να δημιουργήσουμε ένα νέο υπέρ-διαχειριστή (super-administrator) με άλλο όνομα χρήστη και έναν ισχυρό κωδικό πρόσβασης, όπως περιγράφτηκε παραπάνω. Επειδή το Joomla δεν μας επιτρέπει να διαγράψουμε τον υπέρ-διαχειριστή, πρέπει να αποσυνδεθούμε και να επανασυνδεθούμε με τα στοιχεία του νέου υπέρ-διαχειριστή, να ορίσουμε τον παλιό υπέρ-διαχειριστη σαν απλό διαχειριστή και έπειτα έχουμε το δικαίωμα να διαγράψουμε τον αρχικό υπέρ-διαχειριστή με id χρήστη 62.

Σε ακόμη ένα σημείο που μπορούμε να βελτιστοποιήσουμε την ασφάλεια του Joomla είναι ότι κάθε διεύθυνση url που οδηγεί στο διαχειριστικό του Joomla είναι ίδια για κάθε Joomla ιστότοπο, δηλαδή είναι της μορφής: http://www.yoursite.com/administrator/.

Αυτό μπορεί να οδηγήσει τον κάθε χρήστη στην είσοδο της διαχείρισης και να του δώσει τη δυνατότητα να αρχίσει δοκιμές για την απόσπαση των στοιχείων εισόδου του διαχειριστή. Με την εγκατάσταση ενός security plugin, όπως είναι το jSecure Authentication plugin μπορούμε να προσθέσουμε ένα επίθεμα, που διαλέγουμε εμείς, στο τέλος του url ώστε να πάρει τη μορφή: http://www.yoursite.com/administrator/?localhost.

Εάν η διεύθυνση url που οδηγεί στη διαχείριση δεν εγγραφεί με τη σωστή κατάληξη, το jSecure Authentication plugin δίνει δύο επιλογές την ανακατεύθυνση σε δεν βρέθηκε σελίδα (404) ή την ανακατεύθυνση στην αρχική σελίδα του ιστοτόπου. Για περισσότερη ασφάλεια μπορούμε να αλλάζουμε το επίθεμα τακτικά.

8.3.4 Αλλαγή του αρχείου .htaccess

Υπάρχει ένα αρχείο που βρίσκεται στον πυρήνα του Joomla και ονομάζεται htaccess.txt. Όσο το αρχείο ονομάζεται htaccess.txt, αυτό δεν έχει καμία απολύτως επίπτωση στο δικτυακό τόπο. Αφού μετονομαστεί το αρχείο σε .htaccess επηρεάζει κάθε αίτηση που υποβάλλεται από τον ιστότοπο.

Συνήθως, μετονομασία του αρχείου σε .htaccess γίνεται για επανεγγραφή των κρυπτογραφημένων urls από ένα δυναμικό σύστημα διαχείρισης περιεχομένου σε πιο ευανάγνωστα urls έτσι ώστε να γίνουν πιο φιλικά στις μηχανές αναζήτησης. Όμως υπάρχουν πολλές άλλες χρήσεις για ένα .htaccess αρχείο όπως ο καθορισμός κωδικού προστασίας σε "ευαίσθητους" φακέλους, ο περιορισμός πρόσβασης σε ευαίσθητα καταλόγους από την IP διεύθυνσή τους και διάφορα άλλα. Αυτό το αρχείο μπορεί να

γίνει πολύ ισχυρό, επομένως είναι σημαντικό να εξασφαλιστεί ότι κανένα μη εξουσιοδοτημένο άτομο δεν θα μπορέσει να το επεξεργαστεί.

Κατά την εγκατάσταση του Joomla οι παρακάτω ρυθμίσεις ασφαλείας περιλαμβάνονται στο αρχείο htaccess.txt:

Κώδικας

```
########## Begin-Rewrite rules to block out some common exploits
#
# Block out any script trying to set a mosConfig value through the
URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [OR]
# Block out any script that includes a <script> tag in URL
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]
#
########## End-Rewrite rules to block out some common exploits
```

Επιπλέον, μπορούμε να παραμετροποιήσουμε το αρχείο .htaccess προσθέτοντας τεχνικές οι οποίες θα αυξήσουν την ασφάλεια του ιστοτόπου μας. Μερικές από αυτές περιγράφονται παρακάτω[20]:

- Αποφυγή επιθέσεων τύπου Injection (Global Variable Injection και Code Injection) και Cross Site Scripting (XSS) ρυθμίζοντας τη δομή των php boolean directives χρησιμοποιώντας php_flag. Η μορφή για php_flag είναι: "*php flag όνομα on|off* ". Προσθέτουμε οποιοδήποτε από τα ακόλουθα δείγματα κώδικα στο αρχείο .htaccess, το καθένα σε διαφορετική γραμμή:
    - Πρόληψη από επιθέσεις Global Variable Injection
      Κώδικας
      ```
      php_flag register_globals off
      ```
    - Πρόληψη από επιθέσεις Cross Site Scripting (XSS)
      Κώδικας
      ```
      php flag allow_url_fopen off
      ```
    - Πρόληψη από επιθέσεις Code Injection
      Κώδικας
      ```
      php_flag magic_quotes_gpc on
      ```
- Ο περιορισμός πρόσβασης στον κατάλογο από τη διεύθυνση IP μπορεί να αποτελέσει ένα πολύ αποτελεσματικό τρόπο για την προστασία του καταλόγου του διαχειριστή σε ιστότοπο Joomla. Κάθε άλλος κατάλογος στο μπορεί να προστατευτεί με τον ίδιο τρόπο. Αυτή η μέθοδος λειτουργεί μόνο αν υπάρχει μια στατική διεύθυνση IP. Όποιος προσπαθήσει να περιηγηθεί

[20] http://forum.joomla.gr/viewtopic.php?f=54&t=8932

στους καταλόγους αυτούς, χρησιμοποιώντας μια διαφορετική διεύθυνση IP, εμφανίζεται ένα σφάλμα 403 Forbidden.

Στον κατάλογο που θέλουμε να προστατεύσουμε, ανοίγουμε το αρχείο .htaccess ή αν δεν υπάρχει δημιουργούμε ένα νέο αρχείο με αυτή την ονομασία και προσθέτουμε τον ακόλουθο κώδικα, αντικαθιστώντας τους αριθμούς 100.100.100.100 με τη στατική διεύθυνση IP σκοπεύουμε να επιτρέψουμε:

Κώδικας

```
<Limit GET>
    Order Deny, Allow
    Deny from all
    Allow from 100.100.100.100
</Limit>
```

8.3.5 Ρυθμίσεις διακομιστή (αρχείο php.ini)

Το Joomla διευκρινίζει ορισμένες ρυθμίσεις που συνιστώνται για την ορθή λειτουργία του συστήματος. Μια λίστα με τις συνιστώμενες και τις πραγματικές ρυθμίσεις εμφανίζεται κατά την εγκατάσταση του Joomla. Μία από τις συνιστώμενες ρυθμίσεις πρέπει να έχει την επιλογή "Display Errors" ενεργοποιημένη. Αυτό είναι πολύ χρήσιμο κατά την ανάπτυξη και την αποσφαλμάτωση ενός ιστοτόπου, αλλά υπάρχει ένα θέμα ευπάθειας ασφαλείας σε ορισμένες εκδόσεις της PHP το οποίο μπορεί να επιτρέψει cross-site scripting επιθέσεις, όταν επιλογή "Display Errors" είναι ενεργοποιημένη, εάν υπάρχει κάποιο script που δημιουργεί σφάλμα.

Μπορούμε να καταστείλουμε τα μηνύματα λάθους στο Joomla με τη μετάβαση στο "Site|Global Configuration" και κάνοντας κλικ στην καρτέλα Server. Ορίζουμε την επιλογή "Error Reporting" σε "None".

Για να απενεργοποιήσετε την εμφάνιση όλων των λαθών στην PHP, θα πρέπει να αλλάξουμε κάποιες ρυθμίσεις στο αρχείο που ονομάζεται php.ini. Μπορεί να μην υπάρχει πρόσβαση σε αυτό το αρχείο, εάν χρησιμοποιούμε κοινή φιλοξενία (shared hosting) αλλά μπορεί να είναι δυνατό να προσθέσουμε το δικό μας php.ini αρχείο σας στον φάκελο του διαχειριστή της ιστοσελίδας μας, το οποία θα επηρεάσει μόνο τον δικό μας ιστότοπο. Εναλλακτικά, ανάλογα με τις ρυθμίσεις στον διακομιστή μας, ίσως υπάρχει δυνατότητα να παρακάμψουμε επιμέρους ρυθμίσεις από το php.ini στο αρχείο .htaccess.

Οι ρυθμίσεις που πρέπει να προσδιορίζονται στο αρχείο php.ini είναι:

```
display_errors = Off
html_errors = Off
display_startup_errors = Off
log_errors = On
```

Αυτές οι ρυθμίσεις επιτρέπουν στα PHP λάθη που ενδέχεται να δημιουργηθούν, να συνδεθούν σε ένα αρχείο κειμένου αντί να εμφανιστούν στο παράθυρο του browser του χρήστη.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Κεφάλαιο 9 Τεχνικές διασφαλίσεις ηλεκτρονικών καταστημάτων

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (εμπιστευτικότητα). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ.Χ, είναι όντως από τον κ.Χ και όχι από κάποιον που παριστάνει τον Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

Οι παραπάνω ιδιότητες, (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

9.1 Ψηφιακές υπογραφές (Digital Signatures)

Μια ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή αποδεικνύει ότι το μήνυμα δημιουργήθηκε από ένα γνωστό αποστολέα και ότι δεν αλλοιώθηκε κατά τη μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούνται συνήθως για διανομή λογισμικού, οικονομικές συναλλαγές, καθώς και σε άλλες περιπτώσεις όπου είναι σημαντικός ο εντοπισμός πλαστογραφίας και παραποίησης. [21]

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η

[21] http://en.wikipedia.org/wiki/Digital_signature

έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού-one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ.128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα.

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).[22]

9.2 Ψηφιακά Πιστοποιητικά (Digital Certificates)

Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την αναγνώριση μίας οντότητας (φυσικό πρόσωπο, εξυπηρετητής, οργανισμός κοκ) και την ανάκτηση του δημοσίου κλειδιού αυτής.

Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, το οποίο συνοπτικά περιλαμβάνει τα εξής στοιχεία:

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.

Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται ευρέως για διάφορες κρυπτογραφημένες ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Παραδείγματα τέτοιων συναλλαγών είναι: Σύνοδοι με βάση το πρωτόκολλο SSL (Client/Server SSL Certificates),

[22] http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

κρυπτογραφημένο και υπογεγραμμένο ηλεκτρονικό ταχυδρομείο (S/MIME Certificates), υπογραφή αντικειμένων (Object-signing Certificates) κοκ.[23]

9.3 Ηλεκτρονική Ανταλλαγή Δεδομένων (EDI-Electronic Data Interchange)

Electronic Data Interchange (EDI) αναφέρεται στην διαρθρωμένη διαβίβαση των δεδομένων μεταξύ των οργανισμών με ηλεκτρονικά μέσα. Χρησιμοποιείται για τη μεταφορά ηλεκτρονικών εγγράφων από το ένα σύστημα υπολογιστή στον άλλο, δηλαδή από ένα εμπορικό εταίρο σε άλλο εμπορικό εταίρο. Είναι κάτι περισσότερο από το απλό e-mail, για παράδειγμα οργανισμοί θα μπορούσαν να αντικαταστήσουν φορτωτικές (bill of lading)[24] και επιταγές με τα κατάλληλα μηνύματα EDI. Η χρήση του EDI προϋποθέτει την εγκατάσταση ενός λογισμικού και από τις δύο πλευρές των συναλλαγών. Αναφέρεται επίσης ρητά στην "οικογένεια προτύπων", συμπεριλαμβανομένης της σειράς X12.

Το Διαδίκτυο εκτός από VAN παρόχους, χρησιμοποιεί τα δικά του πρωτόκολλα επικοινωνίας για να εξασφαλίσει ότι τα EDI έγγραφα διαβιβάζονται με ασφάλεια. Τα πιο δημοφιλείς πρωτόκολλα είναι File Transfer Protocol Secure (FTPS), Hyper Text Transport Protocol Secure (HTTPS), και AS2. [25]

9.4 Επίπεδο Ασφαλών Συνδέσεων (SSL-Secure Sockets Layer)

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε

---

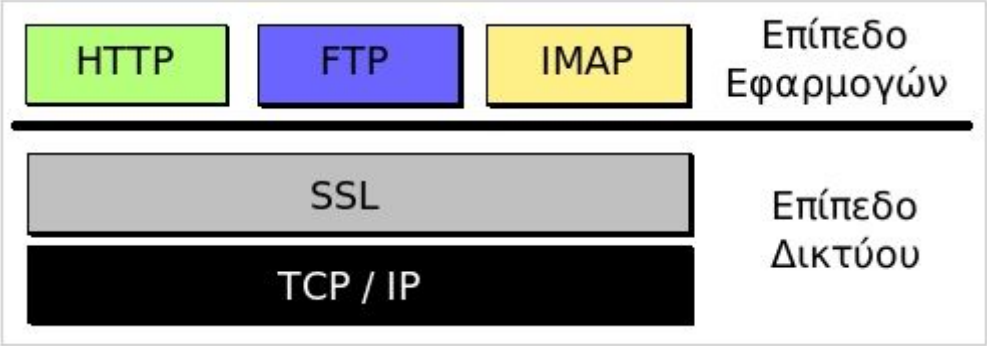
[23] http://el.wikipedia.org/wiki/ψηφιακο_πιστοποιητικο

[24] Η λεγόμενη φορτωτική, (bill of lading), είναι ένα αξιόγραφο που περιέχει προσδιορισμό δικαιώματος χαρακτηριζόμενο ως προς το είδος, την έκταση και την ιδιότητά του. Πρόκειται για πιστωτικό τίτλο.

[25] http://en.wikipedia.org/wiki/Electronic_Data_Interchange

πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol/Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (e-mail). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.



Εικόνα 54: Πως λειτουργεί το SSL.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES-Data Encryption Standard, DSA-Digital Signature Algorithm, KEA-Key Exchange Algorithm, MD5-Message Digest, RC2/RC4, RSA, SHA-1-Secure Hash Algorithm, SKIPJACK, Triple-DES.

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης.

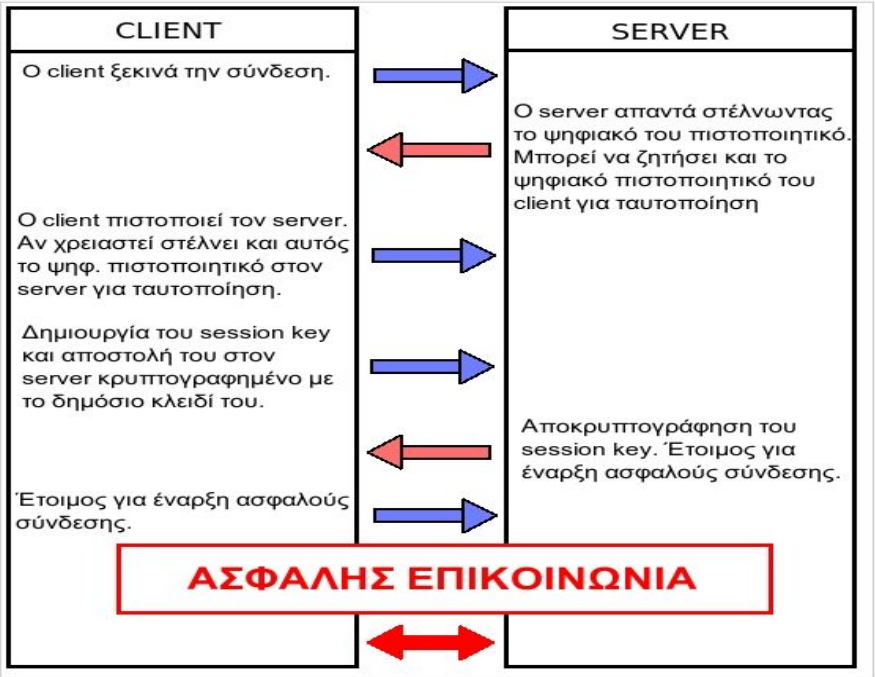
Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client-server) είναι κρυπτογραφημένα.

Η διαδικασία της χειραψίας φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί.



Εικόνα 55: Διαδικασία της χειραψίας δύο συσκευών σύμφωνα με το πρωτόκολλο SSL.

9.4.1 Επιβάρυνση από το SSL

Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

- Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.
- Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (π.χ. μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

9.4.2 Αντοχή του SSL σε γνωστές επιθέσεις

Dictionary Attack

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το

κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

Brute Force Attack

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

Replay Attack

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

Man-In-The-Middle-Attack

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.

Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

9.5 Ασφαλείς Ηλεκτρονικές Συναλλαγές (SET-Secure Electronic Transactions)

Το Secure Electronic Transaction (SET) ήταν ένα πρότυπο πρωτόκολλο για τη διασφάλιση των συναλλαγών με πιστωτική κάρτα μέσω ανασφαλών δικτύων, ειδικότερα μέσω του Διαδίκτυου. Το SET δεν ήταν ένα σύστημα πληρωμών, αλλά ένα σύνολο πρωτοκόλλων ασφάλειας που επιτρέπουν στους χρήστες να χρησιμοποιούν την υπάρχουσα υποδομή της πιστωτικής κάρτας πληρωμής σε ένα ανοικτό δίκτυο, με ασφαλή τρόπο. Αναπτύχθηκε από την MasterCard και την Visa.

Η διαδικασία περιλαμβάνει ένα αριθμό ελέγχων ασφαλείας που πραγματοποιείται με τη χρήση ψηφιακών πιστοποιητικών που χορηγούνται στους εμπλεκόμενους αγοραστές, εμπόρους και τράπεζες.[26]

9.6 Secure HTTP (S-HTTP)

Το HTTPS (Secure HTTP) χρησιμοποιείται στην επιστήμη των υπολογιστών για να δηλώσει μία ασφαλή http σύνδεση. Ένας σύνδεσμος (URL) που αρχίζει με το πρόθεμα https υποδηλώνει ότι θα χρησιμοποιηθεί κανονικά το πρωτόκολλο HTTP, αλλά η σύνδεση θα γίνει σε διαφορετική πόρτα (443 αντί 80) και τα δεδομένα θα ανταλλάσσονται κρυπτογραφημένα. Το σύστημα αυτό σχεδιάστηκε αρχικά από την εταιρία Netscape Communications Corporation για να χρησιμοποιηθεί σε sites όπου απαιτείται αυθεντικοποίηση χρηστών και κρυπτογραφημένη επικοινωνία. Σήμερα χρησιμοποιείται ευρέως στο διαδίκτυο όπου χρειάζεται αυξημένη ασφάλεια διότι διακινούνται ευαίσθητες πληροφορίες (π.χ. αριθμοί πιστωτικών καρτών, passwords κοκ)

Το HTTPS δεν είναι ένα ξεχωριστό πρωτόκολλο αλλά αναφέρεται στον συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL). Η κρυπτογράφηση που χρησιμοποιείται διασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα μπορούν να υποκλαπούν από άλλους κακόβουλους χρήστες ή από επιθέσεις man-in-the-middle.

Για να χρησιμοποιηθεί το HTTPS σε έναν server, θα πρέπει ο διαχειριστής του να εκδώσει ένα πιστοποιητικό δημοσίου κλειδιού. Σε servers που χρησιμοποιούν το λειτουργικό σύστημα UNIX αυτό μπορεί να γίνει μέσω του προγράμματος OpenSSL. Στην συνέχεια το πιστοποιητικό αυτό θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία πιστοποιεί ότι ο εκδότης του πιστοποιητικού είναι νομότυπος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει.

Όπως αναφέρθηκε παραπάνω, το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων. Το επίπεδο προστασίας των δεδομένων εξαρτάται από το πόσο σωστά έχει εφαρμοστεί η διαδικασία ασφάλειας

[26] http://en.wikipedia.org/wiki/Secure_Electronic_Transaction

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

που περιγράφηκε και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται.

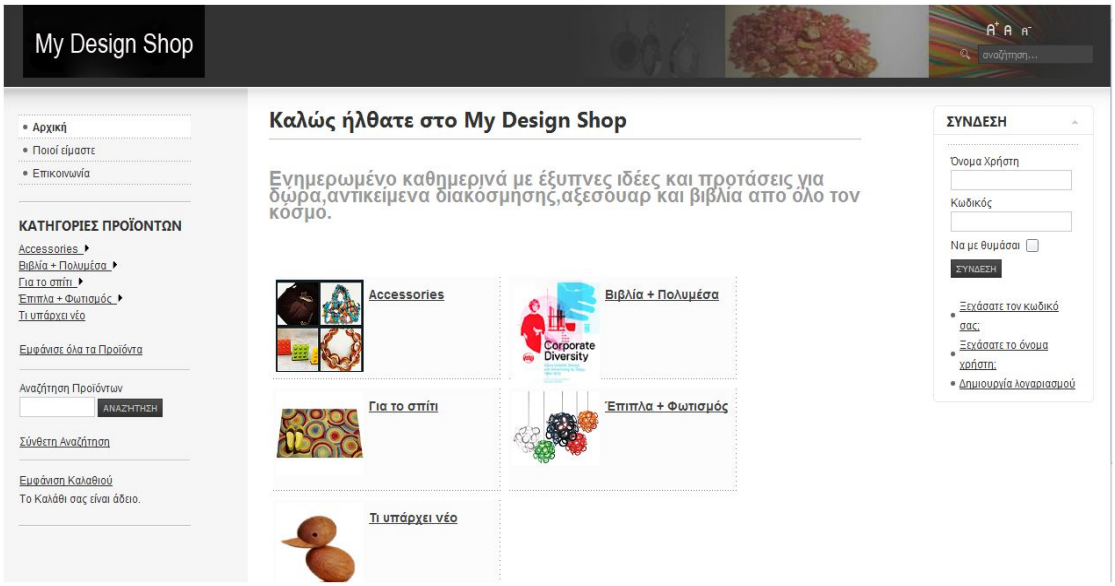
Δεν ισχύει το σενάριο ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής κάρτας, στις ηλεκτρονικές συναλλαγές, από κατάχρηση. Αντιθέτως το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον server. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον server χωρίς κανείς να μπορέσει να τα υποκλέψει. Παρόλα αυτά υπάρχει το ενδεχόμενο διάφοροι κακόβουλοι εισβολείς να έχουν επιτεθεί στον server και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

Κεφάλαιο 10 Βασικές λειτουργίες του ηλεκτρονικού καταστήματος

Κάθε ηλεκτρονικό κατάστημα διαμορφώνεται ανάλογα με τις ανάγκες του και τα προϊόντα που διαθέτει προς πώληση. Στη δική μας περίπτωση έχουμε ένα ηλεκτρονικό κατάστημα ειδών διακόσμησης και design. Ο κάθε χρήστης που επιθυμεί να αγοράσει κάποιο προϊόν πρέπει αρχικά να έχει δημιουργήσει ένα λογαριασμό στον οποίο έχει εισάγει τα προσωπικά του στοιχεία. Έπειτα κάθε φορά που συνδέεται στο κατάστημα και επιθυμεί να πραγματοποιήσει κάποια αγορά θα εισάγει το όνομα πρόσβασης με τον κωδικό που έχει επιλέξει και θα είναι σε θέση να ολοκληρώσει την αγορά του. Αφού επιλέξει τα προϊόντα που επιθυμεί τα προσθέτει στο καλάθι αγορών, έπειτα επιλέγει ένα από τους τρείς τρόπους πληρωμής που διαθέτει το κατάστημα και ολοκληρώνει την αγορά του. Παρακάτω περιγράφεται αναλυτικά η εισαγωγή νέου πελάτη και η διεξαγωγή μιας παραγγελίας στο www.mydesignshop.gr.

10.1 Εισαγωγή νέου πελάτη

Αρχικά, πληκτρολογούμε στον broswer που χρησιμοποιούμε την διεύθυνση του καταστήματος www.mydesignshop.gr. Μας εμφανίζεται η αρχική σελίδα του καταστήματος.

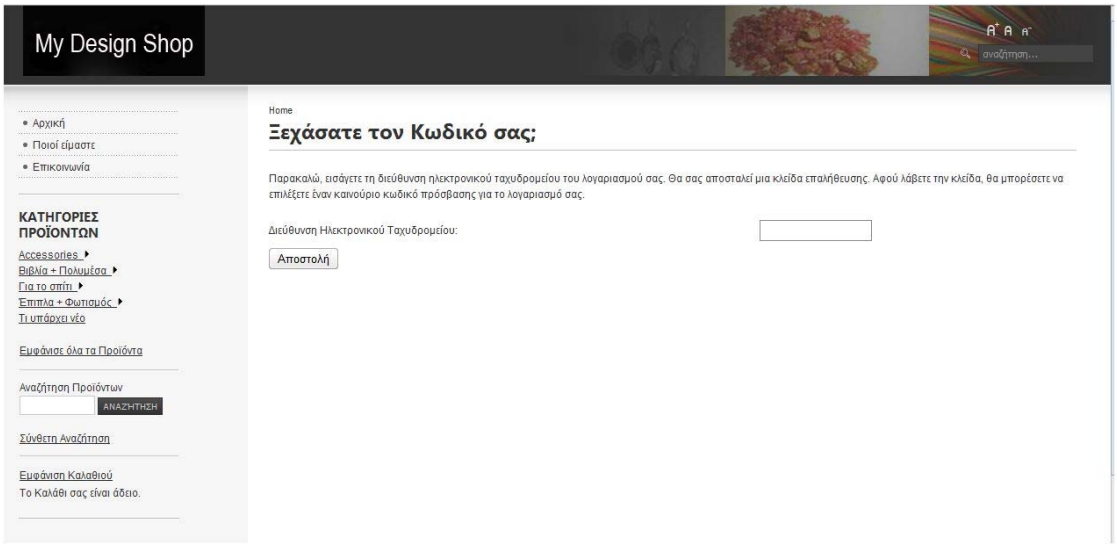


Εικόνα 56: Αρχική σελίδα ηλεκτρονικού καταστήματος, MyDesignShop

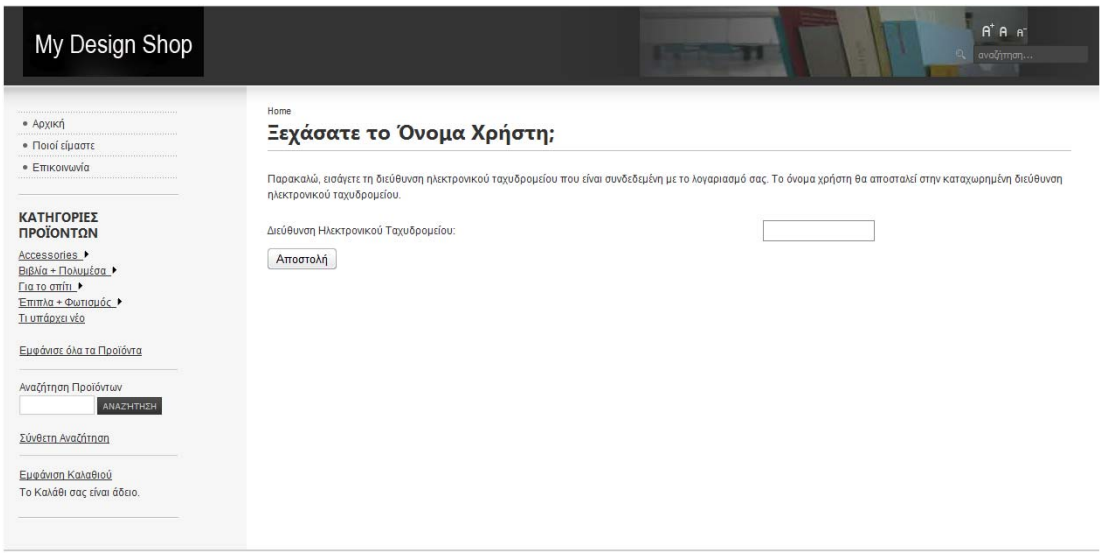
Αν ο χρήστης είναι ήδη πελάτης στο κατάστημά μας στο μενού "ΣΥΝΔΕΣΗ" θα πληκτρολογήσει το "Όνομα Χρήστη" και τον "Κωδικό" που έχει επιλέξει και εφόσον τα στοιχεία που πληκτρολογεί είναι έγκυρα θα εισέλθει στο κατάστημα.

Αν ο χρήστης έχει ξεχάσει τον κωδικό πρόσβασης ή το όνομα χρήστη μπορεί να επιλέξει από το μενού "ΣΥΝΔΕΣΗ" τις επιλογές: "Ξεχάσατε τον κωδικό σας;" και "Ξεχάσατε το όνομα χρήστη;" και να του αποσταλούν τα στοιχεία στην ηλεκτρονική διεύθυνση που θα επιλέξει.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

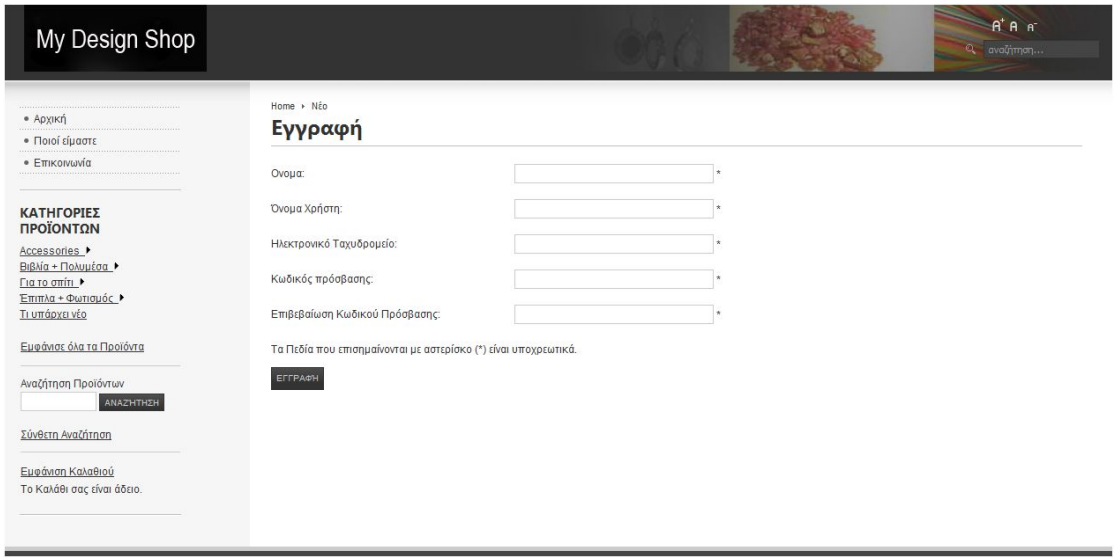


Εικόνα 57: Οθόνη ανάκτησης κωδικού πρόσβασης, My Design Shop



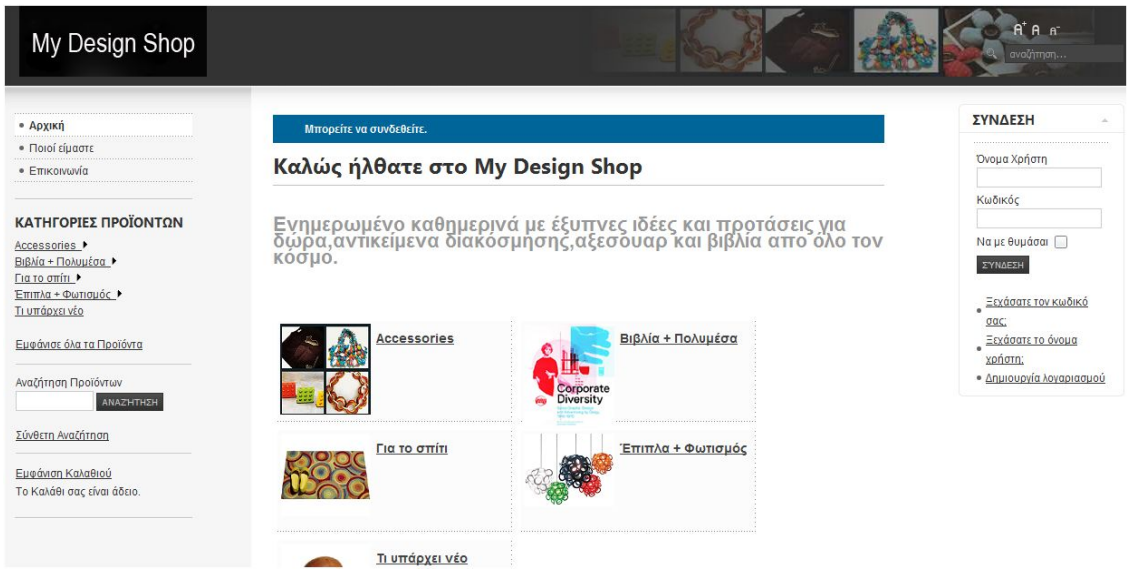
Εικόνα 58: Οθόνη ανάκτησης όνομα χρήστη, My Design Shop

Αν ο χρήστης, δεν έχει δημιουργήσει λογαριασμό ποτέ στο κατάστημά μας, επιλέγει "Δημιουργία λογαριασμού" και του εμφανίζεται μια φόρμα εγγραφής στην οποία πρέπει να συμπληρώσει τα στοιχεία του. Τα πεδία με * είναι υποχρεωτικά.



Εικόνα 59: Φόρμα εγγραφής νέου πελάτη, My Design Shop

Αφού γίνει η εγγραφή, λαμβάνει ο χρήστης ένα ειδοποιητήριο e-mail και έπειτα του εμφανίζεται ένα μήνυμα στην αρχική σελίδα ότι μπορεί να συνδεθεί στο κατάστημα με το "Όνομα χρήστη" και τον "Κωδικό πρόσβασης" που έχει επιλέξει.



Εικόνα 60: Μήνυμα ότι επιτρέπεται η σύνδεση μετά την εγγραφή**,** My Design Shop

10.2 Διαδικασία παραγγελίας

Κατά τη διαδικασία της παραγγελίας ο πελάτης επιλέγει τα προϊόντα που επιθυμεί τα οποία είναι χωρισμένα σε κατηγορίες, για κάθε προϊόν υπάρχει η τιμή του, μία φωτογραφία του προϊόντος, μία σύντομη περιγραφή, πόσα κομμάτια από το συγκεκριμένο προϊόν είναι διαθέσιμα και το χρονικό διάστημα που συνήθως παραδίνεται στον πελάτη το προϊόν αυτής της κατηγορίας.

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

Επίσης, ο πελάτης μπορεί να αξιολογήσει το προϊόν και να γράψει μία κριτική για αυτό, έτσι ώστε να γνωστοποιήσει και στους υπόλοιπους πελάτες τη γνώμη του για το συγκεκριμένο προϊόν.

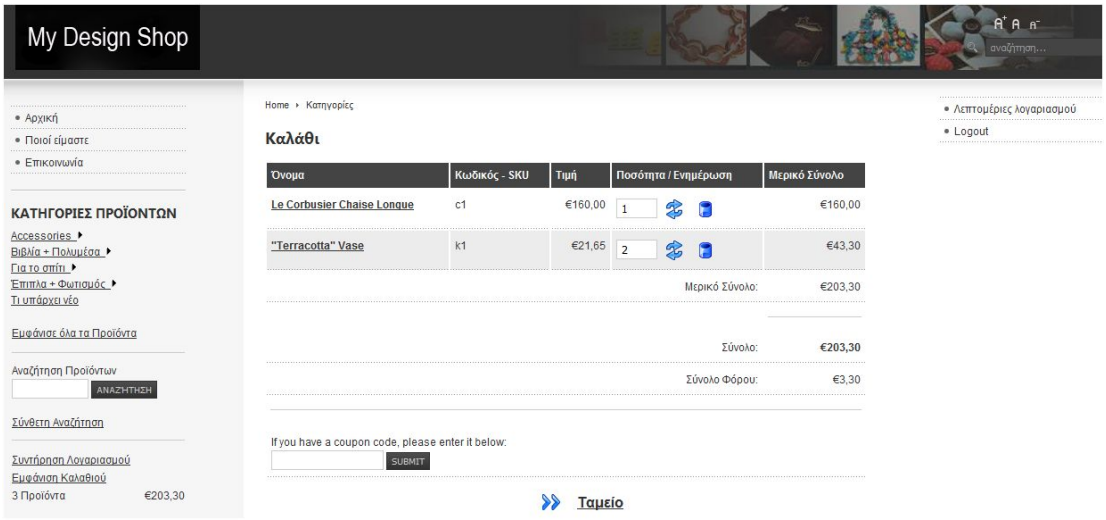
Ο χρήστης αφού έχει κάνει login επιλέγει ένα προϊόν και το τοποθετεί στο καλάθι αγορών, κάνοντας κλικ στο "Προσθήκη στο καλάθι".

Εικόνα 61: Προσθήκη προϊόντος στο καλάθι, My Design Shop

Αφού προσθέσει το προϊόν στο καλάθι μπορεί είτε να συνεχίσει τις αγορές του είτε να επιλέξει το ταμείο. Στο αριστερό μενού βλέπουμε ότι υπάρχει το καλάθι αγορών και ενημερώνει τον πελάτη πόσα προϊόντα έχει προσθέσει και πόσο κοστίζουν.

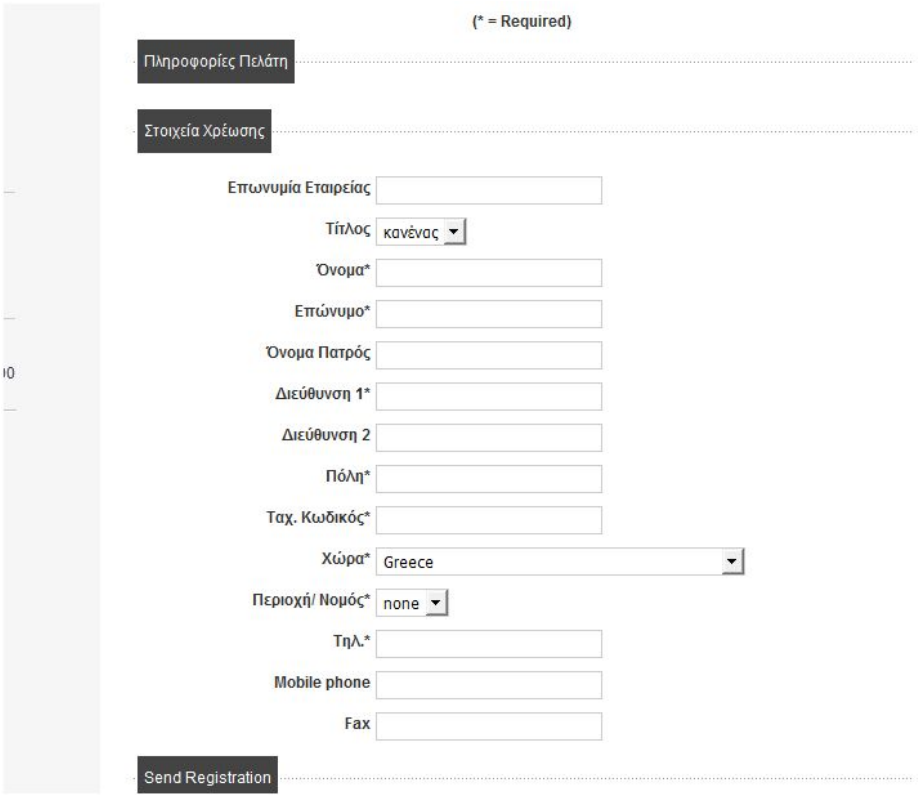
Εικόνα 62: Μενού εμφάνιση καλαθιού, My Design Shop

Αν ο πελάτης επιλέξει εμφανίσει καλαθιού και εμφανίζεται μια λίστα με τα προϊόντα που έχει επιλέξει, η τιμή τους, ο κωδικός του κάθε προϊόντος και η ποσότητα από το κάθε προϊόν.



Εικόνα 63: Καλάθι αγορών, My Design Shop

Για ολοκληρώσει της παραγγελίας ο πελάτης επιλέγει "Ταμείο". Στο σημείο αυτό πρέπει να συμπληρώσει μία φόρμα, στην οποία αναγράφονται τα στοιχεία χρέωσης του πελάτη (ονοματεπώνυμο, διεύθυνση, πόλη, ταχ. κωδικός, χώρα, νομός, τηλέφωνο) και να αποδεχτεί τους όρους εξυπηρέτησης. Τα πεδία με * είναι υποχρεωτικά. Εφόσον συμπληρώσει μια φορά τα στοιχεία χρέωσης, αποθηκεύονται στον λογαριασμό του.

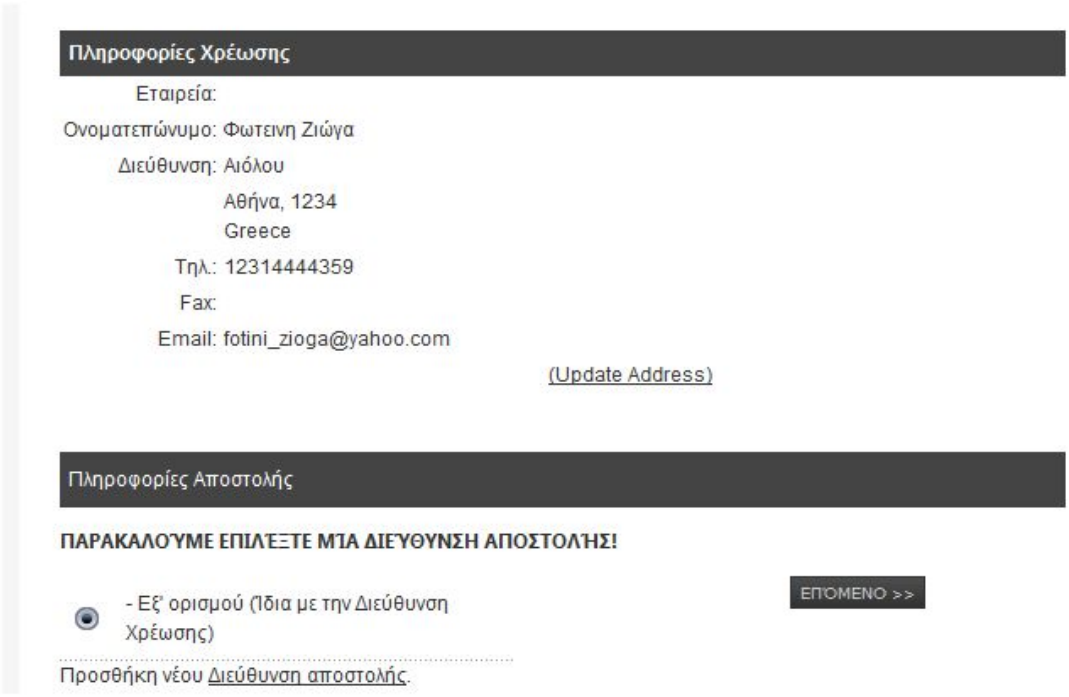


Εικόνα 64: Φόρμα εισαγωγής στοιχείων χρέωσης του πελάτη, My Design Shop

Αφού η φόρμα συμπληρωθεί σωστά και κάνει κλικ στο κουμπί "Send Registration", εμφανίζεται το καλάθι αγορών με τα προϊόντα που έχει επιλέξει ο πελάτης και στο κάτω μέρος τις σελίδας εμφανίζονται δύο καρτέλες με τίτλους "Πληροφορίες Χρέωσης" και "Πληροφορίες Αποστολής", όπου στην πρώτη περιέχονται οι

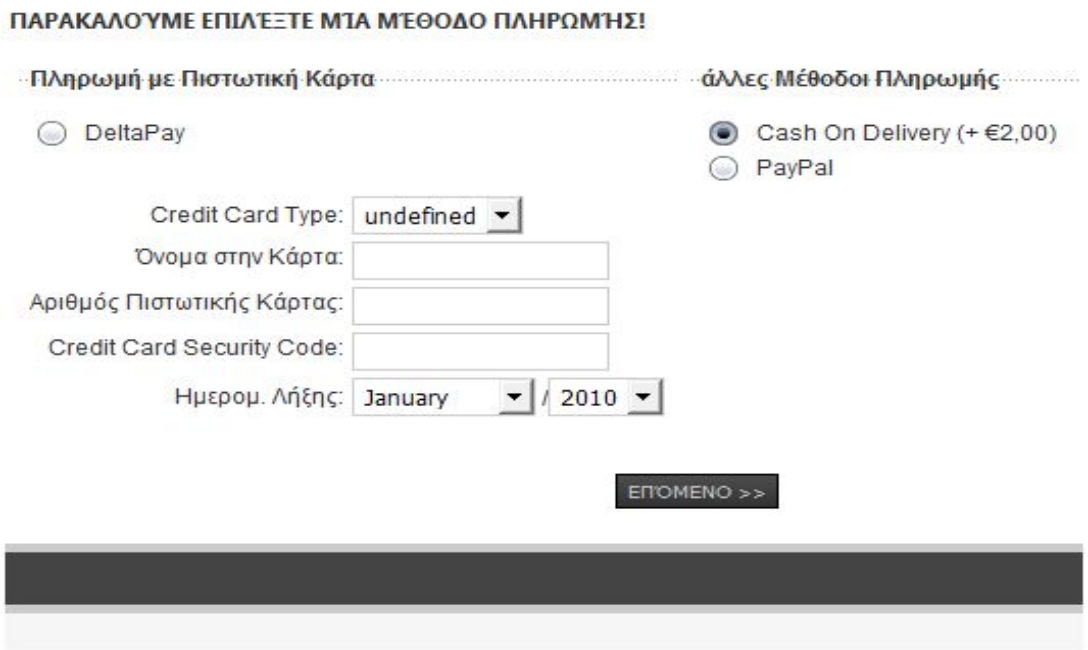
Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

πληροφορίες χρεώσεις που έχουν συμπληρωθεί παραπάνω και στην δεύτερη μπορεί ο πελάτης να επιλέξει αν η διεύθυνση αποστολής του προϊόντος θα είναι ίδια με την διεύθυνση που αναφέρεται στις πληροφορίες χρεώσεις. Αν όχι, μπορεί να πληκτρολογήσει μια νέα διεύθυνση αποστολής και συνεχίζει.



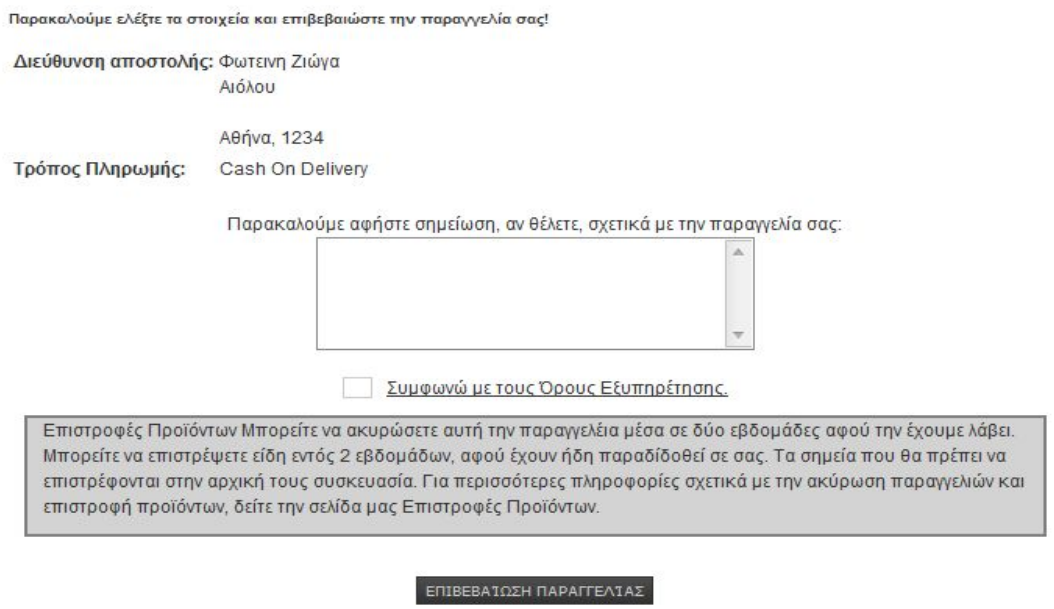
Εικόνα 65: Πληροφορίες Αποστολής προϊόντος, My Design Shop

Στη συνέχεια πρέπει να επιλεγεί ο τρόπος πληρωμής. Όπως αναφέρεται στο κεφάλαιο 5 (ενότητα 5.4) στο www.mydesignshop.eu χρησιμοποιούμαι τρεις διαφορετικές μεθόδους πληρωμής.



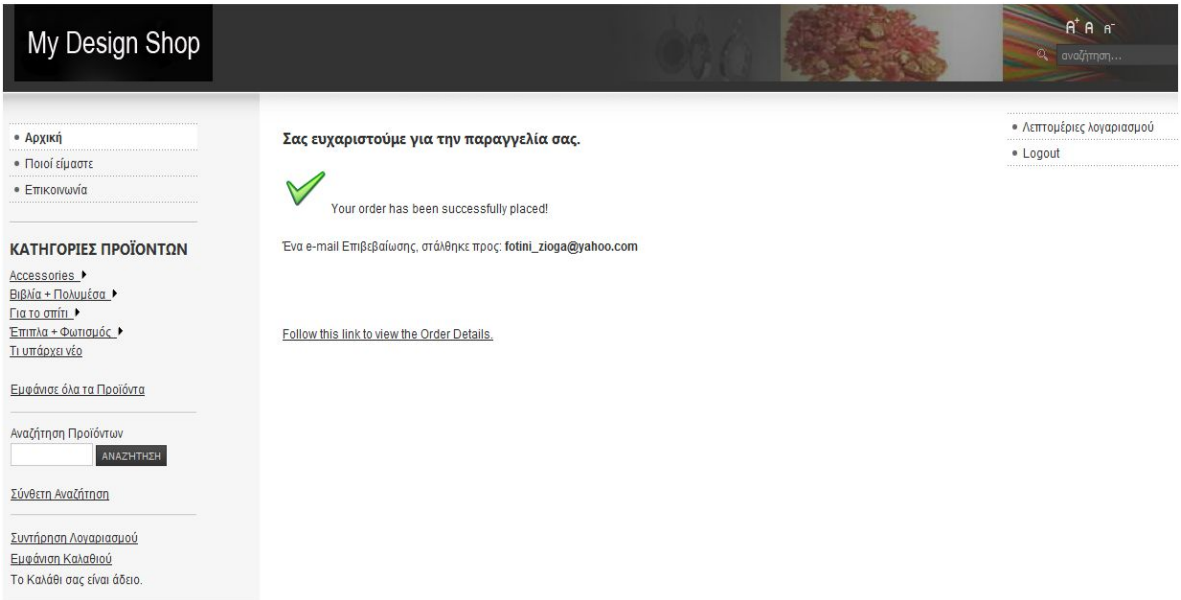
Εικόνα 66: Επιλογή μεθόδου πληρωμής, My Design Shop

Έπειτα, στο τελευταίο στάδιο πριν την ολοκλήρωση της παραγγελίας ο πελάτης μπορεί να αφήσει αν επιθυμεί μία σημείωση σχετικά με την παραγγελία. Επίσης, εμφανίζεται ένα μήνυμα το οποίο αφορά τις συνθήκες που επικρατούν για τις επιστροφές των προϊόντων.



Εικόνα 67: Επιβεβαίωση παραγγελίας, My Design Shop

Αφού επιβεβαιώσει την παραγγελία, εμφανίζεται ένα ευχαριστήριο μήνυμα και η ενημέρωση ότι ένα e-mail επιβεβαίωσης έχει σταλεί στην ηλεκτρονική διεύθυνση που έχει χρησιμοποιηθεί από τον πελάτη.



Εικόνα 68: Μήνυμα επιβεβαίωσης παραγγελίας

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

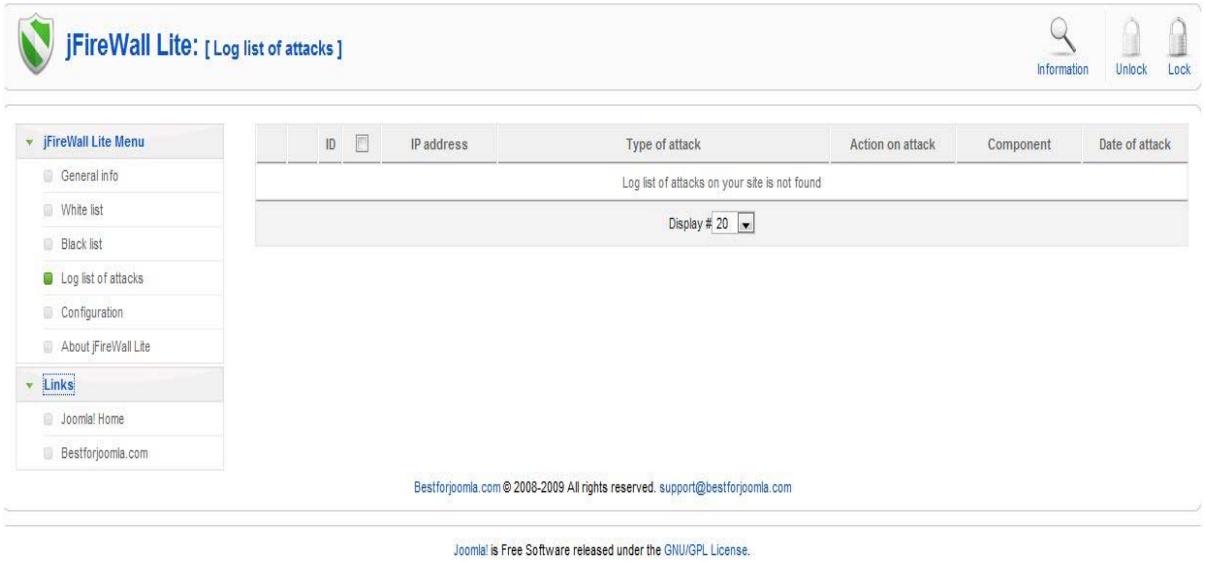
10.3 Modules και components σχετικά με την ασφάλεια που χρησιμοποιήθηκαν στο ηλεκτρονικό κατάστημα

Για την διασφάλιση του ηλεκτρονικού καταστήματος από κακόβουλες επιθέσεις χρησιμοποιήθηκαν διαφορά components, modules, plugins και τεχνικές. Οι τεχνικές που χρησιμοποιήθηκαν αναφέρονται πιο αναλυτικά στο Κεφάλαιο 8. Σε αυτή την παράγραφο γίνεται μια συνοπτική περιγραφή των components, modules, plugins και των τεχνικών που χρησιμοποιήθηκαν.

10.3.1 jFire Wall Litel Component, Plugin, Version 1.0

Είναι ένα εργαλείο που προστατεύει το ηλεκτρονικό κατάστημα από SQL-Injection. Αντιδρά αμέσως σε κάθε απόπειρα επίθεσης από κακόβουλους εισβολείς στην ιστοσελίδα σας και να λαμβάνει μέτρα για να αποκλείσουμε τον εισβολέα από παρόμοια επίθεση στο μέλλον.

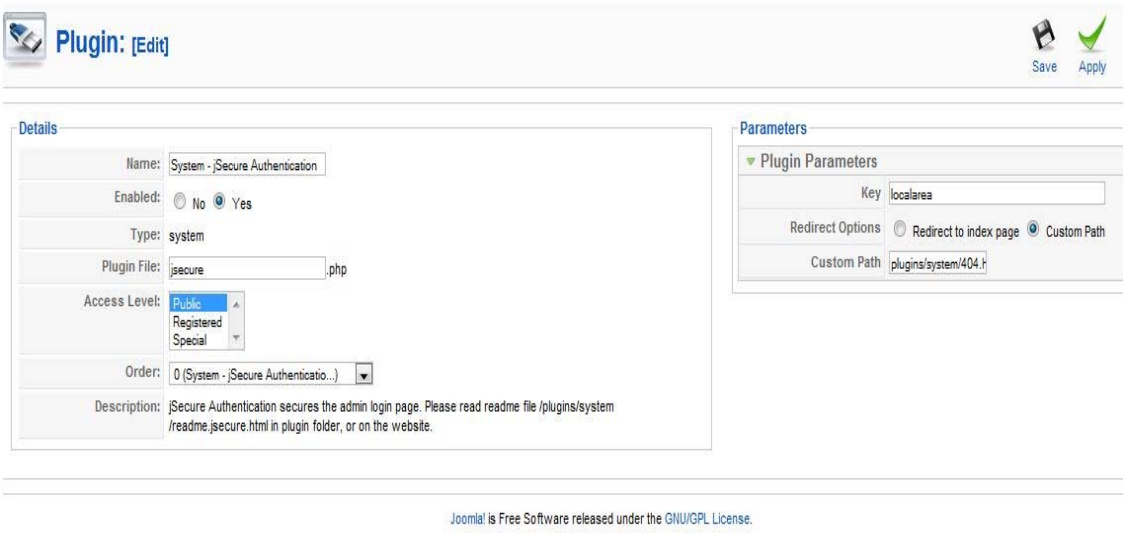
Στο διαχειριστικό κομμάτι του component αυτού μπορούμε να παρακολουθήσουμε στατιστικά στοιχεία με τις επιθέσεις που έχουμε δεχτεί στο ηλεκτρονικό κατάστημα. Αν επισκεφτούμε το μενού την επιλογή "Log list of attacks " παρουσιάζεται μια λίστα με τις IP διευθύνσεις που έχουν επιτεθεί, καθώς και από ποιο μέρος προέρχονται οι συγκεκριμένες διευθύνσεις.



Εικόνα 69: Attack Statistics από το jFireWall Litel Component,

10.3.2 jSecure Authentication Plugin, Version 1.0.9

Σε όλες τις εγκαταστάσεις Joomla ιστοσελίδων, η διεύθυνση που οδηγεί στην διαχείριση είναι κοινή και έχει τη μορφή www.mydesignshop.eu/administrator/. Το συγκεκριμένο plugin μας δίνει την δυνατότητα να προσθέσουμε ένα επίθεμα μετά το www.mydesignshop.eu/administrator/ έτσι ώστε να μην μπορεί ο απλός χρήστης να εισέλθει στη σελίδα διαχείρισης.

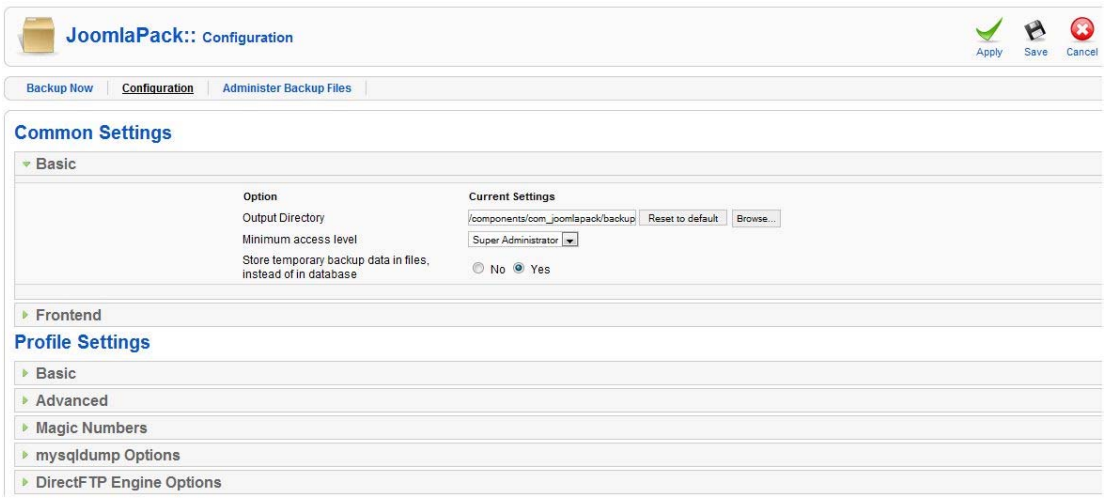


Εικόνα 70: Διαχείριση του jSecure Authentication plugin

Όπως βλέπουμε και στην εικόνα, το επίθεμα που έχουμε επιλέξει είναι "localarea" και η διεύθυνση που οδηγεί στη διαχείριση παίρνει την μορφή www.mydesignshop.eu/administrator/?localarea.

10.3.3 JoomlaPack Component, Version 2.4.1

Η λειτουργία αυτού του component είναι η δημιουργία ενός πλήρους αντιγράφου ασφαλείας του ιστότοπου σε ένα ενιαίο αρχείο. Το αρχείο περιέχει όλα τα αρχεία, ένα στιγμιότυπο βάσης δεδομένων και ένα πρόγραμμα εγκατάστασης που προέρχεται από το πρότυπο πρόγραμμα εγκατάστασης του Joomla. Η δημιουργία αντιγράφων ασφαλείας και η διαδικασία επαναφοράς υποστηρίζεται από AJAX για να αποφευχθούν οι διακοπές του server, ακόμη και σε ιστοτόπους μεγάλους σε μέγεθος αρχείων. Εναλλακτικά, μπορούμε να κάνουμε ένα αντίγραφο ασφαλείας της βάσης δεδομένων μόνο.



Εικόνα 71: Διαχείριση του JoomlaPack Component

Υλοποίηση site με τη χρήση ενός web content management εργαλείου (joomla) και η ασφαλής θωράκισή του.

10.3.4 Redirect Failed Login, Plugin, Version 1.51

Αυτό το plugin μας επιτρέπει να διαχειριστούμε τα logins των χρηστών που απέτυχαν. Μπορεί να αποτρέψει τους κακόβουλους εισβολείς προσθέτοντας μια προγραμματιζόμενη χρονική καθυστέρηση μετά από κάθε αποτυχημένη προσπάθεια σύνδεσης. Επίσης, μπορούμε να ανακατευθύνουμε το ηλεκτρονικό κατάστημα σε μια εντελώς διαφορετική τοποθεσία ή να παραμείνει στην αρχική σελίδα και να εμφανιστεί ένα μήνυμα όπως "Το όνομα χρήστη και ο κωδικός πρόσβασης δεν ταιριάζουν. Δοκιμάστε ξανά.".

Με την χρονική καθυστέρηση που προσθέτει κατά τις αποτυχημένες προσπάθειες σύνδεσης, αποθαρρύνει βίαιες επιθέσεις σύνδεσης στο ηλεκτρονικό κατάστημα. Η καθυστέρηση επιλέγουμε να είναι 10 δευτερόλεπτα.

Επιλέγουμε να μην ανακατευθύνουμε το ηλεκτρονικό κατάστημα σε μια εντελώς διαφορετική τοποθεσία και απλά προσθέτουμε μια χρονική καθυστέρηση, δέκα δευτερολέπτων μετά από αποτυχημένες απόπειρες σύνδεσης. Αυτό θα αποθαρρύνει βίαιες επιθέσεις σύνδεσης στο ηλεκτρονικό κατάστημα. Η χρονική καθυστέρηση συμβάλλει στην προστασία τόσο του Front-end και Back-end.

Εικόνα 72: Διαχείριση του Redirect Failed Login, Plugin.

10.3.5 Τεχνικές διασφάλισης

Επιγραμματικά οι τεχνικές διασφάλισης που χρησιμοποιήθηκαν είναι:

- Αλλαγή του προεπιλεγμένου προθέματος "jos_" στην ονομασία των πινάκων της βάσης δεδομένων κατά την εγκατάσταση του Joomla για την αποφυγή SQL injection.
- Προσθήκη κώδικα ο οποίος καθορίζει τα requests που μπορεί να δεχτεί ο ιστότοπος ανά λεπτό, προς αποφυγή επιθέσεων Denial Of Service.
- Αλλαγή δικαιωμάτων των φακέλων.

- Το προεπιλεγμένο όνομα του διαχειριστή σε Joomla ιστοτόπους είναι admin, δημιουργούμε ένα νέο υπέρ-διαχειριστή (super-administrator) με άλλο όνομα χρήστη και έναν ισχυρό κωδικό πρόσβασης.
- Παραμετροποίηση του αρχείου .htaccess προσθέτοντας τεχνικές οι οποίες θα αυξήσουν την ασφάλεια του ιστοτόπου μας.
- Πρόσθετες ρυθμίσεις ασφαλείας που μπορούν να προσδιοριστούν στο αρχείο php.in.

Βιβλιογραφία

Βιβλία

1. The 2008 Open Source CMS. Market Share Report, **Ric Shreves.**
2. Joomla! Web Security, **Tom Canavan.**
3. Joomla! E-Commerce with VirtueMart, **Suhreed Sarkar.**
4. XSS Attacks, Jeremiah Grossman, **Robert "RSnake" Hansen, Petko "pdp" D. Petkov, Anton Rager.**
5. SQL Injection Attacks and Defense, **Justin Clarke.**

Links

http://www.slideshare.net/toons01/cms-315058

http://www.webmasterslife.gr/joomla-cms/55-Τι-είναι-το-joomla.html

http://www.snek.gr/content/view/13/1/lang,el_GR/

http://techtips.gr/texnologika-nea/2958/2958

http://www.ibm.com

http://www.authorize.net/

http://en.wikipedia.org/wiki/IKobo

http://en.wikipedia.org/wiki/ITransact

http://en.wikipedia.org/wiki/Noce

http://en.wikipedia.org/wiki/PayPal

http://en.wikipedia.org/wiki/WorldPay

http://www.service-architecture.com/
http://www.alpha.gr/

http://www.piraeusbank.gr/

http://en.wikipedia.org/wiki/Denial-of-service_attack#Methods_of_attack

http://www.acunetix.com/websitesecurity/xss.htm

http://www.hacker4lease.com/hidden-manipulation.html

http://el.wikipedia.org/wiki/Packet_sniffer

http://www.securityfocus.com/infocus/1549

http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

http://developer.joomla.org/tutorials/181-preventing-sql-injections.html

http://www.netshinesoftware.com/security/joomla-security.html

http://forum.joomla.gr/viewtopic.php?f=54&t=8932

http://en.wikipedia.org/wiki/Digital_signature

http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

http://el.wikipedia.org/wiki/ψηφιακο_πιστοποιητικο

http://en.wikipedia.org/wiki/Electronic_Data_Interchange

http://en.wikipedia.org/wiki/Secure_Electronic_Transaction