



Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης
Σχολή Μηχανικών Πληροφορικής



Πτυχιακή εργασία

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Ματσάγκος Ηρακλής Χρήστος (ΑΜ 1583)
Μαυρόπουλος Βασίλειος (ΑΜ 2527)

Ηράκλειο 27/6/2014

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τους γονείς μας για την αμέριστη υποστήριξή τους κατά την διάρκεια εκπόνησης της εργασίας αυτής.

Να ευχαριστήσουμε τον καθηγητή κ. Μανιφάβα Χαράλαμπο για την πολύτιμη καθοδήγηση και υποστήριξη του σε όλη τη διάρκεια εκπόνησης της εργασίας αυτής.

Πίνακας Περιεχομένων

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης.....	1
Σχολή Μηχανικών Πληροφορικής.....	1
Πτυχιακή εργασία.....	1
Δημιουργία ηλεκτρονικού καταστήματος σε Joomla.....	1
Μαυρόπουλος Βασίλειος (ΑΜ 2527).....	1
Ηράκλειο 27/6/2014.....	1
Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος.....	1
Ευχαριστίες.....	2
Κεφάλαιο 1 - Εισαγωγή.....	7
1.1 Γενικά.....	7
1.2 Σκοπός.....	7
Κεφάλαιο 2 – Content Management System (CMS).....	8
2.1 Τί είναι CMS.....	8
2.2 Web content management system.....	8
2.3 Γνωριμία με το Joomla.....	8
2.4 Χαρακτηριστικά της πλατφόρμας Joomla.....	9
2.5 Δομή του Joomla.....	9
2.5.1 Front-end και Back-end (Δημόσιο τμήμα και περιοχή διαχείρισης).....	9
2.5.2 Access Rights (Δικαιώματα πρόσβασης).....	9
Κεφάλαιο 3 – Δημιουργία των υποδομών του e-shop.....	11
3.1 Λειτουργικό Σύστημα.....	11
3.2 – Apache PHP PhpMyAdmin.....	15
3.3 – Εγκατάσταση Joomla.....	18
Κεφάλαιο 4 – VirtueMart.....	24
4.1 – Περιγραφή του VirtueMart.....	24
4.2 – Χαρακτηριστικά του VirtueMart.....	24
4.3 – Εγκατάσταση του VirtueMart.....	26
4.4 - Επιλογές ρυθμίσεων του VirtueMart.....	30
4.5 - Χρήστες και ομάδες χρηστών του VirtueMart.....	38
4.6 – Δημιουργία ιστοσελίδας του ηλεκτρονικού καταστήματος.....	41
4.7 – Μέθοδοι Πληρωμής.....	57
Κεφάλαιο 5 – Τράπεζα και ηλεκτρονικές συναλλαγές.....	62
5.1 – Ηλεκτρονικές συναλλαγές μέσα απο τράπεζα.....	62
5.2 – Επιλογές διασύνδεσης με το Πειραιώς Paycenter.....	62
5.3 - Alpha e-Commerce.....	65
Κεφάλαιο 6 – Ηλεκτρονικό εμπόριο και κίνδυνοι.....	68
6.1 – Βασικές έννοιες και αρχές.....	68
6.2 – DoS attack ή DDoS attack.....	69
6.3 – SQL Injection.....	71
6.4 – Phishing.....	72
6.5 - Cross Site Scripting.....	73
6.6 - Hidden Field Manipulation.....	76
6.7 - Cross-Site Request Forgery.....	77
6.8 - S-HTTP και HTTPS.....	78
Κεφάλαιο 7 – Προστασία του ηλεκτρονικού καταστήματος.....	80
7.1 – Προστασία από επιθέσεις SQL injection.....	80
7.2 – Προστασία από επιθέσεις DoS και DDoS.....	83
7.3 – Δημιουργία αντιγράφων ασφάλειας.....	92

7.4 – Δικαιώματα αρχείων και φακέλων.....	93
7.5 – Προτεινόμενες ρυθμίσεις για τα αρχεία htaccess και php.ini.....	95
7.5 - Ψηφιακές Υπογραφές.....	96
7.6 - Ψηφιακό πιστοποιητικό.....	98
7.7 - Secure Sockets Layer.....	98
Πηγές.....	103

Πίνακας Εικόνων

Εικόνα 1: Το λογότυπο Joomla.....	11
Εικόνα 2: Virtual Box με λειτουργικό σύστημα Debian.....	12
Εικόνα 3: Επίσημη σελίδα για το Virtual Box.....	13
Εικόνα 4: Επίσημη σελίδα για την διανομή Debian.....	14
Εικόνα 5: Εγκατάσταση Apache PHP.....	15
Εικόνα 6: Πρόσβαση στο phpMyAdmin.....	17
Εικόνα 7: Η έκδοση Joomla που κατεβάσαμε.....	18
Εικόνα 8: Ετοιμασία του φακέλου www για την εγκατάσταση Joomla.....	19
Εικόνα 9: Δημιουργία της βάσης joomla25.....	20
Εικόνα 10: Οδηγός εγκατάστασης Joomla.....	21
Εικόνα 11: Τέλος οδηγού εγκατάστασης.....	22
Εικόνα 12: Μεταφόρτωση του συστατικού VirtueMart.....	26
Εικόνα 13: Αποσυμπίεση VirtueMart.....	27
Εικόνα 14: Εγκατάσταση του VirtueMart στο Joomla.....	28
Εικόνα 15: Ολοκλήρωση οδηγού εγκατάστασης.....	29
Εικόνα 16: VirtueMart Configuration - Shop.....	30
Εικόνα 17: VirtueMart Configuration - Shopfront.....	31
Εικόνα 18: VirtueMart Configuration - Templates.....	33
Εικόνα 19: VirtueMart Configuration - Pricing.....	34
Εικόνα 20: VirtueMart Configuraion - Checkout.....	35
Εικόνα 21: VirtueMart Configuration - Product Order Settings.....	37
Εικόνα 22: VirtueMart configuration - SEO.....	38
Εικόνα 23: VirtueMart - Shopper Groups list.....	39
Εικόνα 24: VirtueMart - Shopper Fields.....	40
Εικόνα 25: Αρχική μορφή της ιστοσελίδας.....	41
Εικόνα 26: Menu Manager: New Menu Item.....	42
Εικόνα 27: Επιλογή του Menu Item.....	43
Εικόνα 28: Ορισμός αντικειμένου ως αρχική σελίδα.....	44
Εικόνα 29: Η μορφή που πήρε η ιστοσελίδα.....	45
Εικόνα 30: Ορισμός νομισμάτων με τα οποία θα γίνονται οι συναλλαγές.....	46
Εικόνα 31: VirtueMart - Δημιουργία κατηγορίας προϊόντος.....	47
Εικόνα 32: Κατηγορίες προϊόντων ηλεκτρονικού καταστήματος.....	48
Εικόνα 33: Αντιστοίχιση προϊόντων σε κατηγορίες.....	49
Εικόνα 34: VirtueMart - Shipment Method Information.....	50
Εικόνα 35: VirtueMart - Shipment Method Configuraion.....	52
Εικόνα 36: Μορφή ηλεκτρονικού καταστήματος - 1.....	53
Εικόνα 37: Μορφή ηλεκτρονικού καταστήματος - 2.....	54
Εικόνα 38: Μορφή ηλεκτρονικού καταστήματος - 3.....	55
Εικόνα 39: Μορφή ηλεκτρονικού καταστήματος - 4.....	56
Εικόνα 40: VirtueMart - Payment Method Information.....	59
Εικόνα 41: VirtueMart - Payment Method Configuraion.....	60
Εικόνα 42: Λίστα μεθόδων πληρωμής που δημιουργήσαμε.....	61
Εικόνα 43: VPOS redirect - UML Sequence Diagram.....	67
Εικόνα 44: Σχήμα επίθεσης DDoS.....	70
Εικόνα 45: Σχήμα επίθεσης XSS.....	73
Εικόνα 46: Μορφή της σελίδας που επισκεφτήκαμε.....	74
Εικόνα 47: Εμφάνιση φόρμας που δεν προβλέπονταν από τον προγραμματιστή.....	75
Εικόνα 48: Δημιουργία ψευδοτυχαίου προθέματος.....	80

Εικόνα 49: Αλλαγή προθέματος.....	81
Εικόνα 50: Ενημέρωση της πλατφόρμας για το καινούριο πρόθεμα.....	81
Εικόνα 51: Μεταβλητή που περιέχει το όνομα της βάσης.....	92
Εικόνα 52: Προβολή δικαιωμάτων.....	94
Εικόνα 53: Διάγραμμα ψηφιακού πιστοποιητικού.....	97
Εικόνα 54: Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.....	99
Εικόνα 55: Η διαδικασία της χειραψίας των δύο συσκευών σύμφωνα με το πρωτόκολλο SSL.....	101

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Κεφάλαιο 1 - Εισαγωγή

1.1 Γενικά

Τα ηλεκτρονικά καταστήματα κερδίζουν μέρα με την μέρα όλο και μεγαλύτερη αναγνωρισιμότητα για την εξωστρέφεια μιας επιχείρησης ακόμη και στη χώρα μας. Ένα ηλεκτρονικό κατάστημα είναι ένας δικτυακός τόπος, στο οποίο πραγματοποιούνται πωλήσεις οικονομικών αγαθών.

1.2 Σκοπός

Σκοπός αυτής της εργασίας είναι η δημιουργία ενός ηλεκτρονικού καταστήματος χρησιμοποιώντας την πλατφόρμα Joomla!. Στο οποίο θα εφαρμόσουμε όλες τις απαραίτητες τεχνικές και τεχνολογίες έτσι ώστε να παρέχει με ασφάλεια τις υπηρεσίες του. Για να γίνει αυτό εφικτό, εκτός από την δημιουργία του ηλεκτρονικού καταστήματος, θα αναλυθούν τα παρακάτω θέματα:

1. DoS και DdoS attack.
2. SQL injection.
3. Phishing.
4. Cross Site Scripting.
5. Hidden Field Manipulation
6. Cross-Site Request Forgery (CSRF)
7. S-HTTP και HTTPS

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Κεφάλαιο 2 – Content Management System (CMS)

2.1 Τί είναι CMS

Ένα σύστημα διαχείρισης περιεχομένου (cms) είναι ένα λογισμικό, σκοπός του οποίου είναι η δημοσίευση, διαχείριση και επεξεργασία περιεχομένου μέσα από μια κεντρική διεπαφή. Επίσης ένα CMS προσφέρει διαχείριση ροών εργασιών σε ένα συνεργατικό περιβάλλον. Οι τρεις κύριες κατηγορίες των συστημάτων διαχείρισης περιεχομένου είναι:

- Web content management system.
- Component content management system.
- Enterprise content management system.

Για την εργασία αυτή θα μας απασχολήσει η πρώτη κατηγορία, η Web content management system.

2.2 Web content management system

Ένα web CMS είναι λογισμικό που χρησιμοποιείται για την δημιουργία, διαχείριση, αποθήκευση και ανάπτυξη περιεχομένου πάνω σε σελίδες διαδικτύου.

Το διαδικτυακό περιεχόμενο μπορεί να περιλαμβάνει κείμενο, ενσωματωμένα γραφικά, φωτογραφίες, ήχο, βίντεο και κώδικα (π.χ. για εφαρμογές) που προβάλλει περιεχόμενο ή αλληλεπιδρά με τον χρήστη.

2.3 Γνωριμία με το Joomla.

Το Joomla είναι ένα παγκοσμίως αναγνωρισμένο cms που χρησιμοποιείται εκτενώς για τη δημιουργία διαδικτυακού περιεχομένου και εφαρμογών.

Το διακρίνει η ευκολία χειρισμού και η επεκτασιμότητά του. Επίσης διατίθεται δωρεάν και είναι ανοιχτού κώδικα. Κάποιες από τις εφαρμογές της πλατφόρμας περιλαμβάνουν:

- Εταιρικές ιστοσελίδες ή πύλες (portals).
- Εταιρικά intranets και extranets.
- Online περιοδικά, εφημερίδες και δημοσιεύσεις.
- Ηλεκτρονικό εμπόριο.
- Ιστοσελίδες μικρών και μεσαίων επιχειρήσεων.
- Ιστοσελίδες μη κερδοσκοπικών οργανισμών.
- Προσωπικές ιστοσελίδες.

Το Joomla ως ελεύθερο λογισμικό και ανοιχτού κώδικα προσφέρει τα εξής κύρια πλεονεκτήματα:

- Μηδενικό κόστος απόκτησης του λογισμικού.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Πληρώνεις μόνο για την υπηρεσία και την υποστήριξη που σου παρέχεται
- Ευκολία παραμετροποίησης
- Πιο ασφαλές, με την λογική πως αφού έχουμε πρόσβαση στον πηγαίο κώδικα του λογισμικού, τότε θα έχουμε πλήρη έλεγχο των λειτουργιών του.

2.4 Χαρακτηριστικά της πλατφόρμας Joomla.

- Οι τεχνολογίες που χρησιμοποιεί, για την προγραμματιστική λογική php, για σύστημα διαχείρισης βάσεων δεδομένων mySQL ή MSSQL ή PostgreSQL, xml, css και δυνατότητα RSS.
- Γρήγορη φόρτωση της σελίδας χρησιμοποιώντας page caching και GZIP page compression.
- Debugging mode και αναφορά σφαλμάτων.
- Είναι πολυγλωσσικό
- Δυνατότητα πολλών επιπέδων χρηστών
- Ευκολία στη χρήση, ακόμη και από αρχάριους χρήστες.

2.5 Δομή του Joomla.

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

Γενικά ένα Web CMS αποτελείται από δύο τμήματα, το front-end και το back-end. Το δημόσιο τμήμα (front-end) είναι το τμήμα το οποίο προβάλλεται προς τα έξω. Δηλαδή είναι προσβάσιμο από τους τελικούς χρήστες της σελίδας (απλοί επισκέπτες και εγγεγραμμένοι χρήστες). Μέσα στο δημόσιο τμήμα βρίσκονται το περιεχόμενο και η διεπαφή της σελίδας.

Σε αντίθεση με το δημόσιο τμήμα, η περιοχή διαχείρισης είναι προσβάσιμη μόνο σε εξουσιοδοτημένους χρήστες. 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 μέρος.

Το back-end βρίσκεται σε διαφορετική διεύθυνση URL από την ιστοσελίδα.

2.5.2 Access Rights (Δικαιώματα πρόσβασης)

Το Joomla ελέγχει την πρόσβαση στις περιοχές και χαρακτηριστικά μιας σελίδας μέσα από έναν μηχανισμό ACL (Access Control Level) με όνομα Groups. Συγκεκριμένα groups έχουν συγκεκριμένα χαρακτηριστικά πρόσβασης και είναι άμεσα σχετιζόμενα με την

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

δημιουργία, επεξεργασία και δημοσίευση περιεχομένου (μέσα από τις front-end και back-end διεπαφές) καθώς και να έχουν πρόσβαση στην Administrative back-end διεπαφή.

Κάθε group έχει διαφορετικά δικαιώματα πρόσβασης και όταν ένας χρήστης γίνει μέλος αυτού του group τότε κληρονομεί αυτά τα δικαιώματα

Υπάρχουν τέσσερα front-end groups διαθέσιμα:

- Registered – Αυτό το group επιτρέπει τον χρήστη να συνδεθεί στη front-end διεπαφή. Οι χρήστες αυτού του group δεν μπορούν να συμβάλουν στο περιεχόμενο, αλλά μπορεί να τους επιτραπεί η πρόσβαση σε άλλες περιοχές, όπως ένα forum.
- Author – Αυτό το group επιτρέπει τον χρήστη την τοποθέτηση περιεχομένου, συνήθως μέσα από ένα σύνδεσμο από το User Menu. Μπορεί να υποβάλει καινούριο περιεχόμενο, να αλλάξει τις επιλογές που θα εμφανιστεί το αντικείμενο στο front page και να διαλέξει ημερομηνίες δημοσίευσης αλλά δεν μπορούν άμεσα να δημοσιεύσουν περιεχόμενο. Όταν κάποιο περιεχόμενο υποβάλλεται από έναν χρήστη αυτού του group για δημοσίευση, λαμβάνει ένα σχετικό μήνυμα που τον ενημερώνει πως το υποψήφιο προς δημοσίευση περιεχόμενό του θα περάσει από αξιολόγηση.
- Editor – Αυτό το group δίνει το επιπλέον δικαίωμα στο χρήστη να επεξεργαστεί οπουδήποτε (όχι μόνο το δικό του) περιεχόμενο από το front-end. Επίσης μπορεί να επεξεργαστεί περιεχόμενο που δεν έχει ακόμη δημοσιευτεί.
- Publisher – Αυτό το group δίνει το δικαίωμα στο χρήστη να υποβάλει, επεξεργαστεί και δημοσιεύσει οποιοδήποτε (όχι μόνο το δικό του) περιεχόμενο από το front-end. Οι χρήστες αυτοί μπορούν να αξιολογήσουν όλα τα άρθρα, να επεξεργαστούν και να αλλάξουν τις επιλογές δημοσίευσης αλλά και να αποφασίσουν πότε ένα άρθρο είναι έτοιμο για δημοσίευση, κάνοντάς το ορατό στο εγγεγραμμένο ή όχι κοινό.

Υπάρχουν τρία groups διαχείρισης που επιτρέπουν πρόσβαση στο Joomla.

- Manager – Αυτό το group επιτρέπει πρόσβαση στη δημιουργία περιεχομένου και πληροφορίες συστήματος που αφορούν το back-end. Ένας χρήστης του group αυτού είναι επί της ουσίας publisher με back-end προσβασιμότητα. Μπορεί να συνδεθεί μέσα από την διεπαφή του διαχειριστή, αλλά τα δικαιώματα του και η προσβασιμότητα του περιορίζονται στη διαχείριση περιεχομένου. Μπορεί να δημιουργήσει ή να επεξεργαστεί οποιοδήποτε περιεχόμενο και να έχει πρόσβαση σε μερικά μόνο μέρη του back-end, όπως η προσθήκη, διαγραφή και επεξεργασία περιοχών και κατηγοριών του Front Page και των μενού, αλλά δεν έχει πρόσβαση στους μηχανισμούς του Joomla ή να εγκαταστήσει components και modules. Επίσης εάν ένας manager συνδεθεί μέσα από τη διεπαφή του front-end, τότε αντιμετωπίζεται όπως ένας χρήστης publisher, με τα ίδια δικαιώματα και προσβασιμότητα.
- Administrator – Αυτό το group επιτρέπει την πρόσβαση σε πολλές διαχειριστικές διεργασίες. Ένας χρήστης administrator έχει όλα τα προνόμια ενός χρήστη manager, αλλά έχει το δικαίωμα επίσης να ενεργοποιεί επιλογές, να εγκαταστήσει

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

ή να διαγράψει componets, modules και bots και να προβάλει τα στατιστικά χρήσης. Αυτό που δεν μπορεί να κάνει όμως είναι η επεξεργασία ή εγκατάσταση Site Template και να κάνει αλλαγές στις επιλογές του Global configuration. Αν συνδεθεί μέσα από το front-end, τότε αντιμετωπίζεται ως Publisher, όπως θα γινόταν με τον χρήστη Manager. Επίσης όταν ένας χρήστης Administrator ανοίξει την λίστα User manager, θα δει τους χρήστες και τα δικαιώματά τους, καθώς μπορεί και να τα αλλάξει εκτός του Super Administrator.

- Super Administrator - Αυτό το group επιτρέπει πρόσβαση σε όλες τις διαχειριστικές διεργασίες. Μόνο ένας χρήστης μπορεί να δημιουργήσει ή να αλλάξει έναν λογαριασμό Super Administrator.



Joomla!™

Εικόνα 1: Το λογότυπο Joomla

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Κεφάλαιο 3 – Δημιουργία των υποδομών του e-shop

3.1 Λειτουργικό Σύστημα

Το λειτουργικό σύστημα που θα χρησιμοποιήσουμε σε αυτή την πτυχιακή εργασία είναι το Debian 7.5 (wheezy) το οποίο το θα τρέχει σε μια εικονική μηχανή Virtual Box.



Εικόνα 2: Virtual Box με λειτουργικό σύστημα Debian

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

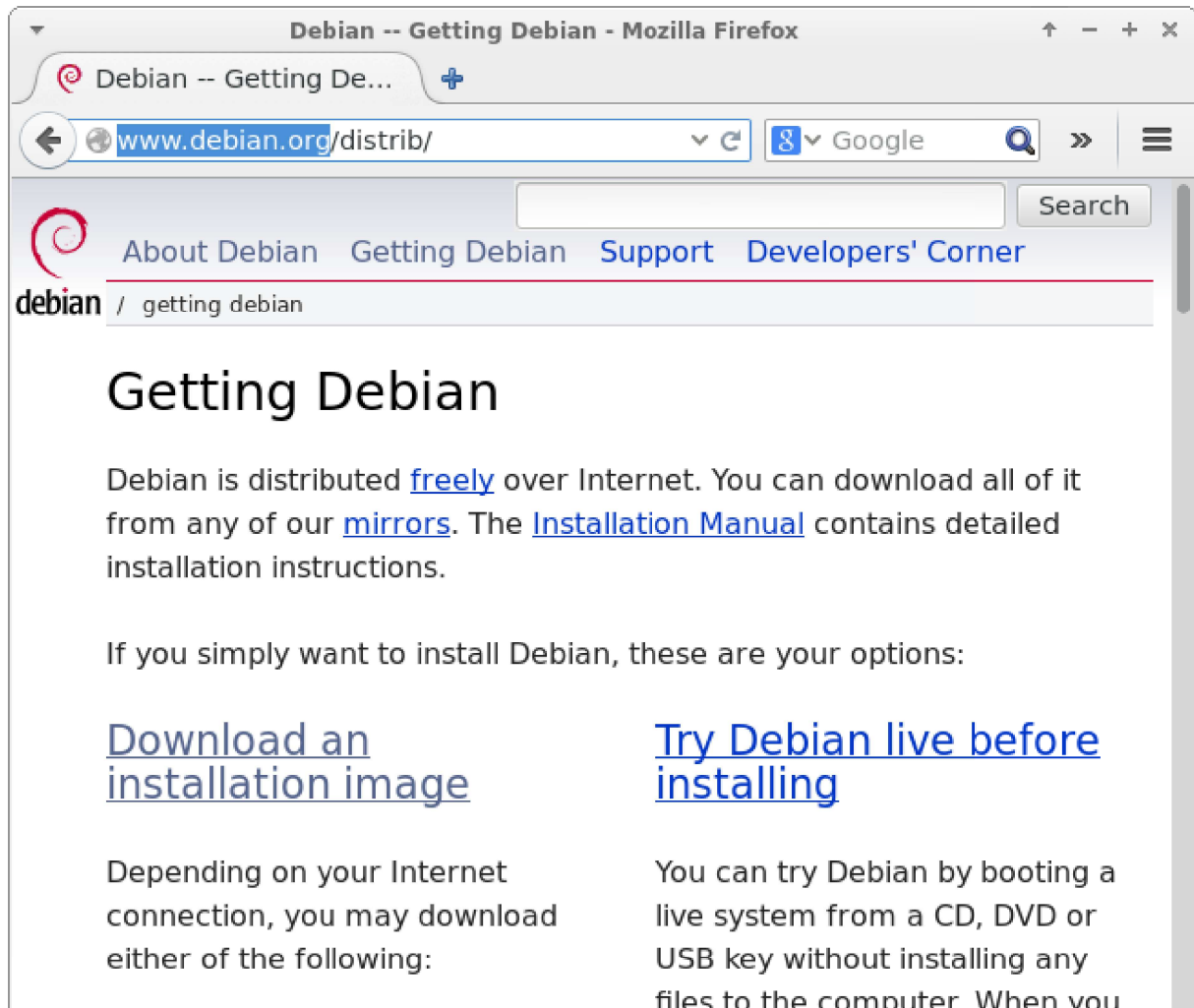
Για να στήσουμε το σύστημα αυτό χρειάστηκε να κατεβάσουμε το Virtual Box από την επίσημη σελίδα www.virtualbox.org.



Εικόνα 3: Επίσημη σελίδα για το Virtual Box

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Επίσης κατεβάσαμε και ένα αντίγραφο της διανομής Linux Debian από την επίσημη σελίδα <http://www.debian.org>.



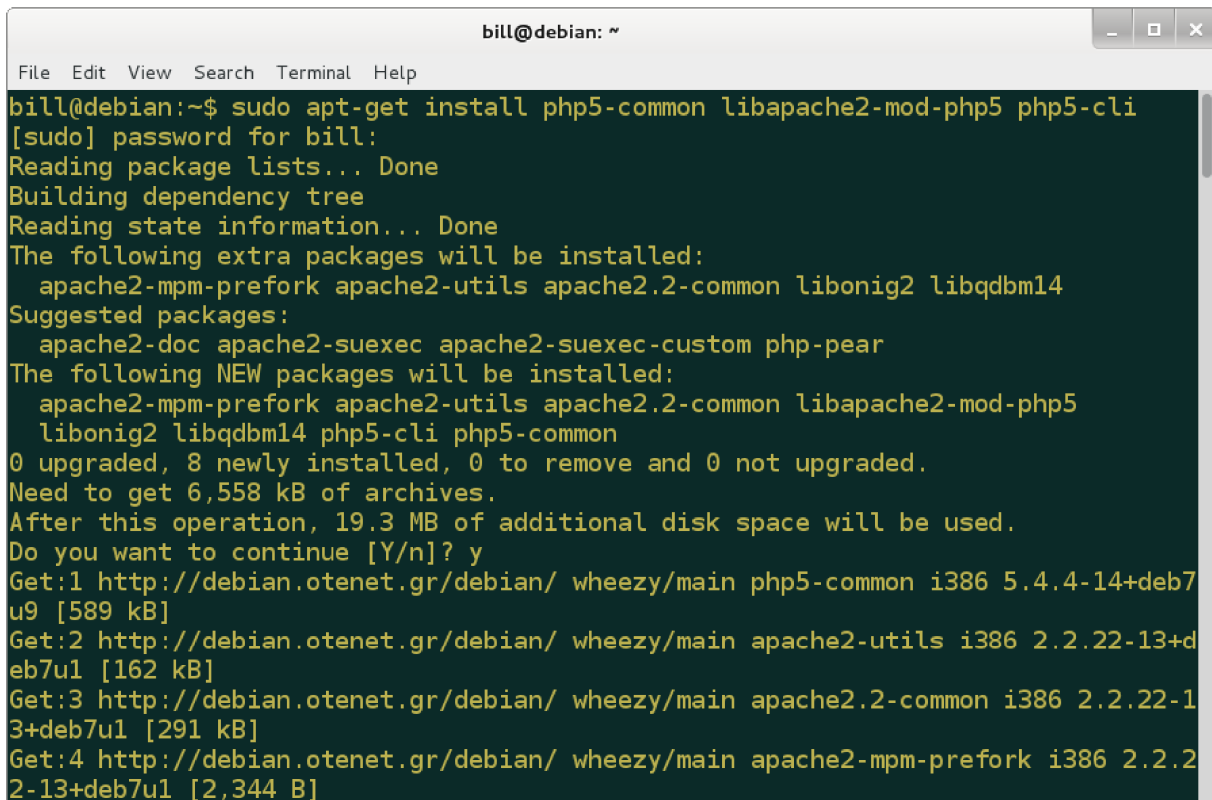
Εικόνα 4: Επίσημη σελίδα για την διανομή Debian

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

3.2 – Apache PHP PhpMyAdmin

Αφού λοιπόν τελειώσαμε με την εγκατάσταση των δύο παραπάνω, ενημερώσαμε το λειτουργικό σύστημα. Μετά περάσαμε με την εγκατάσταση του http server και της php. Για να το κάνουμε αυτό χρησιμοποίησαμε τις παρακάτω εντολές στο τερματικό.

```
apt-get install php5-common libapache2-mod-php5 php5-cli  
apt-get install php5-mysql php5-curl
```



```
bill@debian: ~  
File Edit View Search Terminal Help  
bill@debian:~$ sudo apt-get install php5-common libapache2-mod-php5 php5-cli  
[sudo] password for bill:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following extra packages will be installed:  
  apache2-mpm-prefork apache2-utils apache2.2-common libonig2 libqdbm14  
Suggested packages:  
  apache2-doc apache2-suexec apache2-suexec-custom php-pear  
The following NEW packages will be installed:  
  apache2-mpm-prefork apache2-utils apache2.2-common libapache2-mod-php5  
  libonig2 libqdbm14 php5-cli php5-common  
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.  
Need to get 6,558 kB of archives.  
After this operation, 19.3 MB of additional disk space will be used.  
Do you want to continue [Y/n]? y  
Get:1 http://debian.otenet.gr/debian/ wheezy/main php5-common i386 5.4.4-14+deb7  
u9 [589 kB]  
Get:2 http://debian.otenet.gr/debian/ wheezy/main apache2-utils i386 2.2.22-13+d  
eb7u1 [162 kB]  
Get:3 http://debian.otenet.gr/debian/ wheezy/main apache2.2-common i386 2.2.22-1  
3+deb7u1 [291 kB]  
Get:4 http://debian.otenet.gr/debian/ wheezy/main apache2-mpm-prefork i386 2.2.2  
2-13+deb7u1 [2,344 B]
```

Εικόνα 5: Εγκατάσταση Apache PHP

Ύστερα εγκαταστήσαμε τον server της βάσης δεδομένων, τον mySQL, και το phpMyAdmin για την απομακρυσμένη διαχείρισής της. Για να δουλέψουν μαζί ο mySQL, phpMyAdmin, Apache χρειάστηκε με την βοήθεια του τερματικού να κάνουμε τα εξής:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
sudo apt-get install phpmyadmin
```

Βάλουμε το phpMyAdmin στο αρχείο config του Apache και τον επανεκινήσαμε.

```
sudo nano /etc/apache2/apache2.conf
Include /etc/phpmyadmin/apache.conf
sudo service apache2 restart
```

Εδώ πρέπει να πούμε πως υπάρχει περίπτωση κενού ασφαλείας λόγω του phpMyAdmin το οποίο να δίνει root πρόσβαση στο σύστημά μας. Για να αποφύγουμε ένα μεγάλο μέρος των επιθέσεων μπορούμε να κλειδώσουμε την πρόσβαση στη login σελίδα του phpMyAdmin. Ξανά λοιπόν με την βοήθεια ενός τερματικού ακολουθήσαμε την εξής διαδικασία:

```
sudo nano /etc/phpmyadmin/apache.conf
```

Κάτω απο την περιοχή του directory προσθέσαμε την γραμμή “AllowOverride All” κάτω από το Directory Index, κάνοντάς την περιοχή να φαίνεται ως εξής:

```
<Directory /usr/share/phpmyadmin>
    Options FollowSymLinks
    DirectoryIndex index.php
    AllowOverride All
    [...]
```

Μετά δημιουργήσαμε την σελίδα .htaccess μέσα στον κατάλογο του phpMyAdmin

```
sudo nano /usr/share/phpmyadmin/.htaccess
```

Μέσα στην σελίδα βάλαμε τις εξής γραμμές:

```
AuthType Basic
AuthName "Restricted Files"
AuthUserFile /etc/passwords/.htpasswd
Require valid-user
```

Επεξήγηση των γραμμών που γράψαμε:

- AuthType: Αναφέρεται στην πιστοποίηση που θα χρησιμοποιηθεί για τον έλεγχο των κωδικών. Οι κωδικοί ελέγχονται χρησιμοποιώντας HTTP.
- AuthName: Η γραμμή αυτή περιέχει το μήνυμα που θα εμφανιστεί ως ερώτηση για τον κωδικό πρόσβασης.
- AuthUserFile: Αυτή η γραμμή δηλώνει τη διαδρομή του αρχείου κωδικών (το οποίο

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

το δημιουργούμε στο επόμενο βήμα).

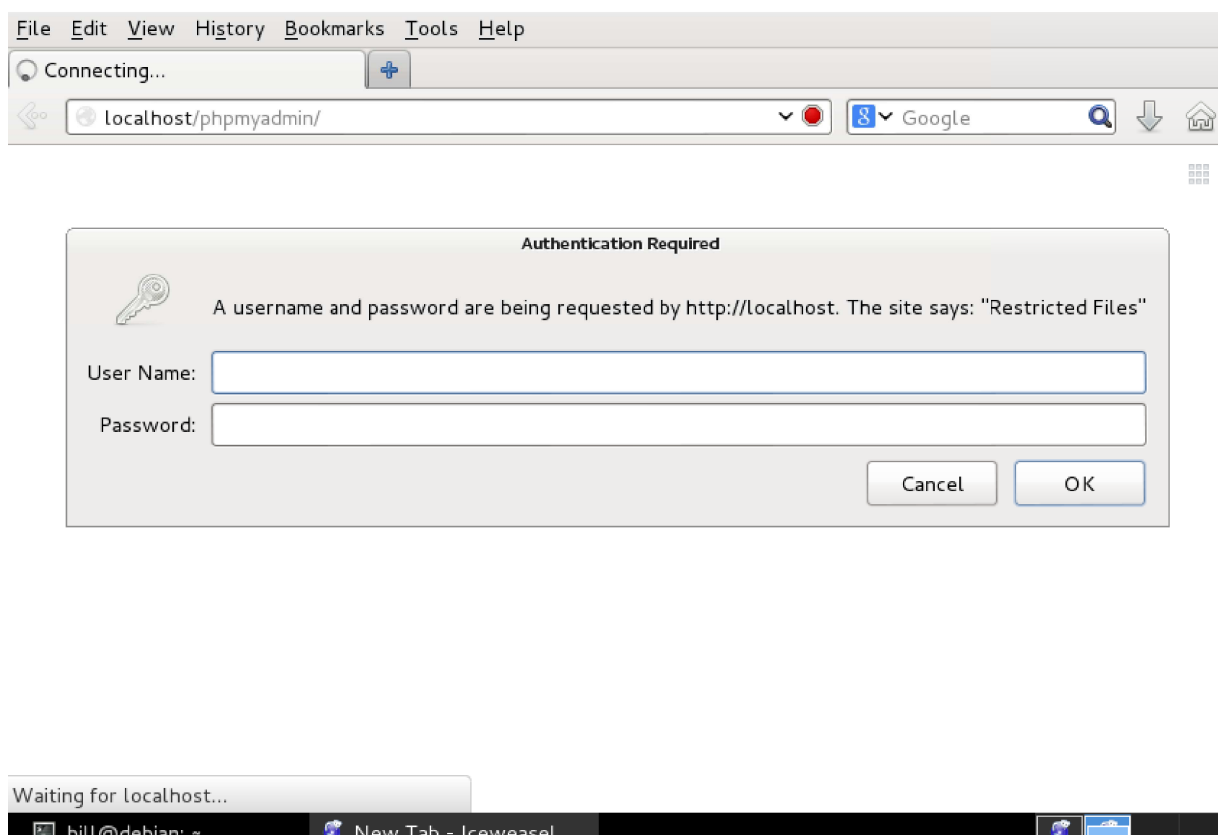
- **Require valid-user:** Αυτή η γραμμή δηλώνει πως μόνο οι χρήστες που είναι δηλωμένοι στο αρχείο κωδικών μπορούν να έχουν πρόσβαση στη login σελίδα του phpMyAdmin.

Τέλος δημιουργούμε το αρχείο κωδικών και επανεκινούμε τον server.

```
sudo htpasswd -c /etc/passwords .htpasswd
```

```
sudo service apache2 restart
```

Τώρα αν γράψουμε στην γραμμή διεθύνσεων του browser localhost/phpmyadmin πριν εμφανιστεί η σελίδα πρόσβασης του phpMyAdmin θα μας εμφανιστεί το μήνυμα που ρυθμίσαμε στα προηγούμενα βήματα.



Εικόνα 6: Πρόσβαση στο phpMyAdmin

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

3.3 – Εγκατάσταση Joomla

Η επιλογή της έκδοσης του Joomla έγινε με βάση τη συμβατότητα της επέκτασης VirtueMart η οποία υποστηρίζει την έκδοση Joomla 2.5(LTS). Η τελευταία έκδοση που θα υποστηρίζει το VirtueMart είναι η Joomla 3.5(LTS) αλλά κατά τη διάρκεια δημιουργίας της πτυχιακής αυτής, δεν έχει εκδοθεί ακόμη.

Για το λόγο αυτό κατεβάσαμε από την επίσημη σελίδα την έκδοση Joomla 2.5(LTS) και αποσυμπιέσαμε το αρχείο.

Download Joomla! 2.5.x

Joomla 2.5 is the previous version of Joomla, which will be supported until December 31, 2014. For upgrade instructions to Joomla 3, please see the FAQs below.



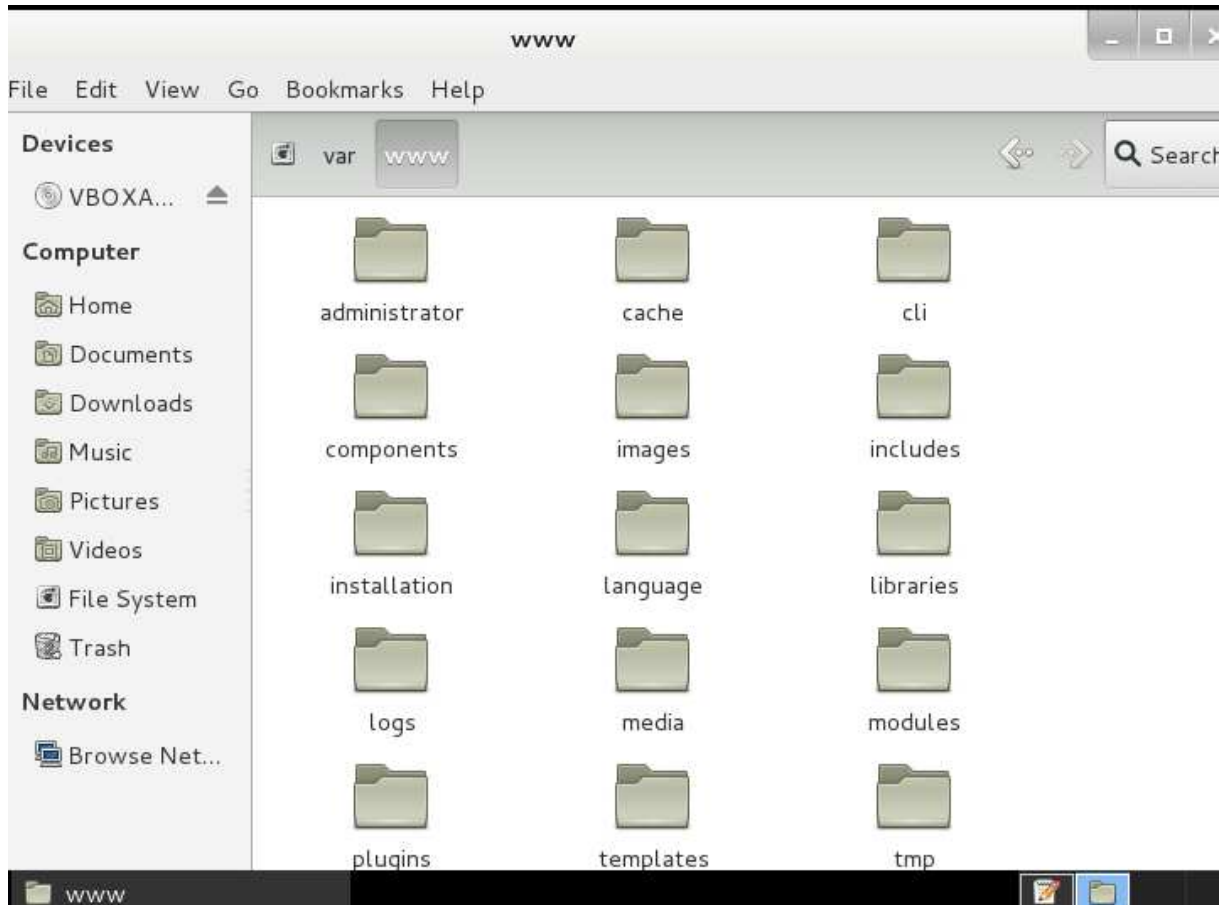
[Other Joomla 2.5.x packages »](#)

[Release Notes »](#)

Εικόνα 7: Η έκδοση Joomla που κατεβάσαμε

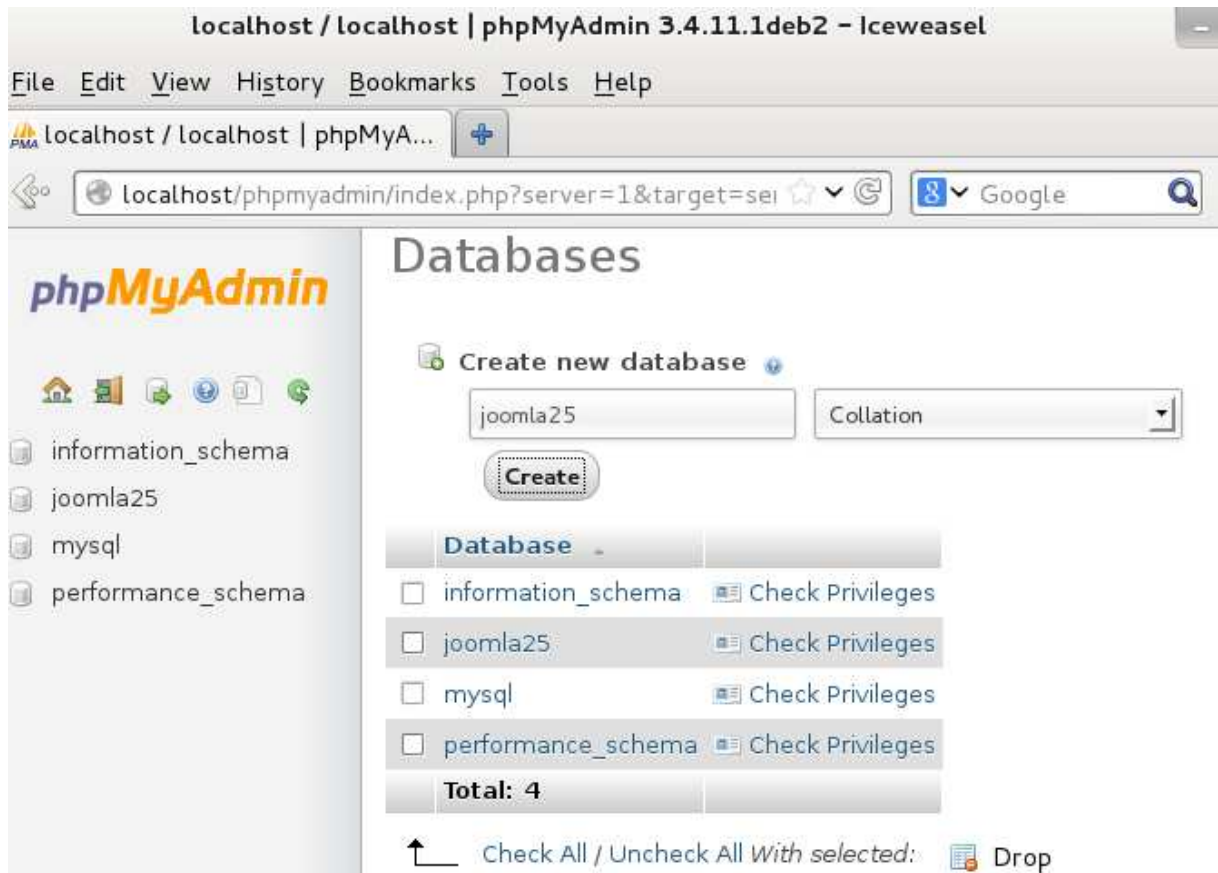
Μετά μεταφέραμε τα αποσυμπιεσμένα αρχεία μέσα στο φάκελο www και δημιουργήσαμε μία βάση στον mySQL server με όνομα joomla25.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 8: Ετοιμασία του φακέλου www για την εγκατάσταση Joomla

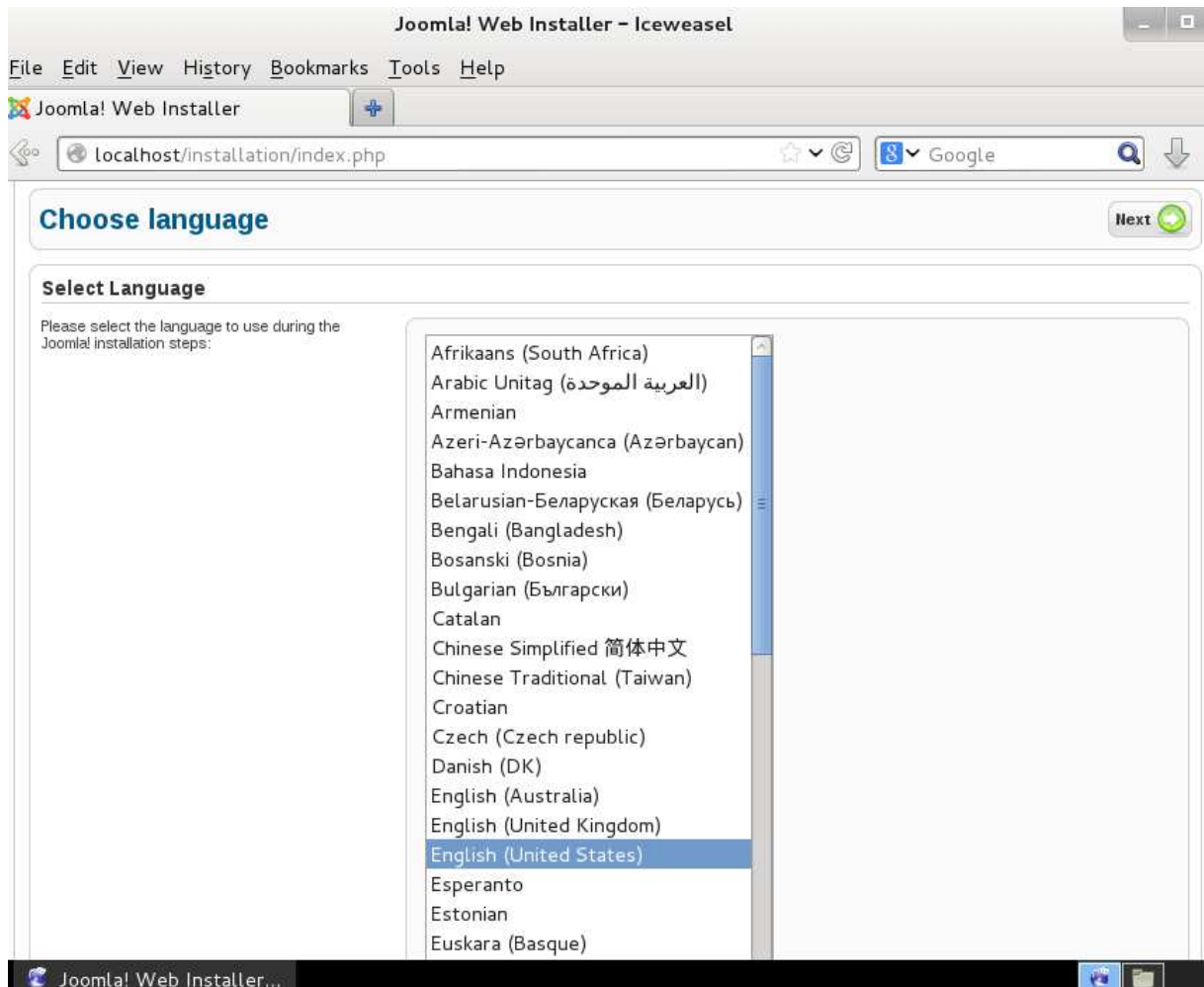
Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 9: Δημιουργία της βάσης joomla25

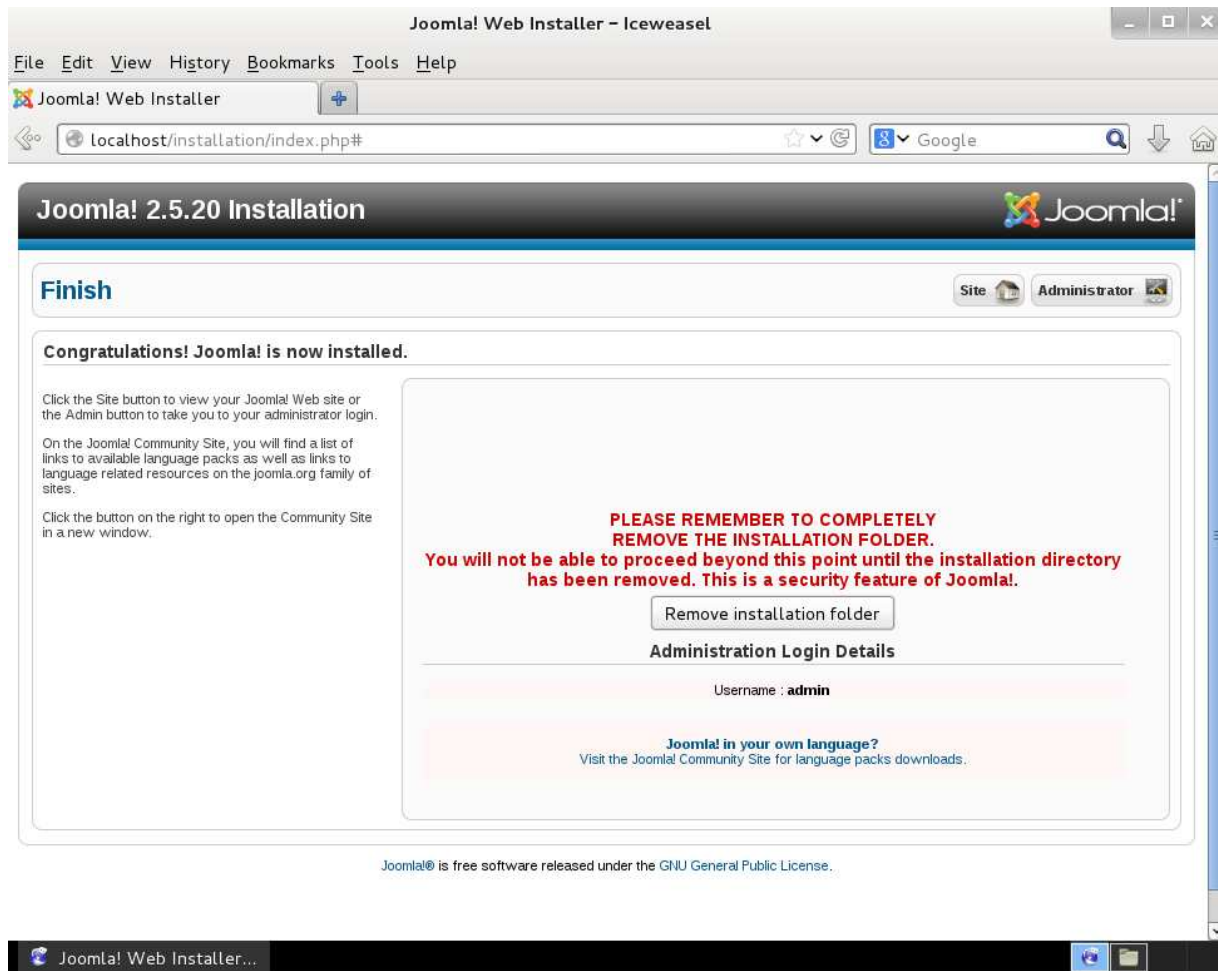
Είμαστε έτοιμοι για να ξεκινήσουμε την εγκατάσταση. Οπότε ανοίγουμε έναν browser και στην γραμμή διευθύνσεων γράφουμε localhost και πατάμε enter για να εκινήσουμε τον οδηγό εγκατάστασης.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 10: Οδηγός εγκατάστασης Joomla

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



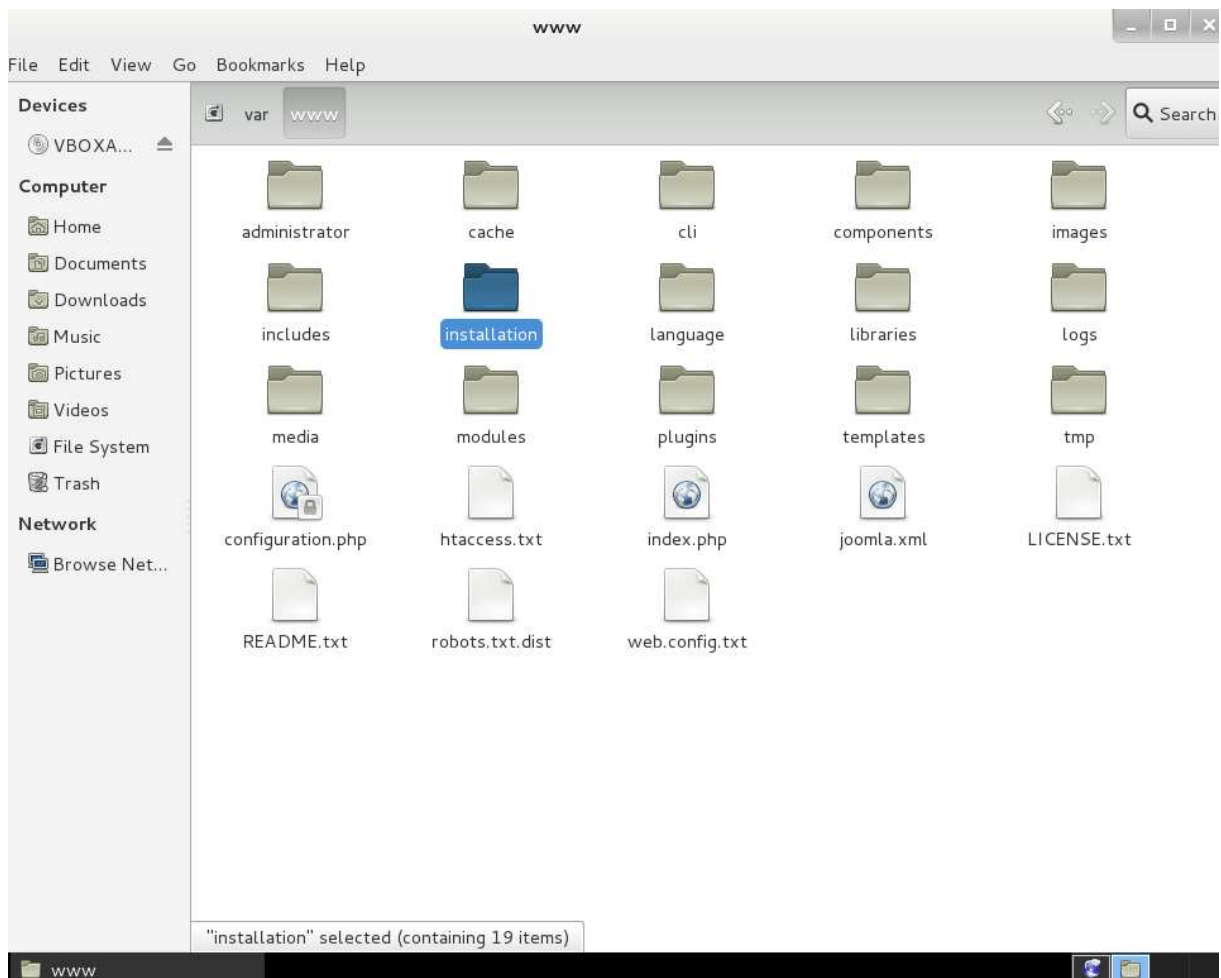
Εικόνα 11: Τέλος οδηγού εγκατάστασης

Λίγο πριν την ολοκλήρωση της εγκατάστασης, ο οδηγός μας λέει πως πρέπει να διαγράψουμε το φάκελο “installation”, ένας λόγος που μας το λέει αυτό είναι πως, αν σε περίπτωση που κάποιος αποκτήσει πρόσβαση στο φάκελο αυτό, μπορεί να εκινήσει τον οδηγό εγκατάστασης από την αρχή. Έτσι η σελίδα μας θα αντικατασταθεί με την αρχική.

Σε εμάς ο οδηγός απέτυχε να διαγράψει το φάκελο αυτό, οπότε θα πρέπει να το κάνουμε χειροκίνητα.

Έτσι λοιπόν ανοίγουμε τον φάκελο “www” και εντοπίζουμε τον φάκελο “installation” και τον διαγράφουμε.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Κεφάλαιο 4 – VirtueMart

4.1 – Περιγραφή του VirtueMart

Το VirtueMart, πρώην γνωστό ως mambo-phpShop είναι μια λύση ηλεκτρονικού εμπορίου, ανοιχτού κώδικα σχεδιασμένη ως επέκταση των Mambo και Joomla συστημάτων διαχείρισής περιεχομένου. Το VirtueMart είναι γραμμένο στην γλώσσα php και προαπαιτεί το σύστημα διαχείρισής βάσεων δεδομένων MySQL για την αποθήκευση και διαχείριση πληροφορίας.

Το VirtueMart, είχε ξεκινήσει ως απόγονος της αυτοδύναμης web εφαρμογής ηλεκτρονικού εμπορίου, phpShop. Πέρνοντας το όνομα mambo-phpShop έγινε συστατικό τοθ συστήματος διαχείρισής περιεχομένου Mambo. Αργότερα η κοινότητα ανάπτυξης το μετέφερε στο Joomla όπου και πήρε το όνομα VirtueMart.

4.2 – Χαρακτηριστικά του VirtueMart

- 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).

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).

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Δίνει τη δυνατότητα της γρήγορης αναζήτησης ανά προϊόντα, κατηγορίες και κατασκευαστές προϊόντων, φιλτράροντάς τα αναλόγως με τα χαρακτηριστικά τους ή με εκπαιδευτικά 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 διαχείρισής:

- 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 πίνακα 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.

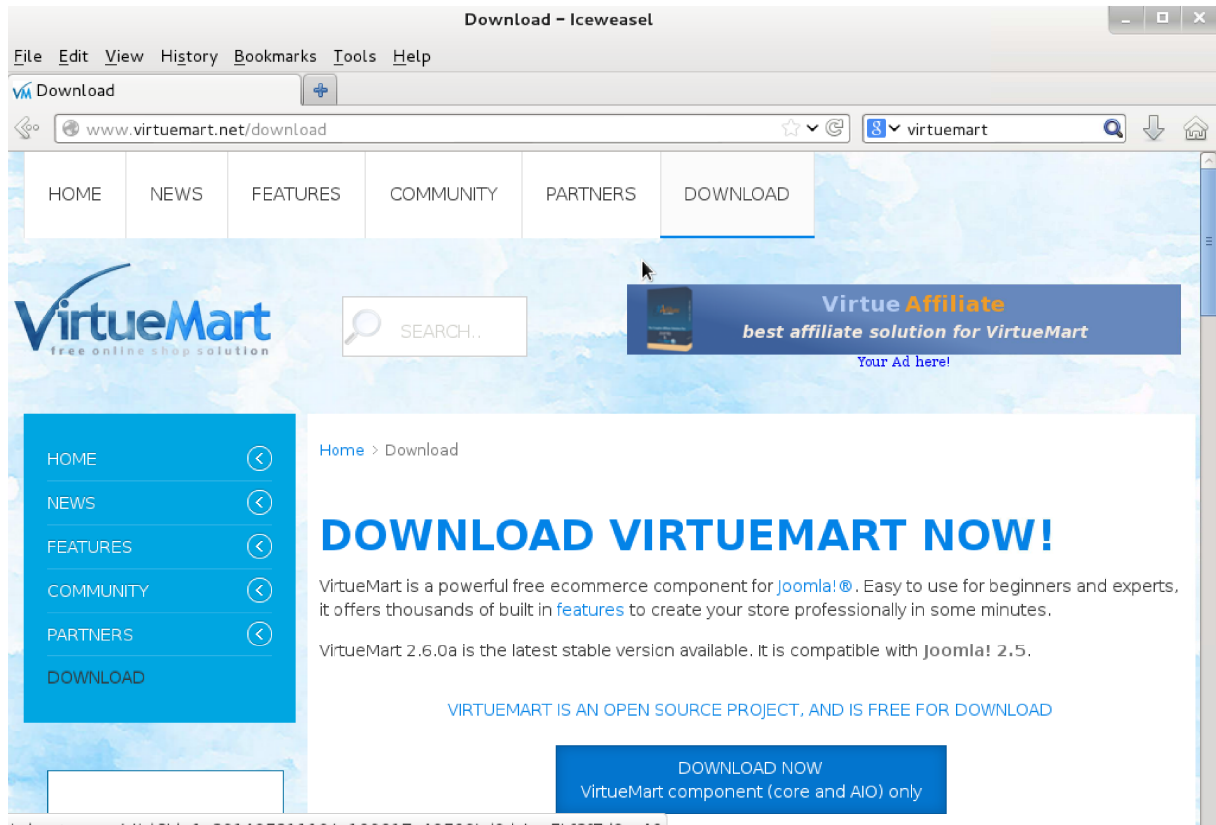
Τα modules πληρωμής μπορούν να διαμορφωθούν ως εξής:

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

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

4.3 – Εγκατάσταση του VirtueMart

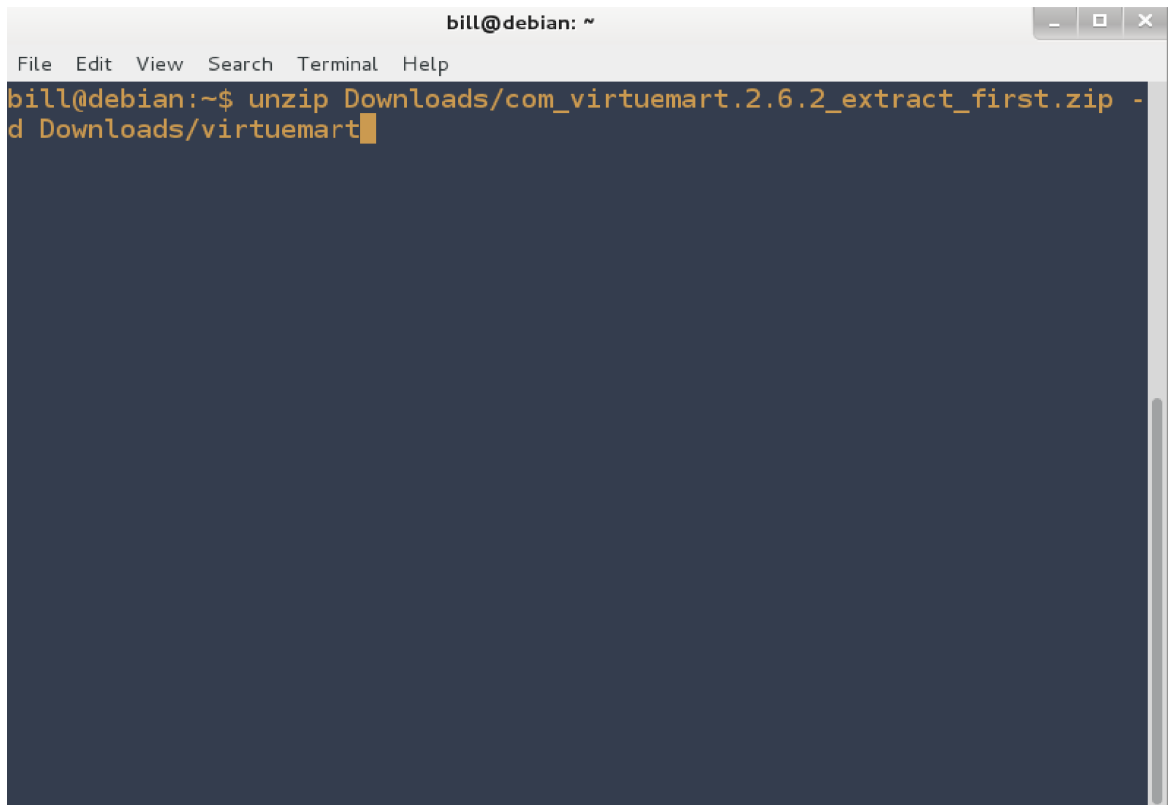
Αρχικά πρέπει να κατεβάσουμε το συστατικό VirtueMart από την επίσημη σελίδα.



Εικόνα 12: Μεταφόρτωση του συστατικού VirtueMart

Μετά αποσυμπιέζουμε το αρχείο που κατεβάσαμε.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

A terminal window titled "bill@debian: ~" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows the command: "bill@debian:~\$ unzip Downloads/com_virtuemart.2.6.2_extract_first.zip -d Downloads/virtuemart" with a cursor at the end of the second line.

```
bill@debian:~$ unzip Downloads/com_virtuemart.2.6.2_extract_first.zip -  
d Downloads/virtuemart
```

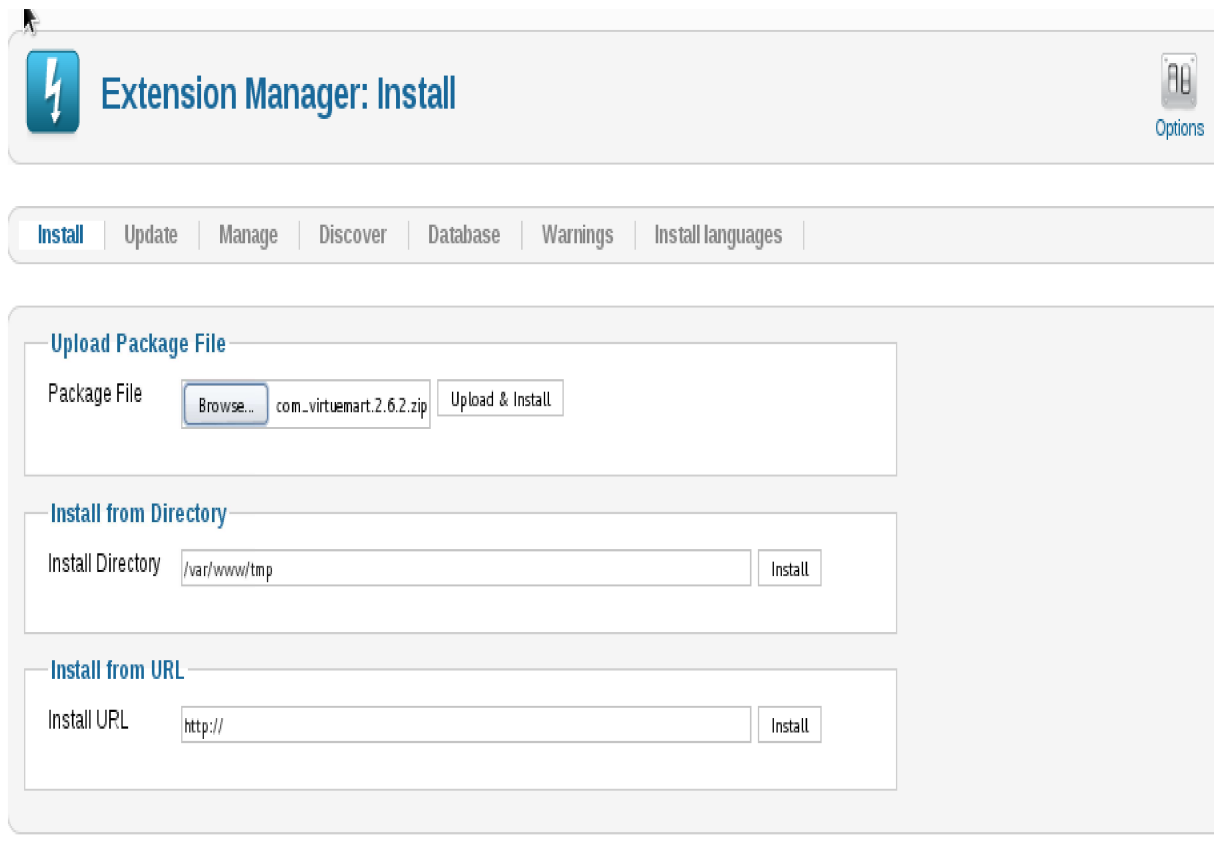
Εικόνα 13: Αποσυμπίεση VirtueMart

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Τώρα για να εγκαταστήσουμε το VirtueMart στο Joomla, θα πρέπει να συνδεθούμε στο Administrator back-end του συστήματος διαχείρισης περιεχομένου, το οποίο είναι προσβάσιμο από το localhost/administrator. Μετά πηγαίνουμε στο μενού Extentions, Extention Manager και στην περιοχή Upload Package File πατάμε Browse για να επιλέξουμε το αρχείο com_virtuemart.2.6.9.zip και τέλος πατάμε το κουμπί Upload & Install.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Joomla! 2.5.20

Εικόνα 14: Εγκατάσταση του VirtueMart στο Joomla

Μετά την επιτυχή εγκατάσταση, ο οδηγός μας δίνει τις επιλογές “Install Sample Data” και “Go to the Shop”, καθώς επίσης μας υπενθυμίζει και να ενημερώσουμε τις επεκτάσεις με τον AIO installer, ο οποίος βρίσκεται στο αρχείο `com_virtuemart.2.6.9_ext_aio.zip`.

Επιλέγουμε λοιπόν “Install Sample Data” και μετά ακολουθούμε την προηγούμενη διαδικασία για να ανεβάσουμε το αρχείο `com_virtuemart.2.6.9_ext_aio.zip` και να τρέξουμε τον AIO installer.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

The screenshot displays the Joomla! administrator interface during the VirtueMart installation process. At the top, a blue information bar shows a list of SQL queries executed, including 'setStoreOwner VmUser inserted new main vendor has user id 836' and several 'created table' statements for VirtueMart components. Below this, another blue bar indicates 'Installing component was successful.' The main content area features the VirtueMart logo and a 'Welcome to VirtueMart' message. To the right, a green 'SUCCESSFUL' status is displayed with a reminder to update extensions. Two buttons are visible: 'Install Sample Data' and 'Go to the Shop'.

```
setStoreOwner VmUser inserted new main vendor has user id 836
created table lolct_virtuemart_products_en_gb
created table lolct_virtuemart_vendors_en_gb
created table lolct_virtuemart_categories_en_gb
created table lolct_virtuemart_manufacturers_en_gb
created table lolct_virtuemart_manufacturercategories_en_gb
created table lolct_virtuemart_paymentmethods_en_gb
created table lolct_virtuemart_shipmentmethods_en_gb
```

Installing component was successful.

VirtueMart
shopping cart software

Welcome to VirtueMart
The complete e-Commerce shopping cart solution for Joomla

The Installation was **SUCCESSFUL**
Reminder! Also update your extensions with the AIO installer

Install Sample Data Go to the Shop

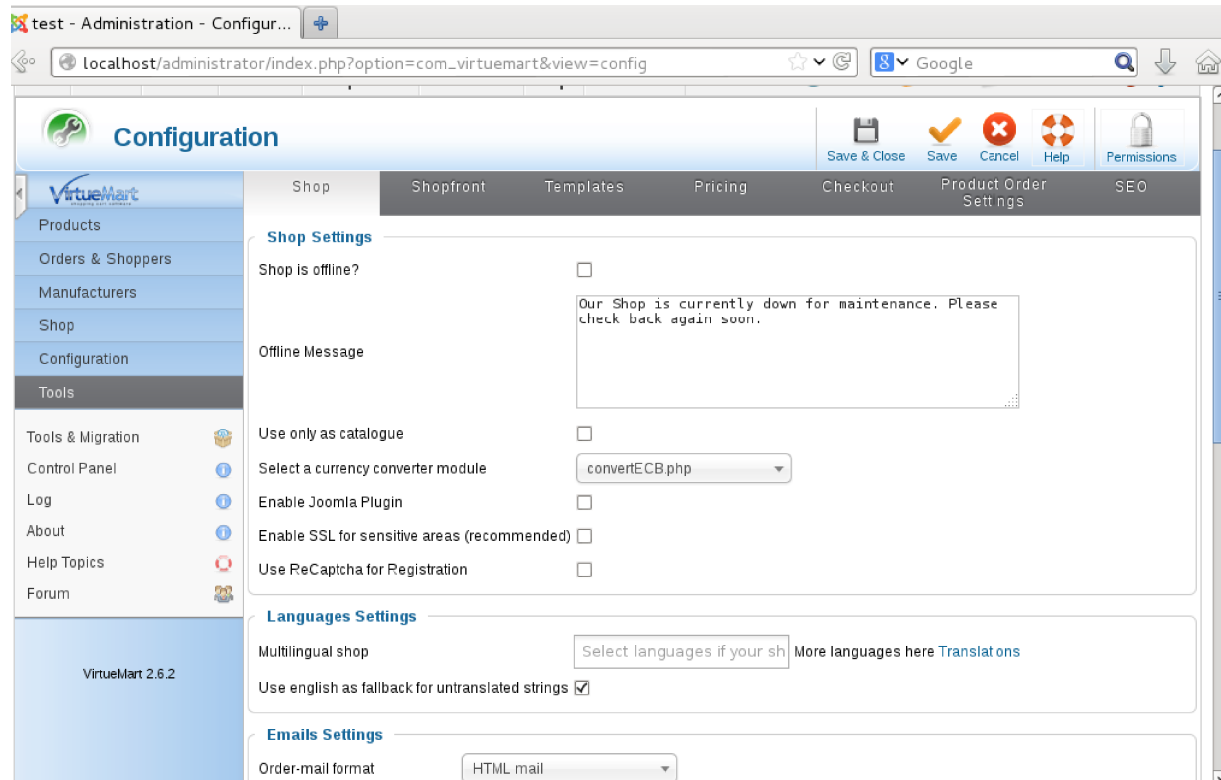
Εικόνα 15: Ολοκλήρωση οδηγού εγκατάστασης

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

4.4 - Επιλογές ρυθμίσεων του VirtueMart.

Για να ανοίξουμε τις ρυθμίσεις του VirtueMart ακολουθούμε στο μενού Components, VirtueMart, VirtueMart Configuration.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 16: VirtueMart Configuration - Shop

Στις ρυθμίσεις Shop μας δίνονται οι εξής επιλογές:

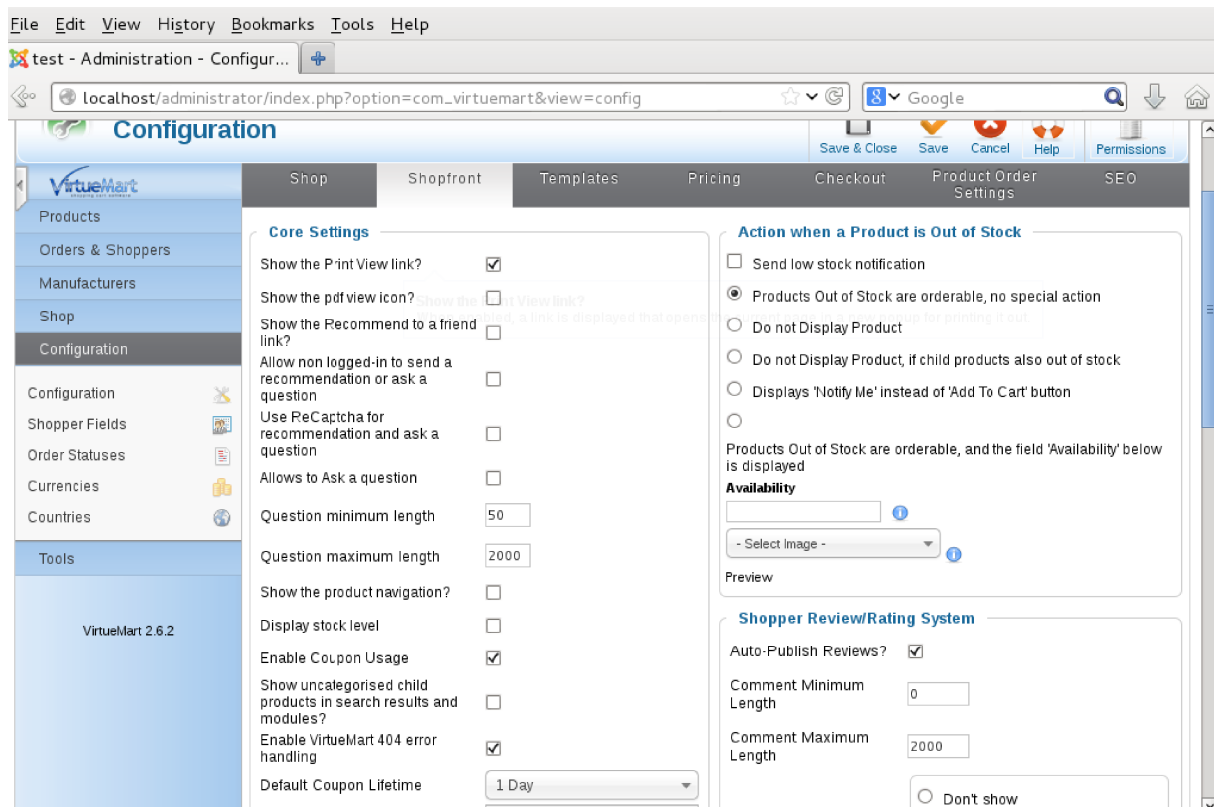
- **Shop is offline?:** Με την επιλογή αυτή το ηλεκτρονικό μας κατάστημα δεν θα είναι διαθέσιμο, αλλά θα εμφανίζεται ένα σχετικό ενημερωτικό μήνυμα.
- **Offline message:** Εδώ πληκτρολογούμε το ενημερωτικό μήνυμα που θα εμφανίζεται όταν το ηλεκτρονικό μας κατάστημα δεν θα είναι διαθέσιμο.
- **Use only as catalog:** Αν ενεργοποιήσουμε την επιλογή αυτή, η λειτουργία καλάθι θα απενεργοποιηθεί.
- **Select a currency converter module:** Σε περίπτωση που έχουμε εγκαταστήσει πρόσθετες μονάδες μετατροπής νομίσματος, εδώ μπορούμε να επιλέξουμε ποια θέλουμε. Τέτοιες μονάδες ενημερώνονται για τις συναλλαγματικές ισοτιμίες από κάποιον διακομιστή και μετατρέπουν ένα νόμισμα σε κάποιο άλλο για τον επισκέπτη, αυτόματα.
- **Order-mail format:** Αν θέλουμε οι πελάτες να λαμβάνουν το ηλεκτρονικό μήνυμα σε μορφή απλού κειμένου, επιλέγουμε Text. Αλλιώς, για ηλεκτρονικά μηνύματα εμπλουτισμένου περιεχομένου επιλέγουμε Html.
- **Enable SSL for sensible areas (recommended):** Για να λειτουργήσει η επιλογή αυτή, πρέπει πρώτα ο εξυπηρετητής ιστότοπου να υποστηρίζει SSL. Η επιλογή αυτή

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

προσθέτει SSL κρυπτογράφηση για τους συνδέσμους στο καλάθι και την περιοχή χρήστη.

- **Multilingual shop:** Αν έχουμε ανεβάσει επιπρόσθετες γλώσσες στον πίνακα ελέγχου του εξυπηρετητή ιστότοπου, μπορούμε να τις επιλέξουμε εδώ.
- **Untranslated strings in english:** Σε περίπτωση που υπάρχει κείμενο που δεν έχει μεταφραστεί, αντί να εμφανιστεί σε κώδικα υπολογιστή, θα εμφανιστεί στα αγγλικά.
- **Additional settings:** Ρυθμίσεις που αφορούν τους προγραμματιστές.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 17: VirtueMart Configuration - Shopfront

Στις ρυθμίσεις Shopfront μας δίνονται οι εξής επιλογές:

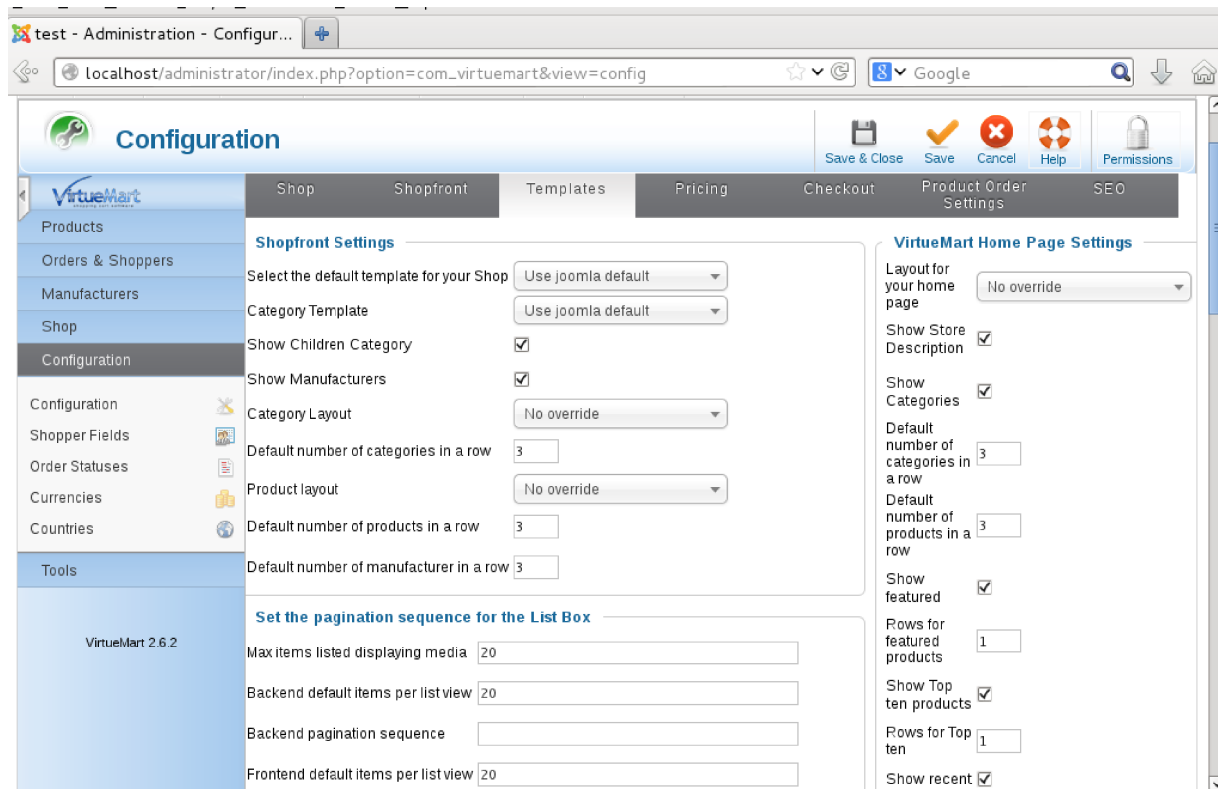
- Core settings
 - Show the recommended to a friend link: Όταν ενεργοποιηθεί, θα εμφανίζεται ένας σύνδεσμος ο οποίος επιτρέπει στον καταναλωτή να στείλει μια σύσταση με ένα ηλεκτρονικό μήνυμα για κάποιο συγκεκριμένο προϊόν.
 - Show the print view link: Όταν ενεργοποιηθεί, ένας σύνδεσμος θα εμφανίζεται που θα ανοίγει την τρέχουσα σελίδα σε ένα καινούριο αναδυόμενο παράθυρο, για την εκτύπωση της σελίδας.
 - Show the PDF view icon: Εμφάνιση ή απόκρυψη του εικονιδίου συνδέσμου pdf.
 - Show the ask a question link: Όταν ενεργοποιηθεί, θα εμφανίζεται ένας σύνδεσμος που θα ανοίγει την τρέχουσα σελίδα σε ένα καινούριο αναδυόμενο παράθυρο, που θα επιτρέπει τους πελάτες να στείλουν μια ερώτηση στον ιδιοκτήτη του καταστήματος.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Show the product navigation: Όταν ενεργοποιηθεί, η πλοήγηση προϊόντος θα εμφανίζεται πάνω στη σελίδα προϊόντος.
- Action when a product is out of stock: Εδώ μπορούμε να επιλέξουμε την ενέργεια που θα παρθεί όταν η διασημότητα ενός προϊόντος είναι περιορισμένη.
 - Προϊόντα με μικρό στόκ είναι διαθέσιμα για παραγγελία, καμία ενέργεια.
 - Να μην εμφανίζεται το προϊόν.
 - Να μην εμφανίζεται το προϊόν, αν και μόνο τα υποπροϊόντα είναι και αυτά σε μικρό στόκ.
 - Εμφάνιση κουμπιού για ενημέρωση αντί του κουμπιού προσθήκης στο καλάθι.
- Shopper Review/Rating System:
 - Show Review: Όταν ενεργοποιηθεί, θα επιτρέπει στους πελάτες να διαβάζουν τις κριτικές.
 - Show Rating: Όταν ενεργοποιηθεί, θα επιτρέπει στους πελάτες να βαθμολογήσουν τα προϊόντα.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



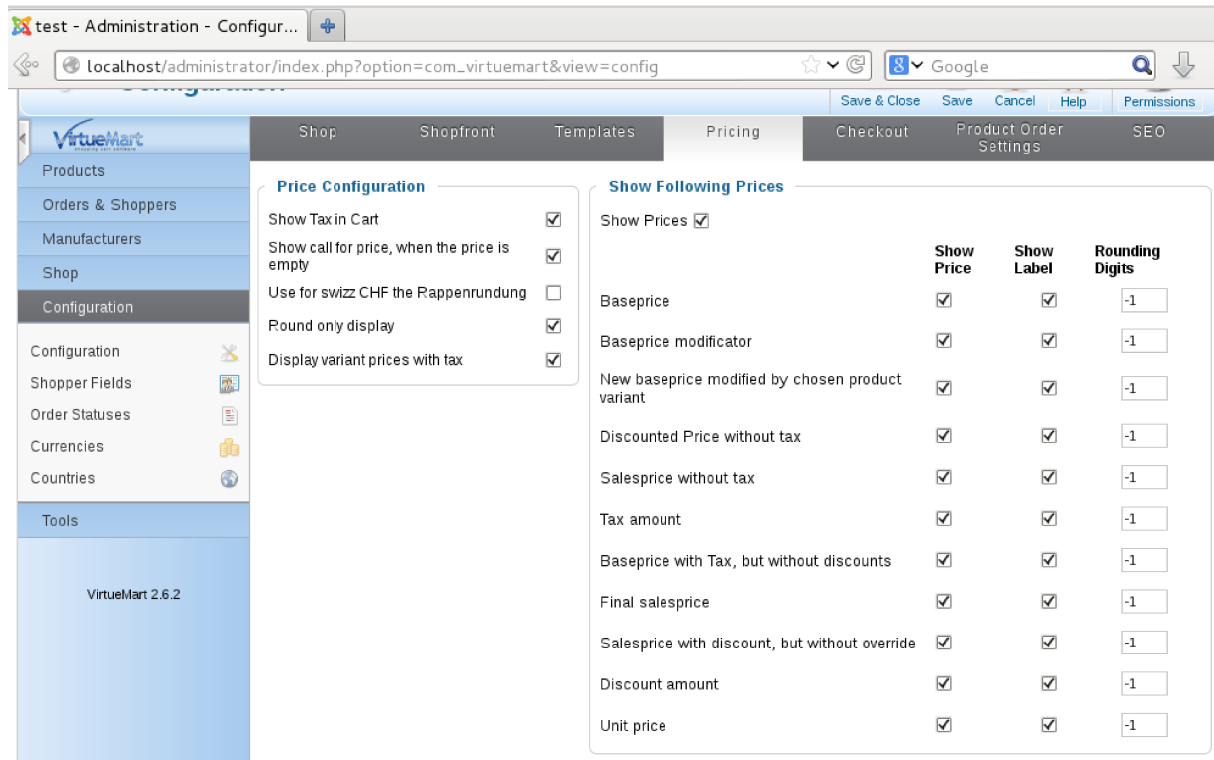
Εικόνα 18: VirtueMart Configuration - Templates

Το VirtueMart 2 αυτόματα χρησιμοποιεί το template του Joomla, έτσι δεν υπάρχει ανάγκη για ξεχωριστό template. Δεν είναι όμως υποχρεωτικό να χρησιμοποιήσουμε το template του Joomla, εδώ μπορούμε να ορίσουμε ένα ξεχωριστό και να προσδιορίσουμε την εμφάνισή του.

- **Shopfront Settings:** Αν έχουμε ανεβάσει επιπρόσθετα templates μπορούμε να τα επιλέξουμε εδώ. Επίσης εδώ μπορούμε να επιλέξουμε αν θα εμφανίζονται οι υποκατηγορίες και οι κατασκευαστές.
- **VirtueMart Home Page Settings:** Αν έχουμε ανεβάσει επιπρόσθετες διατάξεις σελίδας μπορούμε να τις επιλέξουμε εδώ. Επίσης μπορούμε να επιλέξουμε αν θα εμφανίζονται προτεινόμενα προϊόντα ή όχι, τα δέκα κορυφαία προϊόντα, τα πρόσφατα προϊόντα και πόσα προϊόντα σε κάθε γραμμή.
- **Media Files Settings:** Αν θέλουμε το VirtueMart να δημιουργεί προεπισκοπήσεις εικόνων, μπορούμε να ορίσουμε το μέγεθος, καθώς μπορούμε να ορίσουμε την προεπιλεγμένη φωτογραφία που θα εμφανίζεται όταν δεν έχουμε ανεβάσει κάποια.
- **Activate CSS Styles & Javascripts:** Τα αντικείμενα αυτά είναι, από προεπιλογή, ενεργοποιημένα και πρέπει να μείνουν έτσι για να έχουμε την προβλεπόμενη λειτουργία του VirtueMart.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 19: VirtueMart Configuration - Pricing

Στις ρυθμίσεις Price Configuration μπορούμε να ορίσουμε τον τρόπο με τον οποίο οι τιμές θα εμφανίζονται στο ηλεκτρονικό κατάστημα.

- **Show Tax in Cart:** Εμφανίζει τις λεπτομέρειες φορολόγησης στο καλάθι.
- **Show call for price, when the price is empty:** Αν επιθυμούμε η τιμή να μην φαίνεται, μπορούμε να δώσουμε την δυνατότητα στον πελάτη να μας ρωτήσει την τιμή. Για να λειτουργήσει η επιλογή αυτή, θα πρέπει να ενεργοποιήσουμε την επιλογή Allow ask questions.
- **Use for swizz CHF the Rappenrundung:** Μόνο για τους Ελβετούς, στρογγυλοποιεί την προβολή της τιμής κατά 0,00 ή 0,05.
- **Round only display:** Προτείνεται να είναι ενεργοποιημένη, η στρογγυλοποίηση γίνεται μόνο στην εμφάνιση της τιμής.

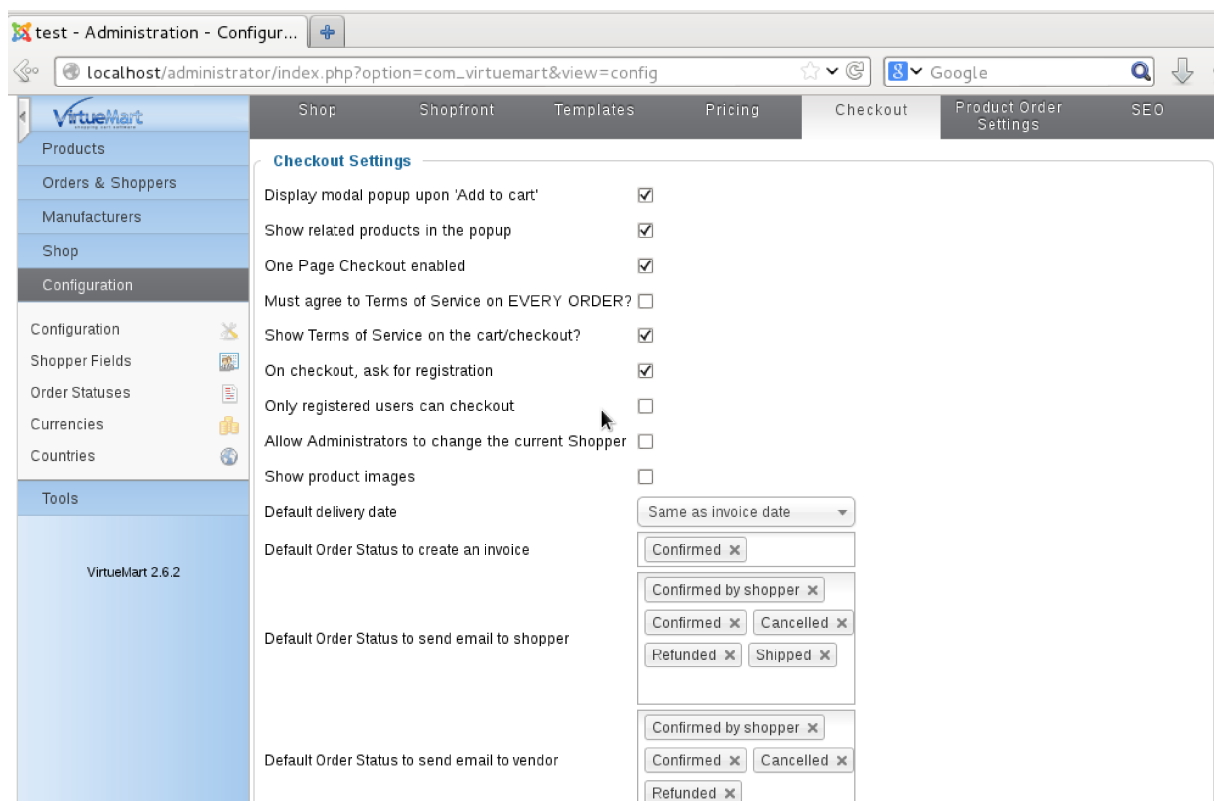
Στις ρυθμίσεις Show Following Prices:

- **Show Prices:** Επιλέγουμε αν θέλουμε ή όχι να εμφανίζονται οι τιμές στους πελάτες. Θα πρέπει οι πελάτες μετά να επικοινωνήσουμε με εμάς για να μάθουν την χρέωση.
- **Base price modifcator:** Αν το προϊόν μας μεταβάλει την τιμή περισσότερο ή λιγότερο, για παράδειγμα το διαμάντι ανεβάζει την τιμή κατά 100\$ ενώ το ρουμπίνι κατεβάζει

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

την τιμή κατά 50\$, μπορούμε να εμφανίσουμε την βασική τιμή.

- **New base price modiflicated by chosen product variant:** Αν χρησιμοποιούμε μεταβαλλόμενα προϊόντα που ανεβάζουν ή κατεβάζουν την τιμή, μπορούμε να εμφανίσουμε την τελική βασική τιμή μαζί με τις μεταβολές.
- **Discounted price without tax και Sales price without tax:** Αν έχουμε προϊόντα σε προσφορά, εμφανίζουμε την τιμή χωρίς φόρους, καθώς επίσης και τα προϊόντα που δεν είναι σε προσφορά.
- **Tax amount:** Εμφανίζει μόνο τους φόρους.
- **Base price with tax, but without discounts:** Εμφανίζει την τιμή μαζί με τους φόρους, αλλά πριν οποιαδήποτε έκπτωση.
- **Final salesprice:** Η τελική τιμή που ο πελάτης πληρώνει.
- **Discount amount:** Εμφανίζει στον πελάτη ακριβώς πόση έκπτωση έχει.



Εικόνα 20: VirtueMart Configuraion - Checkout

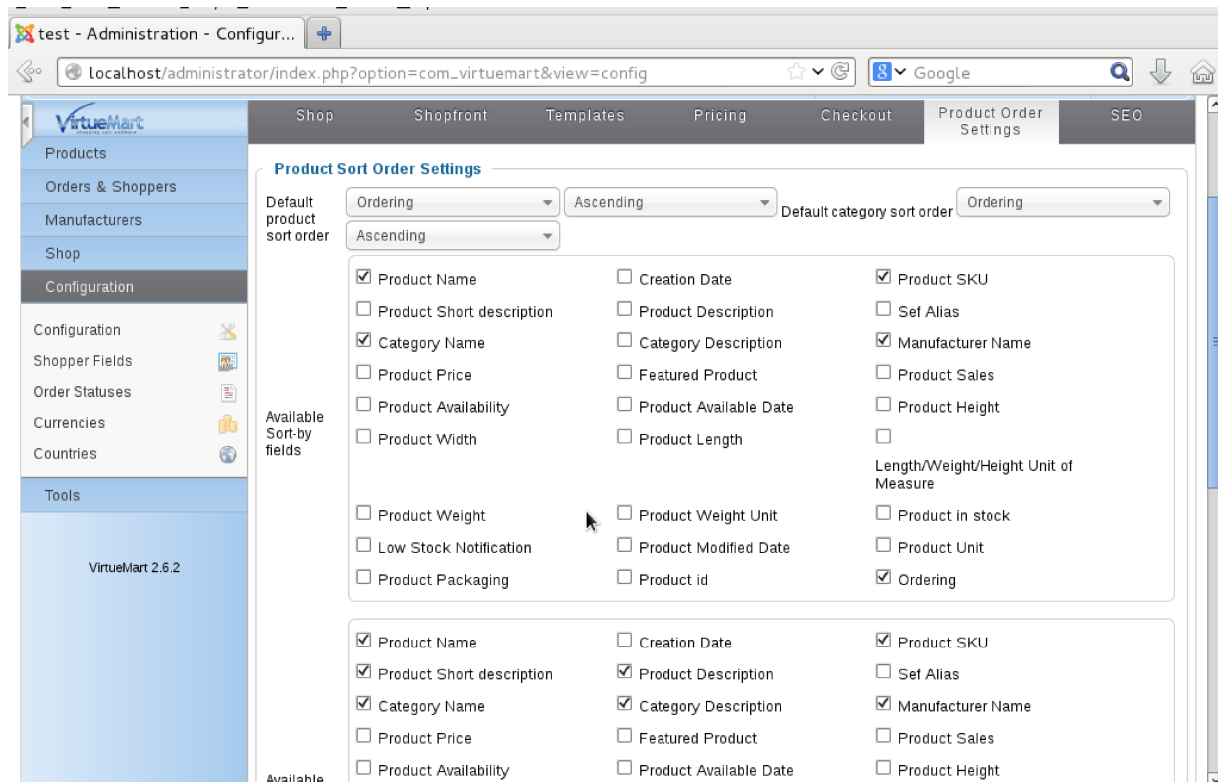
Στο μενού checkout μπορούμε να ρυθμίσουμε την διαδικασία πληρωμής.

- **Display modal popup upon 'Add to cart':** Θα εμφανίζεται ένα modal παράθυρο.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Show related products in the popup: Εμφάνιση σχετικών προϊόντων.
- One page Checkout enabled: Όταν ενεργοποιηθεί, οι επιλογές αποστολής και πληρωμής θα εμφανίζονται μέσα στο καλάθι.
- Must agree to Terms of Service on EVERY ORDER?: Ενεργοποιείτε αν θέλουμε ο καταναλωτής να συμφωνεί με τους όρους υπηρεσίας σε κάθε παραγγελία.
- Show Terms of Service on the cart/checkout: Σχεδόν σε όλες τις Ευρωπαϊκές χώρες, οι ιδιοκτήτες καταστημάτων είναι υποχρεωμένοι να δείχνουν στους πελάτες τους όρους ακύρωσης και επιστροφής παραγγελίας, οπότε σχεδόν σε όλες τις περιπτώσεις πρέπει να είναι ενεργοποιημένο.
- On checkout, ask for registration: Κατά την διάρκεια πληρωμής, ο πελάτης μπορεί να κάνει εγγραφή στο κατάστημα.
- Only registered users can checkout: Η επιλογή αυτή επιτρέπει μόνο τους εγγεγραμμένους πελάτες του καταστήματος, να ακολουθήσουμε την διαδικασία πληρωμής, οπότε η προηγούμενη επιλογή προτείνεται να είναι ενεργοποιημένη.
- Allow Administrators to change the current Shopper: Η επιλογή αυτή επιτρέπει τους διαχειριστές να αλλάζουν τον τρέχον πελάτη. Η συνεδρία του χρήστη θα αλλάξει στον επιλεγμένο χρήστη και το ID του χρήστη διαχειριστή αποθηκεύεται στον πίνακα παραγγελιών ως created_by. Αυτό είναι χρήσιμο αν θέλουμε να κάνουμε μια παραγγελία εκ μέρους του πελάτη.
- Show product images: Εμφάνιση μικρών φωτογραφιών των προϊόντων μέσα στο καλάθι.
- Default delivery date: Ορίζουμε την προεπιλεγμένη ημερομηνία παράδοσης στο τιμολόγιο.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

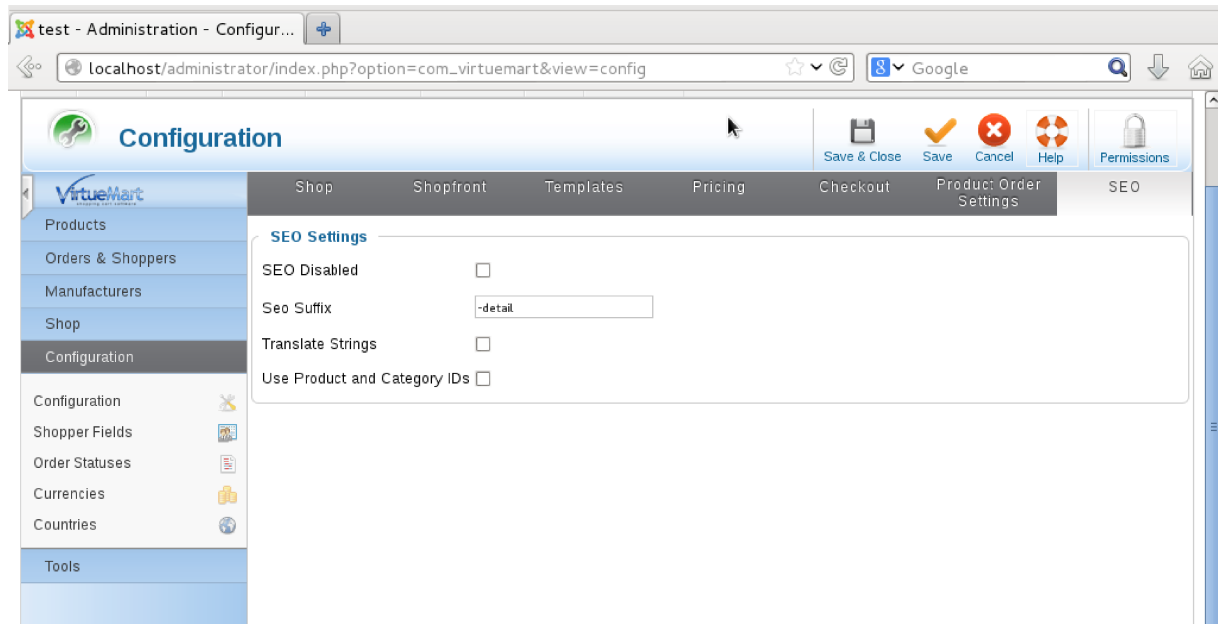


Εικόνα 21: VirtueMart Configuration - Product Order Settings

- Default product sort order: Ορίζουμε τα πεδία με βάση τα οποία θα γίνεται η ταξινόμηση των προϊόντων στον φυλλομετρητή.
- Available sort-by fields: Τα πεδία τα οποία είναι διαθέσιμα στον πελάτη για να κάνει ταξινόμηση των προϊόντων βάση με αυτά.
- Available search fields: Τα πεδία τα οποία είναι διαθέσιμα στον πελάτη για να κάνει αναζήτηση προϊόντων βάση με αυτά.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 22: VirtueMart configuration - SEO

- SEO Disabled: Όταν είναι επιλεγμένο, η λειτουργία SEO είναι απενεργοποιημένη.
- SEO Suffix: Ορίζουμε την κατάληξη που θα έχει το URL του προϊόντος.
- Translate Strings: Αν το ηλεκτρονικό μας κατάστημα χρησιμοποιεί διαφορετικές γλώσσες, ενεργοποιούμε την επιλογή αυτή για να μεταφράζονται και τα URL.
- Use product and category IDs: Προσθέτει το ID προϊόντος και κατηγορίας.

4.5 - Χρήστες και ομάδες χρηστών του VirtueMart

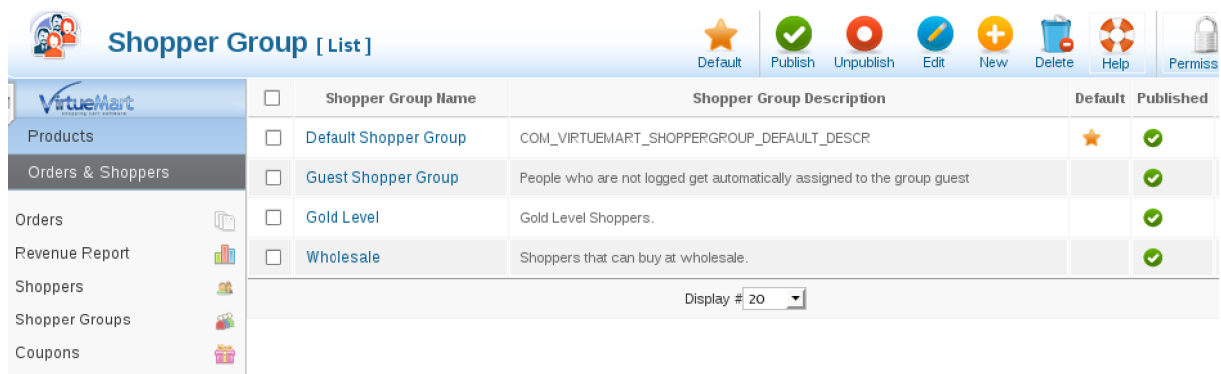
Το VirtueMart έρχεται με ένα επεκταμένο σύστημα διαχείρισης χρηστών και κάλο είναι εκτός από τους λειτουργικούς λόγους, να το μάθουμε και για λόγους ασφάλειας. Διότι αν το σύστημα μας είναι μεν ασφαλές αλλά δεν έχουμε γνώση για το τι δικαιώματα δίνουμε και σε ποιόν, τότε η ασφάλεια του δεν θα είναι το ίδιο ισχυρή.

Πάντα θα πρέπει να χρησιμοποιούμε το σύστημα διαχείρισής χρηστών του VirtueMart όταν εισάγουμε ή επεξεργαζόμαστε και διαγράφουμε χρήστες στην Joomla ιστοσελίδα μας. Αν χρησιμοποιήσουμε το σύστημα διαχείρισης χρηστών του Joomla, πολύ πιθανό να αντιμετωπίσουμε προβλήματα, διότι οι απαιτούμενες εγγραφές στους πίνακες, για τους αντίστοιχους χρήστες δεν δημιουργούνται στην βάση δεδομένων. Αντίστοιχα, αν διαγράψουμε χρήστες που έχουν δημιουργηθεί από το σύστημα διαχείρισής χρηστών του VirtueMart, από την βάση δεδομένων μας, χρησιμοποιώντας το σύστημα διαχείρισης χρηστών του Joomla, θα μας μείνουν άχρηστες εγγραφές.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Το VirtueMart επίσης δίνει, επιπλέον την ικανότητα να αποθηκεύουμε πολλές διευθύνσεις για τον κάθε χρήστη. Δηλαδή είμαστε σε θέση να κρατάμε πληροφορία για την διεύθυνση χρέωσης και διεύθυνση αποστολής, αλλά την διεύθυνση κατοικίας και εργασίας.

- **Shopper Groups:** Στο VirtueMart μπορούμε να εκχωρήσουμε χρήστες στην ομάδα Shopper Groups. Αυτό δίνει την δυνατότητα σε αυτόν που έχει το κατάστημα, να δημιουργεί Shopper Groups για την οποιαδήποτε ανάγκη του (π.χ. προσβασιμότητα στην ιστοσελίδα, βαθμολογία πελατών, εμφάνιση φόρου κ.ο.κ.). Μπορούμε να προσθέσουμε ή να τροποποιήσουμε την ομάδα χρηστών Shopper Groups, ακολουθώντας το μενού Components → VirtueMart → Shoppers → Shopper Groups



	Shopper Group Name	Shopper Group Description	Default	Published
<input type="checkbox"/>	Default Shopper Group	COM_VIRTUEMART_SHOPPERGROUP_DEFAULT_DESCR	★	✓
<input type="checkbox"/>	Guest Shopper Group	People who are not logged get automatically assigned to the group guest		✓
<input type="checkbox"/>	Gold Level	Gold Level Shoppers.		✓
<input type="checkbox"/>	Wholesale	Shoppers that can buy at wholesale.		✓

Εικόνα 23: VirtueMart - Shopper Groups list

- **User Groups:** Η ομάδα χρηστών αυτή μπορεί να περιγραφεί και ως “ομάδα προσβασιμότητας”, και υπάρχει για να μπορούμε να ορίσουμε περιορισμένη πρόσβαση στα διάφορα μέρη και λειτουργίας του ηλεκτρονικού καταστήματος. Κάθε εγγεγραμμένος χρήστης εκχωρείτε σε ένα User Group και από προεπιλογή είναι μέλος της ομάδας shopper.
- **Shopper Fields:** Εδώ μπορούμε να ορίσουμε τα πεδία που θα εμφανίζονται κατά την εγγραφή καινούριου χρήστη ή διαχείριση του λογαριασμού. Τέτοια πεδία είναι First Name, Last Name, Telephone κ.ο.κ. Η λειτουργία αυτή είναι προσβάσιμη από το μενού Components → VirtueMart → Shoppers → Shopper Fields

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

	Name	Type	Required	Visible	Searchable	Filterable	Sortable	Default Value	Order	Group
<input type="checkbox"/>	password	Password	password	✓	✓	✓	✗	✓	10	2
<input type="checkbox"/>	password2	Confirm Password	password	✓	✓	✓	✗	✓	12	3
<input type="checkbox"/>	agreed	I agree to the Terms of Service	checkbox	✓	✓	✓	✗	✓	13	4
<input type="checkbox"/>	delimiter_userinfo	Shopper Information	delimiter	✗	✓	✓	✗	✓	14	24
<input type="checkbox"/>	address_type_name	Address Nickname	text	✓	✓	✗	✓	✗	16	7
<input type="checkbox"/>	delimiter_billto	Bill To Information	delimiter	✗	✓	✓	✗	✓	18	8
<input type="checkbox"/>	company	Company Name	text	✗	✓	✓	✓	✓	20	9
<input type="checkbox"/>	title	Title	select	✗	✓	✓	✗	✓	22	10
<input type="checkbox"/>	first_name	First Name	text	✓	✓	✓	✓	✓	24	11
<input type="checkbox"/>	middle_name	Middle Name	text	✗	✓	✓	✓	✓	26	12
<input type="checkbox"/>	last_name	Last Name	text	✓	✓	✓	✓	✓	28	13
<input type="checkbox"/>	address_1	Address 1	text	✓	✓	✓	✓	✓	30	14
<input type="checkbox"/>	address_2	Address 2	text	✗	✓	✓	✓	✓	32	15
<input type="checkbox"/>	zip	Zip / Postal Code	text	✓	✓	✓	✓	✓	34	16
<input type="checkbox"/>	city	City	text	✓	✓	✓	✓	✓	36	17
<input type="checkbox"/>	virtuemart_country_id	Country	select	✓	✓	✓	✓	✓	38	18

Display # 20 Start Prev 1 2 Next End Page 1 of 2

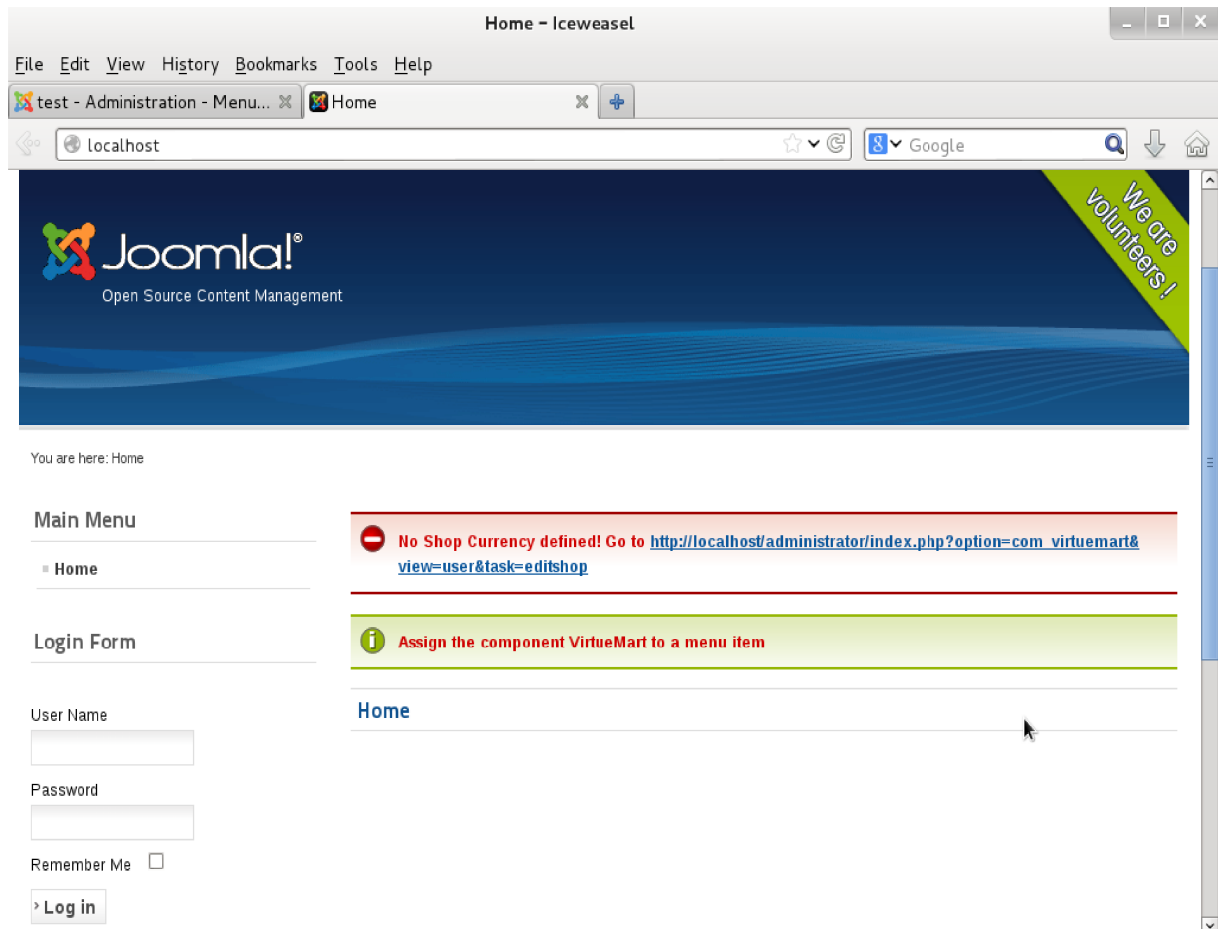
Εικόνα 24: VirtueMart - Shopper Fields

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

4.6 – Δημιουργία ιστοσελίδας του ηλεκτρονικού καταστήματος.

Αφού κάναμε όλα τα προηγούμενα βήματα, πρέπει να δημιουργήσουμε την ιστοσελίδα του ηλεκτρονικού μας καταστήματος. Για να πάρουμε μια εικόνα του πως είναι η ιστοσελίδα μας (αν υπάρχει) αυτή τη στιγμή, απλά πληκτρολογούμε στη γραμμή διευθύνσεων του browser “localhost” ή μέσα από τη διεπαφή διαχείρισης του Joomla πατάμε το σύνδεσμο “View Site”.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

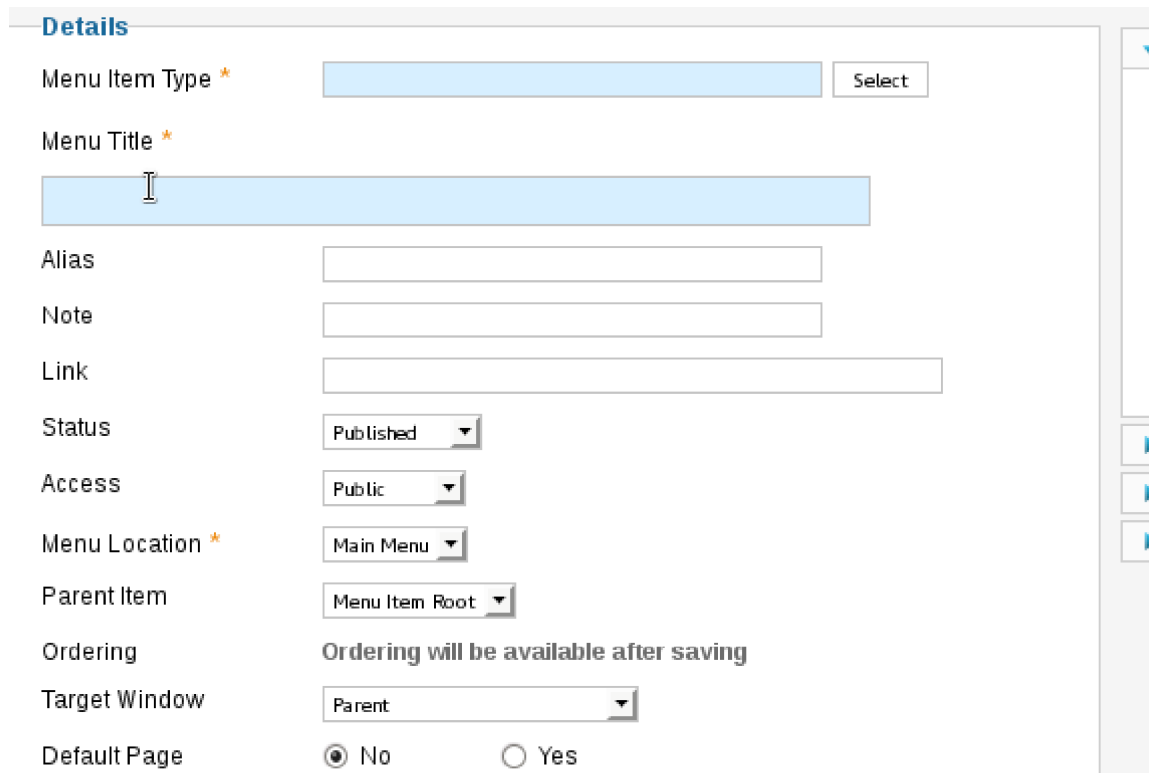


Εικόνα 25: Αρχική μορφή της ιστοσελίδας

Όπως βλέπουμε μας εμφανίζεται ένα μήνυμα υπενθύμισης, που μας λέει πως πρέπει να εκχωρήσουμε το component VirtueMart σε ένα μενού. Για να το κάνουμε αυτό, μέσα από τη διεπαφή διαχείρισης, ακολουθούμε το μενού Menus → Main Menu → Add New Menu Item.

Έστω τώρα πως θέλουμε να βάλουμε ως αρχική σελίδα, την αρχική σελίδα του VirtueMart. Στο μενού που βρισκόμαστε, στο πεδίο Menu Item Type πατάμε το κουμπί Select.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



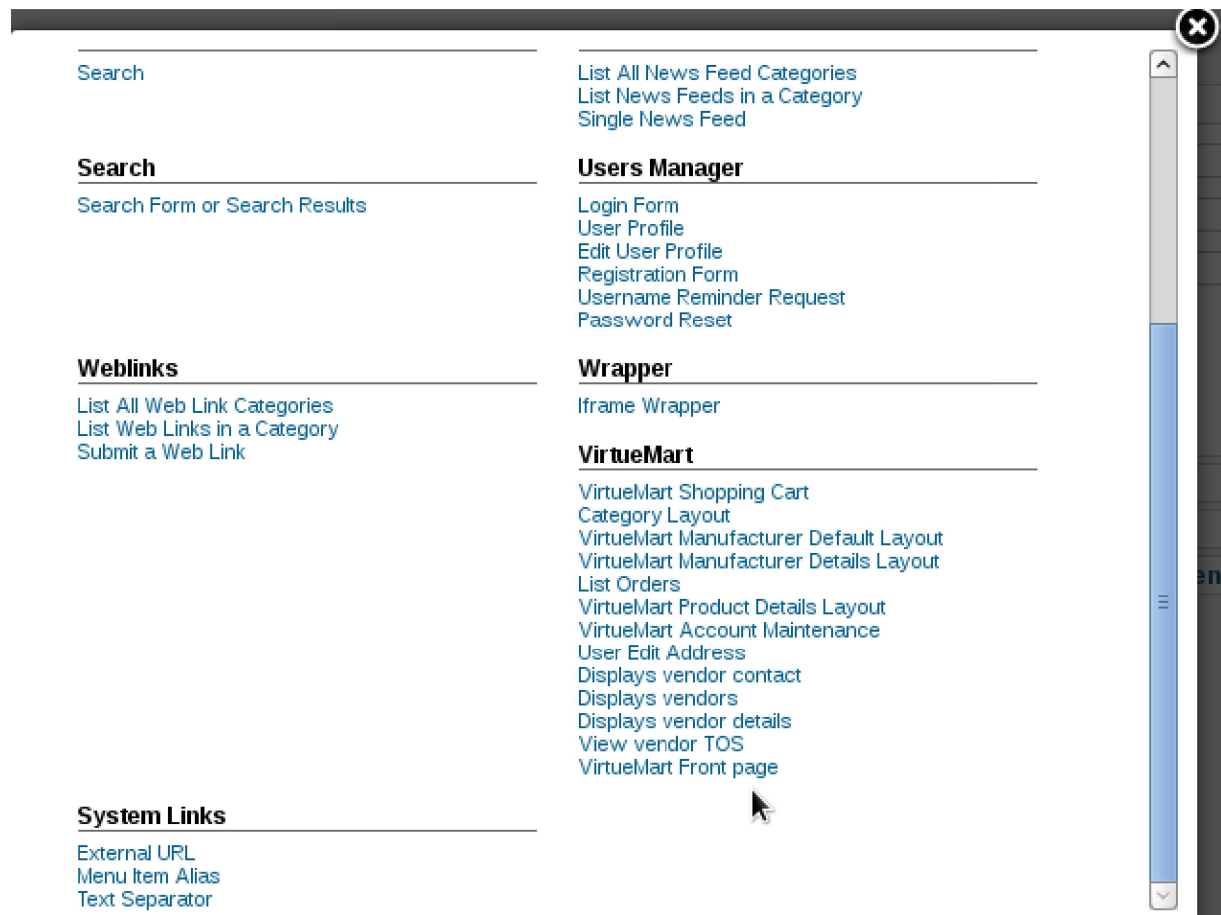
The screenshot shows the 'Details' section of the Joomla! Menu Manager interface for creating a new menu item. The form includes the following fields and options:

- Menu Item Type ***: A text input field with a 'Select' button.
- Menu Title ***: A large text input field with a cursor.
- Alias**: A text input field.
- Note**: A text input field.
- Link**: A text input field.
- Status**: A dropdown menu set to 'Published'.
- Access**: A dropdown menu set to 'Public'.
- Menu Location ***: A dropdown menu set to 'Main Menu'.
- Parent Item**: A dropdown menu set to 'Menu Item Root'.
- Ordering**: A message stating 'Ordering will be available after saving'.
- Target Window**: A dropdown menu set to 'Parent'.
- Default Page**: Radio buttons for 'No' (selected) and 'Yes'.

Εικόνα 26: Menu Manager: New Menu Item

Στο αναδυόμενο μενού που ανοίγει, κατεβένουμε κάτω, ψάχνοντας για το αντικείμενο “VirtueMart Front page”.

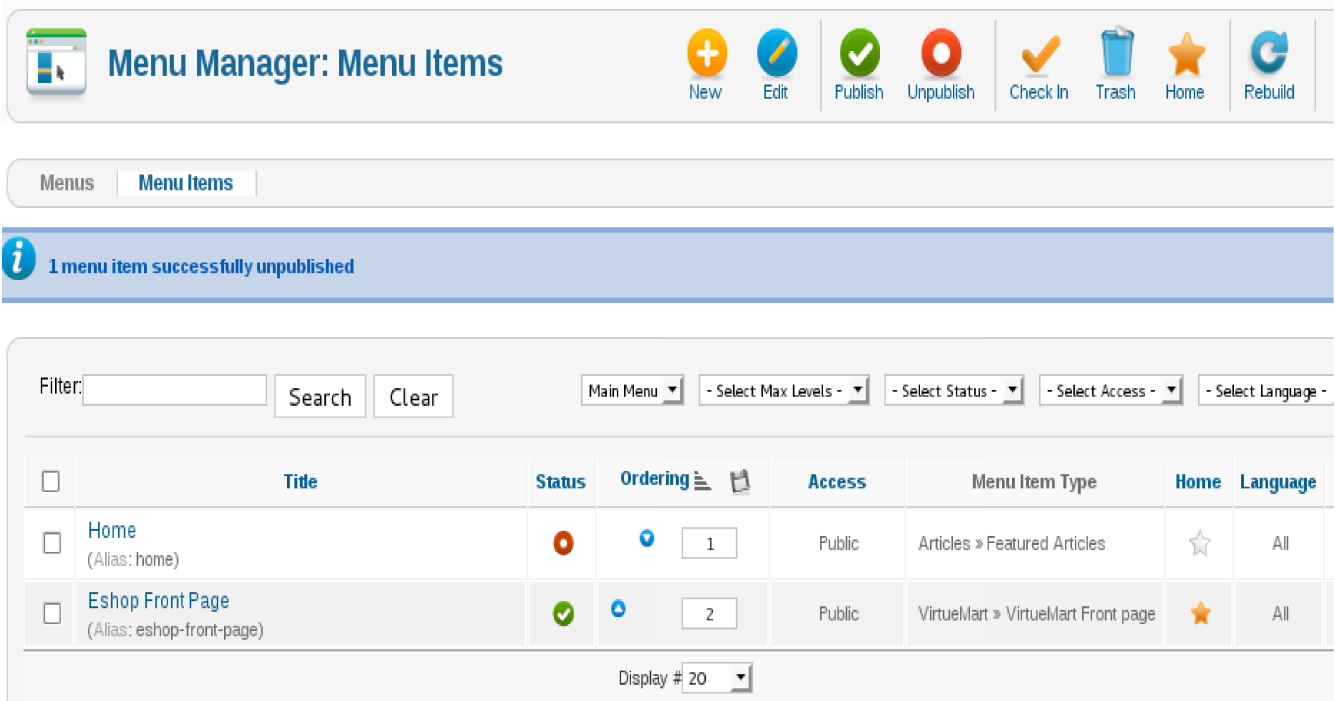
Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 27: Επιλογή του Menu Item

Το επιλέγουμε, και μετά δίνουμε έναν τίτλο στο “Menu Title” έστω το “Eshop Front Page” και μετά πατάμε “Save&Close”. Θα οδηγηθούμε στο μενού “Menu Manager: Menu Items” όπου εμφανίζεται το νέο αντικείμενο μενού που δημιουργήσαμε. Για να το βάλουμε να εμφανίζεται ως “Home” στη σελίδα μας, αρκεί να πατήσουμε το αστεράκι στην στήλη “Home”. Αν θέλουμε μπορούμε να απενεργοποιήσουμε το αρχικό αντικείμενο “Home”, τσεκάροντας από την λίστα και πατώντας “Unpublish” ή να το διαγράψουμε πατώντας “Trash”

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



The screenshot shows the Joomla! Menu Manager interface. At the top, there is a header with the title "Menu Manager: Menu Items" and several action icons: New, Edit, Publish, Unpublish, Check In, Trash, Home, and Rebuild. Below the header, there are tabs for "Menus" and "Menu Items". A blue notification bar indicates "1 menu item successfully unpublished". The main content area features a filter section with a search box, a "Clear" button, and several dropdown menus for "Main Menu", "Select Max Levels", "Select Status", "Select Access", and "Select Language". Below the filter is a table with the following columns: Title, Status, Ordering, Access, Menu Item Type, Home, and Language. The table contains two rows of menu items.

<input type="checkbox"/>	Title	Status	Ordering	Access	Menu Item Type	Home	Language
<input type="checkbox"/>	Home (Alias: home)		1	Public	Articles » Featured Articles		All
<input type="checkbox"/>	Eshop Front Page (Alias: eshop-front-page)		2	Public	VirtueMart » VirtueMart Front page		All

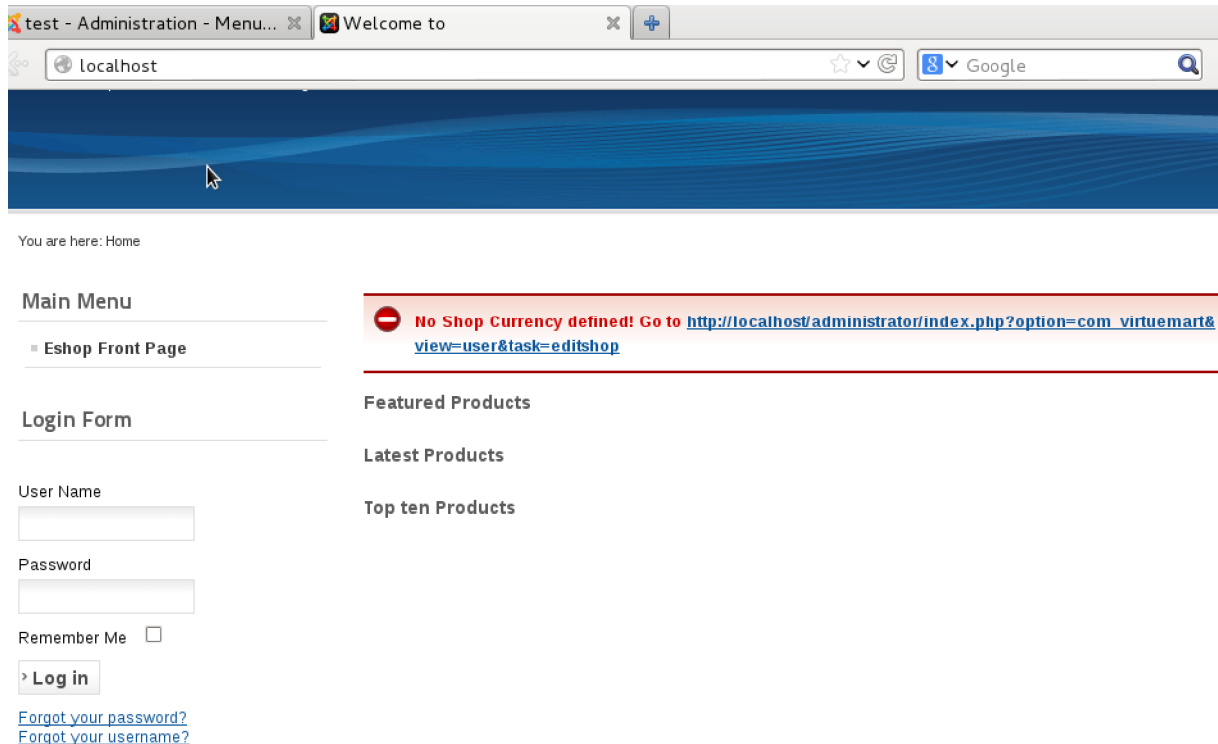
Display # 20

Εικόνα 28: Ορισμός αντικειμένου ως αρχική σελίδα

Για να δούμε την καινούρια μορφή που πήρε η ιστοσελίδα μας, πατάμε “View Site” και βλέπουμε το αποτέλεσμα στην παρακάτω εικόνα:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 29: Η μορφή που πήρε η ιστοσελίδα

Βλέπουμε πως έχουμε ένα ενημερωτικό μήνυμα από το VirtueMart “No Shop Currency defined”, το οποίο μας λέει πως δεν έχουμε ορίσει το νόμισμα στο οποίο θα γίνονται οι συναλλαγές. Για να το ορίσουμε, στο σημείο που βρισκόμαστε, μπορούμε να πατήσουμε στον σύνδεσμο που μας εμφανίζεται.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Στο παράθυρο που θα μας οδηγήσει ο παραπάνω σύνδεσμος, κατεβένουμε και βρίσκουμε την περιοχή “Currency”. Αν θέλουμε οι συναλλαγές μας να γίνονται σε ευρώ, στο πεδίο “Currency” ορίζουμε το νόμισμα Euro. Στο επόμενο πεδίο “List of accepted currencies” δηλώνουμε τα επιπλέον νομίσματα στα οποία δεχόμαστε συναλλαγές, τα οποία εμείς θέλουμε να είναι το αμερικάνικο δολάριο και η βρετανική λίρα.

Currency

Currency:

List of accepted currencies:

-
-

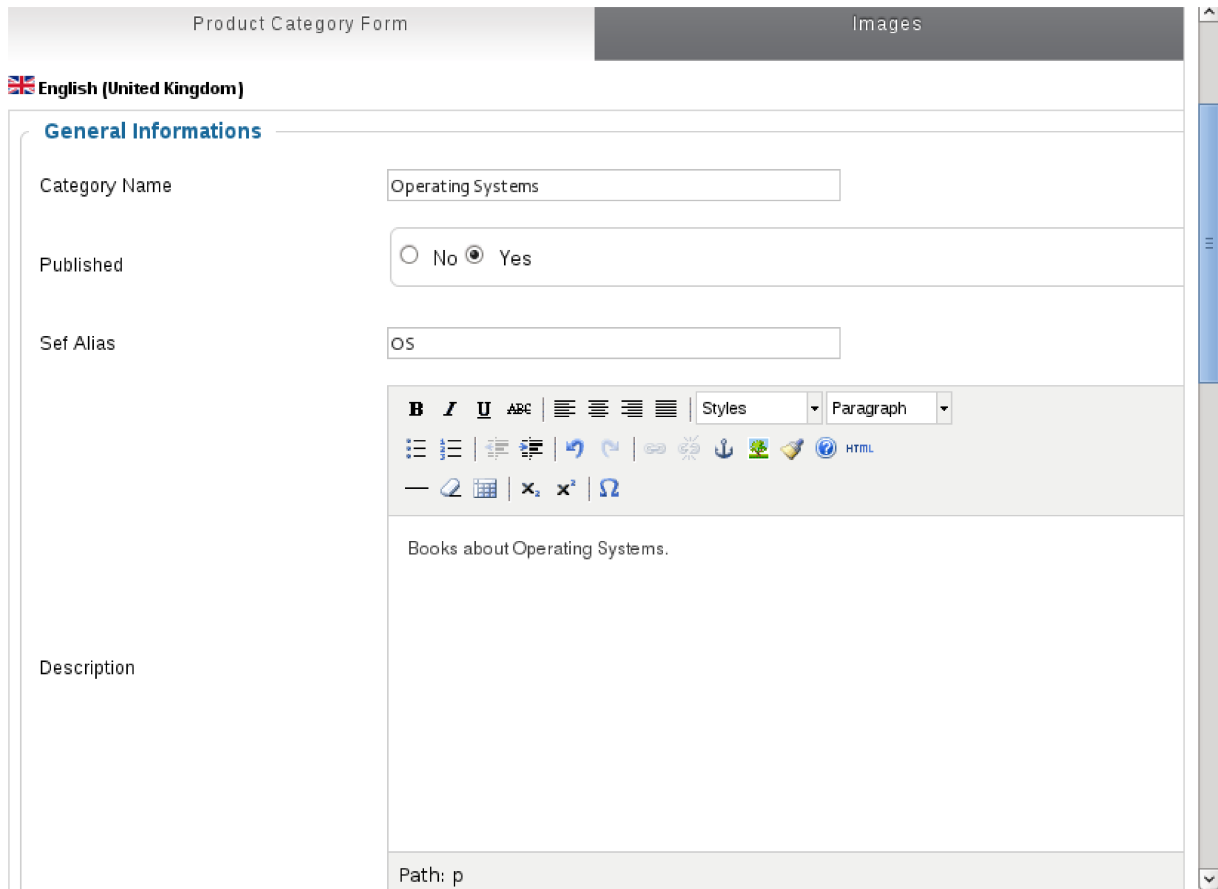
Εικόνα 30: Ορισμός νομισμάτων με τα οποία θα γίνονται οι συναλλαγές

Ολοκληρώνοντας τα προηγούμενα βήματα, θα πρέπει τώρα να δημιουργήσουμε τα προϊόντα τα οποία προσφέρουμε. Έστω πως το ηλεκτρονικό κατάστημά μας προσφέρει βιβλία σχετικά με την πληροφορική. Ως γνωστό η πληροφορική, όπως και άλλες επιστήμες, είναι πολύ μεγάλη. Οπότε αν βάζουμε στο κατάστημα βιβλία τα οποία δεν τοποθετούνται με μια λογική σειρά, θα είναι δύσκολο στον επισκέπτη να βρει αυτό που αναζητά. Για αυτό το λόγο πρέπει να δημιουργήσουμε τις κατηγορίες στις οποίες θα βρίσκονται τα βιβλία.

Για να δημιουργήσουμε κατηγορίες προϊόντων στο VirtueMart, ακολουθούμε το μενού VirtueMart → Product Categories → New και συμπληρώνουμε τα πεδία που εμφανίζονται, όπως στην επόμενη εικόνα:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Product Category Form

Images

English (United Kingdom)

General Informations

Category Name: Operating Systems

Published: No Yes

Sef Alias: OS

Description: Books about Operating Systems.

Path: p

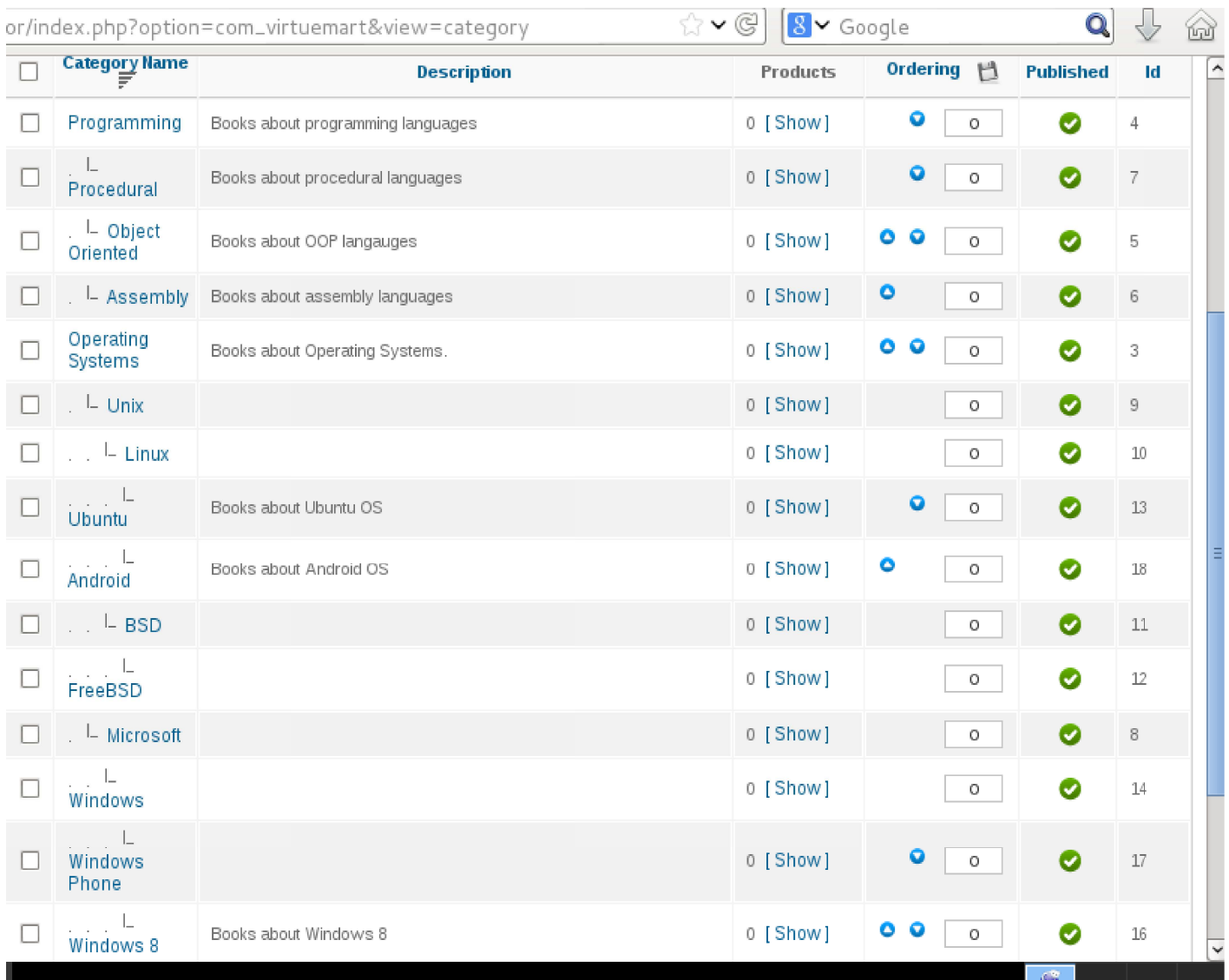
Εικόνα 31: VirtueMart - Δημιουργία κατηγορίας προϊόντος

Τα πεδία σε αυτό το μενού περιλαμβάνουν:

- Category Name: Το όνομα της κατηγορίας.
- Published: Αν θα εμφανίζεται ή όχι.
- Sef Alias: Search Engine URL ή αλλιώς clean URL ή Semantic URL είναι το URL που έχει τέτοια μορφή που είναι κατανοητό από ανθρώπους και μηχανές αναζήτησης. Τέτοια URL αποσκοπούν στην χρησιμότητα και προσβασιμότητα μιας ιστοσελίδας χωρίς να αποδίδουν την εσωτερική δομή του συστήματος. Αν το αφήσουμε κενό το πεδίο αυτό, το VirtueMart θα το συμπληρώσει σύμφωνα με το πεδίο “Category Name”, το οποίο δεν προτείνεται, ιδιαίτερα αν η κατηγορία έχει αρκετά μεγάλο τίτλο.
- Description: Η περιγραφή της κατηγορίας.

Συνεχίζοντας με την ίδια λογική, μπορούμε να δημιουργήσουμε και άλλες κατηγορίες προϊόντων, αλλά και υποκατηγορίες. Το τελικό αποτέλεσμα φαίνεται στην επόμενη εικόνα.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



The screenshot shows a Joomla! VirtueMart interface displaying a table of product categories. The browser address bar shows 'or/index.php?option=com_virtuemart&view=category'. The table has columns for 'Category Name', 'Description', 'Products', 'Ordering', 'Published', and 'Id'. Each row represents a category, such as 'Programming', 'Procedural', 'Object Oriented', etc., with corresponding descriptions and product counts.

<input type="checkbox"/>	Category Name	Description	Products	Ordering	Published	Id
<input type="checkbox"/>	Programming	Books about programming languages	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	4
<input type="checkbox"/>	Procedural	Books about procedural languages	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	7
<input type="checkbox"/>	Object Oriented	Books about OOP languages	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	5
<input type="checkbox"/>	Assembly	Books about assembly languages	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	6
<input type="checkbox"/>	Operating Systems	Books about Operating Systems.	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	3
<input type="checkbox"/>	Unix		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	9
<input type="checkbox"/>	Linux		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	10
<input type="checkbox"/>	Ubuntu	Books about Ubuntu OS	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	13
<input type="checkbox"/>	Android	Books about Android OS	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	18
<input type="checkbox"/>	BSD		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	11
<input type="checkbox"/>	FreeBSD		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	12
<input type="checkbox"/>	Microsoft		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	8
<input type="checkbox"/>	Windows		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	14
<input type="checkbox"/>	Windows Phone		0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	17
<input type="checkbox"/>	Windows 8	Books about Windows 8	0 [Show]	<input type="text" value="0"/>	<input checked="" type="checkbox"/>	16

Εικόνα 32: Κατηγορίες προϊόντων ηλεκτρονικού καταστήματος

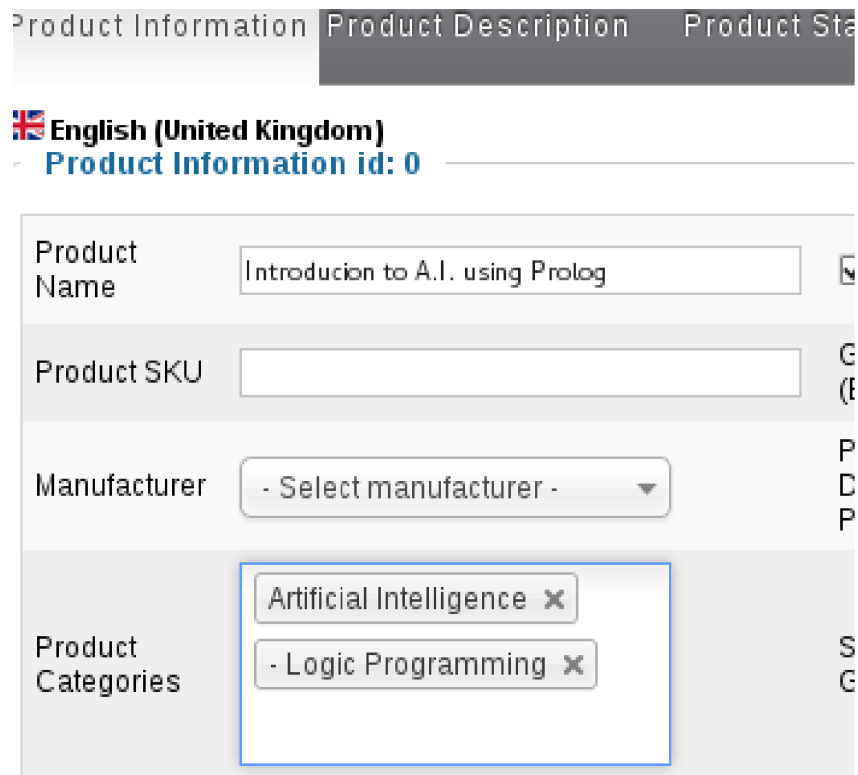
Όσο αφορά τώρα την δημιουργία προϊόντων, αρκεί να ακολουθήσουμε το μενού VirtueMart → Products → New και να συμπληρώσουμε τα αντίστοιχα πεδία. Εδώ να σημειώσουμε πως ένα προϊόν μπορεί να υπάρχει σε πάνω από μία κατηγορίες.

Για παράδειγμα, έστω πως έχουμε ένα βιβλίο, με τον ενδεικτικό τίτλο “Introduction to A.I. using Prolog”. Το βιβλίο αυτό μπορεί να υπάρξει στην κατηγορία “Artificial Intelligence” και την κατηγορία “Programming” και πιο συγκεκριμένα, στην υποκατηγορία “Logic Programming”.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



The image shows a Joomla! administration interface for editing a product. At the top, there are three tabs: 'Product Information', 'Product Description', and 'Product Status'. The 'Product Information' tab is active. Below the tabs, the language is set to 'English (United Kingdom)' and the product ID is '0'. The main form contains several fields: 'Product Name' with the value 'Introduction to A.I. using Prolog', 'Product SKU' (empty), 'Manufacturer' (dropdown menu showing '- Select manufacturer -'), and 'Product Categories'. The 'Product Categories' field is highlighted with a blue border and contains two selected categories: 'Artificial Intelligence' and '- Logic Programming'. To the right of the form, there are vertical labels for each field: 'N' for Product Name, 'G' and '(E' for Product SKU, 'P', 'D', and 'P' for Manufacturer, and 'S' and 'C' for Product Categories.

Εικόνα 33: Αντιστοίχιση προϊόντων σε κατηγορίες

Αφού δημιουργήσουμε τα προϊόντα, θα πρέπει να δημιουργήσουμε και τις μεθόδους

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

παράδοσης. Για να το κάνουμε αυτό ακολουθούμε το μενού Shop → Shipment Methods.

Στην περιοχή “Shipment Method Information” βλέπουμε τα εξής πεδία:

- **Shipment Name:** Το όνομα της μεθόδου αποστολής, το οποίο πρέπει να είναι μοναδικό και θα εμφανίζεται στην σελίδα πληρωμής.
- **Published:** Αν θα εμφανίζεται ή όχι η συγκεκριμένη μέθοδος αποστολής, στο ηλεκτρονικό κατάστημα.
- **Shipment Description:** Η περιγραφή της μεθόδου αποστολής, η οποία θα εμφανίζεται στην σελίδα πληρωμής.
- **Shipment Method:** Η έκδοση του VirtueMart εμπεριέχει μόνο μία μέθοδο αποστολής η οποία βασίζεται στο βάρος, την χώρα, αριθμό προϊόντων ή μέγεθος παραγγελίας. Αν θέλουμε να χρησιμοποιήσουμε και άλλους τρόπους, θα πρέπει να εγκαταστήσουμε μια επέκταση για το VirtueMart.
- **Shopper Group:** Αν επιθυμούμε η μέθοδος αποστολής να είναι προσβάσιμη μόνο από κάποιο συγκεκριμένο shopper group, μπορούμε να το επιλέξουμε εδώ.
- Αν έχουμε πάνω από μια μέθοδο αποστολής, εδώ βάζουμε την σειρά με την οποία θα εμφανίζεται.

The screenshot shows the VirtueMart administration interface. The top navigation bar includes a 'Shipment Method' link with a '[New]' indicator. On the right side of the top bar, there are buttons for 'Save & Close', 'Save', 'Cancel', 'Help', and 'Permissions'. The left sidebar contains a menu with items like 'Products', 'Orders & Shoppers', 'Manufacturers', 'Shop', 'Shop', 'Media Files', 'Shipment Methods', 'Shipment Methods', 'Configuration', and 'Tools'. The main content area is titled 'Shipment Method Information' and is divided into two sections: 'Shipment Method Information' and 'Configuration'. The 'Shipment Method Information' section includes a language selector for 'English (United Kingdom)', a title 'Shipment Method', and several form fields: 'Shipment Name' (text input), 'Sef Alias' (text input), 'Published' (radio buttons for 'No' and 'Yes'), 'Shipment Description' (text area), 'Shipment Method' (dropdown menu with 'VM Shipment - By weight, ZIP and countries'), 'Shopper Group' (text input with '- Use Default -'), and 'List Order' (text input with '0'). The 'Configuration' section is currently empty.

Εικόνα 34: VirtueMart - Shipment Method Information

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Στην περιοχή “Configuration” βλέπουμε τα εξής πεδία:

- **Logo:** Αν έχουμε ανεβάσει στο σύστημα μας, μια εικόνα μικρού μεγέθους, μπορούμε να την επιλέξουμε εδώ για να εμφανίζεται ως λογότυπο της μεθόδου παραγγελίας.
- **Countries:** Αν θέλουμε να παραδίδουμε τα προϊόντα μας σε όλες τις χώρες, αφήνουμε το πεδίο αυτό κενό. Αλλιώς μπορούμε να επιλέξουμε σε ποιες θέλουμε.
- **Zip range start και Zip range end:** Αν θέλουμε να περιορίσουμε την παράδοση προϊόντων σε ένα εύρος ταχυδρομικών κωδικών, απλά συμπληρώνουμε τα αντίστοιχα πεδία.
- **Lowest Weight, Highest weight και Weight Unit:** Αν θέλουμε να περιορίσουμε την δυνατότητα παράδοσης μέσα σε ένα όριο βάρους, συμπληρώνουμε τα πεδία αυτά.
- **Minimum και Maximum Number of Products:** Αν θέλουμε να περιορίσουμε την δυνατότητα παράδοσης μέσα σε συγκεκριμένο αριθμό προϊόντων, συμπληρώνουμε τα πεδία αυτά.
- **Minimum και Maximum Order Amount:** Αν θέλουμε να περιορίσουμε την παράδοση προϊόντων για σε ένα όριο αξίας παραγγελίας, συμπληρώνουμε τα πεδία ελάχιστης και μέγιστης αξίας παραγγελίας.
- **Shipment Cost, Package Fee, Tax:** Πόσο θα πληρώσει ο πελάτης για την αποστολή προϊόντων σύμφωνα με τα κριτήρια αυτά.
- **Minimum Amount for Free Shipment:** Συμπληρώνουμε το πεδίο αυτό, αν θέλουμε να κάνουμε αποστολή προϊόντων όταν η αξία ξεπερνάει το όριο που θέλουμε.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Site Users Menus Content Components Extensions Help VirtueMart 0 Visitors 1 Admin 0 View Site Log out

Shipment Method [Edit] Save & Close Save Cancel Help Permissions

Shipment Method Information Configuration

Shipment based on the Weight, ZIP and Countries

Logo

Countries

ZIP range start

ZIP range end

Lowest Weight

Highest Weight

Weight Unit

Minimum number of products

Maximum number of products

Minimum order amount

Maximum order amount

Shipment Cost

Package Fee

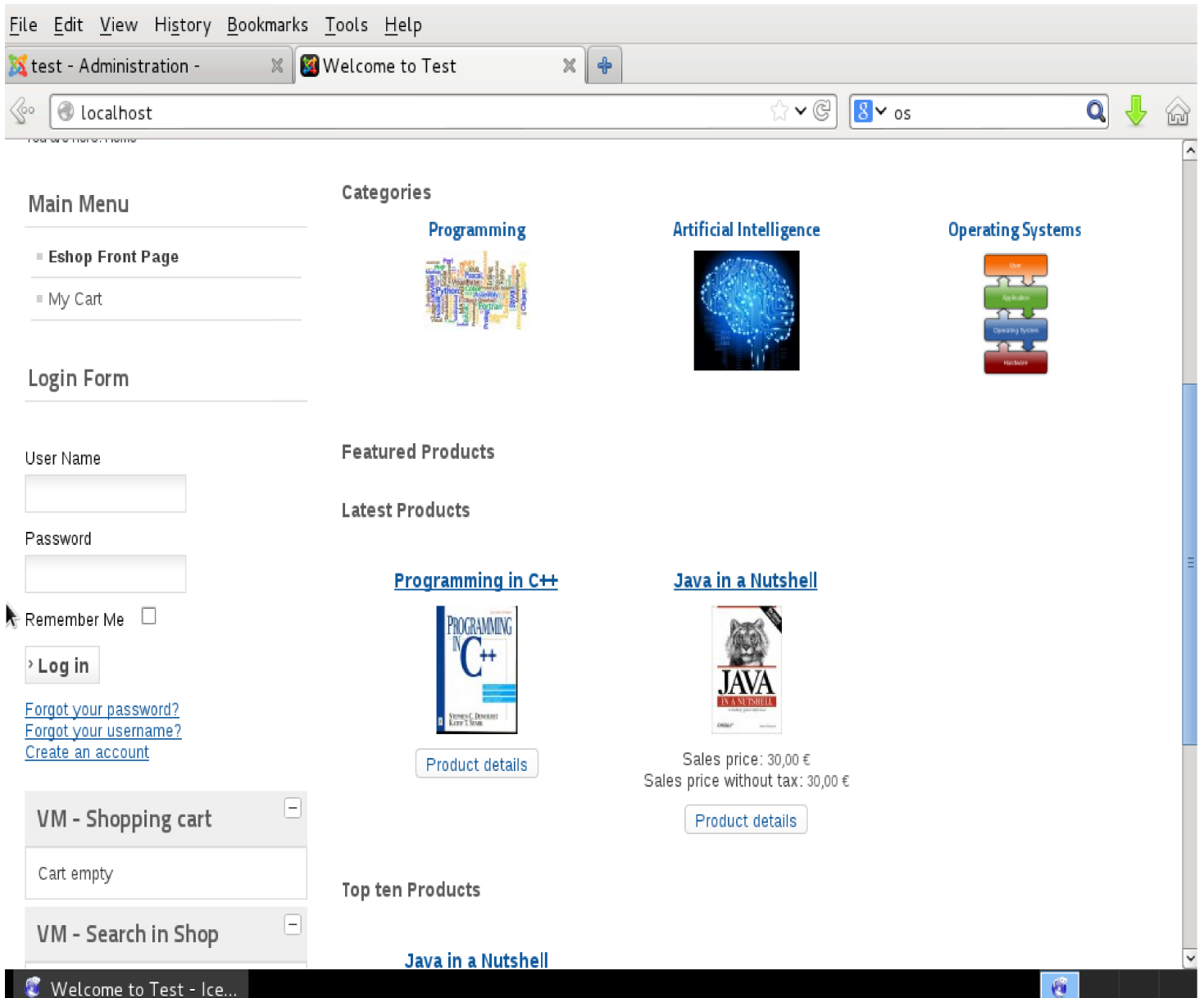
Tax

Minimum Amount for Free Shipment

Εικόνα 35: VirtueMart - Shipment Method Configuration

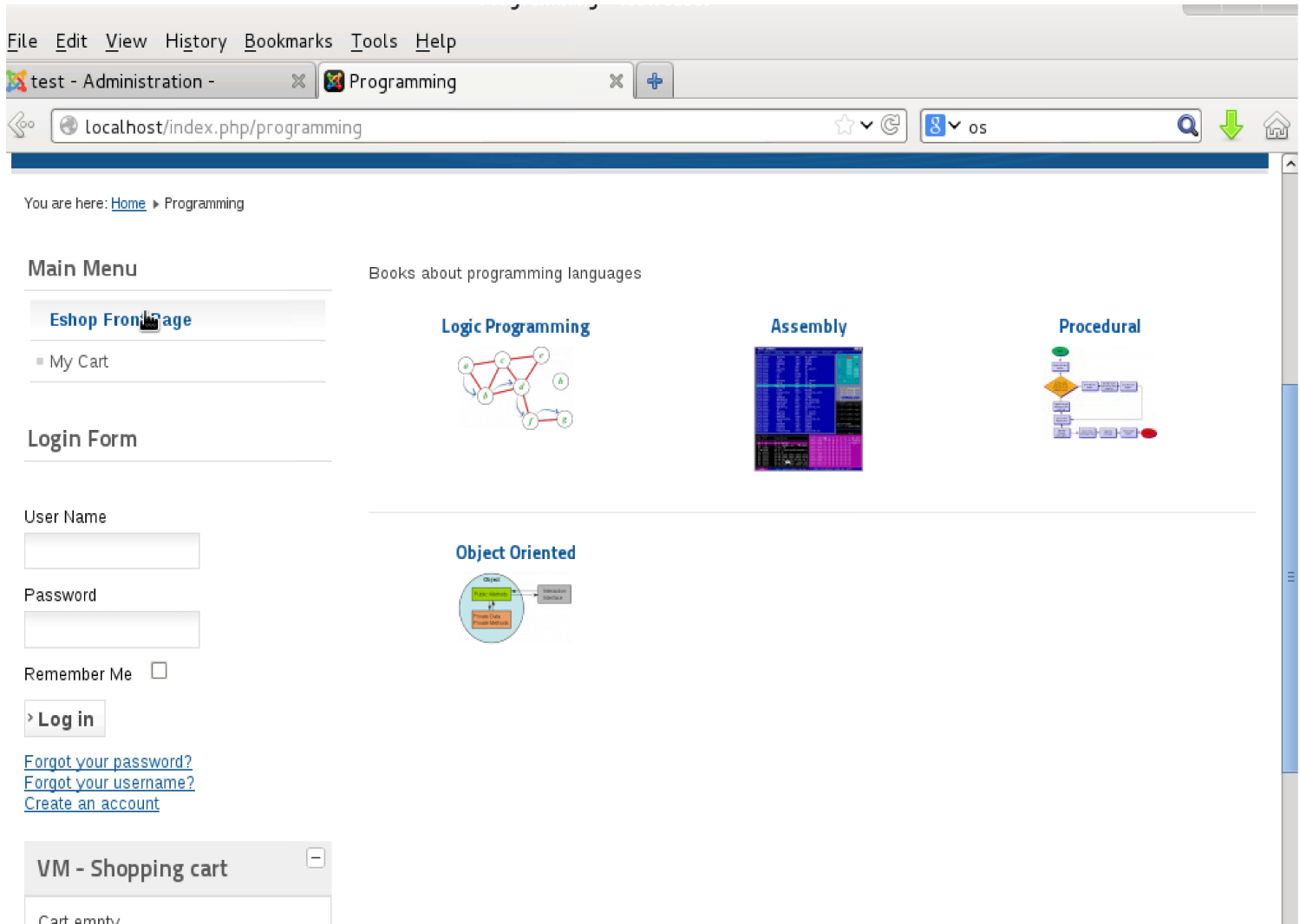
Αφού κάνουμε τις επιθυμητές ρυθμίσεις και εισάγουμε προϊόντα στο ηλεκτρονικό μας κατάστημα μπορούμε να δούμε την μορφή που έχει πάρει αυτή τη στιγμή.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 36: Μορφή ηλεκτρονικού καταστήματος - 1

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 37: Μορφή ηλεκτρονικού καταστήματος - 2

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

The screenshot shows a Joomla! online store interface. The browser address bar displays `localhost/index.php/programming/oop`. The page title is "Object Oriented". The main content area shows "Books about OOP languages" with search results for "Object Oriented".

Main Menu

- Eshop Front Page
- My Cart

Login Form

User Name:

Password:

Remember Me

[Log in](#)

[Forgot your password?](#)
[Forgot your username?](#)
[Create an account](#)

VM - Shopping cart

Cart empty

VM - Search in Shop

Object Oriented

Sort by: Ordering -/+

Results 1 - 2 of 2

Java in a Nutshell

Sales price: 30,00 €
Sales price without tax: 30,00 €

Rating: Not Rated Yet

Current Stock Level

[Product details](#)

Programming in C++

Call for price

Rating: Not Rated Yet

Current Stock Level

[Product details](#)

Εικόνα 38: Μορφή ηλεκτρονικού καταστήματος - 3

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

The screenshot shows a Joomla! e-commerce site interface. The browser address bar displays `localhost/index.php/programming/oop/java`. The page layout includes a top navigation menu with 'File', 'Edit', 'View', 'History', 'Bookmarks', 'Tools', and 'Help'. Below the navigation, there are two tabs: 'test - Administration' and 'Java'. The main content area is titled 'Books about the Java programming language' and shows a search result for 'Java'. The product listing for 'Java in a Nutshell' includes a book cover, the title, sales price (30,00 €), and a 'Product details' button. The left sidebar contains a 'Main Menu' with 'Eshop Front Page' and 'My Cart', a 'Login Form' with fields for 'User Name', 'Password', and a 'Remember Me' checkbox, and a 'VM - Shopping cart' widget showing 'Cart empty'. The right sidebar shows 'Sort by' options and 'Results 1 - 1 of 1'.

Εικόνα 39: Μορφή ηλεκτρονικού καταστήματος - 4

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

4.7 – Μέθοδοι Πληρωμής

Η έκδοση του VirtueMart που χρησιμοποιούμε έρχεται με κάποιες ενσωματωμένες μεθόδους πληρωμής. Αυτές είναι:

- **Authorize.net:** Είναι ένας πάροχος, πύλης πληρωμής (payment gateway) που επιτρέπει τους εμπόρους να δέχονται πληρωμές από πιστωτικές κάρτες και ηλεκτρονικές επιταγές μέσα από το ηλεκτρονικό τους κατάστημα. Η Authorize.net υδρίθηκε το 1996, στην Γιούτα από τον Jeff Knowles, ο οποίος από νωρίς αναγνώρισε την ανάγκη να συνδέσει ιστοσελίδες με επεξεργαστές πιστωτικών καρτών και να κάνει αποδεχτή τις πληρωμές με πιστωτική κάρτα μέσα από το Internet.
- **Paypal:** Είναι μια διεθνής επιχείρηση ηλεκτρονικού εμπορίου, που επιτρέπει τις πληρωμές και μεταφορές χρημάτων να γίνονται μέσα από το Internet. Η Paypal εκτελεί ηλεκτρονικές συναλλαγές χρημάτων, εκ μέρους των πελατών της, χρεώνοντας τους ένα μικρό ποσό.
- **Moneybookers:** Είναι μια παγκόσμια επιχείρηση ηλεκτρονικών συναλλαγών που επιτρέπει τις πληρωμές μέσα από το Internet. Για ιδιώτες χρήστες, προσφέρει έναν καταθετικό λογαριασμό (ή ηλεκτρονικό πορτοφόλι) και ηλεκτρονικές εναλλακτικές των παραδοσιακών χρηματικών συναλλαγών.
 - Moneybookers Credit Cards
 - Moneybookers iDeal
 - Moneybookers Online Bank Transfer
 - Moneybookers Przelewy24
 - Moneybookers Sofortueberweisung
 - Moneybookers Skrill Digital Wallet
 - Moneybookers Giropay
 - Moneybookers Lastschrift
- **Standard:** Μπορεί να χρησιμοποιηθεί για πληρωμές με αντικαταβολή και για πληρωμές με επιταγή.

Επιπλέον μέθοδοι πληρωμής μπορούν να προστεθούν στο VirtueMart εγκαθιστώντας τις αντίστοιχες επεκτάσεις από την σελίδα extensions.virtuemart.net/payments.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Για να χρησιμοποιήσουμε μια μέθοδο πληρωμής, θα πρέπει να δημιουργήσουμε μια, και να την ρυθμίσουμε. Για να γίνει αυτό ακολουθούμε το μενού VirtueMart → Payment Methods → New. Η περιοχή που εμφανίζεται είναι η “Payment Method Information” που αποτελείται από τα εξής πεδία:

- **Payment Name:** Το όνομα της μεθόδου πληρωμής.
- **Published:** Αν η μέθοδος αυτή θα είναι δημοσιευμένη στο ηλεκτρονικό κατάστημα.
- **Payment Description:** Η περιγραφή της μεθόδου πληρωμής, που θα εμφανίζεται στην σελίδα διαδικασίας πληρωμής και θα ενημερώνει τον πελάτη για τις επιλογές του.
- **Payment Method:** Η μέθοδος πληρωμής που θα χρησιμοποιήσουμε.
- **Shopper Group:** Σε ποιες ομάδες χρηστών του VirtueMart θα είναι διαθέσιμη αυτή η μέθοδος πληρωμής.
- **List Order:** Αν χρησιμοποιούμε πάνω από μια μέθοδο πληρωμής, εδώ βάζουμε με ποια σειρά θα εμφανίζεται.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

The screenshot displays the Joomla! administration interface for configuring a new payment method in VirtueMart. The top navigation bar includes 'Site', 'Users', 'Menus', 'Content', 'Components', 'Extensions', 'Help', and 'VirtueMart'. A 'Save & Close' button is visible in the top right. The left sidebar contains a menu with categories like 'Products', 'Orders & Shoppers', and 'Configuration'. The main content area is titled 'Payment Method Information' and shows the following fields:

- Language:** English (United Kingdom)
- Payment Method:** Payment Method
- Payment Name:** Text input field
- Sef Alias:** Text input field
- Published:** Radio buttons for 'No' (selected) and 'Yes'
- Payment Description:** Text area
- Payment Method:** Dropdown menu showing 'VM Payment - Authorize.net'
- Shopper Group:** Text input field with '- Use Default -'
- List Order:** Text input field

Εικόνα 40: VirtueMart - Payment Method Information

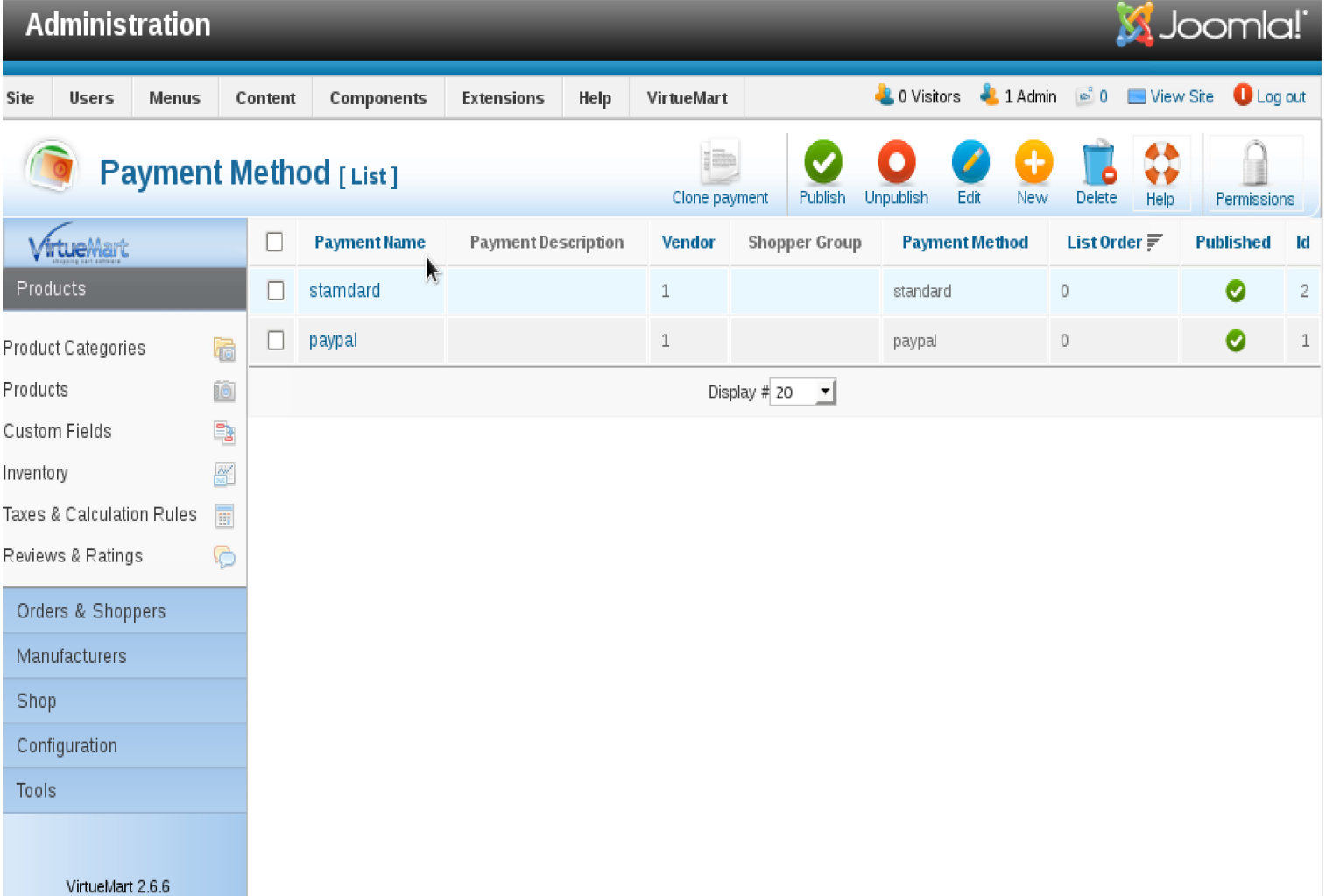
Στην δεύτερη περιοχή “Configuration” βρίσκονται τα πεδία ρύθμισης της μεθόδου πληρωμής. Αυτά βέβαια αλλάζουν ανάλογα με το ποια μέθοδο χρησιμοποιούμε κάθε φορά.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

The screenshot shows the Joomla! administrator interface for configuring the PayPal payment method. The left sidebar contains the VirtueMart menu with 'Configuration' selected. The main content area is titled 'Payment Method Information' and 'Configuration'. It features the PayPal logo and the text 'PayPal payment plugin'. A link suggests registering for a PayPal account. Below this are several configuration sections: 'BASIC PARAMETERS' with a dropdown for 'Standard' and radio buttons for 'Production' (selected) and 'Sandbox'; 'PayPal settings' with a descriptive text and three dropdown menus for 'Let buyers override their PayPal addresses?' (No), 'Prompt buyers for a shipping address' (Prompt for an address, ...), and 'Display only one item and amount for the whole order' (Direct payment); and 'Order status' with a descriptive text and four dropdown menus for 'Pending transactions' (Confirmed by shopper), 'Successful transactions' (Confirmed), 'Cancel transactions' (Cancelled), and 'Capture Payment' (Shipped).

Εικόνα 41: VirtueMart - Payment Method Configuration

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



The screenshot shows the Joomla! Administration interface for the VirtueMart extension. The top navigation bar includes 'Administration' and the Joomla! logo. Below it, a secondary navigation bar lists 'Site', 'Users', 'Menus', 'Content', 'Components', 'Extensions', 'Help', and 'VirtueMart'. The main content area is titled 'Payment Method [List]' and features a toolbar with icons for 'Clone payment', 'Publish', 'Unpublish', 'Edit', 'New', 'Delete', 'Help', and 'Permissions'. A table lists the payment methods:

<input type="checkbox"/>	Payment Name	Payment Description	Vendor	Shopper Group	Payment Method	List Order	Published	Id
<input type="checkbox"/>	standard		1		standard	0	<input checked="" type="checkbox"/>	2
<input type="checkbox"/>	paypal		1		paypal	0	<input checked="" type="checkbox"/>	1

Below the table, there is a 'Display #' dropdown menu set to '20'. The left sidebar contains a navigation menu with categories like 'Products', 'Product Categories', 'Orders & Shoppers', etc. The footer of the sidebar indicates 'VirtueMart 2.6.6'.

Εικόνα 42: Λίστα μεθόδων πληρωμής που δημιουργήσαμε

Κεφάλαιο 5 – Τράπεζα και ηλεκτρονικές συναλλαγές

5.1 – Ηλεκτρονικές συναλλαγές μέσα απο τράπεζα

Την χρονική περίοδο έρευνας και συγγραφής αυτής της πτυχιακής εργασίας, όσο αφορά τις μεγάλες τράπεζες που βρίσκονται στην Ελλάδα, δύο από αυτές προσφέρουν υπηρεσίες ηλεκτρονικών συναλλαγών προς τα ηλεκτρονικά καταστήματα, οι οποίες είναι η Τράπεζα Πειραιώς και η AlphaBank.

Οι υπηρεσίες που προσφέρουν, απευθύνονται σε επιχειρήσεις που διαθέτουν ιστότοπο και ηλεκτρονικό κατάστημα. Μέσα από το οποίο εμπορεύονται τα προϊόντα και υπηρεσίες τους. Οι πληρωμές γίνονται αυτόματα μέσα από το κέντρο πληρωμών της τράπεζας (paycenter) και το ποσό κατατίθεται στον λογαριασμό της επιχείρησης που υπάρχει στην αντίστοιχη τράπεζα.

5.2 – Επιλογές διασύνδεσης με το Πειραιώς Paycenter

- Redirection

Διασύνδεση

1. Ο πελάτης ολοκληρώνει τις αγορές του στο e-shop της επιχείρησής σας.
2. Ξεκινώντας τη διαδικασία πληρωμής, μεταβαίνει αυτόματα στην ειδική σελίδα πληρωμών του Πειραιώς Paycenter. Εκεί ενημερώνεται για τη σχετική χρέωση και πληκτρολογεί τα στοιχεία της κάρτας του.
3. Η διεκπεραίωση της πληρωμής γίνεται με απόλυτη ασφάλεια από το Πειραιώς Paycenter, που ενημερώνει την επιχείρησή σας αυτόματα.
4. Ο πελάτης επιστρέφει στο δικτυακό τόπο της επιχείρησής σας (e-shop). Από εκεί ενημερώνεται για την ολοκλήρωση της συναλλαγής του.

Πλεονεκτήματα

- Η επιχείρησή σας δεν κρατά κανένα στοιχείο της κάρτας που χρησιμοποιήθηκε κατά την πληρωμή. Αυτό διευκολύνει τη διαδικασία πιστοποίησης κατά PCI
- Η υλοποίηση μπορεί να ολοκληρωθεί πολύ γρήγορα

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- iFrame

Διασύνδεση

1. Ο πελάτης ολοκληρώνει τις αγορές του στο δικτυακό τόπο του e-shop. Εκεί ξεκινά τη διαδικασία πληρωμής. Ενημερώνεται για τη σχετική χρέωση και πληκτρολογεί τα στοιχεία της κάρτας του
2. Η διεκπεραίωση της πληρωμής γίνεται με απόλυτη ασφάλεια από το Πειραιώς Paycenter, χωρίς να το αντιλαμβάνεται ο πελάτης.
3. Το Πειραιώς Paycenter ενημερώνει την επιχείρησή σας αυτόματα.
4. Ο πελάτης ενημερώνεται για την ολοκλήρωση της συναλλαγής του από το e-shop σας.

Πλεονεκτήματα

- Ομοιόμορφη εμπειρία χρήσης για τον πελάτη σας κατά την πλοήγηση και χρήση του ηλεκτρονικού καταστήματος (e-shop)
- Διατίθεται χωρίς να φέρει λογότυπα της Τράπεζας Πειραιώς ή άλλα χαρακτηριστικά. Επομένως, η επιχείρησή σας μπορεί να την προσαρμόσει απόλυτα στις απαιτήσεις της εξασφαλίζοντας την εξαιρετική εμπειρία χρήσης του πελάτη
- Η επιχείρησή σας δεν κρατά κανένα στοιχείο της κάρτας που χρησιμοποιήθηκε κατά την πληρωμή. Αυτό διευκολύνει τη διαδικασία πιστοποίησης κατά PCI

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

XML Web Service

Διασύνδεση

1. Ο πελάτης ολοκληρώνει τις αγορές του στο δικτυακό τόπο του e-shop σας. Εκεί παραμένει για όλη τη διαδικασία πληρωμής, στο περιβάλλον χρήσης που η επιχείρηση έχει διαμορφώσει. Από τις σελίδες του διαδικτυακού τόπου της επιχείρησής σας ενημερώνεται για τη σχετική χρέωση και πληκτρολογεί τα στοιχεία της κάρτας του.
2. Τα στοιχεία της κάρτας του πελάτη αποστέλλονται μέσω ασφαλούς διασύνδεσης με τη χρήση XML web service στο Πειραιώς Paycenter. Η επιχείρηση υποχρεωτικά οφείλει να παρέχει ελάχιστη κρυπτογράφηση SSL 128bit.
3. Η διεκπεραίωση της πληρωμής γίνεται με απόλυτη ασφάλεια από το Πειραιώς Paycenter. Αυτό ενημερώνει την επιχείρησή σας αυτόματα.
4. Ο πελάτης ενημερώνεται για την ολοκλήρωση της συναλλαγής του από το e-shop σας.

Πλεονεκτήματα

- Απόλυτος έλεγχος εμπειρίας χρήσης κατά την πλοήγηση και χρήση του δικτυακού τόπου της επιχείρησης
- Κατάλληλη για επιχειρήσεις με ανεπτυγμένη υποδομή ασφαλείας και διαχείρισης της πελατείας τους, όταν η επιχείρηση έχει ειδικές απαιτήσεις και ανάγκες

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

5.3 - Alpha e-Commerce

Η Alpha Bank, μέσω της υπηρεσίας ηλεκτρονικού εμπορίου Alpha e-Commerce, προσφέρει στην επιχείρησή σας τη δυνατότητα να παρέχει ολοκληρωμένη εξυπηρέτηση στους Πελάτες της, καλύπτοντας όλες τις ανάγκες που προκύπτουν από την πραγματοποίηση συναλλαγών με κάρτες από απόσταση.

Η υπηρεσία υποστηρίζει πληρωμές με χρεωστικές, πιστωτικές και προπληρωμένες κάρτες:

- American Express
- Visa, Visa Electron
- MasterCard
- Maestro
- Diners

Επιλογές διασύνδεσης:

- Διασύνδεση Re-direct: Επιλέγοντας σαν τρόπο πληρωμής την κάρτα, ο Πελάτης, μεταφέρεται αυτομάτως στην ασφαλή σελίδα πληρωμής της υπηρεσίας Alpha e-Commerce, όπου αφού ενημερωθεί για τα στοιχεία της συναλλαγής και τη χρέωση, εισάγει τα στοιχεία της κάρτας του.

Μετά την επεξεργασία της πληρωμής από την Τράπεζα, ο Πελάτης επιστρέφει αυτομάτως στον δικτυακό τόπο της επιχείρησής, όπου ενημερώνεται για την ολοκλήρωση της συναλλαγής. Παράλληλα, σε περίπτωση εγκρίσεως της συναλλαγής, αποστέλλεται από την Τράπεζα σχετικό ενημερωτικό email στην επιχείρηση.

Βασικά Χαρακτηριστικά:

- Σελίδα πληρωμής που φιλοξενείται στην Τράπεζα, με δυνατότητα προσαρμογής της εμφανίσεώς της βάσει του σχεδιασμού που επιθυμεί η επιχείρηση.
- Εμφάνιση διαφορετικής σελίδας πληρωμής στους Πελάτες, ανάλογα με την γλώσσα που έχει επιλεγεί από τον κάθε Πελάτη.
- Εύκολη υλοποίηση με βάση τις οδηγίες που παρέχονται στα αναλυτικά τεχνικά εγχειρίδια της υπηρεσίας.
- Πλήρως πιστοποιημένη πλατφόρμα σύμφωνα με τις προδιαγραφές PCI DSS.
- Σύγχρονο χειριστικό εργαλείο για άμεση παρακολούθηση των συναλλαγών και διαχείριση των εισπράξεων.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Διασύνδεση XML Direct: Ο Πελάτης παραμένει στην ιστοσελίδα της επιχειρήσεως, ολοκληρώνοντας την πληρωμή του σε αυτή. Υποχρεωτικά παρέχεται SSL encryption 128 bit ενώ πρέπει να πληρούνται και οι προδιαγραφές ασφαλείας των Διεθνών Οργανισμών Visa, MasterCard, American Express & PCI Security Standards Council

Βασικά Χαρακτηριστικά:

- Έλεγχος της εμπειρίας του Πελάτη αποκλειστικά από το ηλεκτρονικό κατάστημα της επιχειρήσεως.
- Απαραίτητη συμμόρφωση της επιχειρήσεως κατά PCI DSS.
- Σύγχρονο διαχειριστικό εργαλείο για άμεση παρακολούθηση των συναλλαγών και διαχείριση των εισπράξεων.

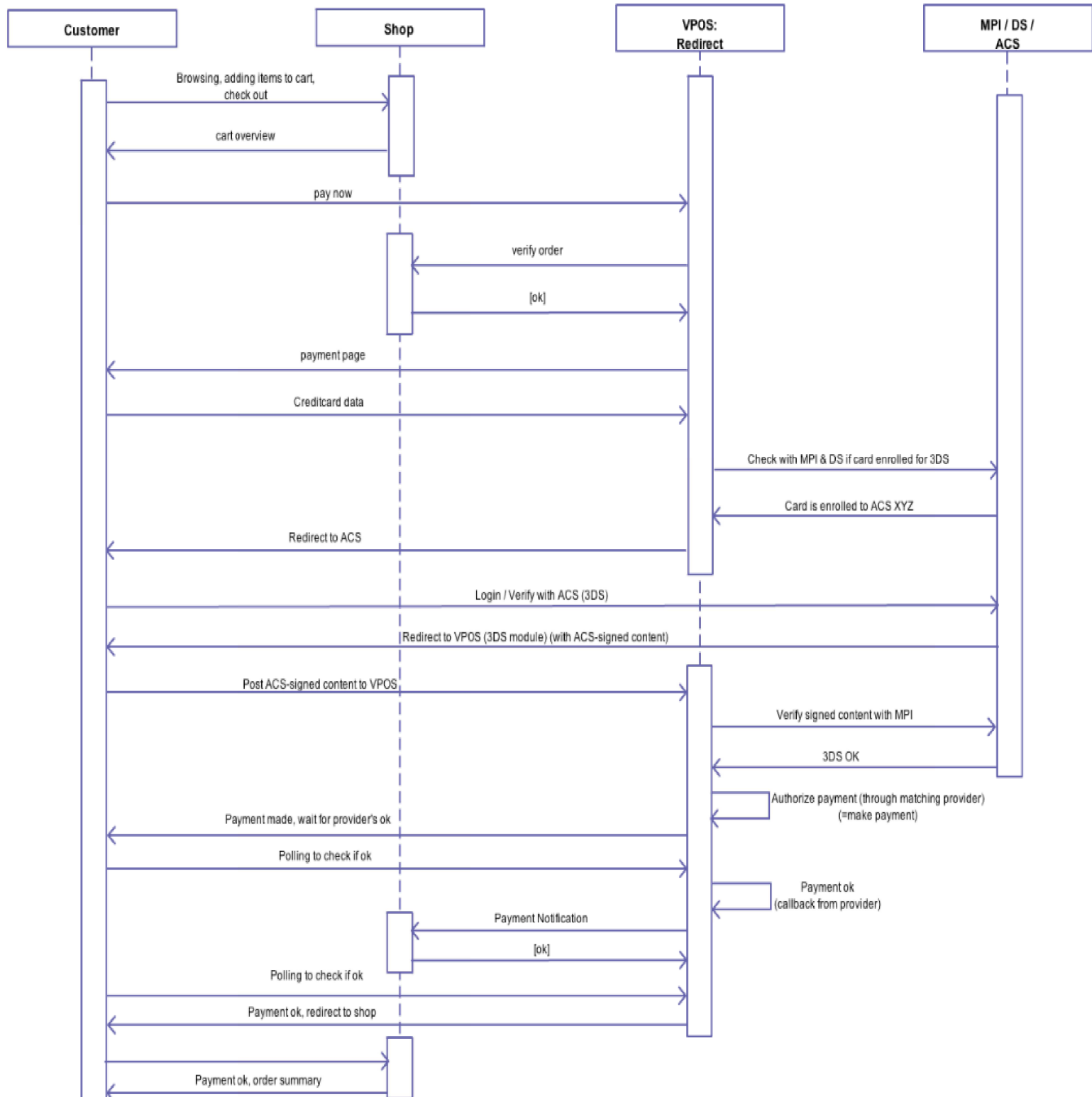
Το επίπεδο ασφαλείας της υπηρεσίας Alpha e-Commerce εξασφαλίζεται από τα παρακάτω:

- Οι πληροφορίες σχετικά με την κάρτα (αριθμός κάρτας, CVV2/CVC2, ημερομηνία λήξεως) μεταδίδονται / μεταφέρονται μέσω διαδικτύου σε κρυπτογραφημένη μορφή (SSL 128-bit encryption) και δεν είναι προσβάσιμες από το ηλεκτρονικό σας κατάστημα.
- Τα συστήματα και οι διαδικασίες που χρησιμοποιούνται από την Alpha Bank εμποδίζουν σε μη εξουσιοδοτημένους τρίτους την πρόσβαση στα δεδομένα και τα πληροφοριακά της συστήματα.
- Η ιστοσελίδα της Τραπέζης στην οποία εισάγει τα στοιχεία της κάρτας του ο Πελάτης της επιχειρήσεως, φέρει ψηφιακό πιστοποιητικό για να μπορεί ο καθένας να ελέγξει τη γνησιότητά της, δηλαδή να διαπιστώσει ότι ανήκει πραγματικά στην υπηρεσία Alpha e-Commerce ή Alpha e-Pay (πρώην delta pay) της Alpha Bank.
- Η διαχείριση της Υπηρεσίας Ηλεκτρονικού Εμπορίου Alpha e-Commerce γίνεται από εξουσιοδοτημένα άτομα της επιχειρήσεως, στους οποίους παραδίδονται ατομικοί κωδικοί πρόσβασης (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 ανάλογο κωδικό, η Υπηρεσία Ηλεκτρονικού Εμπορίου Alpha e-Commerce ζητά αυτομάτως από τον Πελάτη σας να πληκτρολογήσει τον μυστικό του κωδικό.
- Η Υπηρεσία Ηλεκτρονικού Εμπορίου Alpha e-Commerce ακολουθεί τις βέλτιστες διεθνείς πρακτικές στον τομέα των πληρωμών για το ηλεκτρονικό εμπόριο και είναι πλήρως συμβατή με τα πρωτόκολλα ασφαλείας των διεθνών οργανισμών καρτών Verified by Visa και MasterCard SecureCode για ασφαλείς on-line πληρωμές με κάρτα.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 43: VPOS redirect - UML Sequence Diagram

Κεφάλαιο 6 – Ηλεκτρονικό εμπόριο και κίνδυνοι

6.1 – Βασικές έννοιες και αρχές

Στην ασφάλεια πληροφοριακών συστημάτων, μπορούν να διακριθούν τέσσερις βασικές έννοιες

1. Πόρος – Resource:

Είναι η οντότητα που έχει ανάγκη προστασίας. Τέτοιες οντότητες μπορεί να είναι δεδομένα, εφαρμογές, διακομιστές ή επικοινωνιακός εξοπλισμός.

2. Απειλή – Threat:

Είναι η οντότητα εκείνη που δυνητικά μπορεί να αποκτήσει ανεπιθύμητη πρόσβαση σε έναν προστατευμένο πόρο.

3. Κενό ασφάλειας – Vulnerability:

Κενό ασφάλειας μπορεί να θεωρηθεί το αδύναμο σημείο του συστήματος ασφάλειας του προστατευόμενου πόρου.

4. Exploit:

Σε ελεύθερη μετάφραση μπορεί να αποδοθεί ως “επίθεση που εκμεταλλεύεται ένα κενό ασφάλειας”. Αναφέρεται σε κάποιο λογισμικό ή κομμάτι δεδομένων ή σειρά από εντολές που αποσκοπούν σε απρόβλεπτη συμπεριφορά του πόρου.

Όσο αφορά τις βασικές αρχές της ασφάλειας πληροφοριακών συστημάτων, μπορούν να διακριθούν σε τρεις:

1. Ακεραιότητα:

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

2. Διαθεσιμότητα:

Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

3. Εμπιστευτικότητα

Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

6.2 – DoS attack ή DDoS attack

Denial-of-Service (άρνηση υπηρεσίας) ή Distributed Denial-of-Service (κατανεμημένη άρνηση υπηρεσίας) είναι η επίθεση που αναφέρεται στην απόπειρα, ένας πόρος να μην είναι διαθέσιμος στους χρήστες του. Αν και τα μέσα, τα κίνητρα και οι στόχοι διαφέρουν, γενικώς αποσκοπεί στην προσωρινή ή επ'αόριστον διακοπή της προσφερόμενης υπηρεσίας του πόρου. Από τον ορισμό καταλαβαίνουμε πως μια επίθεση τύπου DDoS γίνεται από πάνω από ένα άτομο, ή bots (botnet). Μια επίθεση DoS γίνεται απο ένα άτομο ή ένα μόνο σύστημα. Κατά το 2014, η συχνότητα αναγνωρισμένων επιθέσεων DDoS είναι περίπου 28 ανά ώρα.

Τυπικά οι επιτιθέμενοι εστιάζουν σε διακομιστές δικτύου μεγάλου μεγέθους. Για παράδειγμα τράπεζες, πύλες πληρωμής πιστωτικών καρτών, ακόμη και root nameservers. Οι επιθέσεις αυτές είναι γνωστές και στις επιχειρήσεις. Επίσης το τελευταίο καιρό είναι και μια μορφή αντίδρασης, για παράδειγμα η ομάδα ακτιβιστών Anonymous . Ο Richard Stallman έχει δηλώσει πως είναι μια μορφή “Internet Street Protests”. Η επίθεση αυτή έχει σχετιστεί με τα δίκτυα υπολογιστών, αλλά δεν περιορίζεται μόνο εκεί.

Μια τυπική μέθοδος υλοποίησης της επίθεσης είναι η συμφόρηση λόγω αιτήσεων επικοινωνίας προς τον πόρο, τόσο όσο να μην μπορεί να ανταποκριθεί στην κίνηση, ή να ανταποκρίνεται αρκετά αργά ώστε να πρακτικά να θεωρείτε μη διαθέσιμος.

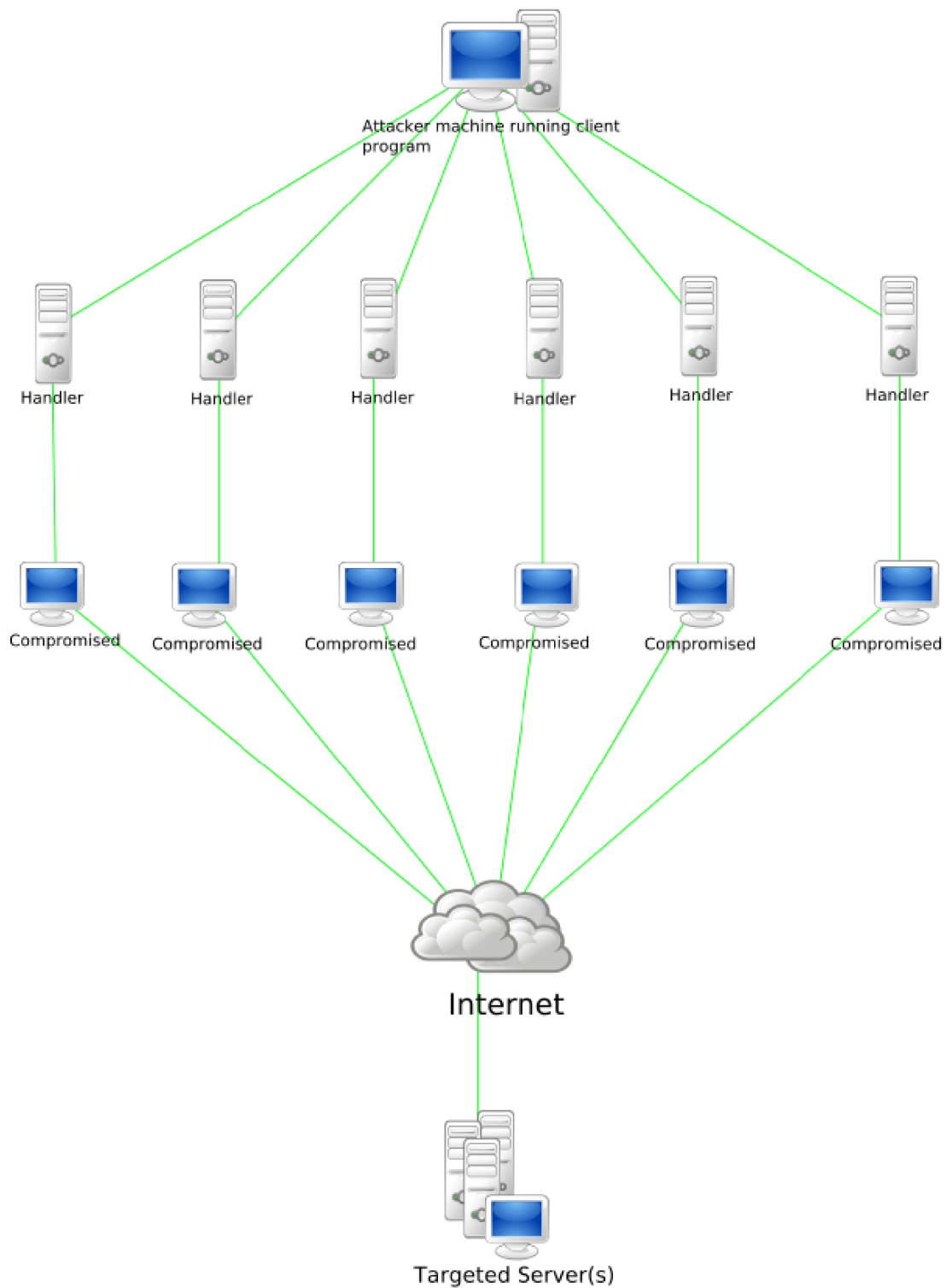
Συμπτώματα μιας επίθεσης DoS ή DDoS περιλαμβάνουν:

- Ασυνήθιστα χαμηλή επίδοση δικτύου.
- Μη διαθεσιμότητα ενός συγκεκριμένου ιστότοπου.
- Ανικανότητα πρόσβασης σε οποιοδήποτε ιστότοπο.
- Δραματική αύξηση στον αριθμό λήψης spam ηλεκτρονικών μηνυμάτων.
- Άρνηση πρόσβασης στο δίκτυο.

Οι επιθέσεις τέτοιου τύπου μπορούν να κατηγοριοποιηθούν σε πέντε ομάδες:

- Κατανάλωση υπολογιστικών πόρων, όπως μνήμη, χώρου αποθήκευσης, χρόνος επεξεργασίας ή εύρος ζώνης.
- 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.
- Παρεμπόδιση των μέσων επικοινωνίας μεταξύ των χρηστών και του θύματος, έτσι ώστε να μην μπορούν πλέον να επικοινωνούν επαρκώς

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 44: Σχήμα επίθεσης DDoS

80

Ματσάγκος Ηρακλής Χρήστος (ΑΜ 1583),
Μαυρόπουλος Βασίλειος (ΑΜ 2527)

6.3 – SQL Injection

Γενικά η έγχυση κώδικα (code injection) είναι η εκμετάλλευση ενός κενού ασφάλειας (exploitation) που προκαλείται από την επεξεργασία μη έγκυρων δεδομένων. Η έγχυση κώδικα χρησιμοποιείται για να αλλάξει την πορεία εκτέλεσης ενός προγράμματος.

Πιο συγκεκριμένα, μια επίθεση SQL injection χρησιμοποιείτε στις επιθέσεις δεδομενοστραφών λογισμικών, κατά τη διάρκεια της οποίας, SQL δηλώσεις εισάγονται για εκτέλεση μέσα από ένα πεδίο εισαγωγής.

Σε μια επίθεση SQL injection ένα κακόβουλο κομμάτι κώδικα εισάγεται μέσα σε strings τα οποία θα περάσουν αργότερα στον SQL Server για μεταγλώτιση και εκτέλεση. Ο SQL Server θα εκτελέσει όλα τα συντακτικά έγκυρα ερωτήματα που λαμβάνει. Ακόμη και παραμετροποιημένα δεδομένα μπορεί να αλλοιωθούν από ένα εξειδικευμένο εισβολέα.

Η πρωταρχική μορφή της επίθεσης 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.

Η διαδικασία της έγχυσης 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

Κάποιες από τις τεχνικές υλοποίησης είναι οι παρακάτω:

- Λανθασμένη επεξεργασία χαρακτήρων διαφυγής.

Έστω πως έχουμε το κομμάτι κώδικα:

```
statement = "SELECT * FROM users WHERE name = '" +  
userName + "';"
```

Ο κώδικας αυτός έχει σχεδιαστεί για να τραβάει εγγραφές για έναν χρήστη που ορίζεται στην μεταβλητή userName από την πίνακα users της βάσης δεδομένων. Αν τώρα ορίσουμε την μεταβλητή userName ως:

```
' or '1'='1' ή ' or '1'='1' --
```

Η δήλωση θα πάρει την μορφή:

```
SELECT * FROM users WHERE name = '' OR '1'='1'; ή
```

```
SELECT * FROM users WHERE name = '' OR '1'='1' -- ';
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Αν ο κώδικας αυτός χρησιμοποιούνταν σε μια διαδικασία πιστοποίησης, θα μπορούσαμε να επιλέξουμε έναν έγκυρο χρήστη μια και η έκφραση '1'='1' είναι πάντα αληθής. Η παρακάτω έγχυση κώδικα μέσα απο την μεταβλητή userName μπορεί να χρησιμοποιηθεί για την διαγραφή του πίνακα users.

```
a';DROP TABLE users; SELECT * FROM userinfo WHERE 't' = 't
```

Ο παραπάνω κώδικας μπορεί να αποδοθεί στην έκφραση:

```
SELECT * FROM users WHERE name = 'a';DROP TABLE users; SELECT * FROM userinfo WHERE 't' = 't';
```

- Λανθασμένος χειρισμός τύπων:

Αυτή η μορφή SQL injection μπορεί να συμβεί όταν ένα πεδίο που συμπληρώνεται από τον χρήστη δεν ελέγχεται για το σωστό τύπο δεδομένων. Για παράδειγμα έστω πως έχουμε την παρακάτω εντολή

```
statement = "SELECT * FROM userinfo WHERE id =" + a_variable + ";"
```

Αμέσως καταλαβαίνουμε πως ο προγραμματιστής θέλει η μεταβλητή a_variable να είναι τύπου ακέραιου αριθμού. Όμως ο χρήστης μπορεί να εισάγει το παρακάτω παρακάμπτοντας την ανάγκη χαρακτήρων διαφυγής.

```
1;DROP TABLE users
```

Έτσι η δήλωση θα πάρει την μορφή

```
SELECT * FROM userinfo WHERE id=1;DROP TABLE users;
```

Με αποτέλεσμα ο πίνακας users να διαγραφεί.

6.4 – Phishing

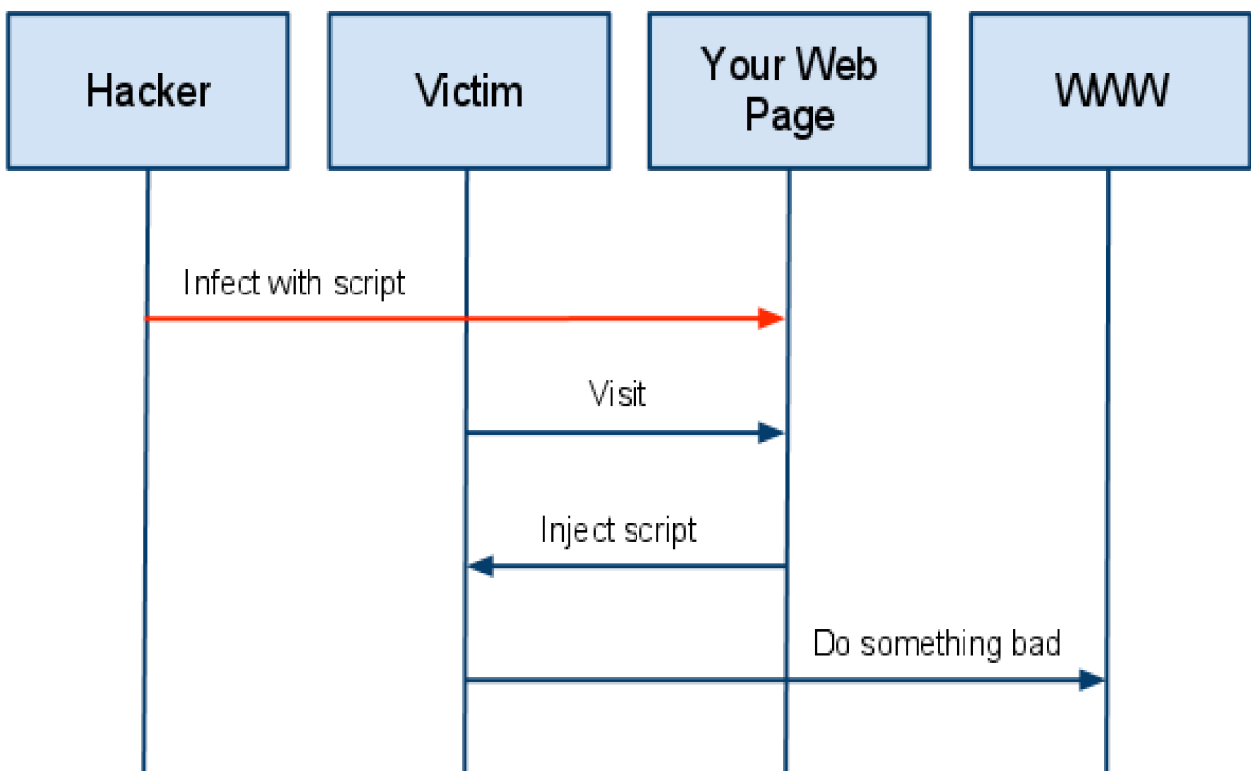
Η επίθεση Phishing μπορεί να συμπεριληφθεί στην κατηγορία του Social engineering και αναφέρετε στην απόπειρα απόκτησης ευαίσθητων πληροφοριών όπως ονόματα χρηστών, κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών.

Στόχος αυτής της επίθεσης είναι ο χρήστης να πειστεί πως η επικοινωνία γίνεται μεταξύ αυτού και τον εμπιστευόμενο πόρο. 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.

6.5 - Cross Site Scripting

Cross Site Scripting ή XSS, είναι μια από τις πιο κοινές επιθέσεις που γίνονται σε επίπεδο εφαρμογής μέσα από το δίκτυο. Μια επίθεση XSS συνήθως στοχεύει σε scripts που ενσωματώνονται σε μια σελίδα και εκτελούνται από την μεριά του πελάτη αντί της μεριάς του διακομιστή. Η απειλή προέρχεται από την αδύναμη ασφάλεια των client-side scripting γλωσσών, όπως η HTML, JavaScript VBScript, ActiveX, Flash κ.ο.κ. Η λογική της επίθεσης XSS είναι η εκμετάλλευση των client-side scripts μιας δικτυακής εφαρμογής για να τρέξει με τον τρόπο που επιθυμεί ο κακόβουλος χρήστης.

Σε μια τοπική επίθεση XSS ο επιτιθέμενος μολύνει τον διακομιστή με ένα κακόβουλο client-side script. Όταν ο χρήστης επισκεφτεί την ιστοσελίδα του διακομιστή, τότε αυτόματα κατεβάζει το κακόβουλο script και το εκτελεί. Υπάρχουν πολλές διαφοροποιήσεις της επίθεσης αυτής, αλλά γενικώς έχει την μορφή της παρακάτω εικόνας.



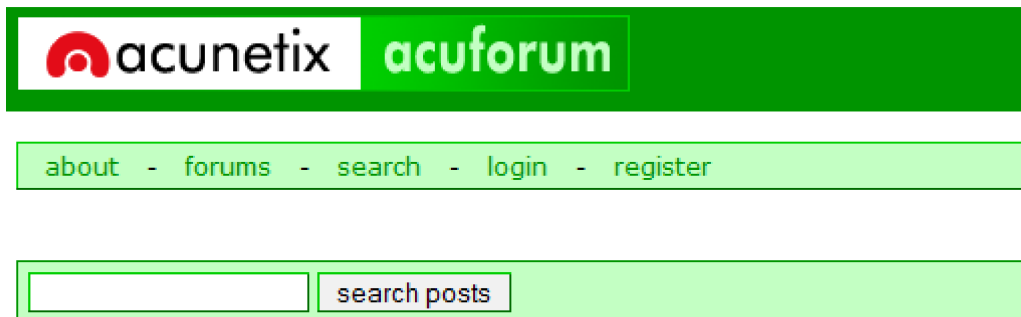
Εικόνα 45: Σχήμα επίθεσης XSS

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Ένα παράδειγμα μιας επίθεσης XSS είναι όταν ένας κακόβουλος χρήστης βάζει ένα script στην διεύθυνση URL μιας σελίδα ηλεκτρονικού καταστήματος το οποίο μετά μεταβιβάζει τον χρήστη σε μια πανομοιότυπη κακόβουλη σελίδα. Η κακόβουλη σελίδα αργότερα εκτελεί ένα script το οποίο συλλαμβάνει το cookie του χρήστη και στέλνεται στον επιτιθέμενο, που μπορεί έτσι να κλέψει την συνεδρία. Παρόλο που καμία πραγματική επίθεση δεν έγινε στην ίδια την σελίδα, η επίθεση κατάφερε να αποκτήσει πρόσβαση στην συνεδρία. Ένα μικρό τρικ που χρησιμοποιείτε συχνά για να γίνονται τα κακόβουλα URLs λιγότερο αντιληπτά είναι η κωδικοποίησή τους.

Οι διαδικτυακές εφαρμογές πλέον δεν είναι στατικές HTML σελίδες. Είναι δυναμικές και αποτελούνται από περιεχόμενο που συνεχώς αλλάζει. Οι σύγχρονες ιστοσελίδες αντλούν δεδομένα από πολλές και διαφορετικές πηγές, τα οποία συγχωνεύονται για να δώσουν το τελικό περιεχόμενο αποτέλεσμα της σελίδας. Το περιεχόμενο αυτό μπορεί να αποτελείται από απλό κείμενο, εικόνες και ετικέτες HTML όπως της παραγράφου <p>, της εικόνας και για script <script>. Πολλές φορές οι επιτιθέμενοι χρησιμοποιούν την δυνατότητα της σελίδας “comments” για να εισάγουν ένα σχόλιο το οποίο περιέχει κάποιο script. Οπότε κάθε χρήστης που θα προβάλει το σχόλιο στον φυλλομετρητή του, θα κατεβάσει και το script το οποίο και θα εκτελεστεί, οδηγώντας έτσι σε ανεπιθύμητες ενέργειες. Κάποιες φορές μια απλή κοινοποίηση σε ένα προφίλ του Facebook μπορεί να περιέχει κάποιο κακόβουλο script, το οποίο αν δεν επεξεργαστεί από το Facebook θα εγχυθεί στον “τοίχο” του χρήστη και θα εκτελεστεί από οποιοδήποτε άλλο χρήστη επισκέπτεται το προφίλ.

Για να δώσουμε ένα παράδειγμα υλοποίησης μια επίθεσης XSS, μπορούμε να φορτώσουμε την σελίδα <http://testasp.vulnweb.com/search.asp> . Βλέπουμε πως η φόρμα της σελίδας αποτελείται από ένα πεδίο εισαγωγής και ένα κουμπί.



Εικόνα 46: Μορφή της σελίδας που επισκεφτήκαμε

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Αν τώρα εισάγουμε τον παρακάτω κώδικα στο πεδίο εισαγωγής θα δούμε πως εμφανίζεται μια φόρμα σύνδεσης ζητώντας όνομα χρήστη και κωδικό πρόσβασης.

```
<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>
```



The screenshot shows the top part of a Joomla! forum page. At the top, there is a navigation bar with the 'acunetix' logo and 'acuforum' text. Below this is a menu with links for 'about', 'forums', 'search', 'login', and 'register'. A search bar is present with a 'search posts' button. Below the search bar, the text 'You searched for \'' is displayed. A bold instruction reads 'Please login with the form below before proceeding:'. Underneath, there are two input fields: 'Login:' and 'Password:'. A 'LOGIN' button is located below the password field.

Εικόνα 47: Εμφάνιση φόρμας που δεν προβλέπονταν από τον προγραμματιστή

Βλέπουμε πως μόλις δημιουργήσαμε μια ψεύτικη φόρμα σύνδεσης μέσα από την οποία το θύμα μπορεί να εισάγει τα στοιχεία του. Επίσης μέσα στον κώδικα, χρησιμοποιώντας το χαρακτηριστικό `action` της φόρμας μπορούμε να αλλάξουμε τον προορισμό

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

destination.asp με έναν δικό μας. Ένας άλλος τρόπος για να πάρουμε το ίδιο αποτέλεσμα είναι αν εισάγουμε ως διεύθυνση στον φυλλομετρητή το παρακάτω:

```
http://testasp.vulnweb.com/Search.asp?tfSearch=%3Cbr%3E%3Cbr%3EPlease+login+with+the+form+below+before+proceeding%3A%3Cform+action%3D%22test.asp%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
```

6.6 - Hidden Field Manipulation

Κάποιες σελίδες και δικτυακές εφαρμογές, ενθέτουν στον κώδικά τους κρυφά πεδία με σκοπό οι τιμές τους να περνάνε ως ορίσματα στις μεθόδους get και post. Ένα τυπικό κρυφό πεδίο έχει την μορφή: `<input type="hidden">`.

Λόγο κακών πρακτικών προγραμματισμού, αρκετές φορές τα πεδία αυτά μπορούν να περιέχουν ευαίσθητη πληροφορία, όπως η τιμή ενός προϊόντος σε ένα ηλεκτρονικό κατάστημα.

Έστω πως έχουμε τον παρακάτω HTML κώδικα μιας φόρμας σε ένα ηλεκτρονικό κατάστημα.

```
<form method="get" action="page.aspx">
<input type="text" name="product" value="Shirt"></br>
<input type="hidden" name="PRICE" value="50">
Product price: 50.00 € </br>
<input type="submit" value="submit">
</form>
```

Για έναν απλό χρήστη το αίτημα θα έχει την μορφή:

<http://www.example.com/page.aspx?product=Shirt&price=50>

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Για έναν κακόβουλο χρήστη που γνωρίζει αυτήν την αδυναμία μπορεί εύκολα να αλλάξει το πεδίο της τιμής με αυτή που επιθυμεί. Δηλαδή το αίτημα θα έχει την μορφή:

<http://www.example.com/page.aspx?product=Shirt&price=2>

6.7 - Cross-Site Request Forgery

Cross-Site Request Forgery ή CSRF είναι μια επίθεση κατά την οποία η εκμετάλλευση ενός αδύναμου σημείου γίνεται μέσα από τον χρήστη τον οποίο το σύστημα εμπιστεύεται. Στην επίθεση Cross-Site Scripting, ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη που έχει ο χρήστης προς τον πόρο, ενώ το αντίθετο συμβαίνει στην επίθεση Cross-Site Request Forgery. Δηλαδή ο επιτιθέμενος εκμεταλλεύεται την εμπιστοσύνη που έχει ο πόρος προς τον χρήστη.

Τυπικά, ο επιτιθέμενος θα ξεγελάσει το θύμα στο να μπει σε μια σελίδα ή να ανοίξει ένα URL σύνδεσμο που θα περιέχει κακόβουλες αιτήσεις. Αποκαλούνται κακόβουλες επειδή στην επίθεση CSRF θα χρησιμοποιηθεί η ταυτότητα και τα δικαιώματα του θύματος για να εκτελεστούν αιτήματα του επιτιθέμενου, που μπορεί να είναι η αλλαγή λεπτομερειών υποβολής, αγορές ή πληρωμές προς τον επιτιθέμενο ή σε κάποιο τρίτο πρόσωπο.

Σε κάθε αίτημα που κάνει ένας φυλλομετρητής ιστού σε κάποια ιστοσελίδα, μαζί με τα δικαιώματα πρόσβασης, θα κρατήσει και το cookie συνεδρίας του χρήστη, διεύθυνση IP του χρήστη κ.ο.κ. Έτσι αν η σύνδεση του χρήστη είναι ακόμη έγκυρη, ο επιτιθέμενος μπορεί να ξεκινήσει μια επίθεση CSRF για να εκτελέσει οποιαδήποτε αιτήματα επιθυμεί προς την ιστοσελίδα. Χωρίς όμως η ιστοσελίδα να μπορεί να διαχωρίσει αν τα αιτήματα είναι νόμιμα ή όχι.

Όπως έχει περιγραφεί πιο πάνω, για να πετύχει μια CSRF επίθεση, ο χρήστης πρέπει πρώτα να συνδεθεί με τον στόχο. Θεωρώντας πως ο χρήστης έχει επικυρώσει τα δικαιώματα του με την ιστοσελίδα-στόχο, ο επιτιθέμενος μπορεί να βάλει έναν σύνδεσμο ή ένα script σε μια τρίτη ιστοσελίδα που το θύμα θα επισκεφθεί. Έτσι όταν το θύμα ανοίξει αυτήν την τρίτη ιστοσελίδα, θα εκτελεστεί το κακόβουλο script χωρίς το θύμα να γνωρίζει κάτι. Κάτι τέτοιο μπορεί να γίνει αν για παράδειγμα, σε κάποιο chat ή forum, ο επιτιθέμενος κοινοποιήσει ένα HTML στοιχείο εικόνας. Μόνο που η πηγή της εικόνας περιέχει έναν σύνδεσμο που εκτελεί μια ενέργεια στο τραπεζικό λογαριασμό του θύματος. Μια τέτοια ενέργεια, όπως μεταφορά χρημάτων, μπορεί να περιγραφεί μέσα σε ένα HTML στοιχείο εικόνας όπως στο παρακάτω κομμάτι κώδικα:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```

```

6.8 - S-HTTP και HTTPS

Το HTTPS (Hypertext Transfer Protocol Secure) χρησιμοποιείται στην πληροφορική για να δηλώσει μία ασφαλή δικτυακή σύνδεση http. 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 (πχ αριθμοί πιστωτικών καρτών, passwords κοκ).

Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, 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 προηγουμένως, 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 που περιγράφηκε στην προηγούμενη ενότητα και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Πολλοί χρήστες πιστωτικών καρτών θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τον αριθμό της πιστωτικής τους κάρτας από κατάχρηση. Αυτό όμως δεν ισχύει: 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 χάκερ να έχουν επιτεθεί στον server και από εκεί να έχουν υποκλέψει τα ευαίσθητα προσωπικά δεδομένα.

Το HTTPS είναι ένα σύστημα URI το οποίο έχει πανομοιότυπη σύνταξη στο καθιερωμένο σύστημα HTTP, εκτός από το πρόγραμμα του token. Ωστόσο, το HTTPS σηματοδοτεί το πρόγραμμα περιήγησης για να χρησιμοποιήσετε ένα επιπλέον επίπεδο κρυπτογράφησης SSL / TLS για την προστασία της κυκλοφορίας. Το SSL είναι ιδιαίτερα κατάλληλο για το HTTP, δεδομένου ότι μπορεί να προσφέρει κάποια προστασία, ακόμη και αν μόνο η μία πλευρά της επικοινωνίας έχει πιστοποιηθεί. Αυτή είναι η περίπτωση με τις συναλλαγές HTTP μέσω του Διαδικτύου, όπου συνήθως μόνο ο διακομιστής είναι πιστοποιημένος.

Το HTTPS δημιουργεί ένα ασφαλές κανάλι σε ένα μη ασφαλές δίκτυο. Αυτό εξασφαλίζει επαρκή προστασία από man-in-the-middle επιθέσεις, υπό την προϋπόθεση ότι η επαρκής κρυπτογράφηση χρησιμοποιείται και ότι το πιστοποιητικό του διακομιστή επαληθεύεται και είναι αξιόπιστο.

Το S-HTTP αναπτύχθηκε από τον Eric Rescorla και Allan M. Schiffman, και δημοσιεύθηκε το 1999 ως RFC 2660. Το Secure Hypertext Transfer Protocol (S-HTTP) είναι μια εναλλακτική λύση για τα URI HTTPS για την κρυπτογράφηση των web επικοινωνιών που μεταφέρονται μέσω HTTP.

Προγράμματα περιήγησης στο Ιντερνετ τυπικά χρησιμοποιούν HTTP για την επικοινωνία με τους web servers, για αποστολή και λήψη πληροφοριών, χωρίς να τα κωδικοποιούν. Για ευαίσθητες συναλλαγές, όπως το ηλεκτρονικό εμπόριο ή σε online πρόσβαση σε χρηματοοικονομικούς λογαριασμούς, τα προγράμματα περιήγησης και οι διακομιστές θα πρέπει να κρυπτογραφούν τις πληροφορίες. Τα HTTPS και S-HTTP ορίστηκαν στα μέσα της δεκαετίας του 1990 για να ανταποκριθούν στην ανάγκη αυτή. Η Netscape και η Microsoft υποστήριξαν το HTTPS αντί για το S-HTTP, με αποτέλεσμα το HTTPS να γίνει ο στάνταρ μηχανισμός για την εξασφάλιση επικοινωνίας μέσω διαδικτύου.

Όσο αφορά τις διαφορές μεταξύ SHTTP και HTTPS το SHTTP κρυπτογραφεί μόνο τα στοιχεία της ιστοσελίδας και υποβάλει τα στοιχεία των πεδίων POST, αφήνοντας την έναρξη του πρωτοκόλλου αμετάβλητη. Εξαιτίας αυτού, το S-HTTP μπορεί να χρησιμοποιηθεί ταυτόχρονα με HTTP (unsecured) στην ίδια θύρα, όπως η μη κρυπτογραφημένη επικεφαλίδα θα καθορίσει κατά πόσον το υπόλοιπο της μετάδοσης είναι κρυπτογραφημένη.

Αντίθετα, το HTTP «τυλίγει» ολόκληρο την επικοινωνία μέσα στο SSL, οπότε η κρυπτογράφηση ξεκινά πριν οποιοδήποτε πρωτόκολλο ξεκινήσει να στέλνει δεδομένα. Αυτό δημιουργεί ένα «chicken and egg» θέμα που έχει να κάνει με τον προσδιορισμό του ονόματος DNS που προοριζόταν για την αίτηση, πράγμα που σημαίνει ότι οι εφαρμογές, χωρίς Server Name απαιτούν ξεχωριστή IP ανά όνομα DNS, και όλες οι εφαρμογές απαιτούν μια ξεχωριστή θύρα (συνήθως 443 έναντι https πρότυπο 80) για τη σαφή χρήση της

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

κρυπτογράφησης (αντιμετωπίζονται στα περισσότερα προγράμματα περιήγησης ως ένα χωριστό πρωτόκολλο URI, https://).

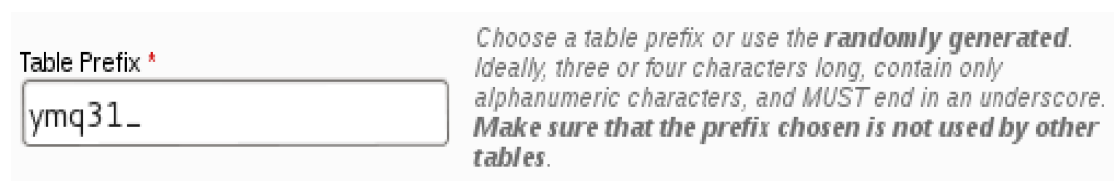
Στην S-HTTP, η επιθυμητή διεύθυνση URL δεν μεταδίδεται στις cleartext κεφαλίδες, αλλά μένει κενή, ένα άλλο σύνολο κεφαλίδων παρουσιάζεται μέσα στο κρυπτογραφημένο ωφέλιμο φορτίο. Σε HTTPS, όλες οι επιγραφές είναι μέσα στο κρυπτογραφημένο φορτίο, και η εφαρμογή του διακομιστή HTTPS δεν έχει γενικά την ευκαιρία να ανακάμψει χάρη των TLS μοιραίων λαθών.

Κεφάλαιο 7 – Προστασία του ηλεκτρονικού καταστήματος

7.1 – Προστασία από επιθέσεις SQL injection

Η βάση δεδομένων για μια ιστοσελίδα είναι πολύ σημαντικό συστατικό, αφού όλη η πληροφορία διαχειρίζεται και αποθηκεύεται σε αυτό. Οπότε είναι αναγκαίο να προστατέψουμε το σύστημα βάσης δεδομένων από κακόβουλους χρήστες.

Σε παλαιότερες εκδόσεις της πλατφόρμας Joomla, οι πίνακες ξεκινούσαν με ένα συγκεκριμένο πρόθεμα. Αυτό δυνητικά είναι μια αδυναμία, αφού υπάρχουν bots που ψάχνουν για πίνακες σε βάσης δεδομένων που έχουν αυτό το πρόθεμα, με σκοπό να δημιουργήσουν μια λίστα με ιστοσελίδες που βασίζονται στην πλατφόρμα Joomla. Ύστερα αφού ο επιτιθέμενος έχει αναγνωρίσει τους στόχους του ξεκινάει την διαδικασία της επίθεσης. Το πρόβλημα αυτό φαίνεται να έχει διορθωθεί στην έκδοση της πλατφόρμας Joomla που χρησιμοποιούμε, βάζοντας ένα πρόθεμα το οποίο πλέον δεν είναι σταθερό, αλλά δημιουργείτε ψευδοτυχαία κατά την διαδικασία εγκατάστασης.



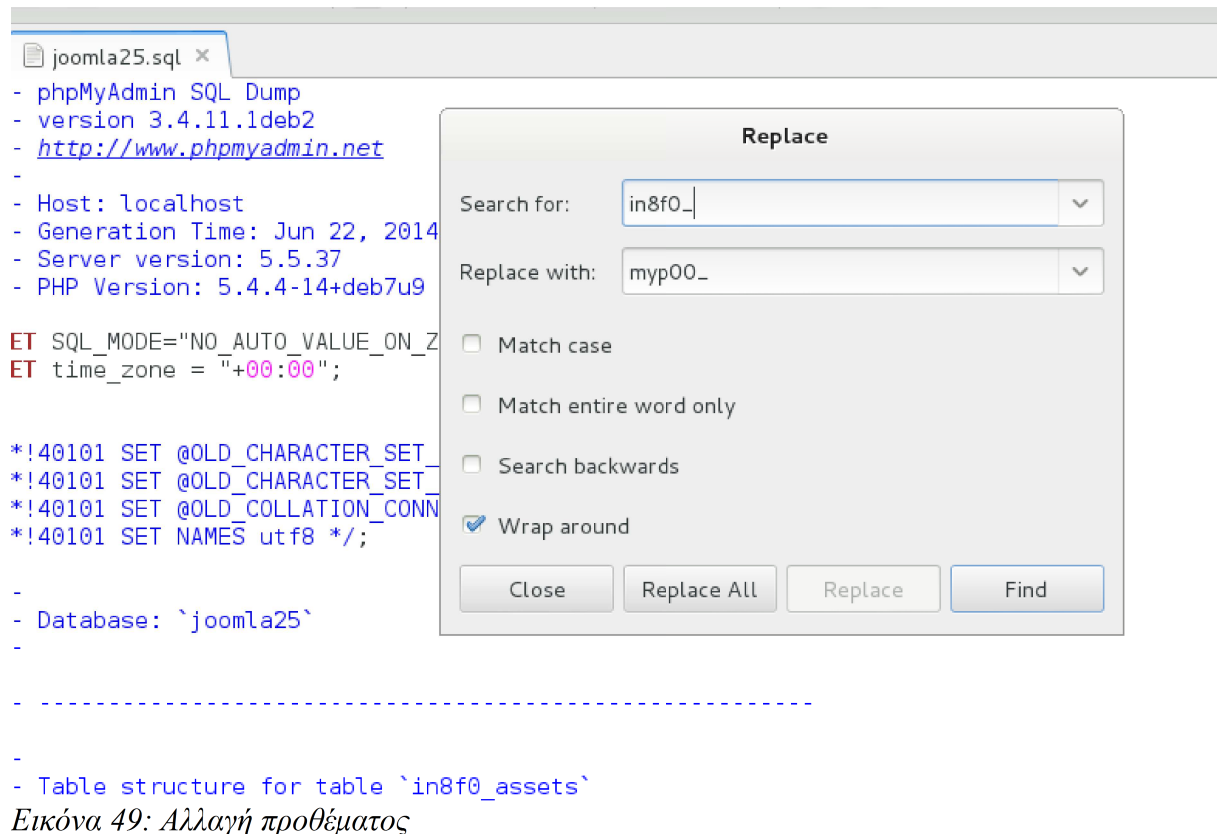
Εικόνα 48: Δημιουργία ψευδοτυχαίου προθέματος

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Για ακόμη όμως μεγαλύτερη ασφάλεια όσο αφορά το κομμάτι αυτό, θα ήταν συνετό να βάζουμε δικά μας προθέματα. Αυτό για να γίνει θα πρέπει να πάρουμε ένα αρχείο dump όλης της βάσης που χρησιμοποιεί η πλατφόρμα, ο πιο σύντομος και εύκολος τρόπος είναι να κάνουμε εξαγωγή της βάσης μέσα από την διεπαφή του phpMyAdmin. Μετά ανοίγουμε το αρχείο με έναν επεξεργαστή κειμένου και κάνουμε “εύρεση και αντικατάσταση” για να αλλάξουμε το παλιό πρόθεμα με το καινούριο.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



The image shows a SQL dump file named 'joomla25.sql' with the following content:

```
- phpMyAdmin SQL Dump
- version 3.4.11.1deb2
- http://www.phpmyadmin.net
-
- Host: localhost
- Generation Time: Jun 22, 2014
- Server version: 5.5.37
- PHP Version: 5.4.4-14+deb7u9

ET SQL_MODE="NO_AUTO_VALUE_ON_ZERO"
ET time_zone = "+00:00";

/*!40101 SET @OLD_CHARACTER_SET_CHARACTER_SET
/*!40101 SET @OLD_CHARACTER_SET_CHARACTER_SET
/*!40101 SET @OLD_COLLATION_CHARACTER_SET
/*!40101 SET NAMES utf8 */;

-
- Database: `joomla25`
-
-----
-
- Table structure for table `in8f0_assets`
```

Overlaid on the right is a 'Replace' dialog box with the following settings:

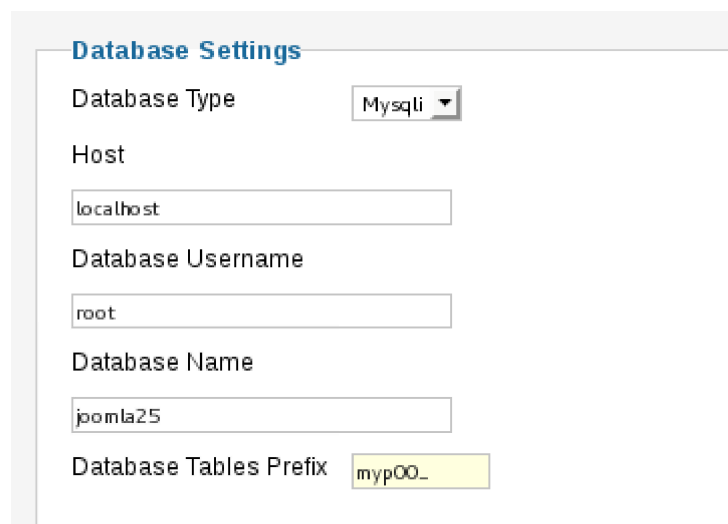
- Search for: in8f0_
- Replace with: myp00_
- Match case:
- Match entire word only:
- Search backwards:
- Wrap around:

Buttons at the bottom: Close, Replace All, Replace, Find.

- Table structure for table `in8f0_assets`

Εικόνα 49: Αλλαγή προθέματος

Ύστερα ελέγχουμε αν το πρόθεμα που χρησιμοποιεί η πλατφόρμα είναι ίδιο με το καινούριο. Ο έλεγχος αυτός μπορεί να γίνει ακολουθώντας το μενού Site → Global Configuration.



The image shows the 'Database Settings' configuration page in Joomla! with the following values:

- Database Type: Mysql
- Host: localhost
- Database Username: root
- Database Name: joomla25
- Database Tables Prefix: myp00_

Εικόνα 50: Ενημέρωση της πλατφόρμας για το καινούριο πρόθεμα

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Βέβαια η διαδικασία αλλαγής του προθέματος των πινάκων μπορεί να γίνει αυτόματα και ανώδυνα εγκαθιστώντας κάποια επέκταση.

Όσο αφορά την ίδια την επίθεση SQL injection υπάρχουν κάποιες καλές συμπεριφορές που πρέπει να ακολουθηθούν:

- 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 ιστοτόπου 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 μεγαλύτερες 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.
- 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) $int;`
- Η αλληλουχία από strings είναι το πρωταρχικό σημείο εισόδου για script injection. Αν κατά την είσοδο του χρήστη λάβουμε κάποιου είδους μεταβλητής (string) κάλο θα ήταν να αποφύγουμε τη χρήση της
`$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);`

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

Επίσης μπορούμε να προσθέσουμε ένα συστατικό (component) στην πλατφόρμα το οποίο αυτοματοποιεί την διαδικασία ασφάλειας. Τέτοια συστατικά μπορούν να βρεθούν και να αγοραστούν από τον παρακάτω εγκεκριμένο σύνδεσμο:

<http://extensions.joomla.org/extensions/access-a-security/site-security/site-protection>

7.2 – Προστασία από επιθέσεις DoS και DDoS

Ένας τρόπος προστασίας του συστήματος από τέτοιες επιθέσεις είναι να περιορίσουμε τον αριθμό των αιτημάτων που γίνονται μέσα σε ένα χρονικό διάστημα. Ένα παράδειγμα υλοποίησης γίνεται στο παρακάτω κώδικα:

```
<?php
    // class.floodblocker.php - FloodBlocker class, ver.0.01
    (April 15, 2005)
    //
    // Description:
    //   Class allowing to protect the scripts from flooding
    and to prevent
    //   automatic download of the site from single IP.
    //
    // Author:
    //   Vagharshak Tozalakyan <hide@address.com>
    //   This module was written by author on its leisure
    time.
    //
    // Warning:
    //   This class is non commercial, non professional work.
    It should not have
    //   unexpected results. However, if any damage is caused
    by this class the
    //   author can not be responsible. The use of this class
    is at the risk of
    //   the user.
    //
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
// Requirements:
//   PHP >= 4.1.0
//
//
-----
-----

// Errors and warnings

define ( 'E_TMP_DIR',      'Incorrect temporary directory
specified.' );

define ( 'E_IP_ADDR',      'Incorrect IP address
specified.' );

define ( 'E_LOG_FILE',    'Log file access error! Check
permissions to write.' );

define ( 'E_CRON_FNAME',  'The name of cron file must
begin with dot.' );

define ( 'E_CRON_FILE',   'Cron file access error! Check
permissions to write.' );

define ( 'E_CRON_JOB',    'Unable to perform the cron
job.' );

// Class definition
class FloodBlocker
{
    // The directory where log files will be saved. Must
    have permissions to write.
    var $logs_path;

    // IP address of current connection. REMOTE_ADDR will
    be used by default.
    var $ip_addr;

    // An associative array of [$interval=>$limit] format,
    where $limit is the
    // number of possible requests during $interval seconds.
    var $rules;

    // The name of the cron file. Must begin with dot.
    Default filename is '.time'.
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
var $cron_file;
// Cron execution interval in seconds. 1800 secs (30
mins) by default.
var $cron_interval;
// After how many of seconds to consider a file as old?
By default the files
// will consider as old after 7200 secs (2 hours).
var $logs_timeout;
/*
Description:
Class constructor.
Prototype:
void FloodBlocker ( string logs_path, string ip =
'' )
Parameters:
logs_path - the directory where log files will be
saved
ip - the ip address of the current connection,
$_SERVER['REMOTE_ADDR'] will be used if ip=''
*/
function FloodBlocker ( $logs_path, $ip = '' )
{
if ( ! is_dir ( $logs_path ) )
trigger_error ( E_TMP_DIR, E_USER_ERROR );

$logs_path = str_replace ( '\\', '/', $logs_path );
if ( substr ( $logs_path, -1 ) != '/' )
$logs_path .= '/';

$this->logs_path = $logs_path;

if ( empty ( $ip ) )
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
        $ip = $_SERVER['REMOTE_ADDR'];
        $ip = ip2long ( $ip );
        if ( $ip == -1 || $ip === FALSE )
            trigger_error ( E_IP_ADDR, E_USER_ERROR );
        $this->ip_addr = $ip;
        $this->rules = array ( );
        $this->cron_file = '.time';
        $this->cron_interval = 1800; // 30 minutes
        $this->logs_timeout = 7200; // 2 hours
    }
/*
    Description:
        Used to check flooding. Generally this function
acts as private method
        and will be called internally by public methods.
However, it can be called
        directly when storing logs in db.
    Prototype:
        bool RawCheck ( array &info )
    Parameters:
        info - $interval=>$time, $interval=>$count array
    Return:
        FALSE if flood detected, otherwise - TRUE.
*/
function RawCheck ( &$info )
{
    $no_flood = TRUE;

    foreach ( $this->rules as $interval=>$limit )
    {
        if ( ! isset ( $info[$interval] ) )
        {
```


Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
        $info[$interval]['time'] = time ( );
        $info[$interval]['count'] = 0;
    }

    $info[$interval]['count'] += 1;
    if ( time ( ) - $info[$interval]['time'] >
$interval )
    {
        $info[$interval]['count'] = 1;
        $info[$interval]['time'] = time ( );
    }
    if ( $info[$interval]['count'] > $limit )
    {
        $info[$interval]['time'] = time ( );
        $no_flood = FALSE;
    }
    // The following two lines can be used for debugging
    // echo $info[$interval]['count'].' ';
    // echo $info[$interval]['time'].'<br>';
} // foreach
return $no_flood;
}
/*
    Description:
        Checks flooding. Must be called after setting up
all necessary properties.
    Prototype:
        bool CheckFlood ( )
    Return:
        FALSE if flood detected, otherwise - TRUE.
*/
function CheckFlood ( )
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
{
    $this->CheckCron ( );
    $path = $this->logs_path . $this->ip_addr;
    if ( ! ( $f = fopen ( $path, 'a+' ) ) )
        trigger_error ( E_LOG_FILE, E_USER_ERROR);
    flock ( $f, LOCK_EX );
    $info = fread ( $f, filesize ( $path ) + 10 );
    $info = unserialize( $info );
    $result = $this->RawCheck ( $info );
    ftruncate ( $f, 0 );
    fwrite ( $f, serialize( $info ) );
    fflush ( $f );
    flock($f, LOCK_UN);
    fclose($f);
    return $result;
}
/*
    Description:
        Checks the cron file and calls CronJob() to delete
old entries from logs
        directory if the time-out is reached.
    Prototype:
        void CheckCron ( )
*/
function CheckCron ( )
{
    if ( substr ( $this->cron_file, 0, 1 ) != '.' )
    {
        trigger_error ( E_CRON_FNAME, E_USER_WARNING );
        return;
    }
    $path = $this->logs_path . $this->cron_file;
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
if ( ! ( $f = fopen ( $path, 'a+' ) ) )
{
    trigger_error ( E_CRON_FILE, E_USER_WARNING );
    return;
}
flock ( $f, LOCK_EX );
$last_cron = fread ( $f, filesize ( $path ) + 10 );
$last_cron = abs ( intval ( $last_cron ) );
if ( time ( ) - $last_cron > $this->cron_interval )
{
    $this->CronJob ( );
    $last_cron = time ( );
}
ftruncate ( $f, 0 );
fwrite ( $f, $last_cron );
fflush ( $f );
flock ( $f, LOCK_UN );
fclose ( $f );
}
/*
```

Description:

Deletes all old files from logs directory, except the files starting with dot.

Prototype:

```
void CronJob ( )
*/
function CronJob ( )
{

    $path = $this->logs_path;
    if ( ! ( $dir_hdl = opendir ( $this->logs_path ) ) )
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
{
    trigger_error ( E_CRON_JOB, E_USER_WARNING );
    return;
}
while ( $fname = readdir ( $dir_hndl ) )
{
    if ( substr( $fname, 0, 1 ) == '.' )
        continue;
    clearstatcache ( );
    $ftm = filemtime ( $path . $fname );
    if ( time ( ) - $ftm > $this->logs_timeout )
        @unlink ( $path . $fname );
}
closedir ( $dir_hndl );
}
} // end of class definition
/*
    $flb = new FloodBlocker ( 'example/tmp-ips/' );
    $flb->rules = array ( 10=>5 );
    $res = $flb->CheckFlood ( );
    if ( $res )
        echo 'Succeed!';
    else
        die ( 'Too many requests! Please try later.' );
*/
?>
```

Παράδειγμα χρήσης του παραπάνω κώδικα:

```
<?php
    // Place flood protection code at the top of the script
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

you want to protect.

```
// You can write protection code into separate file and
include it in every
// page of your site.
// Sample protection code starts here...
// Include the class definition module.
require_once ( '../class.floodblocker.php' );
// In the following line write the full path to
temporary directory in which
// you want to store flood counters. It is good idea to
create such folder
// somewhere outside your documents directory, to make
it unaccessable from Web.
// Don't forget that the directory must have
permissions to write files in it.
// IMPORTANT!
// All files in this folder (except those that start
with dot, e.g.'.htaccess')
// will be deleted by FloodBlocker, so don't keep
anything there.
$flb = new FloodBlocker ( 'tmp-ips/' );
// Create as many rules as you want...
$flb->rules = array (
    10=>10,    // rule 1 - maximum 10 requests in 10 secs
    60=>30,    // rule 2 - maximum 30 requests in 60 secs
    300=>50,   // rule 3 - maximum 50 requests in 300 secs
    3600=>200  // rule 4 - maximum 200 requests in 3600
secs
);
// At last call CheckFlood(), it will return FALSE if
flood detected on any
// of specified rules.
if ( ! $flb->CheckFlood ( ) )
    die ( 'Too many requests! Please try later.' );
```

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

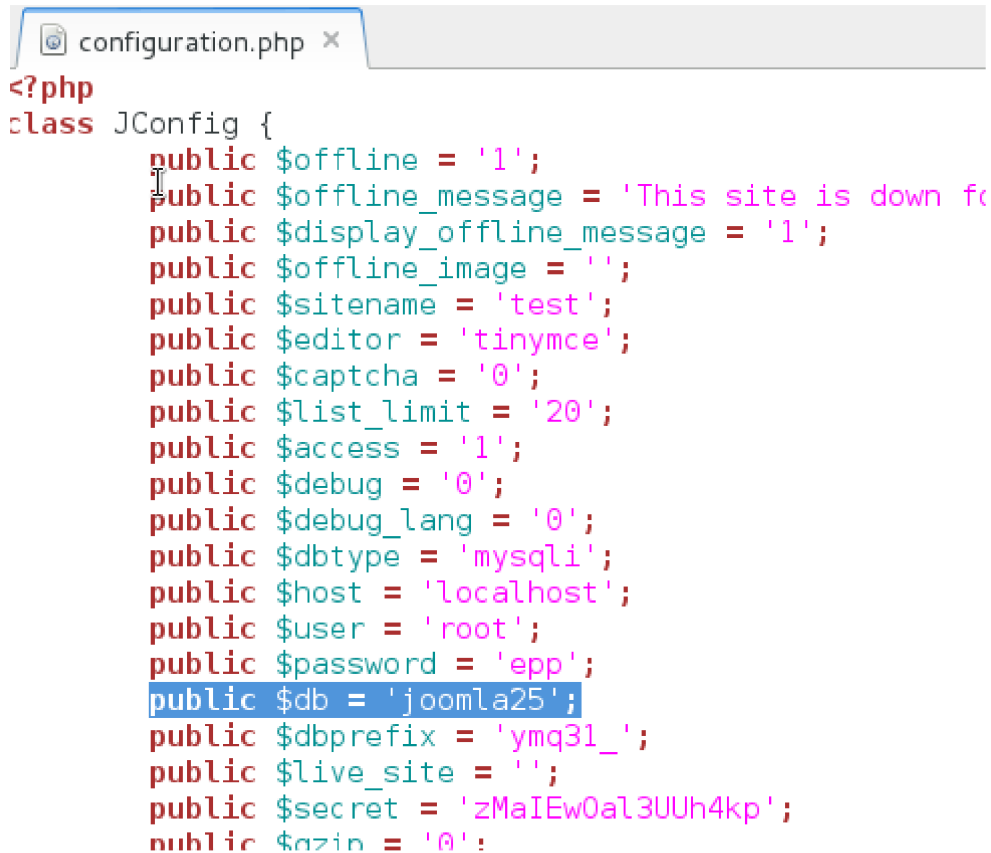
```
// ... that's all. Enjoy!  
?>
```

7.3 – Δημιουργία αντιγράφων ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας είναι χρήσιμη ακόμα και όταν δεν δεχτούμε κάποια επίθεση. Μερικούς από τους λόγους είναι καταστροφή του φυσικού επιπέδου ή προγραμματιστικά λάθη που μπορεί να οδηγήσουν σε δυσλειτουργία. Στο Joomla δεν περιέχεται κάποια αυτοματοποιημένη μέθοδος δημιουργίας αντίγραφου ασφαλείας. Ένας τρόπος για να κάνουμε ένα αντίγραφο είναι χειροκίνητα ακολουθώντας τα παρακάτω βήματα και υποθέτοντας πως ο εξυπηρετητής δεν βρίσκεται σε εμάς:

- Αποσυνδέουμε τον ιστότοπο, για να γίνει αυτό ακολουθούμε το μενού Site → Global Configuration και θέτουμε το πεδίο Site Offline ως Yes
- Αν δεν γνωρίζουμε το όνομα της βάσης που χρησιμοποιεί η πλατφόρμα θα χρειαστεί να κατεβάσουμε το αρχείο configuration.php το οποίο μπορεί να γίνει με FTP. Μέσα σε αυτό υπάρχει μια γραμμή της μορφής `var $db = 'x1234';` ή `public $db = 'x1234';` όπου το `x1234` υποδηλώνει το όνομα της βάσης.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



```
<?php
class JConfig {
    public $offline = '1';
    public $offline_message = 'This site is down fo
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'test';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'root';
    public $password = 'epp';
    public $db = 'joomla25';
    public $dbprefix = 'ymq31_';
    public $live_site = '';
    public $secret = 'zMaIEw0a13UUh4kp';
    public $gzip = '0';
```

Εικόνα 51: Μεταβλητή που περιέχει το όνομα της βάσης

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- Γνωρίζοντας το όνομα της βάσης μπορούμε να συνδεθούμε στο phpMyAdmin και να εξάγουμε την βάση σε ένα αρχείο.
- Τέλος μπορούμε να μεταφορτώσουμε τα αρχεία και τους φακέλους της σελίδας μας.

Ένας άλλος τρόπος για την δημιουργία αντιγράφου ασφάλειας είναι η εγκατάσταση κάποιας επέκτασης. Τέτοιες επεκτάσεις μπορούν να βρεθούν στον παρακάτω σύνδεσμο:

<http://extensions.joomla.org/extensions/access-a-security/site-security/backup>

7.4 – Δικαιώματα αρχείων και φακέλων

Η πλειοψηφία των εξυπηρετητών ως λειτουργικό σύστημα, τρέχουν κάποιο τύπο UNIX. Σε αυτήν την οικογένεια λειτουργικών συστημάτων υπάρχουν τρεις κατηγορίες δικαιωμάτων χρηστών πάνω σε αρχεία και φακέλους.

1. Διάβασμα
2. Εγγραφή
3. Εκτέλεση

Τα δικαιώματα αυτά ορίζονται για το κάθε αρχείο και φάκελο βάση τον τύπο του χρήστη, όπως φαίνεται παρακάτω:

1. Owner Permissions: Τα δικαιώματα που έχει ο ιδιοκτήτης.
2. Group Permissions: Τα δικαιώματα που έχουν οι χρήστες που βρίσκονται στην ίδια ομάδα χρηστών του λειτουργικού συστήματος με τον ιδιοκτήτη.
3. Other Permissions: Τα δικαιώματα που έχουν οι υπόλοιποι χρήστες του λειτουργικού συστήματος.

Η μορφή που έχει η περιγραφή των δικαιωμάτων μπορεί να φανεί στην παρακάτω εικόνα:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

```
bill@debian:~$ ls -la /var/www/
total 116
drwxrwxrwx 16 root    users    4096 Jun 22 22:57
drwxr-xr-x 13 root    root     4096 May 17 00:44 ..
drwxr-xr-x 10 bill    bill     4096 May 21 16:26 administrator
drwxr-xr-x  2 bill    bill     4096 May 21 16:26 cache
drwxr-xr-x  2 bill    bill     4096 May 21 16:26 cli
drwxr-xr-x 13 bill    bill     4096 May 21 16:26 components
-rw-r--r--  1 www-data www-data 1954 Jun 23 01:32 configuration.php
-rw-r--r--  1 bill    bill     3118 Apr 30 16:13 htaccess.txt
drwxr-xr-x  4 bill    bill     4096 May 21 16:26 images
drwxr-xr-x  2 bill    bill     4096 May 21 16:26 includes
-rw-r--r--  1 bill    bill     1319 Apr 30 16:13 index.php
-rw-r--r--  1 bill    bill     1751 Apr 30 16:14 joomla.xml
```

Εικόνα 52: Προβολή δικαιωμάτων

Βλέπουμε πως ο πρώτος χαρακτήρας μπορεί να είναι 'd' ή '-' όπου το d βγαίνει από την λέξη directory και δηλώνει φάκελο. Μετά υπάρχουν τρεις τριάδες χαρακτήρων. Η σειρά της κάθε τριάδας αντιστοιχεί στις ομάδες δικαιωμάτων που αναγράφονται πιο πάνω. Ο κάθε χαρακτήρας που περιέχεται δηλώνει τα δικαιώματα.

'r' → ανάγνωση

'w' → εγγραφή

'x' → εκτέλεση

'-' → δεν υπάρχει το δικαίωμα

Η τρίτη στήλη δηλώνει το όνομα χρήστη – ιδιοκτήτη και η τέταρτη την ομάδα χρηστών.

Ένας άλλος τρόπος απόδοσης δικαιωμάτων είναι αθροίζοντας τους αριθμούς που βρίσκονται παρακάτω:

'r' → 4

'w' → 2

'x' → 1

Με αυτό τον τρόπο τα δικαιώματα του αρχείου configuration.php που βλέπουμε στην παραπάνω εικόνα μπορούν να εκφραστούν και ως 644.

Μια καλή πρακτική για τον ορισμό δικαιωμάτων όσον αφορά το Joomla είναι να χρησιμοποιούμε 755 για τους φακέλους και 644 για τα αρχεία, το οποίο μπορεί να γίνει χρησιμοποιώντας την εντολή chmod.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

7.5 – Προτεινόμενες ρυθμίσεις για τα αρχεία htaccess και php.ini

Όσο αφορά το αρχείο htaccess μπορούμε να αλλάξουμε κάποιες ρυθμίσεις για να καταφέρουμε τα παρακάτω:

- Επιθέσεις τύπου έγχυσης και XSS
 - Πρόληψη χτυπήματος τύπου Global Variable Injection
`php_flag register_globals off`
 - Πρόληψη χτυπήματος τύπου XSS
`php_flag allow_url_fopen off`
 - Πρόληψη χτυπήματος Code injection
`php_flag magic_quotes_gpc on`
- Πρόσβαση καταλόγων από προεπιλεγμένη διεύθυνση IP
`<Limit GET>`
`Order Deny, Allow`
`Deny from all`
`Allow from #Insert IP here`
`</Limit>`

Όσο αφορά το αρχείο php.ini προτείνονται οι παρακάτω ρυθμίσεις:

- `engine = On`
Συγγουρεύουμε πως ο PHP πυρήνας θα τρέχει μέσα από τον apache.
- `safe_mode = On`
Απενεργοποιούνται οι συναρτήσεις που χρησιμοποιούν εντολές του συστήματος, διαβάζουν και γράφουν αρχεία μέσα απο το σύστημα αρχείων.
- `open_basedir = /var/www/`
Περιορίζουμε τις επιτρεπόμενες ενέργειες μόνο σε αυτή την διαδρομή.
- `expose_php = Off`
Απενεργοποιεί την δυνατότητα να φαίνεται αν έχουμε εγκατεστημένη την PHP.
- `max_execution_time = 30, max_input_time = 60, memory_limit = 60M`
Περιορίζουμε τον χρόνο εκτέλεσης του προγράμματος, τον χρόνο επεξεργασίας εισόδου και το μέγιστο χώρο στην μνήμη.

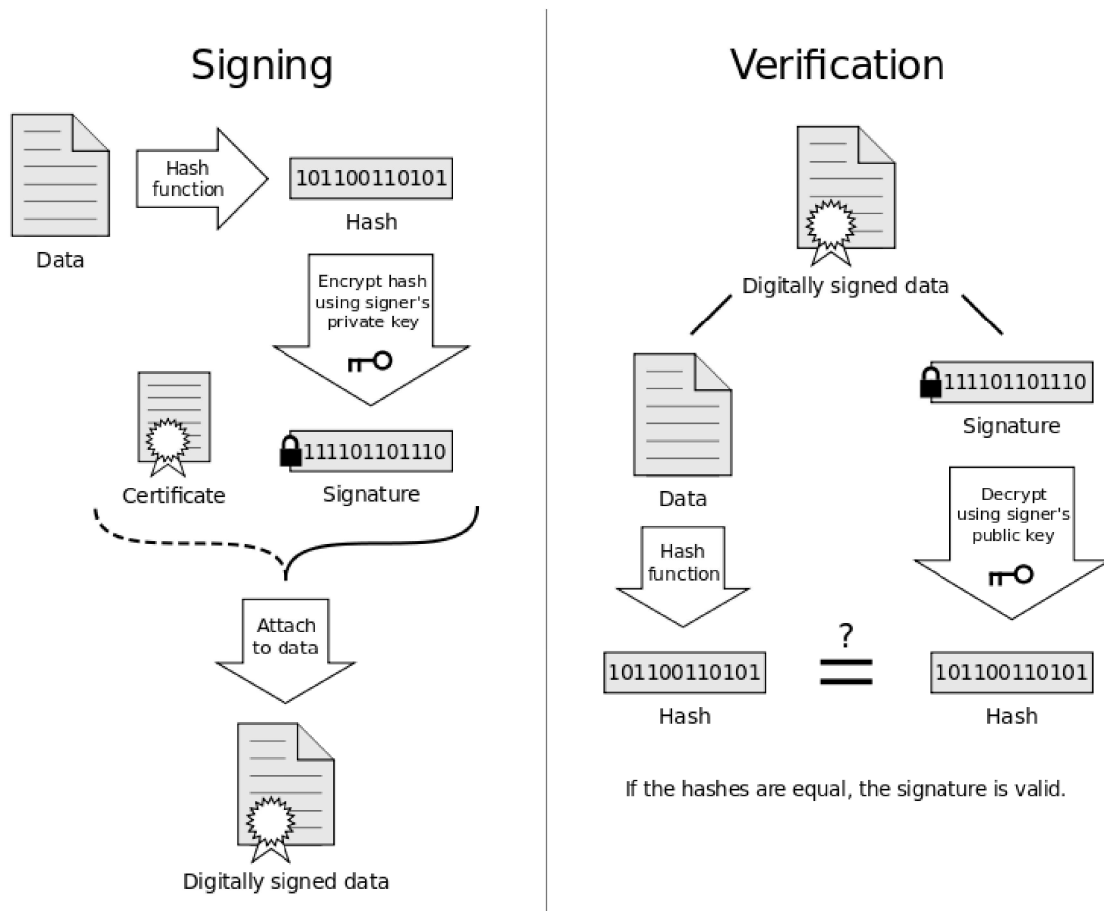
Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

- `display_errors = Off`
Απενεργοποιούμε την προβολή σφαλμάτων κατά την εκτέλεση.
- `log_errors = On`
Αφού απενεργοποιήσαμε αυτήν την χρήσιμη δυνατότητα για τον προγραμματιστή, ενεργοποιούμε την δυνατότητα καταγραφής σφαλμάτων σε ένα αρχείο.
- `error_log = /var/log/php.errorlog`
Το αρχείο στο οποίο θα καταγράφονται τα σφάλματα.
- `register_globals = off`
Αν χρησιμοποιούμε PHP έκδοσης μικρότερη της 4.2.0. Σε νεότερες εκδόσεις από προεπιλογή είναι απενεργοποιημένη και έχει διαγραφεί από την έκδοση 5.4.0 και μετά.
- `upload_tmp_dir = /tmp`
Ο φάκελος στον οποίο θα αποθηκεύονται τα προσωρινά αρχεία
- `upload_max_filesize = 30M`
Το μέγιστο μέγεθος που μπορεί να έχει ένα αρχείο που μεταφορτώνεται προς τον διακομιστή.

7.5 - Ψηφιακές Υπογραφές

Μια ψηφιακή υπογραφή, είναι ένας μαθηματικός σχεδιασμός για την πιστοποίηση γνησιότητας ενός ηλεκτρονικού μηνύματος ή εγγράφου. Μια ψηφιακή υπογραφή, δίνει στον παραλήπτη έναν λόγο για να πιστεύει πως αυτό που παρέλαβε δημιουργήθηκε από έναν γνωστό αποστολέα. Έτσι ο αποστολέας δεν μπορεί να αρνηθεί πως δεν ήταν αυτός που έστειλε τον μήνυμα (αυθεντικότητα και μη-αποκήρυξη) και πως το μήνυμα δεν άλλαξε κατά την μεταφορά (ακεραιότητα). Η παρακάτω εικόνα δείχνει το διάγραμμα ψηφιακού πιστοποιητικού.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!



Εικόνα 53: Διάγραμμα ψηφιακού πιστοποιητικού

Η μεθοδολογία των ψηφιακών υπογραφών αποτελείται από τρεις αλγόριθμους:

- Έναν αλγόριθμο δημιουργίας κλειδιών, που δημιουργεί ένα τυχαίο κλειδί μέσα από ένα σύνολο έγκυρων συνδυασμών. Η έξοδος του μετά είναι ένα ιδιωτικό και ένα δημόσιο κλειδί.
- Έναν αλγόριθμο υπογραφής, που χρησιμοποιώντας το μήνυμα και το ιδιωτικό κλειδί δημιουργεί την υπογραφή.
- Έναν αλγόριθμο επιβεβαίωσης υπογραφής που χρησιμοποιώντας το μήνυμα που λήφθηκε και το δημόσιο κλειδί, είτε αποδέχεται είτε απορρίπτει την αυθεντικότητα του μηνύματος.

Οι λόγοι για την ύπαρξη και εκμετάλλευση των ψηφιακών υπογραφών είναι:

- **Αυθεντικότητα:** Αν και τα μηνύματα πολλές φορές περιέχουν πληροφορίες σχετικά με το πρόσωπο που, η πληροφορία αυτή μπορεί να μην είναι ακριβής. Όταν ένας χρήστης είναι κάτοχος ενός κλειδιού υπογραφής, τότε δεν υπάρχει θέμα στο να πιστοποιήσει την αυθεντικότητά του.
- **Ακεραιότητα:** Σε πολλά σενάρια ο αποστολέας και ο παραλήπτης έχουν την ανάγκη το μήνυμα να παραμένει αυτούσιο χωρίς να αλλάξει. Αν και χρησιμοποιώντας κάποια μέθοδο κρυπτογράφησης, μπορούμε να αποκρύψουμε το μήνυμα, υπάρχει περίπτωση

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

να γίνει αλλαγή στο μήνυμα χωρίς να γίνει αντιληπτό.

- Μή αποκήρυξη: Με την ιδιότητα αυτή, η οντότητα που υπέγραψε το μήνυμα, δεν μπορεί σε μελλοντικό χρόνο να ισχυριστεί πως δεν δημιουργήθηκε από αυτήν.

7.6 - Ψηφιακό πιστοποιητικό

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

7.7 - Secure Sockets Layer

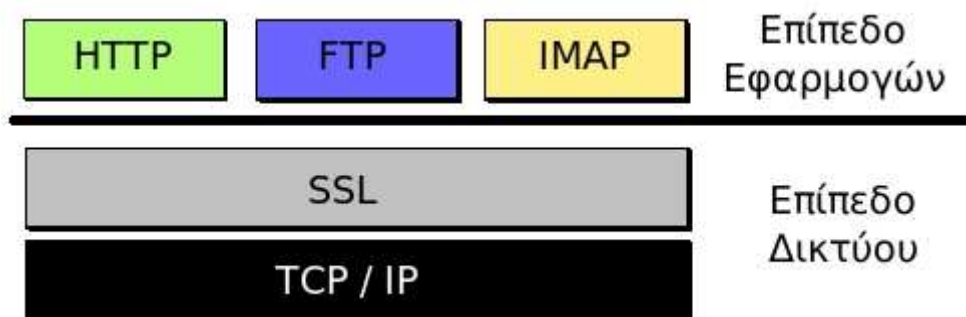
Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου 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

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

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 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 (email). 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: Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου.

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:

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

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.

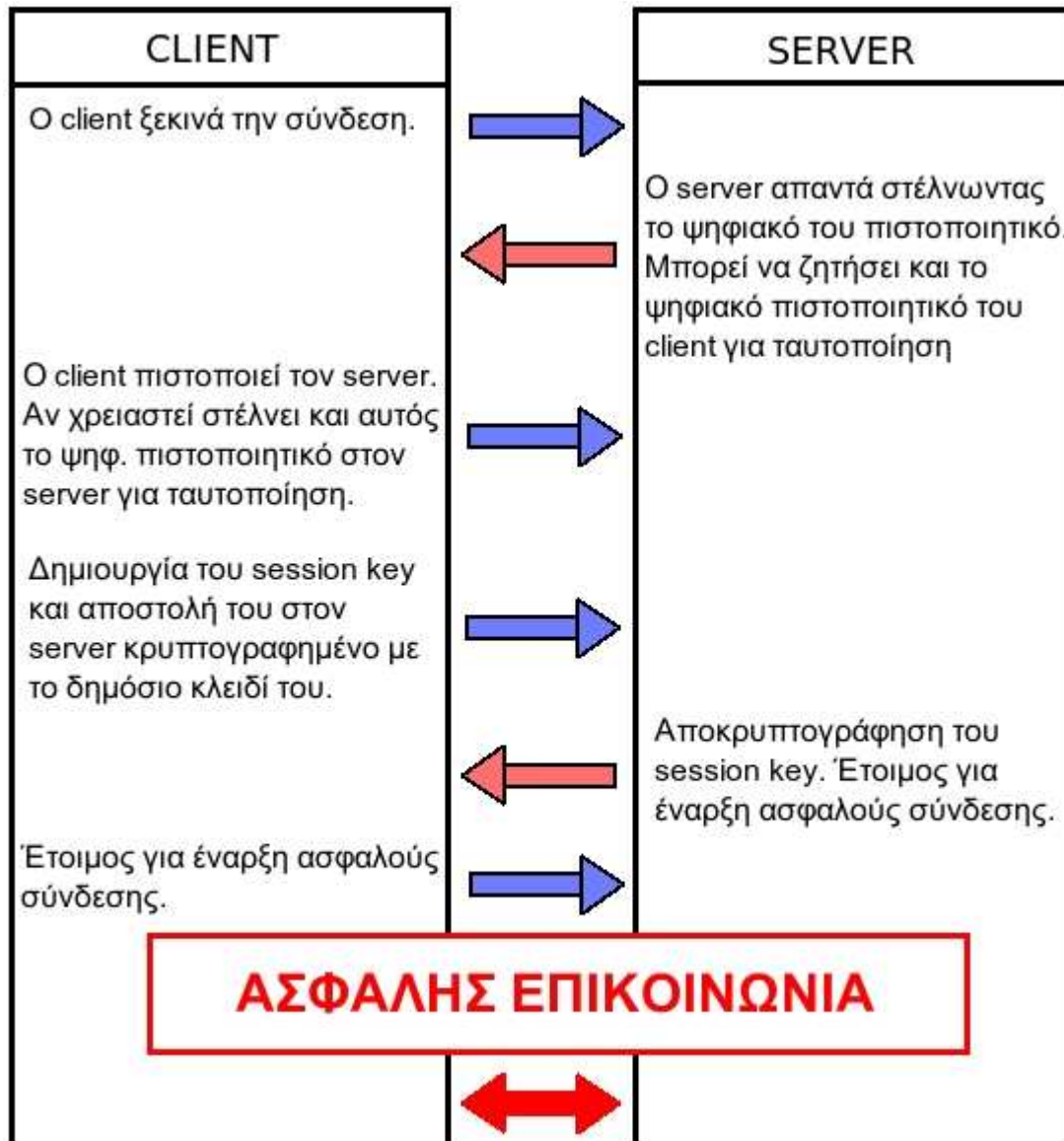
Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση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

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

7. Από εδώ και πέρα η χειραγία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

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



Εικόνα 55: Η διαδικασία της χειραγίας των δύο συσκευών σύμφωνα με το πρωτόκολλο SSL.

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

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

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

Πηγές

<http://blog.wikimedia.org/2014/05/07/launching-a-privacy-policy-built-the-wiki-way/>

[http://docs.joomla.org/Security Checklist 1 - Getting Started](http://docs.joomla.org/Security_Checklist_1_-_Getting_Started)

<http://docs.virtuemart.net/manual/21-configuration-menu/62-configuration.html#shop>

Δημιουργία ηλεκτρονικού καταστήματος σε Joomla!

<http://www.inmotionhosting.com/support/website/joomla-25/link-to-virtuemart-store-front>

<http://www.scribd.com/doc/99097140/%CE%A4%CE%BF-Web-banking-%CE%A4%CF%81%CE%B1%CF%80%CE%B5%CE%B6%CE%B9%CE%BA%CE%AD%CF%82-%CF%83%CF%85%CE%BD%CE%B1%CE%BB%CE%BB%CE%B1%CE%B3%CE%AD%CF%82-%CE%BC%CE%AD%CF%83%CF%89-Internet-%CE%A0%CF%81%CE%BF%CF%83%CF%86%CE%B5%CF%81%CF%8C%CE%BC%CE%B5%CE%BD%CE%B5%CF%82-%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%AF%CE%B5%CF%82-web-banking-%CF%84%CF%89%CE%BD-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA%CF%8E%CE%BD-%CF%84%CF%81%CE%B1%CF%80%CE%B5%CE%B6%CF%8E%CE%BD>

<http://www.acunetix.com/websitesecurity/xss/>

http://funwhichuwant.blogspot.gr/2012/10/webapplication-attack-hidden-field_12.html

<https://www.acunetix.com/what-are-csrf-attacks/>

<http://www.phpkode.com/scripts/item/flood-blocker/>

http://docs.joomla.org/Backup_Basics_for_a_Joomla!_Web_Site

<http://el.wikipedia.org/wiki/SSL>