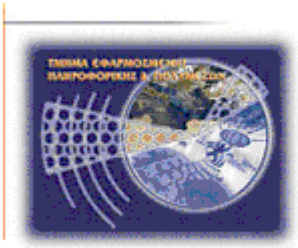
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Τίτλος: Κατασκευή ηλεκτρονικού καταστήματος

Ζαχαρούλα Καλοκύρη (ΑΜ: 808)

Ηράκλειο - Ημερομηνία

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Πίνακας περιεχομένων

1. Εισαγωγή

Τα ηλεκτρονικά καταστήματα έχουν μπει δυναμικά πλέον στο χώρο του εμπορίου και ολοένα και περισσότεροι είναι αυτοί που τα εμπιστεύονται για την διεκπεραίωση των αγορών τους. Η δημιουργία ενός τέτοιου καταστήματος απασχολεί τις παρακάτω ενότητες.

Το εργαλείο που χρησιμοποιείται για την δημιουργία του καταστήματος είναι το **osCommerce**. Το osCommerce είναι ένα open source λογισμικό μέσω του οποίου θα δημιουργήσουμε ένα ηλεκτρονικό κατάστημα, το οποίο θα προσφέρει μια μεγάλη πληθώρα δυνατοτήτων. Δυνατότητες που επιτρέπουν στους ιδιοκτήτες των ηλεκτρονικών καταστημάτων να τα διαχειρίζονται εύκολα, γρήγορα και χωρίς κόστος. Ξεκίνησε τον Μάρτιο του 2000 και από τότε έχει χρησιμοποιηθεί σε περίπου 6500 e-shops σε όλο τον κόσμο. Το osCommerce βασίζεται στην γλώσσα προγραμματισμού **PHP** και χρησιμοποιεί για βάση δεδομένων την **MySQL**. Με την κατάλληλη παραμετροποίηση δημιουργείται ένα εύχρηστο και καλαίσθητο γραφικό περιβάλλον, ενώ το τελικό αποτέλεσμα προσφέρει στον χρήστη τις παρακάτω δυνατότητες:

- Υποστήριξη απεριόριστων προϊόντων - κατηγοριών
- Δομή ‘προϊόντα – κατηγορίες’
- Δομή ‘προϊόντα – προϊόντα’
- Προσθήκη / επεξεργασία / διαγραφή προϊόντων, προμηθευτών, πελατών
- Υποστήριξη προϊόντων με παραγγελία, αλλά και προϊόντων που παραδίδονται άμεσα (download)
- Συνεργασία με τράπεζες για χρέωση πιστωτικών καρτών
- Ασφαλές control panel διαχειριστή με username και password τα οποία δηλώνονται κατά την εγκατάσταση
- Άμεση επικοινωνία με τους πελάτες μέσω email ή newsletter
- Εύκολο backup και restore της βάσης δεδομένων
- Δυνατότητα έκδοσης Παραστατικών
- Στατιστικά για τα προϊόντα και τους πελάτες
- Συναλλαγές σε διαφορετικά νομίσματα
- Μπορεί κάποιος να διαλέξει τον τρόπο εμφάνισης των προϊόντων
- Υποστήριξη για στατικά και δυναμικά banner με πλήρη στατιστικά
- Οι παραγγελίες αποθηκεύονται σε βάση δεδομένων για εύκολη πρόσβαση
- Οι πελάτες μπορούν να δουν το ιστορικό των παραγγελιών τους
- Βιβλίο διευθύνσεων πελατών
- Προσωρινή κάρτα αγορών για τους επισκέπτες και μόνιμη κάρτα αγορών για τους πελάτες
- Γρήγορη και φιλική προς τον χρήστη αναζήτηση
- Περιγραφές και σχόλια για τα προϊόντα
- Ασφαλείς συναλλαγές με SSL
- Ο αριθμός των προϊόντων για την κάθε κατηγορία μπορεί να είναι ορατός ή να μην φαίνεται.
- Λίστα με τα πρώτα σε πωλήσεις προϊόντα
- Εύκολη πλοήγηση στο site
- Αποστολή email σχετικών με την ανάλογη κατηγορία προϊόντων
- Πολλαπλοί τρόποι πληρωμής online ή offline
- Αυτόματος υπολογισμός του φόρου ανάλογα με το προϊόν

Τόσο για τον ιδιοκτήτη του καταστήματος όσο και για τον πελάτη, ο οποίος εμπιστεύεται τις «ευαίσθητες» πληροφορίες του, υποβόσκουν κάποιοι κίνδυνοι. Αυτοί οι κίνδυνοι αναλύονται στις παρακάτω ενότητες. Τέλος προτείνονται τρόποι για την διασφάλιση του ηλεκτρονικού καταστήματος**.**

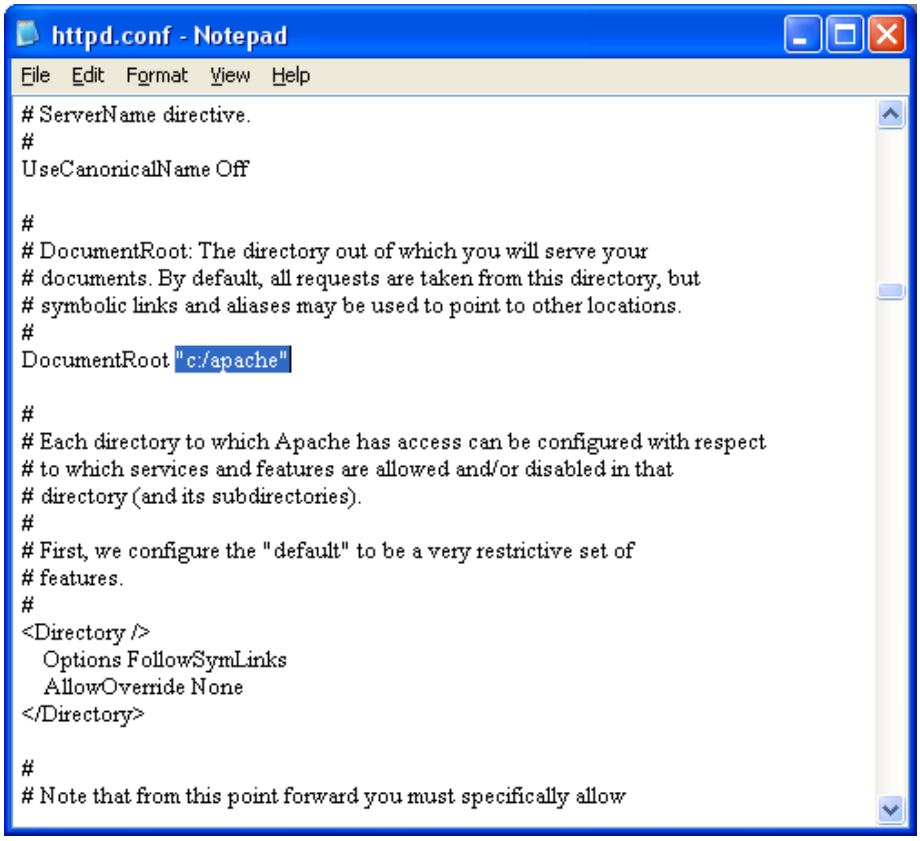
2. Τρόπος εγκατάστασης των απαραίτητων εργαλείων

Για την δημιουργία του ηλεκτρονικού καταστήματος απαιτούνται κάποια προγράμματα. Το πρώτο που χρειάζεται είναι ένας server πάνω στον οποίο θα στηθεί το κατάστημα. Ο server που χρησιμοποιείται σε αυτή την περίπτωση είναι ο Apache SSL. Ένας επιπλέον server, ο SMTP server, χρησιμοποιείται για την επικοινωνία μέσω e-mail μεταξύ του καταστήματος και των πελατών Για την δημιουργία της βάσης δεδομένων, στην οποία θα αποθηκεύονται όλες οι πληροφορίες που αφορούν το κατάστημα, γίνεται χρήση της MySQL, ενώ για την δημιουργία συνδέσεων και για την διαχείριση των πινάκων της MySQL, γίνεται εγκατάσταση του προγράμματος Navicat. Επίσης χρησιμοποιείται η PHP η οποία είναι η γλώσσα προγραμματισμού για την διαμόρφωση του site και τέλος το πρόγραμμα osCommerce αποτελεί μία φόρμουλα ενός ηλεκτρονικού καταστήματος. Με τις κατάλληλες τροποποιήσεις αυτή η φόρμουλα θα αποτελέσει το κατάστημα μας.

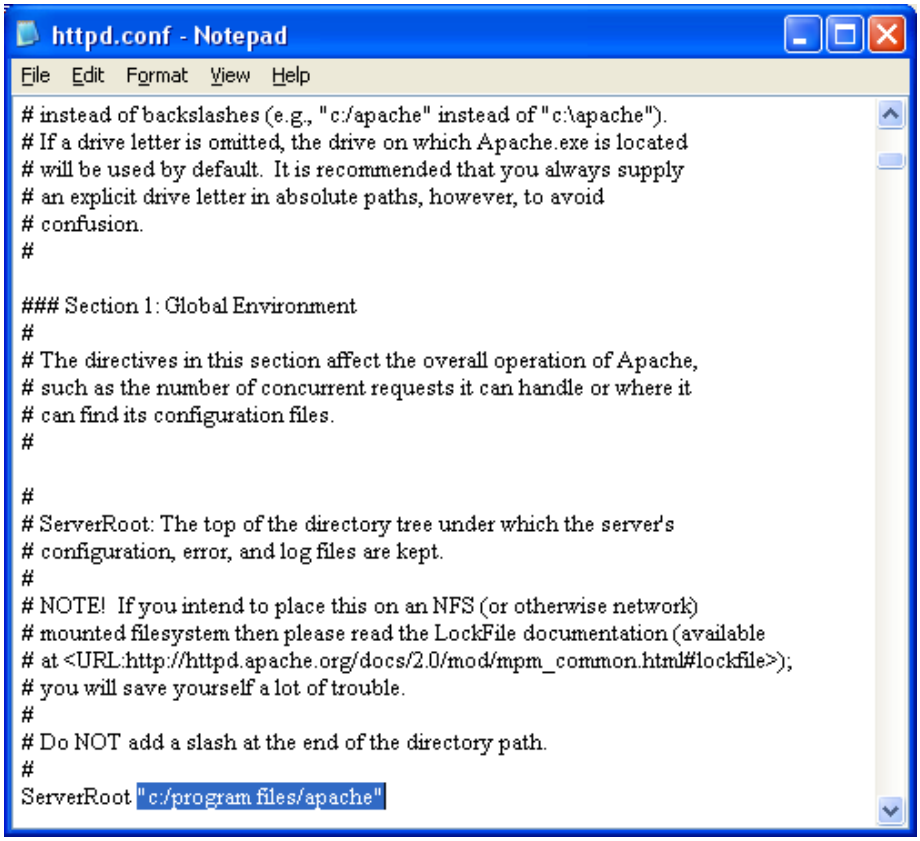
2.1 Εγκατάσταση Apache SSL

Αρχικά αποσυμπιέζουμε τα περιεχόμενα του Apache_2.0.59-Openssl_0.9.8d-Win32.zip στο root του Apache το οποίο στην περίπτωση αυτή είναι στο c:\program files\apache .Στον c:\ δημιουργούμε δύο φακέλους, τον πρώτο τον ονομάζουμε ssl.crt και τοποθετούμε σ’ αυτόν το πιστοποιητικό MyWebserver.crt. Τον δεύτερο τον ονομάζουμε ssl.key και περιέχει το κλειδί MyWebserver.key. Δημιουργούμε ένα αρχείο κειμένου και γράφουμε @echo dj_rigo82.Αυτό το αρχείο το αποθηκεύουμε στον c:\ με το όνομα passphrase.bat. Τόσο το πιστοποιητικό με το κλειδί όσο και η κωδική λέξη «dj_rigo82» μας έχουν δοθεί από κάποια αρχή πιστοποίησης.

Στον φάκελο conf του apache ανοίγουμε το αρχείο httpd.conf. Κάνουμε αναζήτηση για τον όρο documentroot και αλλάζουμε τον εξ ορισμού κατάλογο σε c:\apache.

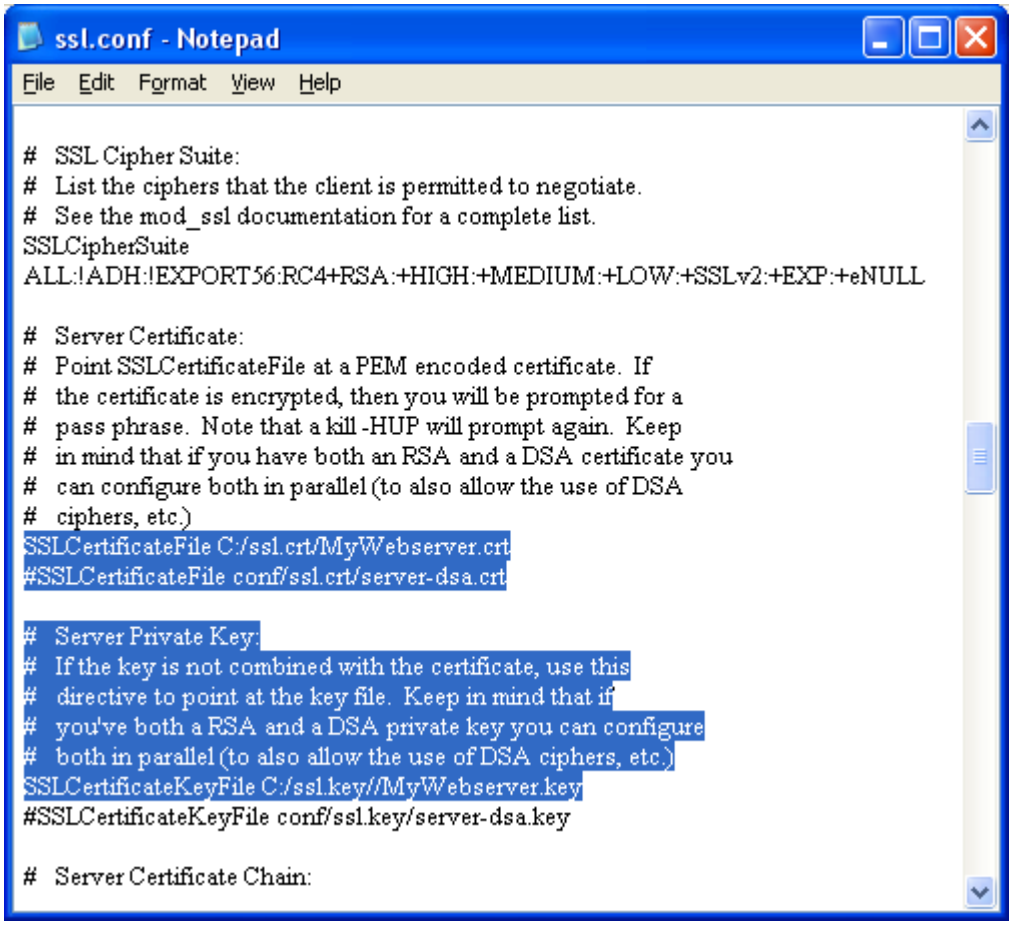


Πατάμε τον F3 για να βρει το επόμενο και κάνουμε το ίδιο. Στη συνέχεια αντικαθιστούμε σε όλο το αρχείο όπου C:\apache με C:\program files\apache.

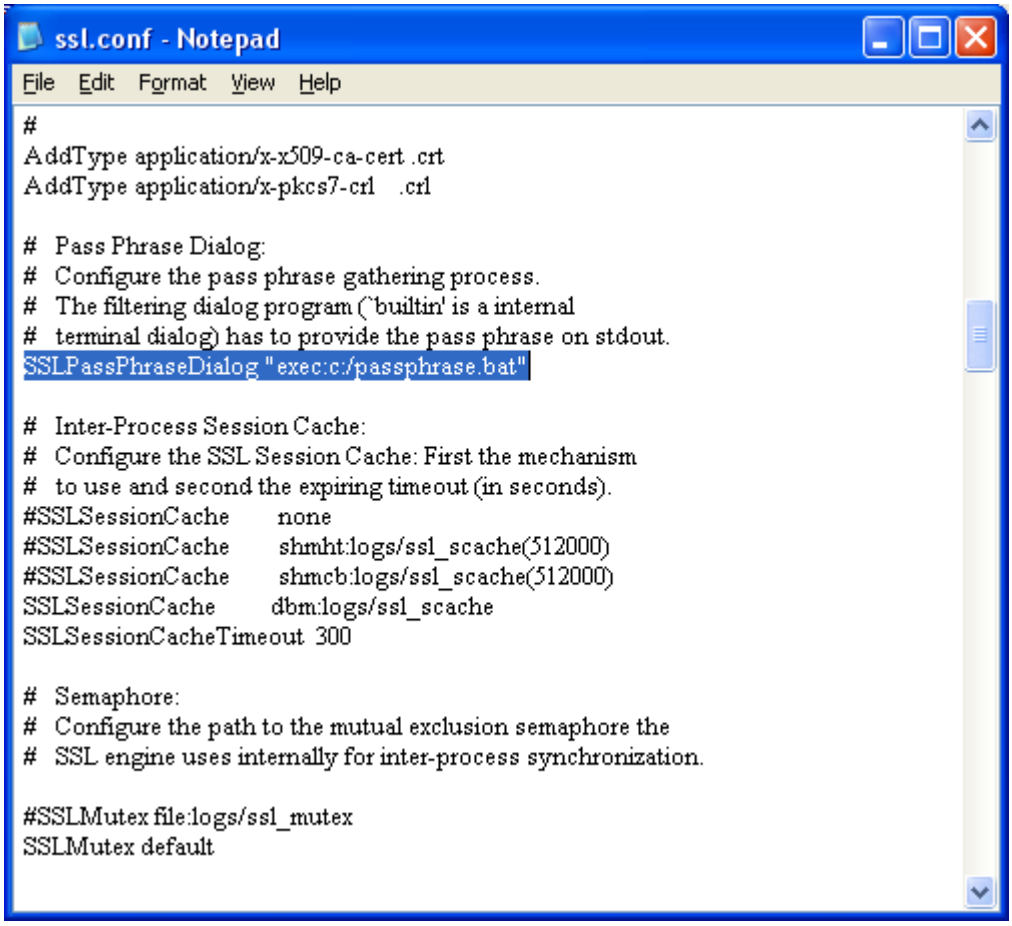


Τέλος αφαιρούμε το σχόλιο από την εντολή LoadModule ssl_module modules/mod_ssl.so και αποθηκεύουμε τις αλλαγές.

Ανοίγουμε το αρχείο ssl.conf το οποίο βρίσκεται και αυτό στον φάκελο conf και κάνουμε και σ' αυτό κάποιες αλλαγές. Όπως και στο httpd.conf έτσι και εδώ αντικαθιστούμε όπου c:\apache με c:\program files\apache και ορίζουμε στο documentroot τον c:\apache. Ακόμα δίνουμε στο SSLCertificateFile και στο SSLCertificateKeyFile τα path στα οποία βρίσκονται το πιστοποιητικό και το κλειδί αντίστοιχα.



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

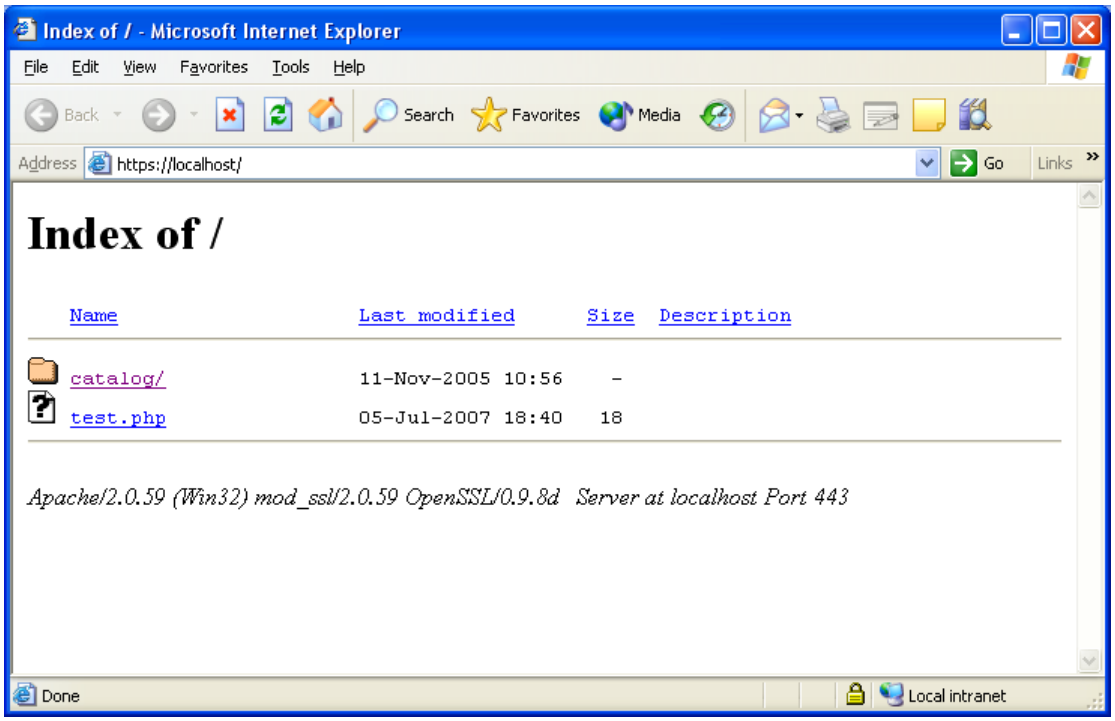


Για να ξεκινήσουμε τον apache ανοίγουμε ένα cmd και πληκτρολογούμε τις παρακάτω εντολές:

cd c:\program files\apache\bin
apache –D SSL

Έτσι αν προσθέσουμε κάποια αρχεία στο documentroot αυτά θα είναι προσβάσιμα και αν γράψουμε https://localhost/ στον browser μας θα εμφανιστεί η παρακάτω εικόνα η οποία μας ενημερώνει ότι η σελίδα είναι ασφαλής .

Επιλέγουμε Yes και έτσι εμφανίζονται τα αρχεία που είναι αποθηκευμένα στο documentroot.

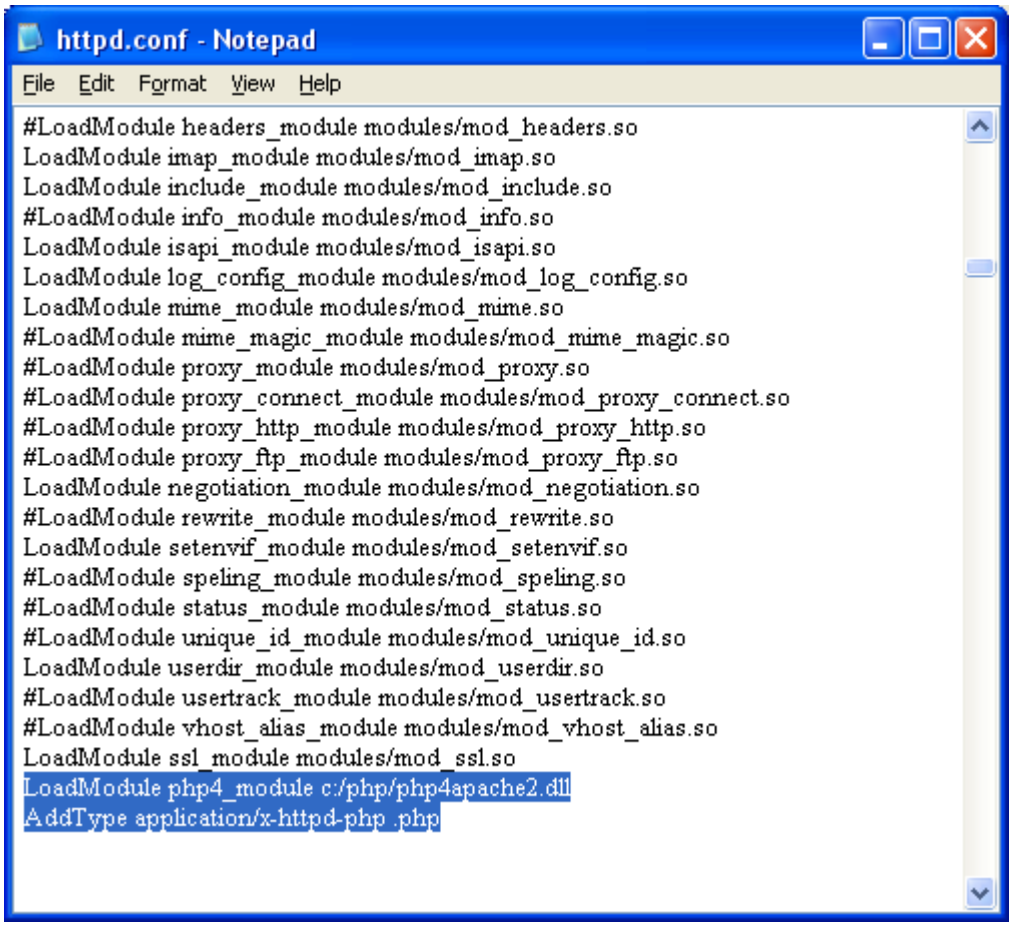


Η διαφορά σε σχέση με άλλες, μη ασφαλής σελίδες, όσον αφορά στην προβολή της σελίδας, είναι ότι εμφανίζεται ένα λουκέτο στο κάτω και δεξί μέρος ενώ στην διεύθυνση αντί του http χρησιμοποιείται το https. Με αυτόν τον τρόπο επιβεβαιωνόμαστε για την επιτυχή εγκατάσταση του Apache SSL.

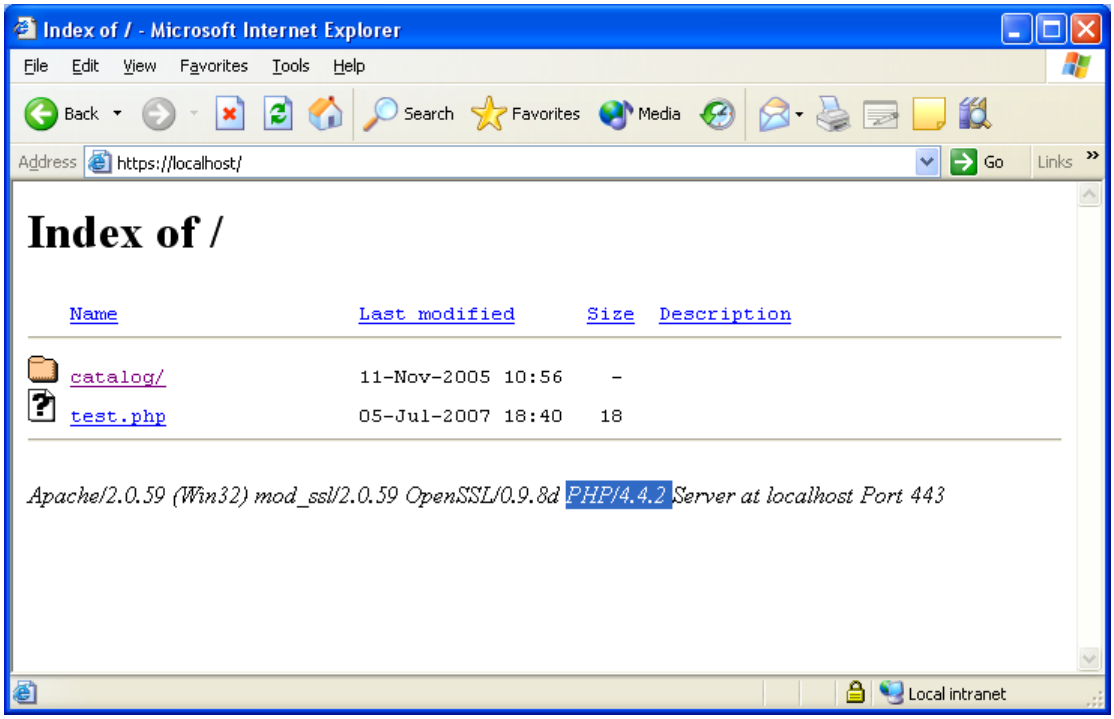
2.2 Εγκατάσταση PHP

Η έκδοση που χρησιμοποιείται είναι η PHP 4.4.2[php-4.4.2-Win32].Δημιουργούμε στον c:\ ένα φάκελο php μέσα στον οποίο αποσυμπιέζουμε τα περιεχόμενα του "php-4.4.2-Win32". Αφού γίνει αυτό μπαίνουμε στον κατάλογο c:\php και μετονομάζουμε το αρχείο php.ini-dist σε php.ini. Στη συνέχεια 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 apache.Κάνουμε αναζήτηση για τον όρο "loadmodule" και αφού βρει και τον τελευταίο τοποθετούμε τις εξής εντολές μετά από αυτόν:

LoadModule php4_module c:/php/php4apache2.dll
AddType application/x-httpd-php .php

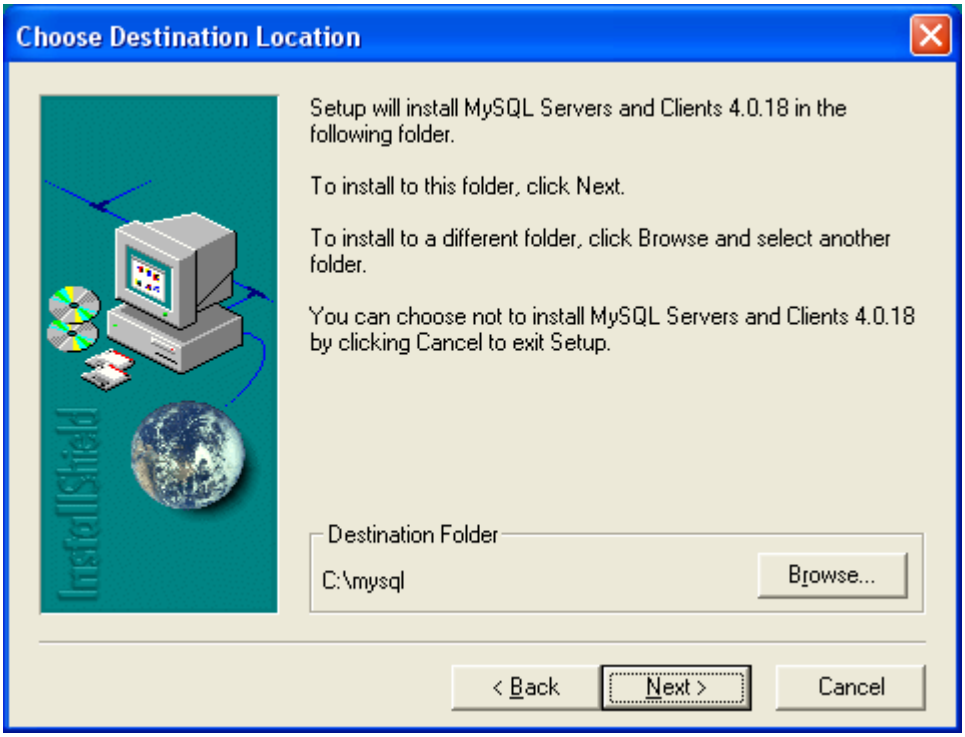


Κάνουμε επανεκκίνηση στον apache και αν γράψουμε τώρα https://localhost/ στον browser μας εμφανίζεται μια μικρή διαφορά, όπως παρατηρούμε στην παρακάτω εικόνα.



2.3 Εγκατάσταση MySQL

Η έκδοση που χρησιμοποιούμε για την βάση δεδομένων MySQL είναι η MySQL 4.0.18. Αποσυμπιέζουμε τα περιεχόμενα του "mysql-4.0.18-win" σε κάποιο κατάλογο και τρέχουμε το setup.Επιλέγουμε next στις δύο πρώτες εικόνες και στην τρίτη δίνουμε σαν φάκελο εγκατάστασης τον c:\mysql.



Επιλέγουμε typical στο επόμενο βήμα και στη συνέχεια next. Αφού τελειώσει το setup ανοίγουμε ένα DOS παράθυρο και πληκτρολογούμε τις εξής εντολές:

cd c:\mysql\bin
mysqld-nt –console

Λογικά βλέπουμε μηνύματα σαν αυτά παρακάτω

C:\mysql\bin>mysqld-nt --console
InnoDB: The first specified data file .\ibdata1 did not exist:
InnoDB: a new database to be created!
040807 10:54:09 InnoDB: Setting file .\ibdata1 size to 10 MB
InnoDB: Database physically writes the file full: wait...
040807 10:54:11 InnoDB: Log file .\ib_logfile0 did not exist: new to be created

InnoDB: Setting log file .\ib_logfile0 size to 5 MB
InnoDB: Database physically writes the file full: wait...
040807 10:54:12 InnoDB: Log file .\ib_logfile1 did not exist: new to be created
InnoDB: Setting log file .\ib_logfile1 size to 5 MB
InnoDB: Database physically writes the file full: wait...
InnoDB: Doublewrite buffer not found: creating new
InnoDB: Doublewrite buffer created
InnoDB: Creating foreign key constraint system tables
InnoDB: Foreign key constraint system tables created
040807 10:54:31 InnoDB: Started
mysqld-nt: ready for connections.
Version: '4.0.18-nt' socket: '' port: 3306[/b]

Ανοίγουμε ένα ακόμη παράθυρο DOS χωρίς όμως να κλείσουμε αυτό που έχουμε ήδη ανοίξει και πηγαίνουμε στον φάκελο c:\mysql\bin και γράφουμε : **mysql**.Τότε εμφανίζονται τα παρακάτω

C:\mysql\bin>mysql
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 1 to server version: 4.0.18-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

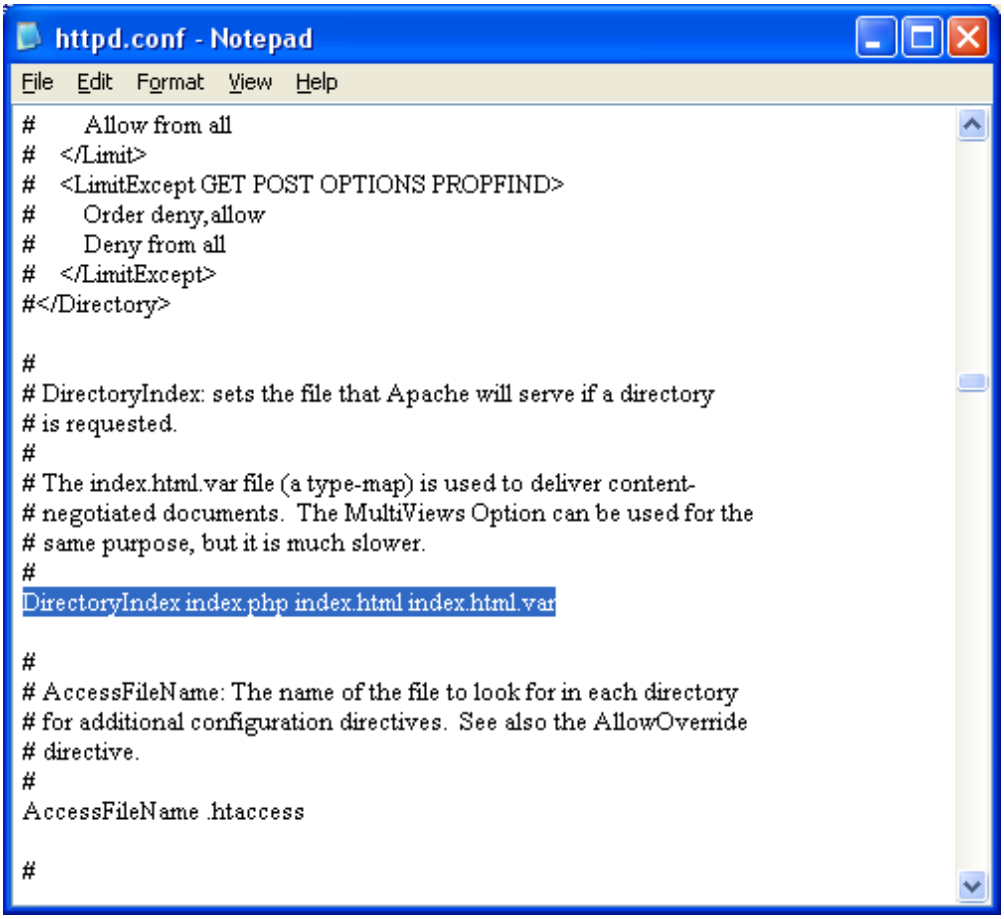
mysql>

Γράφουμε exit για να βγούμε από το monitor της mySQL.
Στη συνέχεια πηγαίνουμε πάλι στο c:\mysql\bin και πληκτρολογούμε τις παρακάτω εντολές:

mysqladmin -u root shutdown
mysqld-nt –install
net start mysql

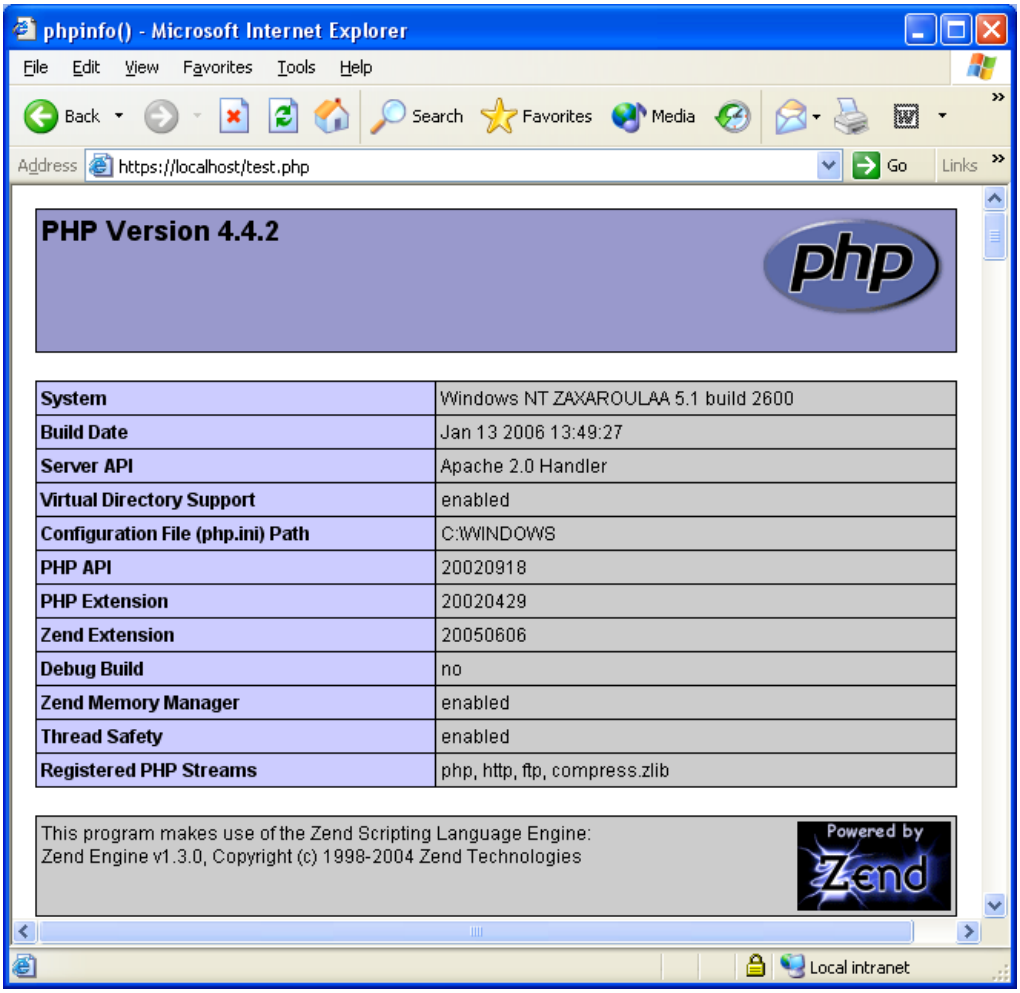
Σ ’αυτό το σημείο κλείνουμε και τα δύο dos παράθυρα και κάνουμε επανεκκίνηση στον υπολογιστή μας .Ανοίγουμε πάλι το httpd.conf και κάνουμε αναζήτηση για τον

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 .



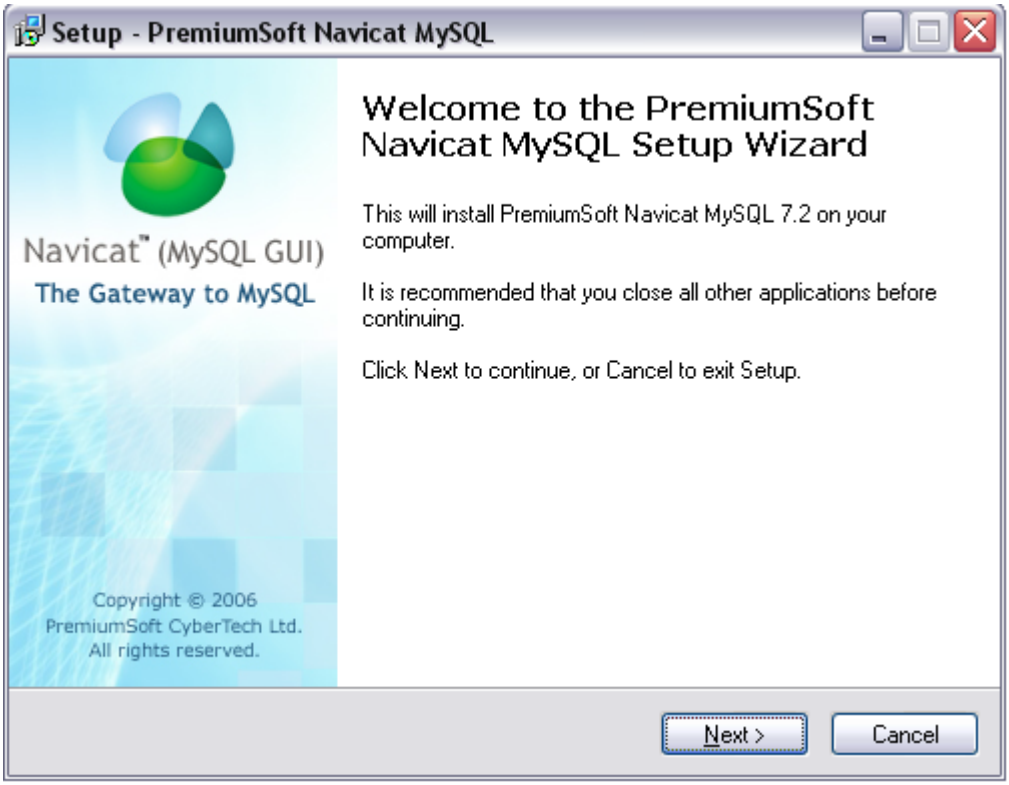
Στο c:\apache δημιουργούμε ένα αρχείο με όνομα test.php στο οποίο γράφουμε **<?php phpinfo();?>**

Ανοίγουμε τον browser μας και πληκτρολογούμε localhost.Τότε θα μας εμφανίσει το αρχείο test.php και αυτό που θα εμφανίσει όταν το επιλέξουμε φαίνεται στην παρακάτω εικόνα.

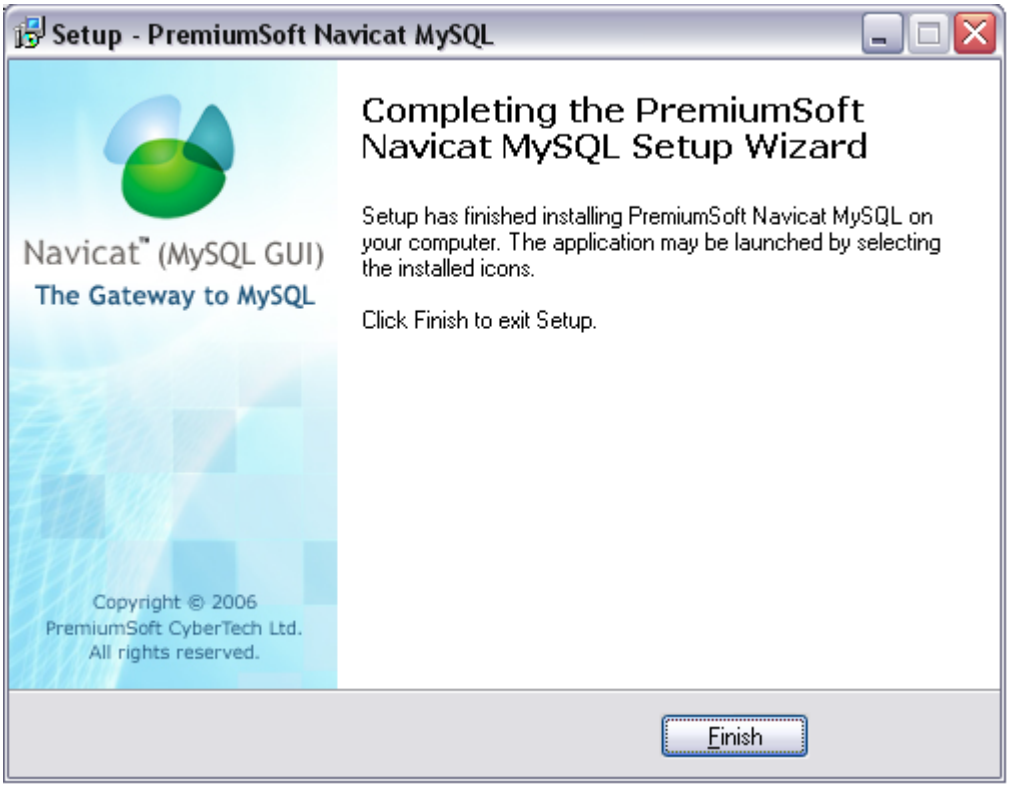

phpinfo() - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://localhost/test.php
Go Links
PHP Version 4.4.2
php
System Windows NT ZAXAROULAA 5.1 build 2600
Build Date Jan 13 2006 13:49:27
Server API Apache 2.0 Handler
Virtual Directory Support enabled
Configuration File (php.ini) Path C:\WINDOWS
PHP API 20020918
PHP Extension 20020429
Zend Extension 20050606
Debug Build no
Zend Memory Manager enabled
Thread Safety enabled
Registered PHP Streams php, http, ftp, compress.zlib
This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2004 Zend Technologies
Powered by Zend
Local intranet

2.4 Εγκατάσταση και δημιουργία βάσης δεδομένων με το Navicat MySQL

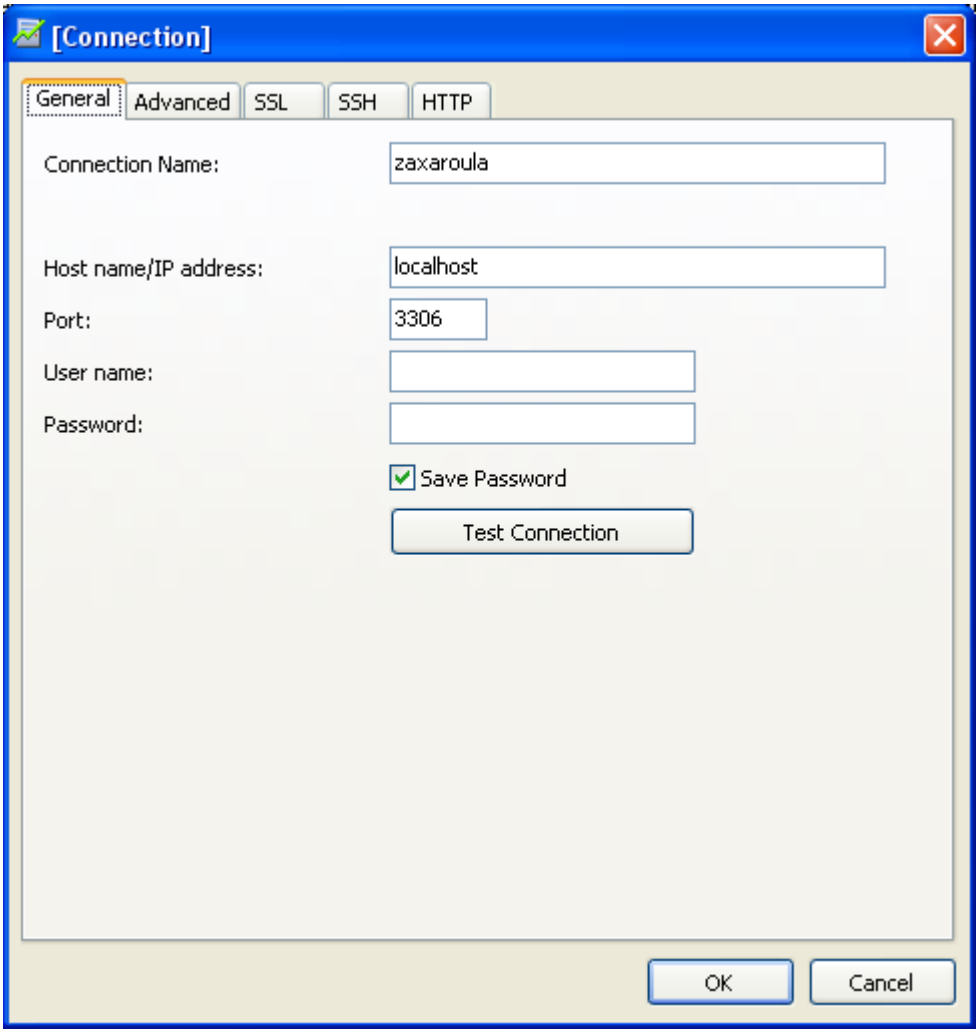
Για να εγκαταστήσουμε το Navicat τρέχουμε το αρχείο navicat.exe και εμφανίζεται η παρακάτω οθόνη



επιλέγουμε next σε όλες τις περιπτώσεις και έτσι ολοκληρώνεται η εγκατάσταση του.

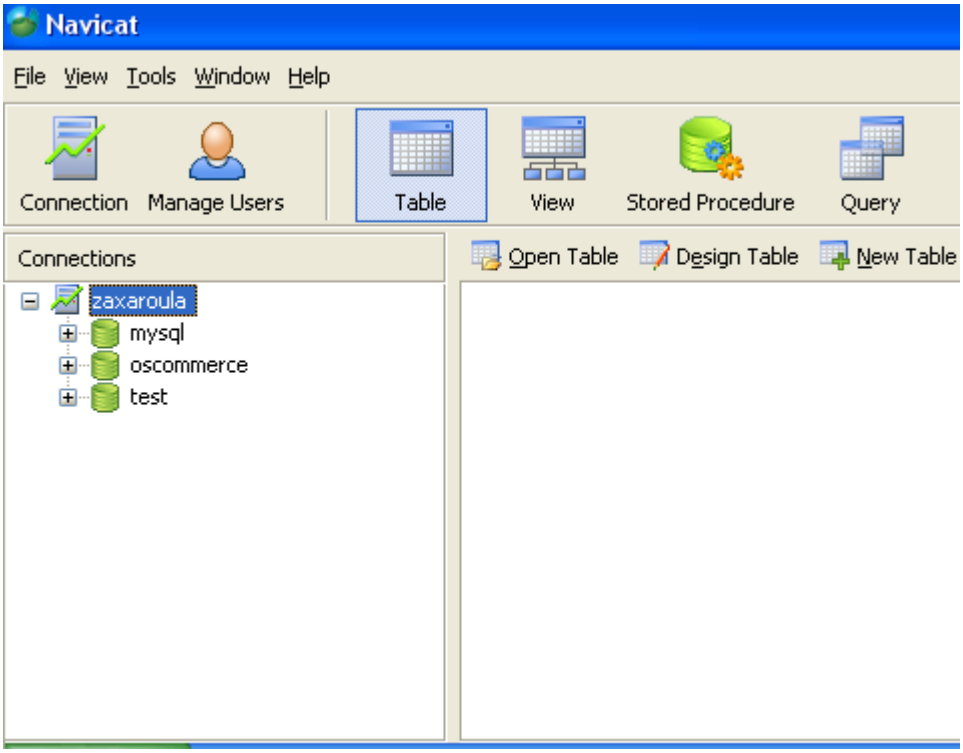


Το πρώτο πράγμα που πρέπει να γίνει για τη δημιουργία μιας βάσης είναι να φτιαχτεί μία σύνδεση. Ανοίγουμε το πρόγραμμα μας και επιλέγουμε Connection. Στο παράθυρο που εμφανίζεται δίνουμε ένα όνομα για την σύνδεση και επιλέγουμε Test Connection.



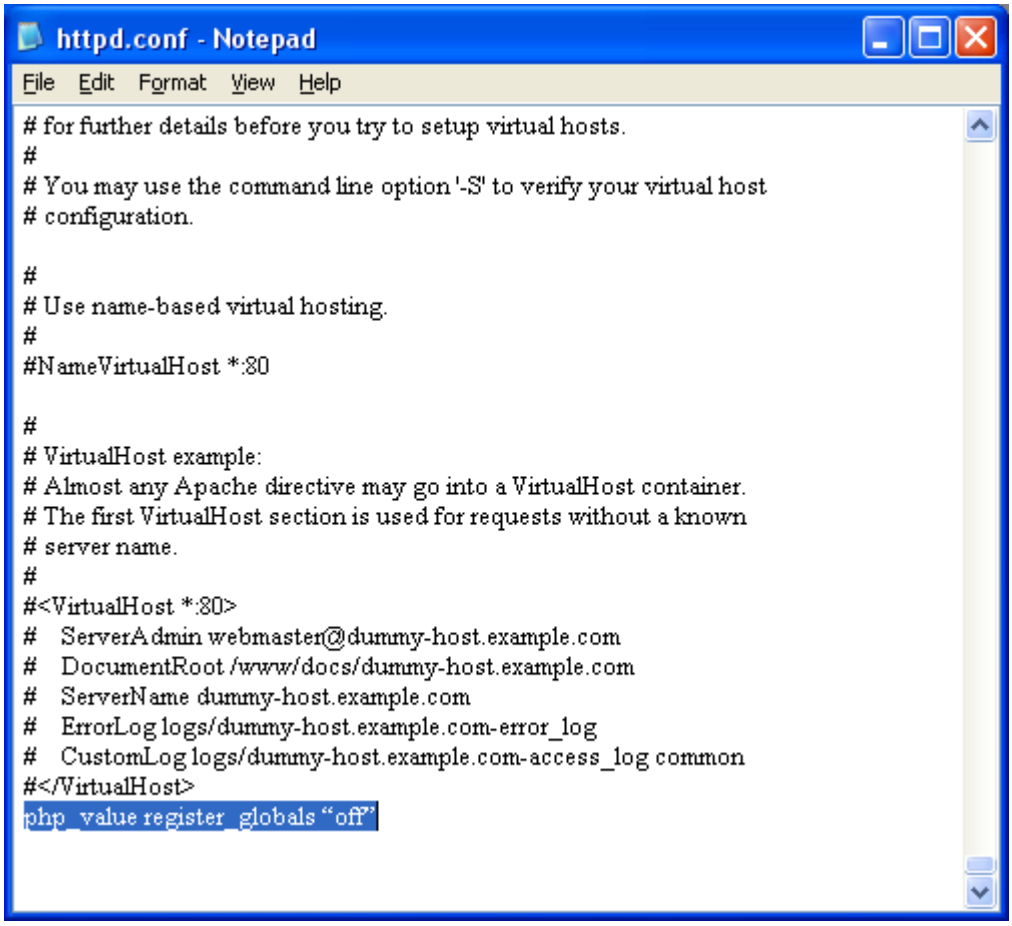
Αν μας εμφανίσει μήνυμα ότι ο έλεγχος της σύνδεσης είναι επιτυχής τότε επιλέγουμε OK και η σύνδεση μας έχει προστεθεί στη λίστα των συνδέσεων στο αριστερό μέρος της εφαρμογής.

Για την δημιουργία μίας βάσης κάνουμε δεξί κλικ στην σύνδεση και επιλέγουμε New Database. Δίνουμε το όνομα που επιθυμούμε να έχει η βάση, στην περίπτωση μας δίνουμε “oscommerce”, επιλέγουμε OK και έτσι δημιουργείται μία κενή, αρχικά βάση.

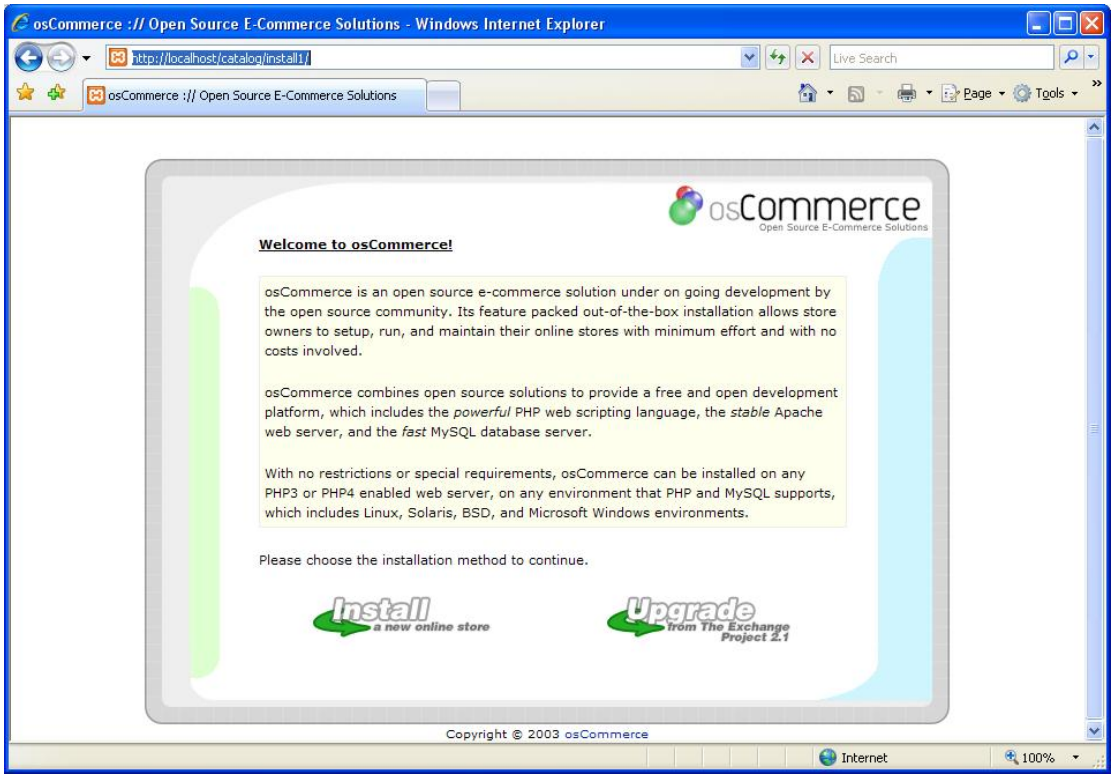


2.5 Εγκατάσταση του osCommerce

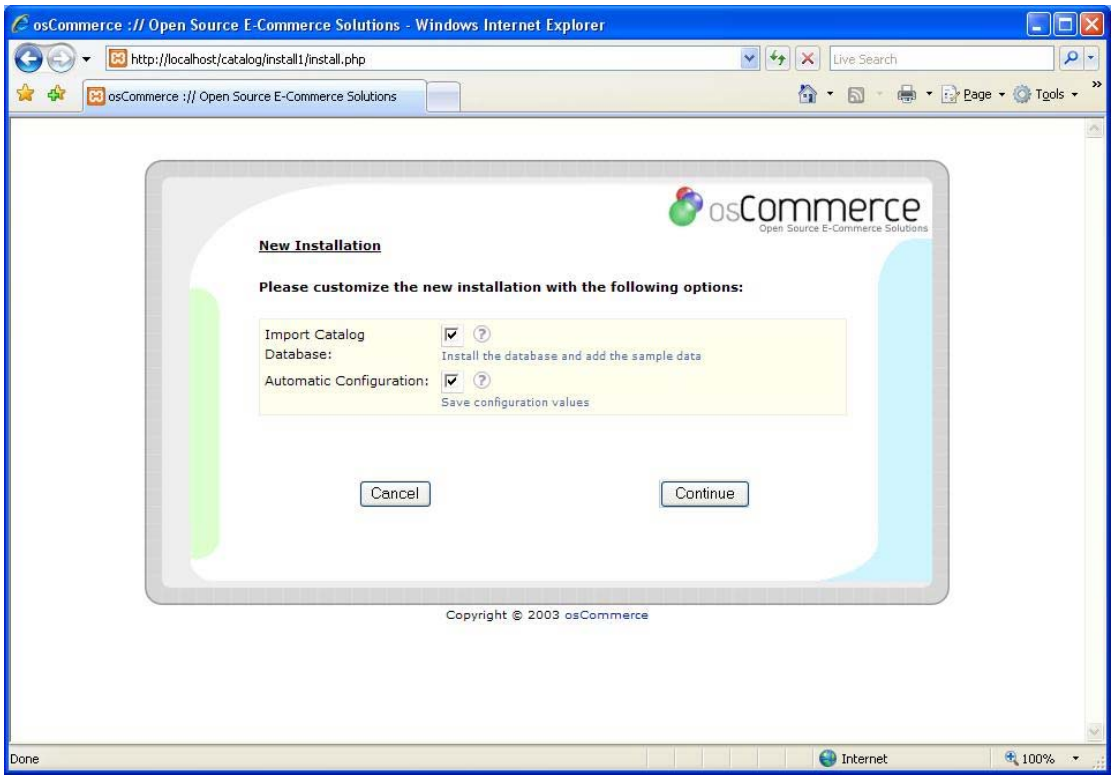
Αρχικά από τον φάκελο **oscommerce-2.2ms2-051113** αντιγράφουμε τον φάκελο catalog στο root του apache δηλαδή στο c:\server. Στη συνέχεια ανοίγουμε έναν browser και γράφουμε http://localhost/catalog/install/. Αν εμφανιστεί το εξής σφάλμα: *Fatal error :register_globals is disabled in php.ini ,please enable it!* ,τότε ανοίγουμε το httpd.conf του Apache και κάνουμε αναζήτηση της λέξης **VirtualHost**. Στην τελευταία λέξη που θα βρει προσθέτουμε πριν από αυτή το εξής : **php_value register_globals "off"** .



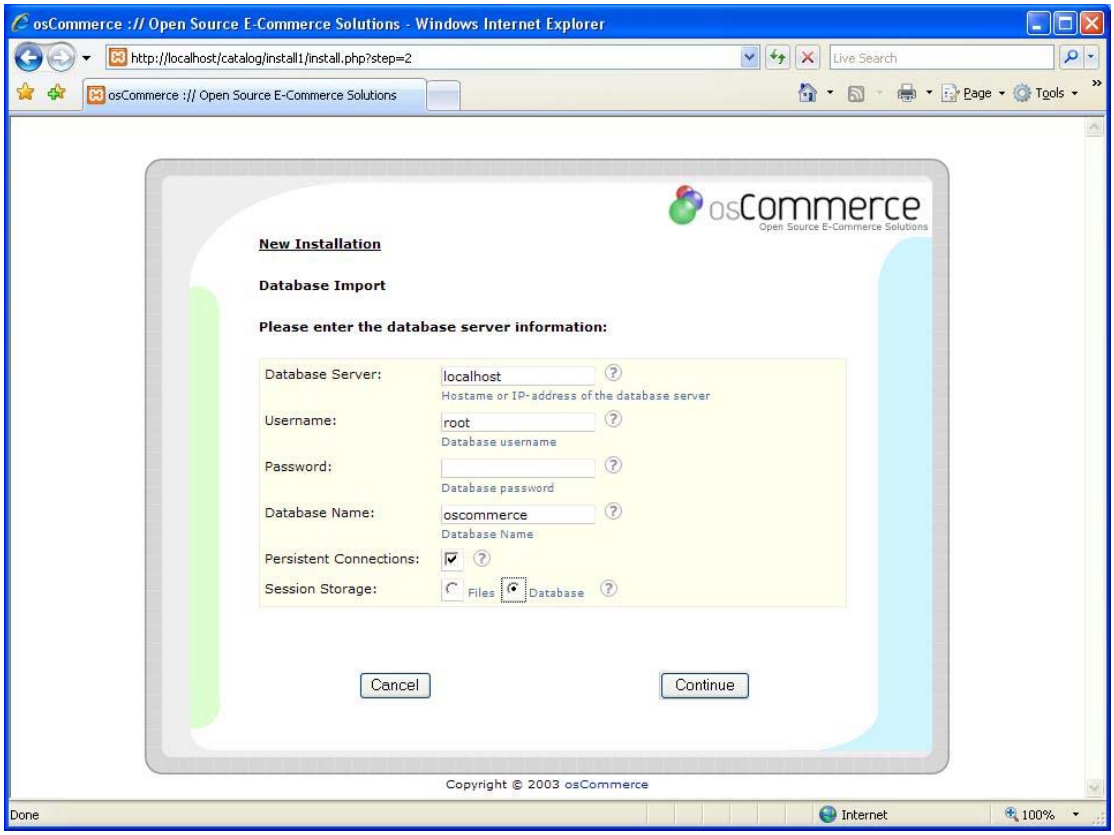
Κάνουμε restart στον Apache και ξαναπροσπαθούμε. Μόλις εμφανιστεί η παρακάτω σελίδα επιλέγουμε install.



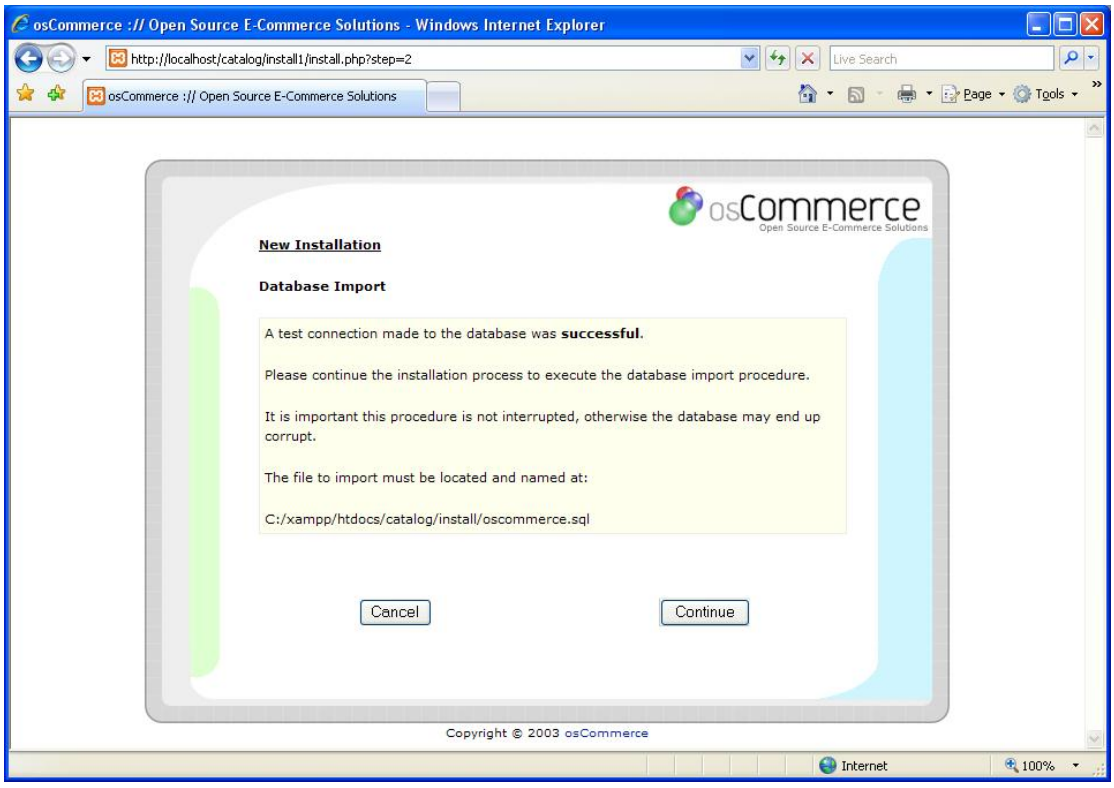
Στην επόμενη σελίδα τσεκάρουμε και τις δύο επιλογές και επιλέγουμε continue .



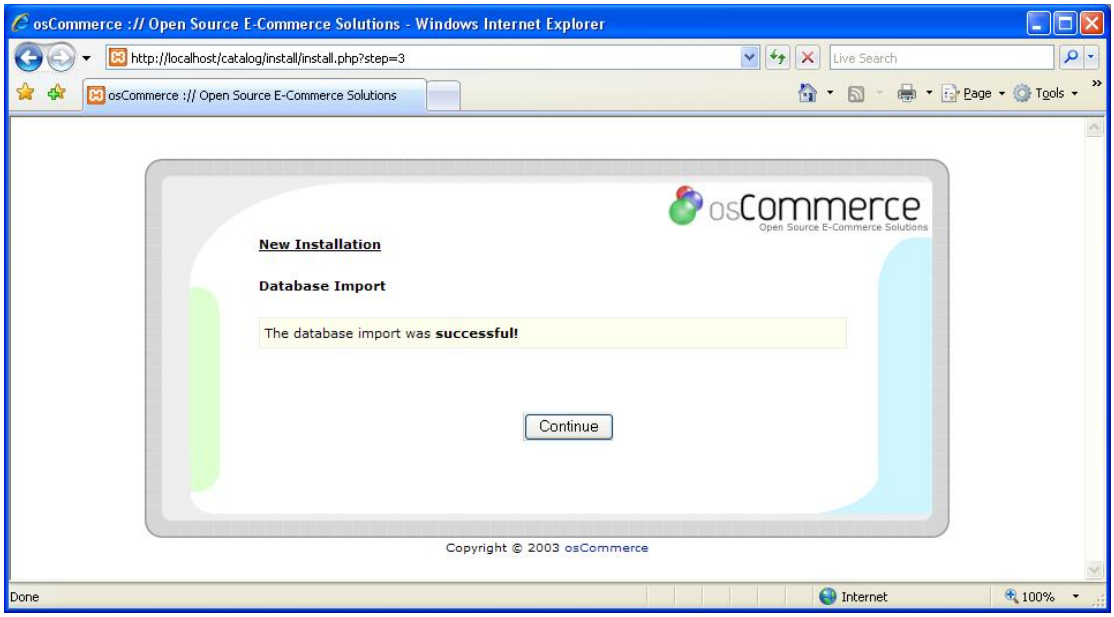
Στην επόμενη σελίδα συμπληρώνουμε το όνομα του server ,της βάσης και δίνουμε το username που επιθυμούμε .Τα στοιχεία που καταχωρήθηκαν στην συγκεκριμένη περίπτωση είναι όπως φαίνονται στην παρακάτω εικόνα. Συνεχίζουμε επιλέγοντας continue .



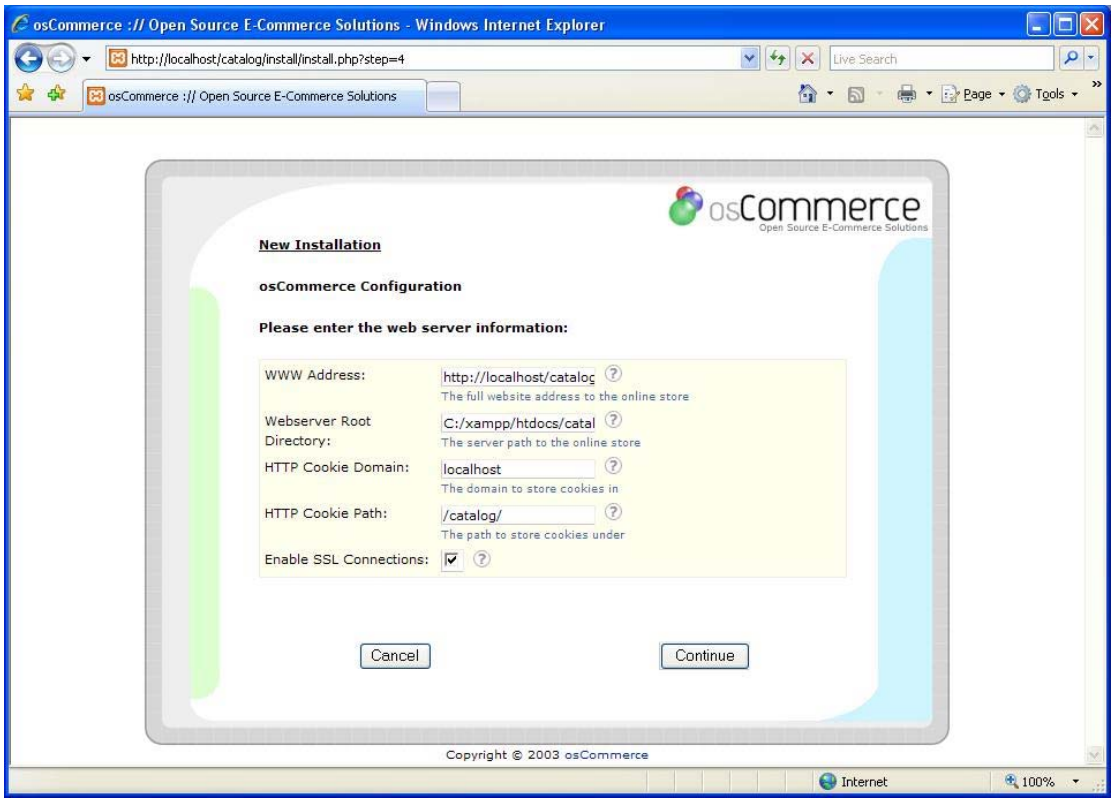
Στην παρακάτω σελίδα ελέγχουμε αν το αρχείο στο οποίο θα εισάγουμε την βάση είναι το **C:\server\catalog\install\oscommerce.sql** .Αν είναι σωστό (όπως συμβαίνει και στην εικόνα) συνεχίζουμε επιλέγοντας continue.



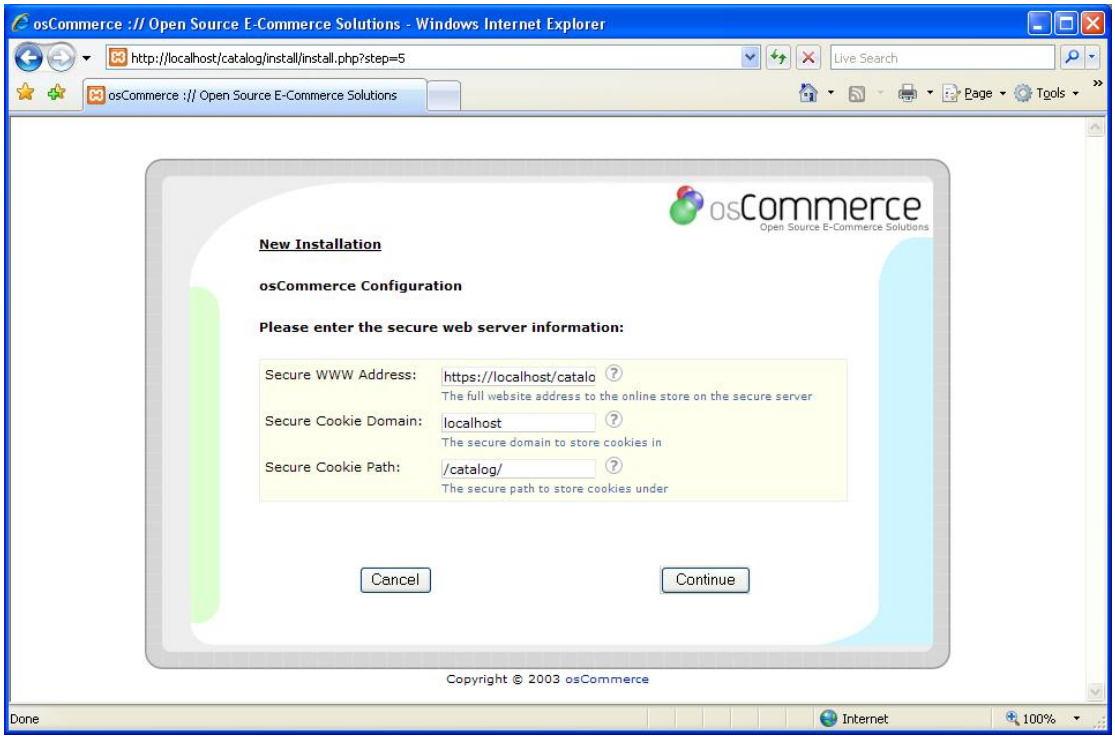
Η παρακάτω σελίδα μας ενημερώνει για την επιτυχή εισαγωγή της βάσης.
Επιλέγουμε continue.



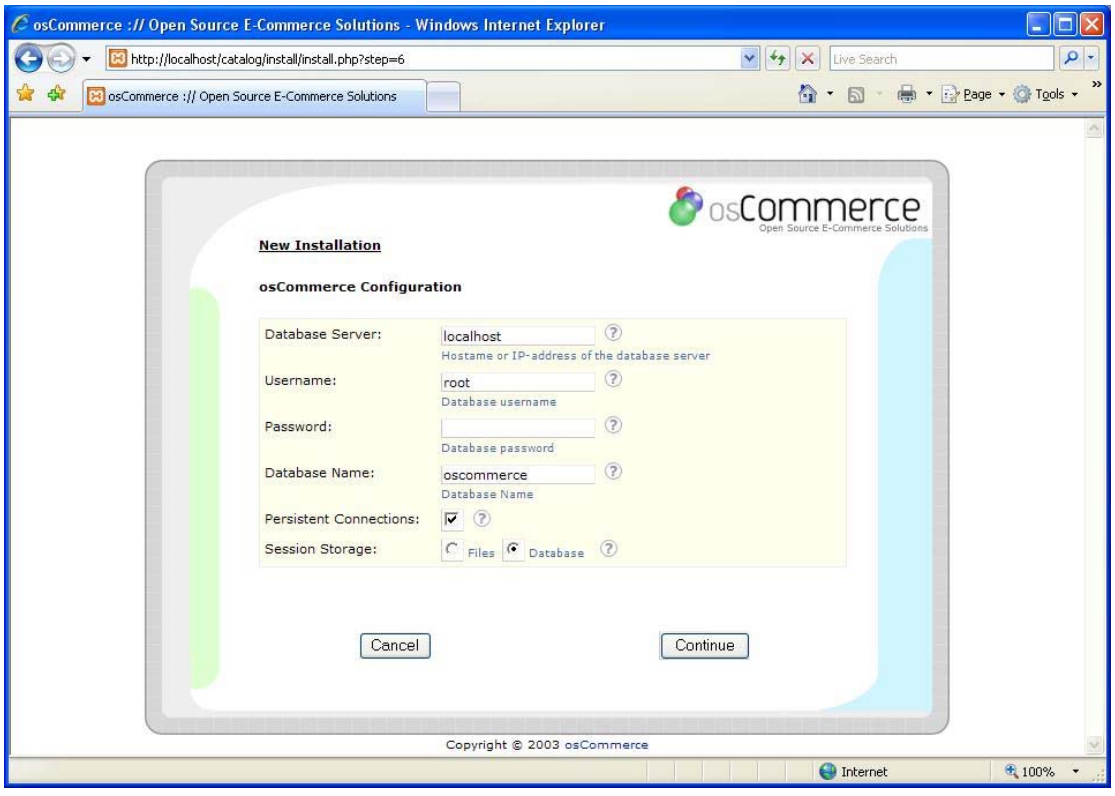
Ακολούθως δίνουμε τις παρακάτω πληροφορίες που αφορούν τον server και συνεχίζουμε πατώντας continue .



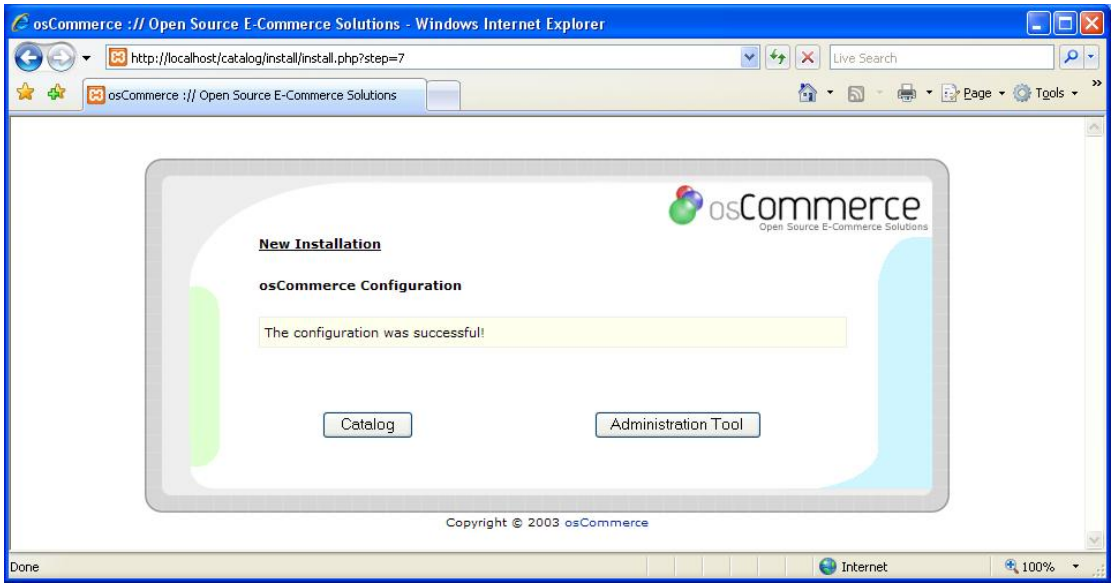
Στην επόμενη σελίδα εισάγουμε τις πληροφορίες για την ασφάλεια του server.



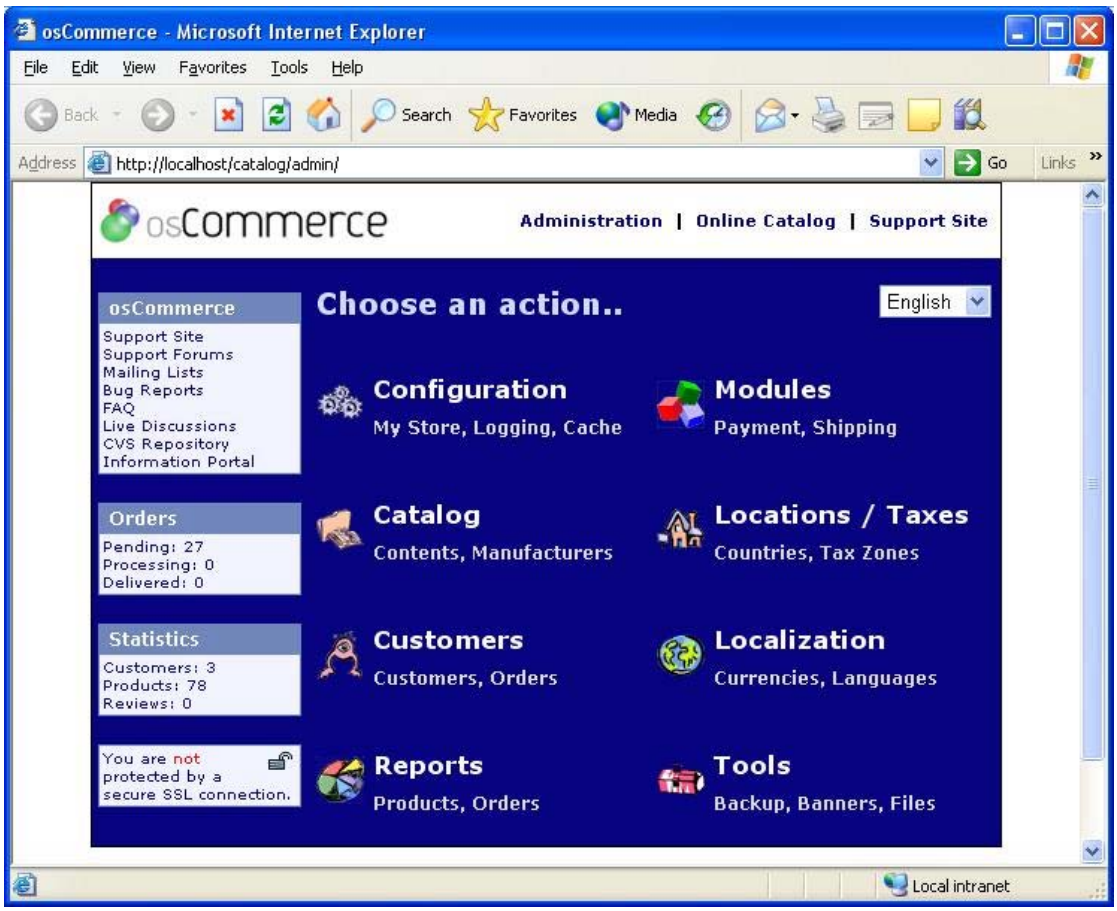
Στη συνέχεια καταχωρούμε ένα ακόμα χρήστη και συνεχίζουμε με continue .



Με την παρακάτω σελίδα ολοκληρώνεται η εγκατάσταση του oscommerce .



Η επιλογή **Catalog** οδηγεί στην αρχική σελίδα του καταστήματος και η επιλογή **Administration Tool** οδηγεί στην σελίδα διαχείρισης του oscommerce.



Εδώ μπορεί ο administrator να διαχειριστεί τους πελάτες, τις παραγγελιές, τα προϊόντα, να δει τις αναφορές και να διαμορφώσει ότι έχει σχέση με το κατάστημα.

Τέλος διαγράφουμε τον φάκελο C:\server\catalog\install και ορίζουμε τις ιδιότητες στα αρχεία configure.php, τόσο στο C:\server\catalog\includes\ όσο και στο C:\server\catalog\admin\includes\, έτσι ώστε να είναι μόνο για ανάγνωση.

2.6 Εγκατάσταση SMTP server

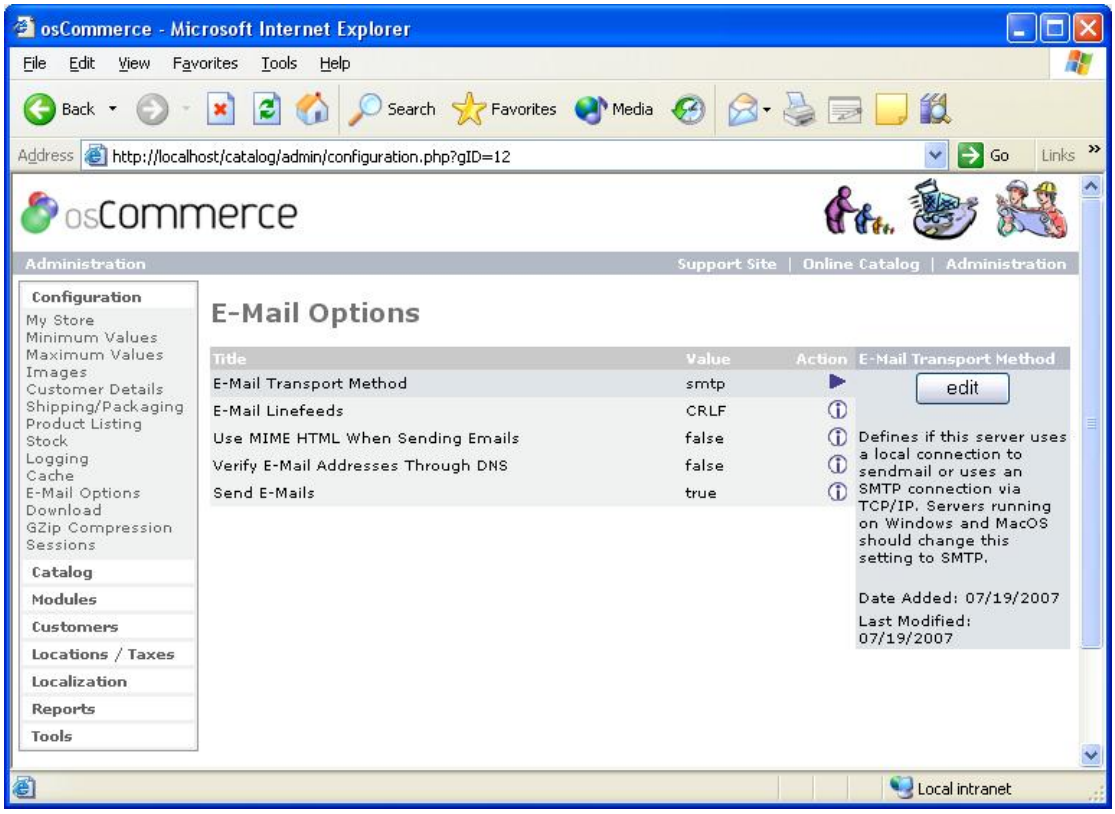
Ο SMTP είναι ένας server ο οποίος καθιστά δυνατή την επικοινωνία, μέσω e-mail, μεταξύ του καταστήματος και του πελάτη. Για παράδειγμα όταν πραγματοποιείται η εισαγωγή ενός νέου πελάτη αυτή επικυρώνεται με την αυτόματη αποστολή ενός e-mail στον πελάτη. Επίσης κατά την διαδικασία της παραγγελίας, ο πελάτης παραλαμβάνει ένα e-mail με όλα τα στοιχεία της, όπως είναι τα προϊόντα, η συνολική αξία και η διεύθυνση αποστολής.

Η εγκατάσταση του SMTP στο osCommerce γίνεται με τη χρήση του phpMailer4osC_v1.O phpMailer περιέχει δύο αρχεία, το class.phpmailer.php και το class.smtp.php. Αυτά τα αρχεία τα αντιγράφουμε τόσο στο C:\apache\catalog\includes\classes όσο και στο C:\apache\catalog\admin\includes\classes. Στη συνέχεια ανοίγουμε το αρχείο C:\apache\catalog\includes\classes\email.php και κάνουμε κάποιες τροποποιήσεις. Βρίσκουμε στο script την εξής εντολή:

```
if '(EMAIL_TRANSPORT == 'smtp')' {
        return mail($to_addr, $subject, $this->output, 'From: ' . $from . $this->lf . 'To: ' . $to . $this->lf . implode($this->lf, $this->headers) . $this->lf . implode($this->lf, $xtra_headers));
```

και την τροποποιούμε όπως φαίνεται στην παρακάτω εικόνα.

Όπως παρατηρούμε σαν host έχουμε ορίσει τον mailscan.epp.teiher.gr ο οποίος είναι ο smtp server του τμήματος πληροφορικής του Α.Τ.Ε.Ι. Σαν username πρέπει να δώσουμε το e-mail που έχουμε στον συγκεκριμένο server και σαν password δίνουμε τον αντίστοιχο κωδικό. Τις ίδιες ρυθμίσεις εφαρμόζουμε και στο αρχείο email.php που βρίσκεται στον κατάλογο C:\apache\catalog\admin\includes\classes**.** Τέλος ανοίγουμε τον browser και γράφουμε http://localhost/catalog/admin/. Η σελίδα που εμφανίζεται είναι η σελίδα διαχείρισης του καταστήματος. Τέλος επιλέγουμε **Configuration**, στη συνέχεια **E-Mail Options** και μετατρέπουμε τις ρυθμίσεις όπου χρειάζεται έτσι ώστε να είναι όπως στην παρακάτω εικόνα.


osCommerce - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/catalog/admin/configuration.php?gID=12
Go Links
osCommerce
Administration
Support Site | Online Catalog | Administration
Configuration
My Store
Minimum Values
Maximum Values
Images
Customer Details
Shipping/Packaging
Product Listing
Stock
Logging
Cache
E-Mail Options
Download
GZip Compression
Sessions
Catalog
Modules
Customers
Locations / Taxes
Localization
Reports
Tools
E-Mail Options
Title
Value
Action
E-Mail Transport Method
E-Mail Transport Method
smtp
edit
E-Mail Linefeeds
CRLF
Use MIME HTML When Sending Emails
false
Verify E-Mail Addresses Through DNS
false
Send E-Mails
true
Defines if this server uses a local connection to sendmail or uses an SMTP connection via TCP/IP. Servers running on Windows and MacOS should change this setting to SMTP.
Date Added: 07/19/2007
Last Modified: 07/19/2007
Local intranet

3. Βασικές λειτουργίες του ηλεκτρονικού καταστήματος

Το επόμενο βήμα από την εγκατάσταση του osCommerce είναι η διαμόρφωση του καταστήματος ανάλογα με τις ανάγκες του ιδιοκτήτη. Στην δική μας περίπτωση, το κατάστημα δημιουργείται για τις ανάγκες ενός κυλικείου το οποίο θέλει να επεκταθεί και να εμπορεύεται τα προϊόντα του μέσω του διαδικτύου. Επομένως τα προϊόντα μας αφορούν καφέδες, αναψυκτικά, μπισκότα κ.τ.λ. Ο κάθε αγοραστής θα πρέπει αρχικά να προστεθεί στο πελατολόγιο του κυλικείου, δίνοντας τα προσωπικά του στοιχεία και τους απαραίτητους κωδικούς πρόσβασης. Αυτή η διαδικασία γίνεται μόνο για την πρώτη παραγγελία, για όλες τις επόμενες εισάγει τον προσωπικό του κωδικό πρόσβασης. Κατά την διαδικασία της αγοράς, ο πελάτης επιλέγει τα προϊόντα, τα προσθέτει στο καλάθι αγορών του και στη συνέχεια επιλέγεται ο τρόπος και όλες οι παράμετροι που αφορούν την πληρωμή. Παρακάτω περιγράφεται αναλυτικά η διαδικασία εισαγωγής ενός προϊόντος, η εισαγωγή νέου πελάτη, καθώς και μία ολοκληρωμένη διαδικασία αγοράς.

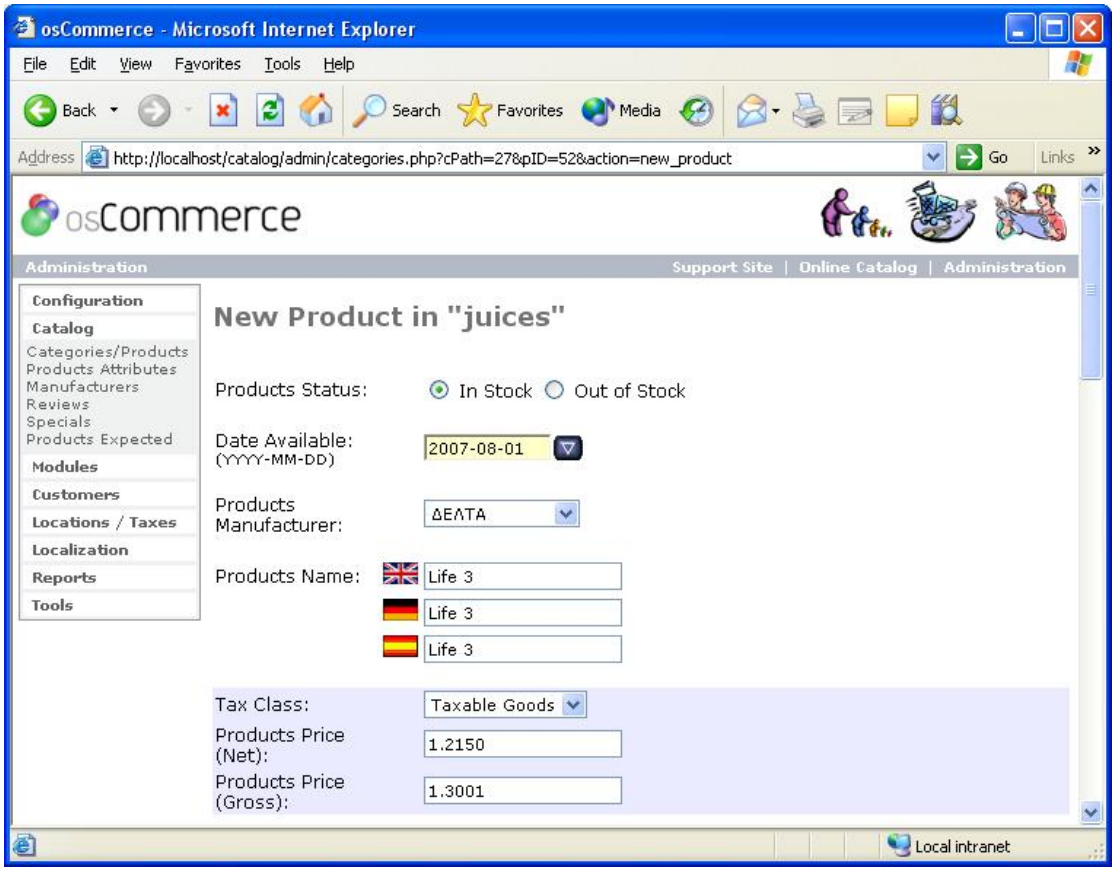
3.1 Εισαγωγή προϊόντος

Αρχικά ανοίγουμε έναν browser και πηγαίνουμε στην σελίδα διαχείρισης του καταστήματος. Για την εισαγωγή των προϊόντων επιλέγουμε **Catalog**.

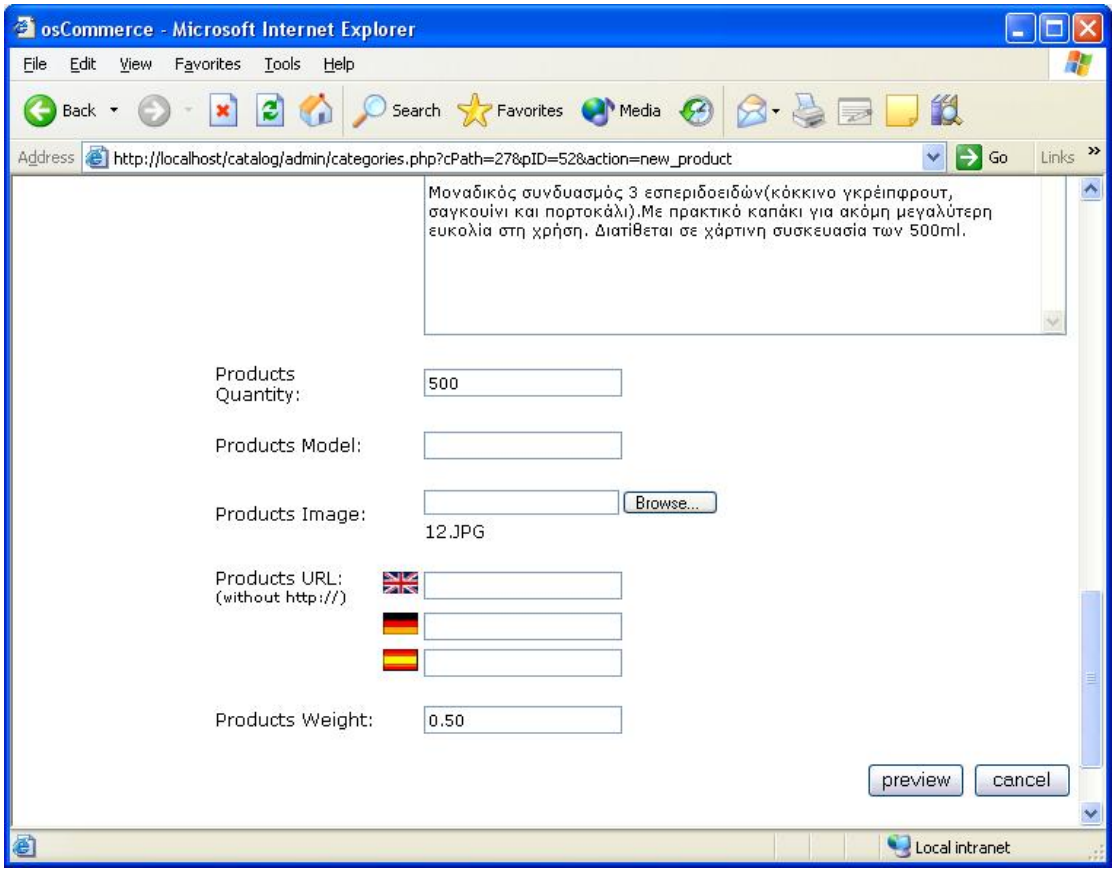
Εδώ παρουσιάζονται όλες οι κατηγορίες και όλα τα προϊόντα που υπάρχουν στην καθεμία από αυτές. Για να δημιουργήσουμε μία νέα κατηγορία επιλέγουμε **new category**.

Συμπληρώνουμε το όνομα, επιλέγουμε την εικόνα που θέλουμε να αντιστοιχεί στην συγκεκριμένη κατηγορία και πατάμε **save**.

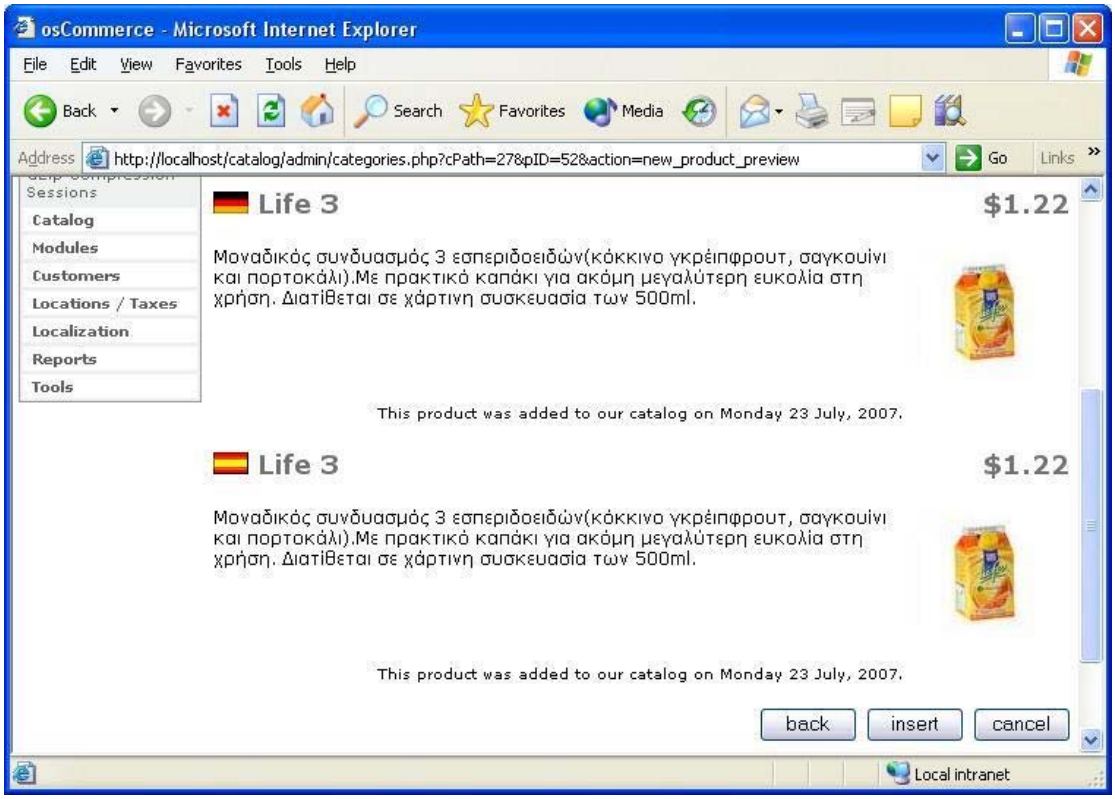
Για να δημιουργήσουμε ένα προϊόν επιλέγουμε **new product**.Έστω ότι θέλουμε να δημιουργήσουμε ένα χυμό, τον Life3. Αρχικά επιλέγουμε αν το προϊόν είναι διαθέσιμο και την ημερομηνία που θα είναι διαθέσιμο. Συμπληρώνουμε το όνομα του κατασκευαστή και του προϊόντος στις 3 γλώσσες(αγγλικά, γερμανικά, ισπανικά) και δίνουμε την αξία του.



Αν θέλουμε μπορούμε να προσθέσουμε κάποια σχόλια ή κάποια περιγραφή για το προϊόν. Τέλος συμπληρώνουμε τη διαθέσιμη ποσότητα, το βάρος και επιλέγουμε την εικόνα που θέλουμε να έχει.



Επιλέγουμε **preview** και στη συνέχεια **insert.**



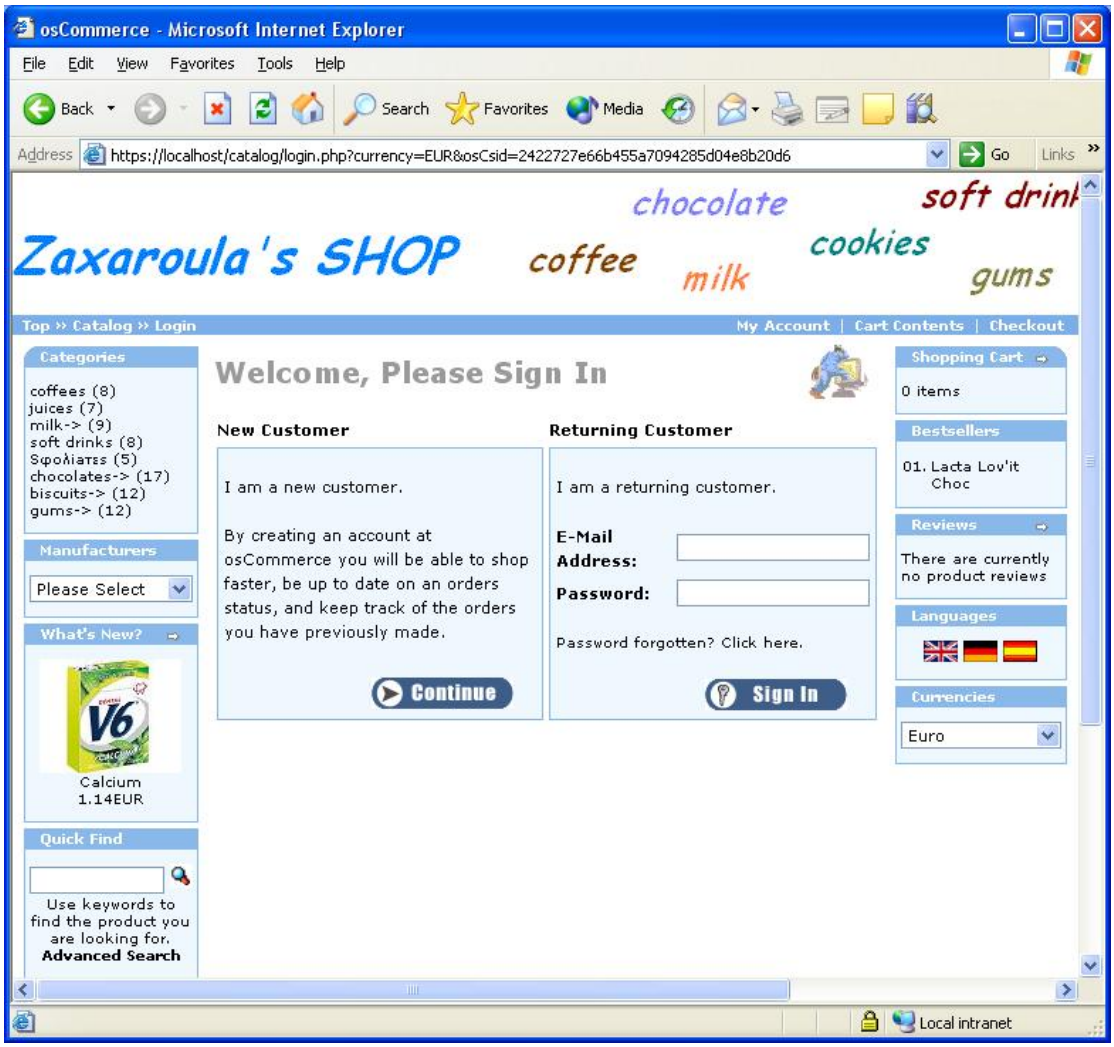
Το προϊόν που δημιουργήσαμε μπορούμε να το εισάγουμε σε όποια κατηγορία θέλουμε επιλέγοντας **move**

και στη συνέχεια την επιθυμητή κατηγορία.

Με τον ίδιο τρόπο εισάγουμε όλες τις κατηγορίες και τα προϊόντα που θα εμπορεύεται το κατάστημα μας.

3.2 Εισαγωγή νέου πελάτη

Στην αρχική σελίδα του καταστήματος επιλέγουμε “My Account” και εμφανίζεται η παρακάτω οθόνη.



Αν ο χρήστης είναι καινούριος και δεν έχει φτιάξει κάποιο λογαριασμό τότε επιλέγει **continue**. Στην φόρμα που εμφανίζεται, ο χρήστης συμπληρώνει τα προσωπικά του στοιχεία. Τα πεδία της φόρμας που έχουν * είναι υποχρεωτικό να συμπληρωθούν διαφορετικά εμφανίζεται μήνυμα λάθους και η καταχώρηση του χρήστη δεν μπορεί να ολοκληρωθεί.

My Account Information

NOTE: If you already have an account with us, please login at the login page.

Your Personal Details * Required information

Gender: ○ Male ◉ Female *
First Name: Christina *
Last Name: Charitwnidi *
Date of Birth: 12/10/1979 * (eg. 05/21/1970)
E-Mail Address: stinaxarit@hotmail.com *

Company Details

Company Name:

Your Address

Street Address: Ikarou 150 *
Suburb:
Post Code: 71408 *
City: Heraklion *
State/Province: Crete *
Country: Greece *

Your Contact Information

Telephone Number: 6965432187 *
Fax Number:

Options

Newsletter: ☐

Your Password

Password: ••••••••• *
Password Confirmation: ••••••••• *

Continue

Αφού συμπληρωθούν επιτυχώς τα πεδία, ο χρήστης επιλέγει **continue** και η σελίδα που εμφανίζεται ενημερώνει τον χρήστη για την επιτυχή καταχώρηση του.

Your Account Has Been Created!

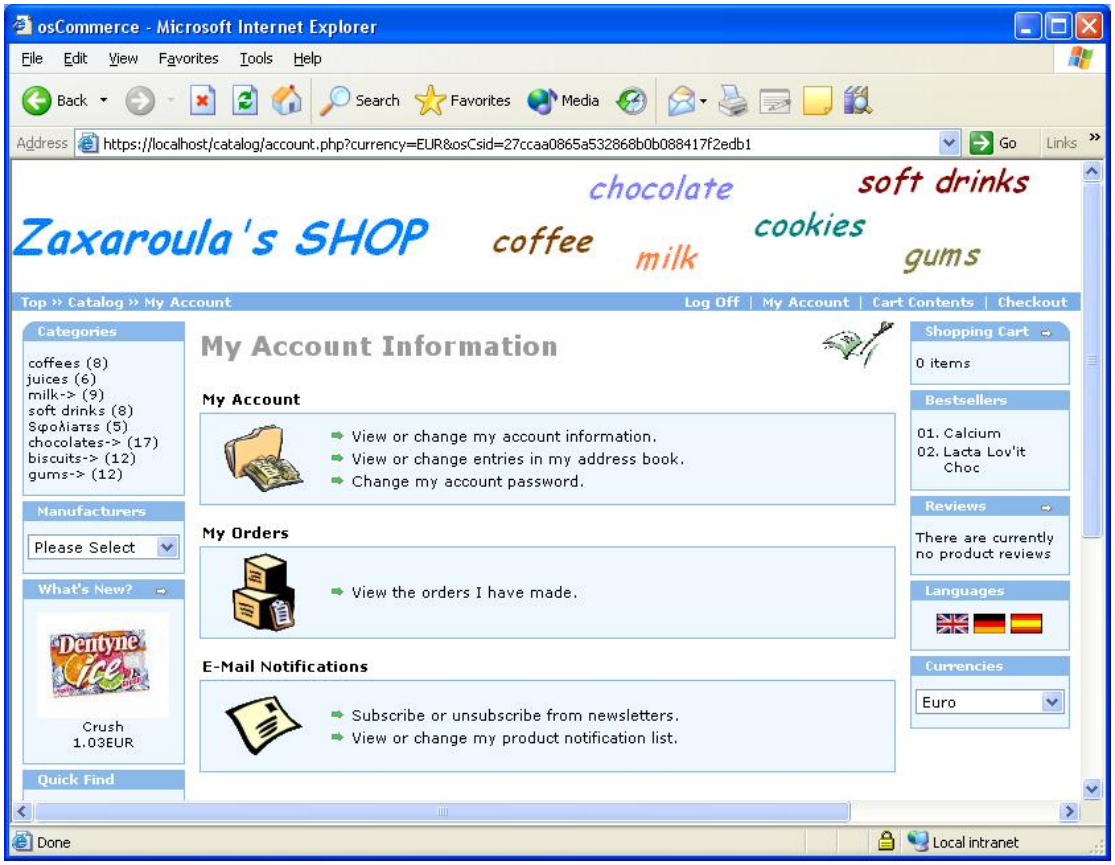
Congratulations! Your new account has been successfully created! You can now take advantage of member priviledges to enhance your online shopping experience with us. If you have **ANY** questions about the operation of this online shop, please email the store owner.

A confirmation has been sent to the provided email address. If you have not received it within the hour, please contact us.

Continue

Παράλληλα αποστέλλεται ένα e-mail στον χρήστη το οποίο τον ενημερώνει για τις υπηρεσίες που θα του παρέχει το κατάστημα.

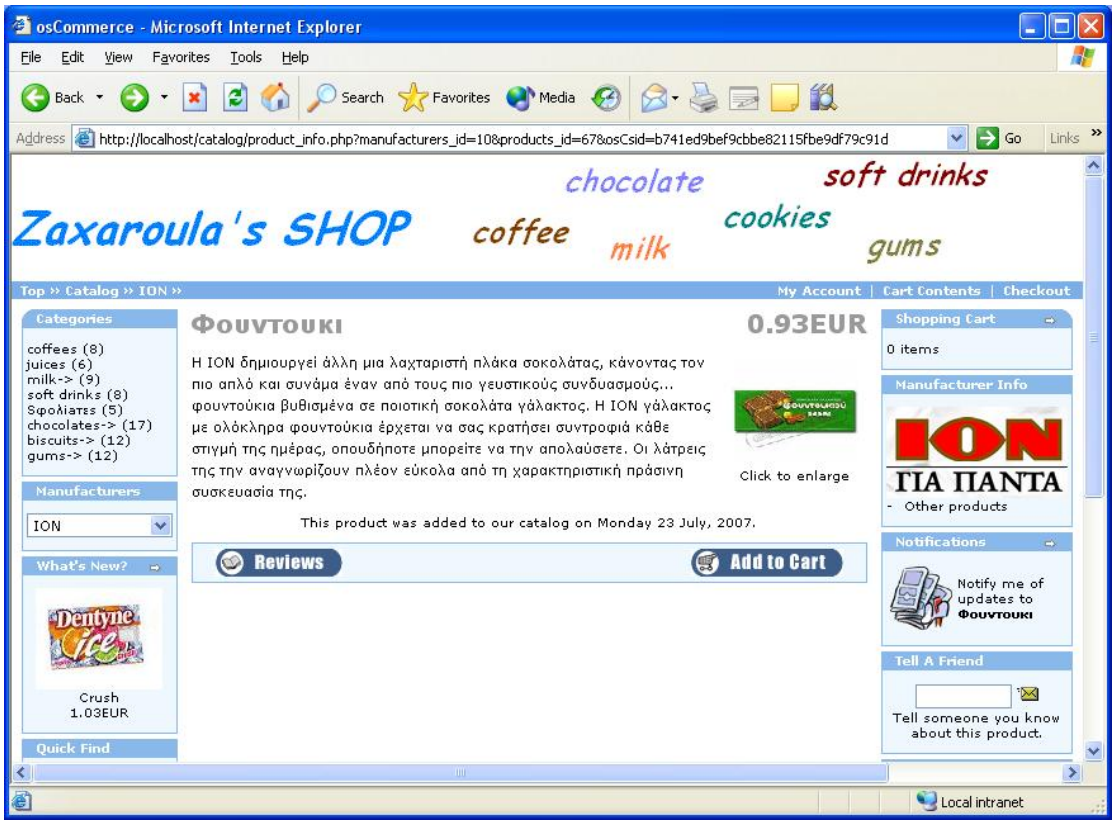
Από την στιγμή που ο χρήστης έχει κάποιο λογαριασμό, για εισέλθει σ' αυτόν επιλέγει **My Account** και στη συνέχεια εισάγει το e-mail και το password που είχε δώσει κατά την εγγραφή του. Επιλέγοντας **sign in** εισάγεται στον λογαριασμό του και βλέπει όλες τις πληροφορίες σχετικά μ΄ αυτόν καθώς και το ιστορικό των παραγγελιών του.



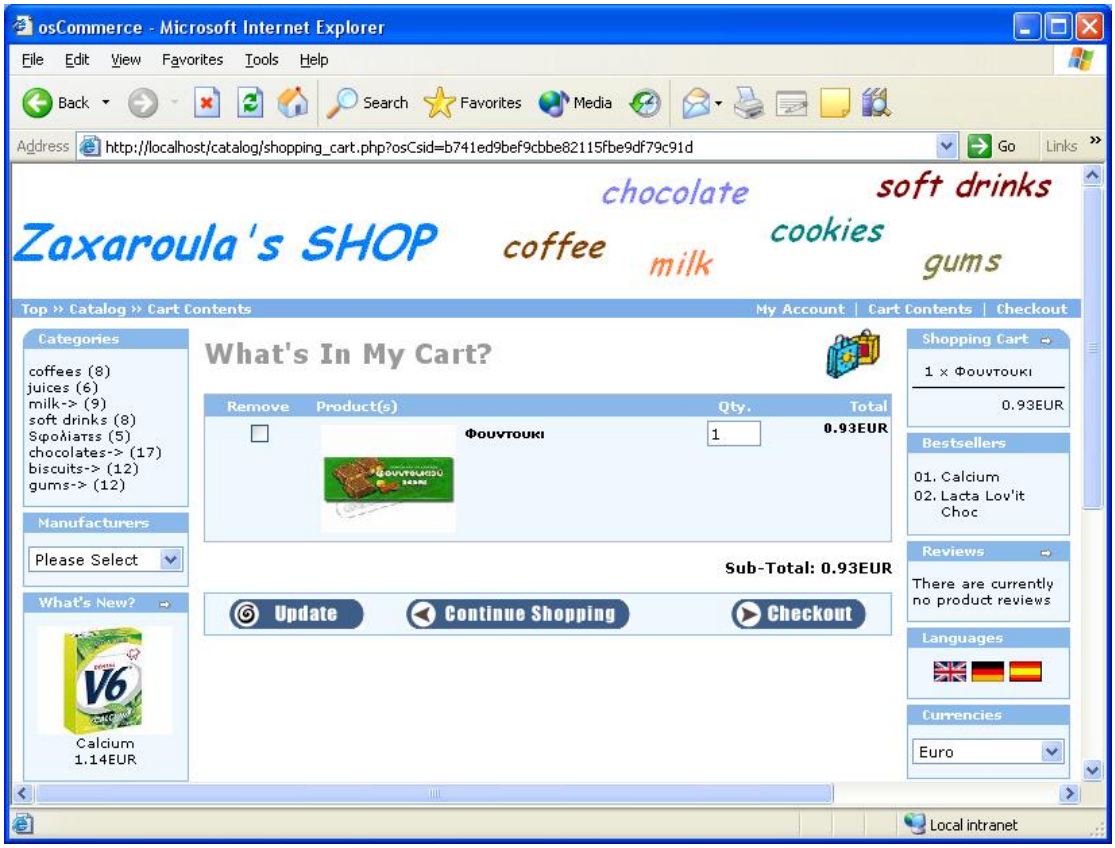
Για να εξέλθει ο χρήστης από τον λογαριασμό του επιλέγει **Log Off** και έτσι επιστρέφει στην αρχική σελίδα του καταστήματος.

3.3 Διαδικασία παραγγελίας

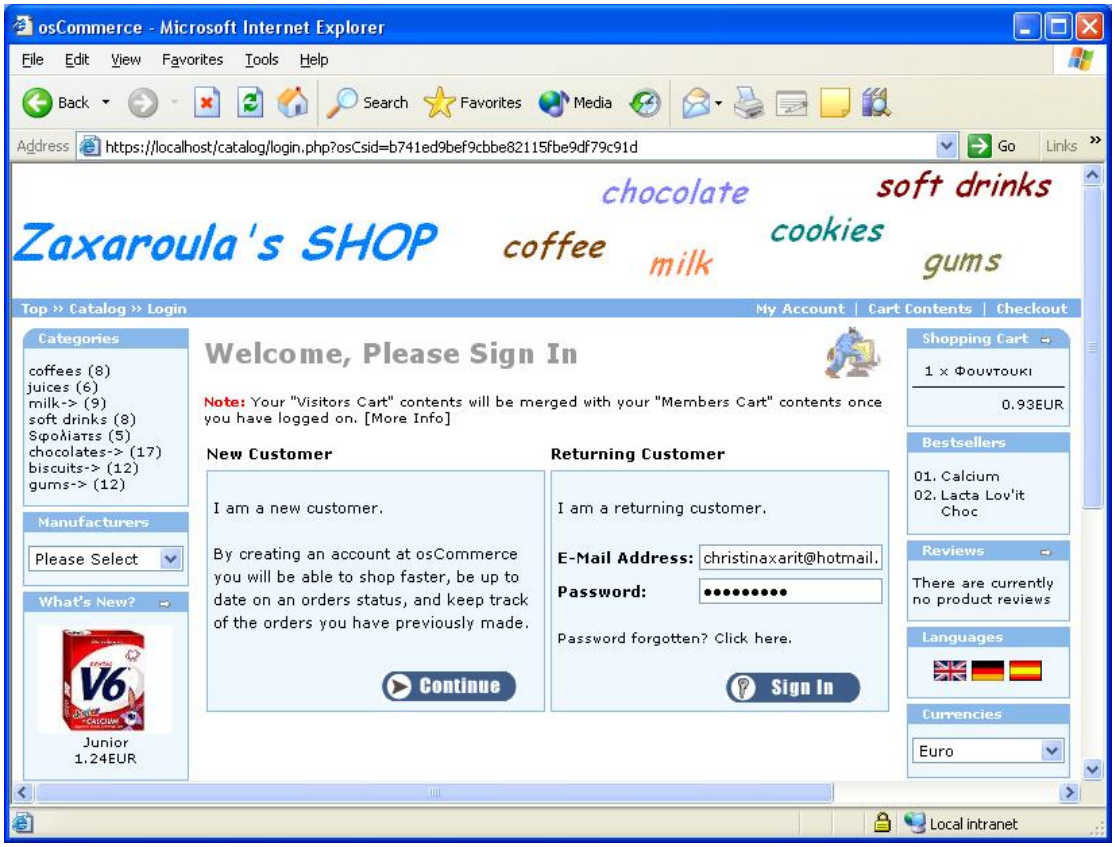
Για την διαδικασία της παραγγελίας το πρώτο πράγμα που πρέπει να γίνει, είναι η επιλογή των προϊόντων. Τα προϊόντα είναι χωρισμένα σε κατηγορίες και για το καθένα από αυτά διατίθεται κάποια σχετική περιγραφή.



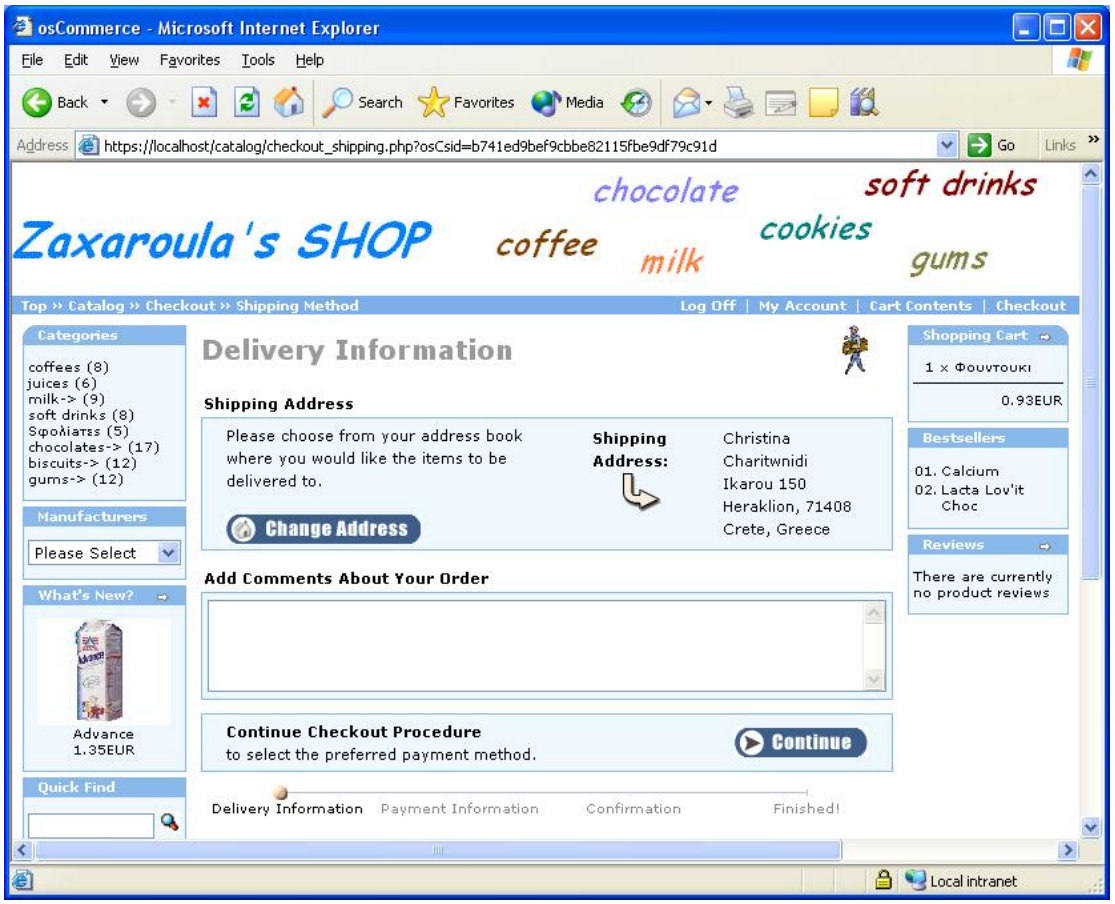
Επιλέγοντας το κουμπί **Reviews** ο πελάτης μπορεί να διαβάσει σχόλια άλλων πελατών για το συγκεκριμένο προϊόν. Όταν αποφασίσει ότι θέλει να αγοράσει κάποιο προϊόν, επιλέγει το κουμπί **Add to Cart** έτσι ώστε να προσθέσει το προϊόν στο καρότσι του.



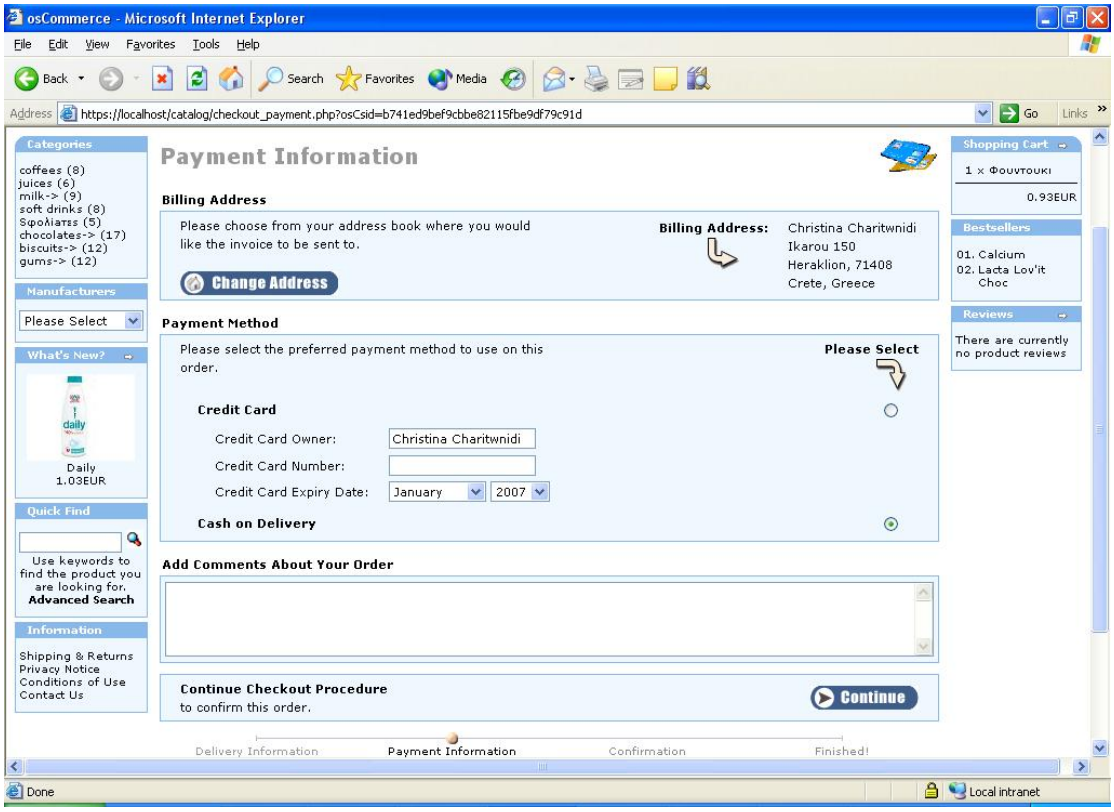
Στη συνέχεια συμπληρώνει την ποσότητα του προϊόντος στο αντίστοιχο πεδίο. Αν ο πελάτης θέλει να αγοράσει κι άλλα προϊόντα τότε επιλέγει το κουμπί **Continue Shopping** και συνεχίζει τα ψώνια του διαφορετικά επιλέγει το κουμπί **Checkout** .



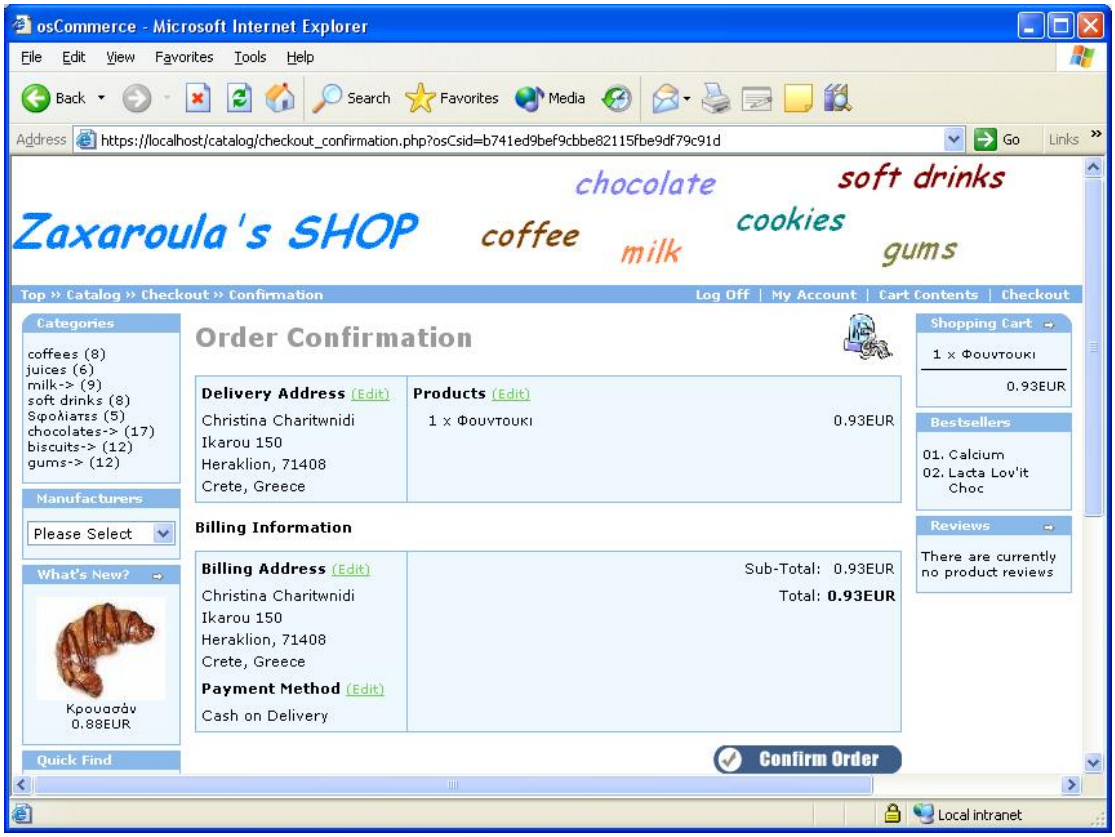
Σ’ αυτό το στάδιο ο πελάτης δίνει το e-mail και τον κωδικό του και επιλέγει **Sign In**.



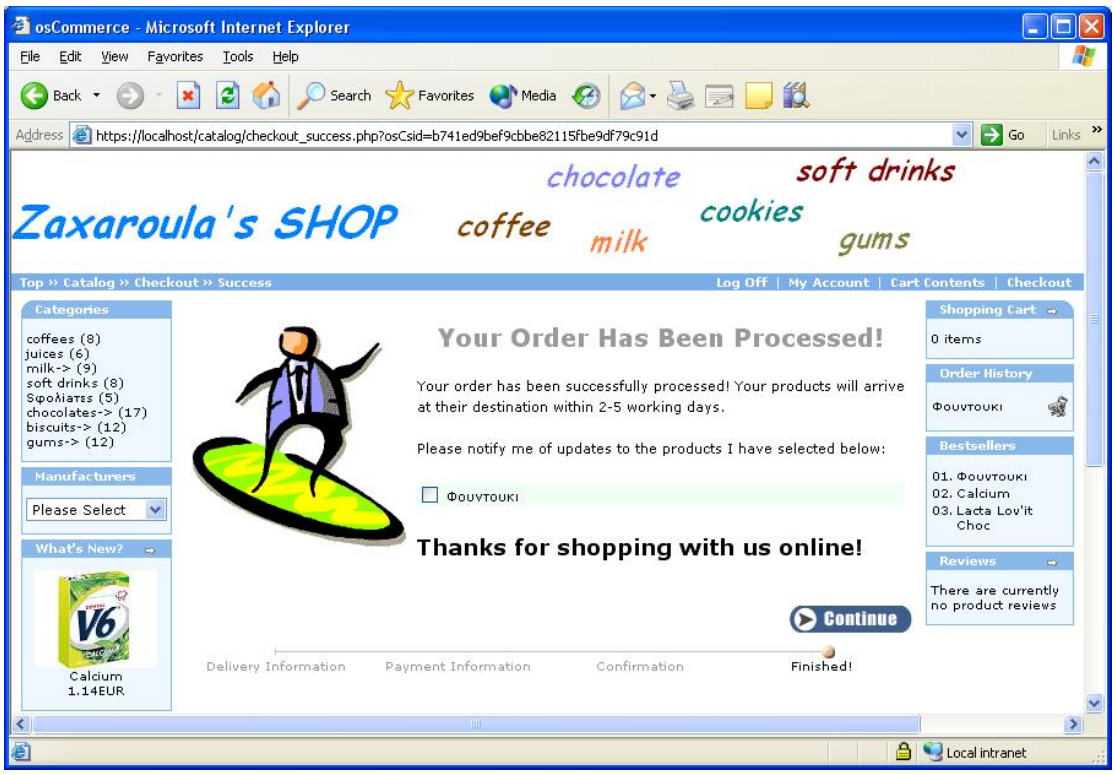
Ακολούθως ελέγχει τις πληροφορίες της παραγγελίας και αν θέλει μπορεί να αλλάξει την διεύθυνση παράδοσης, διαφορετικά επιλέγει **Continue**.



Το επόμενο βήμα είναι να επιλεγεί ο τρόπος πληρωμής. Ο πρώτος τρόπος αφορά πληρωμή με πιστωτική κάρτα ενώ ο δεύτερος πληρωμή την ώρα της παραλαβής. Για να συνεχιστεί η διαδικασία επιλέγει **Continue**.



Ο πελάτης ελέγχει τα συνολικά στοιχεία της παραγγελίας και για να την επικυρώσει επιλέγει **Confirm Order** .



Η παραπάνω σελίδα ενημερώνει τον πελάτη για την επιτυχή διεξαγωγή της παραγγελίας ενώ παράλληλα του αποστέλλεται ένα e-mail με τα στοιχεία της παραγγελίας. Μ' αυτόν τον τρόπο ολοκληρώνεται η παραγγελία.

4. Διεκπεραίωση πληρωμών μέσω τράπεζας

Ένα ηλεκτρονικό κατάστημα μπορεί να παρέχει διάφορους τρόπους πληρωμής στους πελάτες του όπως είναι η πληρωμή κατά την παράδοση των προϊόντων, το PayPal, το PsiGate, η πληρωμή μέσω πιστωτικής κάρτας κ.α. Σε κάποιες από αυτές τις μεθόδους απαιτείται συνεργασία του ηλεκτρονικού καταστήματος με κάποια τράπεζα για την διεκπεραίωση των πληρωμών του. Παρακάτω περιγράφεται ενδεικτικά ο τρόπος με τον οποίο επιτυγχάνεται αυτή η συνεργασία με μία από τις τράπεζες που παρέχουν αυτή τη δυνατότητα, την τράπεζα Πειραιώς.

Η τράπεζα Πειραιώς απευθύνεται σε όλες τις επιχειρήσεις που διαθέτουν websites ή / και ηλεκτρονικά καταστήματα που πωλούν προϊόντα-υπηρεσίες μέσω Internet ή ενδιαφέρονται να δραστηριοποιηθούν στο χώρο του ηλεκτρονικού εμπορίου. Η πληρωμή διεκπεραιώνεται αυτόματα μέσω του winbank paycenter και το ποσό κατατίθεται στον λογαριασμό της επιχείρησης στην Τράπεζα Πειραιώς.

Χρησιμοποιώντας τις υπηρεσίες του **winbank paycenter** εξασφαλίζεται:

- Άμεση είσπραξη μαζί με την on-line παραγγελία του πελάτη
- Χρήση οποιασδήποτε πιστωτικής κάρτας Visa/MasterCard και χρεωστικής Visa Electron
- Εύκολη πληρωμή για τον πελάτη
- Ασφαλή επικοινωνία των συναλλαγών με το winbank paycenter
- Οικονομία στο κόστος είσπραξης
- Αυτο-διαχείριση και πλήρες on-line reporting των εισπράξεων
- Κανένα απολύτως κόστος εγκατάστασης αφού όλες οι υπηρεσίες λειτουργούν από ασφαλή Internet sites

4.1 Μέθοδοι συναλλαγής μέσω του winbank paycenter

Ανάλογα με την ετοιμότητα του ηλεκτρονικού καταστήματος διατίθενται οι παρακάτω επιλογές επικοινωνίας με το winbank paycenter για την ολοκλήρωση της πληρωμής του πελάτη:

4.1.1 Redirection του Πελάτη στο winbank paycenter.

Μόλις ο πελάτης ολοκληρώσει την παραγγελία του στο ηλεκτρονικό κατάστημα και ενημερωθεί για την τελική τιμή και τη διαθεσιμότητα των προϊόντων-υπηρεσιών που παράγγειλε, ανακατευθύνεται για την πληρωμή στην ασφαλή σελίδα του winbank paycenter. Ο πελάτης ενημερώνεται για την χρέωση, πληκτρολογεί τα στοιχεία της πιστωτικής του κάρτας και η αποστολή και διεκπεραίωση της πληρωμής γίνεται με απόλυτη ασφάλεια επικοινωνίας (SSL 128 bit) από το winbank paycenter. Η ολοκλήρωση της συναλλαγής πραγματοποιείται άμεσα. Η κάρτα του πελάτη

χρεώνεται και η επιχείρηση μπορεί πλέον να εισπράττει στο τραπεζικό της λογαριασμό στην Τράπεζα Πειραιώς.

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

4.1.2 Web Service Επικοινωνία με το winbank paycenter.

Με την επιλογή αυτή ο πελάτης με το πέρας της παραγγελίας του καθοδηγείται για την εισαγωγή των στοιχείων της κάρτας του από το τις σελίδες του ίδιου του web-site ή ηλεκτρονικού καταστήματος. Ο web server του ηλεκτρονικού καταστήματος επικοινωνεί με web service (server-to-server επικοινωνία) με το winbank paycenter για την διεκπεραίωση της πληρωμής του πελάτη. Τα στοιχεία πληρωμής μεταβιβάζονται κρυπτογραφημένα στο winbank paycenter. Απαραίτητη προϋπόθεση είναι η εφαρμογή του ηλεκτρονικού καταστήματος να έχει SSL 128 bit κρυπτογράφηση.

Η λύση web service (XML messaging) συνιστάται σε web sites και ηλεκτρονικά καταστήματα με ανεπτυγμένη υποδομή ασφάλειας και διαχείρισης της πελατείας τους.

Πολλά είναι τα πλεονεκτήματα που προκύπτουν από τις On-line Πληρωμές σε Web-Sites μέσω του winbank paycenter.Αυτά συνοψίζονται παρακάτω:

- Δυνατότητα on-line / real-time πληρωμών οποιαδήποτε στιγμή
- Εξυπηρέτηση όλων των πελατών, ανεξάρτητα της τραπεζικής τους σχέσης
- Ελαχιστοποίηση του κόστους είσπραξης για την επιχείρηση
- Μεγιστοποίηση της πελατείας και ωραρίου λειτουργίας για την επιχείρηση
- Τεχνολογική συμβατότητα με κάθε web site και e-shop
- Αυτο-διαχείριση, ενημέρωση και reconciliation μέσω του **paycenter Admintool**
- Αυτόματη είσπραξη σε τραπεζικό λογαριασμό της επιχείρησης

4.2 Paycenter Admintool

Το paycenter AdminTool είναι η σημαντική προστιθέμενη αξία που προσδίδει η winbank στις υπηρεσίες paycenter και προσφέρει δωρεάν στις συνεργαζόμενες επιχειρήσεις.

Για όλες τις υπηρεσίες εισπράξεων winbank paycenter, παρέχεται στην επιχείρηση η εφαρμογή paycenter AdminTool για την on-line διαχείριση κάθε είσπραξης, τον αντιλογισμό (cancel, refund) των συναλλαγών και τη συμφωνία των παραγγελιών με τις εισπράξεις (reconciliation).

Στην ασφαλή internet σελίδα του paycenter AdminTool, αρμόδια στελέχη της επιχείρησης (π.χ. λογιστήριο)έχουν ελεγχόμενη πρόσβαση (username/password) ώστε να παρακολουθούν αναλυτικά τις εισπράξεις - συναλλαγές από τους πελάτες και να διαχειρίζονται το status κάθε συναλλαγής:

- Αναμονή (pending transactions)
- Έγκριση (approved transactions)
- Ολοκλήρωση (accepted transactions)
- Ακύρωση (cancel transactions)
- Επιστροφή (refund)
- Απόρριψη (void transactions)
- Πακέτο συναλλαγών (batches)
- Αναλυτικό reporting ανά υπηρεσία είσπραξης, με πολλαπλά κριτήρια αναζήτησης
- Download των εκτελεσμένων συναλλαγών

Επιπλέον μέσω του paycenter AdminTool παρέχονται οι εξής δυνατότητες**:**

- Αναζήτηση συναλλαγών με πολλαπλά κριτήρια
- Πρόσβαση στο winbank internet (on-line διαχείριση του τραπεζικού λογαριασμού της επιχείρησης)
- On-line βοήθεια με αναλυτικές οδηγίες χρήσης του paycenter AdminTool
- Διαχείριση της ασφάλειας

4.3 Βασικές προϋποθέσεις συνεργασίας για Ηλεκτρονικές Πληρωμές & Εισπράξεις

Οι προϋποθέσεις που πρέπει να πληρεί ένα ηλεκτρονικό κατάστημα για την συνεργασία του με την τράπεζα, είναι οι εξής:

• Η επιχείρησή πρέπει να έχει ελληνικό Α.Φ.Μ.

Η επιχείρησή πρέπει να έχει έδρα στην Ελλάδα ή παράρτημα στην Ελλάδα ή να έχει ορίσει φορολογικό αντιπρόσωπο στην Ελλάδα, ώστε να έχει ελληνικό Α.Φ.Μ.

• Οι συναλλαγές της επιχείρησής να διεξάγονται σε ευρώ

Η Τράπεζα Πειραιώς μπορεί να εξυπηρετήσει την επιχείρησή σε ηλεκτρονικές πληρωμές και εισπράξεις για συναλλαγές που διεξάγονται σε ευρώ και όχι σε άλλα νομίσματα (π.χ. δολλάρια, λίρες κ.α.).

• Να υπάρχει τραπεζικός λογαριασμός νομικού προσώπου στην Τράπεζα Πειραιώς.

Οι εισπράξεις από τις on-line πληρωμές κατατίθενται σε τραπεζικό λογαριασμό της επιχείρησής στην Τράπεζα Πειραιώς. Παρέχεται ενημέρωση για τα απαιτούμενα δικαιολογητικά για το άνοιγμα του τραπεζικού λογαριασμού που αντιστοιχεί στη νομική μορφή της επιχείρησής.

• Η δραστηριότητα της επιχείρησής να είναι αποδεκτή από την Τράπεζα.

Η δραστηριότητα της επιχείρησης εξετάζεται σε κάθε συνεργασία με την Τράπεζα. Ενδεικτικές δραστηριότητες που δεν γίνονται αποδεκτές από την Τράπεζα: Φάρμακα, Time Sharing, Συμπληρώματα Διατροφής, Γραφεία συνοδών, Μασάζ, Τυχερά Παιχνίδια κ.α.

• Η επιχείρησή να μην είναι καταχωρημένη στα αρχεία που τηρεί η ΤΕΙΡΕΣΙΑΣ Α.Ε.

Η Τράπεζα διατηρεί το δικαίωμα ελέγχου των στοιχείων της επιχείρησης καθώς και των προσώπων που την εκπροσωπούν στα αρχεία της ΤΕΙΡΕΣΙΑΣ Α.Ε. και να μην εγκρίνει τη συνεργασία με την επιχείρηση εφόσον διαπιστωθούν δυσμενή στοιχεία τα οποία δεν έχουν τακτοποιηθεί.

4.4 Όροι χρήσης για πληρωμές μέσω του web site

Το web site της επιχείρησής πρέπει *να είναι έτοιμο* και να πληρεί τα παρακάτω βασικά στοιχεία ηλεκτρονικού καταστήματος. Τα στοιχεία αυτά συντάσσονται με τις οδηγίες που εκδίδουν οι οργανισμοί καρτών Visa/MasterCard καθώς και άλλοι φορείς της αγοράς (π.χ. ΙΝΚΑ) και στοχεύουν στην ανάπτυξη εμπιστοσύνης με τους πελάτες και στην αύξηση της ασφάλειας των ηλεκτρονικών αγορών/συναλλαγών στο e-shop/web site. Τα στοιχεία αυτά είναι:

• Παρουσίαση της επιχείρησή και προβολή των στοιχείων επικοινωνίας

Παρουσίαση της επιχείρησης μέσω ενός σύντομου προφίλ, στο οποίο αναφέρετε η δραστηριότητά, η ιστορική αναδρομή, οι σκοποί, τα ανταγωνιστικά πλεονεκτήματά κ.α.

Τα στοιχεία επικοινωνίας πρέπει να περιλαμβάνουν ταχυδρομική διεύθυνση, τηλέφωνο επικοινωνίας και e-mail (κεντρικό ή των επιμέρους τμημάτων της επιχείρησης).

• Ορθή παρουσίαση προϊόντων/υπηρεσιών

Παρουσίαση των προϊόντων/υπηρεσιών με όλες τις απαραίτητες πληροφορίες ώστε να είναι σαφές στον πελάτη τι είναι αυτό για το οποίο θα πληρώσει. Πρέπει να συμπεριλαμβάνονται στην παρουσίαση τυχόν εικόνες, αναλυτικά χαρακτηριστικά, γνώμες/ συστάσεις κ.α.

• Ξεκάθαρη τιμολόγηση

Ο πελάτης πρέπει να ενημερώνεται αναλυτικά και ξεκάθαρα για την τιμή των προϊόντων/ υπηρεσιών, για τυχόν φόρους (π.χ. ΦΠΑ) και λοιπές χρεώσεις (π.χ. έξοδα αποστολής) που αφορούν την παραγγελία του καθώς και για την τελική χρέωσή του.

• Αναλυτική πολιτική για αγορές στο e-shop/web site

Οι όροι αγορών στο e-shop πρέπει να είναι ξεκάθαροι και αναλυτικοί. Ο πελάτης πρέπει να ενημερώνεται για θέματα όπως παράδοση προϊόντων, τρόποι πληρωμής, ακύρωση παραγγελίας, αλλαγή παραγγελίας, επιστροφή προϊόντων, επιστροφή χρημάτων, περιορισμοί αγορών από την επιχείρησή, εγγραφή στο site, ειδικές επιθυμίες, εγγύηση προϊόντων, εξυπηρέτηση μετά την αγορά, διαχείριση παραπόνων κ.α.

• Πολιτική ασφάλειας προσωπικών δεδομένων

Ο πελάτης πρέπει να ενημερώνεται για τον τρόπο με τον οποίο διαχειρίζονται τα προσωπικά στοιχεία που καταχωρεί κατά την παραγγελία του. Ενημέρωση του πελάτη για τα στοιχεία που ζητούνται από εκείνον, για τον τρόπο με τον οποίο αυτά διατηρούνται στην επιχείρησή, εάν διατίθενται σε τρίτους και με ποιόν τρόπο, εάν θα χρησιμοποιηθούν από την επιχείρησή για αποστολή διαφημιστικού υλικού στον πελάτη κ.α.

• Διαφύλαξη ακεραιότητας και ασφάλειας των στοιχείων συναλλαγής

Η πληροφορία που περιέχεται σε μια συναλλαγή πρέπει να είναι τόσο ασφαλής όσο τα συστήματα που την περιέχουν και οι άνθρωποι που έχουν πρόσβαση σε αυτήν. Όλες οι επιχειρήσεις/ οργανισμοί που διενεργούν συναλλαγές χωρίς την παρουσία του πελάτη είναι υποχρεωμένες να συμμορφώνονται με το παγκόσμιο πρότυπο για την προστασία της πληροφορίας των καταναλωτών που ονομάζεται Payment Card Industry (PCI) Data Security Standard.

5. Μέθοδοι πληρωμής που υποστηρίζει το osCommerce

Το osCommerce παρέχει στους πελάτες του διάφορες μεθόδους πληρωμής των αγορών τους έτσι ώστε να είναι σε θέση να επιλέξουν αυτόν που τους ταιριάζει περισσότερο. Οι σημαντικότερες από αυτές τις μεθόδους αναλύονται παρακάτω.

Το **2Checkout** (2CO) είναι ένας εξουσιοδοτημένος τρόπος μεταπώλησης ο οποίος χρησιμοποιείται σε περισσότερα από 40.000 διεθνή websites προσφέροντας μία μεγάλη ποικιλία προϊόντων και online υπηρεσιών. Η τεχνολογία του 2CO υποστηρίζει μεθόδους οι οποίες περιλαμβάνουν οικονομικές αναφορές, πρόληψη από απάτες κ.α. Το 2Checkout καθιερώθηκε το 1999 από το David A. Homewood και βρίσκεται στο Columbus του Οχάιο.

Το 2Checkout προσφέρεται από online επιχειρήσεις οι οποίες παρέχουν υπηρεσίες ή προϊόντα προς πώληση. Κάθε πωλητής προμηθεύει τα προϊόντα του στο 2CO για άμεση μεταπώληση τους στους πελάτες. Οι πελάτες ψωνίζουν τα προϊόντα τους στο website του πωλητή και στη συνέχεια συμπληρώνουν τη φόρμα παραγγελίας στο 2CO για να ολοκληρώσουν την πληρωμή.

Το 2CO συνεργάζεται επιτυχώς με τα ποιο γνωστά software καροτσιών αγοράς συμπεριλαμβανομένου του osCommerce, ενώ δέχεται πληρωμές σε μία ποικιλία νομισμάτων.

Το **Authorize.Net** είναι ένας τρόπος πληρωμής ο οποίος επιτρέπει στους εμπόρους να δεχτούν πιστωτικές κάρτες και ηλεκτρονικές επιταγές μέσα από το website τους χρησιμοποιώντας μία IP σύνδεση. Αποτελεί την μεγαλύτερη υπηρεσία παροχής πληρωμών, καθώς το εμπιστεύονται περισσότερο από 160.000 έμποροι.

Το Authorize.Net προσφέρει δύο μεθόδους για την ολοκλήρωση της υπηρεσίας πληρωμών. Η πρώτη μέθοδος λέγεται Simple Integration Method (SIM) και αποτελεί την λιγότερο πολύπλοκη από τις δύο. Χρησιμοποιώντας αυτή τη μέθοδο, ο έμπορος κατευθύνει τον πελάτη στο website του Authorize.Net όπου σε μία ασφαλή σελίδα θα δοθούν οι πληροφορίες της συναλλαγής και στη συνέχεια ανακατευθύνεται στο website του εμπόρου. Αυτή η μέθοδος χρησιμοποιείται από μικρές συνήθως επιχειρήσεις οι οποίες δεν διαθέτουν τις τεχνικές προδιαγραφές για ακόμα μεγαλύτερη ολοκλήρωση.

Η δεύτερη μέθοδος ολοκλήρωσης λέγεται Advanced Integration Method (AIM) και χρησιμοποιείται από μεγαλύτερες επιχειρήσεις. Είναι πιο πολύπλοκη αλλά και πιο ισχυρή από την SIM. Η AIM χρησιμοποιεί το API του Authorize.Net έτσι ώστε οι πελάτες να μην χρειάζεται να «εγκαταλείψουν» το website του εμπόρου. Σ΄ αυτή τη μέθοδο ο πελάτης δεν γνωρίζει τον τρόπο που γίνεται η συναλλαγή.

Το **PayPal** είναι μία online υπηρεσία μεταφοράς χρημάτων. Χρησιμοποιείται ευρέως για ασφαλείς συναλλαγές μέσω του Internet. Διαθέτει πάνω από 63 εκατομμύρια λογαριασμούς και πάνω από 53.000 άτομα γράφονται καθημερινά σ ΄ αυτό.

Το PayPal λειτουργεί όπως ένας απλός τραπεζικός λογαριασμός ο κάτοχος του οποίου είναι σε θέση να καταθέσει χρήματα, να κάνει ανάληψη ή να στείλει χρήματα

σε κάποιον άλλο λογαριασμό. Χάρη στο σύστημα PayPal, τα στοιχεία της πιστωτικής κάρτας δεν είναι πλέον απαραίτητα κάθε φορά που γίνετε μια συναλλαγή, εξαιτίας της άμεσης χρέωσης του λογαριασμού PayPal.

Είναι ασφαλές καθώς ο μόνος που γνωρίζει τα στοιχεία της κάρτας είναι το ίδιο το PayPal. Ο παραλήπτης το μόνο που κάνει είναι να παραλαμβάνει τα χρήματα και όχι αριθμούς καρτών. Επίσης όλες οι σελίδες του είναι κρυπτογραφημένες, πράγμα που σημαίνει πως κανένας δεν μπορεί να υποκλέψει στοιχεία.

Το **Nochex** έχει την έδρα του στο Ηνωμένο Βασίλειο και αποτελεί έναν πάροχο online πληρωμών ο οποίος επιτρέπει σε ένα website να δέχεται πληρωμές. Είναι ελεύθερο να μεταφέρει χρήματα από τον τραπεζικό λογαριασμό του χρήστη στον λογαριασμό Nochex που διαθέτει και αντίστροφα. Η βασική χρήση του γίνεται για πληρωμές σε websites και σε online δημοπρασίες.

Το Nochex παρέχει δύο τύπους λογαριασμών, τον " Seller Account " και τον " Merchant Account ". Ο πρώτος χρησιμοποιείται για συναλλαγές μέχρι £100 και ο πελάτης υποχρεώνεται να πραγματοποιεί τις πληρωμές του μόνο με αγγλικές κάρτες. Ο δεύτερος τρόπος χρησιμοποιείται για πληρωμές μεγαλύτερων ποσών και εμπεριέχει μεγαλύτερη λειτουργικότητα καθώς επιτρέπει και διεθνής συναλλαγές. Χρησιμοποιείται σε περισσότερα από 50 λογισμικά καροτσιών αγοράς συμπεριλαμβανομένου του osCommerce.

Το **PSiGate** παρέχει τα απαραίτητα εργαλεία για την διευκόλυνση των ηλεκτρονικών συναλλαγών. Χρησιμοποιείται από εμπόρους της Βόρειας Αμερικής για τους οποίους δημιουργεί εμπορικούς λογαριασμούς.

Με τη χρήση του PSiGate επιτυγχάνονται ασφαλής και αξιόπιστες συναλλαγές. Επιτρέπει στους εμπόρους τη χρήση του πρωτοκόλλου SSL καθώς είναι συμβατό με αυτό, ενώ ο πελάτης απ ΄ την πλευρά του λαμβάνει άμεσες ενημερώσεις για κάθε συναλλαγή που πραγματοποιείται από αυτόν αφού είναι δυνατή η real time επικοινωνία με τους επεξεργαστές καρτών.

Το **SECPay** χρησιμοποιείται για ασφαλής, real time, online συναλλαγές πιστωτικών και χρεωστικών καρτών. Με τη χρήση του σε ένα ηλεκτρονικό κατάστημα οι πελάτες βεβαιώνονται ότι οι ευαίσθητες πληροφορίες των πιστωτικών καρτών τους δεν κινδυνεύουν καθώς κρυπτογραφούνται κατά την διέλευση τους μέσα από το internet. Οι πληροφορίες αυτές μεταφέρονται μόνο σε μία τράπεζα η οποία πιστοποιεί την αγορά.

6. Τρωτά σημεία στην ασφάλεια των ηλεκτρονικών καταστημάτων

Η τεράστια αύξηση των διαδικτυακών συναλλαγών έχει συνοδευτεί από μια ισοδύναμη άνοδο στον αριθμό και τον τύπο των επιθέσεων ενάντια στην ασφάλεια των συστημάτων πληρωμής μέσω του διαδικτύου. Μερικές από αυτές τις επιθέσεις χρησιμοποιούν τις δημοσιοποιημένες ευπάθειες των επαναχρησιμοποιήσιμων τμημάτων που χρησιμοποιούνται από τα sites, όπως είναι το λογισμικό του καροτσιού αγορών. Άλλες επιθέσεις χρησιμοποιούν τις ευπάθειες που είναι κοινές σε οποιαδήποτε δικτυακή εφαρμογή, όπως είναι η χρήση της SQL ή η συγγραφή τμημάτων κώδικα και η παράθεση τους σε διάφορα σημεία του site. Παρακάτω αναλύονται με παραδείγματα αυτές οι ευπάθειες. Συγκεκριμένα γίνεται αναφορά στην χρήση της SQL, στην κοινοποίηση κρυφών πληροφοριών, στην κοινοποίηση κρυφών φακέλων και αρχείων, στην παραποίηση των τιμών, και στις υπερχειλίσεις των buffer.

Η επιτυχής εκμετάλλευση αυτών των ευπαθειών μπορεί να οδηγήσει σε ένα ευρύ φάσμα αποτελεσμάτων. Οι ευπάθειες της κοινοποίησης πληροφοριών και αρχείων μπορεί να ενεργήσουν καταλυτικά και να αποτελέσουν τα αρχικά στάδια που θα οδηγήσουν στην περαιτέρω εκμετάλλευση. Οι επιθέσεις στην SQL ή η παραποίηση των τιμών θα μπορούσαν να «ακρωτηριάσουν» το site, να το κάνουν να συμβιβαστεί σε χαμηλά επίπεδα εμπιστευτικότητας, και στη χειρότερη περίπτωση η επιχείρηση ηλεκτρονικού εμπορίου να καταρρεύσει.

Υπάρχουν διάφοροι λόγοι για τους οποίους οι ευπάθειες στην ασφάλεια προκύπτουν στο καρότσι αγορών και στα συστήματα πληρωμής μέσω του διαδικτύου. Οι λόγοι δεν αφορούν αποκλειστικά και μόνο αυτά τα συστήματα, αλλά οι συνέπειες τους είναι πολύ μεγαλύτερες λόγω της ευρείας έκθεσης που έχει ένα website, και λόγω της οικονομικής φύσης των συναλλαγών. Ένας από τους κύριους λόγους για τέτοιες ευπάθειες είναι το γεγονός ότι οι υπεύθυνοι για την ανάπτυξη μιας δικτυακής εφαρμογής δεν είναι συχνά πολύ καλά ενημερωμένοι για τις ασφαλείς τεχνικές προγραμματισμού. Κατά συνέπεια, η ασφάλεια της εφαρμογής δεν αποτελεί απαραιτήτως έναν από τους στόχους στην σχεδίαση. Αυτό επιδεινώνεται από τη βιασύνη για τήρηση των προθεσμιών που υπάρχουν στο γρήγορο κόσμο του ηλεκτρονικού εμπορίου. Ακόμη και η καθυστέρηση μιας ημέρας στην έκδοση ενός καινούργιου χαρακτηριστικού στο website θα μπορούσε να επιτρέψει σε έναν ανταγωνιστή να υπερβεί. Αυτό συμβαίνει συνήθως όταν τα site ηλεκτρονικού εμπορίου πρέπει να προσθέσουν γρήγορα κάποια λειτουργία για να αντεπεξέλθουν σε μια ξαφνική αλλαγή στο επιχειρησιακό περιβάλλον ή απλά για να μείνουν μπροστά από τους ανταγωνιστές. Σε τέτοιες περιπτώσεις το ζητούμενο είναι να αποκτηθεί η λειτουργία ενώ για την ασφάλεια μπορεί να φροντίσουν αργότερα. Ένας άλλος λόγος για τον οποίο εμφανίζονται ευπάθειες στην ασφάλεια είναι λόγω της έμφυτης πολυπλοκότητας των περισσότερων online συστημάτων. Σήμερα, οι χρήστες απαιτούν πολλά από τους προμηθευτές ηλεκτρονικού εμπορίου, και αυτό έχει σαν συνέπεια την δημιουργία σύνθετων σχεδιάσεων και τη χρησιμοποίηση λογικού προγραμματισμού.

Σε διάφορες περιπτώσεις, έχουμε διαπιστώσει ότι τα websites ηλεκτρονικού εμπορίου χρησιμοποιούν πιστοποιητικά SSL των 128bit ως απόδειξη ότι οι περιοχές τους είναι

καλά διασφαλισμένες. Η εμπιστοσύνη των πελατών σε αυτά έχει μειωθεί τα τελευταία χρόνια, αλλά ακόμη και τώρα υπάρχουν χιλιάδες ιστοχώροι που επιδεικνύουν τα πιστοποιητικά Verisign ή Thawte ως απόδειξη της ασφάλειάς τους.

Τα ακόλουθα τμήματα εξετάζουν τις κοινές ευπάθειες ασφάλειας που έχουν ανακαλυφθεί τόσο στο καρότσι αγορών όσο και στα συστήματα πληρωμής μέσω διαδικτύου.

6.1 SQL injection

Η SQL injection αναφέρεται στην εισαγωγή SQL μετα-χαρακτήρων στην είσοδο χρηστών, τέτοια ώστε τα ερωτήματα του επιτιθέμενου να εκτελούνται από τη βάση δεδομένων που βρίσκεται πίσω από το site. Χαρακτηριστικά, οι επιτιθέμενοι θα καθορίσουν αρχικά εάν μια περιοχή είναι τρωτή σε μια τέτοια επίθεση με την αποστολή ενός χαρακτήρα ενιαίου-αποσπάσματος ('). Τα αποτελέσματα από μια επίθεση στην SQL σε μια τρωτή περιοχή μπορούν να κυμανθούν από ένα λεπτομερές μήνυμα λάθους, το οποίο αποκαλύπτει την τεχνολογία που χρησιμοποιείται, ή επιτρέποντας στον επιτιθέμενο να έχει πρόσβαση στις μη προσβάσιμες περιοχές του website με την παραποίηση του ερωτήματος σε μια πάντα-αληθή Boolean τιμή. Ακόμα μπορεί και να επιτρέψει την εκτέλεση εντολών διαχείρισης συστημάτων.

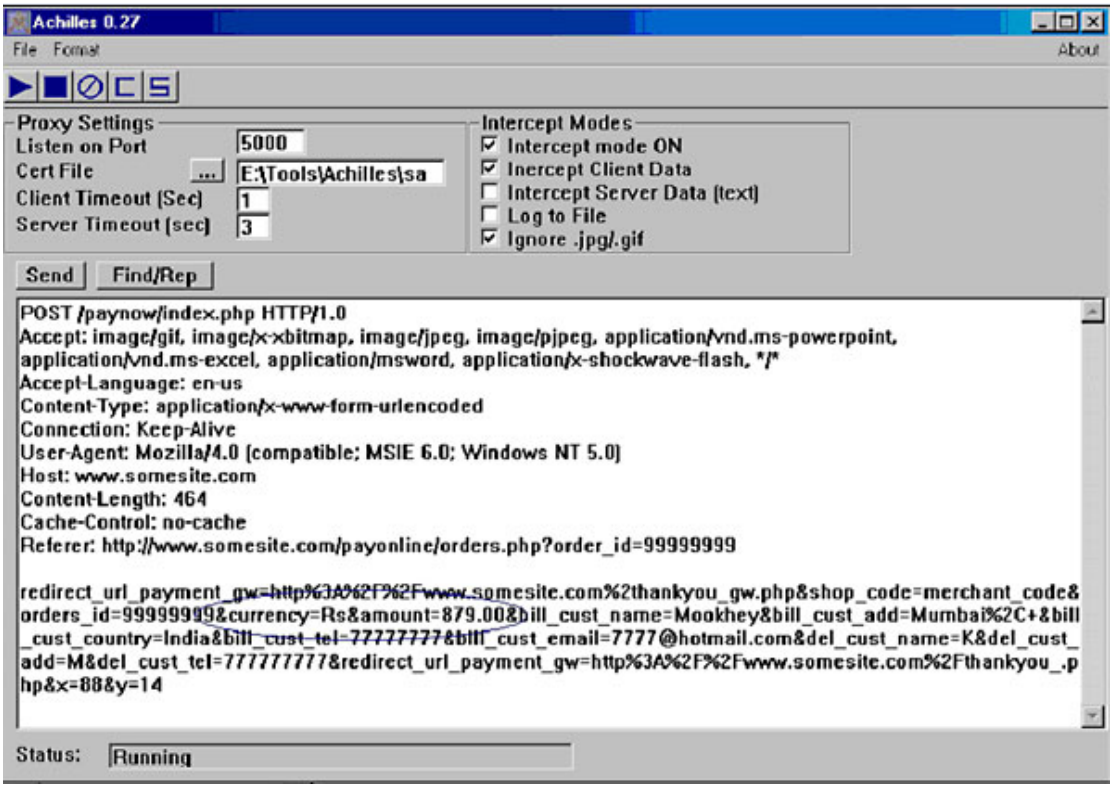
Οι τεχνικές της SQL injection διαφέρουν ανάλογα με τον τύπο της βάσης δεδομένων που χρησιμοποιείται. Παραδείγματος χάριν, η SQL injection σε μια βάση δεδομένων Oracle γίνεται πρώτιστα χρησιμοποιώντας τη λέξη κλειδί UNION και είναι δυσκολότερη απ'ό,τι στον MS SQL Server, όπου τα πολλαπλά ερωτήματα μπορούν να εκτελεσθούν με το διαχωρισμό τους με την άνω τελεία. Στις αρχικές ρυθμίσεις του, ο MS SQL Server δουλεύει με τα προνόμια των τοπικών συστημάτων και έχει την εκτεταμένη διαδικασία "xp_cmdshell", η οποία επιτρέπει την εκτέλεση εντολών διαχείρισης συστημάτων.

Τα πιο γνωστά περιστατικά αυτής της ευπάθειας ήταν στα websites ηλεκτρονικού εμπορίου της Guess.com και της PetCo.com .Ένας εικοσάχρονος προγραμματιστής στην Καλιφόρνια ανακάλυψε ότι ήταν δυνατό να αποκαλυφθούν ιδιαιτέρως ευαίσθητα στοιχεία όπως οι αριθμοί πιστωτικών καρτών, οι λεπτομέρειες συναλλαγής, κ.λπ. από αυτά τα websites καθώς και από άλλα χρησιμοποιώντας ειδικά επεξεργασμένα URLs τα οποία περιελάμβαναν SQL μετα-χαρακτήρες.

Ευπάθειες της SQL injection έχουν ανακαλυφθεί επίσης στο λογισμικό των καροτσιών αγοράς όπως στο VP-ASP Shopping Cart ,στο IGeneric Free Shopping Cart ,στο Web Merchant Services Storefront Shopping Cart κ.λπ.. Από αυτά, η ευπάθεια στο καρότσι αγορών της Storefront εμφανίστηκε στη σελίδα πρόσβασης login.asp, και θα μπορούσε ενδεχομένως να επιτρέψει στον επιτιθέμενο να εκτελέσει τα κακόβουλα ερωτήματα στις βάσεις δεδομένων, χωρίς να χρειάζεται να πιστοποιήσει την αυθεντικότητα του στο website.

6.2 Παραποίηση τιμών

Πρόκειται για μια ευπάθεια η οποία εμφανίζεται στα καρότσια αγορών και στις διαδικασίες πληρωμής. Στην πιο γνωστή μορφή αυτής της ευπάθειας, η συνολική πληρωτέα τιμή των αγαθών αποθηκεύεται σε έναν κρυμμένο πεδίο HTML μιας δυναμικά φτιαγμένης ιστοσελίδας. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει ένα πληρεξούσιο εφαρμογής δικτύου όπως το Achilles για να τροποποιήσει το πληρωτέο ποσό, καθώς οι πληροφορίες ρέουν από τον browser του χρήστη στον server του δικτύου. Παρακάτω παρουσιάζεται ένα στιγμιότυπο μιας τέτοιας ευπάθειας.

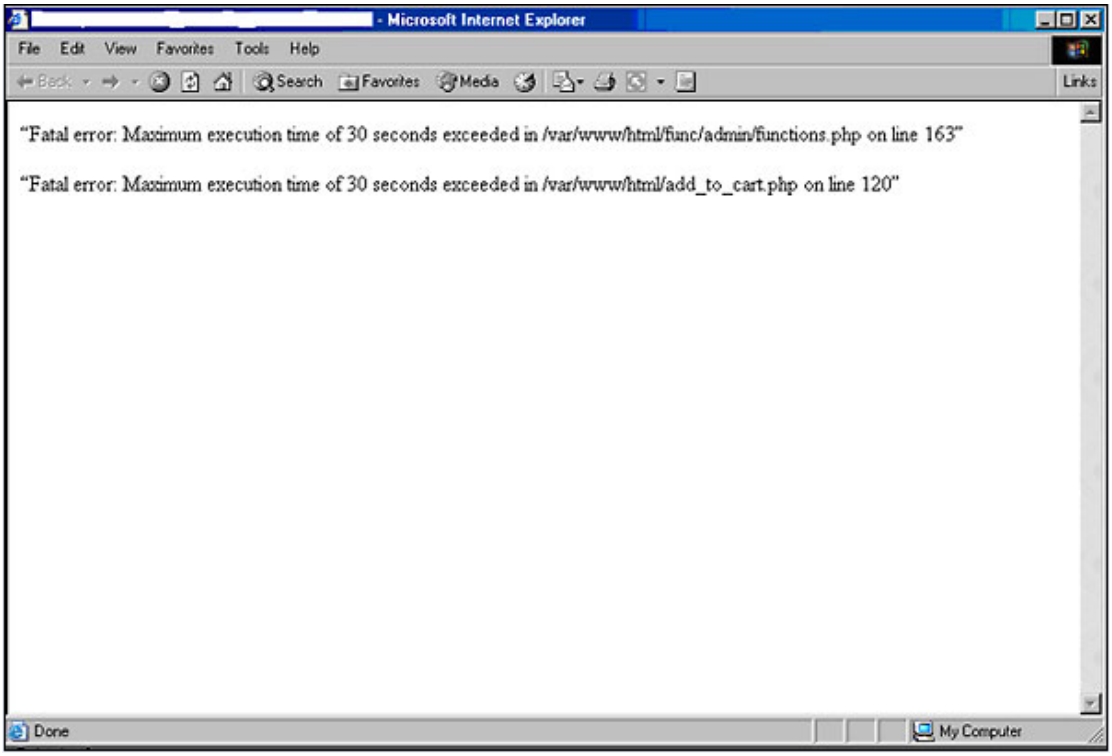


Παρατηρούμε ότι η τελική πληρωτέα τιμή (currency=Rs&amount=879.00) μπορεί να τροποποιηθεί από τον επιτιθέμενο σε μια αξία της επιλογής του. Αυτές οι πληροφορίες στέλνονται τελικά στην έξοδο πληρωμής με την οποία ο «ηλεκτρονικός» έμπορος συνεργάζεται. Εάν ο αριθμός των συναλλαγών είναι πολύ μεγάλος, η παραποίηση τιμών μπορεί να περάσει απαρατήρητη, ή μπορεί να ανακαλυφθεί πάρα πολύ αργά. Οι επαναλαμβανόμενες επιθέσεις αυτής της φύσης θα μπορούσαν ενδεχομένως να ακρωτηριάσουν τη βιωσιμότητα του «ηλεκτρονικού» εμπόρου.

Παρόμοιες ευπάθειες έχουν επίσης παρατηρηθεί σε third-party λογισμικά όπως είναι το 3D3 ShopFactory Shopping Cart, όπου η τιμή και τμήματα σχετικά με τις πληροφορίες του πελάτη αποθηκεύονται, στην μεριά του, σαν cookies, τα οποία θα μπορούσαν εύκολα να χρησιμοποιηθούν από έναν επιτιθέμενο. Ομοίως, το Smartwin Technology's CyberOffice Shopping Cart 2.0 θα μπορούσε να δεχθεί τέτοια επίθεση. Σ ’αύτη την περίπτωση γίνεται φόρτωση της φόρμας παραγγελίας τοπικά και στη συνέχεια επαναφορτώνεται στον server με τα κρυφά πεδία της φόρμας να είναι τροποποιημένα σε αυθαίρετες τιμές.

6.3 Υπερχειλίσεις Buffer

Η ευπάθεια της υπερχείλισης των Buffer δεν είναι πολύ κοινή στο καρότσι αγορών ή σε εφαρμογές που χρησιμοποιούν Perl, PHP, ASP, κ.λπ.. Εντούτοις, η αποστολή μεγάλου αριθμού bytes σε εφαρμογές δικτύου που δεν είναι σε θέση να τα χειριστούν μπορεί να έχει απροσδόκητες συνέπειες. Σε μια προσπάθεια ελέγχου όσον αφορά στην διείσδυση σε ένα site, ήταν δυνατό να αποκαλυφθεί το μονοπάτι (path) των PHP λειτουργιών που χρησιμοποιούνται, με την αποστολή μιας πολύ μεγάλη τιμής στα πεδία εισαγωγής. Όπως παρουσιάζεται στην παρακάτω εικόνα, όταν τροφοδοτήθηκαν περισσότερα από 6000 bytes σε ένα συγκεκριμένο πεδίο, ο κώδικας PHP στο πίσω μέρος ήταν ανίκανος να τα επεξεργαστεί και το λάθος που επιδείχθηκε αποκάλυψε τη θέση αυτών των λειτουργιών PHP.

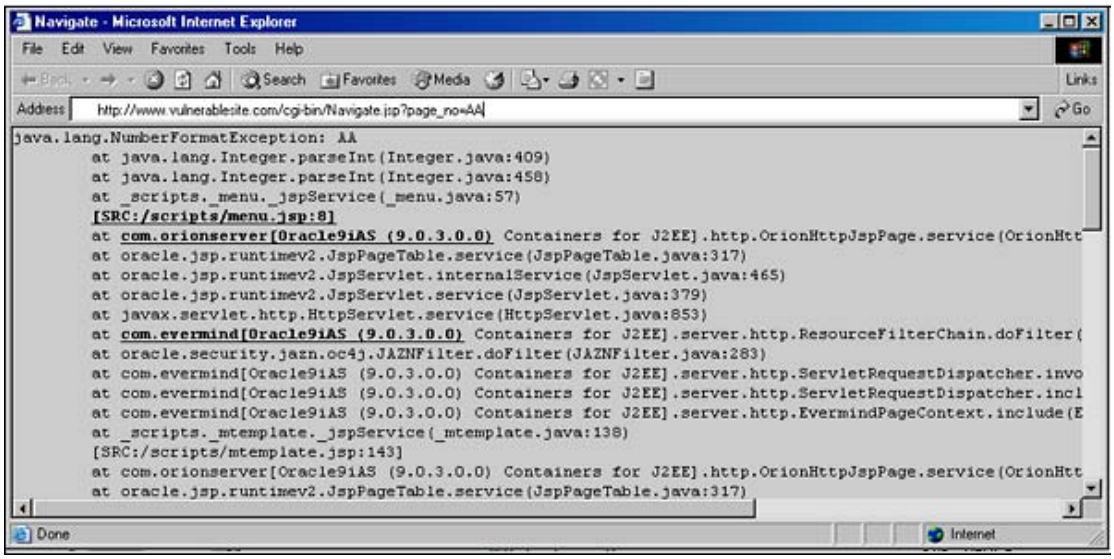


Χρησιμοποιώντας αυτές τις πληροφορίες είναι δυνατό να προσεγγιστεί ο, περιορισμένης πρόσβασης, φάκελος "admin". Από τη δομή του website και από τους υπερσυνδέσμους δεν θα έπρεπε να υπάρχει κανένας τρόπος να προσδιοριστεί ότι ο κατάλογος "admin" βρίσκεται μέσα στον φάκελο "func" κάτω από το documentroot.

Πολλαπλές υπερχειλίσεις Buffer παρουσιάστηκαν επίσης στο καρότσι αγορών PDGSoft, το οποίο επέτρεπε στον επιτιθέμενο να εκτελέσει τον κώδικα της επιλογής του με την επικάλυψη της διεύθυνσης επιστροφής που είχε αποθηκευτεί.

Οι σελίδες λάθους μπορούν να χρησιμεύσουν ως μια πολύτιμη πηγή για τις κρίσιμες πληροφορίες. Αυτά τα λάθη μπορούν να επηρεάσουν τις εφαρμογές οι οποίες δεν ακολουθούν αυστηρές αρχές για την επικύρωση των στοιχείων εισαγωγής. Παραδείγματος χάριν, μια εφαρμογή μπορεί να αποτύχει αν αναμένει αριθμητικές τιμές και της παρέχονται αλφαβητικές τιμές ή σημεία στίξης. Αυτό ακριβώς συμβαίνει παρακάτω.

Εδώ, το website ηλεκτρονικού εμπορίου χρησιμοποιεί αριθμούς για τις διάφορες σελίδες του. Οι χρήστες πλοηγούνται σ' αυτό χρησιμοποιώντας ένα link όπως είναι το http://www.vulnerablesite.com/jsp/Navigate.jsp?pageid=123. Με το χειρισμό του URL και δίνοντας την τιμή "AA" σαν pageid, προκαλείται το ακόλουθο λάθος :



Εάν παρατηρήσουμε προσεκτικά, τις τονισμένες πληροφορίες μπορούμε να διακρίνουμε ότι η έκδοση της εφαρμογής του server της Oracle είναι η Oracle 9iAS 9.0.3.0.0 καθώς επίσης και ορισμένα τμήματα που χρησιμοποιούνται από την εφαρμογή, όπως είναι ο Orion Application server. Αποκαλύπτεται επίσης το μονοπάτι όπου βρίσκονται κάποια, ενδεχομένως τρωτά, .jsp αρχεία (/scripts/menu.jsp).

6.4 Cross-site Scripting

Η επίθεση Cross-site Scripting (XXS) στρέφεται πρώτιστα ενάντια στον τελικό χρήστη και εκμεταλλεύεται δύο παράγοντες:

1. την έλλειψη επικύρωσης εισόδου και εξόδου που γίνεται από την εφαρμογή δικτύου
2. την εμπιστοσύνη που δείχνει ο τελικός χρήστης σε ένα URL που φέρνει το ευάλωτο όνομα του website.

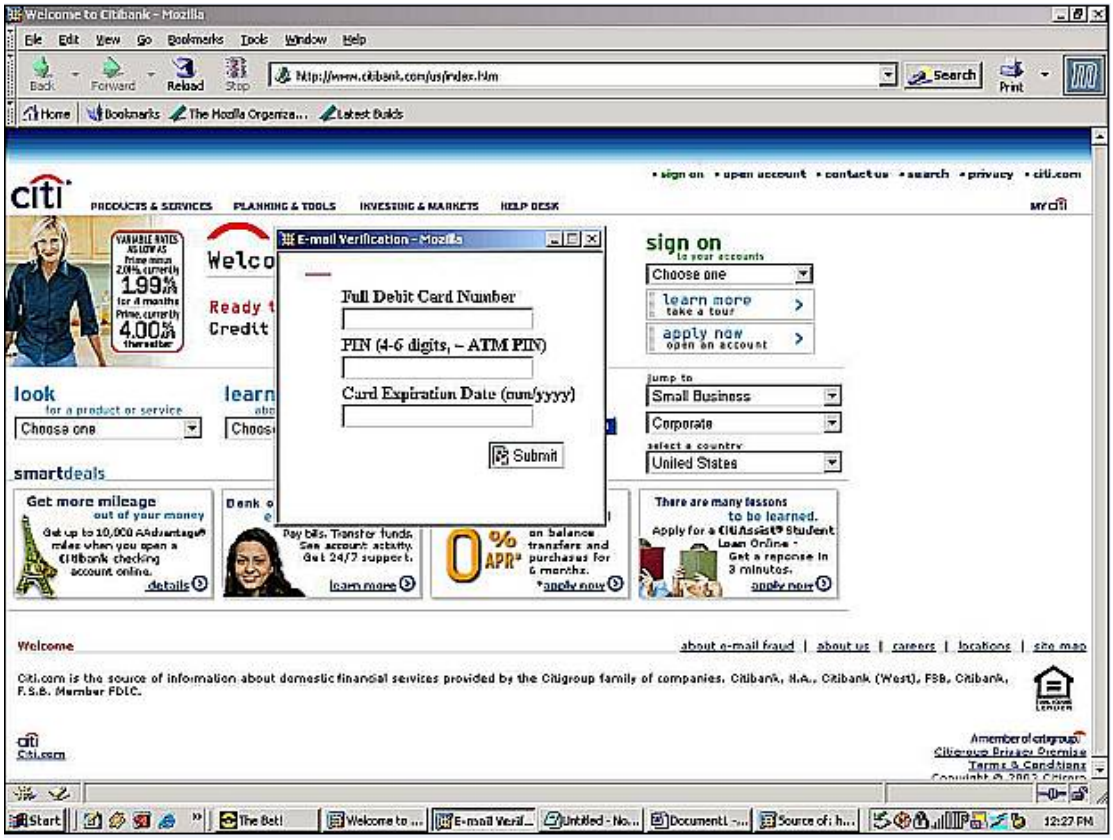
Απαιτείται μια φόρμα η οποία παίρνει τις εισόδους των χρηστών, τις επεξεργάζεται, και εμφανίζει τα αποτελέσματα σε μία ιστοσελίδα, η οποία περιέχει και την αρχική είσοδο τους. Παρατηρείται συνήθως στις εφαρμογές " αναζήτησης ", όπου η λογική αναζήτησης θα εμφανίσει τα αποτελέσματα με μια γραμμή όπως " αποτελέσματα για < user_supplied_input >". Σε αυτήν την περίπτωση, εάν η είσοδος χρηστών εμφανίζεται χωρίς να έχει αναλυθεί, τότε ένας επιτιθέμενος μπορεί να ενσωματώσει τμήματα JavaScript παρουσιάζοντας τα ως τμήματα της εισόδου. Με την δεξιοτεχνία που μπορεί να έχει ένα τέτοιο URL, που περιέχει αυτό το JavaScript, ένα θύμα μπορεί να κάνει κλικ πάνω του και έτσι αυτό να εκτελεσθεί στο σύστημα του θύματος. Μια χαρακτηριστική XSS επίθεση URL θα έμοιαζε με αυτό:

http://www.vulnerablesite.com/cgibin/search.php?keywords=<script>alert("OK")<script>.

Σε αυτήν την περίπτωση, όταν το θύμα κάνει κλικ σε αυτήν την σύνδεση, ένα παράθυρο μηνυμάτων με το κείμενο "OK" θα ανοίξει στο σύστημά του.

Στις περισσότερες περιπτώσεις, ο επιτιθέμενος επεξεργάζεται το URL προκειμένου να κλέψει τα cookies του χρήστη, τα οποία πιθανώς να περιέχουν την ταυτότητα του χρήστη και άλλες ευαίσθητες πληροφορίες. Το JavaScript θα μπορούσε επίσης να τροποποιηθεί έτσι ώστε να προσανατολίσει το χρήστη στο website του επιτιθεμένου, όπου μπορεί να εκτελεστεί κάποιος κακόβουλος κώδικας χρησιμοποιώντας ActiveX controls ή με την εκμετάλλευση των ευπαθειών που έχουν κάποιοι browser όπως ο Internet Explorer ή ο Netscape Navigator.

Επίσης, το JavaScript μπορεί να χρησιμοποιηθεί για να προσανατολίσει το χρήστη σε μια περιοχή που φαίνεται παρόμοια με τον αρχικό website και ζητά από το χρήστη να εισάγει ευαίσθητες πληροφορίες όπως είναι οι λεπτομέρειες επικύρωσής του για εκείνο το website, ή τους αριθμούς πιστωτικών καρτών του. Μια σχετική περίπτωση παρουσιάζεται παρακάτω:



Σε αυτήν την περίπτωση, ο επιτιθέμενος έχει ανοίξει δύο παράθυρα στο σύστημα του θύματος. Αυτό στο υπόβαθρο είναι το αρχικό website της Citibank, ενώ το επάνω παράθυρο ζητά από τον χρήστη να εισάγει τον αριθμό των πιστωτικών καρτών του, τον κωδικό, και την ημερομηνία λήξης καρτών. Όταν πατηθεί το κουμπί “submit”, αυτές οι πληροφορίες στέλνονται στον server του επιτιθεμένου. Αυτού του είδους η επίθεση αποκαλείται "phishing" και γίνεται με την αποστολή ενός ηλεκτρονικού

μηνύματος που υποστηρίζει ότι προέρχεται από την Citibank και ζητάει από τους χρήστες να επικυρώσουν τις λεπτομέρειές τους. Το link που εμφανίζει αυτό το ηλεκτρονικό μήνυμα μοιάζει κάπως έτσι :

http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.pIsEm.NeT/3/?3X6C MW2I2uPOVQW.

Οι περισσότεροι χρήστες δεν γνωρίζουν ότι σύμφωνα με τους κανόνες του HTTP, αυτό το link θα οδηγήσει στο **sd96v.pisem.net**, και όχι στο **www.citibank.com**. Παρόμοιες επιθέσεις μπορούν να πραγματοποιηθούν εάν η εφαρμογή δικτύου περιλαμβάνει κάποια τμήματα που προσανατολίζουν τους χρήστες σε άλλα μέρη του site, ή σε άλλα σχετικά site. Παραδείγματος χάριν, σε μια εφαρμογή παρατηρήθηκε ότι υπάρχει ένα τμήμα το οποίο χρησιμοποιείται για να στείλει το χρήστη στα δυναμικά δημιουργημένα μέρη του site:

http://www.vulnerablesite.com/cgibin/redirect.php?url=some_dynamic_value.

Λόγω της έλλειψης συνειδητοποίησης σε θέματα ασφάλειας, οι υπεύθυνοι για την ανάπτυξη ιστοσελίδων, δεν συνειδητοποίησαν ότι ένας επιτιθέμενος θα μπορούσε να επεξεργαστεί ένα URL κάπως έτσι:

http://www.vulnerablesite.com/cgibin/redirect.php?url=www.attackersite.com

και να το στείλει σε ένα θύμα. Αυτό το URL μπορεί να τροποποιηθεί εύκολα κωδικοποιώντας εξαδικά το τμήμα που ακολουθεί το 'url=' ή μετατρέποντας την IP διεύθυνση του επιτιθέμενου σε δεκαεξαδική ή οκταδική τιμή. Παραδείγματος χάριν, αν η IP διεύθυνση του επιτιθέμενου είναι 192.168.0.1, το URL θα μπορούσε να επεξεργαστεί και να γίνει:

http://www.vulnerablesite.com/cgibin/redirect.php?url=http://7934518627/

6.5 Απομακρυσμένη εκτέλεση εντολών

Οι πιο καταστρεπτικές ευπάθειες στις εφαρμογές διαδικτύου εμφανίζονται όταν το script του CGI επιτρέπει σε έναν επιτιθέμενο να εκτελέσει εντολές διαχείρισης συστημάτων λόγω της ανεπαρκούς επικύρωσης εισόδου. Αυτό συμβαίνει περισσότερο όταν γίνεται " κλήση συστήματος " στα script των Perl και PHP. Χρησιμοποιώντας έναν διαχωριστή εντολών και άλλους shell μεταχαρακτήρες, είναι δυνατό για τον επιτιθέμενο να εκτελέσει τις εντολές με τα προνόμια που έχει ένας server. Παραδείγματος χάριν, το καρότσι αγορών της Hassan Consulting επέτρεψε την απομακρυσμένη εκτέλεση εντολών, επειδή οι shell μεταχαρακτήρες όπως είναι οι | και & δεν απορρίφθηκαν από το λογισμικό. Ωστόσο, η περιήγηση στους καταλόγους (directories) δεν ήταν δυνατή σε αυτό το λογισμικό.

Σε μια άλλη περίπτωση, το καρότσι αγορών Pacific Software's Carello είχε ένα ευάλωτο DLL το οποίο επέτρεπε την εκτέλεση απομακρυσμένων εντολών λόγω των επιθέσεων περιήγησης στους καταλόγους, οι οποίες θα μπορούσαν να πραγματοποιηθούν χρησιμοποιώντας ένα ειδικά επεξεργασμένο URL.

6.6 Αδυναμία στην επικύρωση και στην έγκριση

Οι μηχανισμοί επικύρωσης που δεν απαγορεύουν τα πολλαπλά αποτυχημένα logins μπορούν να δεχθούν επίθεση με τη χρήση εργαλείων όπως είναι το Brutus. Ομοίως, εάν το site χρησιμοποιεί τη βασική επικύρωση HTTP ή δεν περνά session IDs πάνω από το SSL (Secure Sockets Layer), τότε ένας επιτιθέμενος μπορεί να εισχωρήσει στην κυκλοφορία για να ανακαλύψει τα πιστοποιητικά επικύρωσης ή και έγκρισης του χρήστη.

Δεδομένου ότι το HTTP είναι ένα πρωτόκολλο που δεν περιορίζεται σε κάποιο κράτος, οι εφαρμογές διατηρούν συνήθως κάποιο περιορισμό στα κράτη χρησιμοποιώντας session IDs ή IDs συναλλαγών τα οποία αποθηκεύονται σε cookies στο σύστημα του χρήστη. Κατά συνέπεια η session ID γίνεται ο μόνος τρόπος με τον οποίο μία εφαρμογή μπορεί να καθορίσει την ταυτότητα του χρήστη. Εάν η session ID κλαπεί (π.χ μέσω XSS), ή μπορεί να προβλεφθεί, τότε ένας επιτιθέμενος μπορεί να μάθει την γνήσια ταυτότητα του χρήστη. Σε περίπτωση που ο αλγόριθμος που χρησιμοποιείται για να παράγει session IDs είναι αδύνατος, είναι πολύ εύκολο να γραφτεί ένα Perl script για να απαριθμήσει τα sessionIDs μέσα στο πιθανό διάστημα και να εισχωρήσει στα σχέδια επικύρωσης και έγκρισης της εφαρμογής.

Σε μία παρόμοια περίπτωση ανακαλύφθηκε ότι η ταυτότητα της παραγγελίας (order ID) για τις συναλλαγές των χρηστών δεν παράγεται τυχαία, έτσι είναι δυνατό να υπάρχει πρόσβαση στις παραγγελίες άλλων χρηστών απλά με το γράψιμο ενός τμήματος Perl το οποίο απαριθμεί όλες τις πιθανές order IDs μέσα σε ένα δοσμένο φάσμα. Αξιοπρόσεχτο είναι το γεγονός ότι αν και μία εφαρμογή μπορεί να έχει τους μηχανισμούς για να αποτρέψει έναν χρήστη από τις πολλαπλές προσπάθειες εισόδου του κωδικού πρόσβασης κατά τη διάρκεια της επικύρωσης, δεν μπορούν να αποτρέψουν συνήθως έναν χρήστη από το να προσπαθήσει να κλέψει τις sessions IDs με την εκ νέου διαμόρφωση των URLs.

Οι ευπάθειες που συζητούνται παραπάνω δεν αφορούν αποκλειστικά και μόνο τα καρότσια αγορών ή τα συστήματα πληρωμής μέσω διαδικτύου. Θα μπορούσαν να παρουσιαστούν και σε άλλους τύπους δικτυακών εφαρμογών. Εντούτοις, στην περίπτωση των συστημάτων ηλεκτρονικού εμπορίου, οι ευπάθειες αποκτούν μια πιο σοβαρή διάσταση λόγω της οικονομικής φύσης των συναλλαγών. Αυτό που βρίσκεται σε κίνδυνο δεν είναι μόνο μια άμεση απώλεια εισοδημάτων, αλλά οι επιχειρήσεις μπορεί επίσης να αντιμετωπίσουν σοβαρές απώλειες και στη φήμη τους. Σε μερικές περιπτώσεις, μπορεί να βρεθούν αντιμέτωποι με τις νομικές ποινικές ρήτρες για την παραβίαση της ιδιωτικότητας ή της εμπιστοσύνης των πελατών, όπως συνέβη στην περίπτωση των Guess.com και PetCo.com. Είναι ύψιστης σημασίας για τους σχεδιαστές και τους υπεύθυνους ανάπτυξης των διαδικτυακών εφαρμογών να θεωρηθεί η ασφάλεια ως βασικός στόχος της σχεδίασης και να ακολουθηθούν ασφαλείς τρόποι κωδικοποίησης προκειμένου να παρασχεθούν υψηλά επίπεδα διασφάλισης των πελατών τους .

7. Τρωτά σημεία στην ασφάλεια του osCommerce

Το osCommerce έχει παρατηρηθεί ότι είναι ευάλωτο σε κάποιες από τις ευπάθειες που αναφέρθηκαν στην προηγούμενη ενότητα. Συγκεκριμένα αποδείχθηκε ότι οι επιτιθέμενοι μπορούν να υποκλέψουν τις ευαίσθητες πληροφορίες, που βρίσκονται αποθηκευμένες στην βάση δεδομένων του site, εκμεταλλευόμενοι τις SQL injections. Επίσης είναι ευάλωτο σε επιθέσεις cross-site-scripting ενώ η απομακρυσμένη εκτέλεση εντολών βοηθάει τον επιτιθέμενο να περιηγηθεί στους καταλόγους του ηλεκτρονικού καταστήματος. Παρακάτω περιγράφεται ποια είναι η διάσταση αυτών των ευπαθειών στο osCommerce, αν υπάρχουν τρόποι για την αντιμετώπιση τους και ποιοι είναι αυτοί.

7.1 SQL injection στο osCommerce

Αυτή η ευπάθεια επιτρέπει σε κάποιον επιτιθέμενο να εκτελέσει ερωτήματα SQL και να παρεμποδίσει την νόμιμη εξυπηρέτηση των πελατών. Εμφανίστηκε λόγω του ότι πολλοί τύποι μεταβλητών δεν είχαν ελεγχθεί κατά την αρχική σχεδίαση.

Στην πιο απλή μορφή αυτής της ευπάθειας, το osCommerce αδυνατεί να επικυρώσει τις εισόδους ενός νέου χρήστη καθιστώντας το site ευάλωτο. Τα αρχεία που ευθύνονται γι΄ αυτό είναι το "create_account_process.php" και το "account_edit_process.php". Το πρόβλημα δημιουργείται λόγω του ότι η μεταβλητή **country** δεν είναι σωστά επικυρωμένη. Έτσι αυτό που έχει να κάνει ένας επιτιθέμενος είναι να αποθηκεύσει τη φόρμα εισαγωγής νέου χρήστη, στη συνέχεια να επέμβει στο πεδίο country και να εισάγει SQL ερωτήματα. Με αυτόν τον τρόπο μπορεί να τροποποιήσει τα δεδομένα στην βάση ή να έχει πρόσβαση ακόμα και στον host. Οι συναρτήσεις που εμπλέκονται στις εκτελέσεις αυτών των ερωτημάτων ορίζονται στο αρχείο "general.php" και είναι η tep_get_zone_name() και η tep_get_countries().

Παρόμοια προβλήματα δημιουργούνται και από την λάθος επικύρωση της μεταβλητής **product_id**. Σε αυτή την περίπτωση το αρχείο που ευθύνεται είναι το "includes/modules/additional_images.php" καθώς δεν φιλτράρει κατάλληλα τις παραμέτρους αυτής της μεταβλητής. Σαν αποτέλεσμα δημιουργείται σφάλμα στην επικύρωση της εισόδου το οποίο μπορεί να επιτρέψει την εκτέλεση SQL εντολών. Οι συνέπειες αυτού του λάθους εμφανίζονται και κατά την πρόσθεση ενός προϊόντος στο καλάθι αγοράς.

Σε μία ακόμα μορφή αυτής της ευπάθειας, ο επιτιθέμενος στέλνει σε ένα χρήστη ένα ειδικά επεξεργασμένο URL το οποίο απαγορεύει την νόμιμη είσοδο στον λογαριασμό του. Παρακάτω παρουσιάζεται ένα τέτοιο URL και γίνεται επεξήγηση των παραμέτρων του.

/default.php?cPath=[MID]&sort=5a&page=1&action=buy_now&products_id=[PID][JNK]

Το [MID] είναι ένας έγκυρος αριθμός ταυτότητας κατασκευαστή, το [PID] είναι ένας έγκυρος αριθμός προϊόντος και το [JNK] είναι ερώτημα SQL. Αν αντί για SQL βάλουμε π.χ. %00 αυτό θα προσθέσει ένα προϊόν στο καρότσι αγοράς το οποίο δεν γίνεται να μετακινηθεί. Ο μόνος τρόπος για να διαγραφεί είναι να γίνει μετατροπή τη βάσης από τον administrator.

Αν ο χρήστης κάνει log out και στη συνέχεια ξανακάνει log in τότε εμφανίζεται το παρακάτω λάθος:

1064-You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '[Problem_Here]' and pd.products_id=p.products_id and p.langu select p.products_id, pd.products_name, p.products_model,p.products_price,p.products_weight, p.products_tax_class_id from products p, products_description pd where p.products_id='79'[Problem_Here]' and pd.products_id= p.products_id and pd.language_id= '1'.

Ακόμα κι αν ο χρήστης καταφέρει να εισέλθει στην σελίδα αγοράς, δεν είναι σε θέση να αγοράσει οποιοδήποτε προϊόν ή να δει το καρότσι του. Ο επιτιθέμενος μπορεί όμως να εισέλθει στη βάση ακόμα και να εκτελέσει SQL ερωτήματα γι΄ αυτούς.

Το πρόβλημα αυτό εμφανίζεται στην πρώτη έκδοση του osCommerce και δεν υπάρχει τρόπος να αντιμετωπιστεί. Στην δεύτερη έκδοση δεν μπορεί να αποφευχθεί η είσοδος ενός αμετακίνητου προϊόντος αλλά, κάποιος ειδικός σε τέτοιου είδους επιθέσεις, είναι δυνατό να το διαγράψει από τον πίνακα 'customers_basket'. Ωστόσο, η εκτέλεση SQL ερωτημάτων δεν γίνεται να αποτραπεί. Για όλα τα υπόλοιπα προβλήματα η λύση βρίσκεται σε ένα αναβαθμισμένο πακέτο της πρώτης έκδοσης ενώ στην δεύτερη έκδοση δεν εμφανίζονται εξ΄ αρχής.

7.2 Cross Site Scripting (XXS) στο osCommerce

Το oscommerce βρέθηκε ευάλωτο και στην ευπάθεια του XXS επιτρέποντας στον επιτιθέμενο να δημιουργήσει επικίνδυνους URL συνδέσμους οι οποίοι περιλαμβάνουν εχθρικό κώδικα html. Αν αυτοί οι σύνδεσμοι ακολουθηθούν ο εχθρικός κώδικας εγκαθίσταται στον browser του θύματος. Αυτό συμβαίνει συνήθως στο τμήμα του web site που αφορά την ασφάλεια και αφήνει τον επιτιθέμενο να κλέψει τις πληροφορίες που βρίσκονται αποθηκευμένες στα cookies. Με αυτόν τον τρόπο γίνονται επιθέσεις στους λογαριασμούς των χρηστών. Το πρόβλημα αυτό προκύπτει από το γεγονός ότι πολλές μεταβλητές δεν επικυρώνονται σωστά πριν επιστραφούν στους χρήστες.

Ένα αρχείο, που επιτρέπει την ανάπτυξη του XXS, φαίνεται να είναι το "contact_us.php" το οποίο δεν ελέγχει σωστά την μεταβλητή **enquiry** πριν αυτή επιστραφεί στο χρήστη, με αποτέλεσμα την εκτέλεση κακόβουλου κώδικα στον browser του χρήστη. Παρακάτω παρουσιάζεται ένας σύνδεσμος ο οποίος εκμεταλλεύεται αυτή την ευπάθεια.

http://www.victimsite.com/contact_us.php?&name=1&email=1&enquiry=%3C/textarea%3E%3Cscript%3Ealert('w00t');%3C/script%3E

Αν ακολουθηθεί αυτός ο σύνδεσμος, το αποτέλεσμα θα είναι η εμφάνιση ενός pop up κουτιού.

Πολλά είναι επίσης τα αρχεία που εκτίθενται από την λανθασμένη επικύρωση των παραμέτρων **page**, **zpage** και **zone** και στα οποία είναι εμφανείς οι συνέπειες από την εκτέλεση εχθρικού κώδικα, στη μεριά του administrator. Τα αρχεία αυτά αναφέρονται παρακάτω.

admin/banner_manager.php
admin/banner_statistics.php
admin/countries.php
admin/currencies.php
admin/languages.php
admin/manufacturers.php
admin/newsletters.php
admin/orders_status.php
admin/products_attributes.php
admin/products_expected.php
admin/reviews.php
admin/specials.php
admin/stats_products_purchased.php
admin/stats_products_viewed.php
admin/tax_classes.php
admin/tax_rates.php
admin/zones.php

Παρόμοια προβλήματα δημιουργούνται και από τις μεταβλητές **gID** στο αρχείο "configuration.php", **set** και **module** στο "modules.php",**option_order_by**, **value_page** και **option_page** στο "products_attributes.php", **lID** στο "languages.php", **cID** και **selected_box** στο "customers.php" και **spage**, **zID** και **sID** στο "geo_zones.php".

Η επίθεση XXS έχει παρατηρηθεί τόσο στην πρώτη όσο και στην δεύτερη έκδοση του osCommerce. Για την αντιμετώπιση αυτών των επιθέσεων έχει εκδοθεί ένα CVS το οποίο είναι αποτελεσματικό στις περισσότερες περιπτώσεις. Για μεγαλύτερη ασφάλεια ο χρήστης πρέπει να ελέγχει τον κώδικα για να διαβεβαιώνεται ότι οι είσοδοι είναι κατάλληλα επικυρωμένες, ενώ δεν θα πρέπει να ακολουθούνται σύνδεσμοι που προέρχονται από μη έμπιστες πηγές.

7.3 Απομακρυσμένη εκτέλεση εντολών στο osCommerce

Η απομακρυσμένη εκτέλεση εντολών αποτελεί την πιο σημαντική ευπάθεια του osCommerce, καθώς τα αποτελέσματα που προκύπτουν από την εκμετάλλευση της μπορεί να είναι καταστρεπτικά για αυτό. Στην χειρότερη μορφή της δίνει τη δυνατότητα στον επιτιθέμενο, να αποκτήσει ίδια δικαιώματα με αυτά που έχει ένας administrator.

Αυτή η ευπάθεια τις περισσότερες φορές προκύπτει από σφάλματα στην επικύρωση της εισόδου των χρηστών. Χαρακτηριστικό παράδειγμα αποτελεί η αδυναμία του αρχείου "templates_boxes_layout.php" να επικυρώσει την παράμετρο **filter_template**.Το αποτέλεσμα είναι ότι επιτρέπεται στον επιτιθέμενο να επέμβει στο περιεχόμενο των τοπικών αρχείων με τα δικαιώματα ενός web server.

Σε μία ακόμα περίπτωση είναι δυνατή η πρόσβαση στα αρχεία αυτά. Αυτή τη φορά το λάθος στην επικύρωση εισόδου εμφανίζεται στο αρχείο "file_manager.php". Χρησιμοποιώντας των χαρακτήρα "../" στην παράμετρο **filename** είναι δυνατή η προσπέλαση των καταλόγων.

Ένας ακόμα τρόπος για την εκμετάλλευση αυτής της ευπάθειας είναι η εισαγωγή μη έγκυρων τιμών σε ορισμένες παραμέτρους. Αυτό συμβαίνει και στην παράμετρο **in_login** στην οποία αν εισάγουμε οποιαδήποτε μη μηδενική τιμή είναι δυνατή η πρόσβαση σε όλα τα αρχεία του καταλόγου admin.

Το παραπάνω πρόβλημα εμφανίζεται στην δεύτερη έκδοση του osCommerce αλλά είναι πολύ πιθανό να έχει επηρεάσει κι άλλες εκδόσεις. Αυτό που συνιστάται για την εξυγίανση του είναι ο περιορισμός στην πρόσβαση του καταλόγου "admin" χρησιμοποιώντας .htaccess ή κάποια παρόμοια μέθοδο.

8. Βασικές τεχνικές για την διασφάλιση ενός ηλεκτρονικού καταστήματος

Το ηλεκτρονικό εμπόριο σήμερα είναι μία αναγκαία στρατηγική για τους περισσότερο ανταγωνιστικούς οργανισμούς. Αποτελεί το κλειδί για την εύρεση νέων πηγών εισοδήματος, την επέκταση σε νέες αγορές και τη μείωση των δαπανών.

Ωστόσο οι κίνδυνοι που προκύπτουν από το ηλεκτρονικό εμπόριο φαίνονται μερικές φορές σχεδόν τόσο μεγάλοι όσο και οι απολαβές από αυτό. Η υποδομή που υποστηρίζει το ηλεκτρονικό εμπόριο μπορεί να είναι ευάλωτη στην κατάχρηση, την κακή χρήση, και την αποτυχία, προκαλώντας έναν αριθμό επιχειρησιακών προβλημάτων. Αυτά συμπεριλαμβάνουν τις οικονομικές απώλειες λόγω απάτης, χαμένες ευκαιρίες λόγω της διάσπασης των υπηρεσιών, την κακή φήμη για την υπηρεσία, και την απώλειας της εμπιστοσύνης των πελατών. Οι εκτιμήσεις για την επέκταση της ηλεκτρονικής απάτης ποικίλουν.

Παραδείγματος χάριν:

- Η κλοπή online πληροφοριών, συμπεριλαμβανομένου του πειρατικού λογισμικού, οι κλεμμένοι αριθμοί πιστωτικών καρτών, και η πρόσβαση σε εταιρικά μυστικά, υπολογίζεται ότι μόνο στις ΗΠΑ κοστίζει περισσότερο από 10 δισεκατομμύρια δολάρια ετησίως.
- Τα τελευταία δύο χρόνια, σχεδόν οι μισοί οργανισμοί δέχονται τις συνέπειες που απορρέουν από τις οικονομικές απώλειες λόγω της έλλειψης ασφάλειας.
- Η απάτη στις πιστωτικές κάρτες υπολογίζεται ότι είναι 5 δισεκατομμύρια δολάρια ετησίως.

Είναι σαφές ότι οι επιχειρήσεις που σχετίζονται με το ηλεκτρονικό εμπόριο πρέπει να προστατευθούν αλλά δεν είναι πάντα σαφές πώς πρέπει να το κάνουν.
Τα μέτρα ηλεκτρονικής ασφάλειας στοχεύουν στην επίτευξη τεσσάρων θεμελιωδών στόχων:

- Βεβαίωση ότι μόνο τα εξουσιοδοτημένα άτομα έχουν πρόσβαση στις πληροφορίες
- Παρεμπόδιση της ανεπίτρεπτης δημιουργίας, αλλαγής, ή καταστροφής των δεδομένων
- Εξασφάλιση ότι οι νόμιμοι χρήστες θα έχουν πρόσβαση στις πληροφορίες
- Διασφάλιση ότι οι πόροι χρησιμοποιούνται με νόμιμους τρόπους

Οι αρχικές απολαβές από την επίτευξη των παραπάνω στόχων αφορούν την *ασφάλεια επικοινωνιών* και *την ασφάλεια υπολογιστών*. Η πρώτη αναφέρεται στην προστασία των πληροφοριών ενώ μεταφέρονται από ένα σύστημα σε ένα άλλο ενώ η δεύτερη αναφέρεται στην προστασία των πληροφοριών μέσα σε ένα σύστημα ηλεκτρονικού υπολογιστή. Αυτά τα αποτελέσματα πρέπει να λειτουργήσουν μαζί με άλλα μέτρα ασφάλειας, τα οποία περιλαμβάνουν:

- *Φυσική ασφάλεια*, όπως οι κλειδαριές στις πόρτες, η βιομετρική κ.α.
- *Ασφάλεια προσωπικού*, όπως η διαλογή υπαλλήλων
- *Administrative ασφάλεια*, όπως η έρευνα για παραβιάσεις στην ασφάλεια
- *Ασφάλεια πληροφοριών / δεδομένων*, όπως ο έλεγχος της αναπαραγωγής τους
- *Online ασφάλεια*, ή έλεγχος πρόσβασης στα online δεδομένα

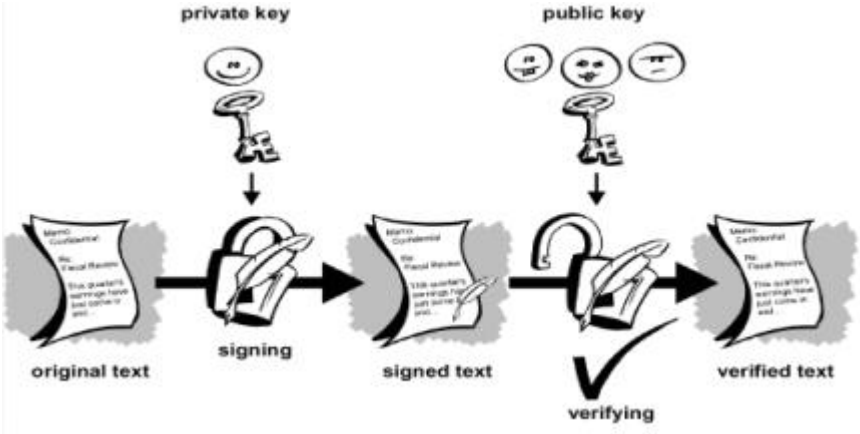
Στο σχεδιασμό μιας κατάλληλης υποδομής ασφάλειας για το ηλεκτρονικό εμπόριο, είναι σημαντικό να μην αγνοηθεί κανένα από τα παραπάνω μέτρα ασφάλειας λαμβάνοντας υπόψη τις επικοινωνίες και τις επιλογές ασφάλειας των υπολογιστών.

Παρακάτω γίνεται μία περιγραφή των βασικών τεχνολογιών ασφάλειας έτσι ώστε να αξιολογηθούν οι διάφορες εναλλακτικές λύσεις που υπάρχουν για τη δημιουργία μιας ασφαλούς υποδομής για το ηλεκτρονικό εμπόριο.

8.1 Ψηφιακές υπογραφές

Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής ψηφιακής υπογραφής (digital signature). Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι.

Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί. Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να επιβεβαιώσει ότι το μήνυμα υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί. Εφόσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, μόνο αυτός θα μπορούσε να το χρησιμοποιήσει, για να υπογράψει κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό.



Πιο αναλυτικά, πρώτο βήμα για την δημιουργία της ψηφιακής υπογραφής είναι η παραγωγή μιας σύνοψης μηνύματος (message digest). Για το σκοπό αυτό, το λογισμικό που παράγει τις υπογραφές χρησιμοποιεί μία συνάρτηση κατακερματισμού (hash function). Η συνάρτηση αυτή αντιστοιχεί σε κάθε μήνυμα μία μοναδική ακολουθία χαρακτήρων, που ονομάζεται σύνοψη του μηνύματος και έχει σταθερό μήκος, ανεξάρτητα από το μήκος του μηνύματος. Η σύνοψη, κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα, αποτελεί την υπογραφή, η οποία επισυνάπτεται στο μήνυμα.

Ο παραλήπτης λαμβάνει τόσο το μήνυμα όσο και την υπογραφή. Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την υπογραφή, οπότε προκύπτει η σύνοψη του μηνύματος, όπως αυτή είχε παραχθεί πριν την αποστολή του μηνύματος. Εφόσον η υπογραφή έχει παραχθεί με το ιδιωτικό κλειδί του αποστολέα, μόνο το δημόσιο κλειδί του μπορεί να την αποκρυπτογραφήσει και να δώσει τη σύνοψη του μηνύματος. Η συνάρτηση κατακερματισμού χρησιμοποιείται για να παραχθεί μία σύνοψη του μηνύματος, όπως αυτό έχει φτάσει στα χέρια του παραλήπτη. Εφόσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά την αποστολή του, η σύνοψη του μηνύματος θα είναι ίδια με αυτήν που είχε προκύψει κατά την υπογραφή του από τον αποστολέα. Με τον τρόπο αυτό, ο παραλήπτης βεβαιώνει την αυθεντικότητα του μηνύματος.

8.2 Ψηφιακά πιστοποιητικά

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

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

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.

- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται ευρέως για διάφορες κρυπτογραφημένες ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Παραδείγματα τέτοιων συναλλαγών είναι: Σύνοδοι με βάση το πρωτόκολλο SSL (Client/Server SSL Certificates), κρυπτογραφημένο και υπογεγραμμένο ηλεκτρονικό ταχυδρομείο (S/MIME Certificates), υπογραφή αντικειμένων (Object-signing Certificates) κοκ.

8.2.1 Το πρότυπο X.509

Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509. Είναι ένα πρότυπο κρυπτογράφησης το οποίο σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP). Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

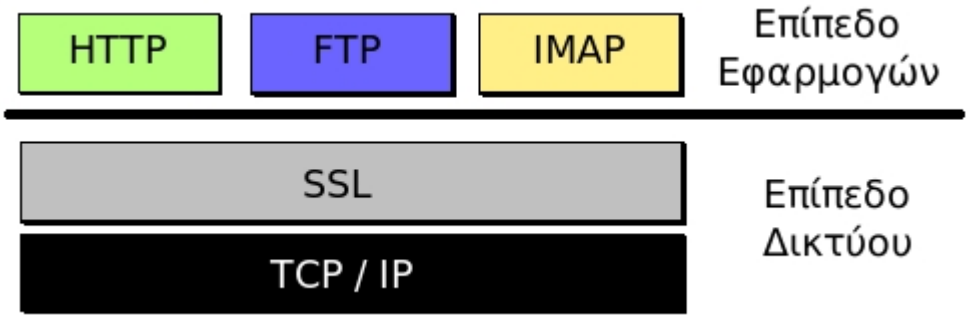
Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών. Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε browsers, servers και προγράμματα λογισμικού, για τη διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server/clients) κτλ., από πολλές γνωστές εταιρίες ανάπτυξης λογισμικού.

8.3 Secure Sockets Layer (SSL)

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

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

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



Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

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

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

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημόσιου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημόσιου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.

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

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

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

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

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

8.4 Secure HTTP (S-HTTP)

Το πρωτόκολλο Secure HTTP παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ενός ζευγαριού HTTP server – client με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές. Στόχος της σχεδίασης ήταν ένα ευέλικτο πρωτόκολλο που διαθέτει πολλαπλούς μηχανισμούς και αλγόριθμους, και την δυνατότητα διαπραγμάτευσης αυτών. Σχεδιάστηκε από τους E. Rescorla και A. Schiffman και αποτελεί υπερσύνολο του HTTP.

Τα χαρακτηριστικά του shttp είναι τα εξής:

1. Το S/HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους HTTP clients και servers. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
2. Αρκετά κρυπτογραφικά πρότυπα ενσωματώνονται στους S/HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP, Kerberos και PKCS-7 (ο πρόγονος του CMS). Είναι συμβατό με το HTTP.
3. Το S/HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα, χωρίς την απαίτηση από τους χρήστες να έχουν ένα έγκυρο ζεύγος δημόσιας – ιδιωτικής κλείδας. Βέβαια, είναι σε θέση να εκμεταλλευτεί την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών.
4. Το S/HTTP υποστηρίζει απ' άκρη σ' άκρη ασφαλής συναλλαγές, σε αντίθεση με το HTTP που προϋποθέτει μία αποτυχημένη προσπάθεια πρόσβασης του χρήστη πριν την εφαρμογή οποιωνδήποτε μηχανισμών ασφαλείας. Με το S/HTTP, σε καμία περίπτωση τα ευαίσθητα δεδομένα δεν μεταδίδονται στο δίκτυο απροστάτευτα.

5. Επιτρέπει πλήρη ευελιξία όσον αφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας (κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.
6. Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.

8.5 MIME και S/MIME

Το Multipurpose Internet Mail Extensions (MIME) είναι ένα πρότυπο δικτύου για την ηλεκτρονική αλληλογραφία. Σχεδόν όλο το ηλεκτρονικό ταχυδρομείο του διαδικτύου διαβιβάζεται μέσω SMTP σε μορφή (format) MIME. Το ηλεκτρονικό ταχυδρομείο διαδικτύου συνδέεται τόσο πολύ με τα πρότυπα SMTP και MIME ώστε μερικές φορές καλείται SMTP/MIME e-mail.

Το MIME είναι ένα θεμελιώδες συστατικό των πρωτοκόλλων επικοινωνίας όπως το HTTP, το οποίο απαιτεί τα δεδομένα να μεταφέρονται στα πλαίσια των ηλεκτρονικών ταχυδρομείων σαν μηνύματα, ακόμη και αν τα στοιχεία δεν είναι πραγματικά ηλεκτρονικά μηνύματα. Κατά κανόνα η κωδικοποίηση του μηνύματος γίνεται αυτόματα στον υπολογιστή του αποστολέα και η αποκωδικοποίηση γίνεται είτε από έναν mail client (πχ outlook) ή από έναν mail server μόλις παραληφθεί το μήνυμα.

Αρχικά οι εκτιμήσεις για την ασφάλεια του MIME ήταν δευτερεύουσες. Με την αύξηση της δημοτικότητας του, η ασφάλεια είναι πλέον θέμα ζωτικής σημασίας και αυτό οδήγησε στην δημιουργία του ασφαλούς MIME (S/MIME).

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Η δεύτερη έκδοση του S/MIME είναι επί του παρόντος ενσωματωμένη σε πολλά δημοφιλή προϊόντα, όπως τα Lotus Domino, Netscape Communicator, Novell GroupWise και Microsoft Exchange. Το S/MIME δίνει την δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.

Η ομάδα Internet Engineering Task Force (IETF) αναπτύσσει την $3^{η}$ έκδοση του S/MIME που περιλαμβάνει την εξειδίκευση Cryptographic Message Syntax (CMS) που ορίζει μια τυποποιημένη σύνταξη για την επικοινωνία των κρυπτογραφικών πληροφοριών που είναι ανεξάρτητες από την μορφή των ενθυλακωμένων περιεχομένων ή από τον μηχανισμό μεταφοράς. Κάθε τύπος δεδομένων μπορεί να προστατευθεί από το CMS. Εκτός από τις εφαρμογές S/MIME, το CMS μπορεί να χρησιμοποιηθεί με τα πρωτόκολλα HTTP, X.400, FTP, SSL και SET. Η στρατηγική ανάπτυξης της τρίτης έκδοσης είναι τέτοια ώστε να διατηρείται η συμβατότητα με την προηγούμενη έκδοση (version 2). Αυτό επιτυγχάνεται με την πρόσθεση νέων, προαιρετικών στοιχείων στην νέα έκδοση, των οποίων η απουσία στις επικεφαλίδες επιτρέπει την συνεργασία των δύο εκδόσεων.

Επίσης, η έκδοση 3 του S/MIME απαιτεί την ύπαρξη ενός ελάχιστου συνόλου κρυπτογραφικών αλγορίθμων που διασφαλίζουν την συνεργασίας μεταξύ διαφορετικών εφαρμογών.

Το S/MIME χρησιμοποιεί τις προδιαγραφές του MIME και παρέχει προστασία στα τμήματα των μηνυμάτων που είναι απροστάτευτα. Με αυτό όλες οι διαφορετικές μορφές της ψηφιακής υπογραφής και της κρυπτογράφησης θεωρούνται παραλλαγές ενός βασικού μετασχηματισμού δεδομένων.

8.6 Πρωτόκολλο SET

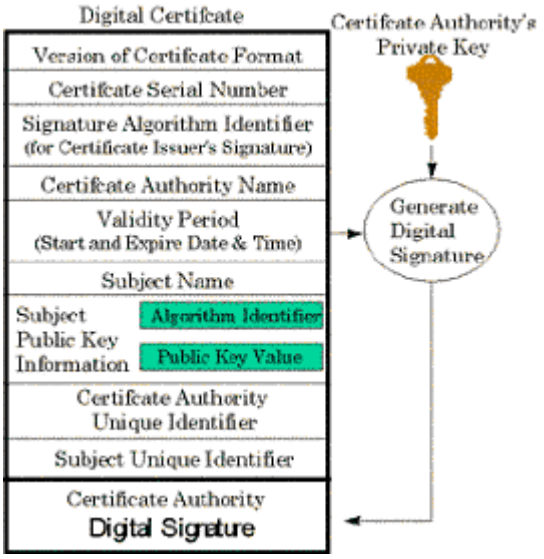
Οι εταιρείες Visa και Mastercard έχουν προτείνει ένα άλλο σύστημα γνωστό με το όνομα SET (Secure Electronic Transaction). Ο διαχειριστής ενός ηλεκτρονικού καταστήματος πρέπει να γνωρίζει πως το SET αποτελείται από τρία μέρη:

1. Μια "ηλεκτρονική πιστωτική κάρτα" η οποία είναι εγκατεστημένη στον Η/Υ του χρήστη (το ειδικό λογισμικό παρέχεται δωρεάν από το SET).
2. Ειδικό λογισμικό εγκατεστημένο στο ηλεκτρονικό κατάστημα.
3. Ειδικό λογισμικό εγκατεστημένο σε μια πιστοποιημένη από το SET τράπεζα.

Χάρη στην εφαρμογή αυτή τα στοιχεία της πιστωτικής κάρτας του αγοραστή διαβιβάζονται από το ηλεκτρονικό κατάστημα στην τράπεζα χωρίς ο πωλητής να μαθαίνει ποτέ το παραμικρό για την κάρτα του αγοραστή (δεν γνωρίζει ούτε το όνομα, ούτε τον αριθμό, ούτε την ημερομηνία λήξεως).

Με τον τρόπο αυτό τα στοιχεία της κάρτας του αγοραστή έχουν μηδαμινές πιθανότητες να υποκλαπούν από τρίτους. Γι' αυτό και οι Visa και Mastercard προσδοκούν πως το σύστημα αυτό θα υιοθετηθεί τελικά ως η βάση για κάθε συναλλαγή ηλεκτρονικού εμπορίου. Είναι μάλιστα τόσο σίγουρες για την ασφάλειά του που εγγυώνται κάθε συναλλαγή η οποία γίνεται μέσω SET. Δηλαδή με το SET ο online έμπορος δεν διατρέχει κανέναν από τους κινδύνους των παραγγελιών με πλαστά στοιχεία. Δυστυχώς, μέχρι σήμερα το SET δεν έχει διαδοθεί ευρέως. Απ' ό,τι φαίνεται η ευκολία της χρήσης πιστωτικής κάρτας με τον παραδοσιακό τρόπο (SSL) είναι τόσο μεγάλη (ή το λογισμικό του SET είναι τόσο περίπλοκο) που οι καταναλωτές δεν το έχουν ακόμη υιοθετήσει παρά τα προφανή πλεονεκτήματα ασφαλείας τα οποία διαθέτει.

Έτσι, συνήθως η χρήση του SET περιορίζεται μόνο στις επικοινωνίες μεταξύ εμπόρου και τράπεζας, ενώ η επικοινωνία του εμπόρου με τον πελάτη εξακολουθεί να διεξάγεται με SSL. Με τον τρόπο αυτό όμως ο κίνδυνος των πλαστών παραγγελιών παραμένει το ίδιο μεγάλος. Στο παρακάτω διάγραμμα παρουσιάζεται μία τυπική ηλεκτρονική συναλλαγή χρησιμοποιώντας το πρωτόκολλο SET.



8.7 Ασφάλεια EDI

Το EDI (Electronic Data Interchange) αποτελεί έναν τρόπο για την ανταλλαγή δεδομένων μεταξύ των επιχειρήσεων χρησιμοποιώντας αυστηρά πρότυπα. Η χρήση του προϋποθέτει την εγκατάσταση ενός λογισμικού και από τις δύο πλευρές των συναλλαγών. Υποστηρίζει Batch-time και real-time επεξεργασία μηνυμάτων, ενώ τα όρια προσβασιμότητας του είναι περιορισμένα λόγω της λειτουργίας του σε intranets και extranets.

Το Internet αποτελεί θεμέλιο για την χρήση του EDI. Παρέχει στιγμιαία μετάδοση δεδομένων, είναι βασισμένο σε ανοικτά πρότυπα και προσφέρεται σε χαμηλότερο κόστος σε σχέση με τα δίκτυα προστιθέμενης αξίας (VAN). Το μόνο που απαιτείται είναι ένα πρότυπο ασφάλειας το οποίο καθιστά τα δημόσια δίκτυα ασφαλή για την μεταφορά ευαίσθητων πληροφοριών.

8.8 Kerberos

Είναι ένα δικτυακό σύστημα ασφαλείας το οποίο αναπτύχθηκε στο MIT. Χρησιμοποιεί κρυπτογραφία συμμετρικού κλειδιού για τη μετάδοση μηνυμάτων προς και από υπολογιστές και χρησιμοποιείται για πιστοποίηση χρηστών. Κάθε χρήστης του Kerberos έχει ένα password το οποίο χρησιμοποιεί. Υπάρχουν εκδόσεις του Kerberos για διάφορα δημοφιλή πρωτόκολλα του Internet όπως το POP3, το Telnet και το FTP.

Ο πυρήνας μιας αρχιτεκτονικής Kerberos είναι το KDC (βασικός server διανομής). Το KDC αποθηκεύει τις πληροφορίες επικύρωσης και τις χρησιμοποιεί για να επικυρώσει τους χρήστες και τις υπηρεσίες. Λόγω της κρίσιμης λειτουργία του KDC, χρησιμοποιούνται πολλαπλάσια KDC. Κάθε KDC αποθηκεύει μια βάση δεδομένων των χρηστών, των servers καθώς και των μυστικών κλειδιών.

Το Kerberos επιτρέπει στις δικτυακές εφαρμογές να αναγνωρίζουν με ασφάλεια την ταυτότητα του χρήστη που ζητά εξυπηρέτηση, χωρίς να στέλνει στο δίκτυο δεδομένα που μπορούν να επιτρέψουν σε ένα πιθανό εισβολέα να προσποιηθεί ότι είναι ο

χρήστης και χωρίς να βασίζεται στις διευθύνσεις των μηχανών του δικτύου. Επίσης, η πιστοποίηση ταυτότητας γίνεται από τον application server και η επικοινωνία γίνεται εν γνώση της πιθανότητας ότι η διακινούμενη πληροφορία μπορεί να τροποποιηθεί και να αναγνωστεί κατά βούληση. Το Kerberos προαιρετικά προσφέρει ακεραιότητα και απόρρητη συναλλαγή για τα δεδομένα που στέλνονται μεταξύ του client και του application server. Σαν application server εννοούμε τον server που προσφέρει υπηρεσίες όπως mail, ftp, http, telnet.

9. Πρόταση ασφάλειας και μυστικότητας του osCommerce

Δεδομένου ότι η επικοινωνία μεταξύ του πελάτη (browser) και του server γίνεται με ένα τρόπο ανεξαρτήτως κράτους, δεν είναι δυνατό να είναι γνωστό ποιος είναι ο πελάτης και πού είναι την κάθε στιγμή στον website.

Το πρωτόκολλο των cookies είναι μια εφαρμογή που χρησιμοποιείται στα websites και επιτρέπει τον εντοπισμό των πελατών. Αυτό αποτελεί τη μεγαλύτερη αλληλεπίδραση μεταξύ του πελάτη και του server δεδομένου ότι ο server είναι σε θέση να πει ποιος είναι ο πελάτης και που είναι την δεδομένη στιγμή στο site.

Χωρίς αυτήν την εφαρμογή, οι αγορές on-line ή οι on-line τραπεζικές συναλλαγές δεν θα ήταν δυνατές.

Το πρωτόκολλο των cookies δουλεύει επιτρέποντας στο website την αποθήκευση ενός αρχείου στον υπολογιστή του πελάτη. Στο αρχείο αυτό ο πελάτης στέλνει την κάθε ενέργεια που εκτελεί σ' αυτό. Το website μπορεί να αποθηκεύσει οποιεσδήποτε πληροφορίες ζητούνται από το αρχείο των cookies αλλά το μέγεθος τους μπορεί να είναι μέχρι 4 KB.

Για λόγους ασφάλειας, το αρχείο των cookies που αποθηκεύεται από το website στον υπολογιστή του πελάτη μπορεί να διαβαστεί μόνο από το website που τον αποθήκευσε. Αυτό ελέγχεται από το url domain του website. Π.χ. το domain www.domain-one.com μπορεί να έχει πρόσβαση μόνο στα αρχεία cookies που το www.domain-one.com αποθήκευσε, κι όχι τα αρχεία cookies που αποθήκευσε το www.domain-two.com.

Για να είναι σε θέση το website να ακολουθήσει τον πελάτη, μια μοναδική ταυτότητα συνόδου (session ID) δημιουργείται και αποθηκεύεται σαν cookie στον υπολογιστή του πελάτη.

Αυτό επιτρέπει στο website να ακολουθήσει τον πελάτη μέσω της session ID και να μάθει αν ο πελάτης βρίσκεται σε μία επικυρωμένη κατάσταση με την εφαρμογή ή όχι.

Δεδομένου ότι είναι δυνατό για τον πελάτη να θέσει εκτός λειτουργίας τα cookies στον browser του, εφαρμόζεται συνήθως μία μέθοδος υποχώρησης στην εφαρμογή για να είναι ακόμα σε θέση να κρατήσει άθικτη τη σύνοδο μεταξύ του πελάτη και του server.

Αυτή η μέθοδος περιλαμβάνει την επισύναψη της session ID σε όλους τους συνδέσμους του website όπως παρουσιάζεται παρακάτω:

http://www.domain-one.com/index.php?session_id=defw452r43tWEFw34352

Ανάλογα με την εφαρμογή, η εμφάνιση της session ID στο url μπορεί να δημιουργήσει ζητήματα σχετικά με την ασφάλεια και την μυστικότητα.

Αν ο πελάτης αντιγράψει το πλήρες url και το στείλει σε έναν φίλο του, εκείνος ο φίλος θα μοιραστεί τη σύνοδο λόγω της session ID που υπάρχει στο url. Αν ο αρχικός πελάτης είναι επικυρωμένος στην εφαρμογή, ο φίλος του θα έχει πρόσβαση στις πληροφορίες του λογαριασμού του αρχικού πελάτη.

Ένα άλλο παράδειγμα προκύπτει αν τα αιτήματα των πελατών περνούν από έναν proxy server.O proxy server καταχωρεί όλα τα ζητήματα συμπεριλαμβανομένων των παραμέτρων του url οι οποίες περιέχουν και την session ID. Είναι δυνατό για τον administrator ή κάποιον hacker , να αποκτήσει πρόσβαση στις καταχωρήσεις και να υποκλέψει τις συνόδους των πελατών, απλά με τη λήψη της καταγραμμένης session ID.

Η πρόταση ασφάλειας και μυστικότητας υποβλήθηκε για να αντιμετωπίσει αυτά τα ζητήματα καθώς μπορούν να είναι σοβαρά για μια εφαρμογή online καταστήματος όπου η διασφάλιση της μυστικότητας των πελατών αποτελεί κορυφαία προτεραιότητα.

Δεδομένου ότι τα ζητήματα σχετικά με την ασφάλεια και την μυστικότητα ποικίλλουν από λύση σε λύση, η πραγματοποίηση αυτής της πρότασης γίνεται για να είναι δυνατό να διαμορφωθεί στα ακόλουθα βασικά ζητήματα:

- Force Cookie Use
- Επικύρωση SSL_SESSION_ID
- Παρεμπόδιση των Spider Sessions
- Αναδημιουργία Session

9.1 Force Cookie Use

Η μόνη κοινή μέθοδος που υπάρχει για να αποτρέψει την εμφάνιση της session ID στο url είναι η αναγκαστική χρήση των cookies στην εφαρμογή.

Η παράμετρος για αυτό το βασικό ζήτημα ονομάζεται SESSION_FORCE_COOKIE_USE. Οι πελάτες που χρησιμοποιούν cookies θα είναι σε θέση να εκτελέσουν ασφαλείς συναλλαγές με την εφαρμογή, ενώ οι πελάτες που τα έχουν απενεργοποιημένα δεν θα είναι σε θέση να εκτελέσουν τέτοιες ενέργειες.

Τέτοιες ενέργειες για το osCommerce περιλαμβάνουν:

- Προσθήκη ενός προϊόντος στο καρότσι αγορών
- Εισαγωγή ή δημιουργία ενός λογαριασμού χρήστη
- Προβολή ή τροποποίηση των προσωπικών πληροφοριών του λογαριασμού, συμπεριλαμβανομένων των παραγγελιών που έχουν γίνει.
- Διαδικασία πληρωμής

Όταν η παράμετρος SESSION_FORCE_COOKIE_USE είναι ενεργοποιημένη και ο πελάτης έχει απενεργοποιημένα τα cookies, μια σελίδα θα εμφανιστεί αντί των παραπάνω ενεργειών περιγράφοντας στον πελάτη με φιλικούς όρους ότι πρέπει να ενεργοποιήσουν τα cookies στον browser τους προκειμένου να προχωρήσουν. Αυτή η μέθοδος προειδοποίησης του πελάτη του δίνει ακόμα την δυνατότητα να περιηγηθεί στο site αντί να τον μπλοκάρει εντελώς όπως συμβαίνει στα περισσότερα online καταστήματα και websites.

Όταν η παράμετρος SESSION_FORCE_COOKIE_USE είναι ενεργοποιημένη, ένα cookie θα υπάρχει πάντα στον browser του πελάτη και θα διαβάζεται πάντα μετά από κάθε αίτημα που υποβάλλεται στην σελίδα. Αυτό επιτρέπει στο osCommerce να ελέγξει για το cookie και να δράσει ανάλογα επιτρέποντας τη διαδικασία της συναλλαγής, ή μεταφέροντας τον πελάτη σε μία φιλική σελίδα που τον ενημερώνει να ενεργοποιήσει το cookie.

Καθώς το cookie ορίζεται στο ανώτερο επίπεδο domain του web server, ο διασφαλισμένος https server πρέπει επίσης να υπάρχει στο ίδιο domain.

Παραδείγματος χάριν, η αναγκαστική χρήση των cookies θα λειτουργήσει για τους ακόλουθους server:

http://www.domain-one.com
https://www.domain-one.com, ή https://ssl.domain-one.com

αλλά όχι για τους ακόλουθους:

http://www.domain-one.com
https://ssl.hosting_provider.com/domain-one/

Το παράδειγμα του ssl.hosting_provider.com χρησιμοποιεί ένα κοινό SSL πιστοποιητικό το οποίο χρησιμοποιείται για ασφαλείς συναλλαγές. Αυτό μπορεί εύκολα να τροποποιηθεί για να λειτουργήσει με την SESSION_FORCE_COOKIE_USE, αγοράζοντας και εγκαθιστώντας ένα SSL πιστοποιητικό για το domain domain-one.com.

Είναι δυνατό να παρακαμφθεί ο έλεγχος των cookies με την επισύναψη της session ID στο url όταν ο πελάτης μετακινείται από το HTTP στο HTTPS, ή από το HTTPS στο HTTP. Εντούτοις ο κύριος στόχος που προσπαθεί να επιτύχει αυτή η εφαρμογή είναι να μην τοποθετηθεί καθόλου η session ID στο url, πράγμα το οποίο συμβαίνει αν ο browser του πελάτη έχει απενεργοποιημένα τα cookies.

Μια απλή περίπτωση αποτυχίας αυτής της εφαρμογής, όπου διαφορετικά HTTP και HTTPS domain χρησιμοποιούνται, συμβαίνει όταν ο πελάτης επισκέπτεται για πρώτη φορά το κατάστημα (το cookie ορίζεται για το HTTP domain) και επιλέγει τον σύνδεσμο για ασφαλές Login (το cookie ορίζεται για το HTTPS domain).

Δεδομένου ότι τα cookies δεν μπορούν να διαβαστούν στο ίδιο αίτημα όταν ορίζονται για πρώτη φορά, η σελίδα Login δεν μπορεί να έχει πρόσβαση στο cookie του HTTPS domain καθώς μόλις ορίστηκε, και δεν μπορεί επίσης να διαβάσει το cookie του HTTP domain.

Ακόμα κι αν ο browser του πελάτη έχει ενεργοποιημένα τα cookies, το cookie δεν μπορεί να διαβαστεί και ο πελάτης θα κατευθυνθεί σε μία σελίδα που θα τον ειδοποιεί ότι πρέπει να ενεργοποιήσει τα cookies.

Η παράμετρος SESSION_FORCE_COOKIE_USE ήταν αρχικά εξ ορισμού ενεργοποιημένη, αλλά με τα προβλήματα που εμφανίζονται στους κοινούς server χρησιμοποιώντας τα κοινά SSL πιστοποιητικά έχει αποφασιστεί ότι η παράμετρος πρέπει εξ ορισμού να είναι απενεργοποιημένη.

Τα cookies που είναι ορισμένα ονομάζονται cookie_test και θα υπάρχουν στον υπολογιστή του πελάτη για 30 ημέρες.

9.2 Επικύρωση SSL_SESSION_ID

Όταν ο πελάτης ζητά μια ασφαλή https σελίδα, ο browser του πελάτη παράγει αυτόματα μια ID που ονομάζεται SSL_SESSION_ID. Αυτή χρησιμοποιείται από τον server για να επικυρώσει τον πελάτη κατά τη διάρκεια των ασφαλών συναλλαγών.

Αυτή η τιμή μπορεί να αποθηκευτεί ως τμήμα της συνόδου των πελατών για να πιστοποιήσει κάθε αίτημα που υποβάλλεται στις https σελίδες. Η παράμετρος για να ενεργοποιήσει αυτήν την πιστοποίηση ονομάζεται SESSION_CHECK_SSL_SESSION_ID και είναι εξ' ορισμού απενεργοποιημένη. Αν ενεργοποιηθεί, όταν το osCommerce ανιχνεύσει ότι μια άλλη SSL_SESSION_ID έχει παραχθεί, ο πελάτης ανακατευθύνεται σε μια φιλική σελίδα που τον ενημερώνει ότι μια άλλη τιμή έχει ανιχνευθεί και ότι πρέπει να κάνει ξανά logon στο κατάστημα για να συνεχίσει τη δράση του.

Αυτό βεβαιώνει ότι κανένα άλλο πρόσωπο δεν έχει υποκλέψει τη σύνοδο του πελάτη το οποίο θα παρήγαγε αυτόματα μία νέα SSL_SESSION_ID κατά την υποβολή των ασφαλών https αιτημάτων στον server.

Αυτή είναι εξ' ορισμού απενεργοποιημένη δεδομένου ότι ένα SSL πιστοποιητικό απαιτείται για ένα ασφαλές domain, και επειδή οι τιμές SSL_SESSION_ID δεν υποστηρίζονται ή δεν παράγονται από όλους τους webservers ή τους browsers.

Είναι γνωστό ότι εργάζεται με τον server Apache με mod_ssl, και με τους browsers Microsoft Internet Explorer, Netscape, και Mozilla.

9.3 Παρεμπόδιση των Spider Sessions

Όταν η παρεμπόδιση των spider sessions είναι ενεργοποιημένη, ο browser του πελάτη ανακτάται και αν ταιριάξει σε μία λίστα με spiders μηχανών αναζήτησης, η session παρακάμπτεται και καμία session ID δεν υποδεικνύεται στα url που συλλέγουν οι spiders των μηχανών αναζήτησης.

Αυτό συμβαίνει επειδή οι spiders μηχανών αναζήτησης δεν δέχονται τα cookies. Αν η χρήση των cookies είναι απενεργοποιημένη, η session ID προστίθεται στα url για να διατηρήσει μία κατάσταση συνόδου.

Θεωρείται επικίνδυνο όταν οι spiders μηχανών αναζήτησης υποδεικνύουν url που περιέχουν session IDs, καθώς τα url θα εμφανιστούν ως σύνδεσμοι στα αποτελέσματα των μηχανών αναζήτησης, και το αποτέλεσμα όταν αυτοί οι σύνδεσμοι επιλεχθούν από πολλούς πελάτες, θα είναι να παραχθούν κοινές σύνοδοι.

Η διαφορά μεταξύ αυτής της παρεμπόδισης και της Force Cookie Use είναι ότι η πρώτη λειτουργεί μόνο ενάντια σε έναν κατάλογο γνωστών μηχανών αναζήτησης spider ενώ η υλοποίηση της δεύτερης λειτουργεί σε μια παγκόσμια κλίμακα.

Η παράμετρος για την ενεργοποίηση της παρεμπόδισης των spider session, ονομάζεται SESSION_BLOCK_SPIDERS, και όταν είναι ενεργοποιημένη, είναι ενεργή μόνο όταν τίθεται εκτός λειτουργίας η SESSION_FORCE_COOKIE_USE.

9.4 Αναγέννηση συνόδου

Για ακόμα μεγαλύτερη διασφάλιση της συνόδου των πελατών, οι session IDs τους που παράχθηκαν κατά την είσοδο τους στο κατάστημα θα αναπαραχθούν είτε όταν αυτοί κάνουν logon με το όνομα χρήστη και τον κωδικό πρόσβασης είτε όταν δημιουργείται ένας νέος λογαριασμός χρήστη.

Η παράμετρος που ελέγχει την αναγέννηση των session ID ονομάζεται SESSION_RECREATE, και λειτουργεί μόνο για servers που έχουν εγκαταστήσει την 4.1 έκδοση της PHP ή μεγαλύτερη και όταν τα ανώτερα επίπεδα domain των HTTP και HTTPS είναι τα ίδια.

Αυτό οφείλεται στο γεγονός ότι το τρέχον cookie συνόδου πρέπει να επαναρυθμιστεί για να παραχθεί ένα νέο cookie συνόδου.

9.5 Πρόοδος εφαρμογής

Όλα τα βασικά ζητήματα πραγματοποιούνται με το 2.2-ms2-cvs, και εμφανίζονται στις εκδόσεις 2.2-ms2 και μετά.

Η πραγματοποίηση αυτή θα επεκταθεί για να προσθέσει τη δυνατότητα επικύρωσης του πελάτη μέσω της IP διεύθυνσης ή/και του browser του χρήστη.

Η εφαρμογή είναι υπό εξέλιξη έτσι ώστε ο εξαναγκασμός της χρήσης cookies να λειτουργήσει σε servers με κοινά SSL πιστοποιητικά.

9.6 Ζητήματα ανάπτυξης

Το cookie_test που ορίζεται για 30 ημέρες μπορεί να προκαλέσει αναταράξεις στην ανάπτυξη αν τα url περιέχουν την session ID.

Όταν η ανάπτυξη για την πραγματοποίηση αυτής της πρότασης γίνεται με ενεργοποιημένη την SESSION_FORCE_COOKIE_USE, τα σχετικά με το site cookies πρέπει να διαγραφούν, και το cookie_test πρέπει να οριστεί μόνο για 0 ημέρες, πράγμα το οποίο ορίζει το cookie μόνο για την session του browser (όσο ο browser παραμένει ανοικτός).

Δηλαδή κλείνοντας τον browser διαγράφονται τα cookies από την μνήμη του.
Το cookie_test ορίζεται στο αρχείο catalog/includes/application_top.php μέσω της λειτουργίας tep_setcookie ().

10. Βιβλιογραφία

Papers

Ασφάλεια στο διαδίκτυο. Κ. Μάγκος Α. Νιξαρλίδης

Ο Δρόμος Προς Το Ηλεκτρονικό Εμπόριο (Τα απαραίτητα βήματα για τη δημιουργία ενός ηλεκτρονικού καταστήματος). Ελληνική Ένωση Επαγγελματιών Ίντερνετ

Κρυπτογραφία. ΑΠΘ Κέντρο Λειτουργίας Δικτύου

"Δίκτυα Προστιθέμενης Αξίας EDI και Είδη Ηλεκτρονικού Εμπορίου" Δρ. Μαρία Γραμματικού

Τράπεζα Πειραιώς

Βασικές προϋποθέσεις συνεργασίας ηλεκτρονικού καταστήματος και τράπεζας

Paycenter- Services

Links από το Internet

http://www.securityfocus.com/infocus/1775

http://www.verisign.com.au/whitepapers/enterprise/ecommerce/infra2.shtml

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

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

http://www.go-online.gr/ebusiness/specials/article.html?article_id=716

http://www.pointer.gr/e-commerce.php

http://www.verisign.com.au/whitepapers/enterprise/ecommerce/infra5.shtml

http://www.oscommerce.info/kb/osCommerce/Developers_Section/Implementations/4

http://www.piraeusbank.gr/ecportal.asp?id=242986&lang=1&nt=98&from=links&fromsearch=234010&tid=234010

http://www.piraeusbank.gr/ecportal.asp?id=242260&lang=1&nt=96&from=links&fromsearch=234010&tid=234010

http://www.piraeusbank.gr/ecportal.asp?id=242995&lang=1&nt=96&from=links&fromsearch=234010&tid=234010

http://www.securityfocus.com/bid/15023/info

http://secunia.com/advisories/10443/

http://www.frsirt.com/english/

http://www.tech-faq.com/ylang/el/kerberos.shtml

http://en.wikipedia.org/wiki/2Checkout.com

http://en.wikipedia.org/wiki/Authorize.Net

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

http://www.secpay.com/secpay/index.php/secpay/content/view/full/116.html