

COUNT UPON SECURITY

Increase security awareness. Promote, reinforce and learn security skills.



Step-by-Step guide for Joomla 1.5.9 and VirtueMart 1.1.4 e-Commerce Vulnerable Lab

1. Summary

With this document you should be able create a simulated real world e-commerce website in a controlled and virtual environment. In this environment you can practice your offensive and defensive security skills legally, safely and for educational purposes. The scenario contains known vulnerabilities with exploits available in the Internet.

The OS installation is not covered since it's an easy and automated step if you are running VMware Workstation 8. It covers the MySQL, Apache and PHP installation and basic configuration. Then it shows how to install and configure the initial settings of Joomla and VirtueMart.

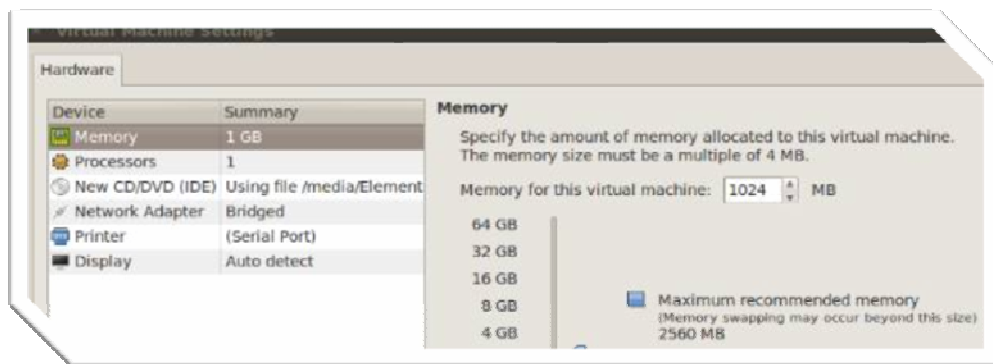
The following Google dork will show a significant number of websites that are running VirtueMart:
`inurl:"?option=com_virtuemart" site:*.com`

Disclaimer: This guide and settings should not be used for any production system. It assumes default configuration for different services and applications. Use it only on your controlled lab since it's easily exploitable.

2. OS Installation

Create a virtual machine with the operating system CentOS 5.3 for x86 architecture. To be able to install and run the e-commerce website you will need a LAMP stack which means Linux, Apache, MySQL and PHP. The virtual machine can be easily installed on virtualization software such as VMware Workstation.

Download the DVD ISO image for CentOS 5.3 from <http://download.filesystems.org/linux/centos/>. Check the MD5 integrity. Then create a new virtual machine. In my case 1CPU, 1GB Ram, 40 GB disk plus 1 NIC directly connected to the internet (bridge mode) to be able to download software and map the ISO file into the CD-ROM.



The installation of the operating system is straightforward. During the installation you can create one user other than root. Specify networking settings. On my network I have a router that will assign IP address to the machines using DHCP. After installation I can login into the machine using SSH and start configuring the initial settings. I will call the machine cms.challeng3.local.

```
[root@cms ~]# hostname cms
[root@cms ~]# echo '192.168.1.29 cms cms.challeng3.local' >> /etc/hosts
[root@cms ~]# ping -c 1 cms.challeng3.local
PING cms.challeng3.local (192.168.1.29) 56(84) bytes of data:
64 bytes from cms.challeng3.local (192.168.1.29): icmp_seq=1 ttl=64 time=0.048 ms
--- cms.challeng3.local ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.048/0.048/0.048/0.000 ms
```

3. LAMP Stack

```
[root@localhost ~]# yum install mysql-server
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: swissmirror.silyus.net
 * updates: swissmirror.silyus.net
 * extras: swissmirror.silyus.net
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
----> Package mysql-server.i386 0:5.0.95-1.el5_7.1 set to be updated
--> Processing Dependency: mysql = 5.0.95-1.el5_7.1 for package: mysql-server
--> Processing Dependency: perl-DBD-MySQL for package: mysql-server
--> Processing Dependency: perl(DBI) for package: mysql-server
--> Processing Dependency: libmysqlclient.so.15(libmysqlclient_15) for package: mysql-server
--> Processing Dependency: perl-DBI for package: mysql-server
--> Processing Dependency: libmysqlclient_r.so.15(libmysqlclient_15) for package: mysql-server
--> Processing Dependency: libmysqlclient.so.15 for package: mysql-server
--> Processing Dependency: libmysqlclient_r.so.15 for package: mysql-server
--> Running transaction check
----> Package mysql.i386 0:5.0.95-1.el5_7.1 set to be updated
----> Package perl-DBD-MySQL.i386 0:3.0007-2.el5 set to be updated
----> Package perl-DBI.i386 0:1.52-2.el5 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
Install      4 Package(s)
Update      0 Package(s)
Remove      0 Package(s)
Total download size: 15 M
Is this ok [y/N]: Y
Downloading Packages:
(1/4): perl-DBD-MySQL-3.0007-2.el5.i386.rpm
| 148 kB    00:00
(2/4): perl-DBI-1.52-2.el5.i386.rpm
| 600 kB    00:00
(3/4): mysql-5.0.95-1.el5_7.1.i386.rpm
| 4.9 MB    00:04
(4/4): mysql-server-5.0.95-1.el5_7.1.i386.rpm
| 9.8 MB    00:06
-----
Total                                                                    932
kB/s | 15 MB    00:16
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID e8562897
Importing GPG key 0xE8562897 "CentOS-5 Key (CentOS 5 Official Signing Key) <centos-5-
key@centos.org>" from /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
Is this ok [y/N]: Y

Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : perl-DBI                                [1/4]
  Installing      : mysql                                  [2/4]
  Installing      : perl-DBD-MySQL                          [3/4]
  Installing      : mysql-server                            [4/4]
Installed: mysql-server.i386 0:5.0.95-1.el5_7.1
Dependency Installed: mysql.i386 0:5.0.95-1.el5_7.1 perl-DBD-MySQL.i386 0:3.0007-2.el5 perl-
DBI.i386 0:1.52-2.el5
Complete!
```

```
[root@localhost ~]# yum install php php-mysql
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: swissmirror.silyus.net
* updates: swissmirror.silyus.net
* extras: swissmirror.silyus.net
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
----> Package php-mysql.i386 0:5.1.6-39.el5_8 set to be updated
--> Processing Dependency: php-common = 5.1.6-39.el5_8 for package: php-mysql
--> Processing Dependency: php-pdo for package: php-mysql
----> Package php.i386 0:5.1.6-39.el5_8 set to be updated
--> Processing Dependency: php-cli = 5.1.6-39.el5_8 for package: php
--> Running transaction check
----> Package php-common.i386 0:5.1.6-39.el5_8 set to be updated
----> Package php-cli.i386 0:5.1.6-39.el5_8 set to be updated
----> Package php-pdo.i386 0:5.1.6-39.el5_8 set to be updated
--> Finished Dependency Resolution
Dependencies Resolved
```

Package Repository	Arch Size	Version	
Installing:			
php	i386	5.1.6-39.el5_8	updates
2.3 M			
php-mysql	i386	5.1.6-39.el5_8	updates
87 k			
Installing for dependencies:			
php-cli	i386	5.1.6-39.el5_8	updates
2.1 M			
php-common	i386	5.1.6-39.el5_8	updates
154 k			
php-pdo	i386	5.1.6-39.el5_8	updates
66 k			

```
Transaction Summary
=====
Install      5 Package(s)
Update       0 Package(s)
Remove       0 Package(s)
Total download size: 4.7 M
Is this ok [y/N]: Y

Downloading Packages:
(1/5): php-pdo-5.1.6-39.el5_8.i386.rpm
| 66 kB    00:00
(2/5): php-mysql-5.1.6-39.el5_8.i386.rpm
| 87 kB    00:00
(3/5): php-common-5.1.6-39.el5_8.i386.rpm
| 154 kB   00:00
(4/5): php-cli-5.1.6-39.el5_8.i386.rpm
| 2.1 MB   00:01
(5/5): php-5.1.6-39.el5_8.i386.rpm
| 2.3 MB   00:01
-----
Total                                     939
kB/s | 4.7 MB    00:05
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : php-common [1/5]
  Installing      : php-cli [2/5]
  Installing      : php-pdo [3/5]
  Installing      : php [4/5]
  Installing      : php-mysql [5/5]
Installed: php.i386 0:5.1.6-39.el5_8 php-mysql.i386 0:5.1.6-39.el5_8
Dependency Installed: php-cli.i386 0:5.1.6-39.el5_8 php-common.i386 0:5.1.6-39.el5_8 php-pdo.i386
0:5.1.6-39.el5_8
Complete!
```

```
[root@localhost ~]# /usr/bin/mysql_install_db --user=mysql
Installing MySQL system tables...
OK
Filling help tables...
OK
To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h cms password 'new-password'
Alternatively you can run:
/usr/bin/mysql_secure_installation
which will also give you the option of removing the test
databases and anonymous user created by default. This is
strongly recommended for production servers.
See the manual for more instructions.
You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &
You can test the MySQL daemon with mysql-test-run.pl
cd mysql-test ; perl mysql-test-run.pl
Please report any problems with the /usr/bin/mysqlbug script!
The latest information about MySQL is available on the web at
http://www.mysql.com
Support MySQL by buying support/licenses at http://shop.mysql.com
```

```
[root@localhost ~]# service mysqld status
mysqld is stopped
[root@localhost ~]# service mysqld start
Starting MySQL: [ OK ]
[root@localhost ~]# /usr/bin/mysqladmin version
/usr/bin/mysqladmin Ver 8.41 Distrib 5.0.95, for redhat-linux-gnu on i686
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Server version          5.0.95
Protocol version        10
Connection               Localhost via UNIX socket
UNIX socket              /var/lib/mysql/mysql.sock
Uptime:                  6 sec
Threads: 1 Questions: 2 Slow queries: 0 Opens: 12 Flush tables: 1 Open tables: 6 Queries
per second avg: 0.333
```

```
[root@localhost ~]# /usr/bin/mysqlshow
+-----+
| Databases |
+-----+
| information_schema |
| mysql |
| test |
+-----+
[root@localhost ~]# service mysqld stop
Stopping MySQL: [ OK ]
[root@localhost ~]# service mysqld start
Starting MySQL: [ OK ]
[root@localhost ~]# mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.0.95 Source distribution
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> select host, user from mysql.user;
+-----+-----+
| host | user |
+-----+-----+
| 127.0.0.1 | root |
| cms | root |
| cms | root |
| localhost | root |
| localhost | root |
+-----+-----+
5 rows in set (0.00 sec)

mysql> set password for 'root'@'localhost' = PASSWORD('password');
Query OK, 0 rows affected (0.00 sec)

mysql> set password for 'root'@'127.0.0.1' = PASSWORD('password');
Query OK, 0 rows affected (0.00 sec)
mysql> quit
Bye

[root@localhost ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.0.95 Source distribution
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> quit
Bye
```

Make sure Mysql and Apache are running on init levels 3,4 and 5.

```
root@localhost ~]# chkconfig --level 345 mysqld on
[root@localhost ~]# chkconfig --level 345 httpd on
```

Set the ServerName directive under httpd.conf

```
#vi /etc/httpd/conf/httpd.conf
ServerName cms.challeng3.local:80
[root@cms ~]# service httpd start
Starting httpd: [ OK ]
```

Add a firewall rule that will allow traffic to port 80. The rule should be before the last one. Then test connectivity to port 80 and check if Apache is running.

```

[root@cms ~]# vi /etc/sysconfig/iptables
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
[root@cms ~]# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules: ip_conntrack_netbios_n[ OK ]

[root@cms ~]# nc cms.challeng3.local 80
OPTIONS / HTTP/1.0
HTTP/1.1 200 OK
Date: Sun, 04 Nov 2012 14:44:18 GMT
Server: Apache/2.2.3 (CentOS)
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Connection: close
Content-Type: httpd/unix-directory

```

A simple test to ensure PHP is configured and integrated with Apache.

```

[root@cms html]# cd /var/www/html
[root@cms html]# vi index.php

<?php
    phpinfo();
?>

[root@cms html]# php -f /var/www/html/index.php | head -4
phpinfo()
PHP Version => 5.1.6
System => Linux cms 2.6.18-128.el5 #1 SMP wed Jan 21 10:44:23 EST 2009 i686

```

The basic setup is done, lets proceed with the Joomla Installation.

4. Joomla Installation

```
[root@cms html]# cd /var/www/html/
[root@cms html]# wget http://joomla.org/gf/download/frsrelease/9294/34965/Joomla_1.5.9-Stable-Full_Package.tar.gz
--06:53:27-- http://joomla.org/gf/download/frsrelease/9294/34965/Joomla_1.5.9-Stable-Full_Package.tar.gz
Resolving joomla.org... 206.123.111.164
Connecting to joomla.org|206.123.111.164|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://downloads.joomla.org/frsrelease/3/4/9/34965/Joomla_1.5.9-Stable-Full_Package.tar.gz [following]
--06:53:32-- http://downloads.joomla.org/frsrelease/3/4/9/34965/Joomla_1.5.9-Stable-Full_Package.tar.gz
Resolving downloads.joomla.org... 206.123.111.167
Connecting to downloads.joomla.org|206.123.111.167|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4215142 (4.0M) [application/x-gzip]
Saving to: 'Joomla_1.5.9-Stable-Full_Package.tar.gz'
100%[=====>] 4,215,142 394K/s in 12s
06:53:44 (353 KB/s) - 'Joomla_1.5.9-Stable-Full_Package.tar.gz' saved [4215142/4215142]

[root@cms html]# md5sum Joomla_1.5.9-Stable-Full_Package.tar.gz
5a55b05339ae2786e589e4c8a343655a Joomla_1.5.9-Stable-Full_Package.tar.gz

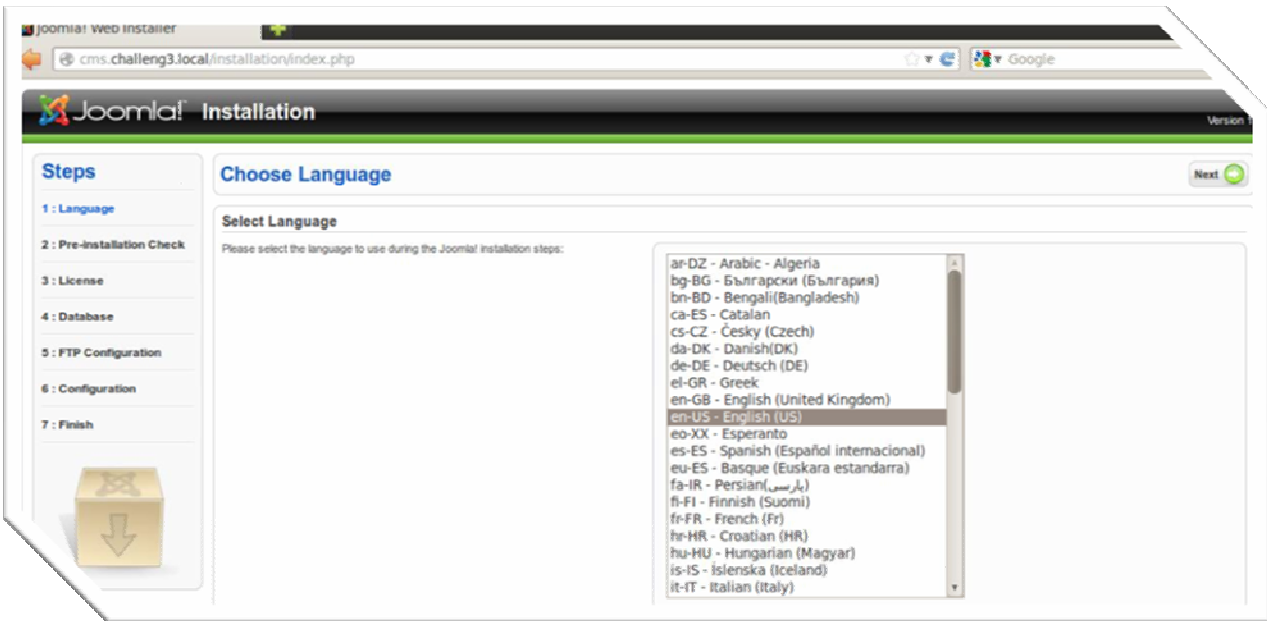
[root@cms html]# tar -xzvf Joomla_1.5.9-Stable-Full_Package.tar.gz

root@localhost html]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.0.95 Source distribution
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

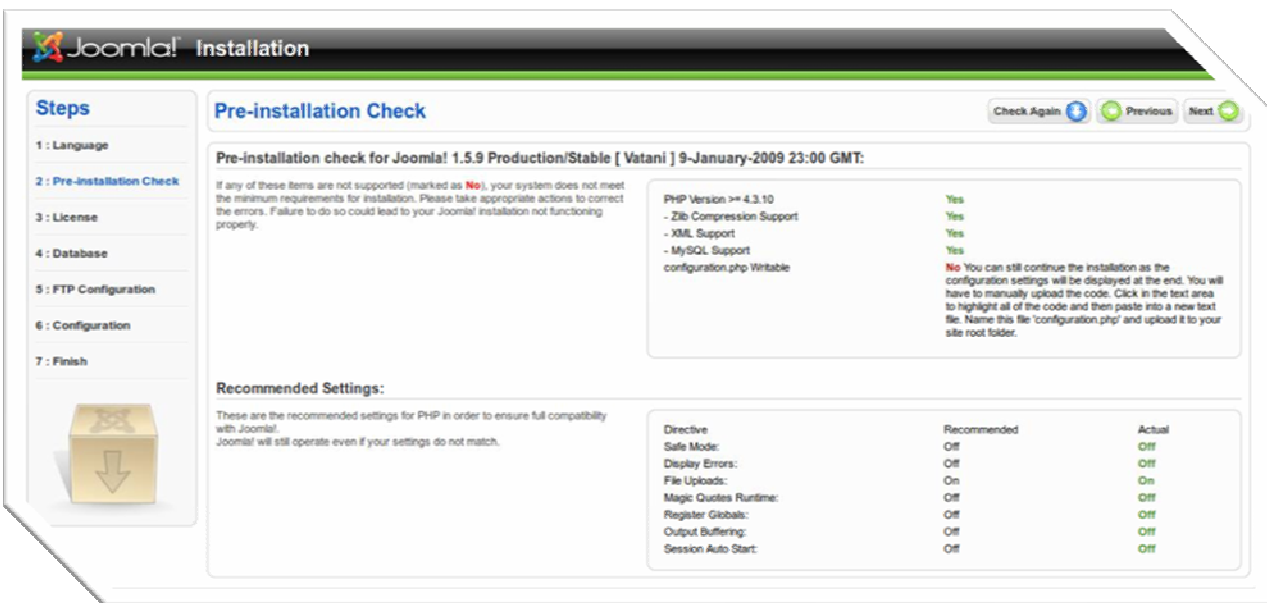
mysql> create DATABASE joomla;
Query OK, 1 row affected (0.01 sec)
mysql> show DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| joomla |
| mysql |
| test |
+-----+
4 rows in set (0.00 sec)
```

Point your browser to the localhost and Joomla Installation will appear :

Choose the language of installation.

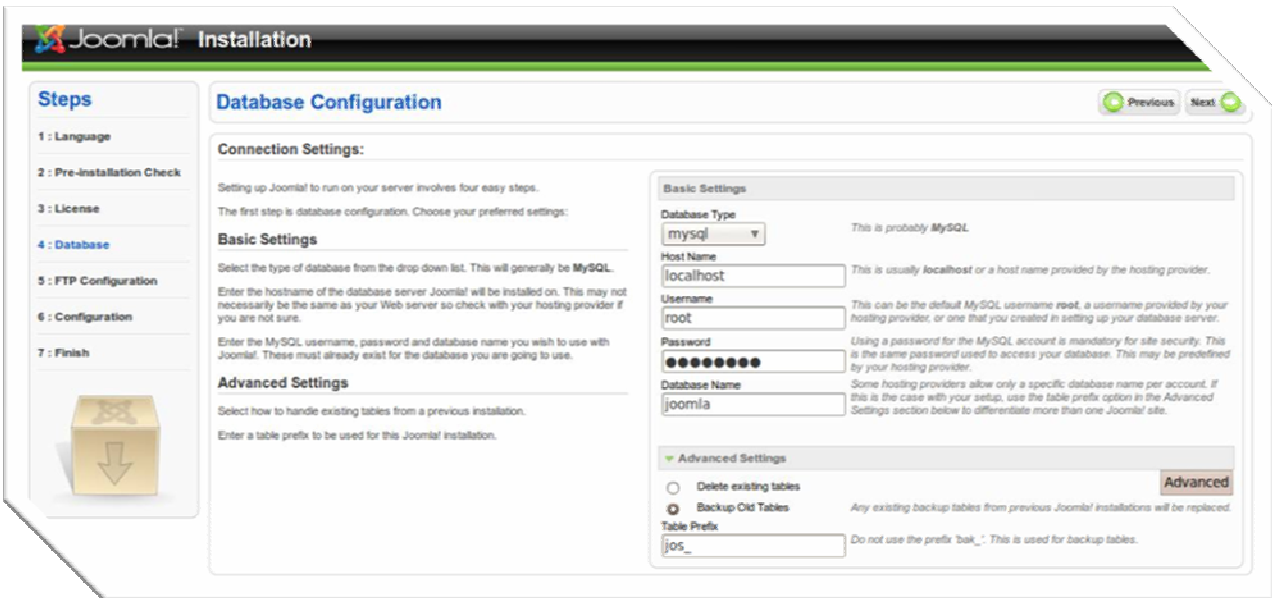


Make sure all the Pre-Installation checks are met. The Configuration. Php Writable setting will be addressed a few steps later.



Accept the License.

Configure the Database settings. With hostname, mysql username and password plus database name



Joomla! Installation

Steps

- 1 : Language
- 2 : Pre-Installation Check
- 3 : License
- 4 : Database
- 5 : FTP Configuration
- 6 : Configuration
- 7 : Finish

Database Configuration

Connection Settings:

Setting up Joomla! to run on your server involves four easy steps. The first step is database configuration. Choose your preferred settings:

Basic Settings

Select the type of database from the drop down list. This will generally be MySQL.

Enter the hostname of the database server Joomla! will be installed on. This may not necessarily be the same as your Web server so check with your hosting provider if you are not sure.

Enter the MySQL username, password and database name you wish to use with Joomla!. These must already exist for the database you are going to use.

Advanced Settings

Select how to handle existing tables from a previous installation.

Enter a table prefix to be used for this Joomla! installation.

Basic Settings

Database Type: This is probably MySQL.

Host Name: This is usually localhost or a host name provided by the hosting provider.

Username: This can be the default MySQL username root, a username provided by your hosting provider, or one that you created in setting up your database server.

Password: Using a password for the MySQL account is mandatory for site security. This is the same password used to access your database. This may be predefined by your hosting provider.

Database Name: Some hosting providers allow only a specific database name per account. If this is the case with your setup, use the table prefix option in the Advanced Settings section below to differentiate more than one Joomla! site.

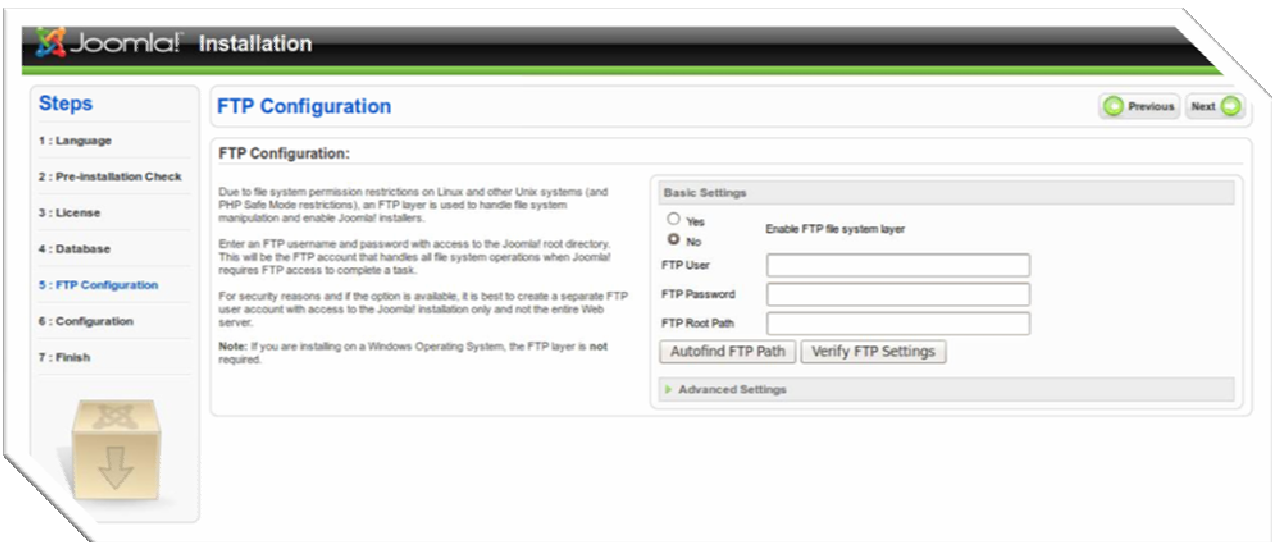
Advanced Settings

☐ Delete existing tables

☒ Backup Old Tables Any existing backup tables from previous Joomla! installations will be replaced.

Table Prefix: Do not use the prefix 'bak_'. This is used for backup tables.

Leave the default FTP configuration settings.



Joomla! Installation

Steps

- 1 : Language
- 2 : Pre-Installation Check
- 3 : License
- 4 : Database
- 5 : FTP Configuration
- 6 : Configuration
- 7 : Finish

FTP Configuration

FTP Configuration:

Due to file system permission restrictions on Linux and other Unix systems (and PHP Safe Mode restrictions), an FTP layer is used to handle file system manipulation and enable Joomla! installers.

Enter an FTP username and password with access to the Joomla! root directory. This will be the FTP account that handles all file system operations when Joomla! requires FTP access to complete a task.

For security reasons and if the option is available, it is best to create a separate FTP user account with access to the Joomla! installation only and not the entire Web server.

Note: If you are installing on a Windows Operating System, the FTP layer is not required.

Basic Settings

☐ Yes

☒ No Enable FTP file system layer

FTP User:

FTP Password:

FTP Root Path:

Autofind FTP Path: Verify FTP Settings:

Advanced Settings

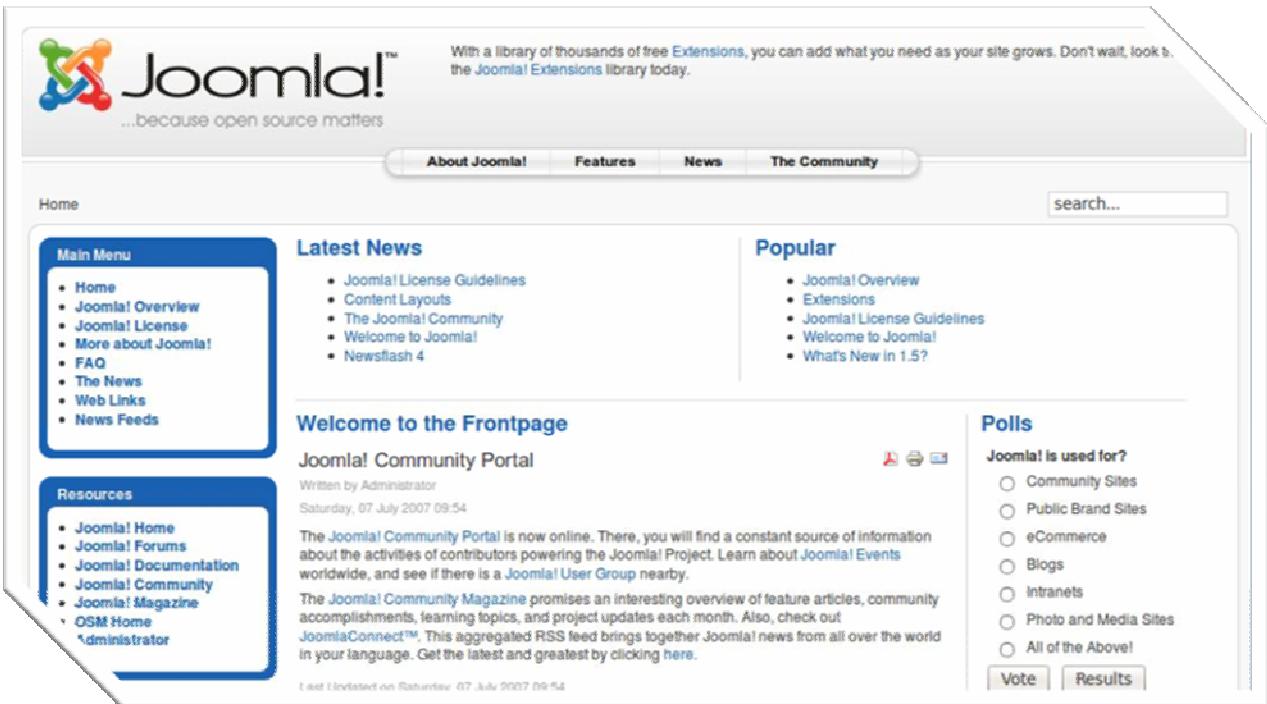
Configure the Main Configuration with site name, email, admin password and install the sample data.

You should see a message “Congratulations ! Joomla is now installed.” And a warning that you need to remove the installation folder before you proceed.

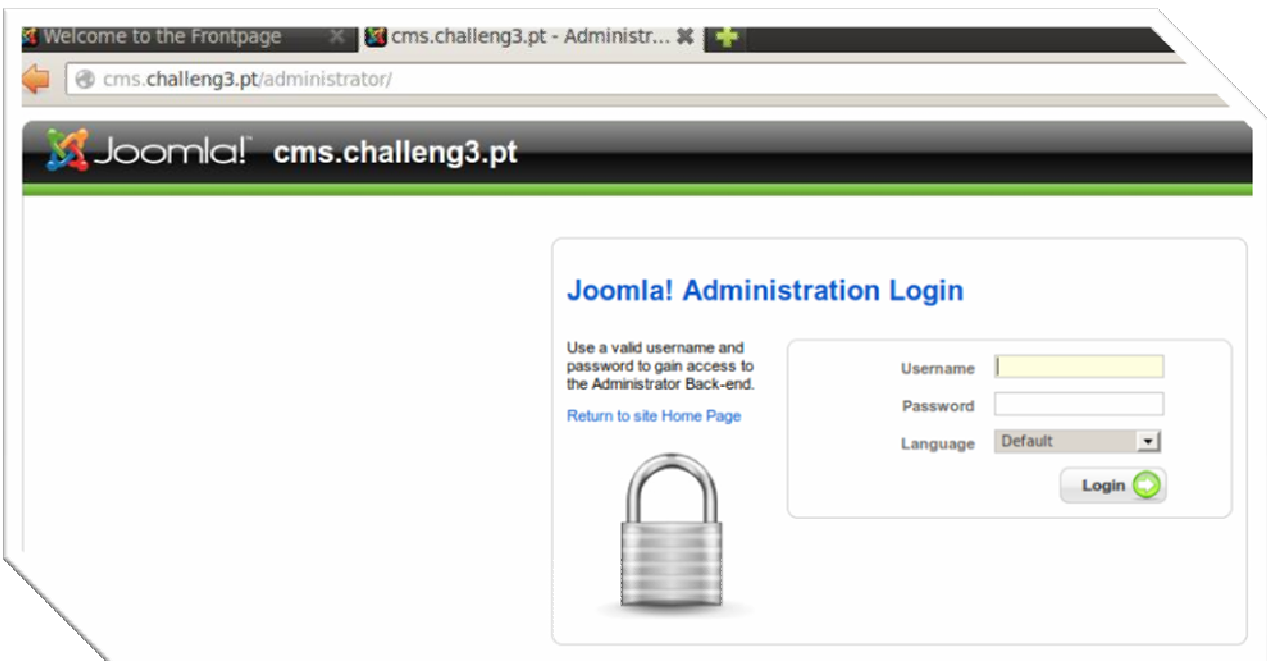
First, let’s edit the file configuration.php and paste into there the php code from the webpage. Then change the ownership of all files and folders to Apache. Last move the installation folder.

```
[root@localhost html]# vi configuration.php
[root@localhost html]# chown -R apache:apache *
#mv installation/ old
```

Point the browser to the <http://cms.challeng3.local> and you should see a similar picture :



And point to the administration interface <http://cms.challeng3.local/administrator> where you should see a screen similar to the following one :



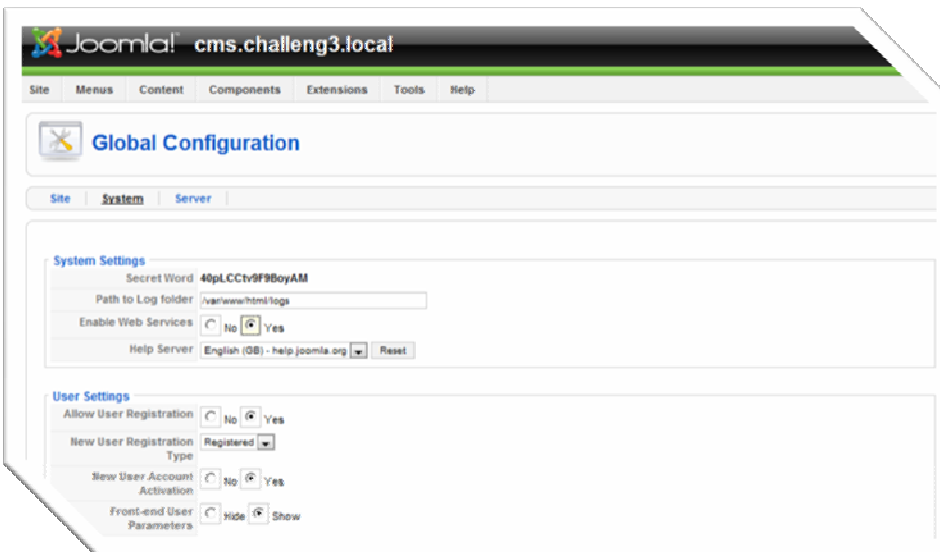
With this, the Joomla installation is complete. Let's proceed with the VirtueMart installation.

5. VirtueMart Installation

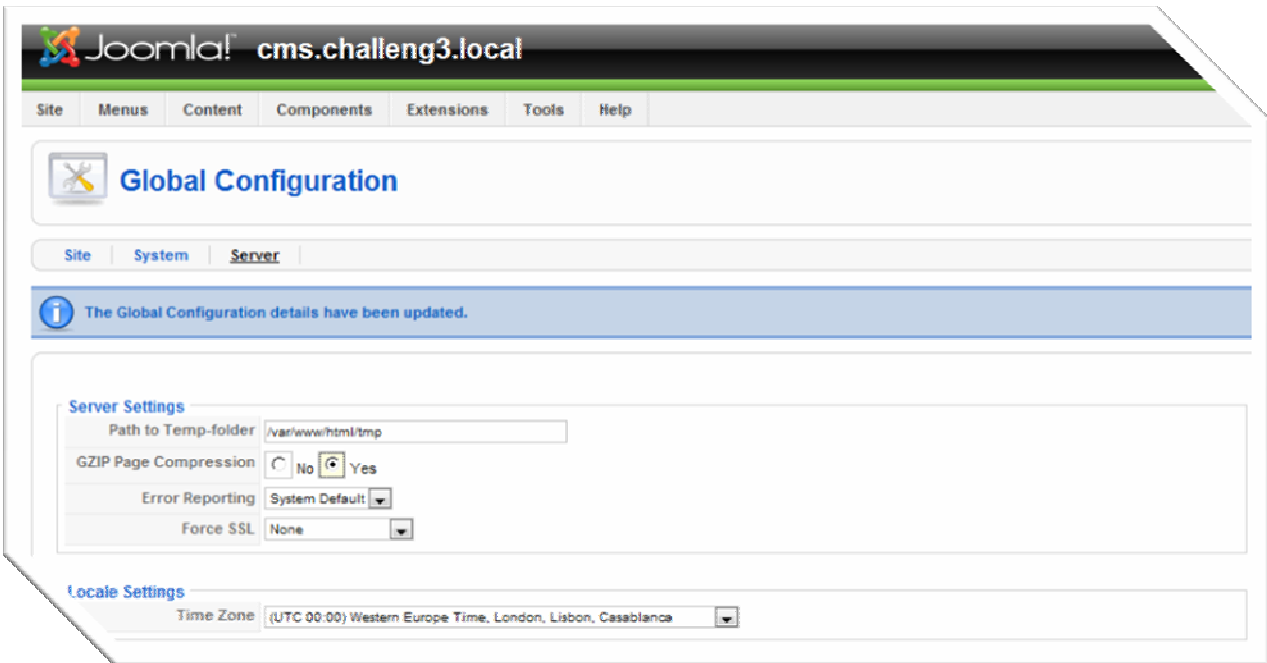
```
#cd /tmp
[root@localhost tmp]# wget http://dev.virtuemart.net/attachments/download/18/VirtueMart_1.1.4-
COMPLETE_PACKAGE.j15.zip
--08:36:11-- http://dev.virtuemart.net/attachments/download/18/VirtueMart_1.1.4-
COMPLETE_PACKAGE.j15.zip
Resolving dev.virtuemart.net... 109.234.218.67
Connecting to dev.virtuemart.net|109.234.218.67|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2283464 (2.2M) [application/x-zip-compressed]
Saving to: `VirtueMart_1.1.4-COMPLETE_PACKAGE.j15.zip'
100%[=====>]
2,283,464 1.57M/s in 1.4s
08:36:12 (1.57 MB/s) - `VirtueMart_1.1.4-COMPLETE_PACKAGE.j15.zip' saved [2283464/2283464]

[root@localhost tmp]# unzip VirtueMart_1.1.4-COMPLETE_PACKAGE.j15.zip
Archive:  VirtueMart_1.1.4-COMPLETE_PACKAGE.j15.zip
  inflating: VirtueMart_1.1_Installation.pdf
  inflating: com_virtuemart_1.1.4.j15.zip
    creating: modules/
  inflating: modules/mod_product_categories_1.1.4.j15.zip
  inflating: modules/mod_productscroller_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_cart_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_currencies_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_featureprod_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_latestprod_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_login_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_manufacturers_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_randomprod_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_search_1.1.4.j15.zip
  inflating: modules/mod_virtuemart_topten_1.1.4.j15.zip
    creating: plugins/
  inflating: plugins/vmproductsnapshots_1.1.4.j15.zip
  inflating: plugins/vmxsearch.plugin_1.1.4.j15.zip
```

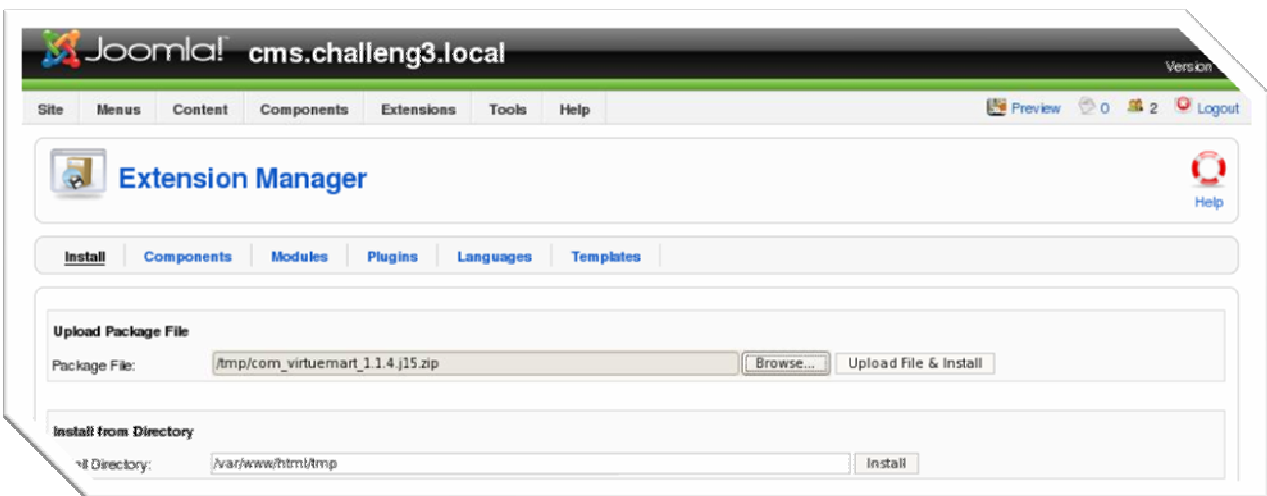
Login in to the Joomla administrator portal. Navigate to Site – Global Configuration – System.
Here click on Yes to Enable Web Services



On the Server tab, enable the Gzip Page Compression.



Navigate to Extensions – Install/Uninstall and browse the file com_virtuemart_1.1.4.j15.zip and click on install



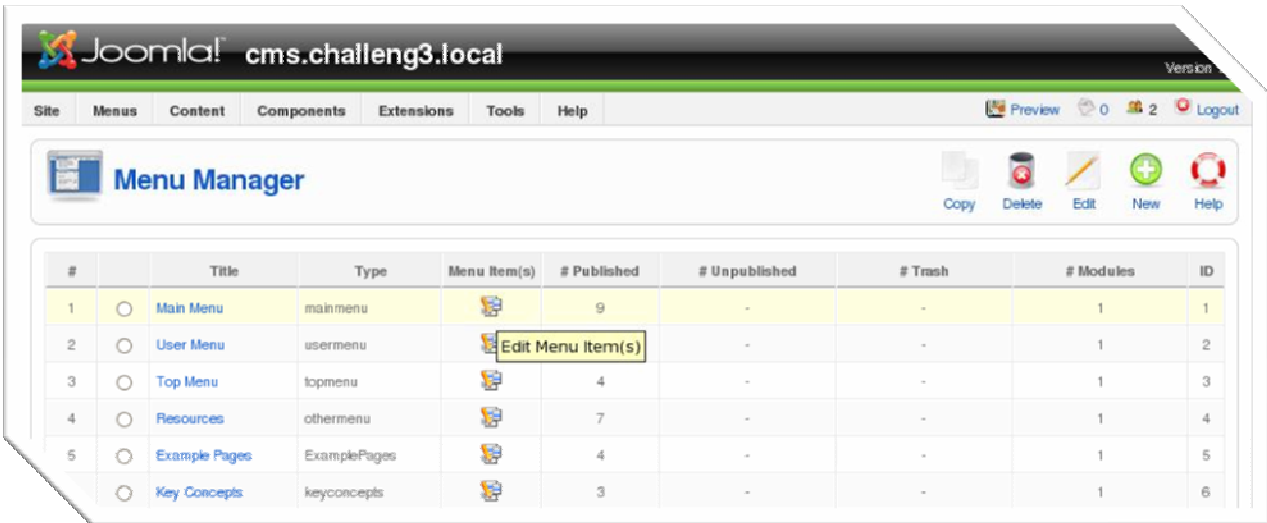
A screen showing that the VirtueMart Installation was successful should show.



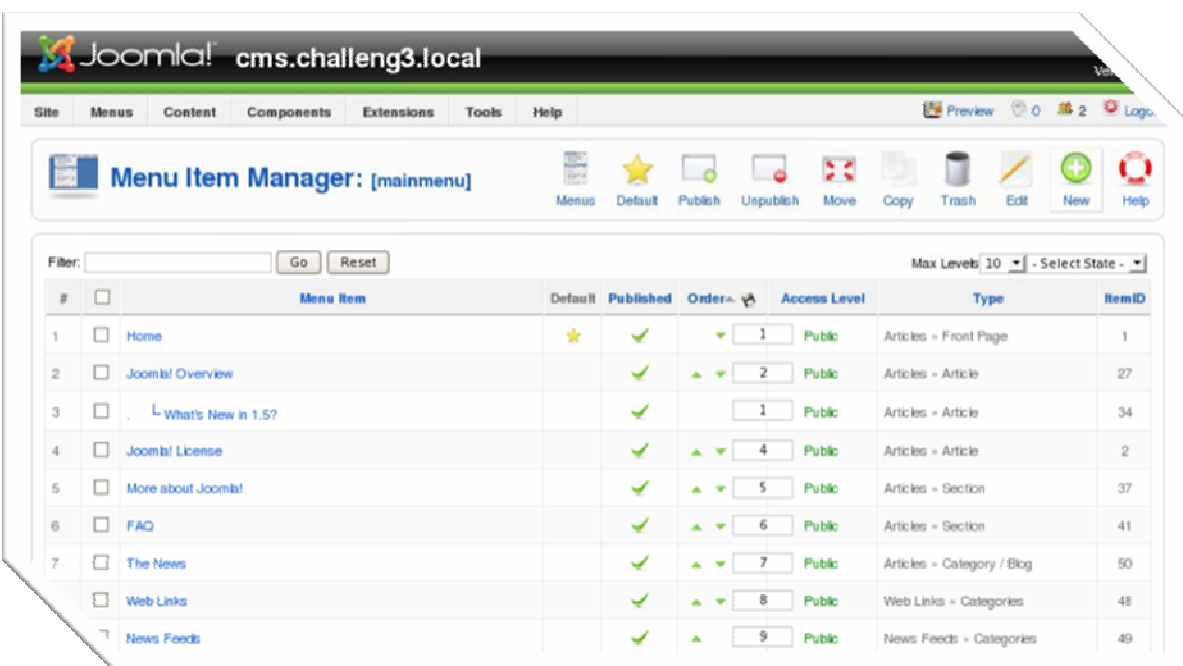
Then you need to repeat these step in order to install the following modules and plugins for VirtueMart. These files are on the extracted folder of VirtueMart.

```
mod_virtuemart_topten_1.1.4.j15.zip
mod_virtuemart_search_1.1.4.j15.zip
mod_virtuemart_randomprod_1.1.4.j15.zip
mod_virtuemart_manufacturers_1.1.4.j15.zip
mod_virtuemart_login_1.1.4.j15.zip
mod_virtuemart_latestprod_1.1.4.j15.zip
mod_virtuemart_featureprod_1.1.4.j15.zip
mod_virtuemart_currencies_1.1.4.j15.zip
mod_virtuemart_cart_1.1.4.j15.zip
mod_virtuemart_1.1.4.j15.zip
mod_productscroller_1.1.4.j15.zip
mod_product_categories_1.1.4.j15.zip
vmxsearch.plugin_1.1.4.j15.zip
vmproductsnapshots_1.1.4.j15.zip
```

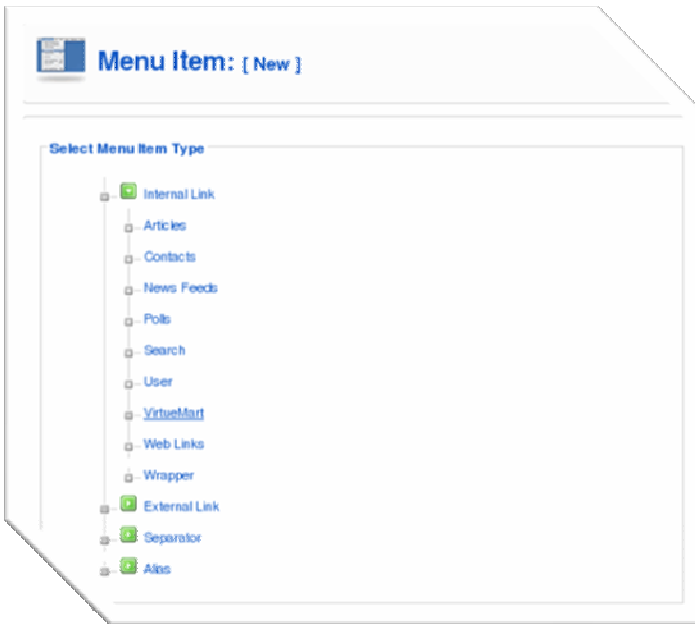
Then navigate to Menus - Menu Manager – click on the Menu Item under Main Menu.



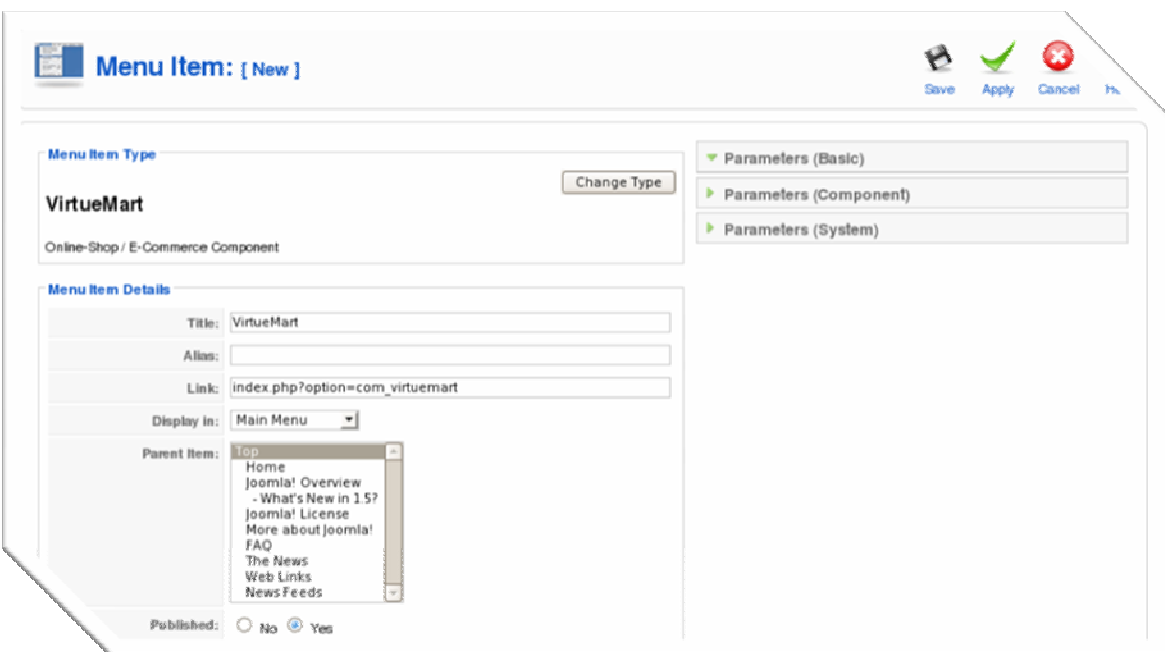
On the Menu Item Manager, Click New



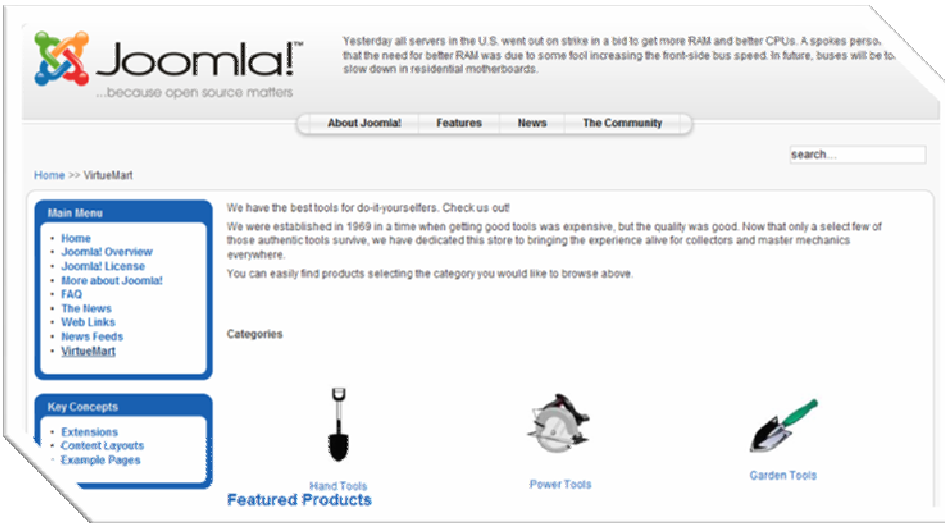
Select "VirtueMart"



Fill the Title settings and Apply and Save.



Navigate to the website and on the left menu you should have a VirtueMart link. Click on it and you should see the sample data.



Your simulated environment should now be ready for testing and practice your network security skills.