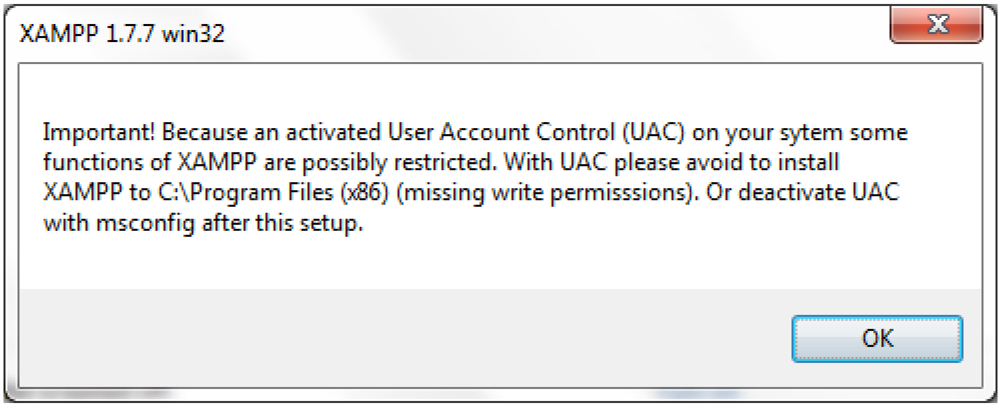
XAMPP Installation

1. **Download XAMPP from http://www.apachefriends.org/en/xampp.html**

2. **XAMPP for Windows exists in three different flavors. The "Installer" version is "probably the most comfortable way to install XAMPP" according to the XAMPP website.**

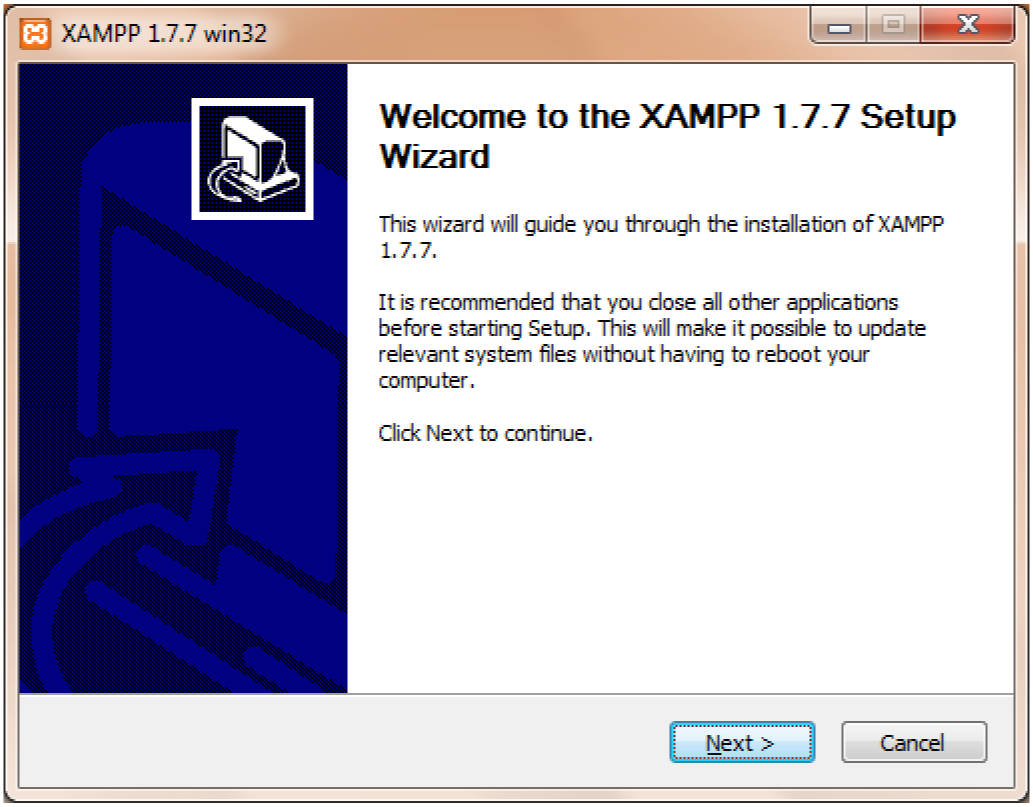
3. **Start the XAMPP installation**

4. **Note that Windows 7 will warn that installing to the Program Files directory will keep XAMPP from being able to write to its directory due to UAC. Disabling UAC is not recommended. XAMPP can be installed to C:\XAMPP to avoid this issue or XAMPP can be given permission to run as Administrator.**



Important! Because an activated User Account Control (UAC) on your sytem some functions of XAMPP are possibly restricted. With UAC please avoid to install XAMPP to C:\Program Files (x86) (missing write permisssions). Or deactivate UAC with msconfig after this setup.

5. **The XAMMP installation starts with a splash screen. Click "Next".**



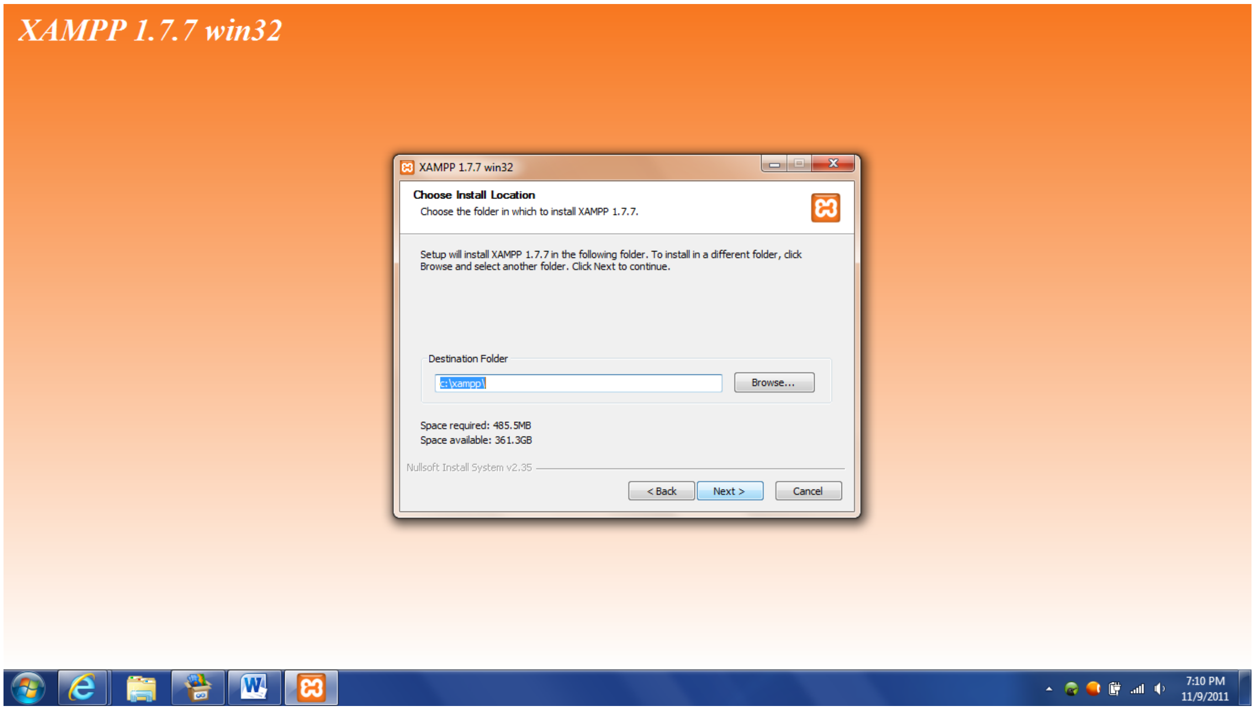
Welcome to the XAMPP 1.7.7 Setup Wizard

This wizard will guide you through the installation of XAMPP 1.7.7.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

6. **Choose which directory to install XAMPP. Installing in C:\XAMPP can make installation easier.**



Choose Install Location

Choose the folder in which to install XAMPP 1.7.7.

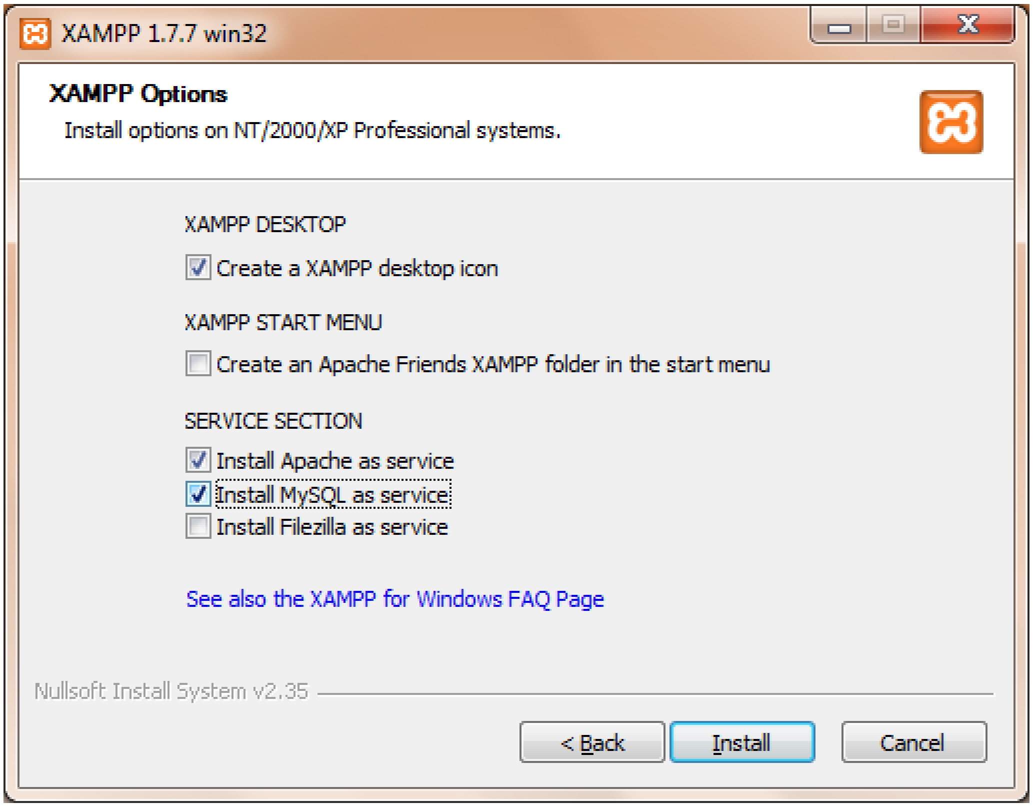
Setup will install XAMPP 1.7.7 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: c:\xampp\

Space required: 485.5MB
Space available: 361.3GB

Nullsoft Install System v2.35

7. **Installing Apache and MySQL as a service can give more options for running XAMPP when desired. When installed as services, the “services.msc” snap-in can be used to set the services to run “manually”. Running XAMPP services manually can help prevent opening security holes accidentally.**



XAMPP Options

Install options on NT/2000/XP Professional systems.

XAMPP DESKTOP

☑ Create a XAMPP desktop icon

XAMPP START MENU

□ Create an Apache Friends XAMPP folder in the start menu

SERVICE SECTION

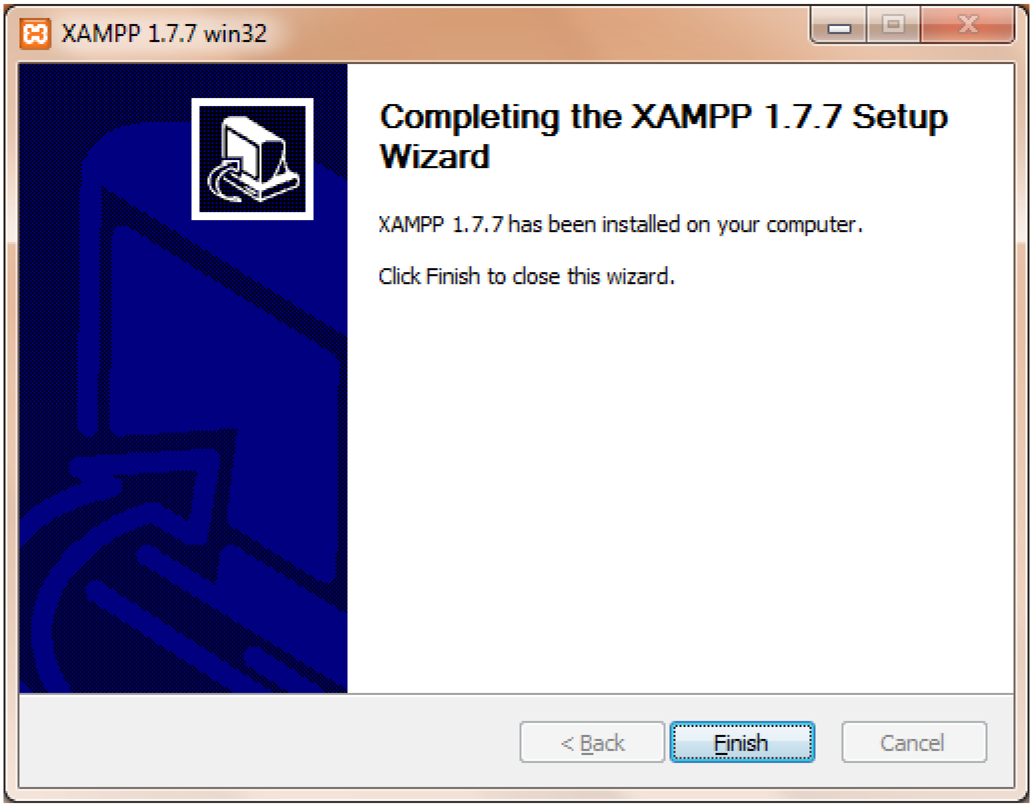
☑ Install Apache as service

☑ Install MySQL as service

□ Install Filezilla as service

See also the XAMPP for Windows FAQ Page

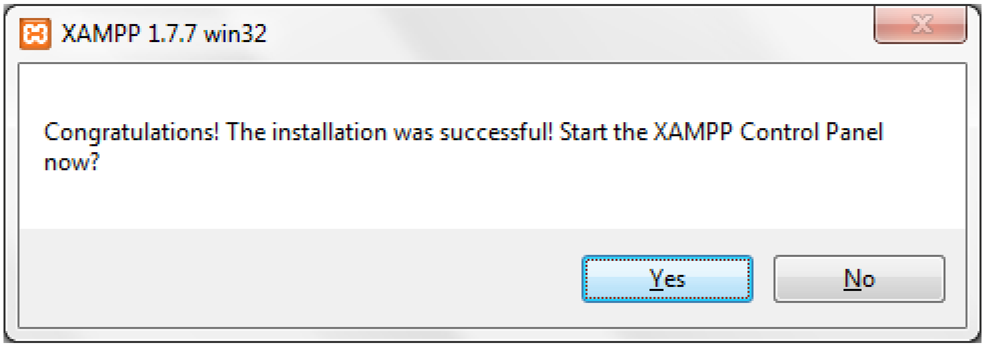
8. **Complete the installation. It may take a while.**



Completing the XAMPP 1.7.7 Setup Wizard

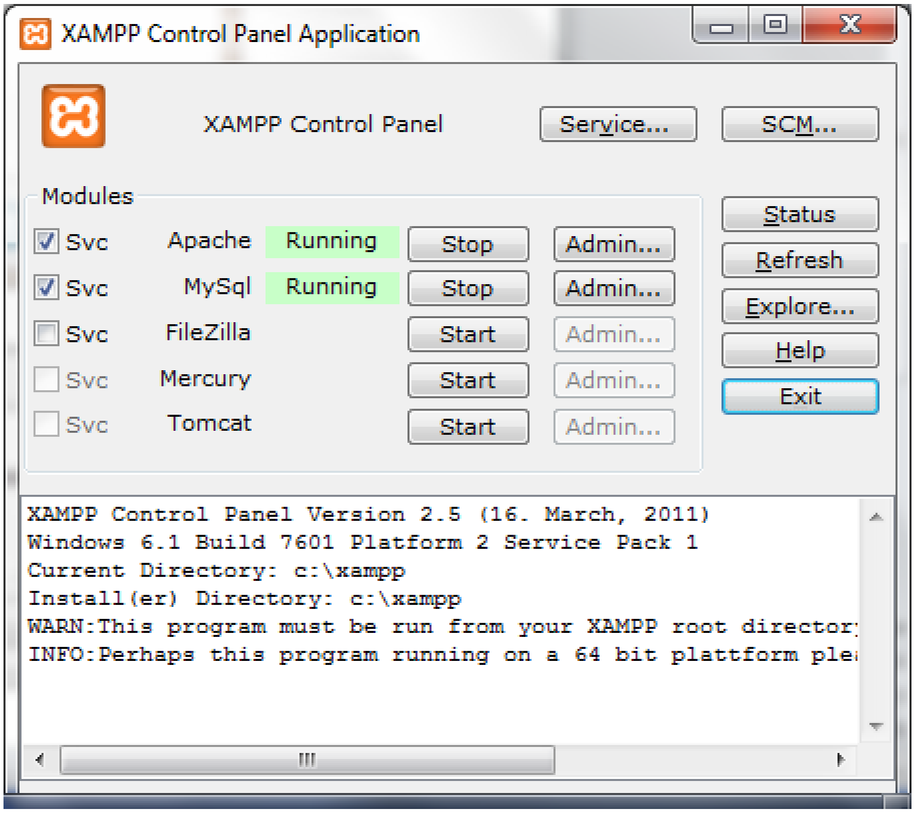
XAMPP 1.7.7 has been installed on your computer.

Click Finish to close this wizard.



Congratulations! The installation was successful! Start the XAMPP Control Panel now?

9. **The XAMPP installation completes. The XAMPP control panel can be started. In Windows, using services.msc can be used to control Apache and MySQL as long as they are installed as a service.**

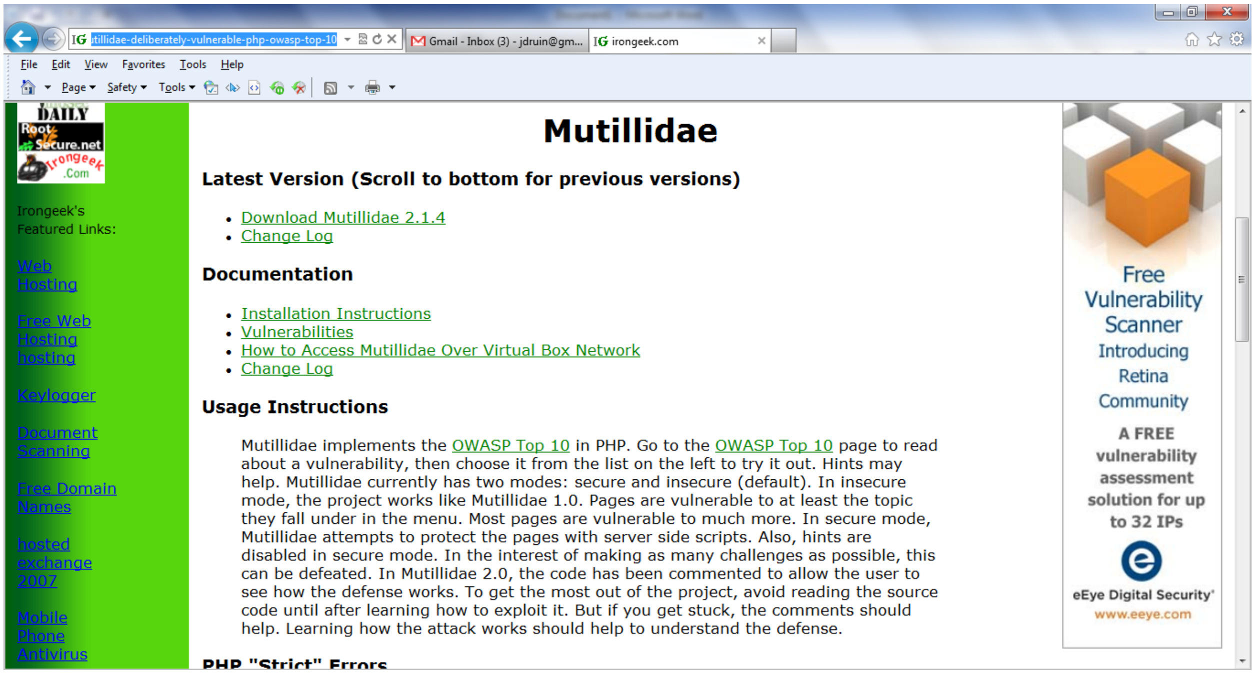


☑ Svc Apache Running Stop
☑ Svc MySql Running Stop
□ Svc FileZilla Start
□ Svc Mercury Start
□ Svc Tomcat Start

```
XAMPP Control Panel Version 2.5 (16. March, 2011)
Windows 6.1 Build 7601 Platform 2 Service Pack 1
Current Directory: c:\xampp
Install(er) Directory: c:\xampp
WARN:This program must be run from your XAMPP root director
INFO:Perhaps this program running on a 64 bit plattform ple
```

10. **Note that the XAMPP installation contains a folder named “htdocs”. For example, if XAMPP is installed to “C:\xampp” then there is an htdocs directory located at “C:\xampp\htdocs”. The “htdocs” folder is where web applications are placed.**

11. **Download Mutillidae files from Irongeek. (URL as of this writing is http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10)**



tillidae-deliberately-vulnerable-php-owasp-top-10
Gmail - Inbox (3) - jdruin@gm...
irongeek.com
File Edit View Favorites Tools Help
Page Safety Tools
DAILY
Root
Secure.net
Irongeek
.Com
Irongeek's Featured Links:
Web Hosting
Free Web Hosting hosting
Keylogger
Document Scanning
Free Domain Names
hosted exchange 2007
Mobile Phone Antivirus
Free Vulnerability Scanner
Introducing Retina Community
A FREE vulnerability assessment solution for up to 32 IPs
eEye Digital Security
www.eeye.com

Mutillidae

Latest Version (Scroll to bottom for previous versions)

- Download Mutillidae 2.1.4
- Change Log

Documentation

- Installation Instructions
- Vulnerabilities
- How to Access Mutillidae Over Virtual Box Network
- Change Log

Usage Instructions

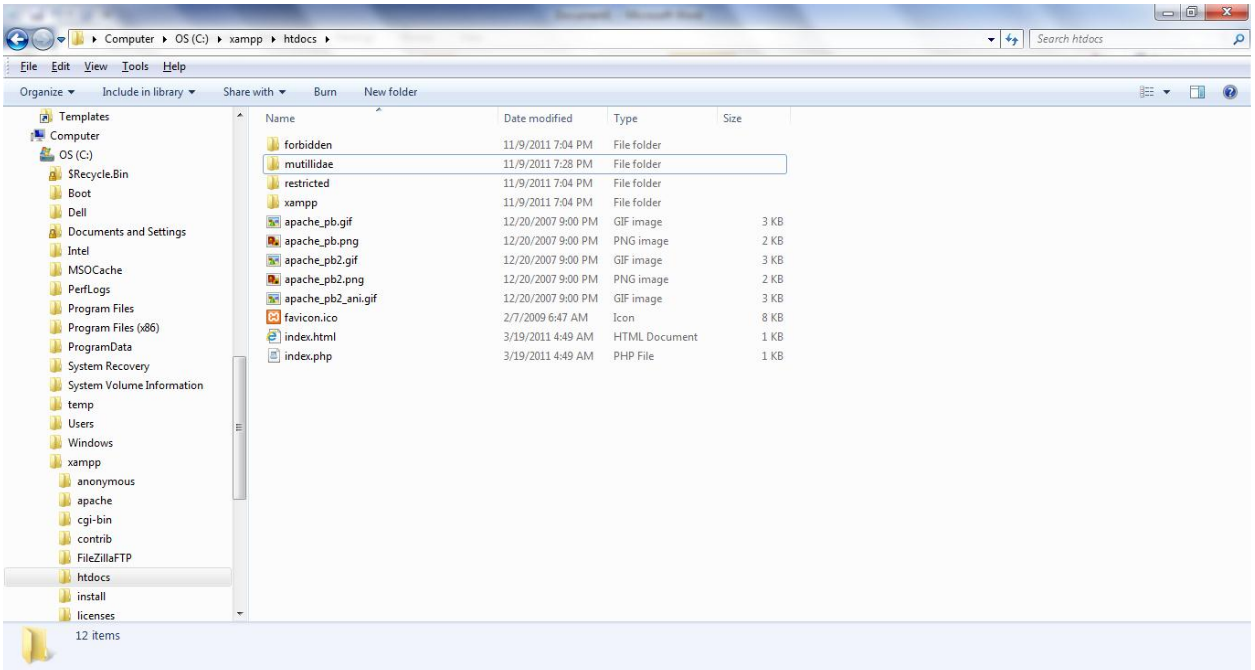
Mutillidae implements the OWASP Top 10 in PHP. Go to the OWASP Top 10 page to read about a vulnerability, then choose it from the list on the left to try it out. Hints may help. Mutillidae currently has two modes: secure and insecure (default). In insecure mode, the project works like Mutillidae 1.0. Pages are vulnerable to at least the topic they fall under in the menu. Most pages are vulnerable to much more. In secure mode, Mutillidae attempts to protect the pages with server side scripts. Also, hints are disabled in secure mode. In the interest of making as many challenges as possible, this can be defeated. In Mutillidae 2.0, the code has been commented to allow the user to see how the defense works. To get the most out of the project, avoid reading the source code until after learning how to exploit it. But if you get stuck, the comments should help. Learning how the attack works should help to understand the defense.

PHP "Strict" Errors

12. **Unzip the Mutillidae download.**

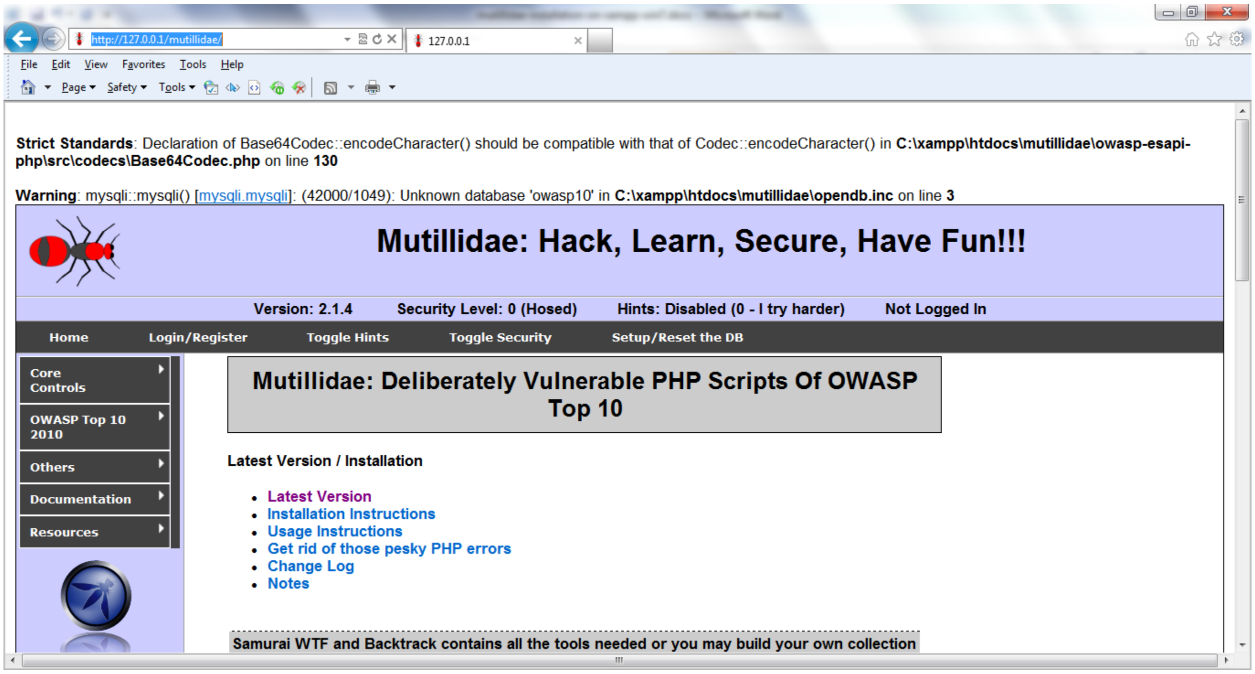
13. **The download contain a single folder named Mutillidae. Leave all the files in this single folder.**

14. Copy the entire Mutillidae folder to the XAMPP htdocs directory. For example, if XAMPP is installed to "C:\xampp" then there is an htdocs directory located at "C:\xampp\htdocs".In this example, copy the mutillidae folder into "C:\xampp\htdocs".



Name	Date modified	Type	Size
forbidden	11/9/2011 7:04 PM	File folder	
mutillidae	11/9/2011 7:28 PM	File folder	
restricted	11/9/2011 7:04 PM	File folder	
xampp	11/9/2011 7:04 PM	File folder	
apache_pb.gif	12/20/2007 9:00 PM	GIF image	3 KB
apache_pb.png	12/20/2007 9:00 PM	PNG image	2 KB
apache_pb2.gif	12/20/2007 9:00 PM	GIF image	3 KB
apache_pb2.png	12/20/2007 9:00 PM	PNG image	2 KB
apache_pb2_ani.gif	12/20/2007 9:00 PM	GIF image	3 KB
favicon.ico	2/7/2009 6:47 AM	Icon	8 KB
index.html	3/19/2011 4:49 AM	HTML Document	1 KB
index.php	3/19/2011 4:49 AM	PHP File	1 KB

15. Open a browser and browse to http://127.0.0.1/mutillidae/



Strict Standards: Declaration of Base64Codec::encodeCharacter() should be compatible with that of Codec::encodeCharacter() in **C:\xampp\htdocs\mutillidae\owasp-esapi-php\src\codecs\Base64Codec.php** on line **130**

Warning: mysqli::mysqli() [mysqli.mysqli]: (42000/1049): Unknown database 'owasp10' in **C:\xampp\htdocs\mutillidae\opendb.inc** on line **3**

Mutillidae: Hack, Learn, Secure, Have Fun!!!

Version: 2.1.4 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

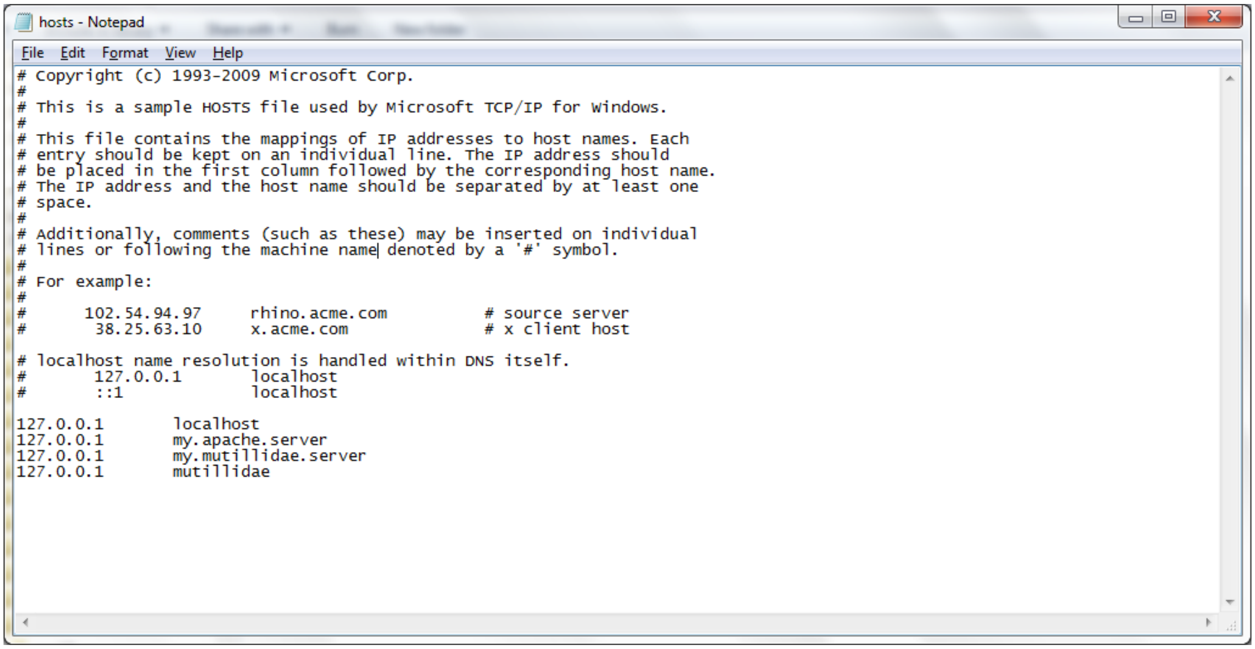
Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

16. **You may add "localhost 127.0.0.1" to your hosts file so you can browse to http://localhost/mutillidae/ instead**

17. **While your in the hosts file, it might be cool to add "my.mutillidae.server 127.0.0.1" to your hosts file (or whatever) so you can browse to http://my.mutillidae.server/mutillidae/. In Win7, do forget to start Notepad as Administrator or you will not be able to save. Again, disabling UAC is not best practice.**



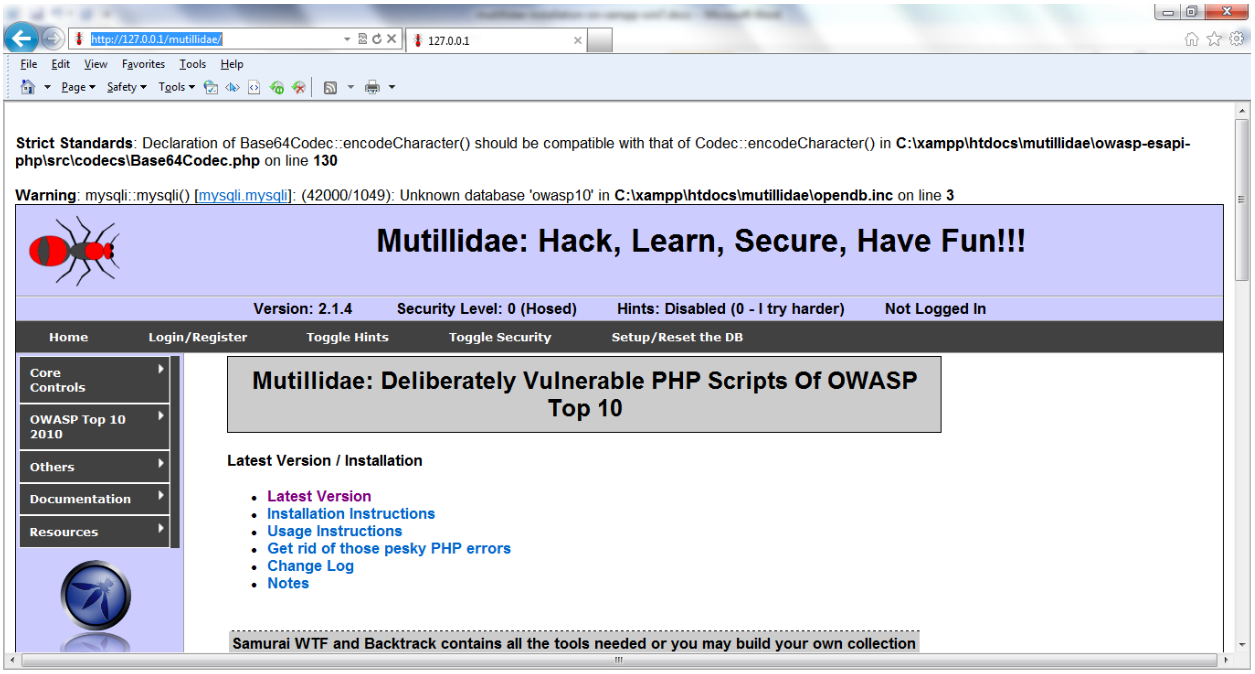
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1       localhost
127.0.0.1       my.apache.server
127.0.0.1       my.mutillidae.server
127.0.0.1       mutillidae
```

18. **By default, Mutillidae only allows access from localhost (127.*.*.*) and 192.168.*.*. Edit the .htaccess file to change this behavior (not recommended on a public network). The .htaccess file is in the mutillidae folder.**

19. Note those pesky PHP errors



Strict Standards: Declaration of Base64Codec::encodeCharacter() should be compatible with that of Codec::encodeCharacter() in **C:\xampp\htdocs\mutillidae\owasp-esapi-php\src\codecs\Base64Codec.php** on line **130**

Warning: mysqli::mysqli() [mysqli.mysqli]: (42000/1049): Unknown database 'owasp10' in **C:\xampp\htdocs\mutillidae\opendb.inc** on line **3**

Mutillidae: Hack, Learn, Secure, Have Fun!!!

Version: 2.1.4 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

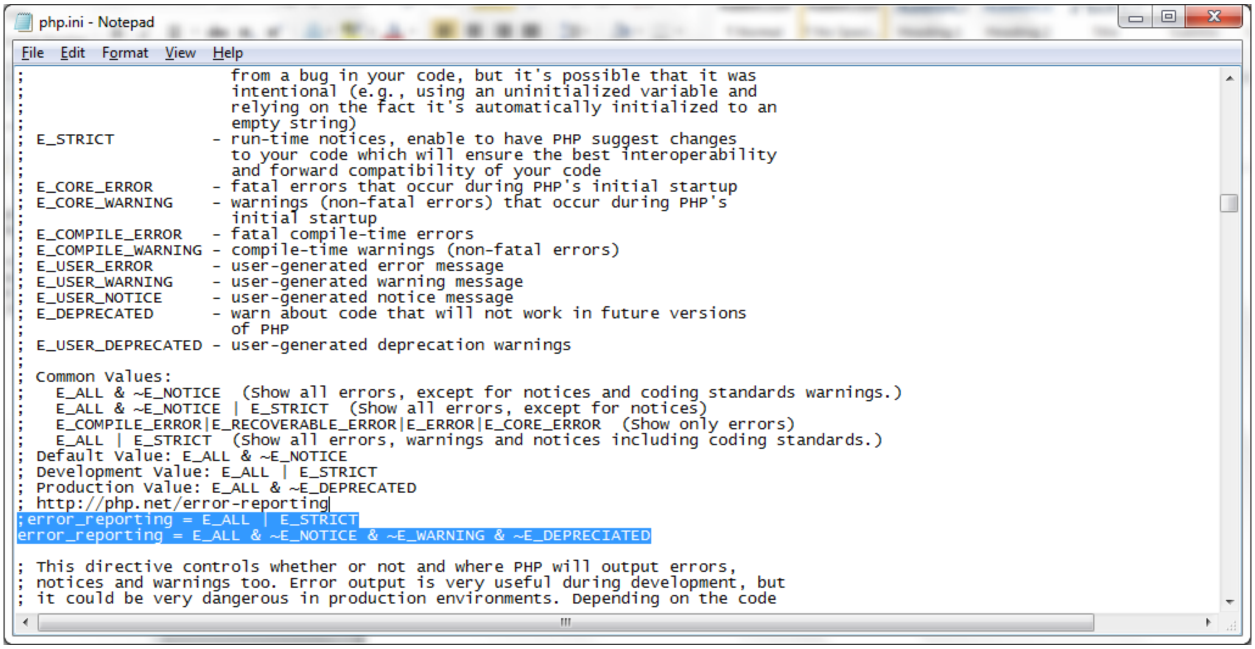
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

20. Get rid of PHP "strict" errors.

a. They are not compatible with the OWASP ESAPI classes in use in Mutillidae 2.0. The error modifies headers disrupting functionality so this is not simply an annoyance issue. To do this, go to the PHP.INI file and change the line that reads "error_reporting = E_ALL | E_STRICT" to "error_reporting = E_ALL & ~E_NOTICE & ~E_WARNING & ~E_DEPRECIATED". Once the modification is complete, restart the Apache service. If you are not sure how to restart the service, reboot.

   Important note: If you use XAMPP Lite or various version of XAMPP on various operating systems, the path for your php.ini file may vary. You may even have multiple php.ini files in which case try to modify the one in the Apache directory first, then the one in the PHP file if that doesnt do the trick.

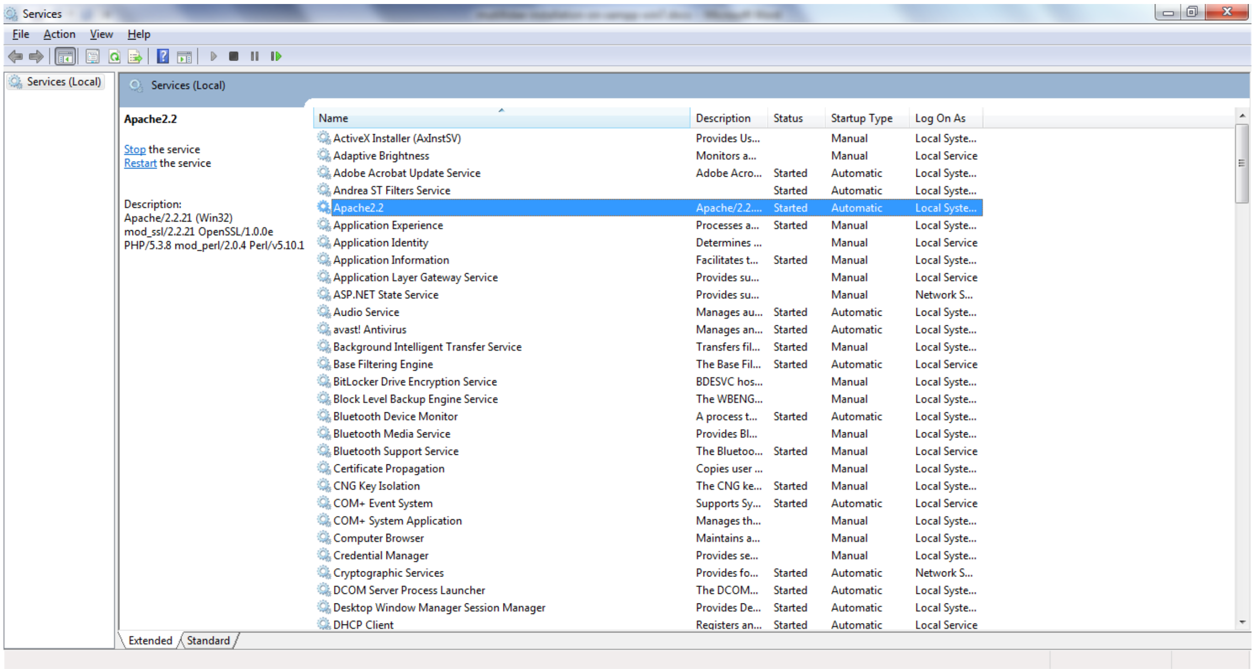
   Windows possible default location C:\xampp\php\php.ini, C:\XamppLite\PHP\php.ini, others Linux possible default locations: /XamppLite/PHP/php.ini, /XamppLite/apache/bin/php.ini, others



```
;                     from a bug in your code, but it's possible that it was
;                     intentional (e.g., using an uninitialized variable and
;                     relying on the fact it's automatically initialized to an
;                     empty string)
; E_STRICT          - run-time notices, enable to have PHP suggest changes
;                     to your code which will ensure the best interoperability
;                     and forward compatibility of your code
; E_CORE_ERROR      - fatal errors that occur during PHP's initial startup
; E_CORE_WARNING    - warnings (non-fatal errors) that occur during PHP's
;                     initial startup
; E_COMPILE_ERROR   - fatal compile-time errors
; E_COMPILE_WARNING - compile-time warnings (non-fatal errors)
; E_USER_ERROR      - user-generated error message
; E_USER_WARNING    - user-generated warning message
; E_USER_NOTICE     - user-generated notice message
; E_DEPRECATED      - warn about code that will not work in future versions
;                     of PHP
; E_USER_DEPRECATED - user-generated deprecation warnings
;
; Common Values:
;   E_ALL & ~E_NOTICE  (Show all errors, except for notices and coding standards warnings.)
;   E_ALL & ~E_NOTICE | E_STRICT  (Show all errors, except for notices)
;   E_COMPILE_ERROR|E_RECOVERABLE_ERROR|E_ERROR|E_CORE_ERROR  (Show only errors)
;   E_ALL | E_STRICT  (Show all errors, warnings and notices including coding standards.)
; Default Value: E_ALL & ~E_NOTICE
; Development Value: E_ALL | E_STRICT
; Production Value: E_ALL & ~E_DEPRECATED
; http://php.net/error-reporting
;error_reporting = E_ALL | E_STRICT
error_reporting = E_ALL & ~E_NOTICE & ~E_WARNING & ~E_DEPRECIATED

; This directive controls whether or not and where PHP will output errors,
; notices and warnings too. Error output is very useful during development, but
; it could be very dangerous in production environments. Depending on the code
```

21. **If Apache is installed as a service, it can be restarted using services.msc. Right click the Apache service and choose “restart”.**

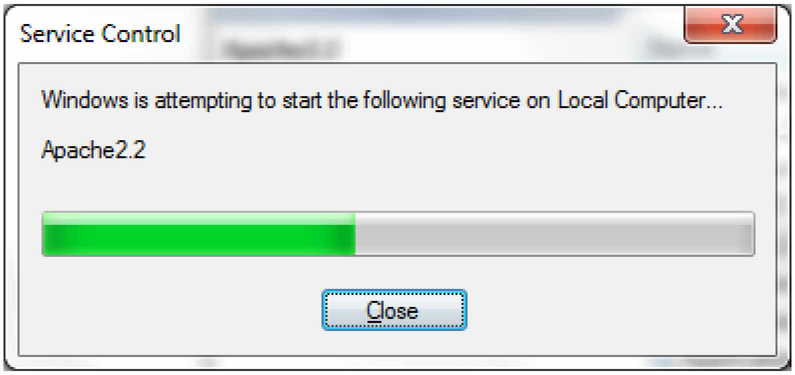


Apache2.2

Stop the service
Restart the service

Description:
Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1

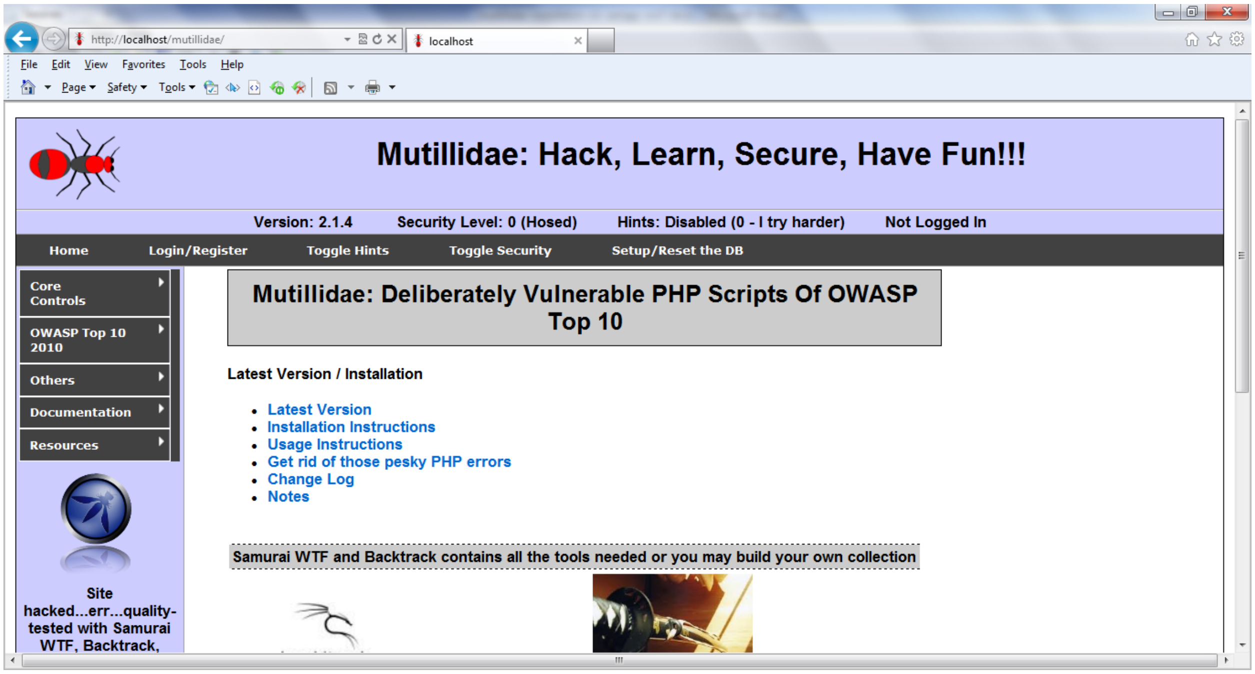
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adaptive Brightness	Monitors a...		Manual	Local Service
Adobe Acrobat Update Service	Adobe Acro...	Started	Automatic	Local Syste...
Andrea ST Filters Service		Started	Automatic	Local Syste...
Apache2.2	Apache/2.2....	Started	Automatic	Local Syste...
Application Experience	Processes a...	Started	Manual	Local Syste...
Application Identity	Determines ...		Manual	Local Service
Application Information	Facilitates t...	Started	Manual	Local Syste...
Application Layer Gateway Service	Provides su...		Manual	Local Service
ASP.NET State Service	Provides su...		Manual	Network S...
Audio Service	Manages au...	Started	Automatic	Local Syste...
avast! Antivirus	Manages an...	Started	Automatic	Local Syste...
Background Intelligent Transfer Service	Transfers fil...	Started	Manual	Local Syste...
Base Filtering Engine	The Base Fil...	Started	Automatic	Local Service
BitLocker Drive Encryption Service	BDESVC hos...		Manual	Local Syste...
Block Level Backup Engine Service	The WBENG...		Manual	Local Syste...
Bluetooth Device Monitor	A process t...	Started	Automatic	Local Syste...
Bluetooth Media Service	Provides Bl...		Manual	Local Syste...
Bluetooth Support Service	The Bluetoo...	Started	Manual	Local Service
Certificate Propagation	Copies user ...		Manual	Local Syste...
CNG Key Isolation	The CNG ke...	Started	Manual	Local Syste...
COM+ Event System	Supports Sy...	Started	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Computer Browser	Maintains a...		Manual	Local Syste...
Credential Manager	Provides se...		Manual	Local Syste...
Cryptographic Services	Provides fo...	Started	Automatic	Network S...
DCOM Server Process Launcher	The DCOM...	Started	Automatic	Local Syste...
Desktop Window Manager Session Manager	Provides De...	Started	Automatic	Local Syste...
DHCP Client	Registers an...	Started	Automatic	Local Service



Windows is attempting to start the following service on Local Computer...

Apache2.2

22. Once complete, browse to mutillidae again. The PHP errors should be gone.



Mutillidae: Hack, Learn, Secure, Have Fun!!!

Version: 2.1.4 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Site hacked...err...quality-tested with Samurai WTF, Backtrack,

23. If you are certain you have correctly configured the php.ini file and the PHP errors still show, then restart windows and try again.

24. With the Apache and MySQL services set to start “manually”, the services can be started with the “services.msc” snap-in. However, an easier way is to create a batch file to start both services. Commands can be placed in a notepad file and saved with a “.bat” extension. In Win7, this batch file will have to be run as Administrator.

25. Example batch file contents

```
echo "Starting apache 2.2 service"
net start apache2.2
echo "Started apache 2.2 service"
pause
echo "Starting MySQL service"
net start mysql
echo "Started MySQL service"
pause
```