Institut
supérieur
d'informatique

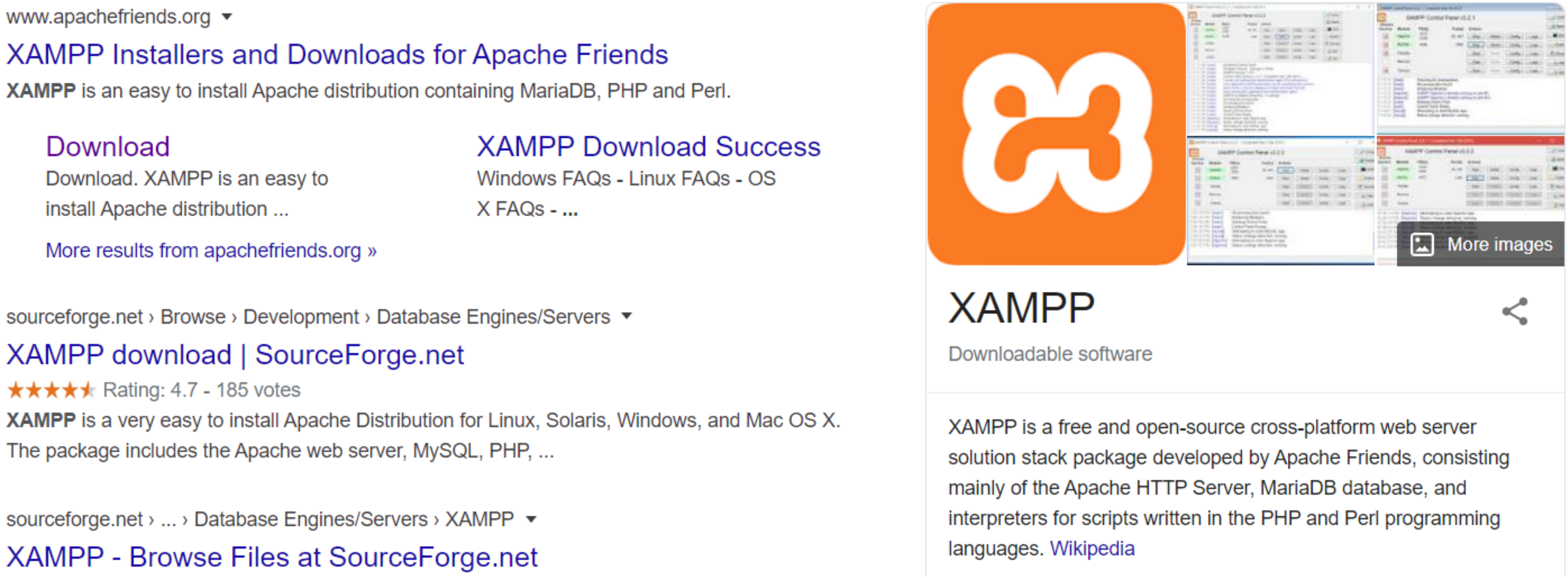
Risk and Incident Management

Amirhossein Ghasemi

March 2020

XAMPP

- ✓ XAMPP is an open source software developed by Apache friends.
- ✓ XAMPP software package contains Apache distributions for Apache server, MariaDB, PHP, and Perl.
- ✓ It is basically a local host or a local server which works on your own desktop or laptop computer.
- ✓ The use of XAMPP is to test the clients or your website before uploading it to the remote web server.
- ✓ The XAMPP server software gives you the suitable environment for testing MYSQL, PHP, Apache and Perl projects on the local computer.
- ✓ The full form of XAMPP is X stands for Cross-platform, (A) Apache server, (M) MariaDB, (P) PHP and (P) Perl. The Cross-platform usually means that it can run on any computer with any operating system.



www.apachefriends.org ▾

XAMPP Installers and Downloads for Apache Friends

XAMPP is an easy to install Apache distribution containing MariaDB, PHP and Perl.

Download

Download. XAMPP is an easy to install Apache distribution ...

XAMPP Download Success

Windows FAQs - Linux FAQs - OS X FAQs - **...**

More results from apachefriends.org »

sourceforge.net › Browse › Development › Database Engines/Servers ▾

XAMPP download | SourceForge.net

★★★★★ Rating: 4.7 - 185 votes

XAMPP is a very easy to install Apache Distribution for Linux, Solaris, Windows, and Mac OS X. The package includes the Apache web server, MySQL, PHP, ...

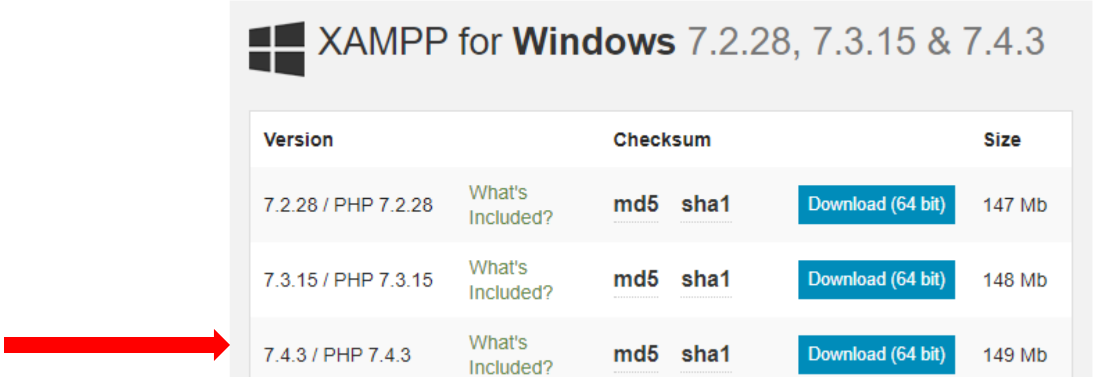
sourceforge.net › ... › Database Engines/Servers › XAMPP ▾

XAMPP - Browse Files at SourceForge.net

XAMPP

Downloadable software

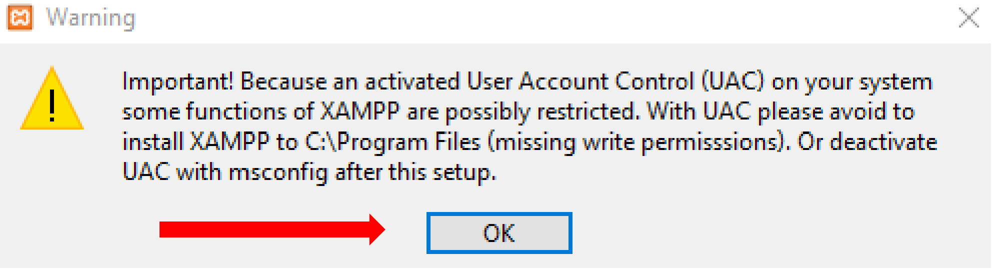
XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. Wikipedia



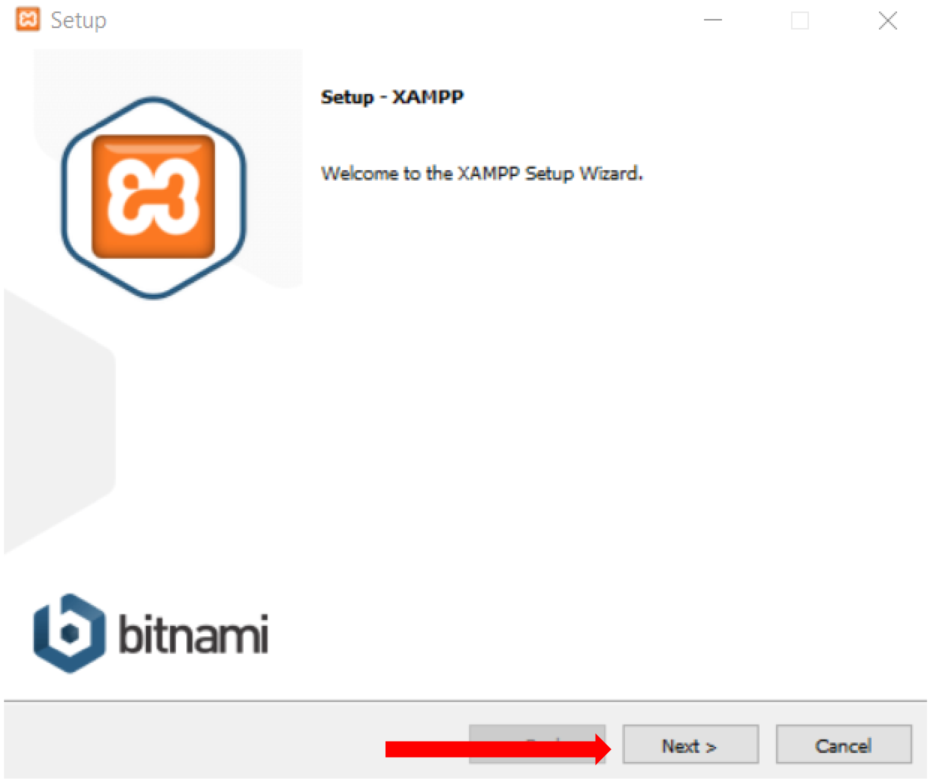
XAMPP for **Windows** 7.2.28, 7.3.15 & 7.4.3

Version		Checksum			Size
7.2.28 / PHP 7.2.28	What's Included?	md5	sha1	Download (64 bit)	147 Mb
7.3.15 / PHP 7.3.15	What's Included?	md5	sha1	Download (64 bit)	148 Mb
7.4.3 / PHP 7.4.3	What's Included?	md5	sha1	Download (64 bit)	149 Mb

Install XAMPP

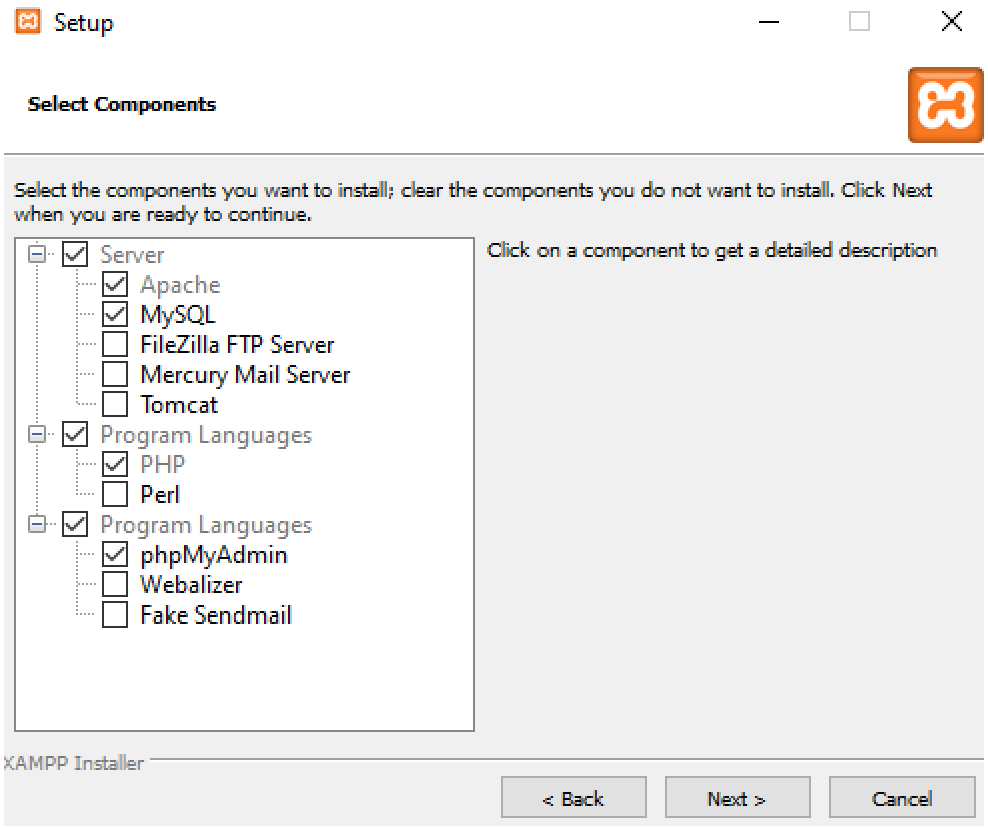


Important! Because an activated User Account Control (UAC) on your system some functions of XAMPP are possibly restricted. With UAC please avoid to install XAMPP to C:\Program Files (missing write permisssions). Or deactivate UAC with msconfig after this setup.



Setup - XAMPP

Welcome to the XAMPP Setup Wizard.



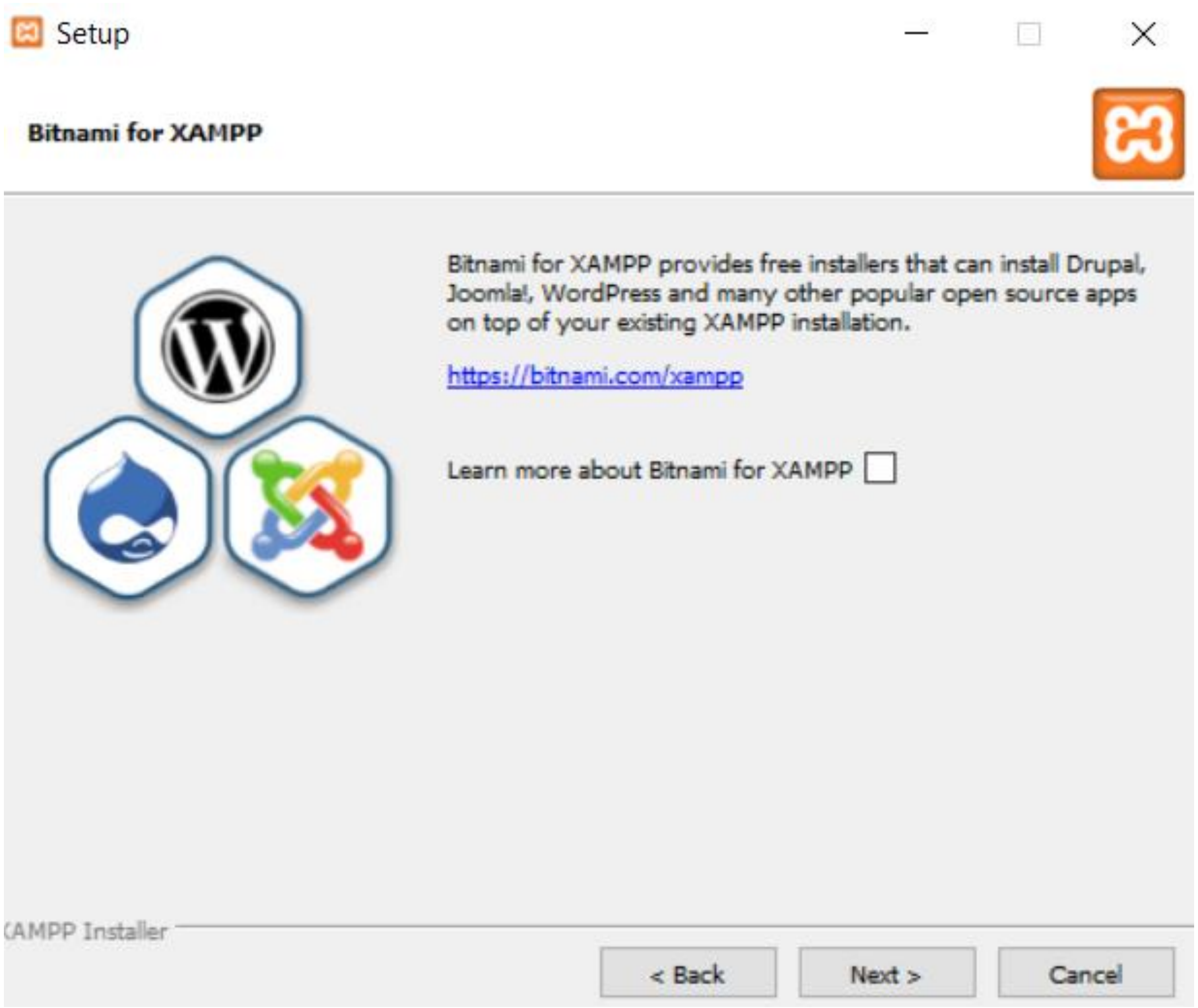
Setup

Select Components

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

- ☑ Server
  - ☑ Apache
  - ☑ MySQL
  - ☐ FileZilla FTP Server
  - ☐ Mercury Mail Server
  - ☐ Tomcat
- ☑ Program Languages
  - ☑ PHP
  - ☐ Perl
- ☑ Program Languages
  - ☑ phpMyAdmin
  - ☐ Webalizer
  - ☐ Fake Sendmail

Click on a component to get a detailed description



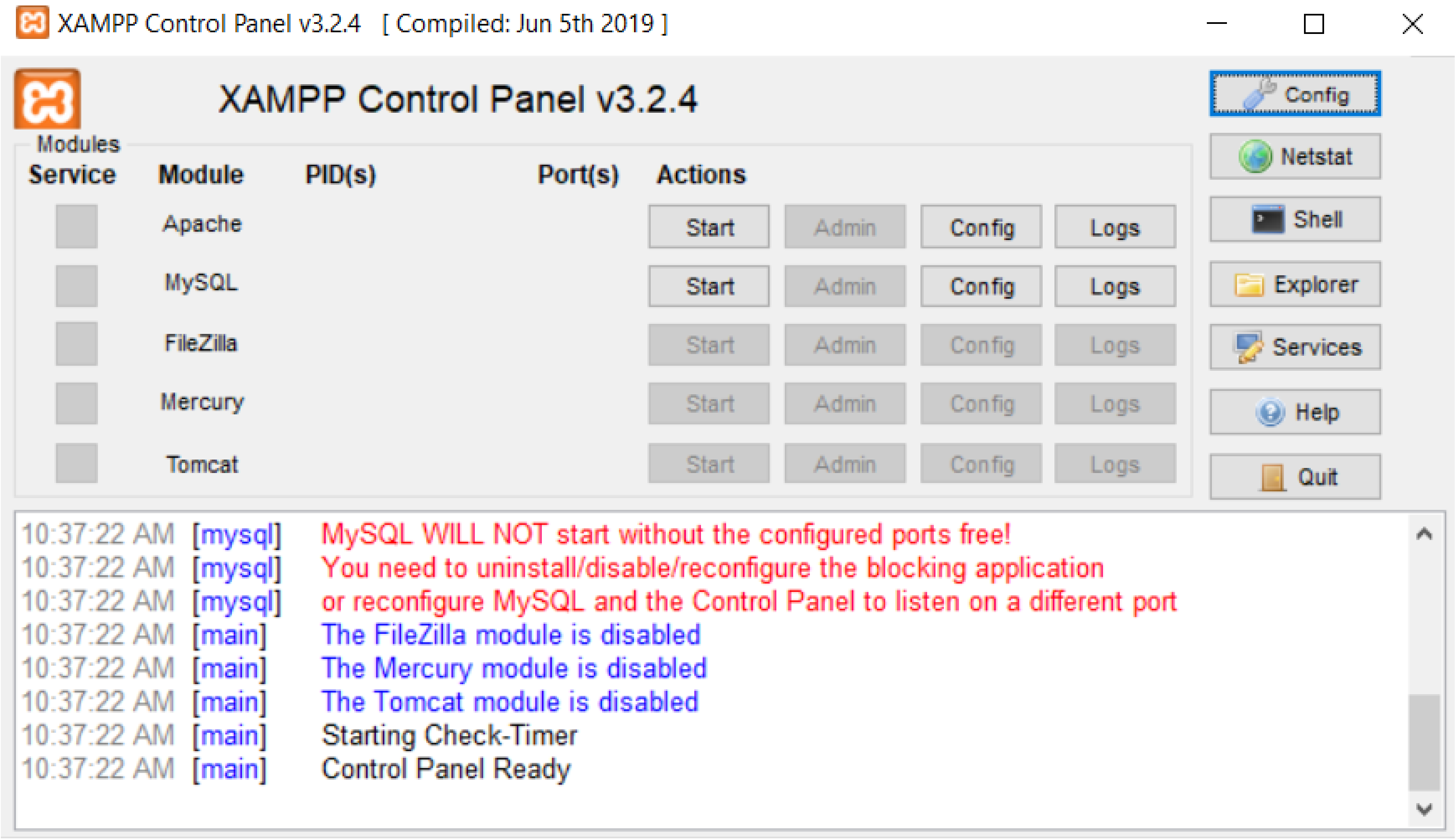
Setup

Bitnami for XAMPP

Bitnami for XAMPP provides free installers that can install Drupal, Joomla!, WordPress and many other popular open source apps on top of your existing XAMPP installation.

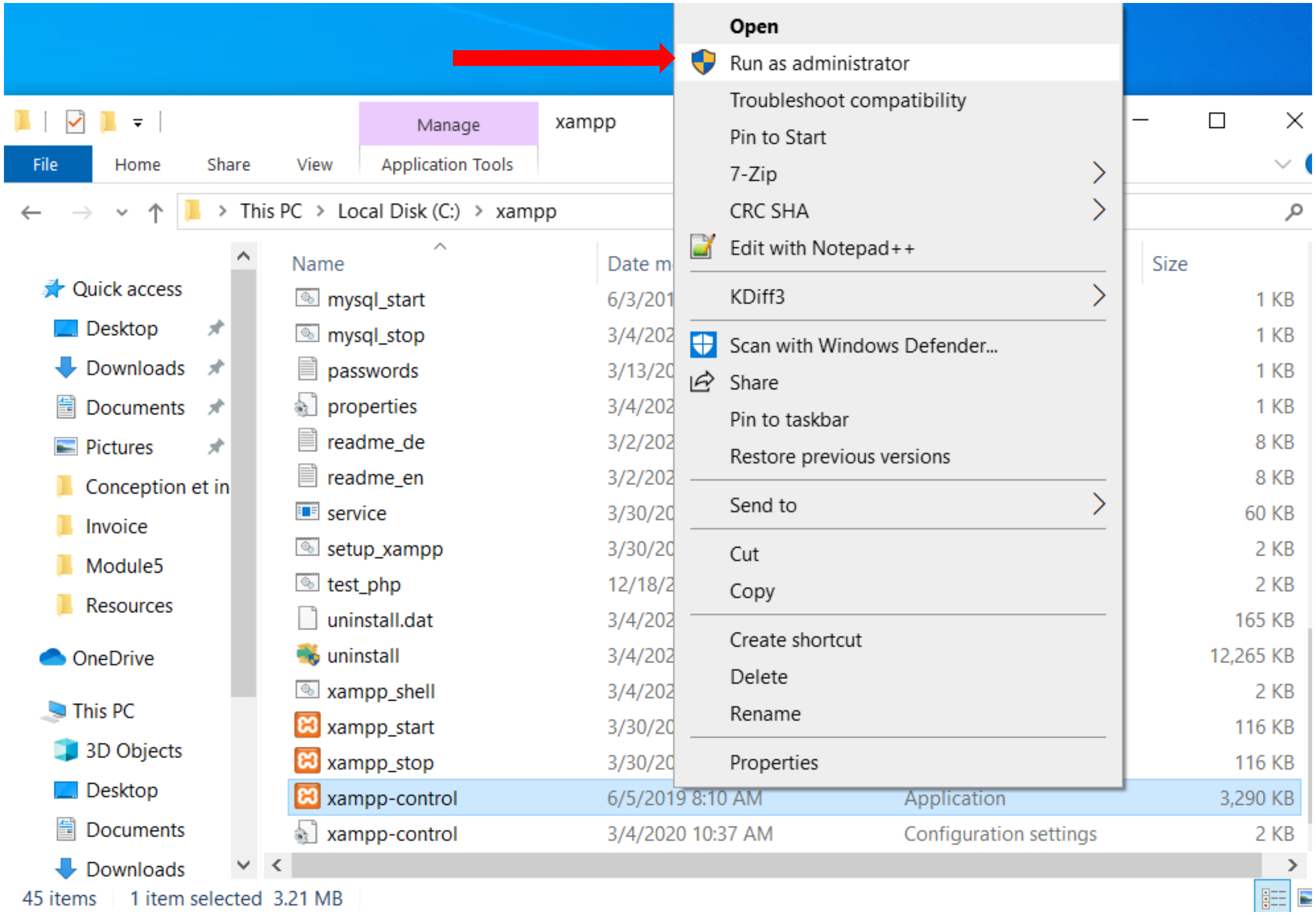
https://bitnami.com/xampp

Learn more about Bitnami for XAMPP □

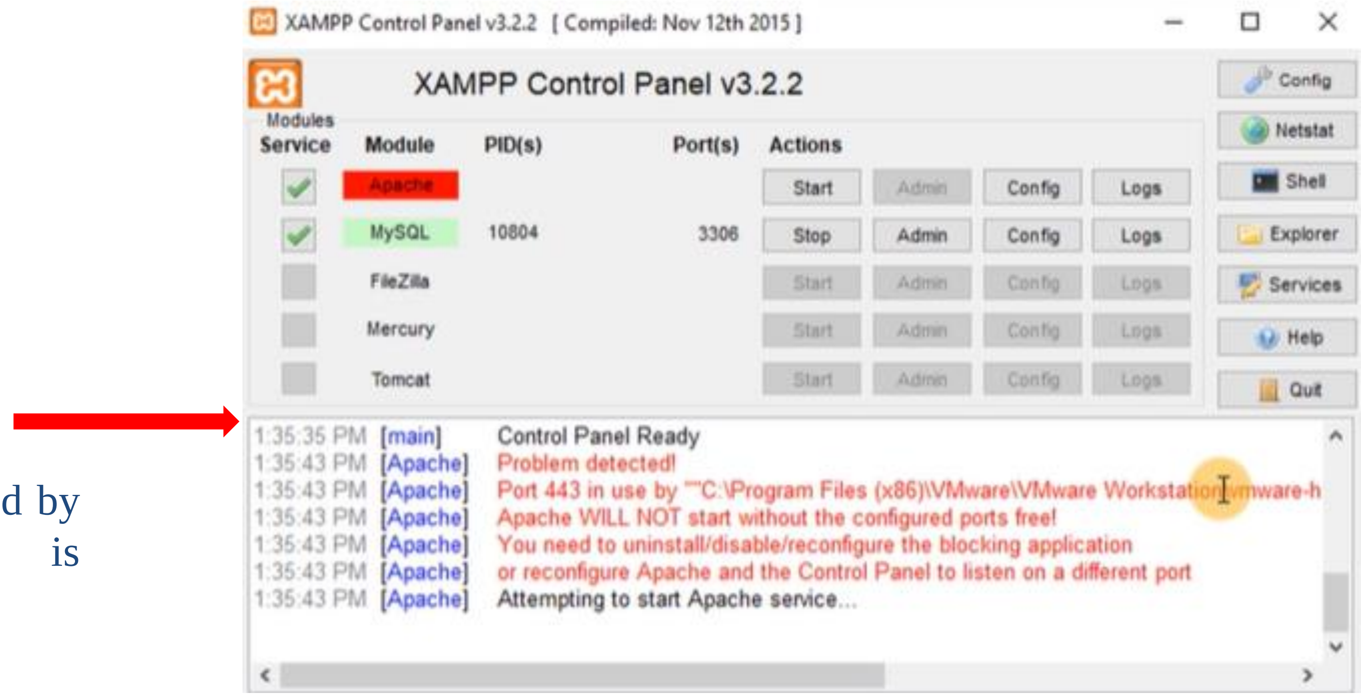


```
10:37:22 AM  [mysql]   MySQL WILL NOT start without the configured ports free!
10:37:22 AM  [mysql]   You need to uninstall/disable/reconfigure the blocking application
10:37:22 AM  [mysql]   or reconfigure MySQL and the Control Panel to listen on a different port
10:37:22 AM  [main]    The FileZilla module is disabled
10:37:22 AM  [main]    The Mercury module is disabled
10:37:22 AM  [main]    The Tomcat module is disabled
10:37:22 AM  [main]    Starting Check-Timer
10:37:22 AM  [main]    Control Panel Ready
```

Run the XAMPP as the administrator :



Name	Date m		Size
mysql_start	6/3/201		1 KB
mysql_stop	3/4/202		1 KB
passwords	3/13/20		1 KB
properties	3/4/202		1 KB
readme_de	3/2/202		8 KB
readme_en	3/2/202		8 KB
service	3/30/20		60 KB
setup_xampp	3/30/20		2 KB
test_php	12/18/2		2 KB
uninstall.dat	3/4/202		165 KB
uninstall	3/4/202		12,265 KB
xampp_shell	3/4/202		2 KB
xampp_start	3/30/20		116 KB
xampp_stop	3/30/20		116 KB
xampp-control	6/5/2019 8:10 AM	Application	3,290 KB
xampp-control	3/4/2020 10:37 AM	Configuration settings	2 KB



XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Config
Netstat
Shell
Explorer
Services
Help
Quit

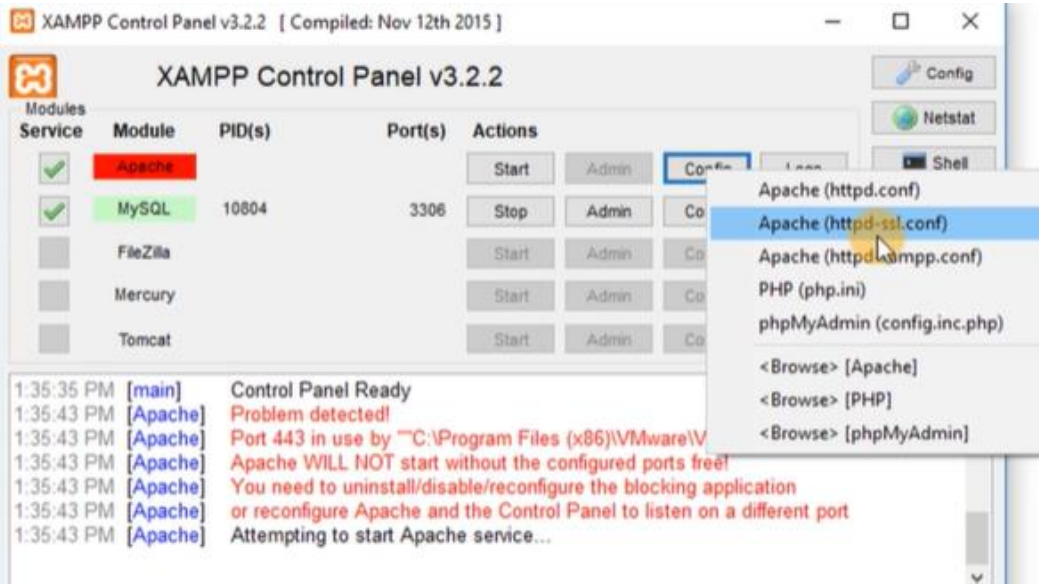
Modules Service	Module	PID(s)	Port(s)	Actions			
✓	Apache			Start	Admin	Config	Logs
✓	MySQL	10804	3306	Stop	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
1:35:35 PM  [main]     Control Panel Ready
1:35:43 PM  [Apache]   Problem detected!
1:35:43 PM  [Apache]   Port 443 in use by ""C:\Program Files (x86)\VMware\VMware Workstation\vmware-h
1:35:43 PM  [Apache]   Apache WILL NOT start without the configured ports free!
1:35:43 PM  [Apache]   You need to uninstall/disable/reconfigure the blocking application
1:35:43 PM  [Apache]   or reconfigure Apache and the Control Panel to listen on a different port
1:35:43 PM  [Apache]   Attempting to start Apache service...
```

The port 443 is being used by another program that is VMware in this case.

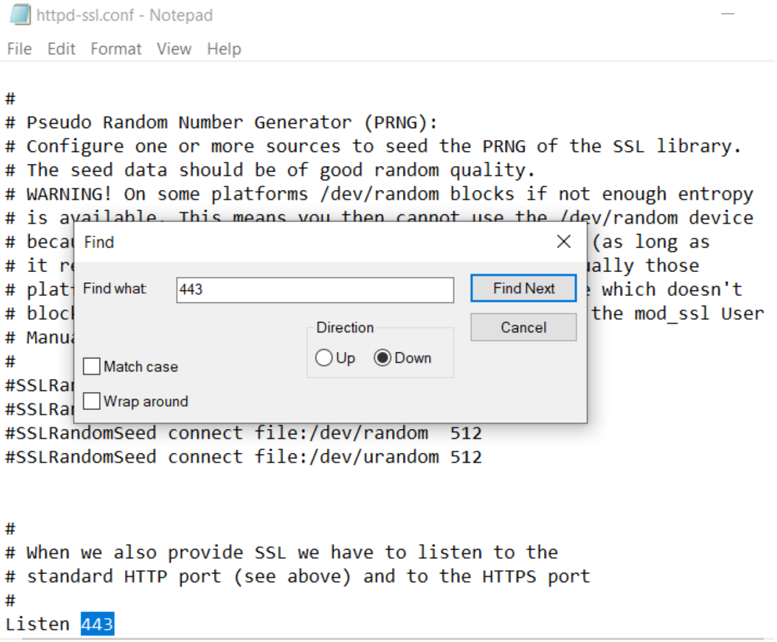
Solution:
Uninstall the program or change the port being used by Apache.

Risk and Incident Management



Module	PID(s)	Port(s)
MySQL	10804	3306

```
1:35:35 PM  [main]    Control Panel Ready
1:35:43 PM  [Apache]  Problem detected!
1:35:43 PM  [Apache]  Port 443 in use by ""C:\Program Files (x86)\VMware\V
1:35:43 PM  [Apache]  Apache WILL NOT start without the configured ports free!
1:35:43 PM  [Apache]  You need to uninstall/disable/reconfigure the blocking application
1:35:43 PM  [Apache]  or reconfigure Apache and the Control Panel to listen on a different port
1:35:43 PM  [Apache]  Attempting to start Apache service...
```

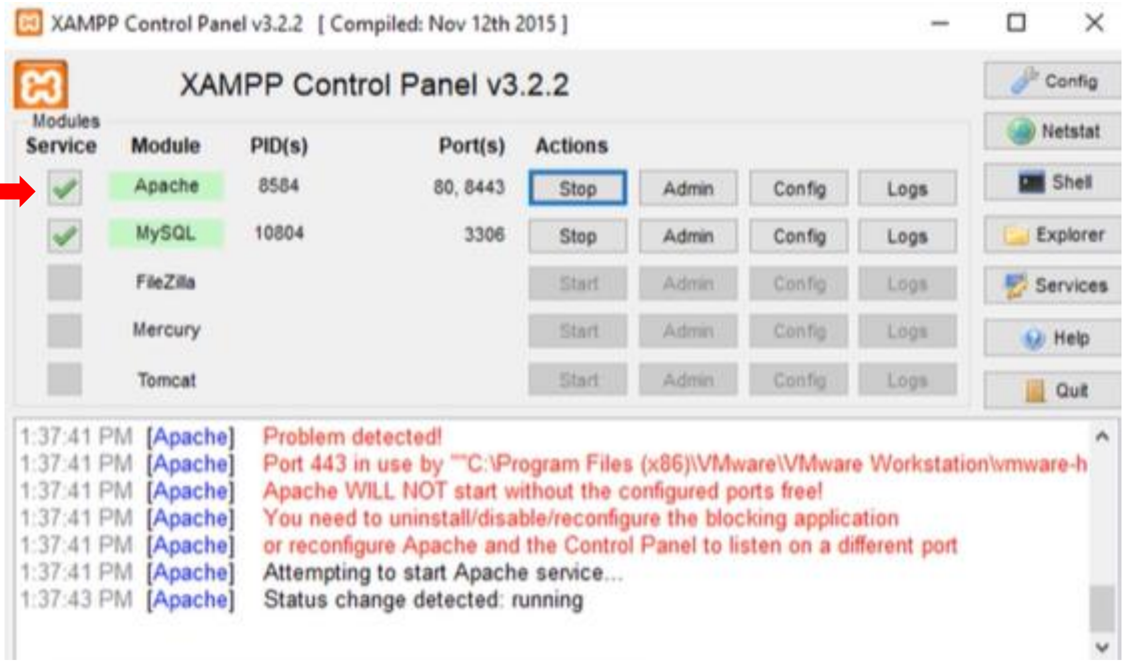


Find what: 443

```
#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough entropy
# is available. This means you then cannot use the /dev/random device
# becau                                                    (as long as
# it r                                                     ally those
# plat                                                     which doesn't
# bloc                                                     the mod_ssl User
# Manu
#
#SSLRa
#SSLRa
#SSLRandomSeed connect file:/dev/random  512
#SSLRandomSeed connect file:/dev/urandom 512


#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
Listen 443
```

Change 443 to 8443 (standard practice) and save.

Risk and Incident Management

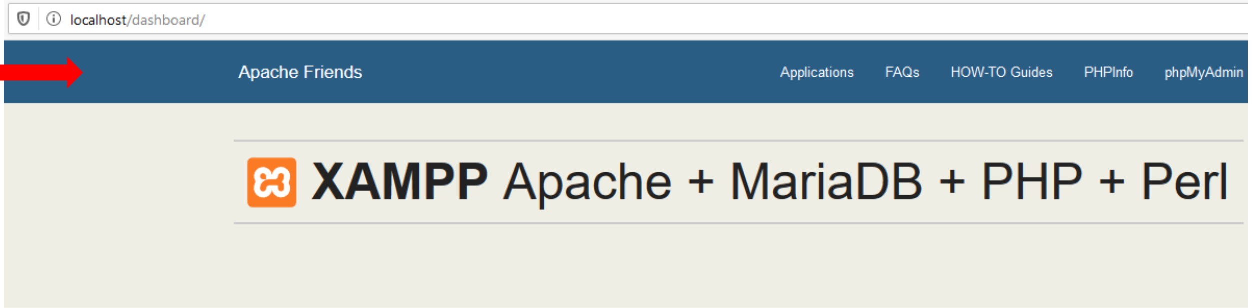

XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Config
Netstat
Shell
Explorer
Services
Help
Quit

Modules

Service	Module	PID(s)	Port(s)	Actions			
✓	Apache	8584	80, 8443	Stop	Admin	Config	Logs
✓	MySQL	10804	3306	Stop	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

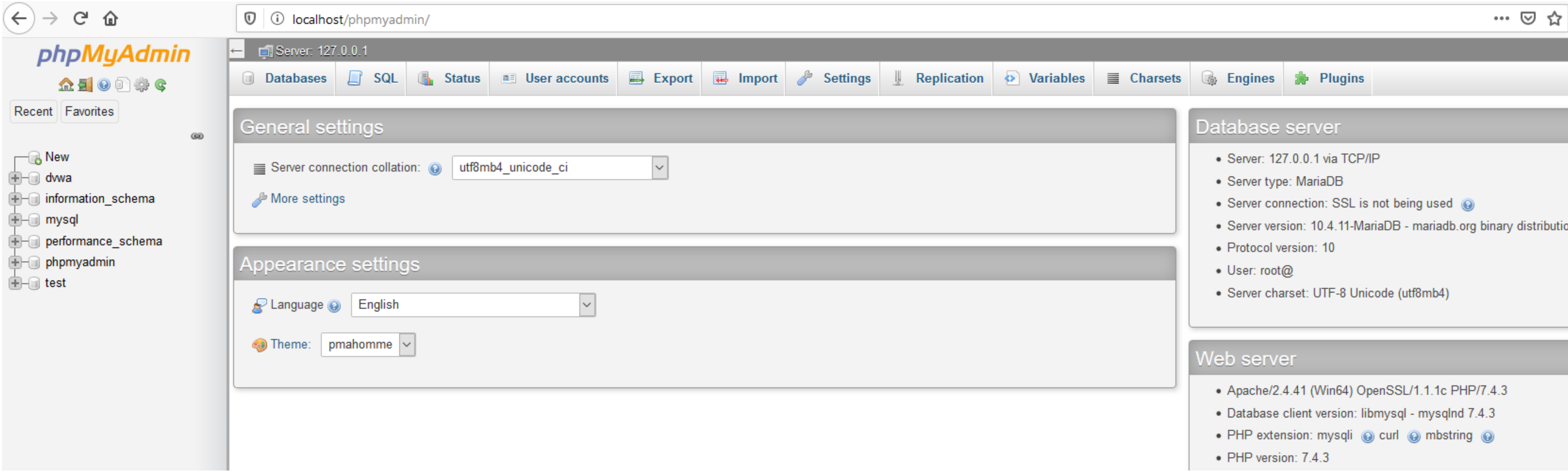
```
1:37:41 PM  [Apache]   Problem detected!
1:37:41 PM  [Apache]   Port 443 in use by ""C:\Program Files (x86)\VMware\VMware Workstation\vmware-h
1:37:41 PM  [Apache]   Apache WILL NOT start without the configured ports free!
1:37:41 PM  [Apache]   You need to uninstall/disable/reconfigure the blocking application
1:37:41 PM  [Apache]   or reconfigure Apache and the Control Panel to listen on a different port
1:37:41 PM  [Apache]   Attempting to start Apache service...
1:37:43 PM  [Apache]   Status change detected: running
```

Working fine



XAMPP Apache + MariaDB + PHP + Perl

Welcome to XAMPP for Windows 7.4.3



General settings

Server connection collation: utf8mb4_unicode_ci

More settings

Appearance settings

Language: English

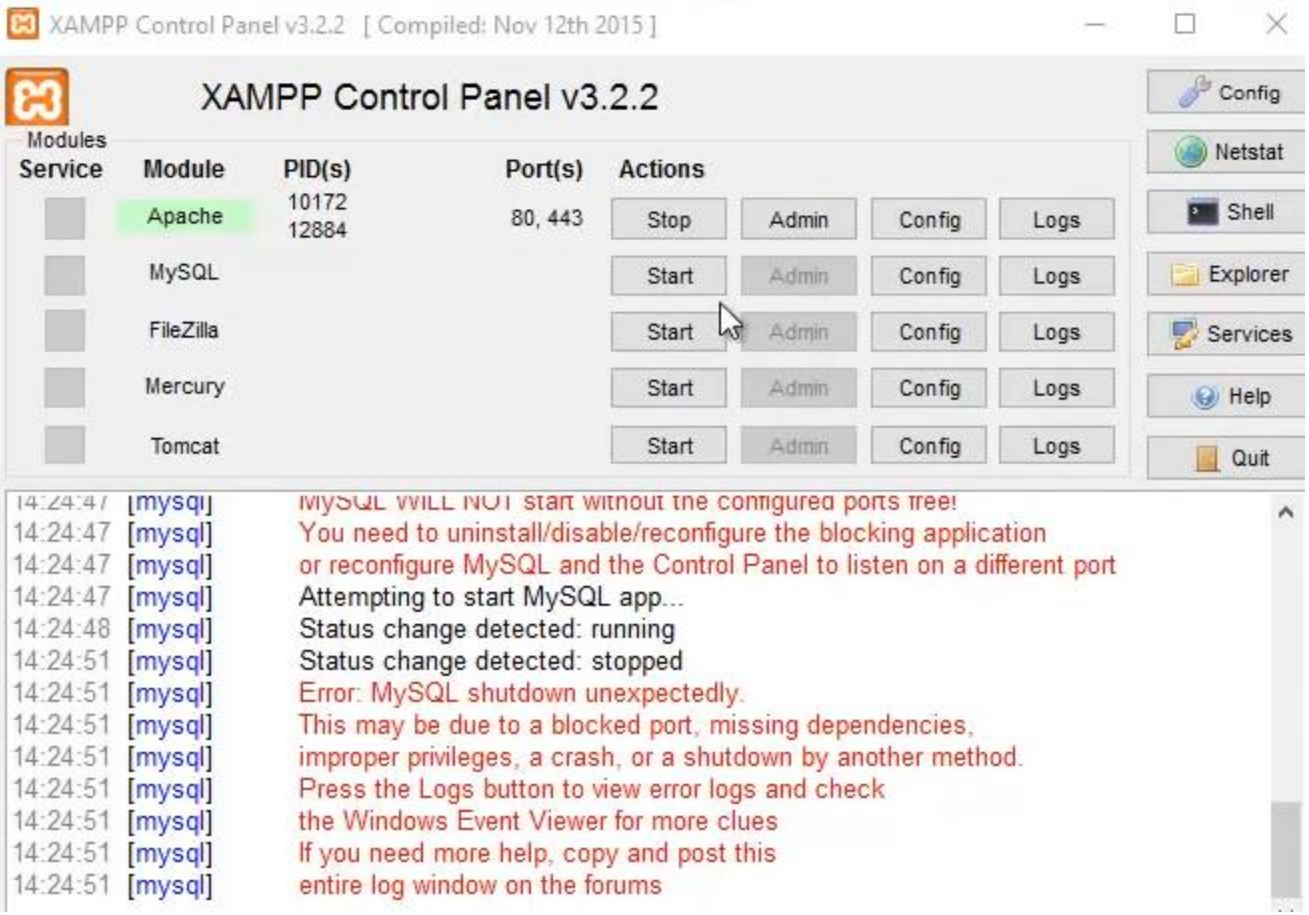
Theme: pmahomme

Database server

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.4.11-MariaDB - mariadb.org binary distributio
- Protocol version: 10
- User: root@
- Server charset: UTF-8 Unicode (utf8mb4)

Web server

- Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.3
- Database client version: libmysql - mysqlnd 7.4.3
- PHP extension: mysqli curl mbstring
- PHP version: 7.4.3

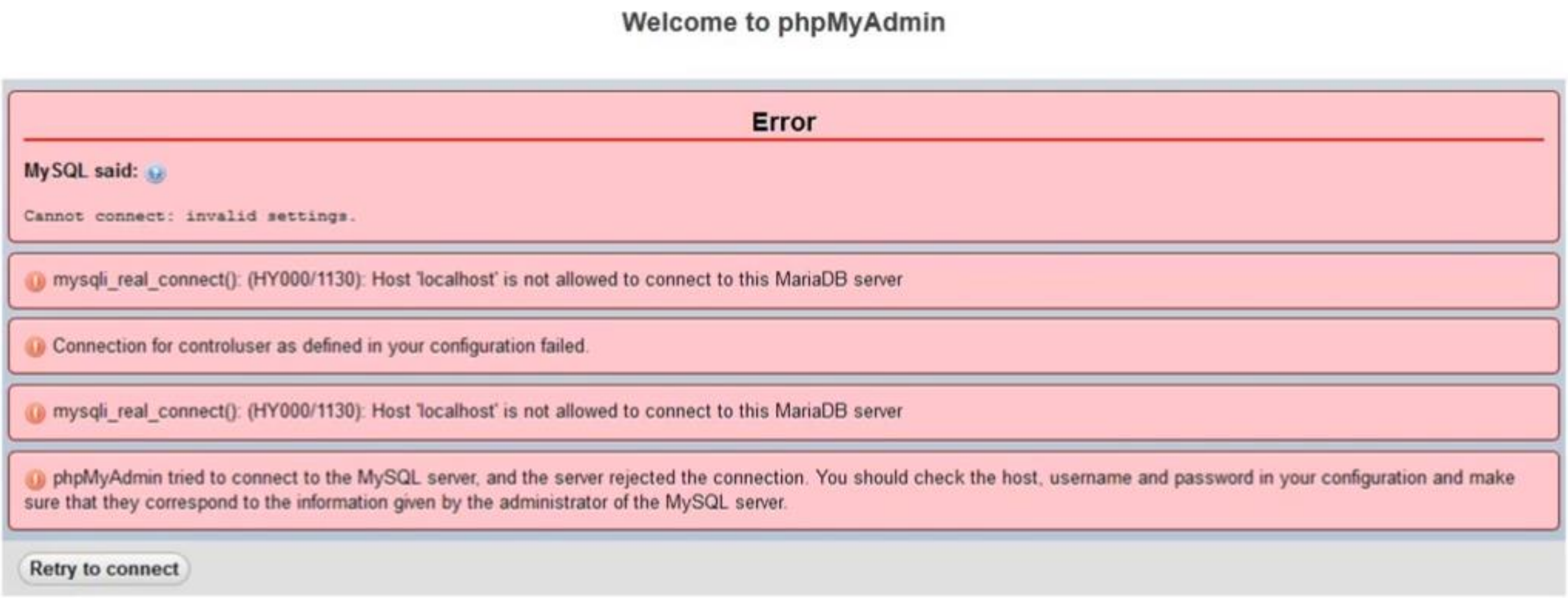

XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Modules
Config
Netstat
Shell
Explorer
Services
Help
Quit

Service	Module	PID(s)	Port(s)	Actions			
	Apache	10172 12884	80, 443	Stop	Admin	Config	Logs
	MySQL			Start	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
14:24:47  [mysql]    MySQL WILL NOT start without the configured ports free!
14:24:47  [mysql]    You need to uninstall/disable/reconfigure the blocking application
14:24:47  [mysql]    or reconfigure MySQL and the Control Panel to listen on a different port
14:24:47  [mysql]    Attempting to start MySQL app...
14:24:48  [mysql]    Status change detected: running
14:24:51  [mysql]    Status change detected: stopped
14:24:51  [mysql]    Error: MySQL shutdown unexpectedly.
14:24:51  [mysql]    This may be due to a blocked port, missing dependencies,
14:24:51  [mysql]    improper privileges, a crash, or a shutdown by another method.
14:24:51  [mysql]    Press the Logs button to view error logs and check
14:24:51  [mysql]    the Windows Event Viewer for more clues
14:24:51  [mysql]    If you need more help, copy and post this
14:24:51  [mysql]    entire log window on the forums
```

Go to Task Manager, find *mysqld* and end task.
Go back to XAMPP and click start.

Error: MYSQL Shutdown Unexpectedly



Welcome to phpMyAdmin

Error

MySQL said:

```
Cannot connect: invalid settings.
```

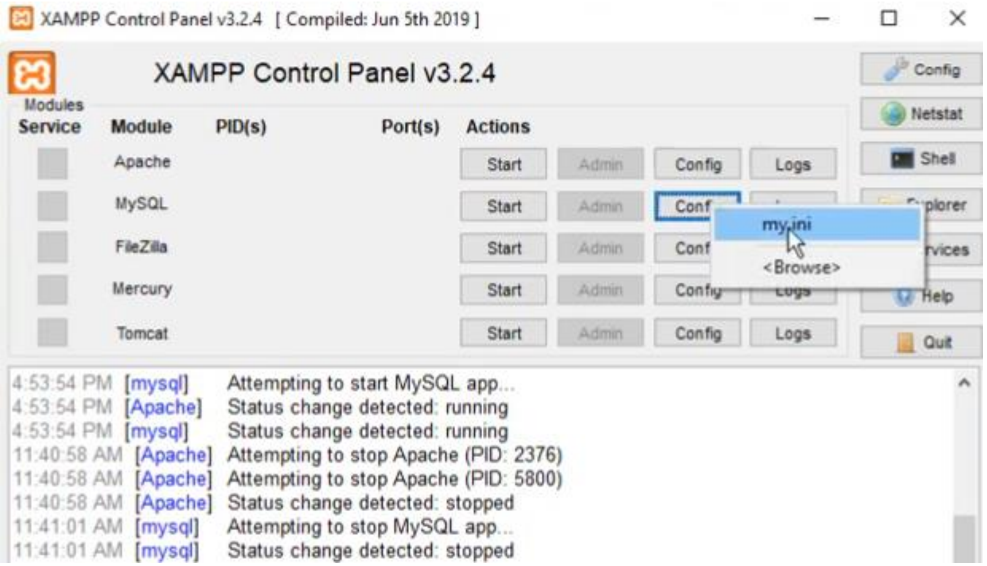
mysqli_real_connect(): (HY000/1130): Host 'localhost' is not allowed to connect to this MariaDB server

Connection for controluser as defined in your configuration failed.

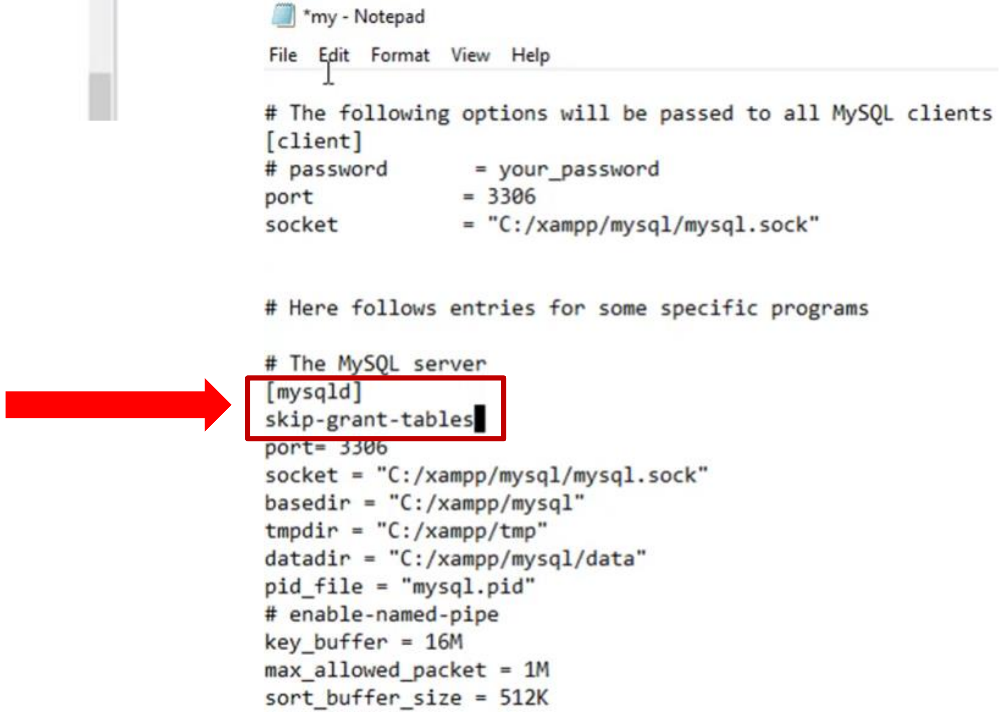
mysqli_real_connect(): (HY000/1130): Host 'localhost' is not allowed to connect to this MariaDB server

phpMyAdmin tried to connect to the MySQL server, and the server rejected the connection. You should check the host, username and password in your configuration and make sure that they correspond to the information given by the administrator of the MySQL server.

Stop *Apache* and *MySQL* on XAMPP.



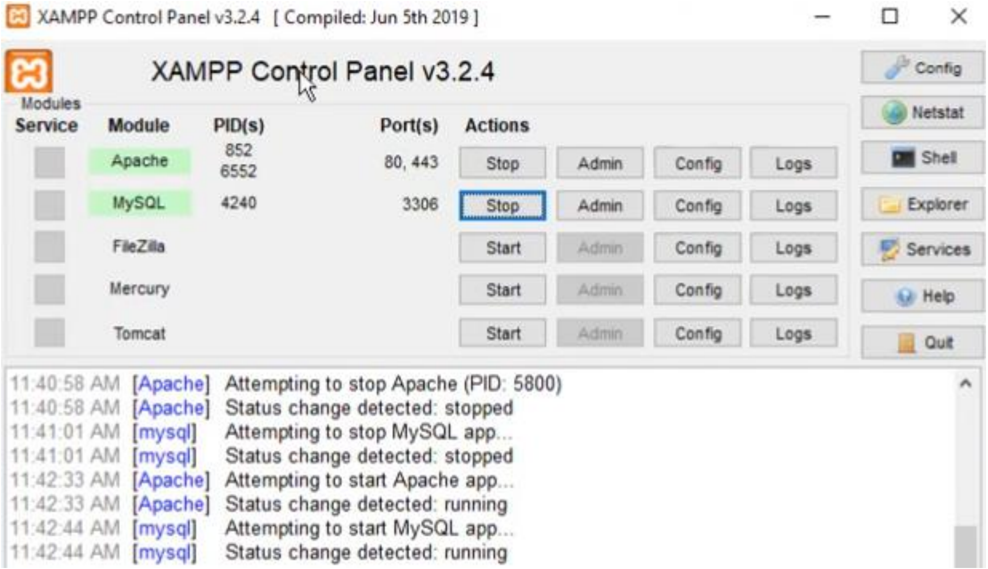
```
4:53:54 PM  [mysql]    Attempting to start MySQL app...
4:53:54 PM  [Apache]   Status change detected: running
4:53:54 PM  [mysql]    Status change detected: running
11:40:58 AM [Apache]   Attempting to stop Apache (PID: 2376)
11:40:58 AM [Apache]   Attempting to stop Apache (PID: 5800)
11:40:58 AM [Apache]   Status change detected: stopped
11:41:01 AM [mysql]    Attempting to stop MySQL app...
11:41:01 AM [mysql]    Status change detected: stopped
```



```
# The following options will be passed to all MySQL clients
[client]
# password       = your_password
port            = 3306
socket          = "C:/xampp/mysql/mysql.sock"


# Here follows entries for some specific programs

# The MySQL server
[mysqld]
skip-grant-tables
port= 3306
socket = "C:/xampp/mysql/mysql.sock"
basedir = "C:/xampp/mysql"
tmpdir = "C:/xampp/tmp"
datadir = "C:/xampp/mysql/data"
pid_file = "mysql.pid"
# enable-named-pipe
key_buffer = 16M
max_allowed_packet = 1M
sort_buffer_size = 512K
```

Error: MYSQL Shutdown Unexpectedly

Start *Apache* and *MySQL* on XAMPP.



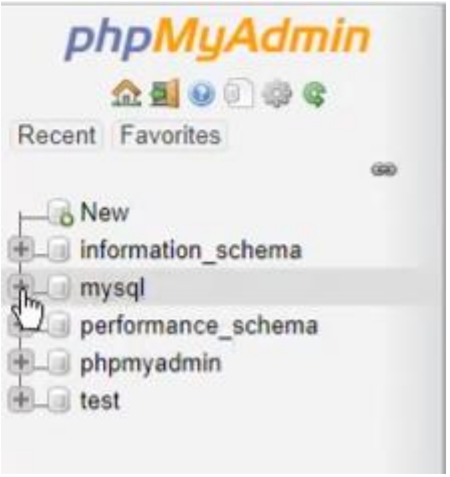
XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]

XAMPP Control Panel v3.2.4

Service	Module	PID(s)	Port(s)	Actions			
	Apache	852 6552	80, 443	Stop	Admin	Config	Logs
	MySQL	4240	3306	Stop	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

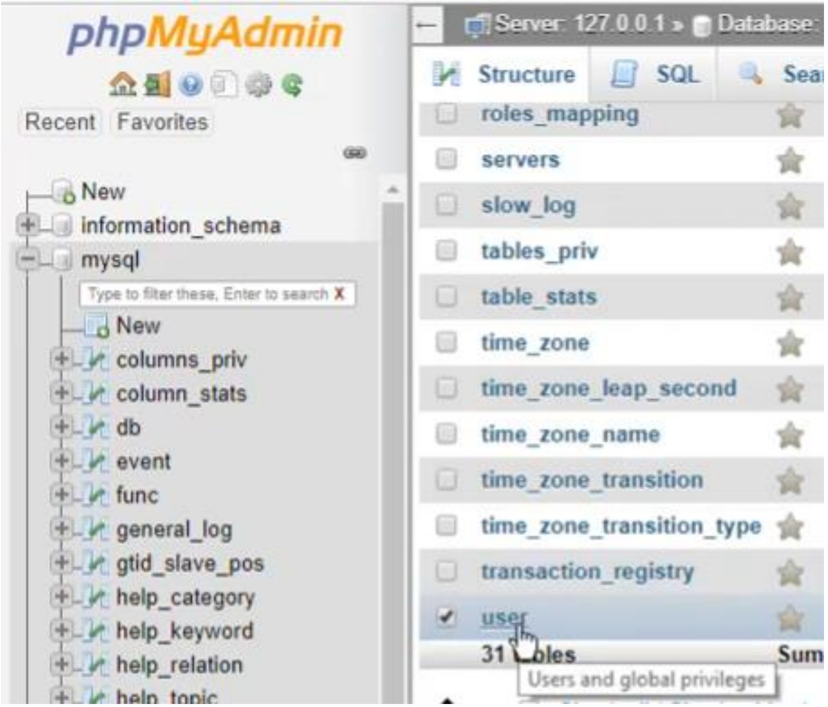
```
11:40:58 AM  [Apache]  Attempting to stop Apache (PID: 5800)
11:40:58 AM  [Apache]  Status change detected: stopped
11:41:01 AM  [mysql]   Attempting to stop MySQL app...
11:41:01 AM  [mysql]   Status change detected: stopped
11:42:33 AM  [Apache]  Attempting to start Apache app...
11:42:33 AM  [Apache]  Status change detected: running
11:42:44 AM  [mysql]   Attempting to start MySQL app...
11:42:44 AM  [mysql]   Status change detected: running
```

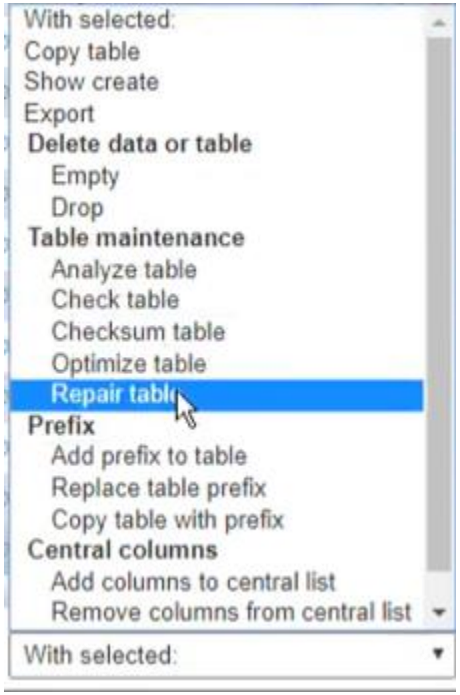
Go to *phpMyAdmin* and open *mysql*



- New
- information_schema
- mysql
- performance_schema
- phpmyadmin
- test

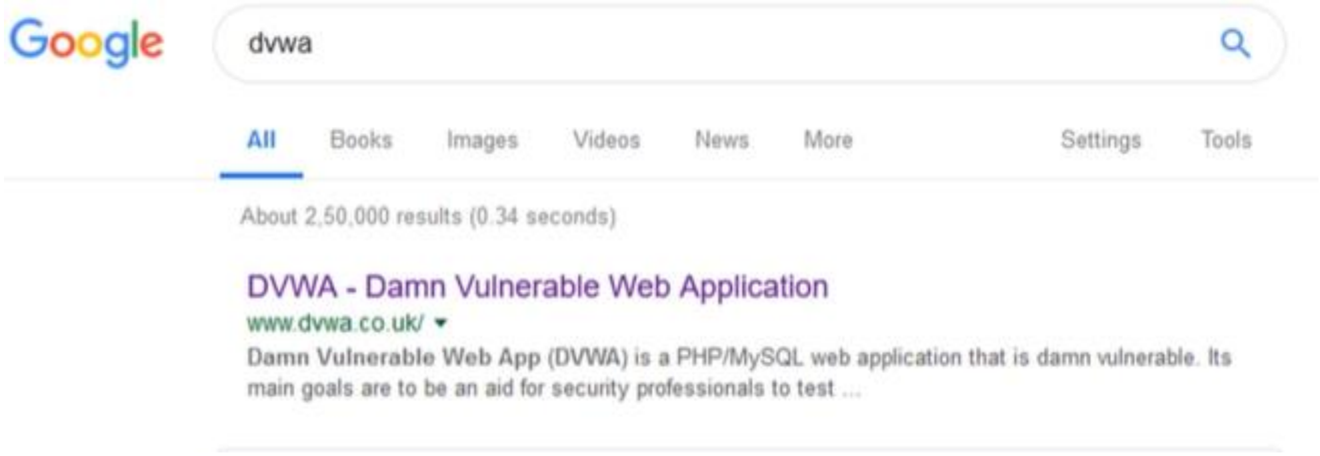
Select *user*:


phpMyAdmin
Recent
Favorites
New
information_schema
mysql
Type to filter these, Enter to search
New
columns_priv
column_stats
db
event
func
general_log
gtid_slave_pos
help_category
help_keyword
help_relation
help_topic
Server: 127.0.0.1 » Database:
Structure
SQL
Sea
roles_mapping
servers
slow_log
tables_priv
table_stats
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
transaction_registry
user
31 tables
Sum
Users and global privileges


With selected:
Copy table
Show create
Export
Delete data or table
Empty
Drop
Table maintenance
Analyze table
Check table
Checksum table
Optimize table
Repair table
Prefix
Add prefix to table
Replace table prefix
Copy table with prefix
Central columns
Add columns to central list
Remove columns from central list
With selected:

- ✓ Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

- ✓ DVWA was made by security professionals, for researchers and enthusiasts to practice and learn different types of vulnerabilities in relation to web applications which can also be used for other things such as software activation keys.

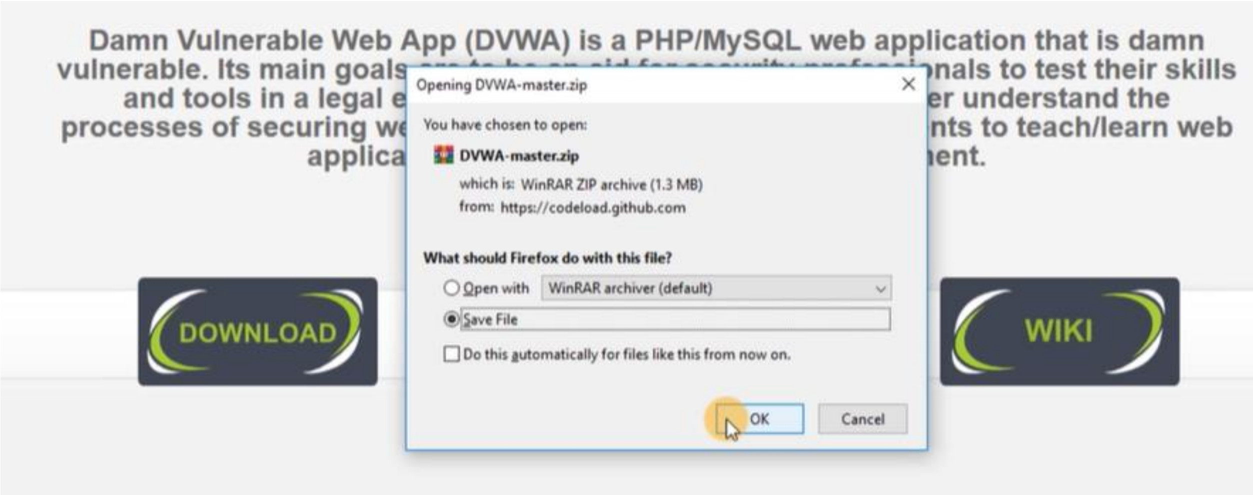


About 2,50,000 results (0.34 seconds)

DVWA - Damn Vulnerable Web Application
www.dvwa.co.uk/

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test ...

Extract in the location where you installed XAMPP



Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals … nals to test their skills and tools in a legal e … er understand the processes of securing we … nts to teach/learn web applica … ent.

Opening DVWA-master.zip

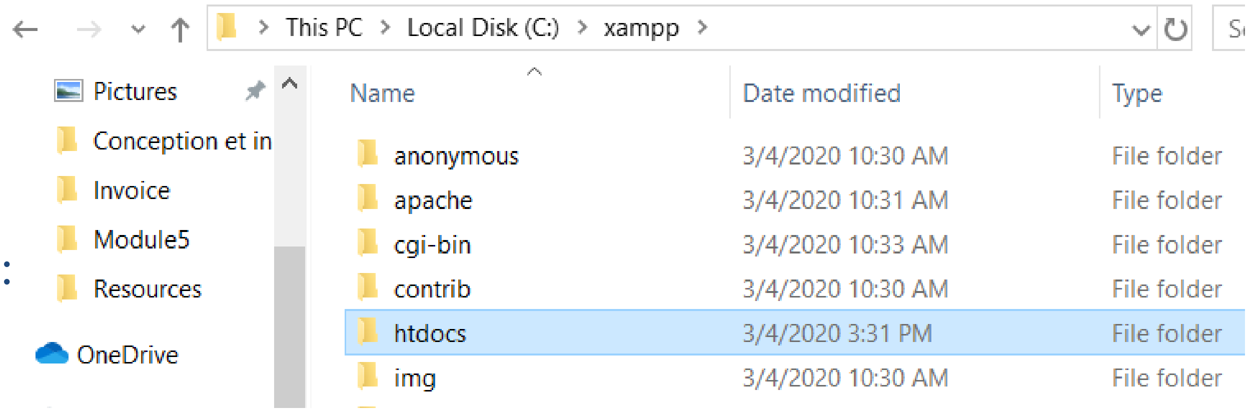
You have chosen to open:

DVWA-master.zip
which is: WinRAR ZIP archive (1.3 MB)
from: https://codeload.github.com

What should Firefox do with this file?

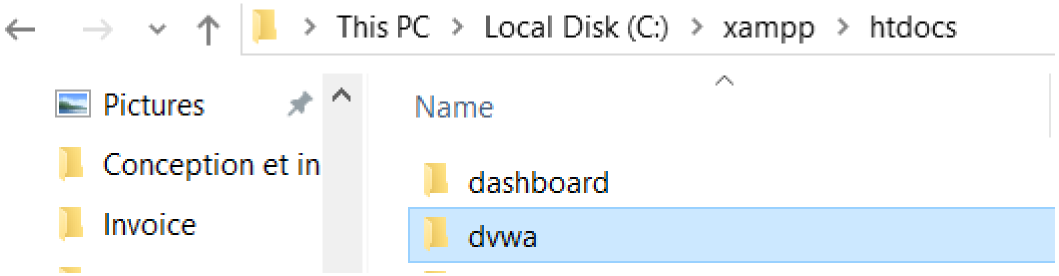
○ Open with WinRAR archiver (default)
● Save File
□ Do this automatically for files like this from now on.

Extract in htdocs:



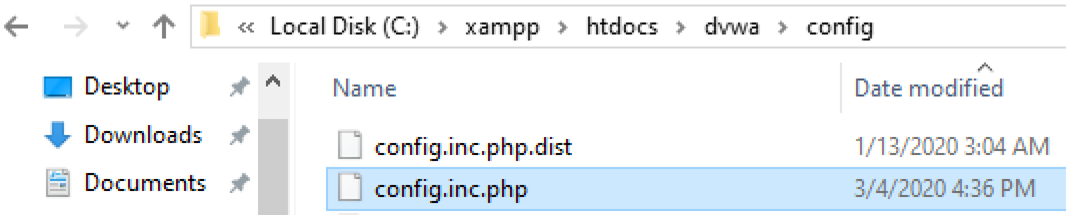
Name	Date modified	Type
anonymous	3/4/2020 10:30 AM	File folder
apache	3/4/2020 10:31 AM	File folder
cgi-bin	3/4/2020 10:33 AM	File folder
contrib	3/4/2020 10:30 AM	File folder
htdocs	3/4/2020 3:31 PM	File folder
img	3/4/2020 10:30 AM	File folder

Rename the file to *dvwa*:



Name
dashboard
dvwa

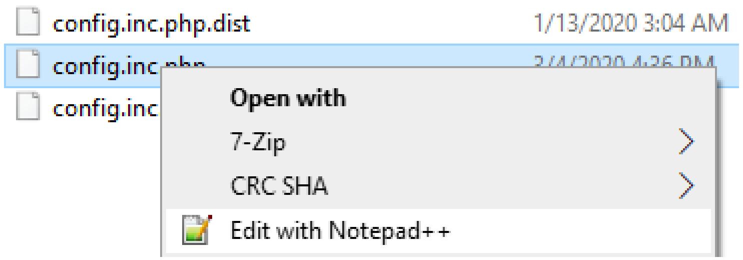
Open the config folder, make a copy from *config.inc.php.dist* end rename it to *config.inc.php* :



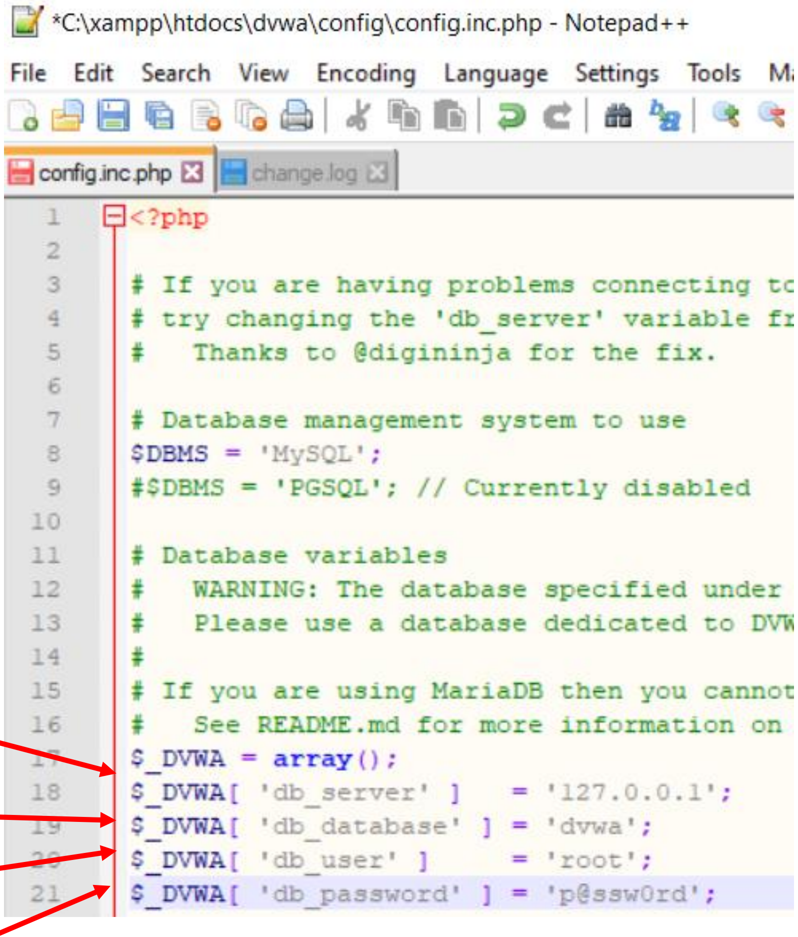
« Local Disk (C:) › xampp › htdocs › dvwa › config

Name	Date modified
config.inc.php.dist	1/13/2020 3:04 AM
config.inc.php	3/4/2020 4:36 PM

Open the *config.inc.php file* with Notepad++ :



config.inc.php.dist	1/13/2020 3:04 AM
config.inc.php	3/4/2020 4:36 PM
config.inc	


*C:\xampp\htdocs\dvwa\config\config.inc.php - Notepad++
File Edit Search View Encoding Language Settings Tools M
config.inc.php
change.log

```
<?php

# If you are having problems connecting to
# try changing the 'db_server' variable fr
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under
#   Please use a database dedicated to DVW
#
# If you are using MariaDB then you cannot
#   See README.md for more information on
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
```

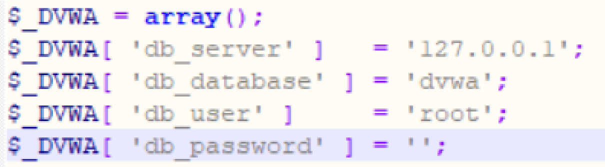
local host IP

database

database user

database password

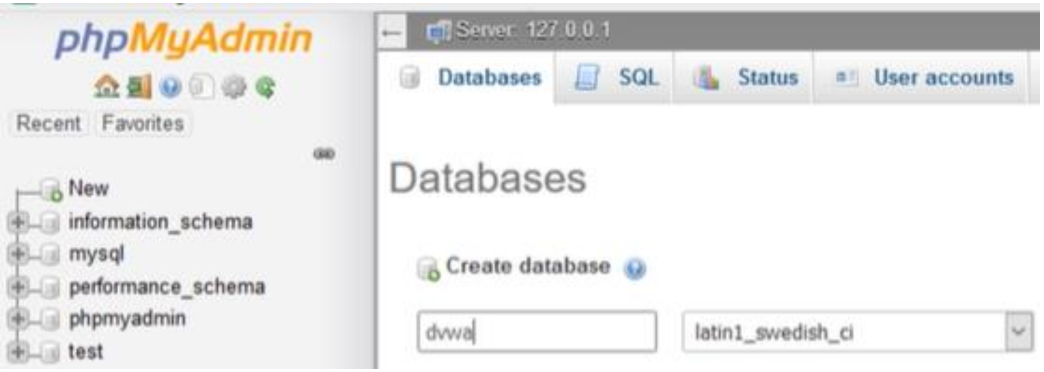
Remove the password:



```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
```

Start *Apache* and *MySQL* on XAMPP.

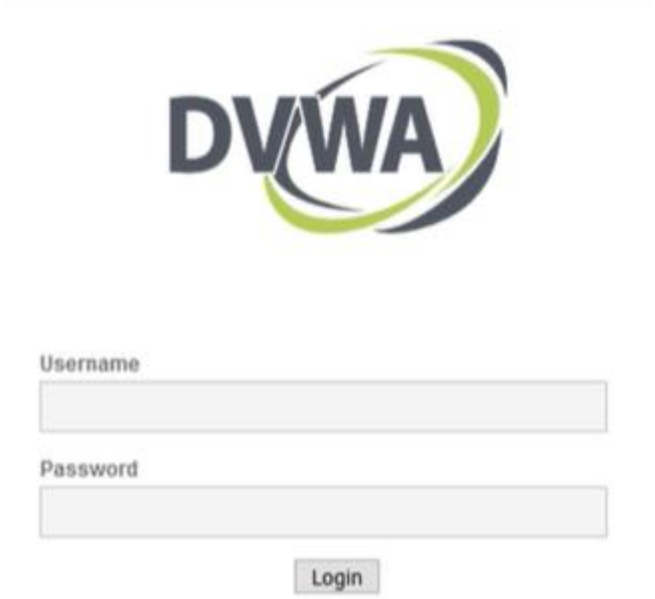
Go to *localhost* and then *phpMyAdmin*. Create a new database named *dvwa*.



dvwa

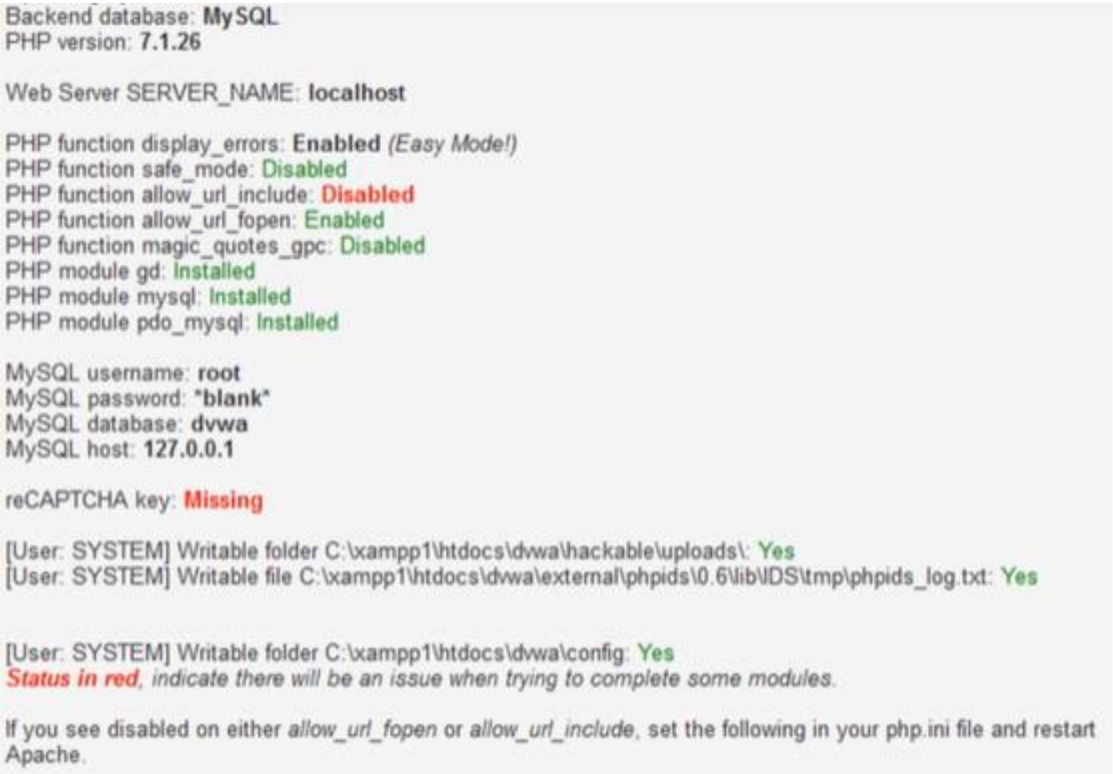
latin1_swedish_ci

Go to localhost/dvwa



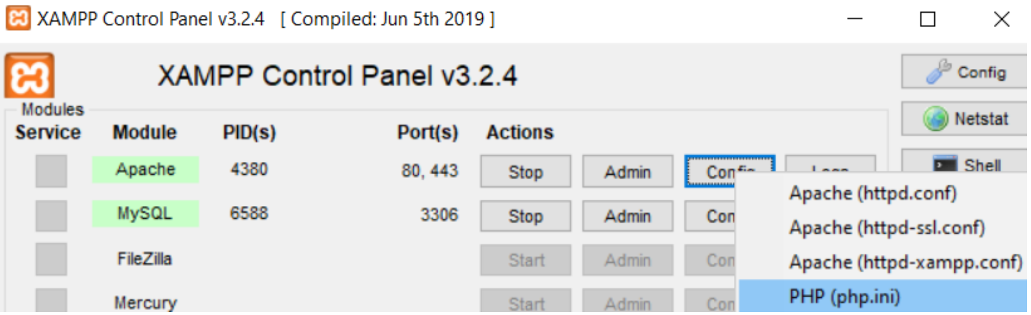
Risk and Incident Management

In dvwa setup check we need to make PHP function allow_url_include enable



```
Backend database: MySQL
PHP version: 7.1.26

Web Server SERVER_NAME: localhost

PHP function display_errors: Enabled (Easy Mode!)
PHP function safe_mode: Disabled
PHP function allow_url_include: Disabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: root
MySQL password: *blank*
MySQL database: dvwa
MySQL host: 127.0.0.1

reCAPTCHA key: Missing

[User: SYSTEM] Writable folder C:\xampp1\htdocs\dvwa\hackable\uploads\: Yes
[User: SYSTEM] Writable file C:\xampp1\htdocs\dvwa\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes


[User: SYSTEM] Writable folder C:\xampp1\htdocs\dvwa\config: Yes
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
```

Go to *Apache* configuration and then *php.ini*

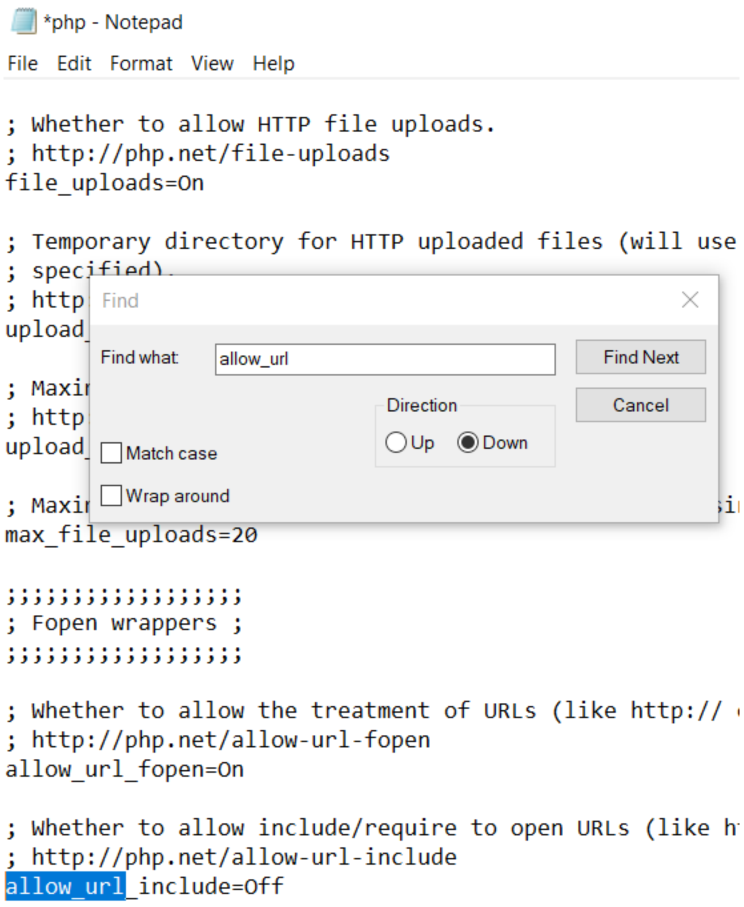


XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]

XAMPP Control Panel v3.2.4

Modules

Service	Module	PID(s)	Port(s)	Actions			
□	Apache	4380	80, 443	Stop	Admin	Config	Logs
□	MySQL	6588	3306	Stop	Admin	Con	
□	FileZilla			Start	Admin	Con	
□	Mercury			Start	Admin	Con	



```
; Whether to allow HTTP file uploads.
; http://php.net/file-uploads
file_uploads=On

; Temporary directory for HTTP uploaded files (will use
; specified).
; http
upload_

; Maxir
; http
upload_

; Maxir                                                  si
max_file_uploads=20

;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http://
; http://php.net/allow-url-fopen
allow_url_fopen=On

; Whether to allow include/require to open URLs (like h
; http://php.net/allow-url-include
allow_url_include=Off
```

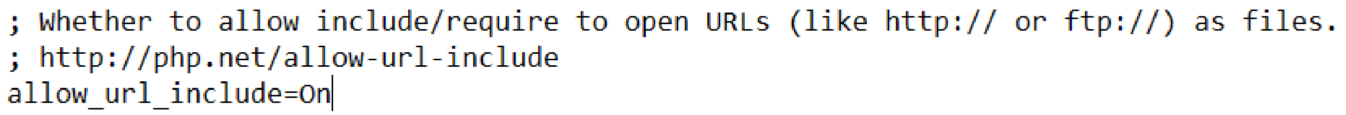
Find what: allow_url

Direction: ○ Up ● Down

□ Match case

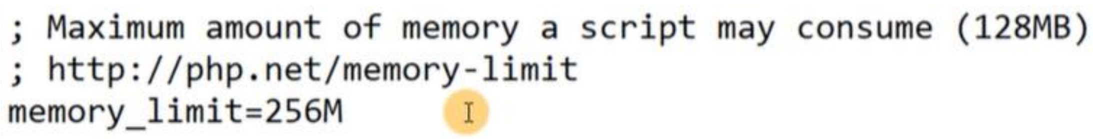
□ Wrap around

Change it to On:



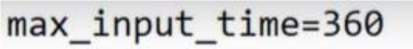
```
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On
```

Change the memory_limit to 256M



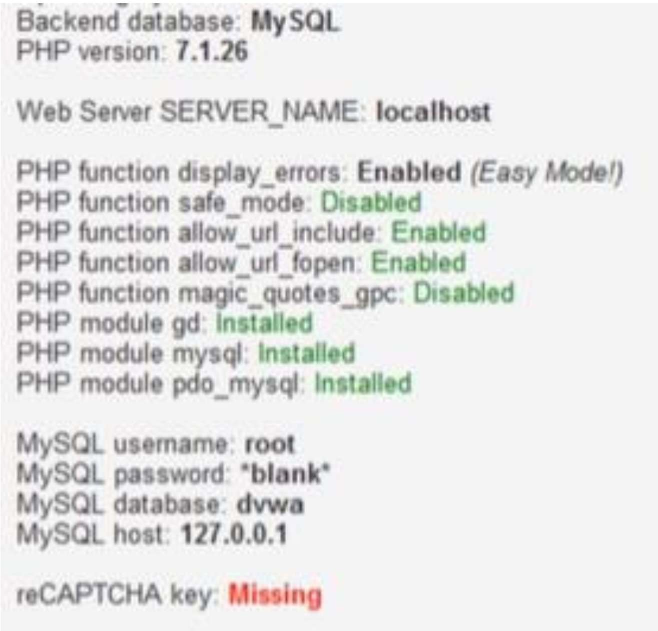
```
; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit=256M
```

Change the max_input_time to 360:



```
max_input_time=360
```

Restart the *Apache* in order to reload the php file.



Backend database: **MySQL**
PHP version: **7.1.26**

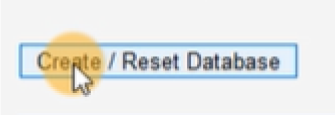
Web Server SERVER_NAME: **localhost**

PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: ***blank***
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

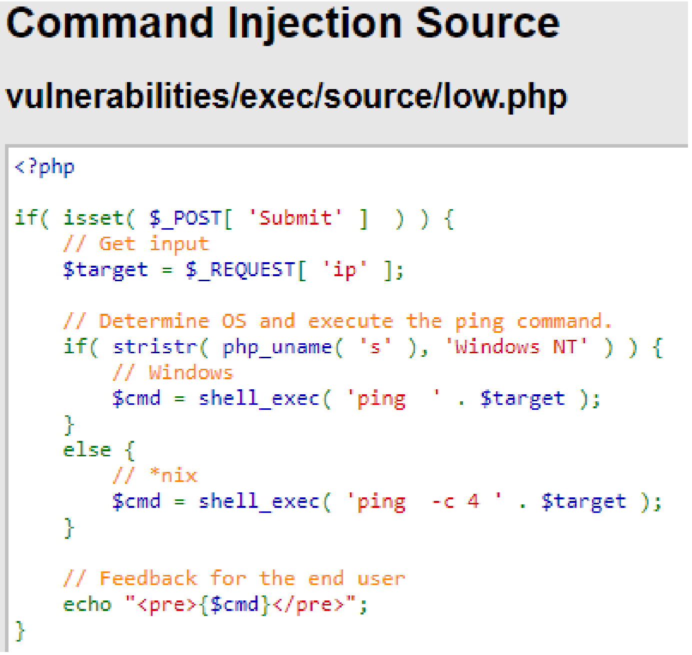
Create/Reset database:



Command Injection occurs when there is a field or an application that is accepting the input from user. However, the rule says Never trust a user. It is wrong and dangerous if the application trust the user that entering e.g. an IP address.

User may enter a command called as injection or execution because user is trying to inject the command in the web application and the command is going to be executed by the web application so just for this source.

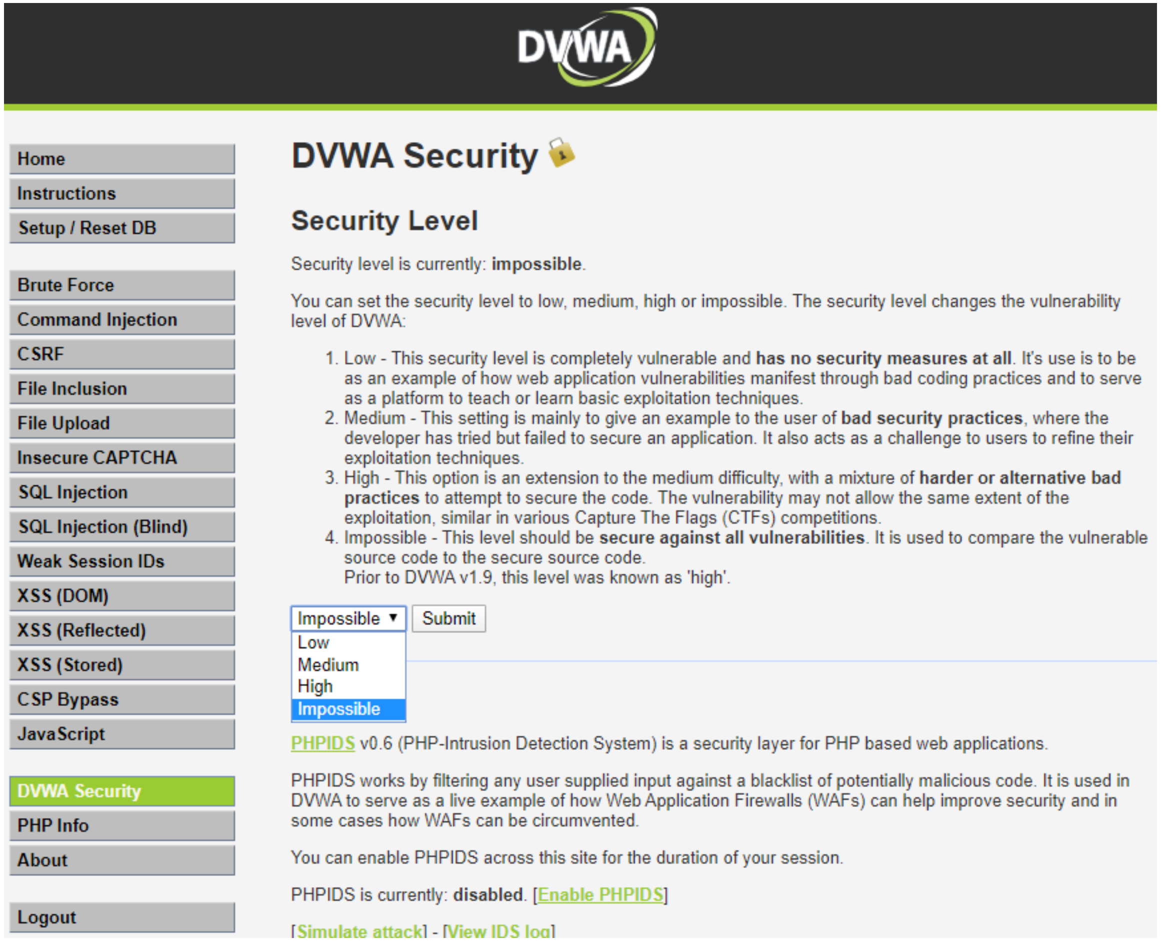
The DVWA security level is submitted at *Low*.



Command Injection Source

vulnerabilities/exec/source/low.php

```
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}
```



DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Impossible ▼ Submit

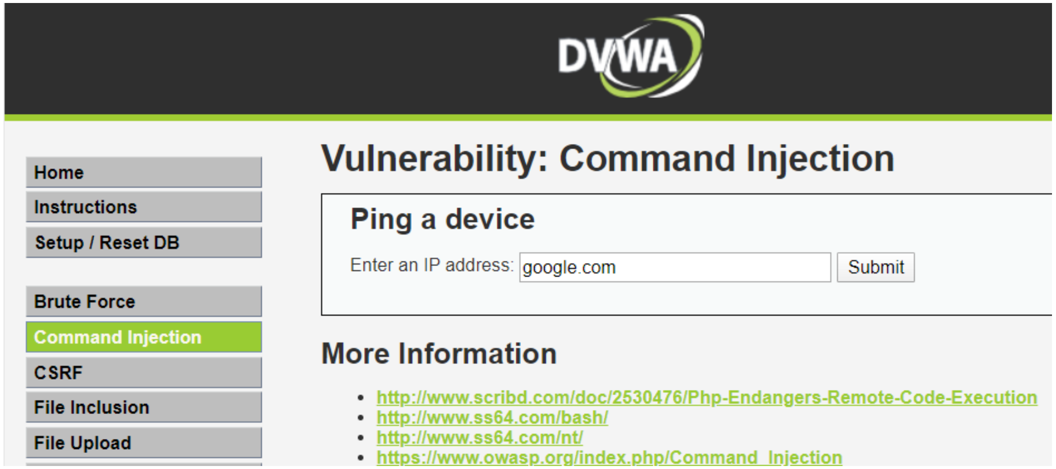
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]



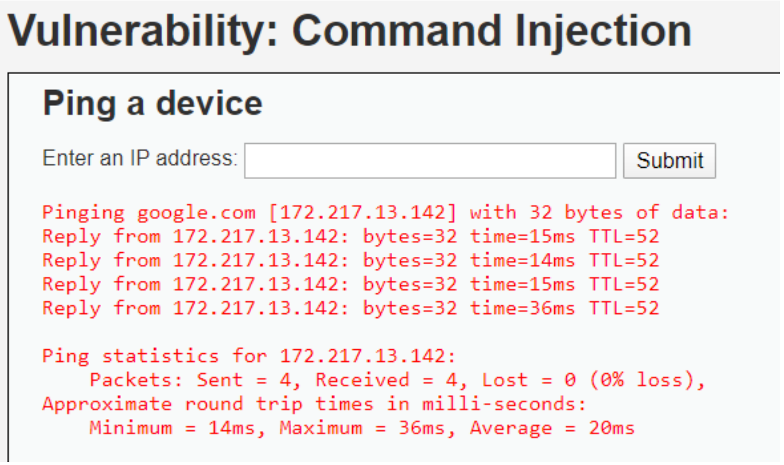
Vulnerability: Command Injection

Ping a device

Enter an IP address: google.com

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection



Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
Pinging google.com [172.217.13.142] with 32 bytes of data:
Reply from 172.217.13.142: bytes=32 time=15ms TTL=52
Reply from 172.217.13.142: bytes=32 time=14ms TTL=52
Reply from 172.217.13.142: bytes=32 time=15ms TTL=52
Reply from 172.217.13.142: bytes=32 time=36ms TTL=52

Ping statistics for 172.217.13.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 36ms, Average = 20ms
```

Special characters used

- An attacker will use the following characters to attach his commands to that of the server:
  - **command1 | command2**:
    - command 2 is executed no matter if command 1 is successfully executed or not.
  - **command1; command2**:
    - command 2 is executed no matter if command 1 is successfully executed or not.
  - **command1 || command2**:
    - command 2 will be executed if the execution of command 1 fails.
  - **command1 && command2**:
    - command 2 will be executed if the execution of command 1 succeeds.
  - **$(command):**
    - what lies between the parentheses will be executed
  - **'cmd':**
    - is used to execute a specific command