


DVWA SETUP ON WINDOWS

RESOURCE	LINK
DVWA	https://github.com/digininja/DVWA
XAMPP	https://www.apachefriends.org/download.html

1. Visit the **XAMPP** page and download the installer for your system.

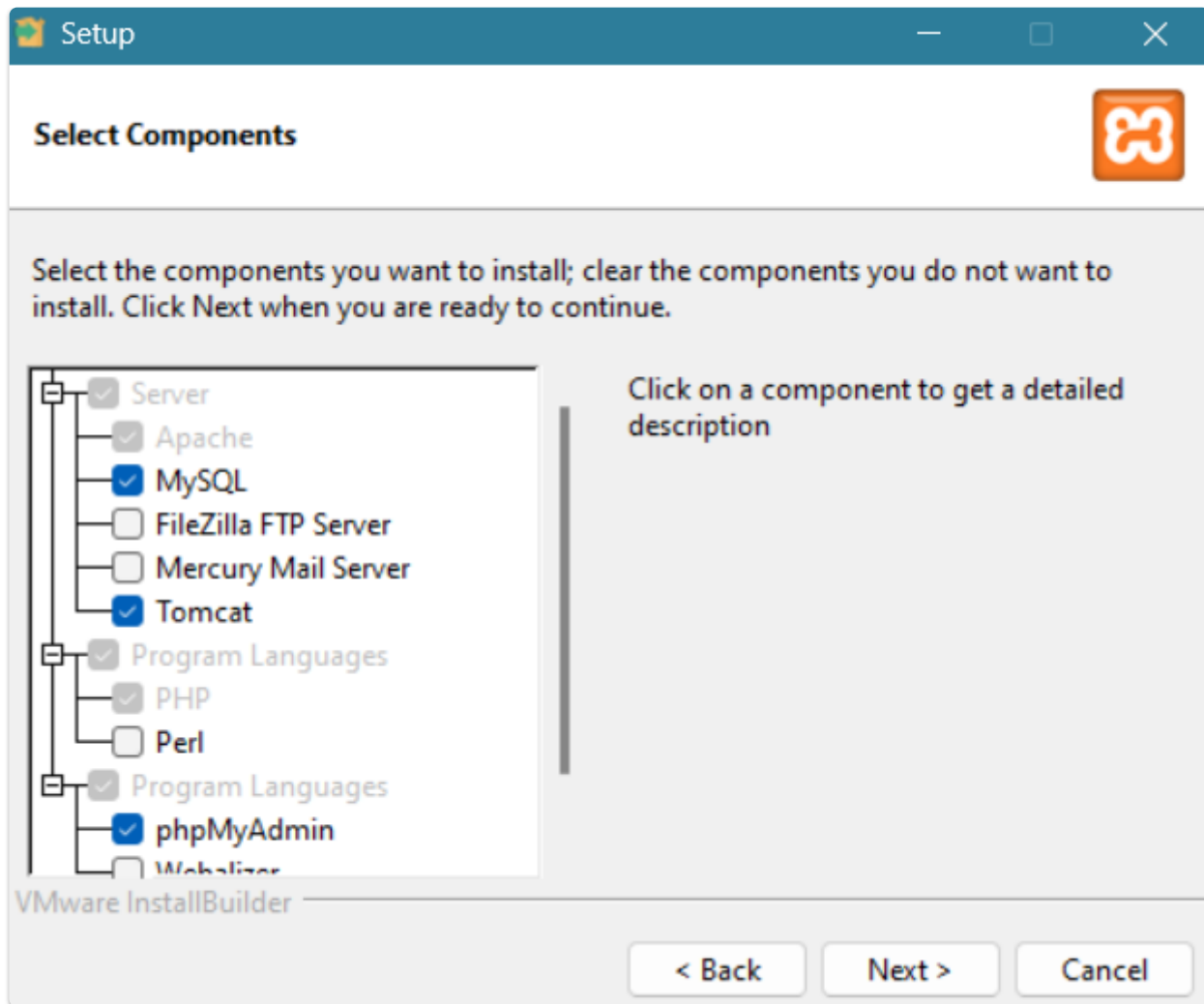
 **XAMPP for Windows 8.0.30, 8.1.25 & 8.2.12**

Version		Checksum		Size
8.0.30 / PHP 8.0.30	What's Included?	md5	sha1	Download (64 bit) 144 Mb
8.1.25 / PHP 8.1.25	What's Included?	md5	sha1	Download (64 bit) 148 Mb
8.2.12 / PHP 8.2.12	What's Included?	md5	sha1	Download (64 bit) 149 Mb

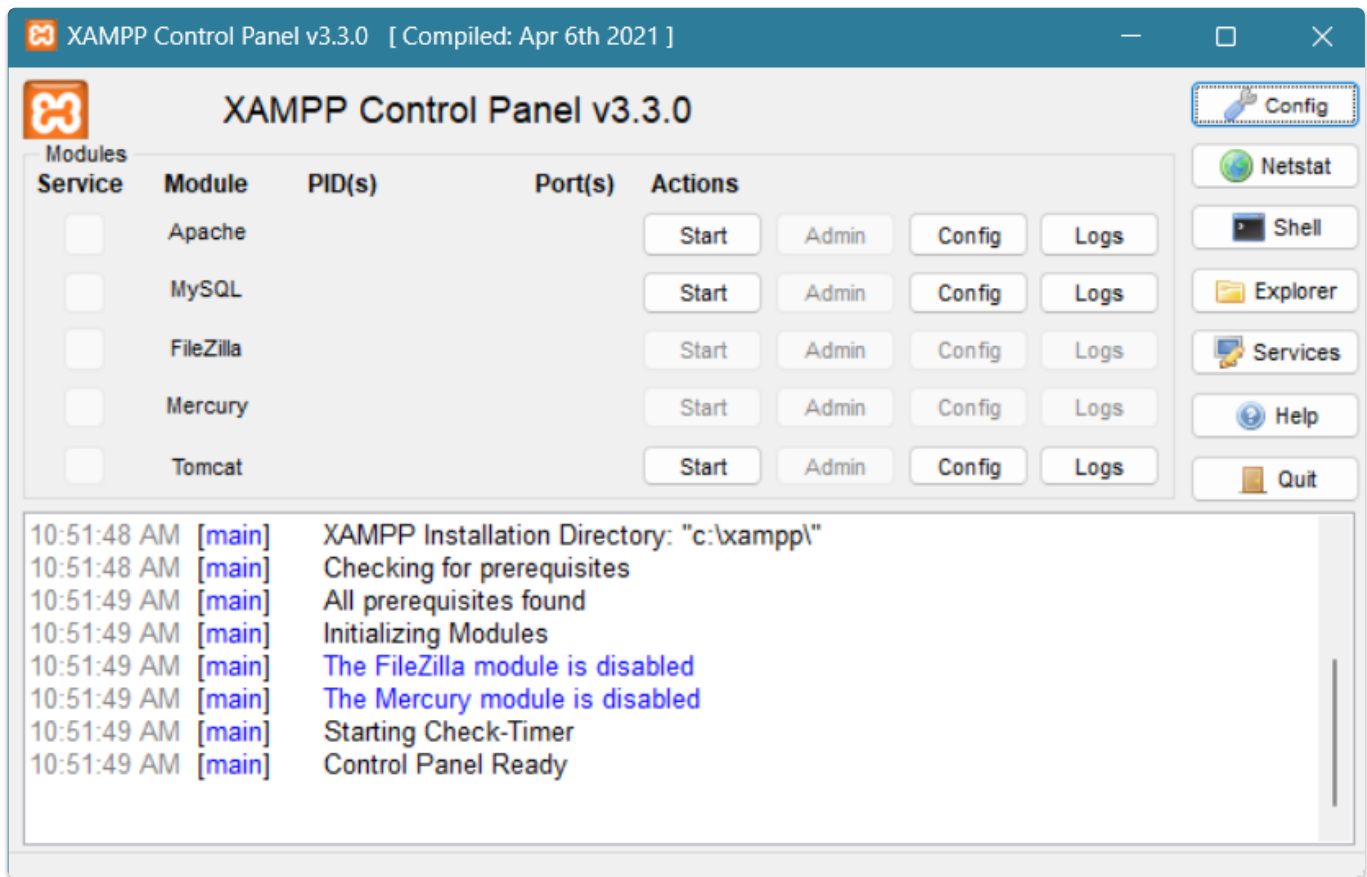
[Requirements](#) [More Downloads »](#)

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms [here](#).

2. Run the installer and make sure you mark the **Apache** and **MySQL** service for installation.



3. The **xampp control panel** will pop up.



4. Apache Server Configuration

- Click on *Config* --> *Apache (httpd.conf)*

XAMPP Control Panel v3.3.0

Service	Module	PID(s)	Port(s)	Actions
<input type="checkbox"/>	Apache			Start Admin Config Logs Shell
<input type="checkbox"/>	MySQL			Start Admin
<input type="checkbox"/>	FileZilla			Start Admin
<input type="checkbox"/>	Mercury			Start Admin
<input type="checkbox"/>	Tomcat			Start Admin

Log Window:

```

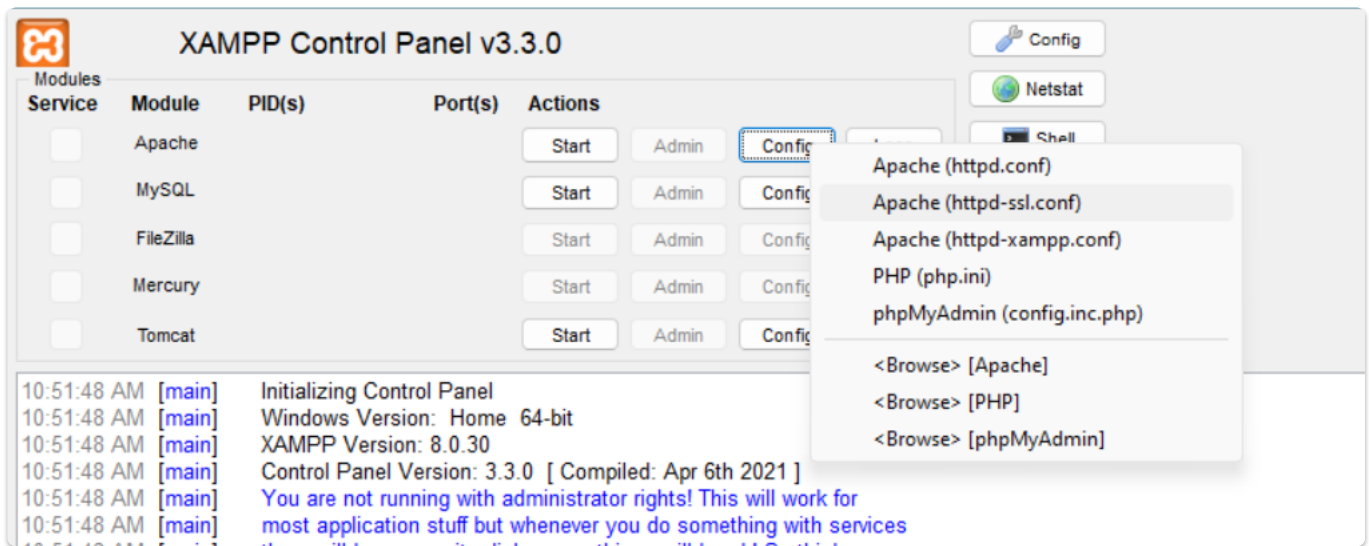
10:51:48 AM [main] Initializing Control Panel
10:51:48 AM [main] Windows Version: Home 64-bit
10:51:48 AM [main] XAMPP Version: 8.0.30
10:51:48 AM [main] Control Panel Version: 3.3.0 [ Compiled: Apr 6th 2021 ]
10:51:48 AM [main] You are not running with administrator rights! This will work for
10:51:48 AM [main] most application stuff but whenever you do something with services
10:51:48 AM [main] there will be a security dialogue or things will break! So think
10:51:48 AM [main] about running this application with administrator rights!
10:51:48 AM [main] XAMPP Installation Directory: "c:\xampp\"
10:51:48 AM [main] Checking for prerequisites
10:51:49 AM [main] All prerequisites found
10:51:49 AM [main] Initializing Modules
10:51:49 AM [main] The FileZilla module is disabled
10:51:49 AM [main] The Mercury module is disabled
10:51:49 AM [main] Starting Check-Timer
10:51:49 AM [main] Control Panel Ready
  
```

- Change the listening port to **8000**

```

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 8000
  
```

- Save and close it. Click on *config* --> *Apache (httpd-ssl.conf)*

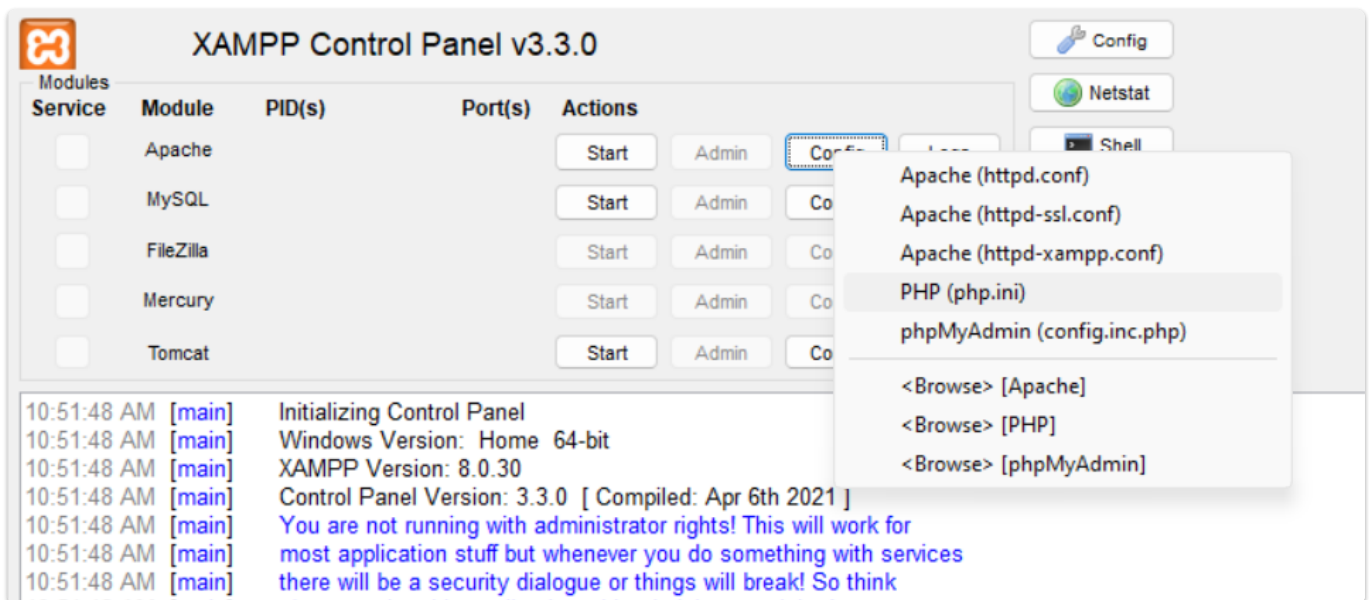


- Change the listening port to 4433

```

#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
Listen 4433
  
```

- Save and close it. Click on *config* --> *PHP (php.ini)*



- Ensure the following values are turned on

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen=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
```

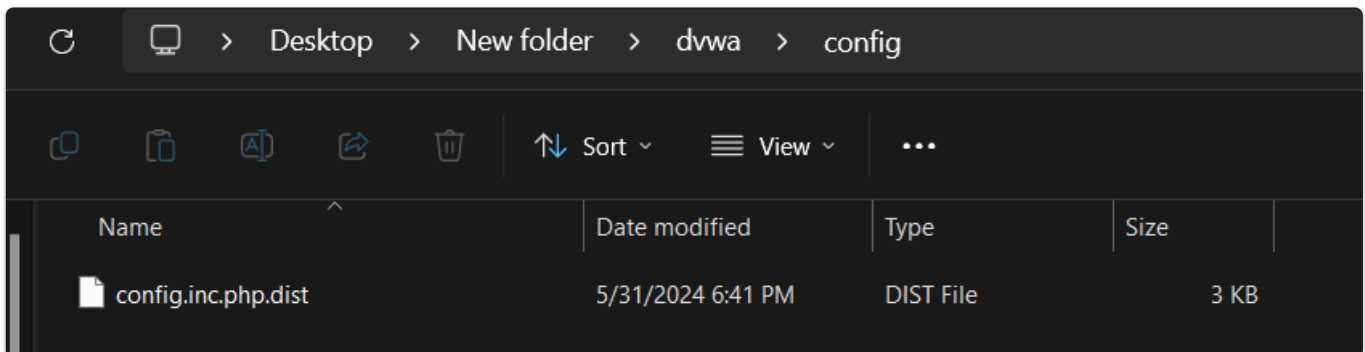
- In the same file, search for `;extension=gd` and remove the `;` from the start.

```
extension=fileinfo
extension=gd
extension=gettext
;extension=gmp
;extension=intl
```

- Finally save and close the file.

5. Download the `dvwa` zip file from the Github link and extract it. Rename the folder to `dvwa`.

6. Open the folder and go inside the `config` folder.



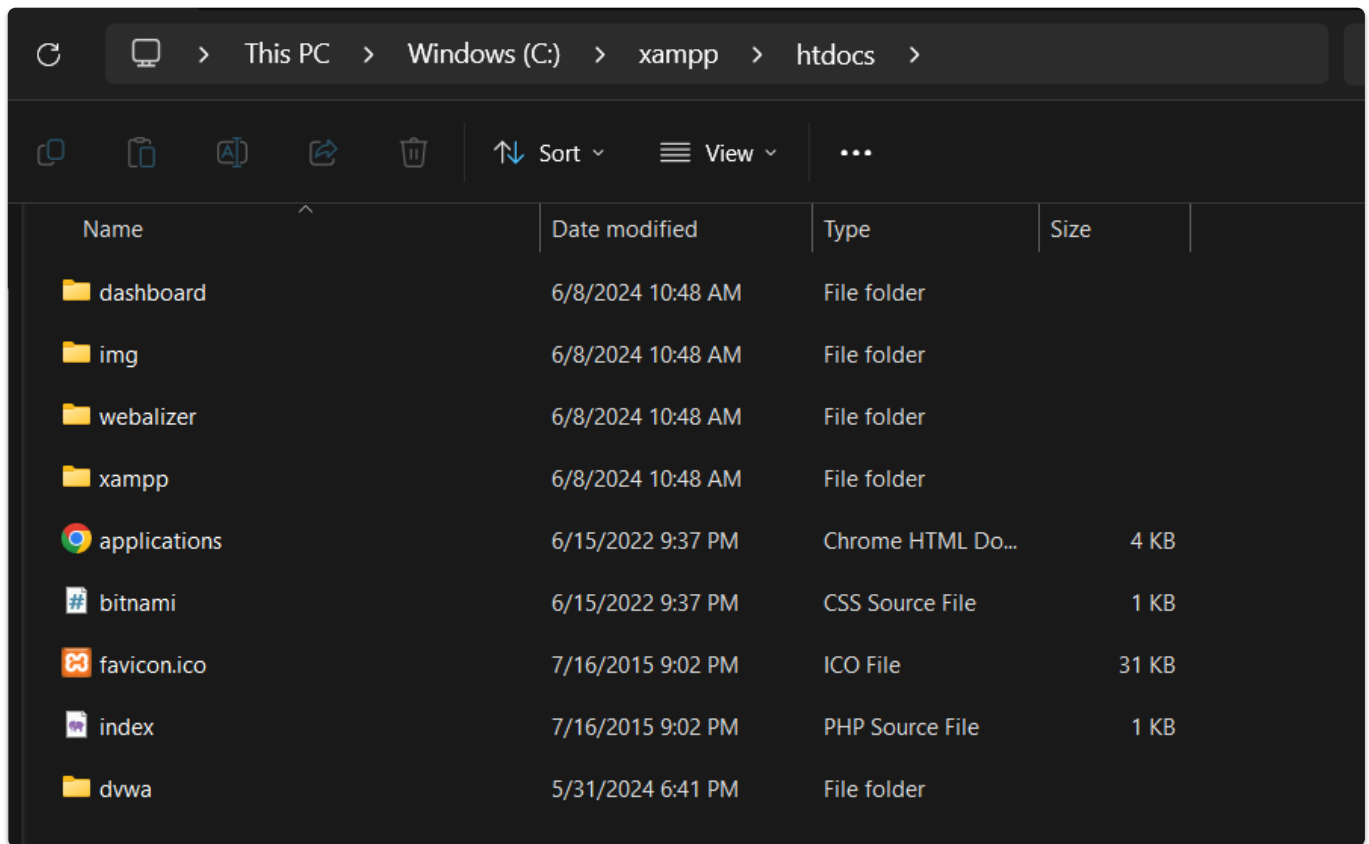
7. Rename the file to `config.inc.php`.

8. Open this file and set the following values.

```
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port' ] = '3306';
```

9. Save and close the file.

10. Finally copy the main folder and paste it in `C:\xampp\htdocs` (inside the xampp\htdocs) folder.
This directory contains files that need to be up on the website.



11. Run the **Apache** and **MySQL** service on the **xampp** control panel and go to your browser and visit `http://127.0.0.1/dvwa`

XAMPP Control Panel v3.3.0

Config
 Netstat
 Shell
 Explorer
 Services
 Help
 Quit

Service	Module	PID(s)	Port(s)	Actions
<input type="checkbox"/>	Apache	10708 8100	4433, 8000	Stop Admin Config Logs
<input type="checkbox"/>	MySQL	4976	3306	Stop Admin Config Logs
<input type="checkbox"/>	FileZilla			Start Admin Config Logs
<input type="checkbox"/>	Mercury			Start Admin Config Logs
<input type="checkbox"/>	Tomcat			Start Admin Config Logs

10:51:48 AM [main] Initializing Control Panel

10:51:48 AM [main] Windows Version: Home 64-bit

10:51:48 AM [main] XAMPP Version: 8.0.30

10:51:48 AM [main] Control Panel Version: 3.3.0 [Compiled: Apr 6th 2021]

10:51:48 AM [main] You are not running with administrator rights! This will work for most application stuff but whenever you do something with services there will be a security dialogue or things will break! So think about running this application with administrator rights!

10:51:48 AM [main] XAMPP Installation Directory: "c:\xampp"

10:51:48 AM [main] Checking for prerequisites

10:51:49 AM [main] All prerequisites found

10:51:49 AM [main] Initializing Modules

10:51:49 AM [main] The FileZilla module is disabled

10:51:49 AM [main] The Mercury module is disabled

10:51:49 AM [main] Starting Check-Timer

10:51:49 AM [main] Control Panel Ready

11:11:24 AM [Apache] Attempting to start Apache app...

11:11:24 AM [Apache] Status change detected: running

11:11:25 AM [mysql] Attempting to start MySQL app...

11:11:25 AM [mysql] Status change detected: running

localhost:8000/dvwa/setup.php

Setup DVWA
 Instructions
 About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: C:\xampp\htdocs\dvwa\config\config.inc.php

If the database already exists, it will be cleared and the data will be reset. You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: localhost

Operating system: Windows

PHP version: 8.0.30
 PHP function display_errors: Enabled
 PHP function display_startup_errors: Enabled
 PHP function allow_url_include: Enabled
 PHP function allow_url_fopen: Enabled
 PHP module gd: Installed
 PHP module mysql: Installed
 PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
 Database username: root
 Database password: "blank"
 Database database: dvwa
 Database host: 127.0.0.1
 Database port: 3306

reCAPTCHA key: **Missing**

Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\ Yes
 Writable folder C:\xampp\htdocs\dvwa\config Yes

Status in red, indicate there will be an issue when trying to complete some modules.

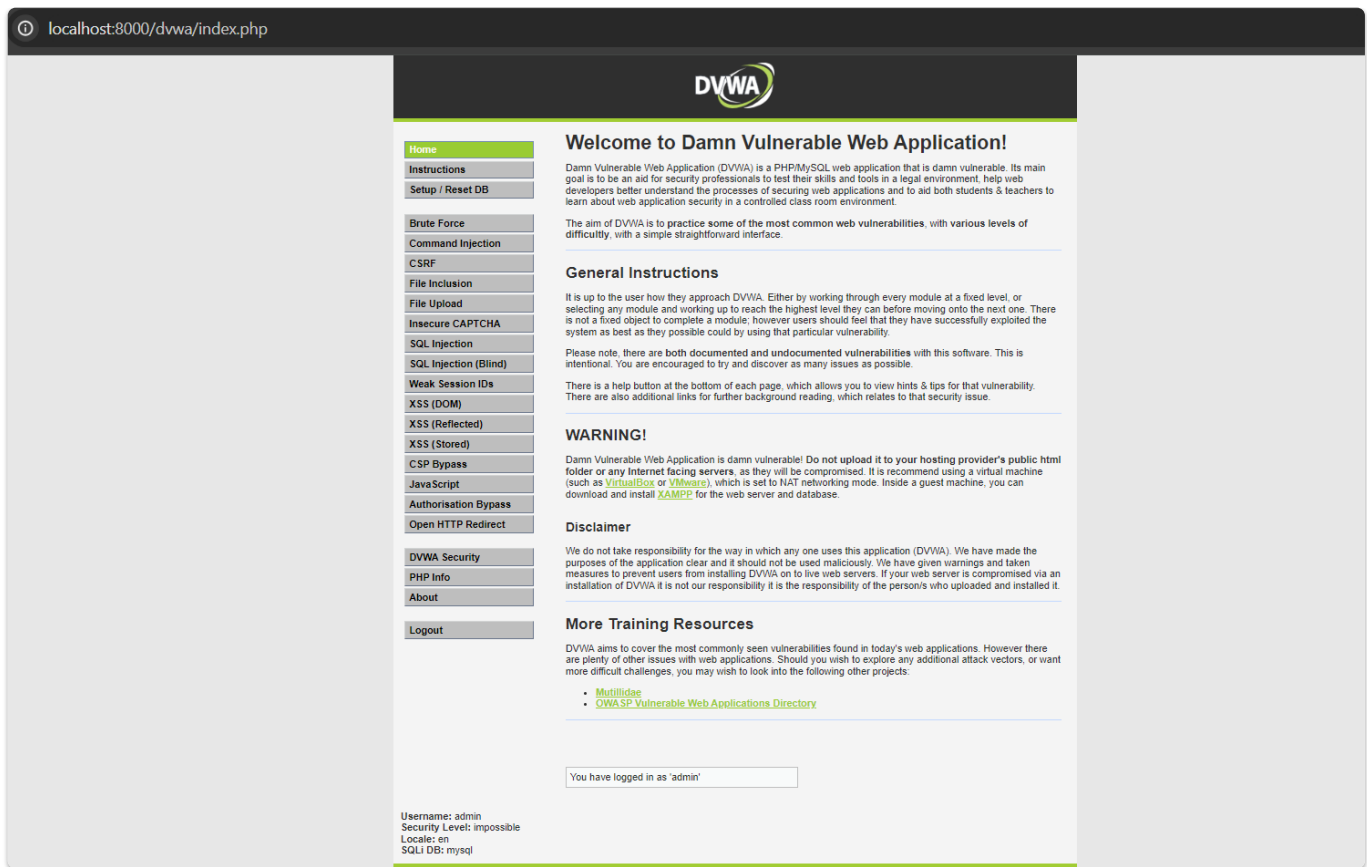
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

allow_url_fopen = On
 allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

12. Click on **Create / Reset Database** and log in using the credentials **admin | password**.



DVWA is up and running. Happy Hacking :)

DVWA SETUP ON LINUX

1. Move to `/var/www/html` and download *DVWA* from github

```
cd /var/www/html/  
git clone https://github.com/digininja/DVWA
```

2. For convenience, rename the folder from *DVWA* to *dvwa* for ease of use.

```
mv DVWA dvwa
```

3. Set read, write and execute permissions to the *dvwa* directory.

```
chmod -R 777 dvwa/
```

4. Set up username and password to access the database:

i. go to the *config* folder and change the filename from *config.inc.php.dist* to *config.inc.php*

```
cd dvwa/config  
cp config.inc.php.dist config.inc.php
```

ii. edit the php file and set the *db_user*='username_of_your_choice' and *db_password*='password_of_your_choice'

```
vim config.inc.php
```

5. Install *MySQL* on your system.

```
apt install default-mysql-server
```

6. Configure the *MySQL* database

i. Start the *MySQL* server and check if it is running

```
service mysql start  
systemctl status mysql
```

ii. Log into the *MySQL* server using super user

```
mysql -u root -p
```

iii. Create a new database and user with the username and password configured in the *dvwa* configuration file.

```
create database dvwa;  
create user 'your_username'@'127.0.0.1' identified by 'your_password'
```

be sure to replace the *your_username* and *your_password* with the username and password set in the config.inc.php file.

iv. Grant this user permission over the *dvwa* database

```
grant all privileges on dvwa.* to 'your_username'@'127.0.0.1' identified by  
'your_password'
```

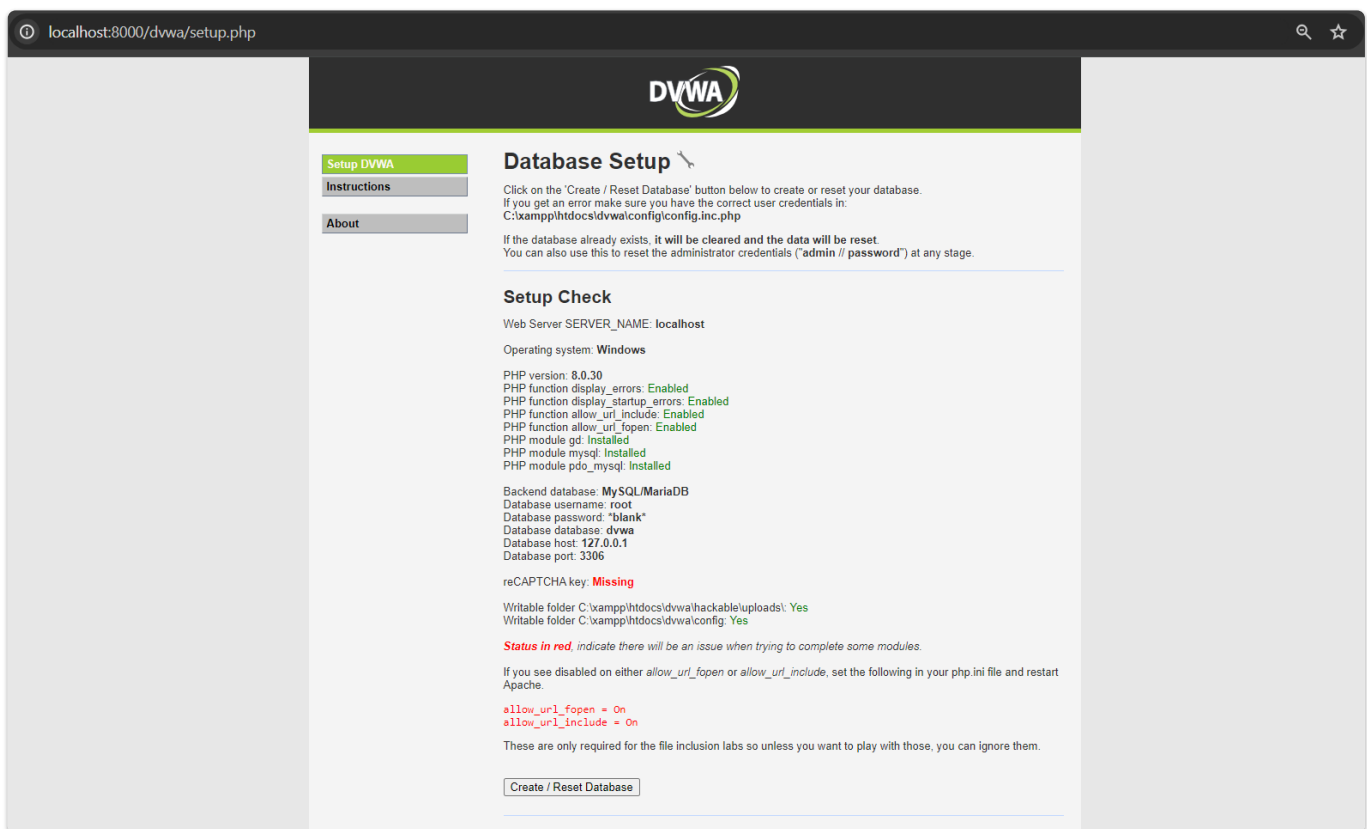
7. Edit the *php.ini* file in *apache2* and make *Allow_url_include=On* and *Allow_url_fopen=On*.

```
vim /etc/php/8.2/apache2/php.ini
```

8. Restart the *apache* and *MySQL* services

```
service apache2 restart  
service mysql restart
```

9. Visit `http://localhost/dvwa` on your browser and click on *create/reset database*



The screenshot shows a web browser window at the URL `localhost:8000/dvwa/setup.php`. The page has a dark header with the DVWA logo. On the left, there is a sidebar with links: "Setup DVWA" (highlighted in green), "Instructions", and "About". The main content area is titled "Database Setup" and contains the following text:

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
`C:\xampp\htdocs\dvwa\config\config.inc.php`

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: localhost

Operating system: Windows

PHP version: 8.0.30
PHP function display_errors: Enabled
PHP function display_startup_errors: Enabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: root
Database password: "blank"
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: **Missing**

Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\ Yes
Writable folder C:\xampp\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.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

At the bottom, there is a button labeled "Create / Reset Database".

10. Login using the username and password set by you in the *config.inc.ini* file.



Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: impossible
Locale: en
SQLi DB: mysql

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is 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 to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module, however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- [Mutillidae](#)
- [OWASP Vulnerable Web Applications Directory](#)

You have logged in as 'admin'