

# Installation DVWA In Windows 10 Using XAMPP

## How To Setup DVWA In Windows 10 Using XAMPP

Before, installation of DVWA we need to what is DVWA and why we use DVWA?

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 classroom 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. 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.

Download DVWA ><http://www.dvwa.co.uk/>

Download and install XAMPP on your computer

**6 Month & 1 Year Master Diploma in  
INFORMATION SECURITY**  
Contact us : +91 9958840889 | 7428116667

**Cyber Security  
SUMMER TRAINING**  
24x7 Online Training Available

**Register**

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

Download Link

><https://www.apachefriends.org/download.html>



Hello you there

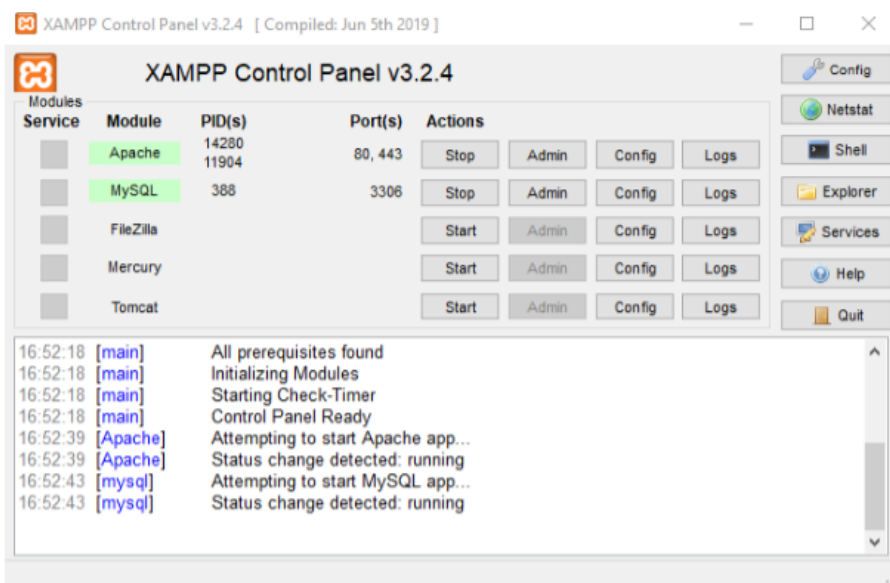
Shakarpur, New  
Delhi 110090  
Contact No.:  
+91- 951 380  
5401

Contact us

Call Now

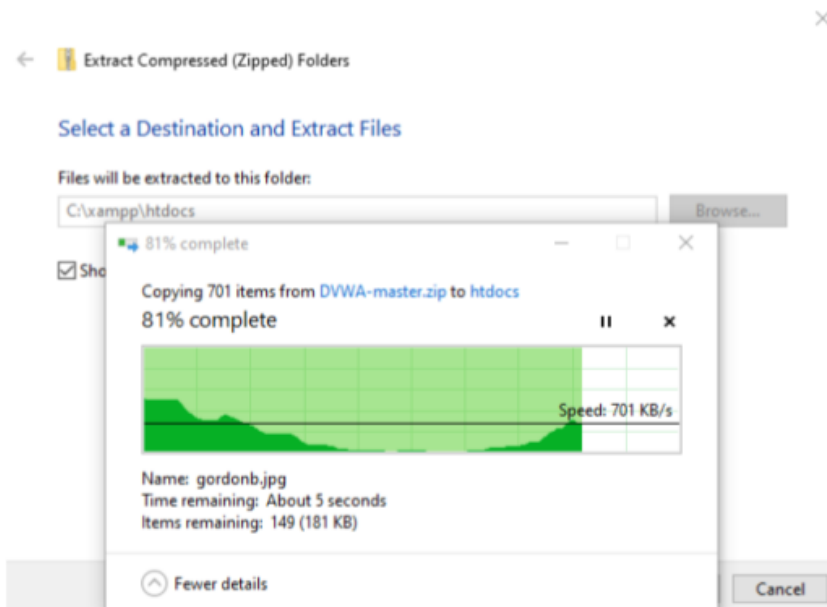


Open XAMPP and start 'Apache and MySQL'



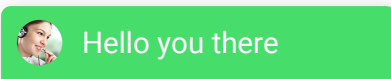
Extract DVWA downloaded file in htdocs that will be available in C:\xampp

Extract DVWA downloaded file in htdocs that will be available in C:\xampp



Open htdocs folder and rename 'DVWA-master' to 'dvwa'

And Open your Browser then type 127.0.0.1/dvwa. It will show this type of error "DVWA System error – config file not found. Copy config/config.inc.php.dist to config/config.inc.php and configure to your environment."

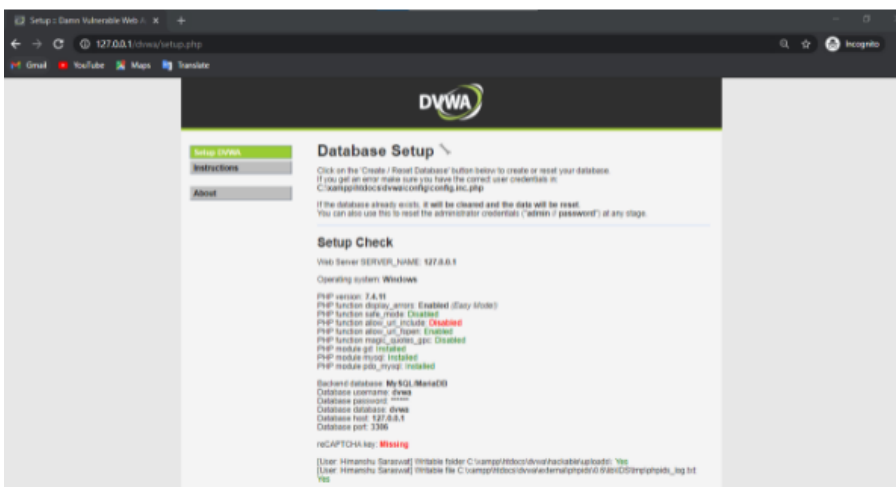




A filename 'config.inc.php.dist' rename it to 'config.inc.php' it will be available in C:\xampp\htdocs\dwva\config

Name	Date modified	Type	Size
config.inc.php	11-11-2020 17:07	PHP File	2 KB

Now, again type '127.0.0.1/dvwa' in url of the browser,



[User: Himanshu Saraswat] Writable folder C:\xampp\htdocs\dwva\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

Click on 'Create/Reset Database'

Could not connect to the database service.  
Please check the config file.  
Database Error #1045: Access denied for user  
'dvwa'@'localhost' (using password: NO).

It will show this type of error



Hello you there

config file that you rename earlier



step,

Then open it by Notepad and in the password tab, clear the password or make the password empty by remove the default password and give the username as root. (its user database user id, password).

```
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# 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';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';
```

Now , again click on 'Create / Reset Database'

[User: Himanshu Saraswat] 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

You will see this type of output,

```
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

---

Database has been created.

'users' table was created.

Data inserted into 'users' table.

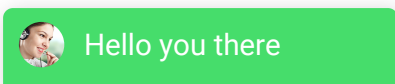
'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

**Setup successful!**

Please [login](#).



automatically redirect to login page,



Username

Password

Login

The default username is 'admin' and password is 'password'.

**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 possibly could by using that particular vulnerability.

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

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users).

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 server, as this will be compromised. It is recommended using a virtual machine.

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

DVWA Security

Great, you successfully installed DVWA in your windows 10.

## Bytecode Cyber Security

We Provide Cyber Security Training to our students,  
Corporate clients, and partners because we believe that the

...ellent output. We prepare our



Hello you there

