DVWA Configuration Setup in Windows

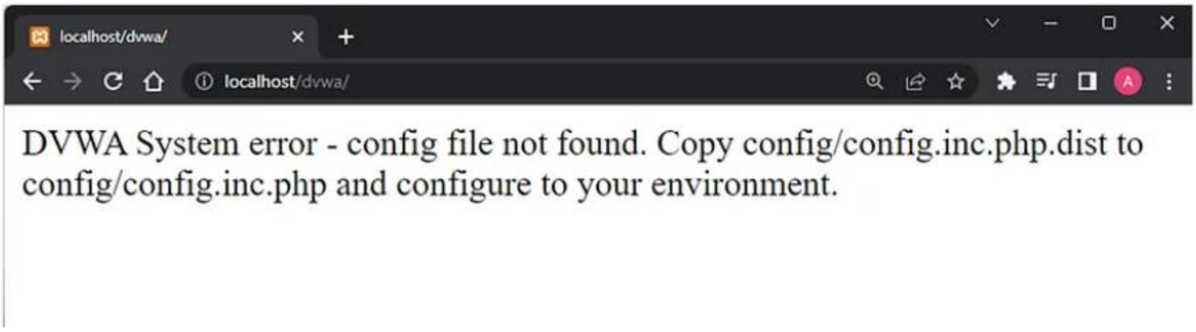
Download DVWA zip file from https://github.com/digininja/DVWA.

Put extracted DVWA file in Xampp/htdocs/

Open the XAMPP Control Panel and start the Apache and MySQL

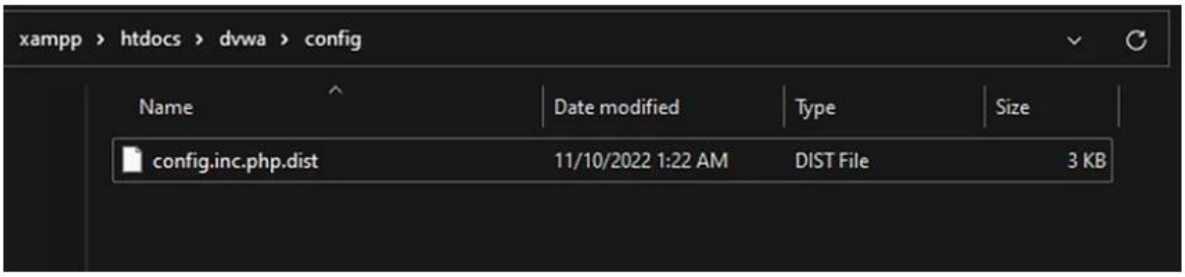
Open your Browser then type 127.0.0.1/DVWA or localhost/DVWA

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."



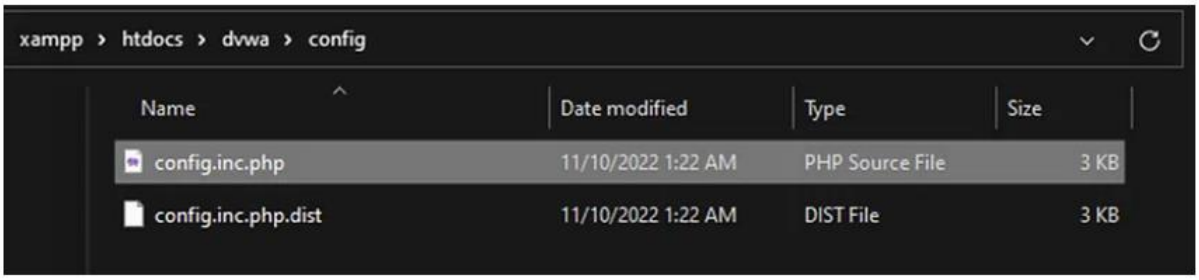
DVWA System error - config file not found. Copy config/config.inc.php.dist to config/config.inc.php and configure to your environment.

A file with name 'config.inc.php.dist' it will be available in C:/xampp/htdocs/DVWA/config,



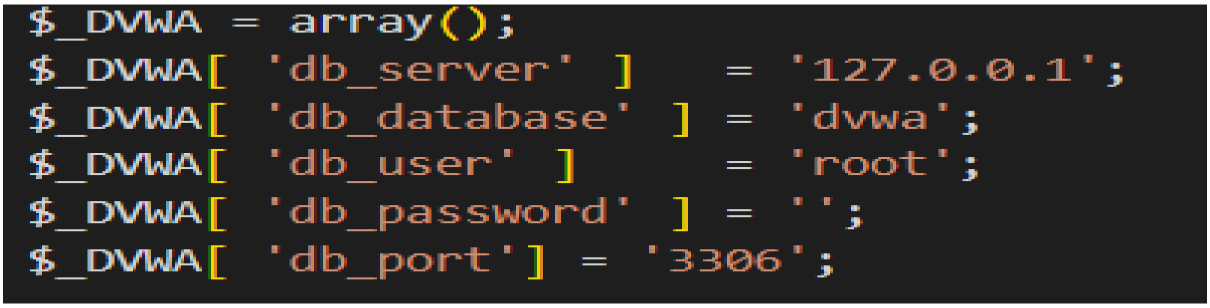
Name	Date modified	Type	Size
config.inc.php.dist	11/10/2022 1:22 AM	DIST File	3 KB

copy it in same folder & rename the copied file to 'config.inc.php'



Name	Date modified	Type	Size
config.inc.php	11/10/2022 1:22 AM	PHP Source File	3 KB
config.inc.php.dist	11/10/2022 1:22 AM	DIST File	3 KB

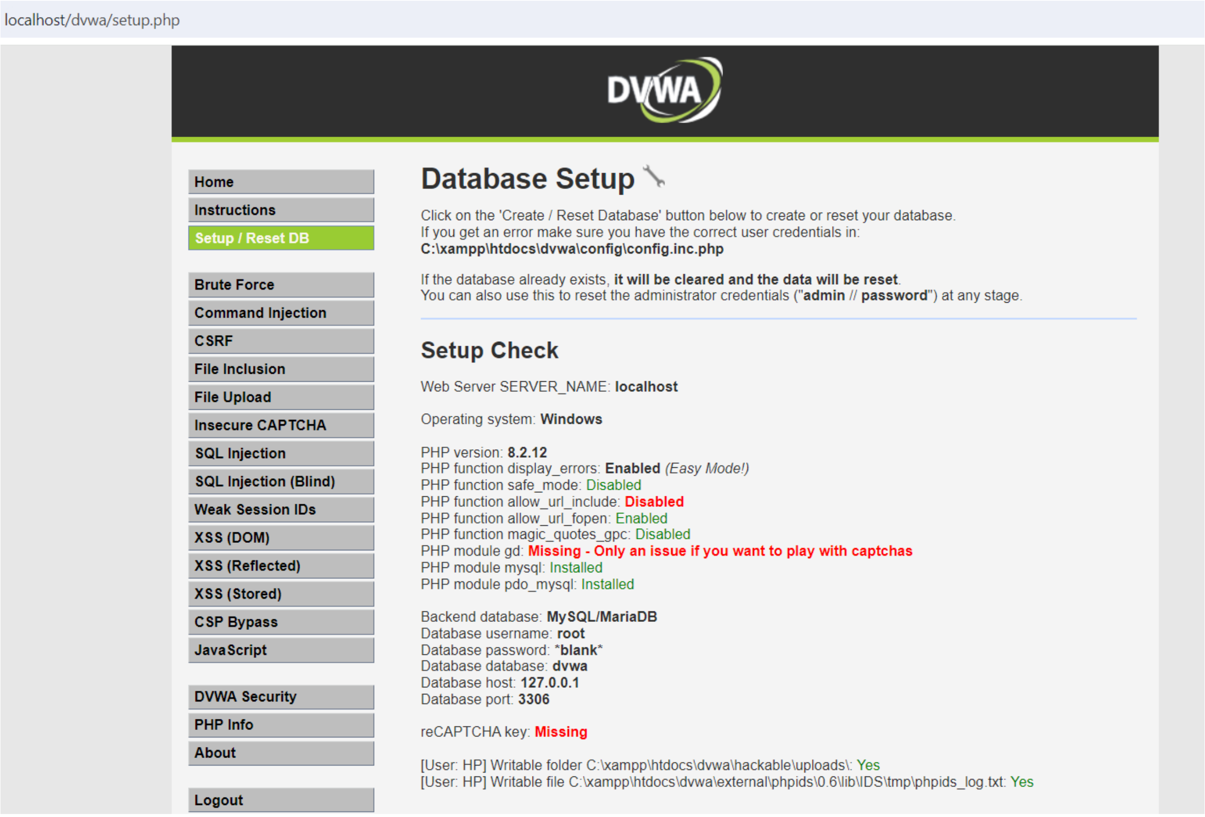
Now, you need to edit the config file that you rename earlier step, Open config.inc.php and change the below parameters-



```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

Right now, if you refresh the page, it will redirect you to localhost/DVWA/setup.php, if not then type this path. Some of the times it will redirect to login.php, means need to login to DVWA.

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



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: **8.2.12**
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: **Missing - Only an issue if you want to play with captchas**
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**

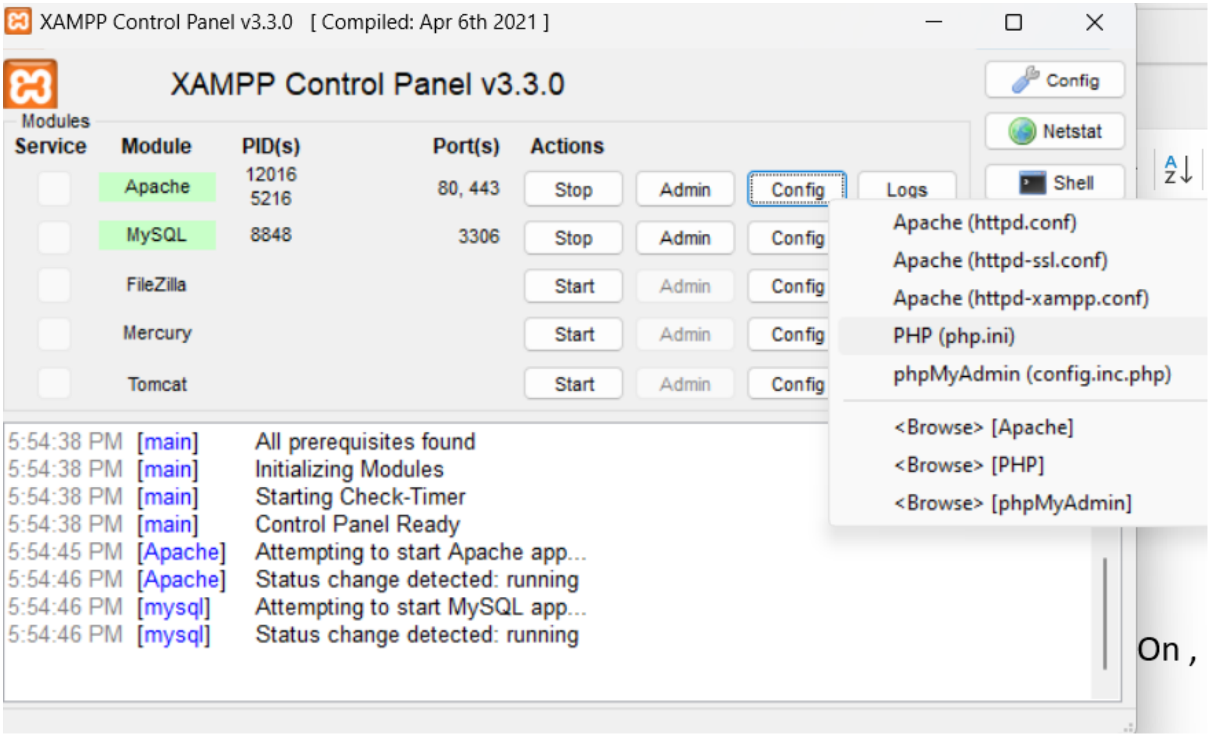
[User: HP] Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\: Yes
[User: HP] Writable file C:\xampp\htdocs\dvwa\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

When scroll down, you find that

allow_url_fopen = Off

allow_url_include = Off

It's needed to make then On, So



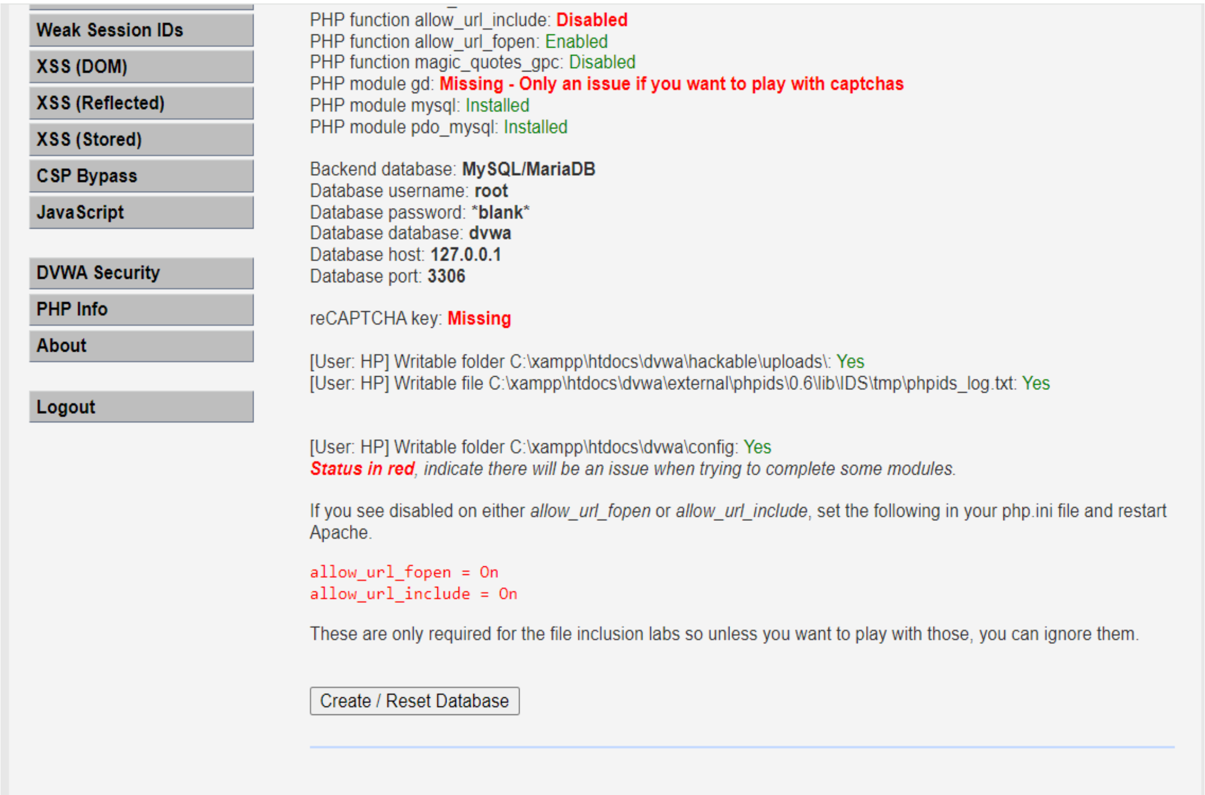
Service	Module	PID(s)	Port(s)	Actions		
	Apache	12016 5216	80, 443	Stop	Admin	Config
	MySQL	8848	3306	Stop	Admin	Config
	FileZilla			Start	Admin	Config
	Mercury			Start	Admin	Config
	Tomcat			Start	Admin	Config

```
5:54:38 PM  [main]     All prerequisites found
5:54:38 PM  [main]     Initializing Modules
5:54:38 PM  [main]     Starting Check-Timer
5:54:38 PM  [main]     Control Panel Ready
5:54:45 PM  [Apache]   Attempting to start Apache app...
5:54:46 PM  [Apache]   Status change detected: running
5:54:46 PM  [mysql]    Attempting to start MySQL app...
5:54:46 PM  [mysql]    Status change detected: running
```

Open php.ini file and do changes as –

allow_url_fopen = On

allow_url_include = On



PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
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**

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

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

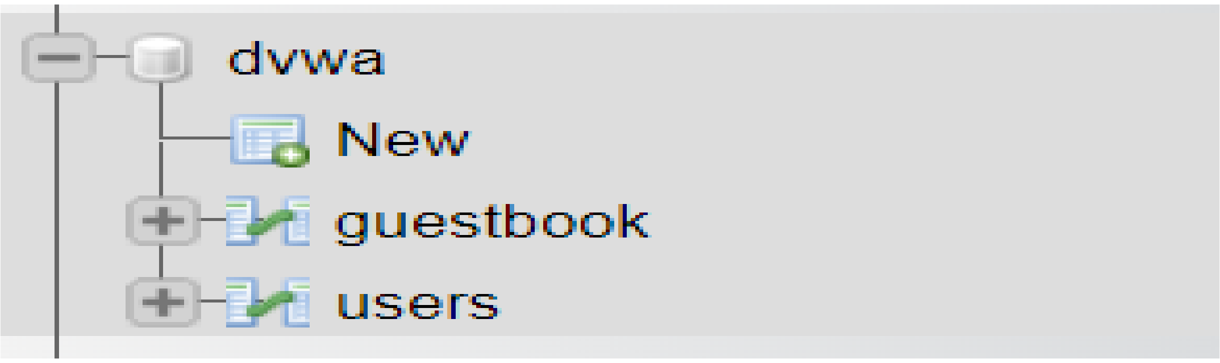
If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
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.

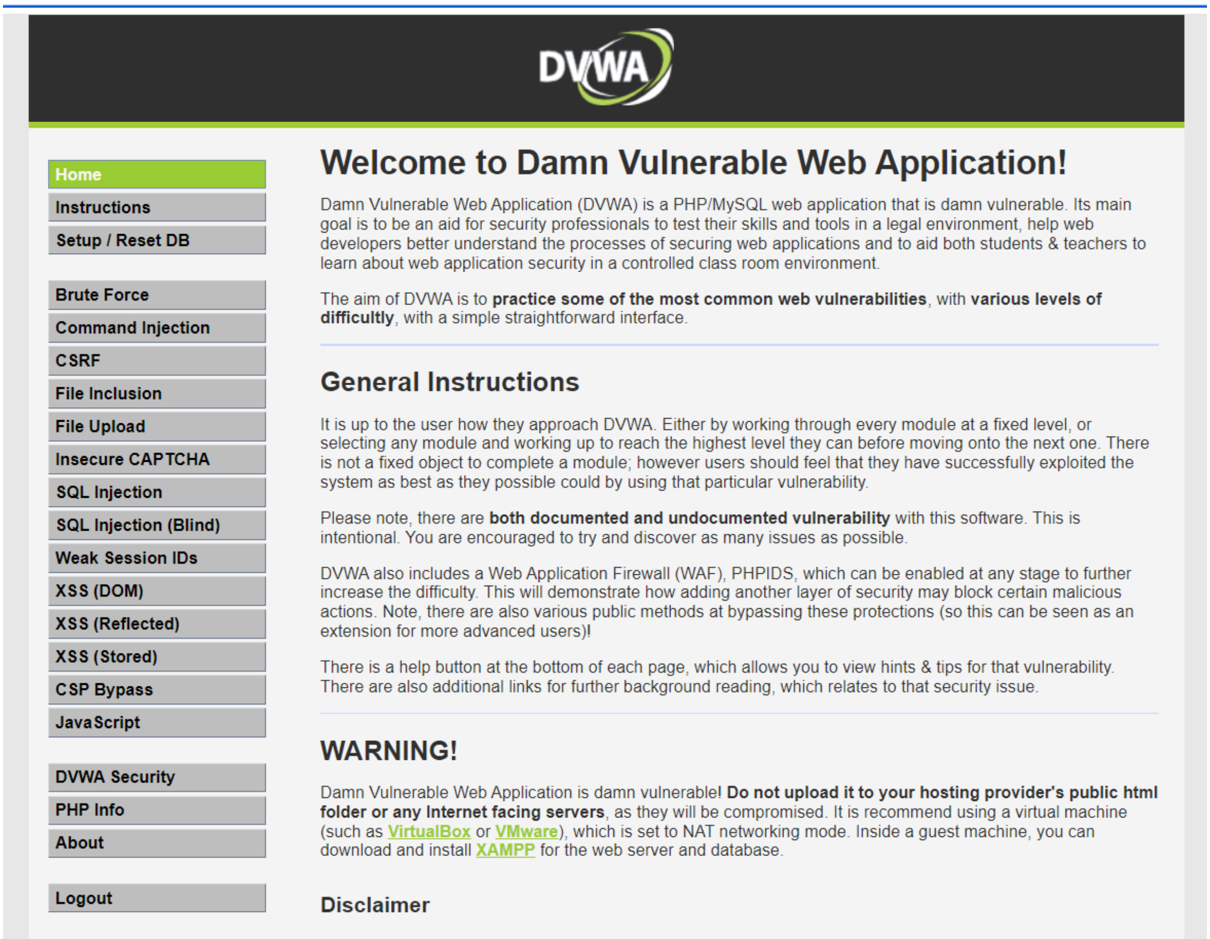
Create / Reset Database

Now, click on ‘Create / Reset Database’, This will create a database dvwa in phpMyAdmin



Great, you successfully installed DVWA in your windows 10.

http://localhost/dvwa/



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 difficultly**, 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 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 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