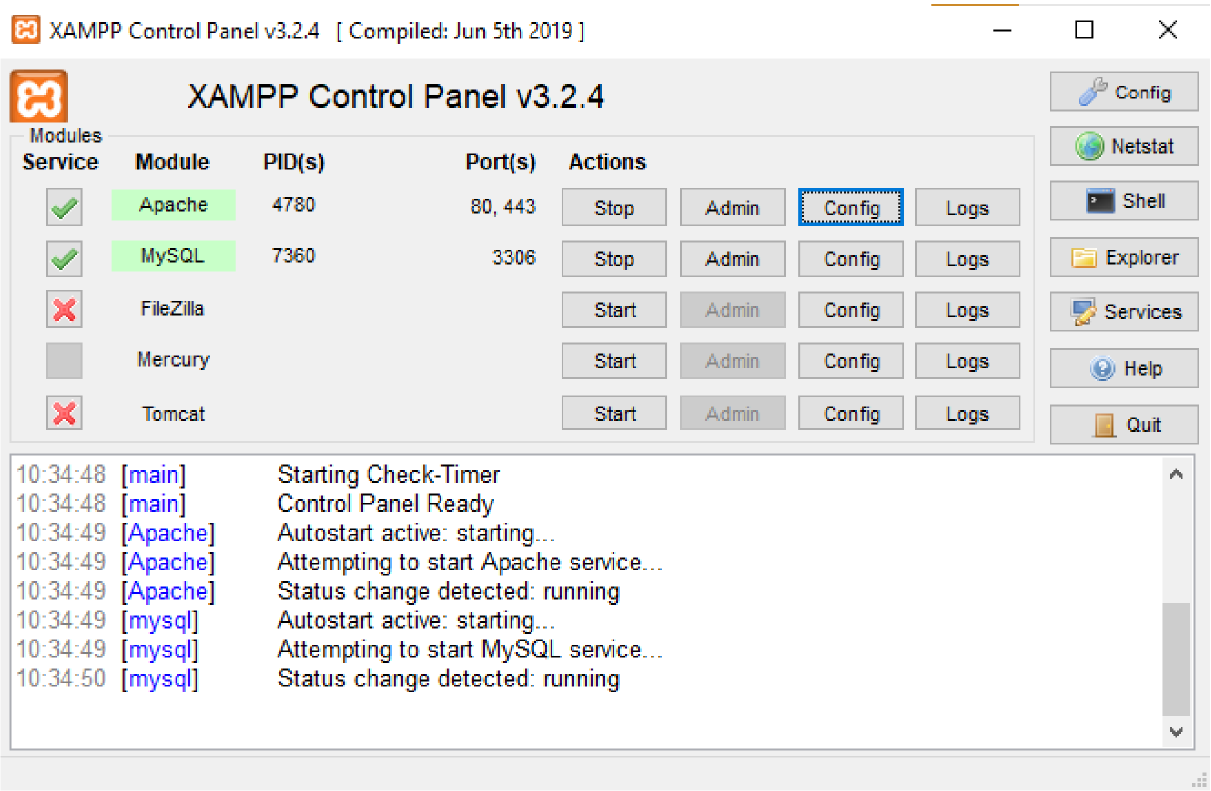
AIM:-

- Persistent Cross-Site Scripting Attack. Set up a vulnerable web application that is susceptible to persistent XSS attacks.
- Craft a malicious script to exploit the XSS vulnerability and execute arbitrary code.
- Observe the consequences of the attack and understand the potential risks associated with XSS vulnerabilities

THEORY:

Cross Site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject clientside scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Steps:
Step 1: Go to „start‟ and open XAMPP.
Step 2: Activate the module Apache and MySQL by clicking on Action button to „Start‟.
Step 3: open default browser and type „localhost/dashboard‟ and a XAMPP dashboard appears.
Edit localhost/dvwa/
Step 4: DVWA login page appears.
Step 5: Enter username as admin Password as password and login.
Step 6: Home page of DVWA appears.
Step 7: Go to DVWA security and Select the checkbox “Low”
Step 8: Go to XSS stored
Enter name and a script in the XSS guestbook field.



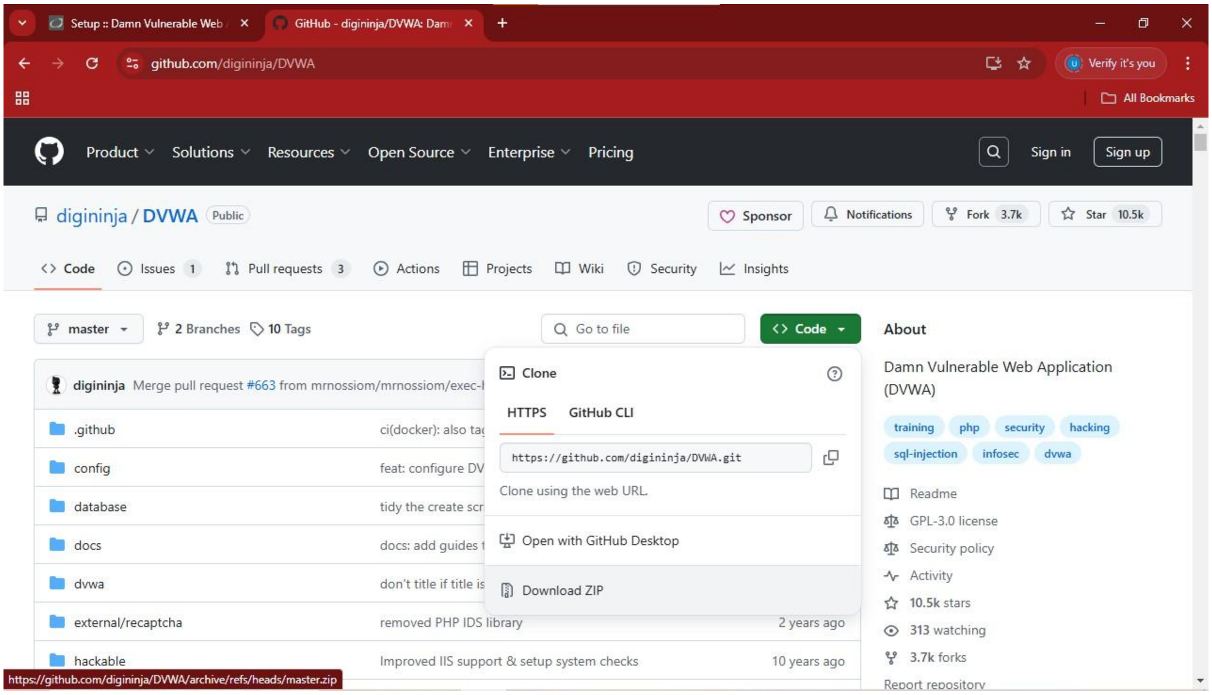
XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]

XAMPP Control Panel v3.2.4

Modules

Service	Module	PID(s)	Port(s)	Actions			
✓	Apache	4780	80, 443	Stop	Admin	Config	Logs
✓	MySQL	7360	3306	Stop	Admin	Config	Logs
☒	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
☒	Tomcat			Start	Admin	Config	Logs

```
10:34:48  [main]     Starting Check-Timer
10:34:48  [main]     Control Panel Ready
10:34:49  [Apache]   Autostart active: starting...
10:34:49  [Apache]   Attempting to start Apache service...
10:34:49  [Apache]   Status change detected: running
10:34:49  [mysql]    Autostart active: starting...
10:34:49  [mysql]    Attempting to start MySQL service...
10:34:50  [mysql]    Status change detected: running
```



digininja / DVWA Public

digininja Merge pull request #663 from mrnossiom/mrnossiom/exec-

.github	ci(docker): also tag	
config	feat: configure DV	
database	tidy the create scr	
docs	docs: add guides f	
dvwa	don't title if title is	
external/recaptcha	removed PHP IDS library	2 years ago
hackable	Improved IIS support & setup system checks	10 years ago

Clone

HTTPS GitHub CLI

https://github.com/digininja/DVWA.git

Clone using the web URL.

Open with GitHub Desktop

Download ZIP

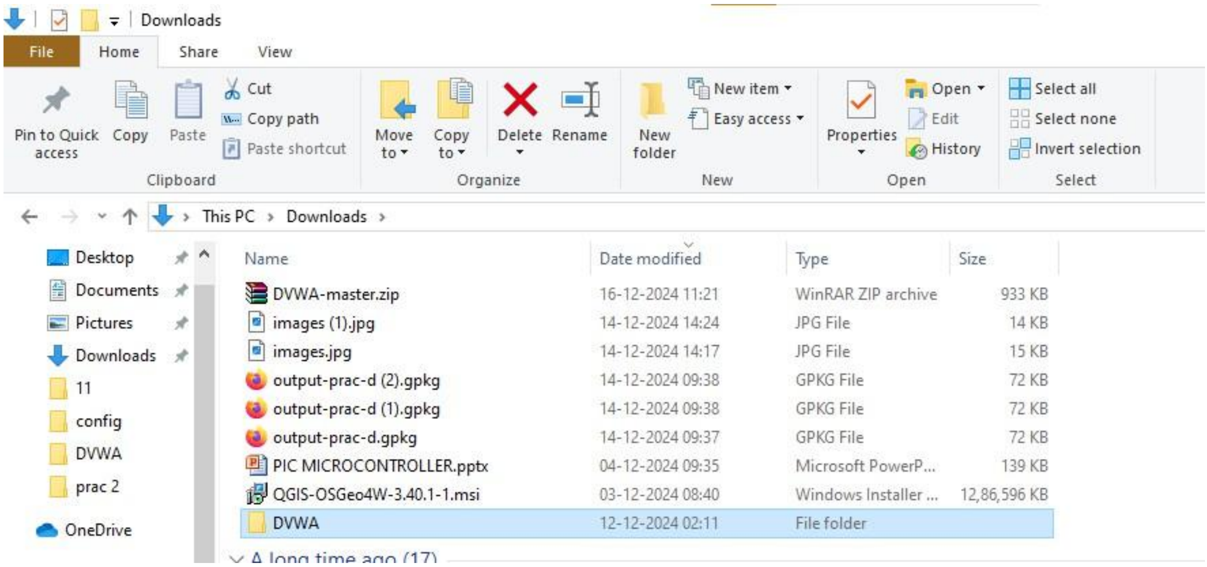
About

Damn Vulnerable Web Application (DVWA)

training php security hacking sql-injection infosec dvwa

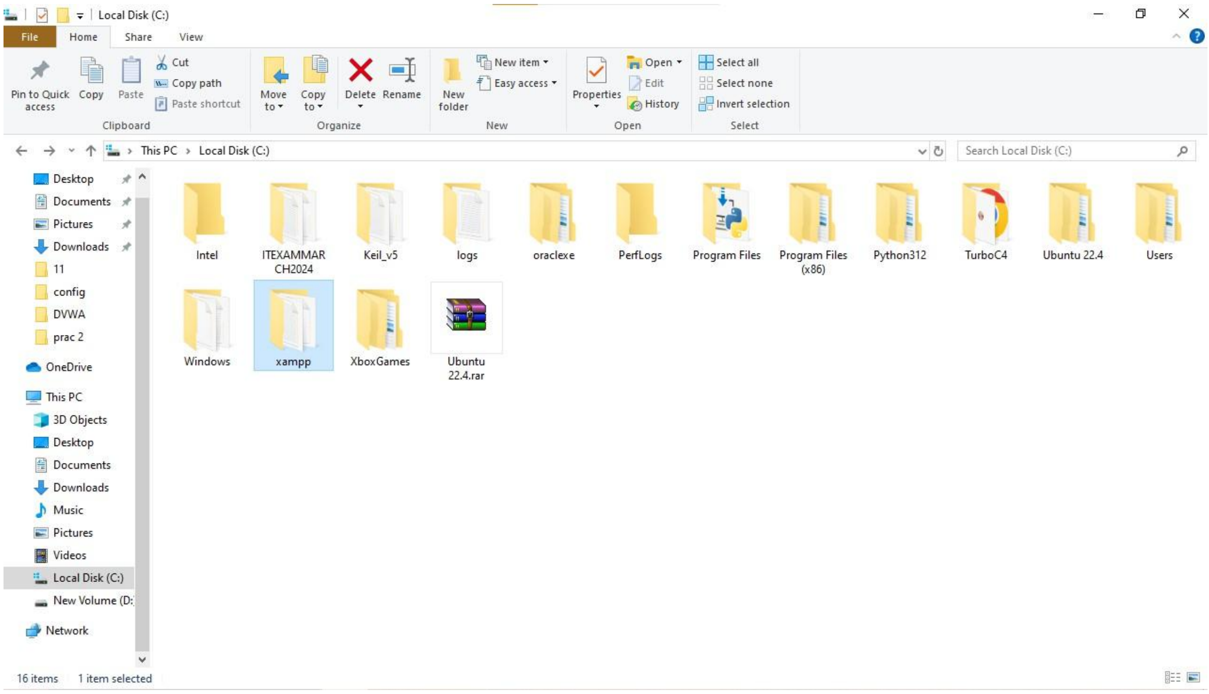
Readme
GPL-3.0 license
Security policy
Activity
10.5k stars
313 watching
3.7k forks
Report repository

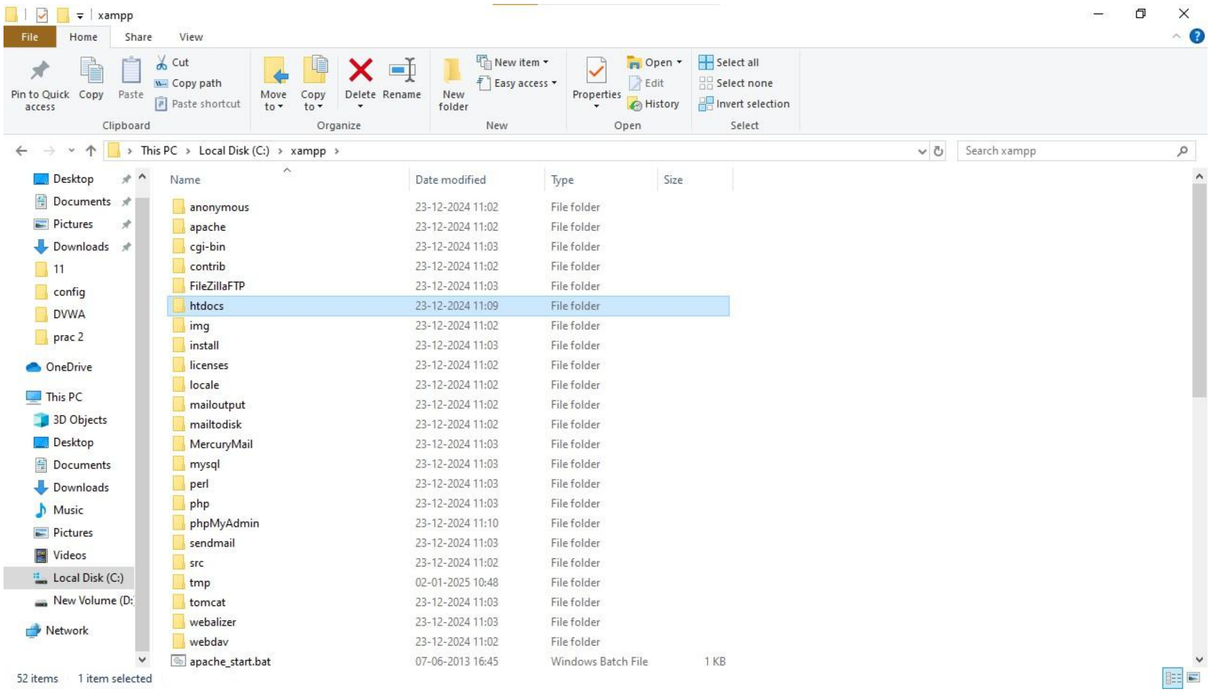
https://github.com/digininja/DVWA/archive/refs/heads/master.zip



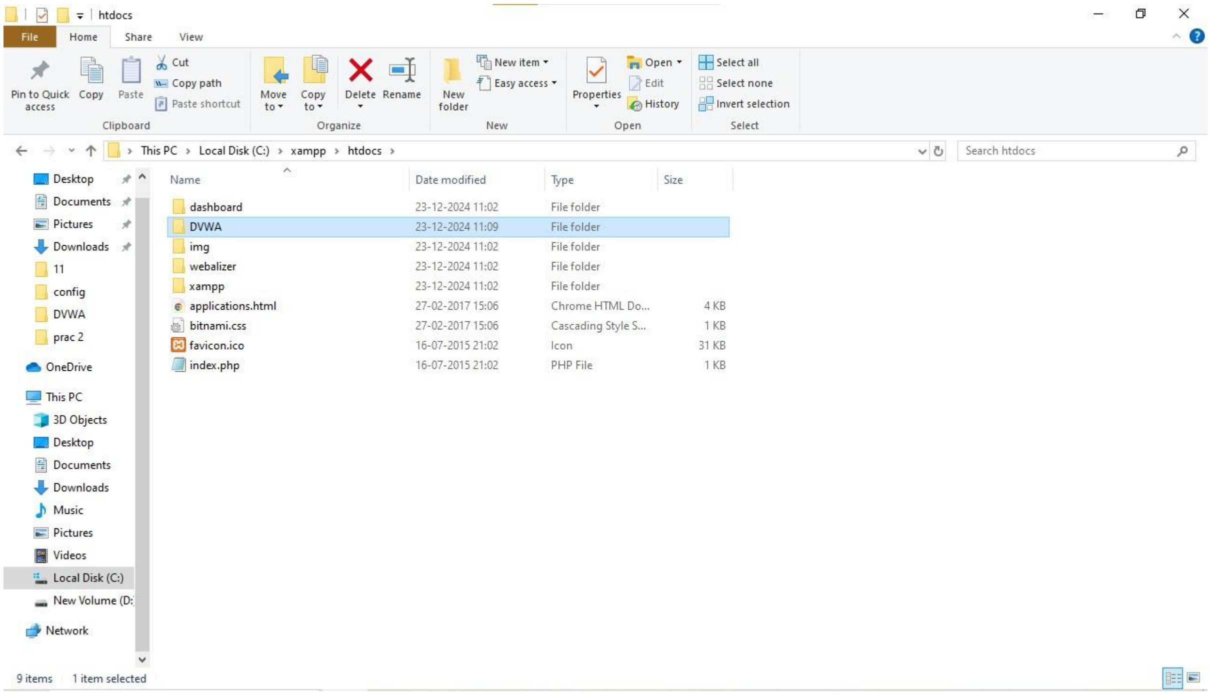
Name	Date modified	Type	Size
DVWA-master.zip	16-12-2024 11:21	WinRAR ZIP archive	933 KB
images (1).jpg	14-12-2024 14:24	JPG File	14 KB
images.jpg	14-12-2024 14:17	JPG File	15 KB
output-prac-d (2).gpkg	14-12-2024 09:38	GPKG File	72 KB
output-prac-d (1).gpkg	14-12-2024 09:38	GPKG File	72 KB
output-prac-d.gpkg	14-12-2024 09:37	GPKG File	72 KB
PIC MICROCONTROLLER.pptx	04-12-2024 09:35	Microsoft PowerP...	139 KB
QGIS-OSGeo4W-3.40.1-1.msi	03-12-2024 08:40	Windows Installer ...	12,86,596 KB
DVWA	12-12-2024 02:11	File folder	

A long time ago (17)

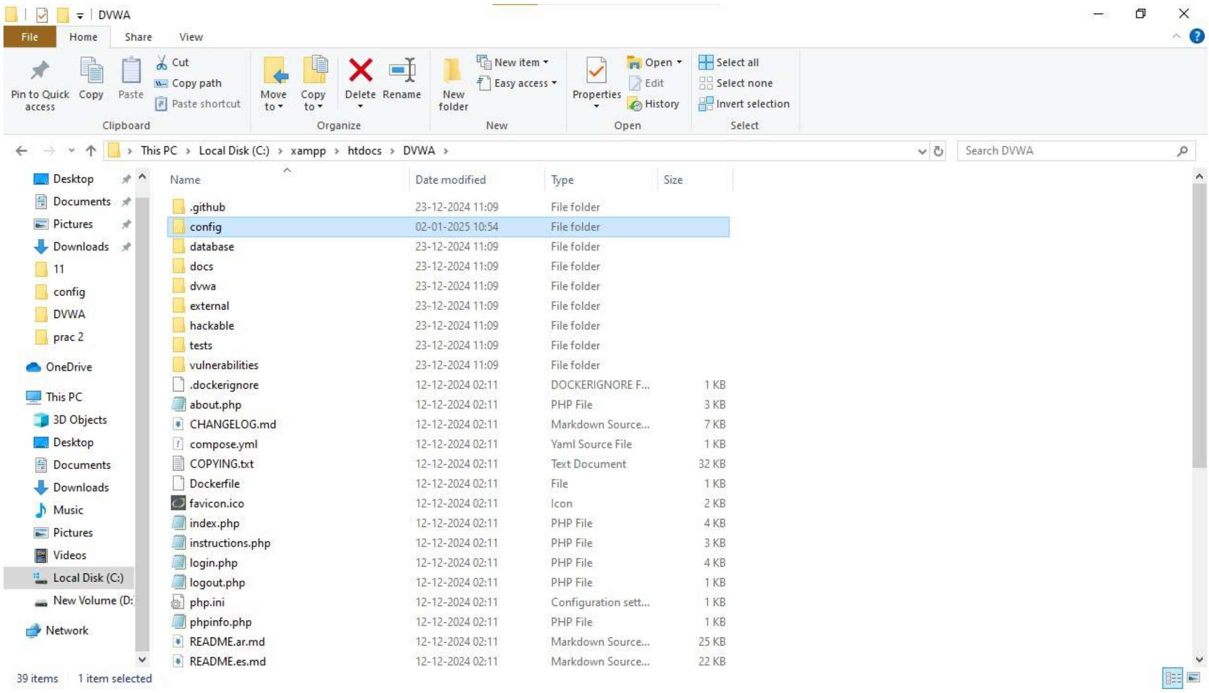




Name	Date modified	Type	Size
anonymous	23-12-2024 11:02	File folder	
apache	23-12-2024 11:02	File folder	
cgi-bin	23-12-2024 11:03	File folder	
contrib	23-12-2024 11:02	File folder	
FileZillaFTP	23-12-2024 11:03	File folder	
htdocs	23-12-2024 11:09	File folder	
img	23-12-2024 11:02	File folder	
install	23-12-2024 11:03	File folder	
licenses	23-12-2024 11:02	File folder	
locale	23-12-2024 11:02	File folder	
mailoutput	23-12-2024 11:02	File folder	
mailtodisk	23-12-2024 11:02	File folder	
MercuryMail	23-12-2024 11:03	File folder	
mysql	23-12-2024 11:03	File folder	
perl	23-12-2024 11:03	File folder	
php	23-12-2024 11:03	File folder	
phpMyAdmin	23-12-2024 11:10	File folder	
sendmail	23-12-2024 11:03	File folder	
src	23-12-2024 11:02	File folder	
tmp	02-01-2025 10:48	File folder	
tomcat	23-12-2024 11:03	File folder	
webalizer	23-12-2024 11:03	File folder	
webdav	23-12-2024 11:02	File folder	
apache_start.bat	07-06-2013 16:45	Windows Batch File	1 KB



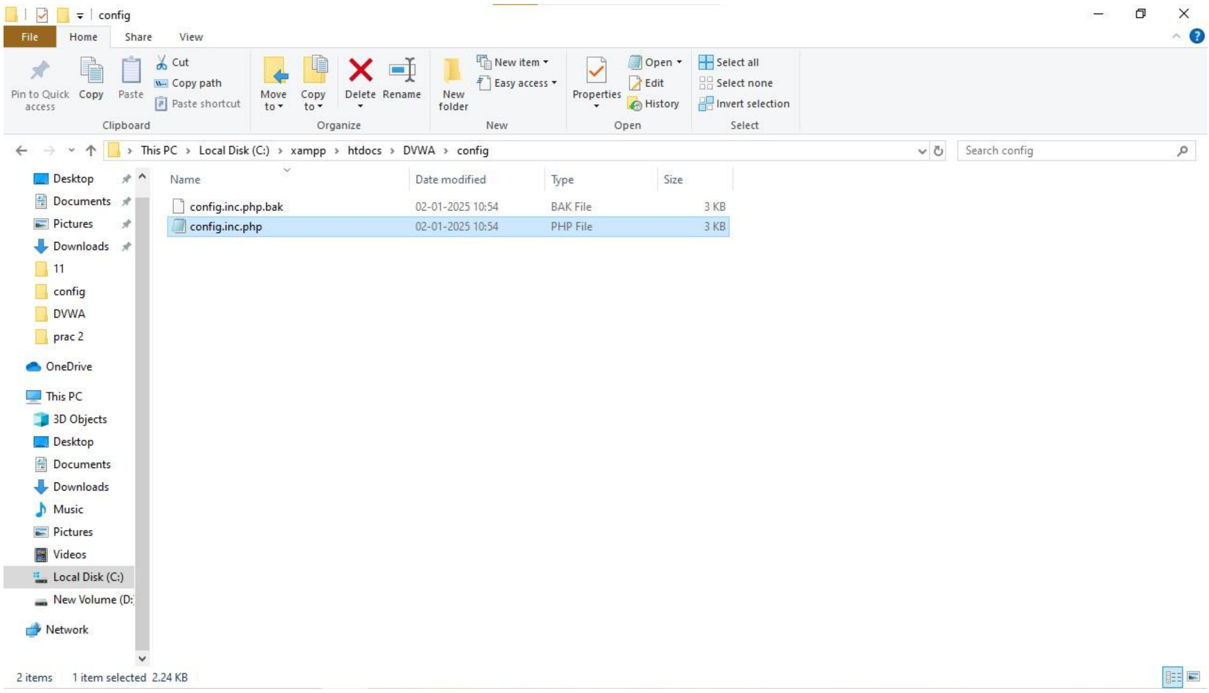
Name	Date modified	Type	Size
dashboard	23-12-2024 11:02	File folder	
DVWA	23-12-2024 11:09	File folder	
img	23-12-2024 11:02	File folder	
webalizer	23-12-2024 11:02	File folder	
xampp	23-12-2024 11:02	File folder	
applications.html	27-02-2017 15:06	Chrome HTML Do...	4 KB
bitnami.css	27-02-2017 15:06	Cascading Style S...	1 KB
favicon.ico	16-07-2015 21:02	Icon	31 KB
index.php	16-07-2015 21:02	PHP File	1 KB



This PC › Local Disk (C:) › xampp › htdocs › DVWA ›

Name	Date modified	Type	Size
.github	23-12-2024 11:09	File folder	
config	02-01-2025 10:54	File folder	
database	23-12-2024 11:09	File folder	
docs	23-12-2024 11:09	File folder	
dvwa	23-12-2024 11:09	File folder	
external	23-12-2024 11:09	File folder	
hackable	23-12-2024 11:09	File folder	
tests	23-12-2024 11:09	File folder	
vulnerabilities	23-12-2024 11:09	File folder	
.dockerignore	12-12-2024 02:11	DOCKERIGNORE F...	1 KB
about.php	12-12-2024 02:11	PHP File	3 KB
CHANGELOG.md	12-12-2024 02:11	Markdown Source...	7 KB
compose.yml	12-12-2024 02:11	Yaml Source File	1 KB
COPYING.txt	12-12-2024 02:11	Text Document	32 KB
Dockerfile	12-12-2024 02:11	File	1 KB
favicon.ico	12-12-2024 02:11	Icon	2 KB
index.php	12-12-2024 02:11	PHP File	4 KB
instructions.php	12-12-2024 02:11	PHP File	3 KB
login.php	12-12-2024 02:11	PHP File	4 KB
logout.php	12-12-2024 02:11	PHP File	1 KB
php.ini	12-12-2024 02:11	Configuration sett...	1 KB
phpinfo.php	12-12-2024 02:11	PHP File	1 KB
README.ar.md	12-12-2024 02:11	Markdown Source...	25 KB
README.es.md	12-12-2024 02:11	Markdown Source...	22 KB

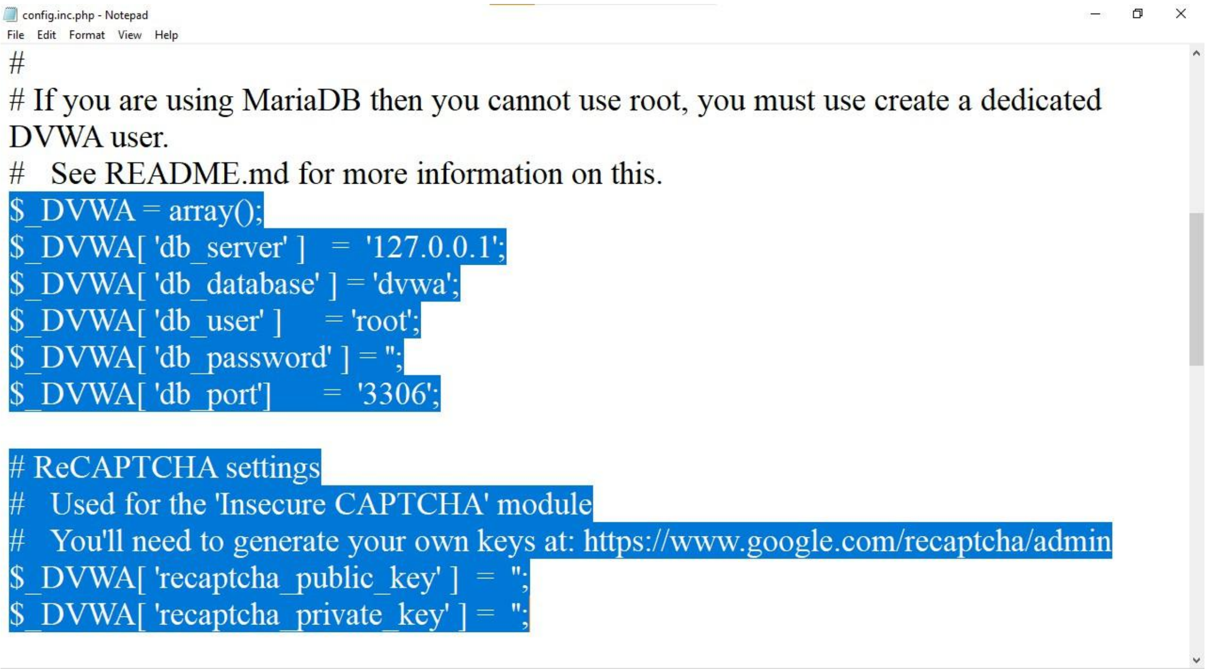
39 items 1 item selected



This PC › Local Disk (C:) › xampp › htdocs › DVWA › config

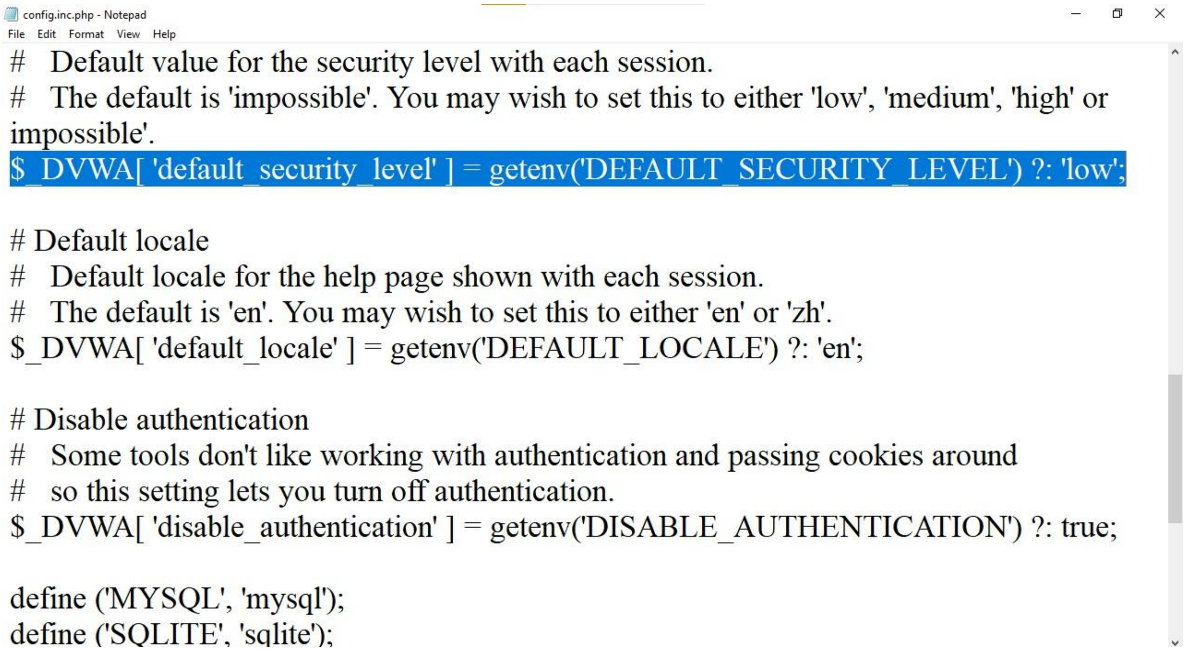
Name	Date modified	Type	Size
config.inc.php.bak	02-01-2025 10:54	BAK File	3 KB
config.inc.php	02-01-2025 10:54	PHP File	3 KB

2 items 1 item selected 2.24 KB



```
#
# 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' ] =  '';
```

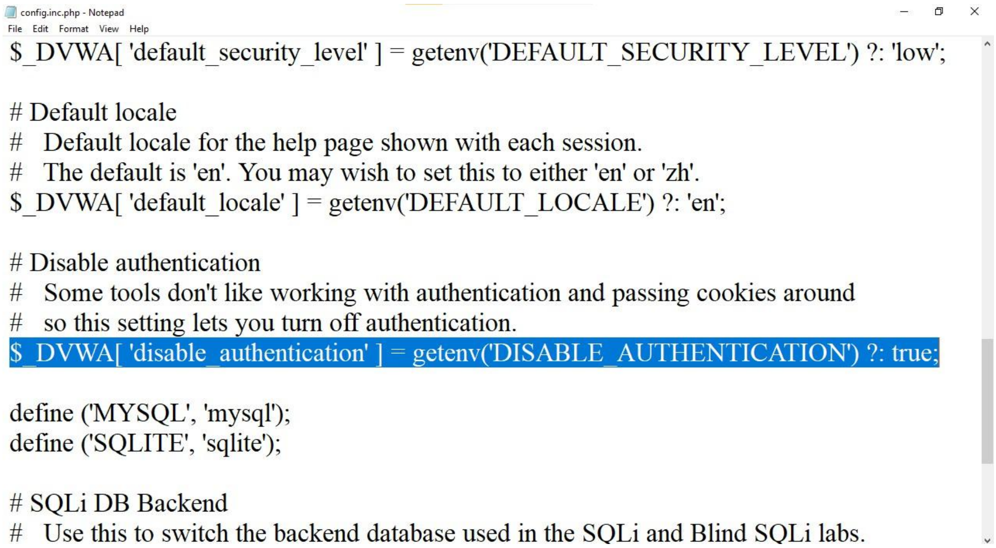


```
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or
impossible'.
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = getenv('DEFAULT_LOCALE') ?: 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = getenv('DISABLE_AUTHENTICATION') ?: true;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');
```



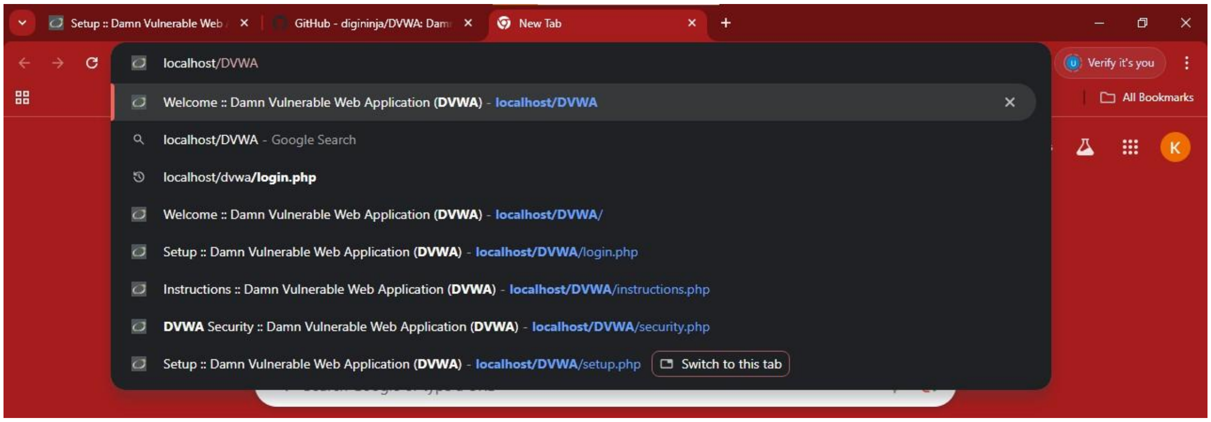
```
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = getenv('DEFAULT_LOCALE') ?: 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = getenv('DISABLE_AUTHENTICATION') ?: true;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
```



localhost/DVWA

Welcome :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA

localhost/DVWA - Google Search

localhost/dvwa/login.php

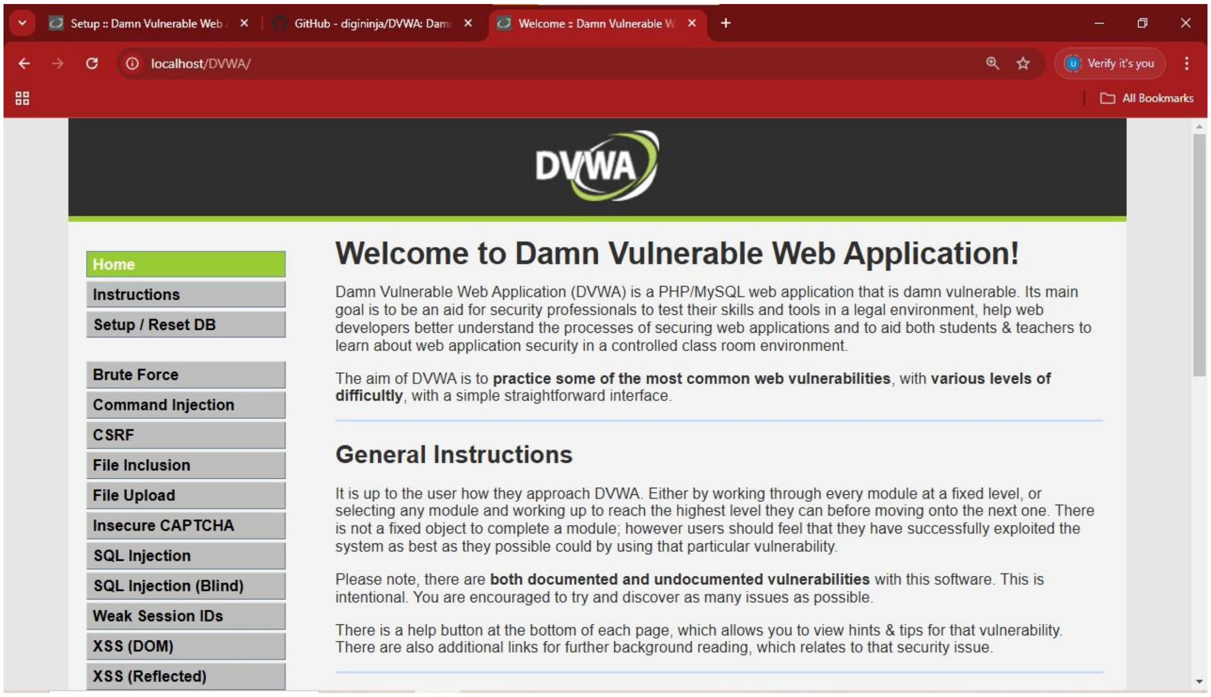
Welcome :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/

Setup :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/login.php

Instructions :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/instructions.php

DVWA Security :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/security.php

Setup :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/setup.php



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.

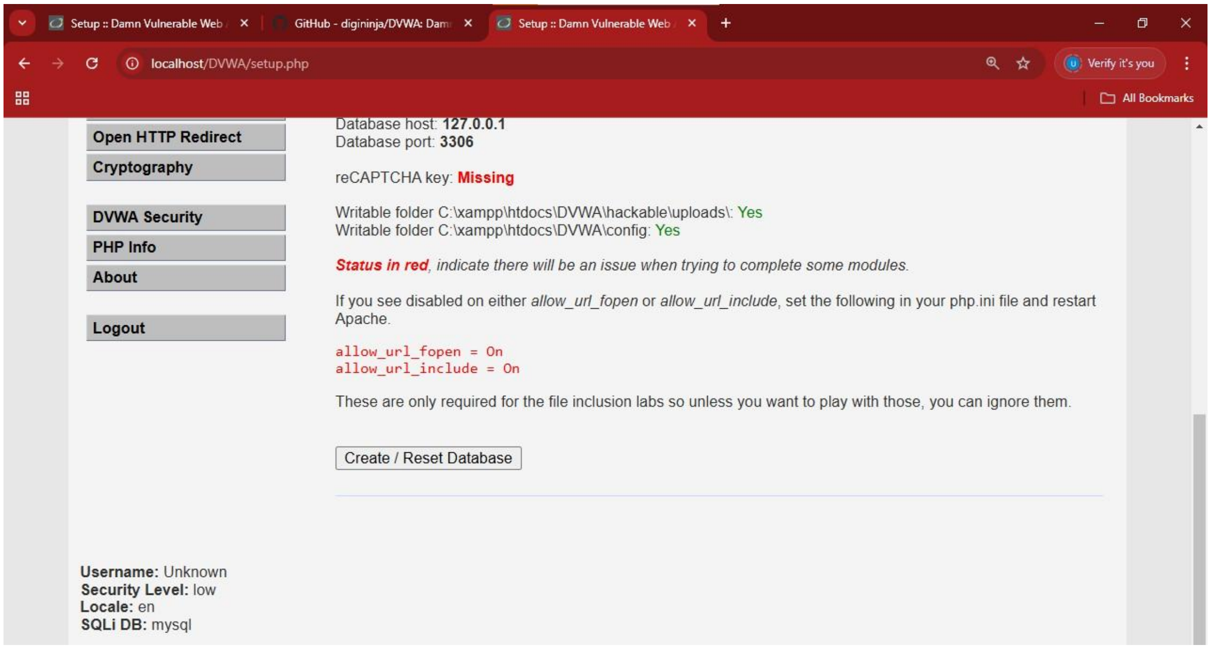
The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

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 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.



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.*

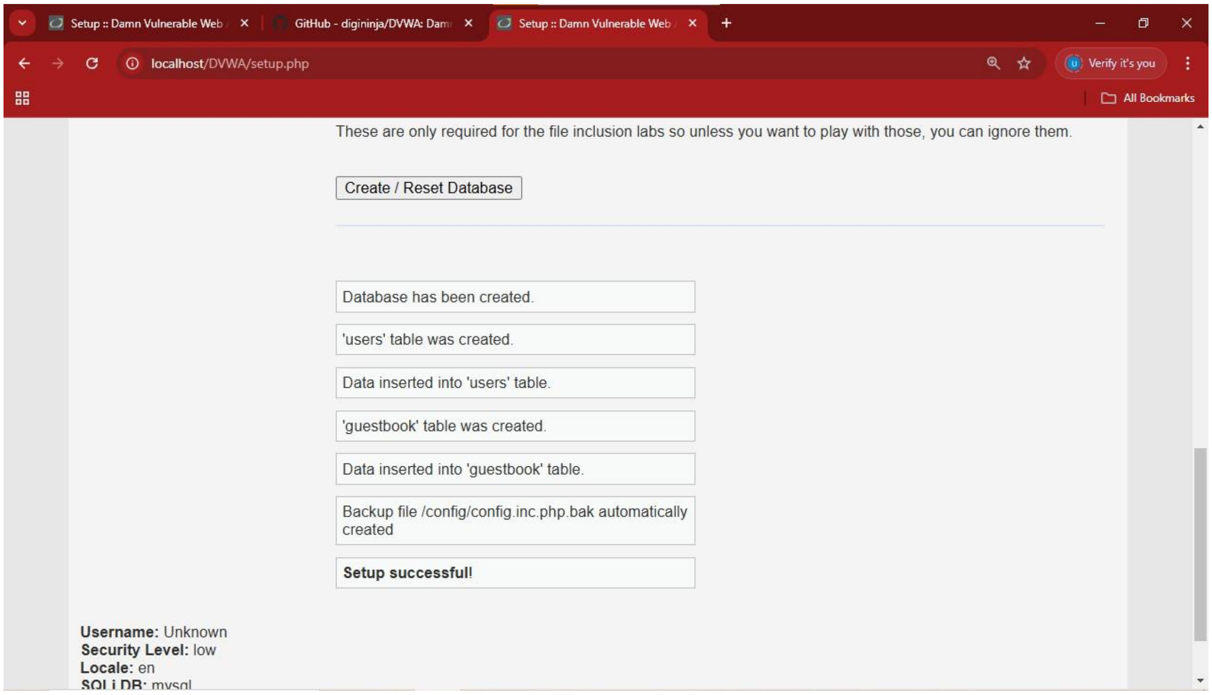
If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
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

Username: Unknown
Security Level: low
Locale: en
SQLi DB: mysql


Setup :: Damn Vulnerable Web
GitHub - digininja/DVWA: Dam
Setup :: Damn Vulnerable Web
localhost/DVWA/setup.php
Verify it's you
All Bookmarks

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.

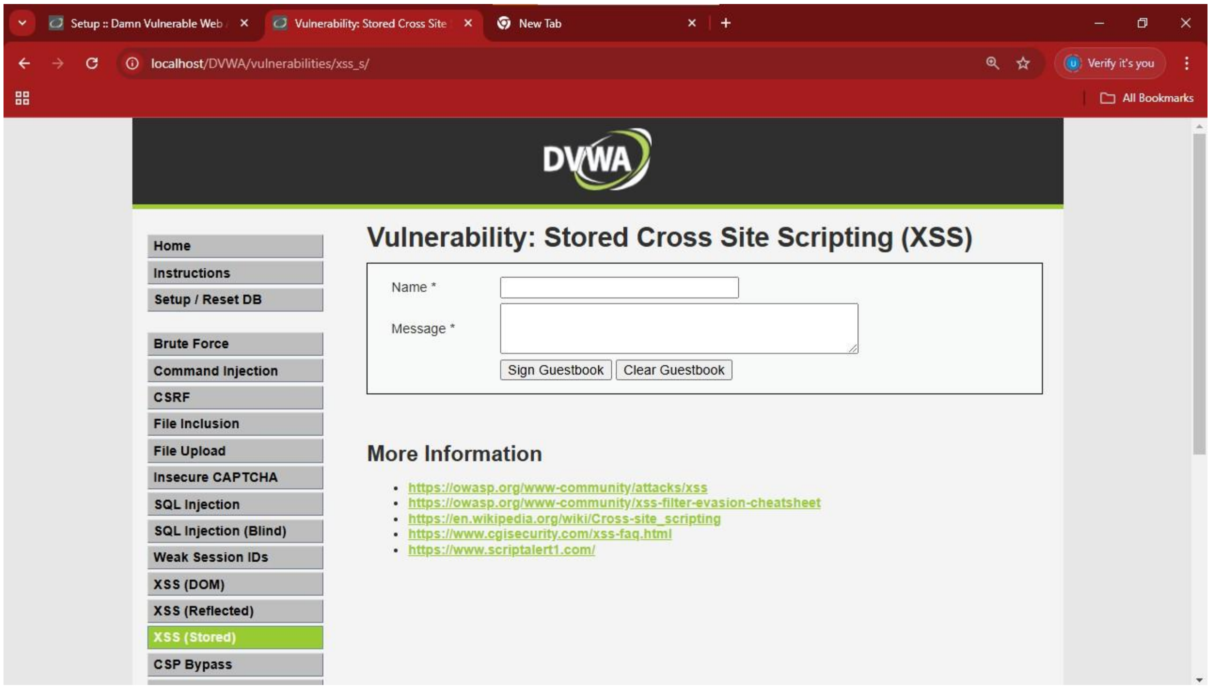
'guestbook' table was created.

Data inserted into 'guestbook' table.

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

Setup successful!

Username: Unknown
Security Level: low
Locale: en
SQLi DB: mysql



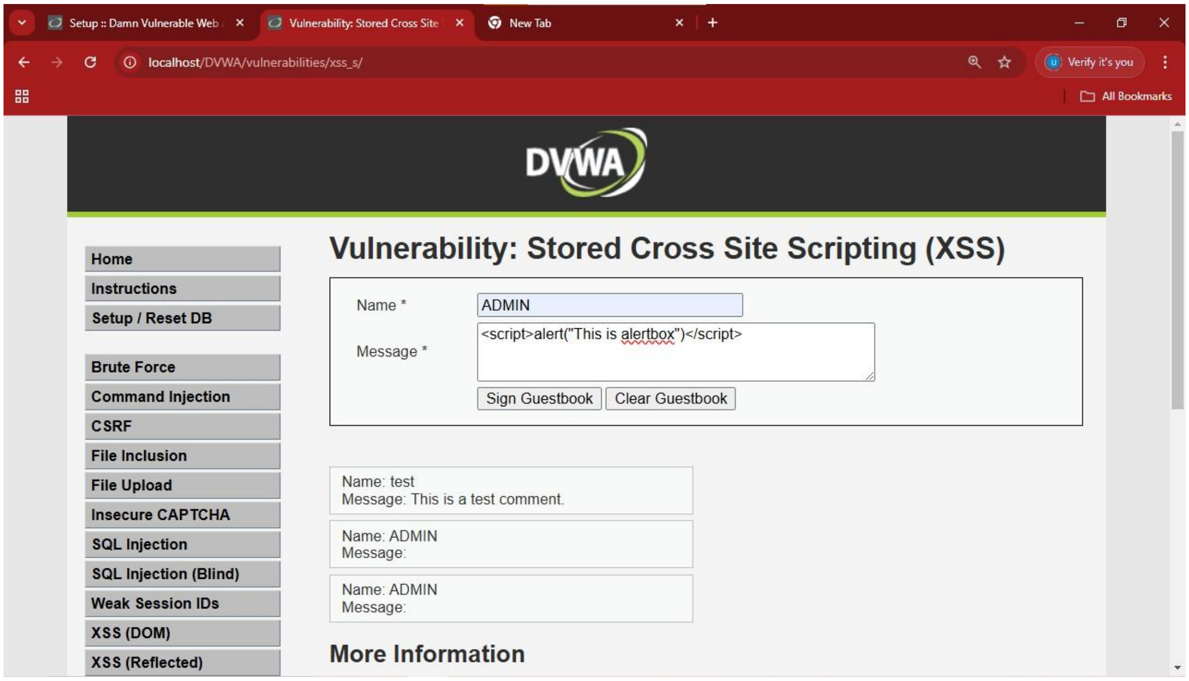
Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/



Vulnerability: Stored Cross Site Scripting (XSS)

Name * ADMIN

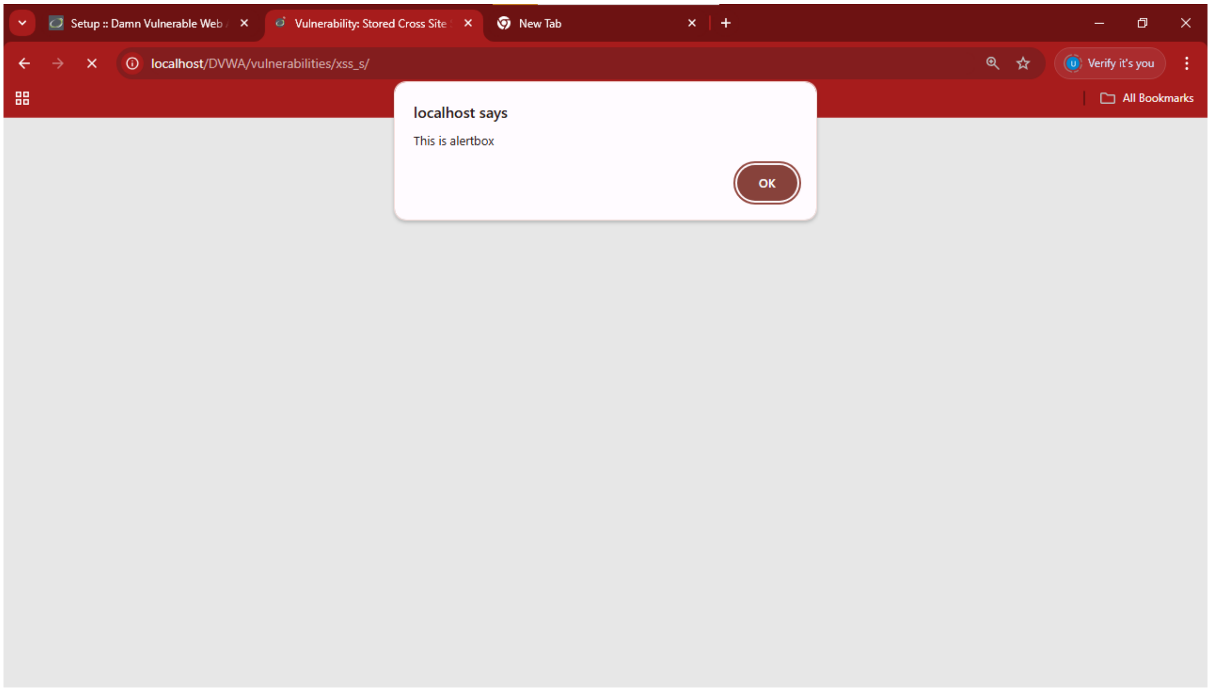
Message * <script>alert("This is alertbox")</script>

Name: test
Message: This is a test comment.

Name: ADMIN
Message:

Name: ADMIN
Message:

More Information


Setup :: Damn Vulnerable Web
Vulnerability: Stored Cross Site
New Tab
localhost/DVWA/vulnerabilities/xss_s/
Verify it's you
All Bookmarks
OK

localhost says

This is alertbox

CONCLUSION: Hence persistent cross-site scripting attack simulated successfully.