Practical :- 6

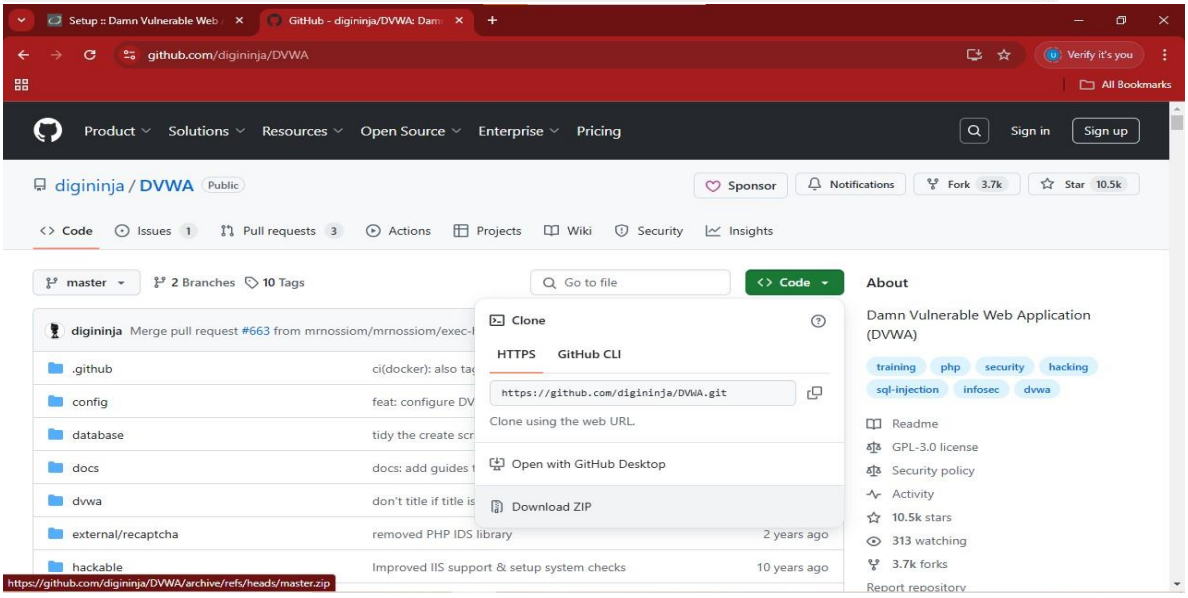
Aim :- Persistent Cross-Site Scripting Attack

- Set up a vulnerable web application that is susceptible to persistent XSS attacks.
- o 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.

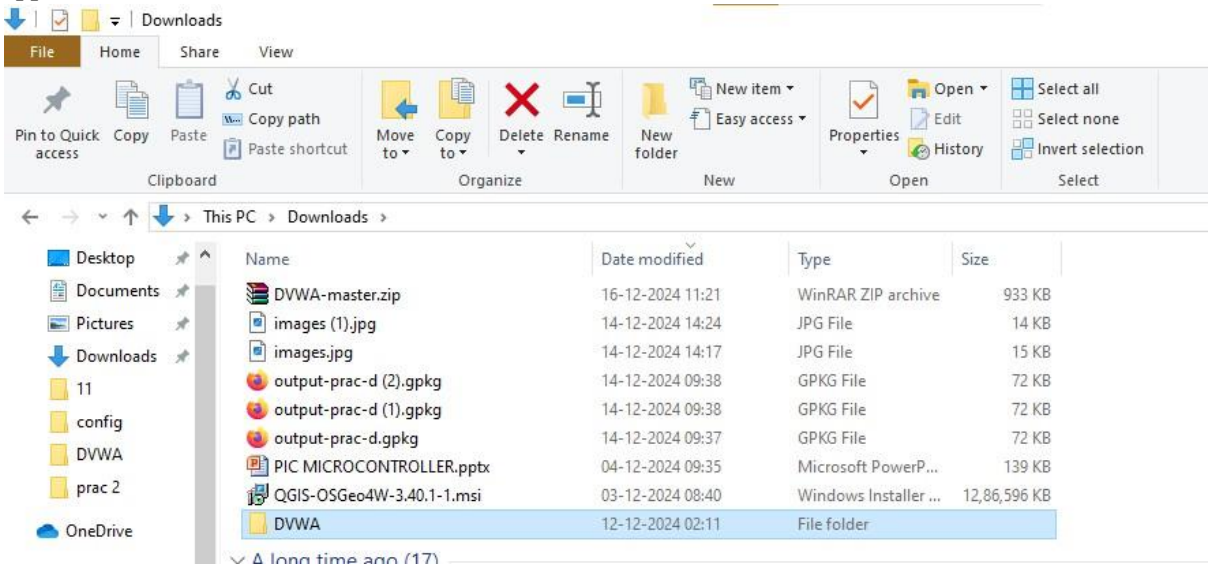
Cross Site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client side scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access controls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

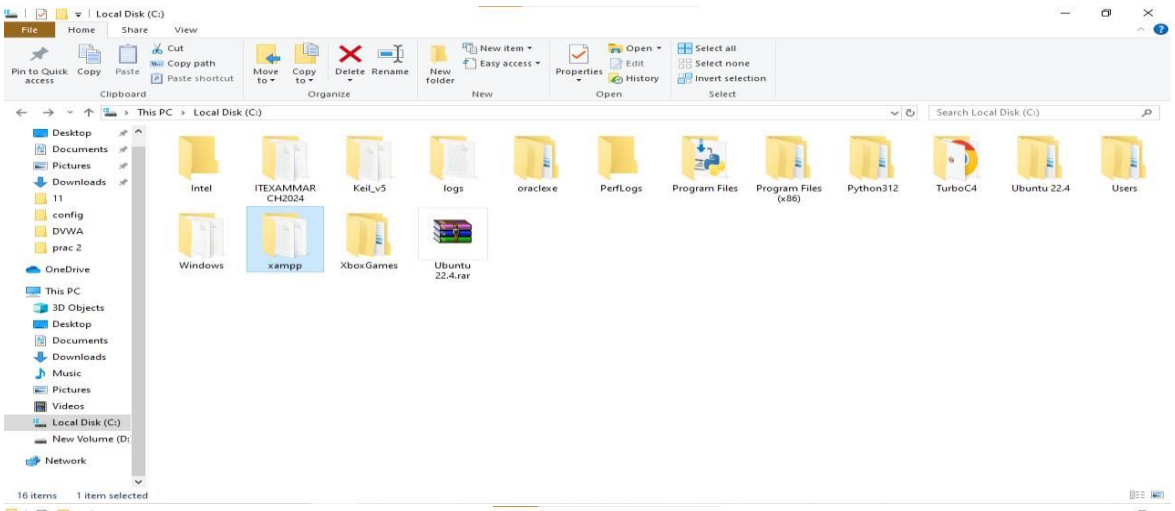
Step 1: Go to „start" and open XAMPP.

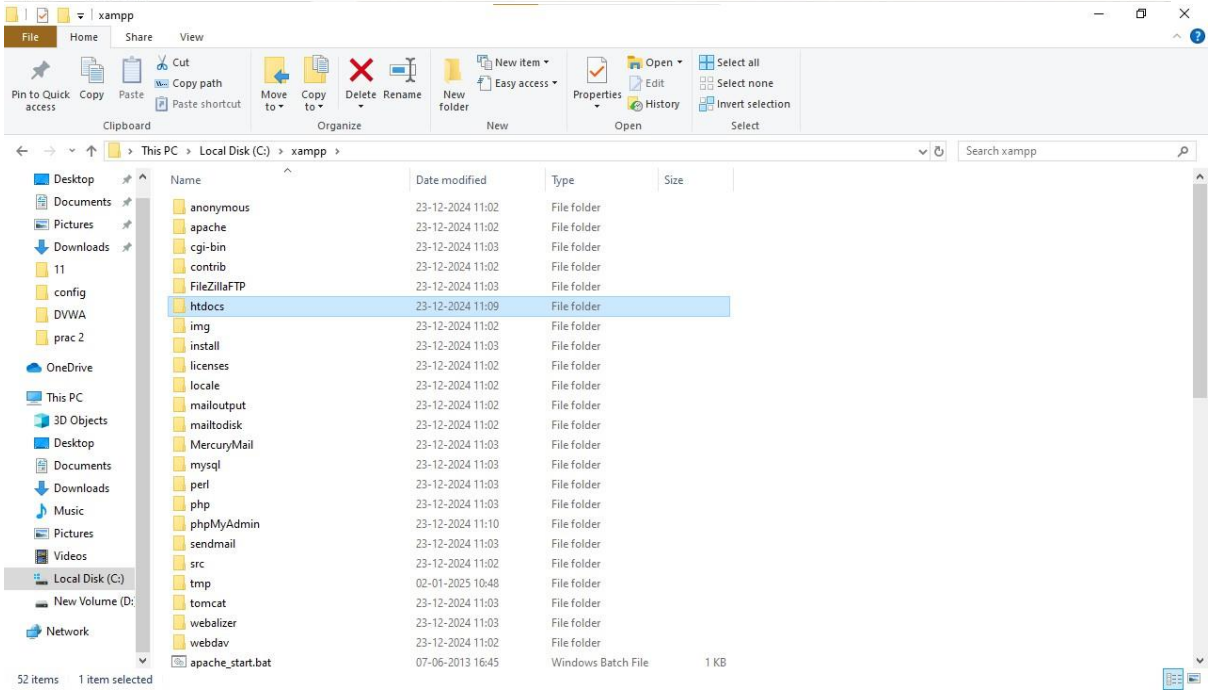
Step 2: Activate the module Apache and MySQL by clicking on Action button to „Start"

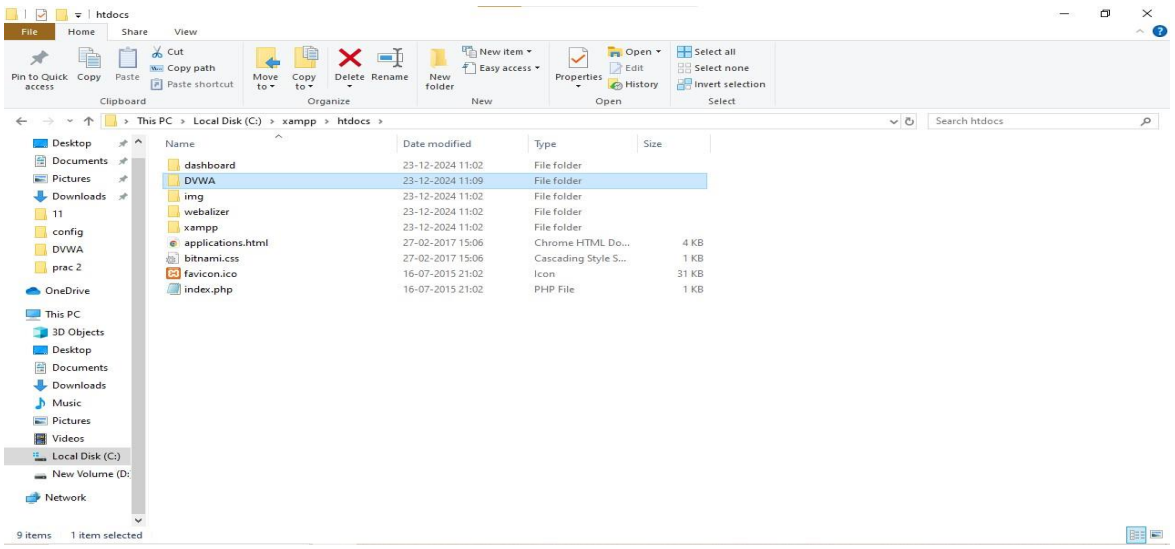


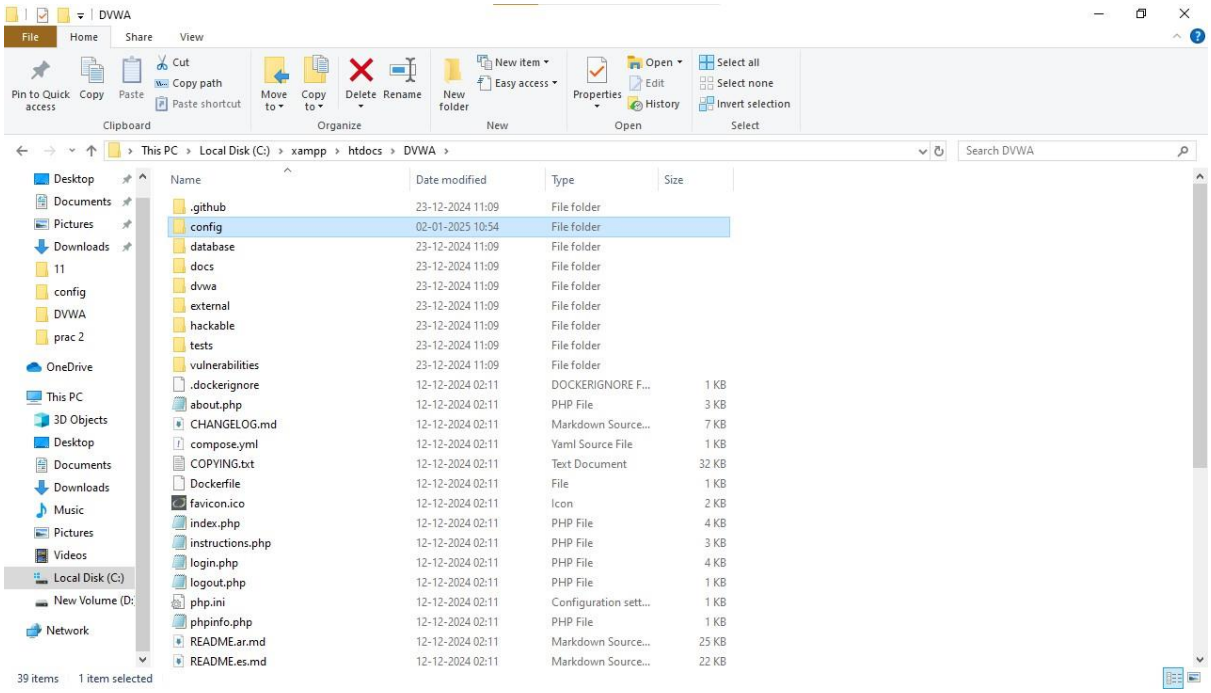
Step 3: open default browser and type „localhost/dashboard“ and a XAMPP dashboard appears.

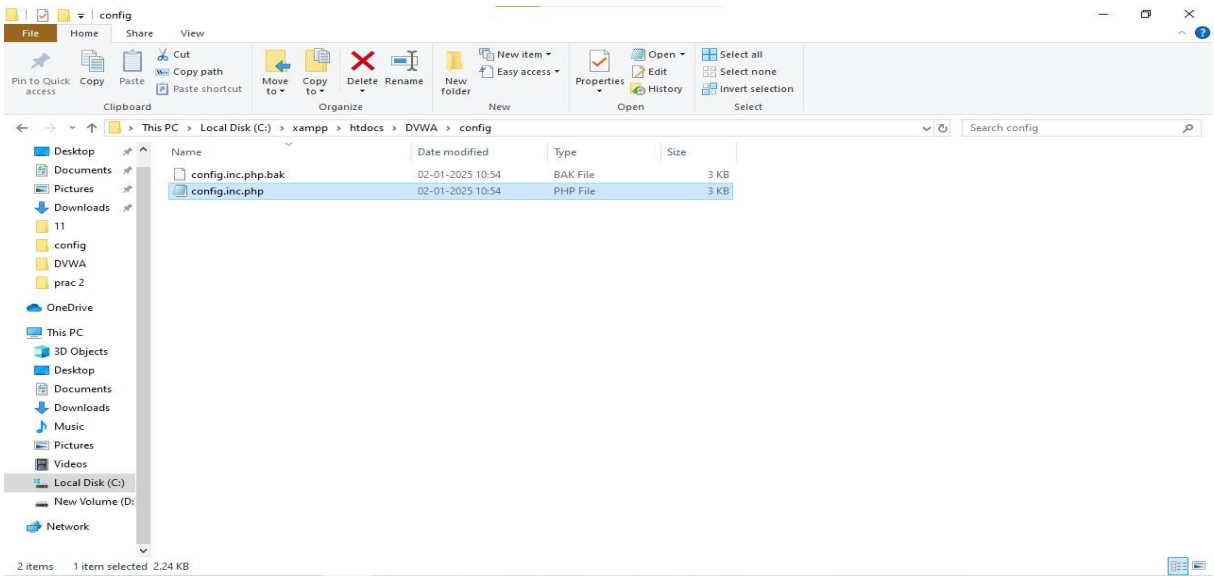


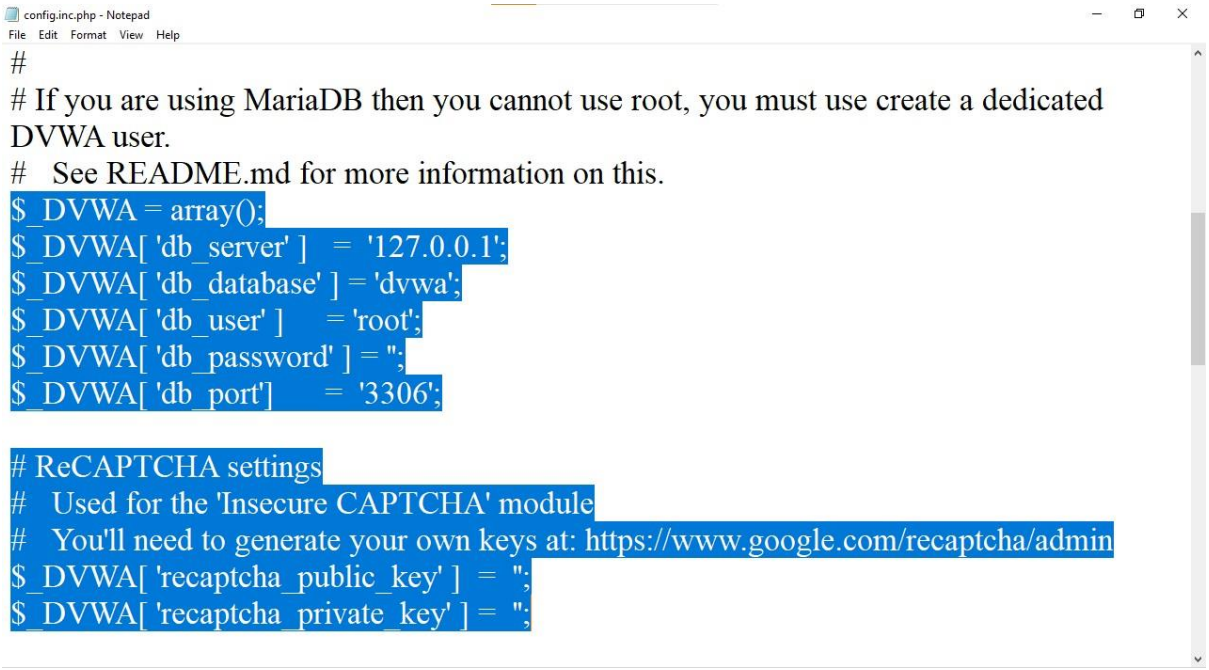


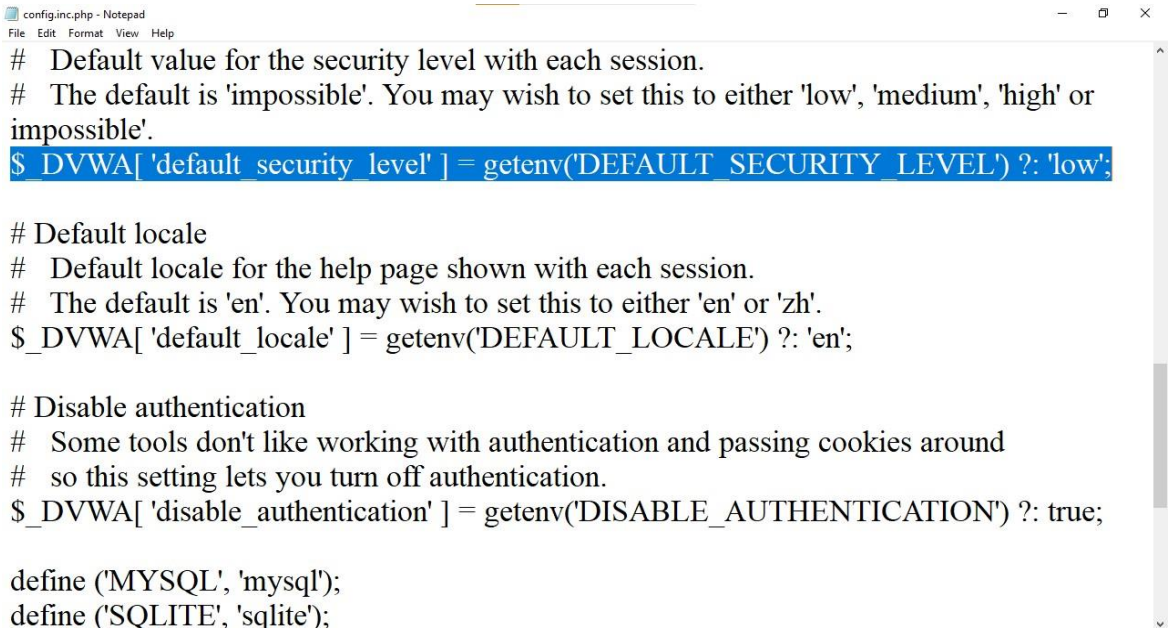


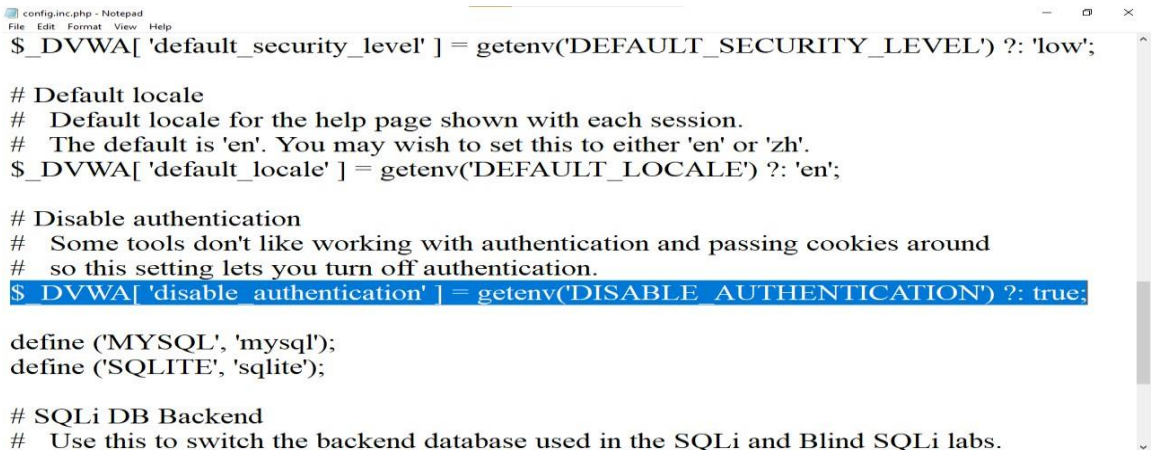

htdocs
This PC › Local Disk (C:) › xampp › htdocs ›
Search htdocs
dashboard 23-12-2024 11:02 File folder
DVWA 23-12-2024 11:09 File folder
img 23-12-2024 11:02 File folder
webalizer 23-12-2024 11:02 File folder
xampp 23-12-2024 11:02 File folder
applications.html 27-02-2017 15:06 Chrome HTML Do... 4 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
9 items 1 item selected

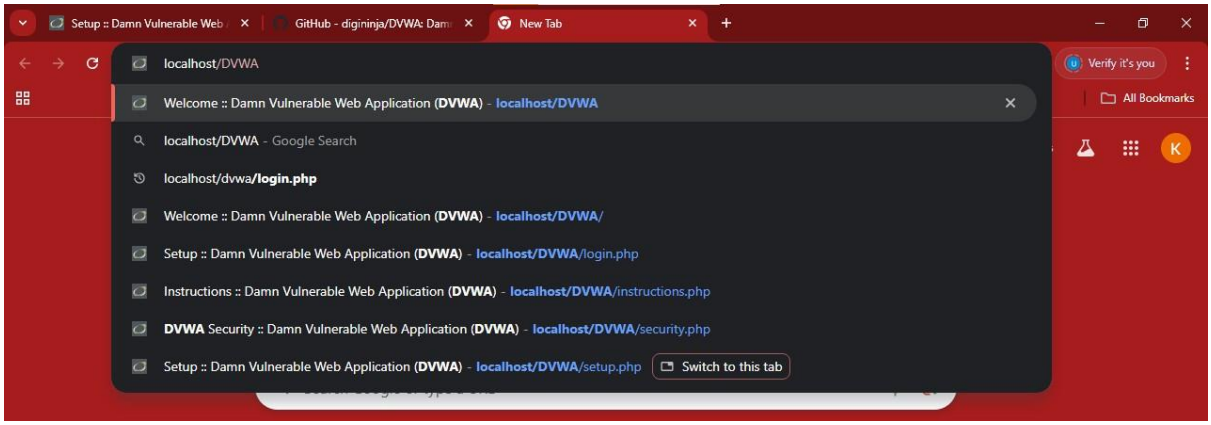

DVWA
This PC › Local Disk (C:) › xampp › htdocs › DVWA ›
Search DVWA
.github 23-12-2024 11:09 File folder
config 02-01-2025 10:54 File folder
database 23-12-2024 11:09 File folder
docs 23-12-2024 11:09 File folder
dvwa 23-12-2024 11:09 File folder
external 23-12-2024 11:09 File folder
hackable 23-12-2024 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

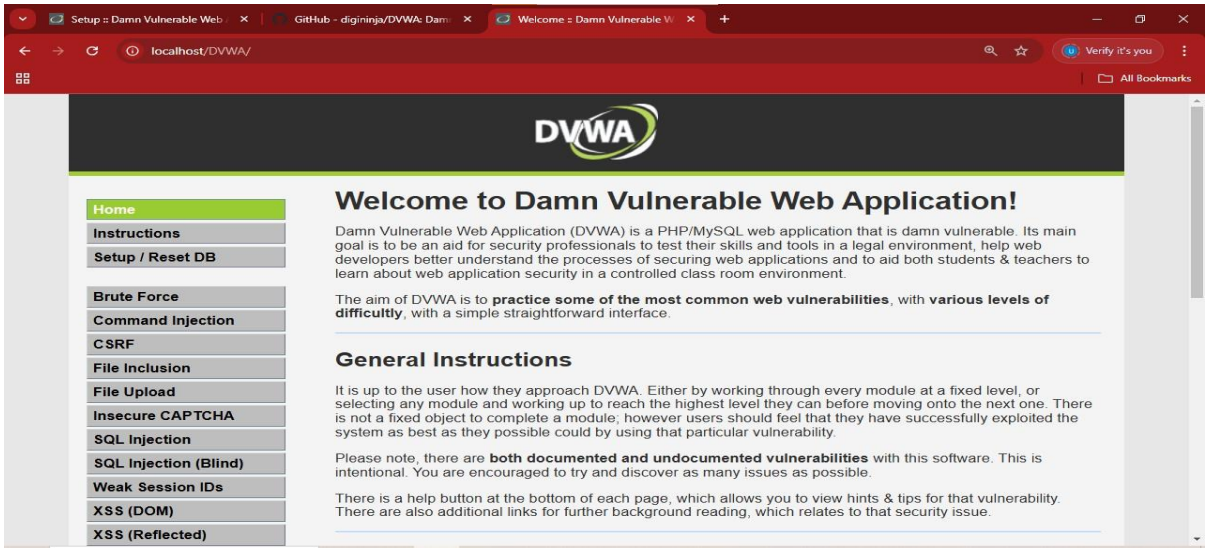

config
This PC › Local Disk (C:) › xampp › htdocs › DVWA › config
Search config
config.inc.php.bak 02-01-2025 10:54 BAK File 3 KB
config.inc.php 02-01-2025 10:54 PHP File 3 KB
2 items 1 item selected 2.24 KB

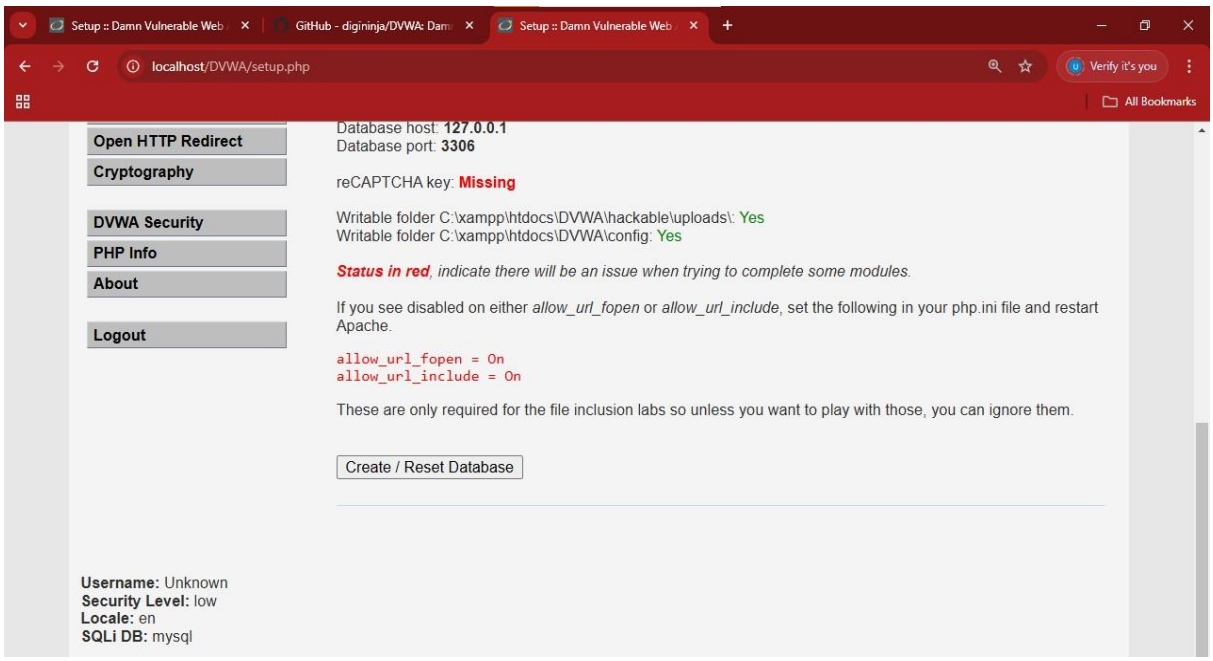

config.inc.php - Notepad
File Edit Format View Help
#
If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'root';
$_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'] = '';

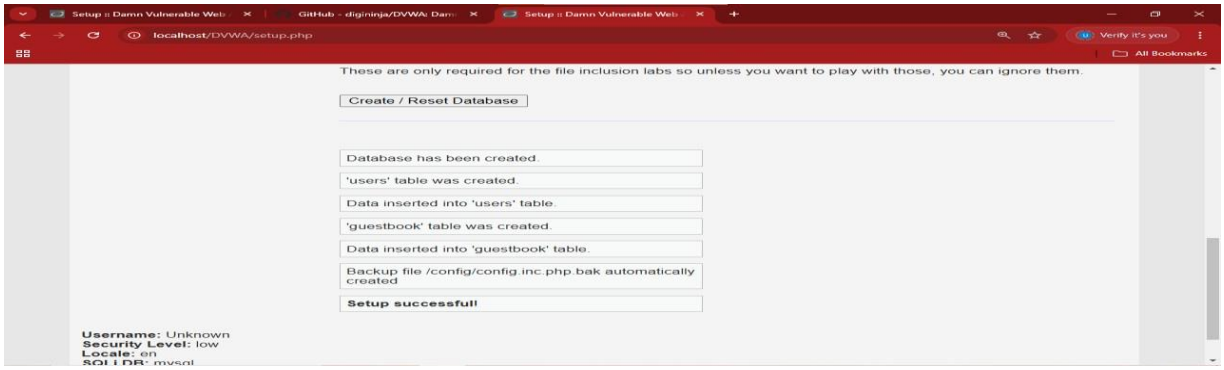

config.inc.php - Notepad
File Edit Format View Help
Default value for the security level with each session.
The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';
Default locale
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');

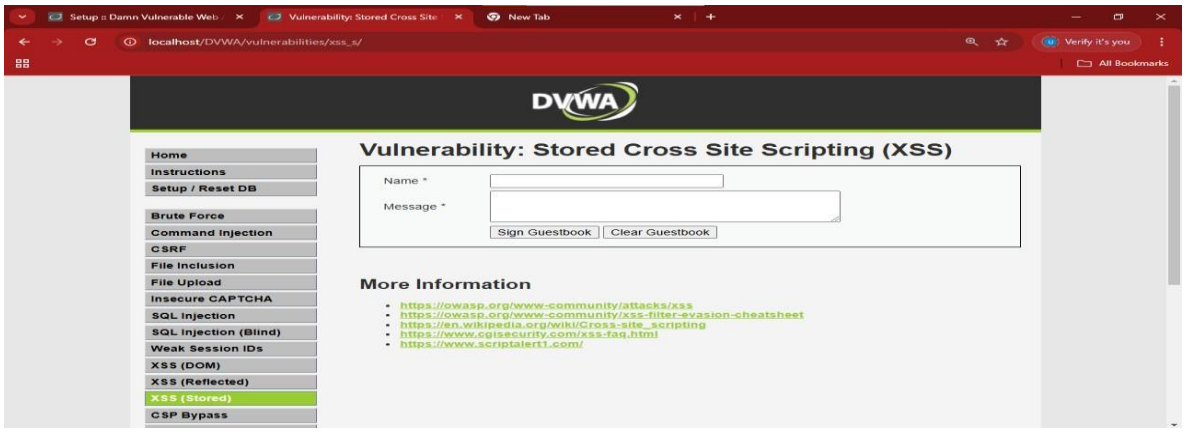

config.inc.php - Notepad
File Edit Format View Help
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';
Default locale
Default locale for the help page shown with each session.
The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA['default_locale'] = getenv('DEFAULT_LOCALE') ?: '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.

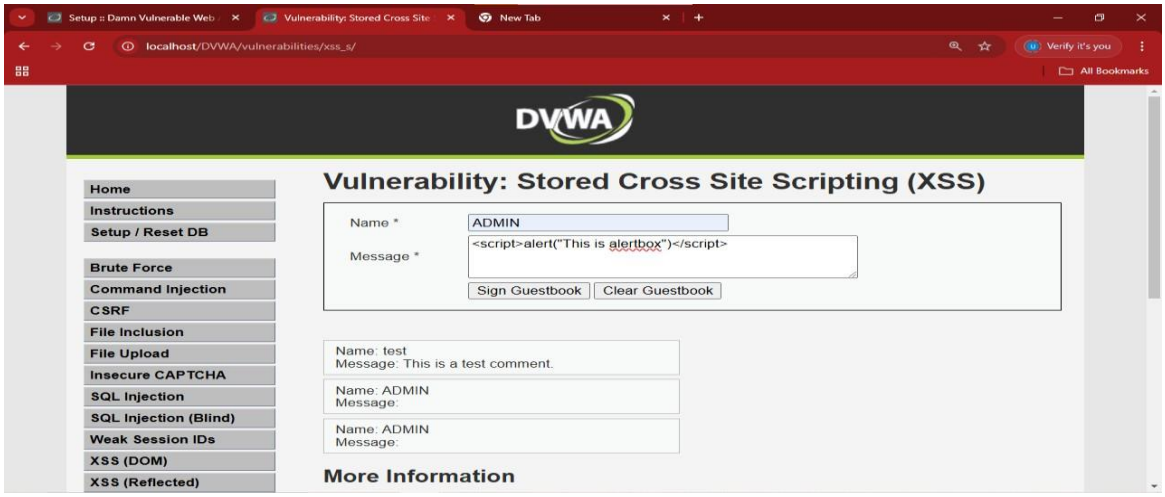

Setup :: Damn Vulnerable Web
GitHub - digininja/DVWA: Dam
New Tab
localhost/DVWA
Welcome :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA
localhost/DVWA - Google Search
localhost/dvwa/login.php
Welcome :: Damn Vulnerable Web Application (DVWA) - localhost/DVWA/
Setup :: Damn Vulnerable Web 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
Switch to this tab
Verify it's you
All Bookmarks

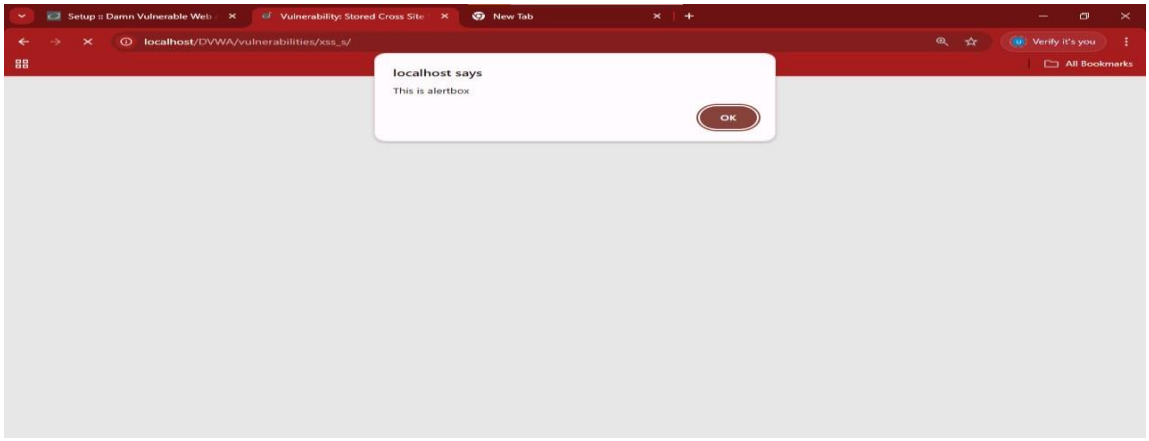

localhost/DVWA/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Welcome to Damn Vulnerable Web Application!
Damn Vulnerable Web Application (DVWA) is a 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.


localhost/DVWA/setup.php
Open HTTP Redirect
Cryptography
DVWA Security
PHP Info
About
Logout
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









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