IJEI FUMNANYA CHUKWUMA DIVINE

CYBERSECURITY ASSIGNMENT 6

TESTING A VULNERABLE WEB APPLICATION

Objective:

Perform basic penetration testing on a deliberately insecure web application.

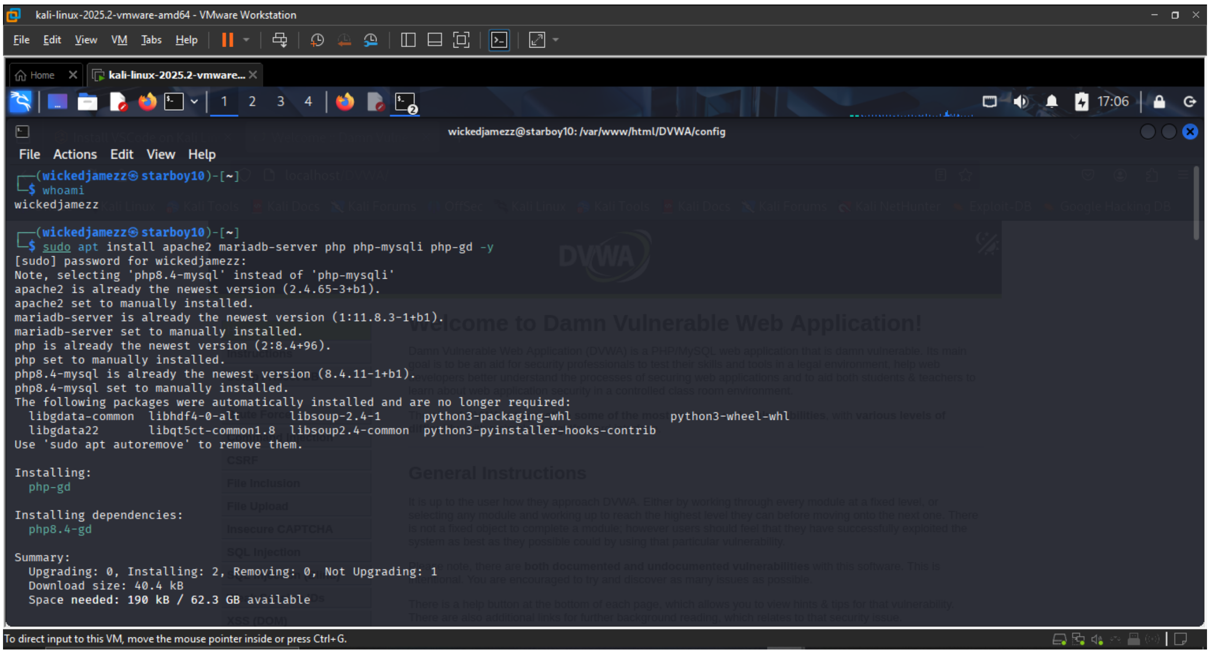
Tools:

Since we are undergoing our training using Kali Linux, I would be using LAMP (Linux, Apache, MySQL, PHP) instead of XAMPP which are the tools for use on windows OS.

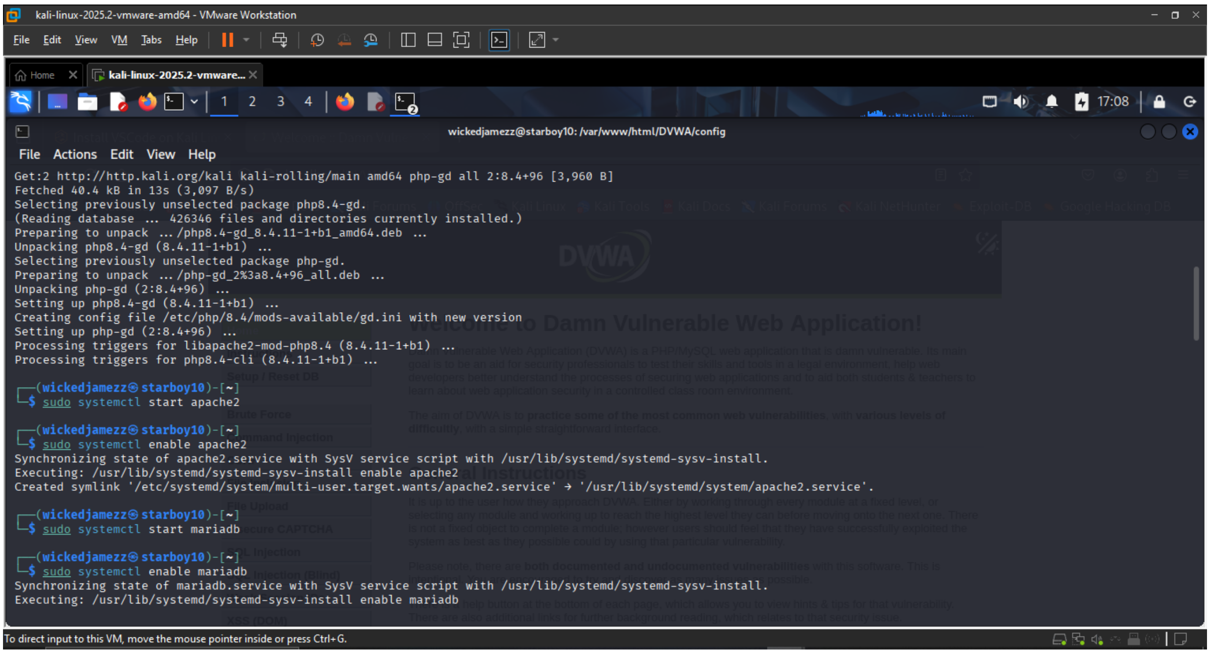
I have been able to download, install and setup my DVWA (Damn Vulnerable Web App) which would be the "Lab" where we would be doing our test exploitation of the 3 web app vulnerabilities given in the assignment questions which are:

1. SQLi (SQL injection)
2. XSS (Cross Site Scripting) – I decided to do two versions of this vulnerability.
3. CSRF (Cross site request forgery)

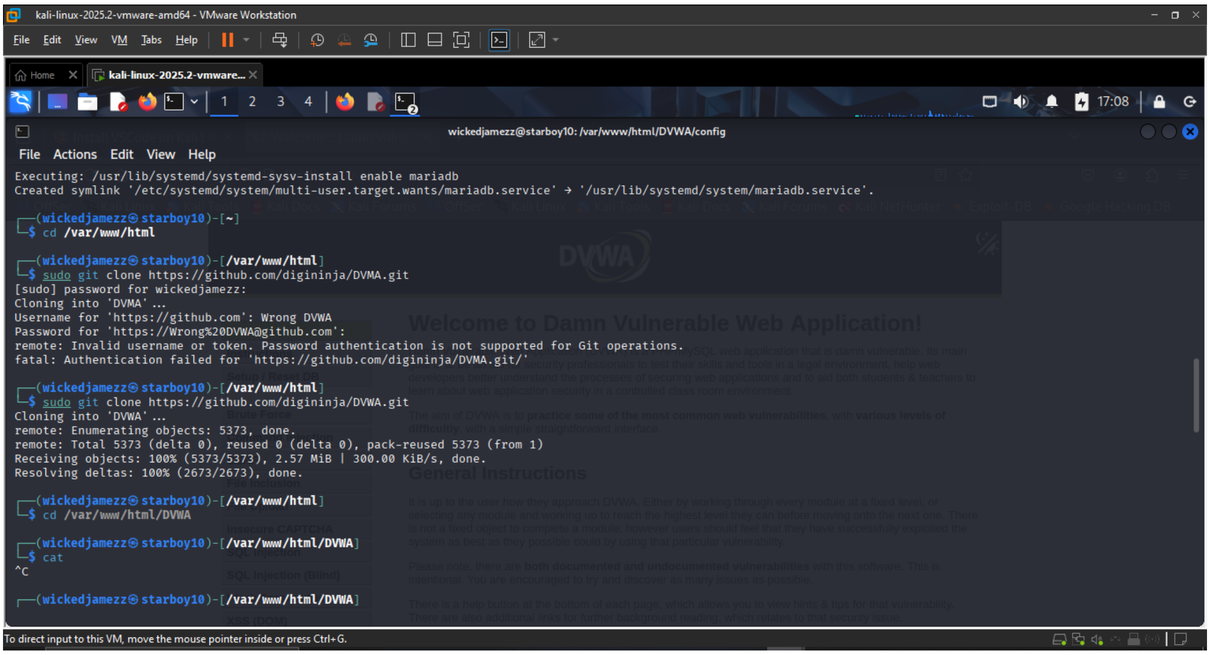
These are screenshots taken during the installation of the DVWA to my Kali UI:


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
1 2 3 4
17:06
wickedjamezz@starboy10: /var/www/html/DVWA/config
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

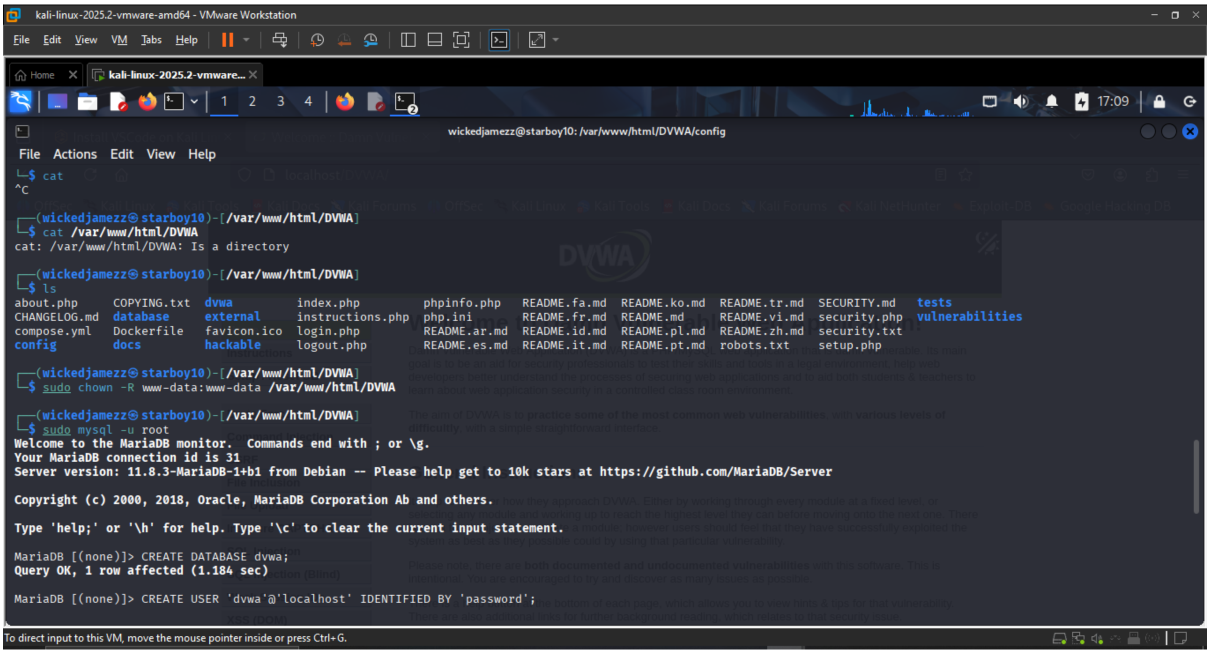
```
┌──(wickedjamezz㉿starboy10)-[~]
└─$ whoami
wickedjamezz

┌──(wickedjamezz㉿starboy10)-[~]
└─$ sudo apt install apache2 mariadb-server php php-mysqli php-gd -y
[sudo] password for wickedjamezz:
Note, selecting 'php8.4-mysql' instead of 'php-mysqli'
apache2 is already the newest version (2.4.65-3+b1).
apache2 set to manually installed.
mariadb-server is already the newest version (1:11.8.3-1+b1).
mariadb-server set to manually installed.
php is already the newest version (2:8.4+96).
php set to manually installed.
php8.4-mysql is already the newest version (8.4.11-1+b1).
php8.4-mysql set to manually installed.
The following packages were automatically installed and are no longer required:
  libgdata-common  libhdf4-0-alt      libsoup-2.4-1       python3-packaging-whl                python3-wheel-whl
  libgdata22       libqt5ct-common1.8 libsoup2.4-common   python3-pyinstaller-hooks-contrib
Use 'sudo apt autoremove' to remove them.

Installing:
  php-gd

Installing dependencies:
  php8.4-gd

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1
  Download size: 40.4 kB
  Space needed: 190 kB / 62.3 GB available
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
17:08
wickedjamezz@starboy10: /var/www/html/DVWA/config
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php-gd all 2:8.4+96 [3,960 B]
Fetched 40.4 kB in 13s (3,097 B/s)
Selecting previously unselected package php8.4-gd.
(Reading database ... 426346 files and directories currently installed.)
Preparing to unpack .../php8.4-gd_8.4.11-1+b1_amd64.deb ...
Unpacking php8.4-gd (8.4.11-1+b1) ...
Selecting previously unselected package php-gd.
Preparing to unpack .../php-gd_2%3a8.4+96_all.deb ...
Unpacking php-gd (2:8.4+96) ...
Setting up php8.4-gd (8.4.11-1+b1) ...
Creating config file /etc/php/8.4/mods-available/gd.ini with new version
Setting up php-gd (2:8.4+96) ...
Processing triggers for libapache2-mod-php8.4 (8.4.11-1+b1) ...
Processing triggers for php8.4-cli (8.4.11-1+b1) ...

┌──(wickedjamezz㉿starboy10)-[~]
└─$ sudo systemctl start apache2

┌──(wickedjamezz㉿starboy10)-[~]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.

┌──(wickedjamezz㉿starboy10)-[~]
└─$ sudo systemctl start mariadb

┌──(wickedjamezz㉿starboy10)-[~]
└─$ sudo systemctl enable mariadb
Synchronizing state of mariadb.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable mariadb
```

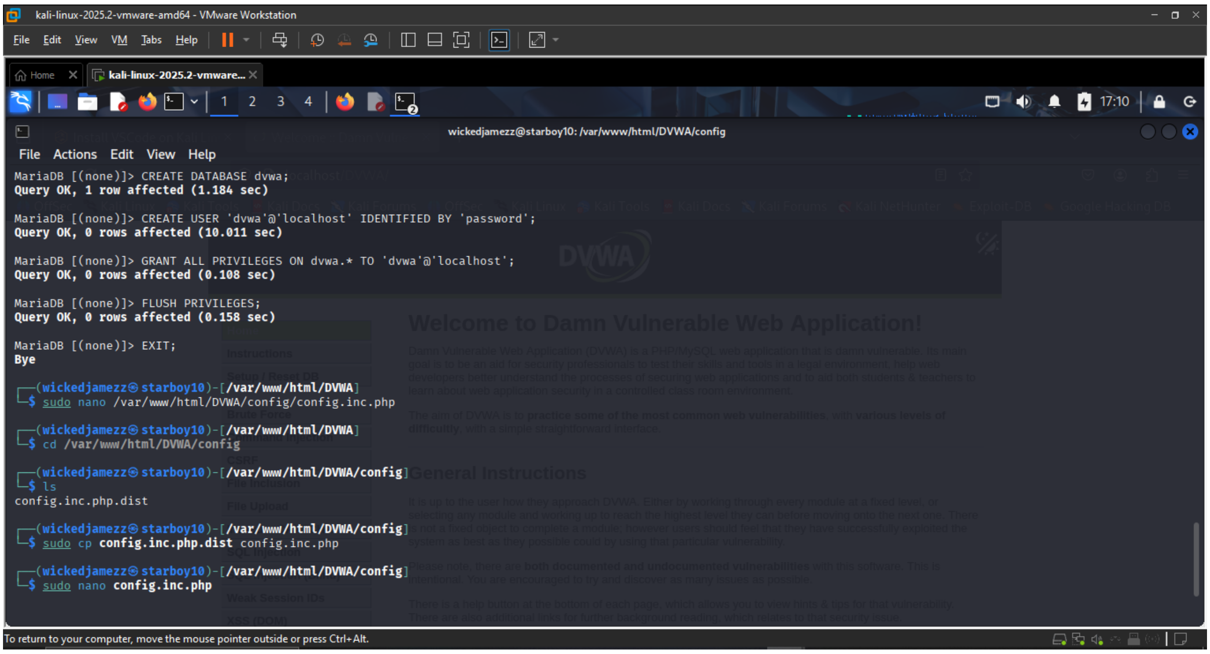

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
17:08
wickedjamezz@starboy10: /var/www/html/DVWA/config
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Executing: /usr/lib/systemd/systemd-sysv-install enable mariadb
Created symlink '/etc/systemd/system/multi-user.target.wants/mariadb.service' → '/usr/lib/systemd/system/mariadb.service'.

┌──(wickedjamezz㉿starboy10)-[~]
└─$ cd /var/www/html

┌──(wickedjamezz㉿starboy10)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVMA.git
[sudo] password for wickedjamezz:
Cloning into 'DVMA'...
Username for 'https://github.com': Wrong DVWA
Password for 'https://Wrong%20DVWA@github.com':
remote: Invalid username or token. Password authentication is not supported for Git operations.
fatal: Authentication failed for 'https://github.com/digininja/DVMA.git/'

┌──(wickedjamezz㉿starboy10)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 300.00 KiB/s, done.
Resolving deltas: 100% (2673/2673), done.

┌──(wickedjamezz㉿starboy10)-[/var/www/html]
└─$ cd /var/www/html/DVWA

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ cat
^C

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
1 2 3 4
17:09
wickedjamezz@starboy10: /var/www/html/DVWA/config
File Actions Edit View Help

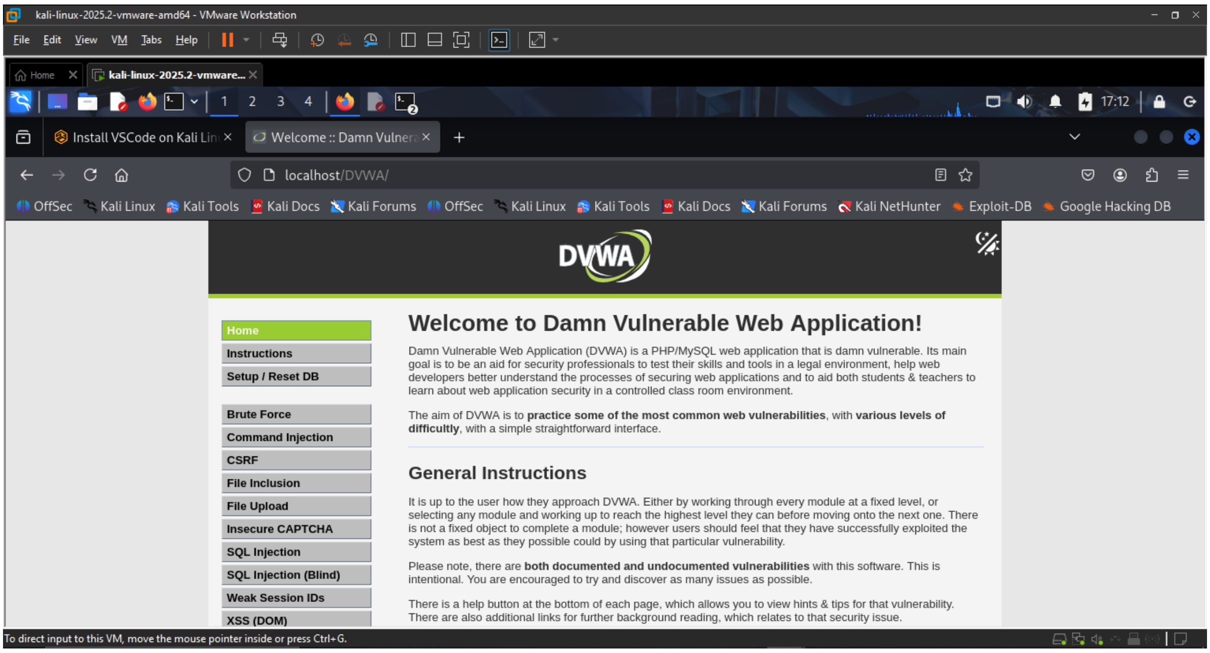
```
└─$ cat
^C

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ cat /var/www/html/DVWA
cat: /var/www/html/DVWA: Is a directory

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ ls
about.php     COPYING.txt  dvwa         index.php         phpinfo.php   README.fa.md  README.ko.md  README.tr.md  SECURITY.md   tests
CHANGELOG.md  database     external     instructions.php  php.ini       README.fr.md  README.md     README.vi.md  security.php  vulnerabilities
compose.yml   Dockerfile   favicon.ico  login.php         README.ar.md  README.id.md  README.pl.md  README.zh.md  security.txt
config        docs         hackable     logout.php        README.es.md  README.it.md  README.pt.md  robots.txt    setup.php

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ sudo chown -R www-data:www-data /var/www/html/DVWA

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ sudo mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (1.184 sec)

MariaDB [(none)]> CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
1 2 3 4
17:10
wickedjamezz@starboy10: /var/www/html/DVWA/config
File Actions Edit View Help

```
MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (1.184 sec)

MariaDB [(none)]> CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (10.011 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
Query OK, 0 rows affected (0.108 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.158 sec)

MariaDB [(none)]> EXIT;
Bye

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ sudo nano /var/www/html/DVWA/config/config.inc.php

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA]
└─$ cd /var/www/html/DVWA/config

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config.inc.php

┌──(wickedjamezz㉿starboy10)-[/var/www/html/DVWA/config]
└─$ sudo nano config.inc.php
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
1 2 3 4
17:12
Install VSCode on Kali Lin
Welcome :: Damn Vulner
localhost/DVWA/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
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)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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.

- ## SQLi ➔

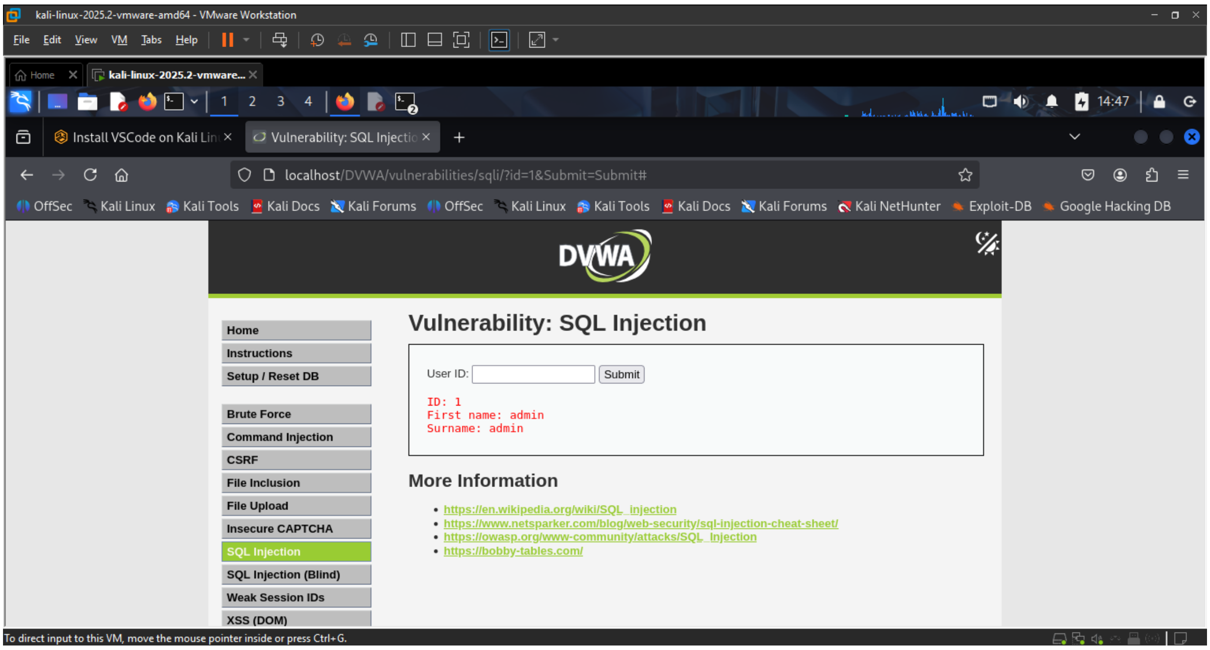
This is one of the vulnerability types of web applications. It can also be called authentication bypass. Because a vulnerable web app does not sanitize input before sending it into an SQL query e.g

"SELECT * FROM users WHERE username = 'input' AND password = 'input';".

When you enter "1" in the input form that says "UserID" it gives the first user with username and password "admin and admin" respectively and if you enter "2" you would see the second user and so on. One way to manually check for an SQLi is by entering a single quote **(')** or a double quote **(")** to see if we get an SQL syntax error. To test the vulnerability, we can input an SQL statement that always results in true **(' OR '1'='1' -- - or 'OR 1=1-- - or ' OR 1=1#)**

Payload(s) used:

- **(' OR '1'='1' -- - or 'OR 1=1-- - or ' OR 1=1#)**


kali-linux-2025.2-vmware-amd64 - VMware Workstation
Install VSCode on Kali Lin
Vulnerability: SQL Injectio
localhost/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#
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)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

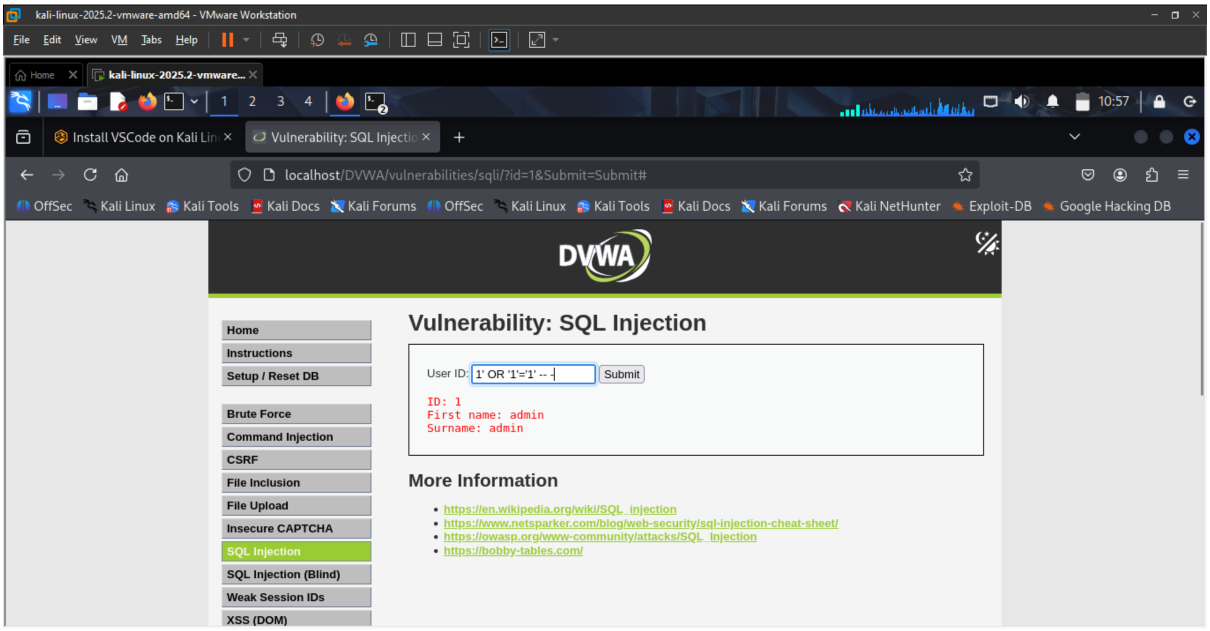
Vulnerability: SQL Injection

User ID: Submit

```
ID: 1
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/



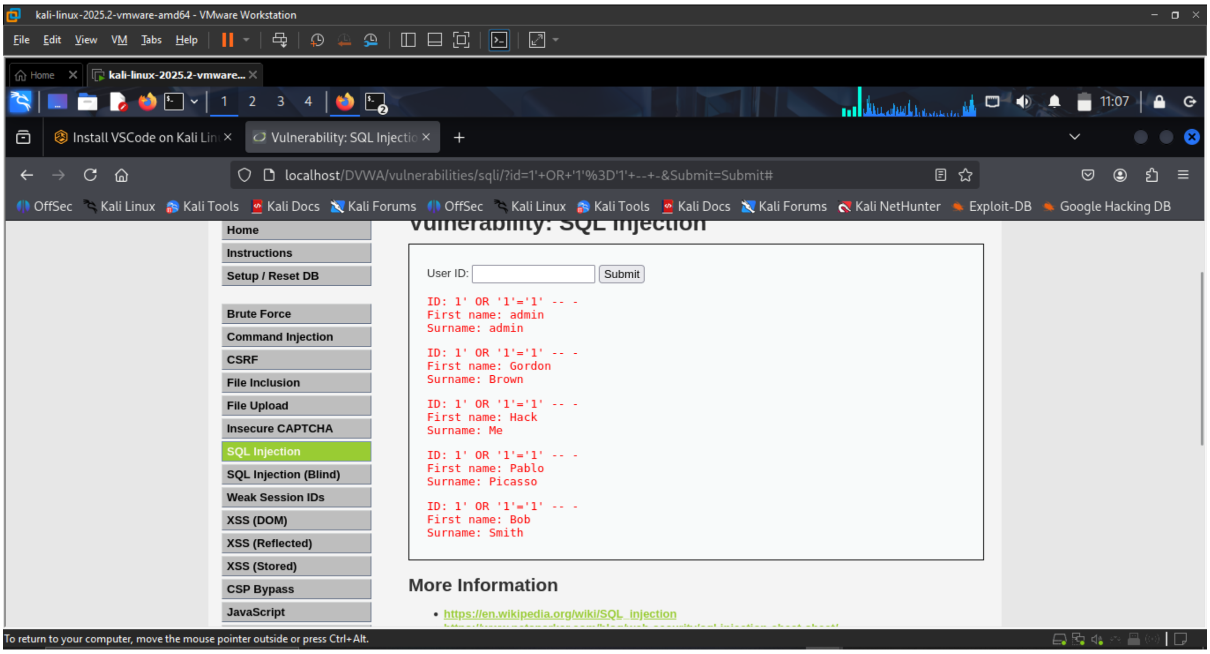
Vulnerability: SQL Injection

User ID: 1' OR '1'='1' -- - Submit

```
ID: 1
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/



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Install VSCode on Kali Lin
Vulnerability: SQL Injectio
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
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
Submit
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

localhost/DVWA/vulnerabilities/sqli/?id=1'+OR+'1'%3D'1'+--+-&Submit=Submit#

Vulnerability: SQL Injection

User ID:

```
ID: 1' OR '1'='1' -- -
First name: admin
Surname: admin

ID: 1' OR '1'='1' -- -
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1' -- -
First name: Hack
Surname: Me

ID: 1' OR '1'='1' -- -
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1' -- -
First name: Bob
Surname: Smith
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection

Mitigation recommended:

- Use prepared statements/parameterised queries (PDO, mysqli).
- Apply Input validation and sanitization.
- Use least-privileged DB (database) accounts.

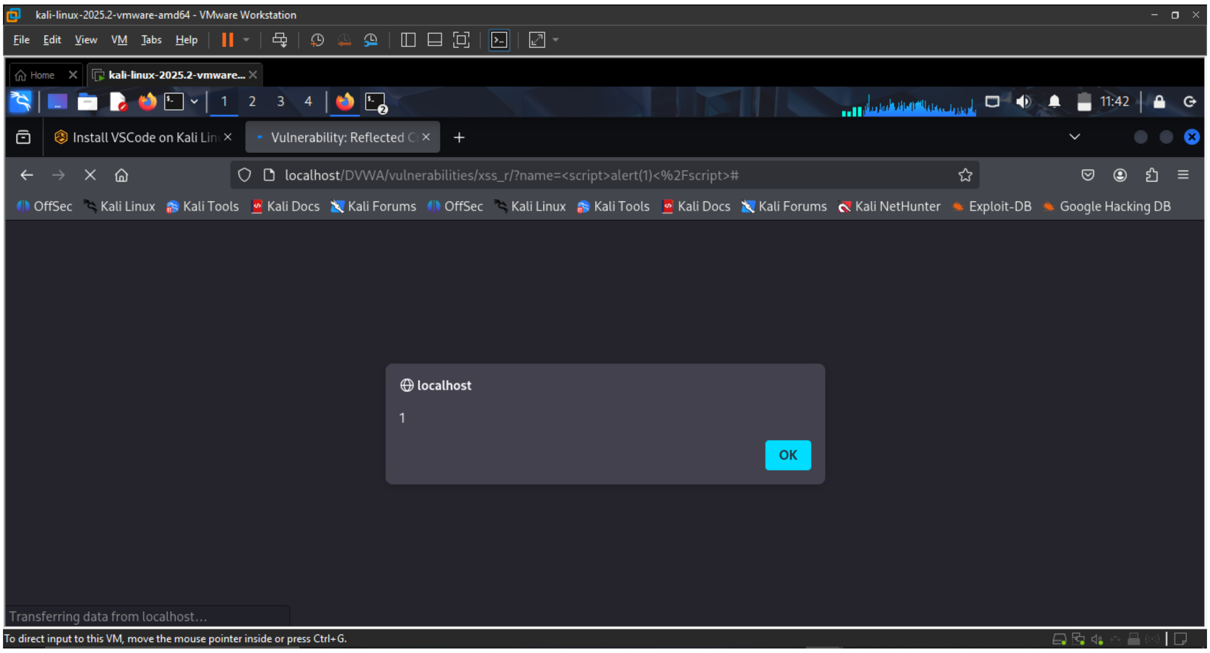
- ## XSS Reflected ➔

Reflected XSS is when a malicious script can be written typically in the URL of a website when a victim clicks the link with malicious script embedded in it the script will be run once for the user. It is not saved permanently to the webpage. Whatever we type into the field on the input form would be what would be displayed on the URL as well as the page. So if we type in a simple javascript code that displays a pop up we could prove the page is vulnerable to XSS (cross site scripting).

Payload used:

- <script>alert(1)</script>

In this payload, we have our JavaScript code that is noted by the two script tags at the end and beginning and in between we have our alert that is going to say “1”.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
11:42
Install VSCode on Kali Lin
Vulnerability: Reflected C
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OK

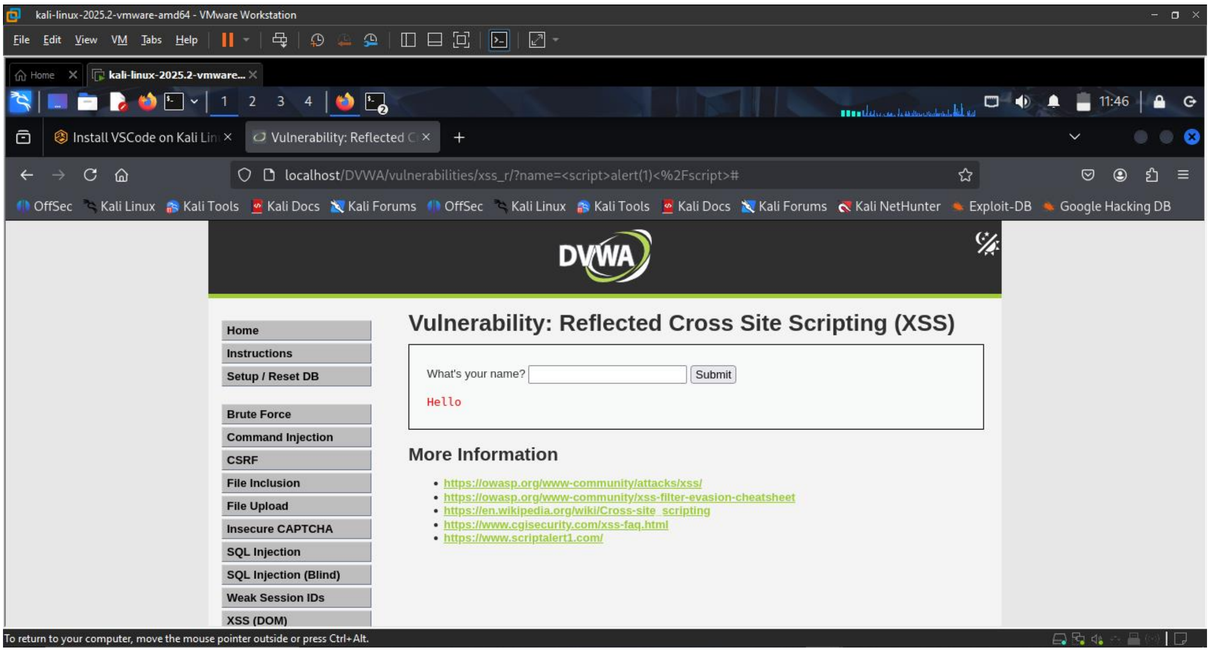
localhost/DVWA/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#

localhost

1

Transferring data from localhost...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
11:46
Install VSCode on Kali Lin
Vulnerability: Reflected C
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
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)
Submit

localhost/DVWA/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

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/

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Mitigation recommended for XSS reflected:

- Escape user input before rendering to HTML.
- Use content security policy (CSP).
- Sanitize input (e.g., strip tag attributes (/) “<script>”).

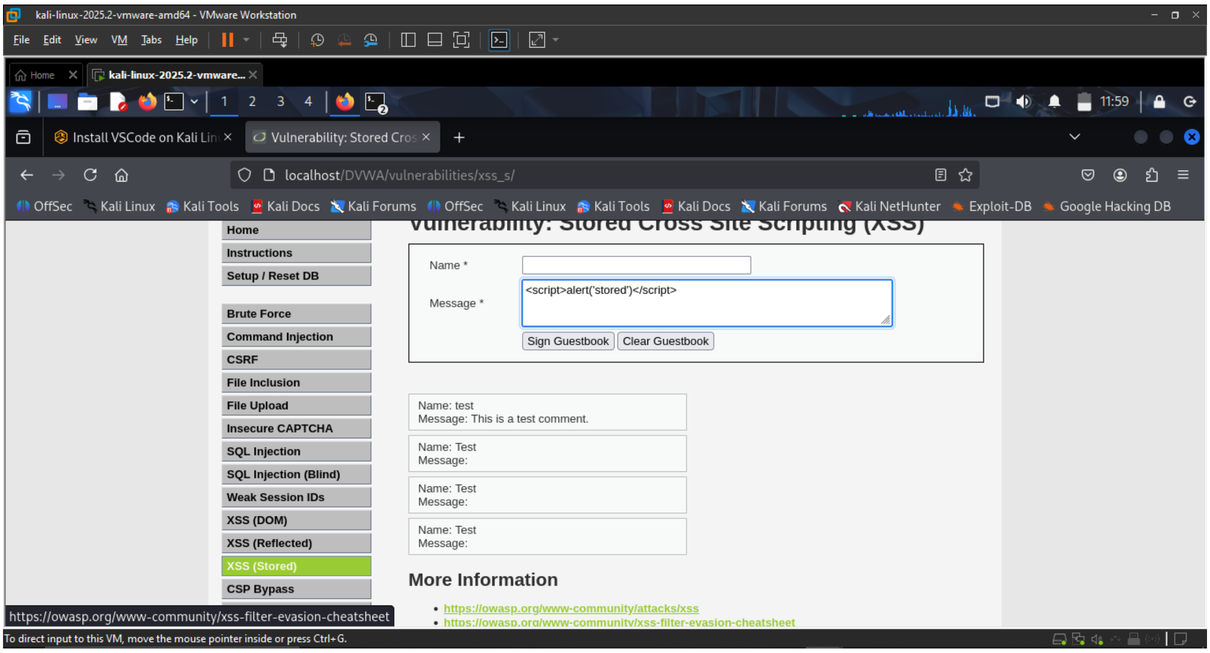
- ### XSS Stored ➔

When a cross site scripting payload is processing on a webpage, likely because it is being saved to a database and fetched by the website it is called a stored cross site scripting vulnerability. This is the most dangerous cross site scripting vulnerability because the payload has the ability to affect every single user that visits the vulnerable site. Now, I will run basic script with an alert saying “stored”.

Payload:

- <script>alert(“stored”)</script>

In this payload, we have our JavaScript code that is noted by the two script tags at the end and beginning and in between we have our alert that is going to say “stored”. This has been saved to a database somewhere on the backend and it will be displayed every time the web page is visited by any users.


kali-linux-2025.2-vmware-amd64 - VMware Workstation

localhost/DVWA/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message * <script>alert('stored')</script>

Name: test
Message: This is a test comment.

Name: Test
Message:

Name: Test
Message:

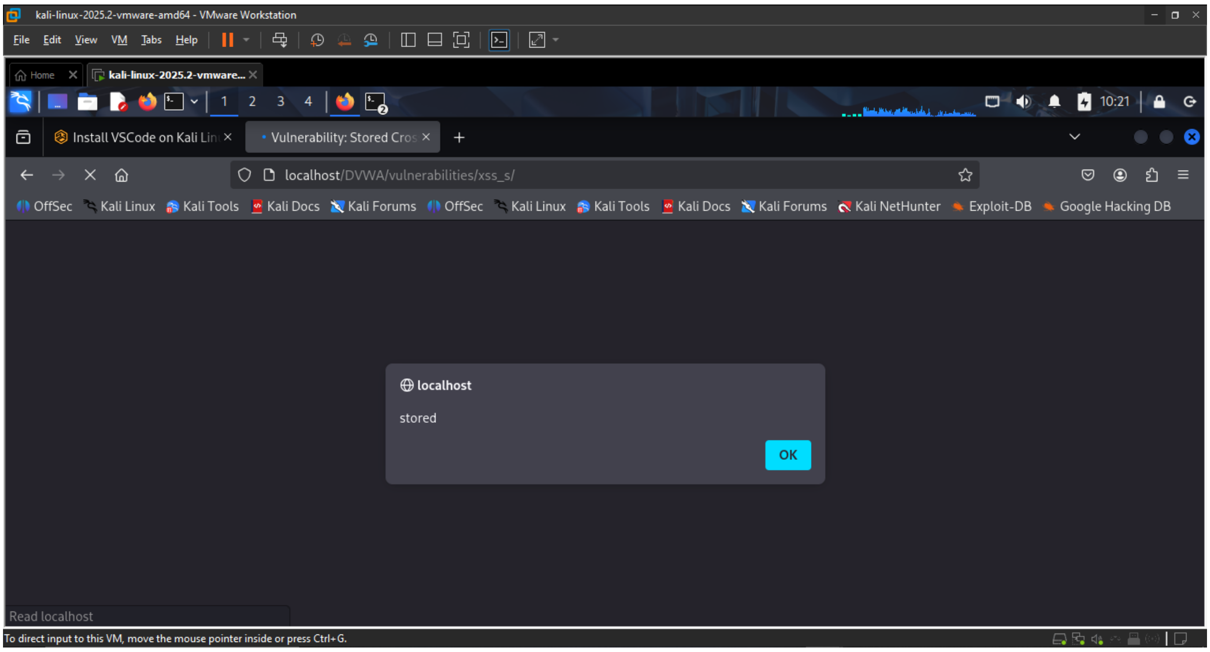
Name: Test
Message:

More Information

- https://owasp.org/www-community/attacks/xss
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet

https://owasp.org/www-community/xss-filter-evasion-cheatsheet

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



localhost

stored

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
10:21
Install VSCode on Kali Lin
Vulnerability: Stored Cros
localhost/DVWA/vulnerabilities/xss_s/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
OK
Read localhost
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

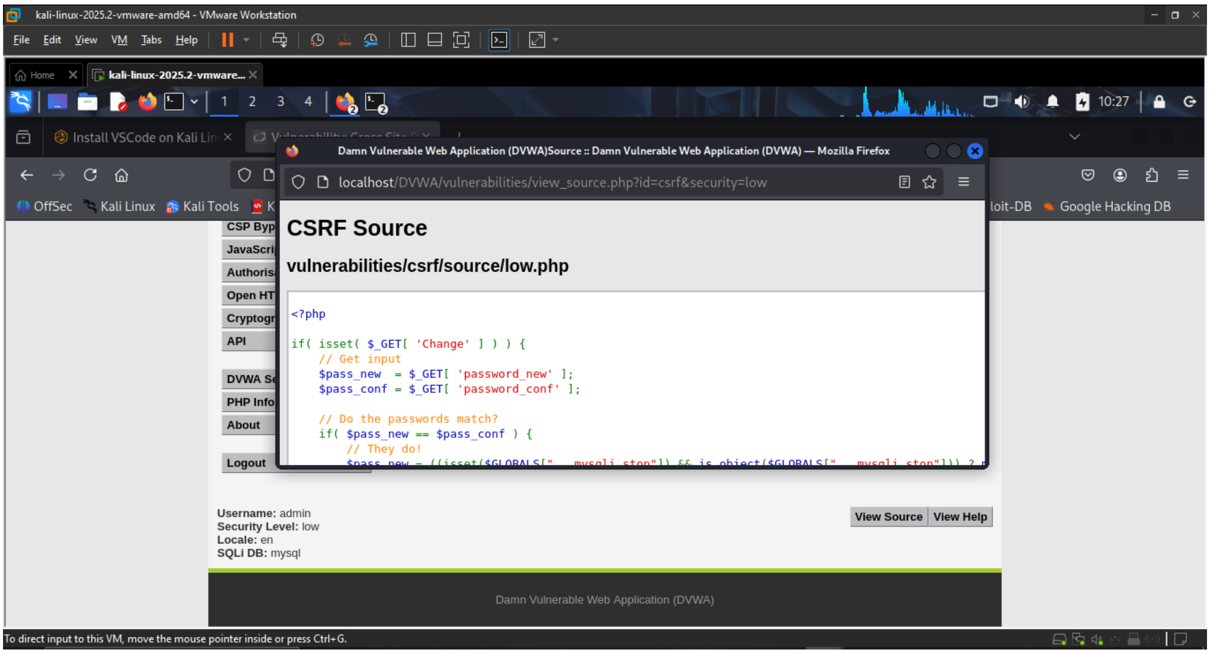
Mitigation recommended:

- Encode output, sanitize input, plus:
- Filter dangerous HTML on both input and output paths.
- Consider a HTML sanitizer library.

- ## CSRF (Cross Site Request Forgery) ➔

A CSRF attack allows us to perform actions on behalf of another user usually by having them click a link. While logged in to DVWA in on tab, we visit a malicious page in another tab. That page silently submits a form to DVWA to change the password. The browser includes the DVWA cookies, so the server thinks YOU did it.

Initially, we click the "View source" at the bottom of the CSRF page on DVWA and we do that to confirm what the form's method is (either GET or POST) and what the forms action is and then we also check if we can see input fields like "password_new" and "password_conf".



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
10:27
Install VSCode on Kali Lin
Damn Vulnerable Web Application (DVWA)Source :: Damn Vulnerable Web Application (DVWA) — Mozilla Firefox
OffSec
Kali Linux
Kali Tools
loit-DB
Google Hacking DB
CSP Byp
JavaScri
Authoris
Open HT
Cryptogr
API
DVWA Se
PHP Info
About
Logout
View Source
View Help
Damn Vulnerable Web Application (DVWA)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

localhost/DVWA/vulnerabilities/view_source.php?id=csrf&security=low

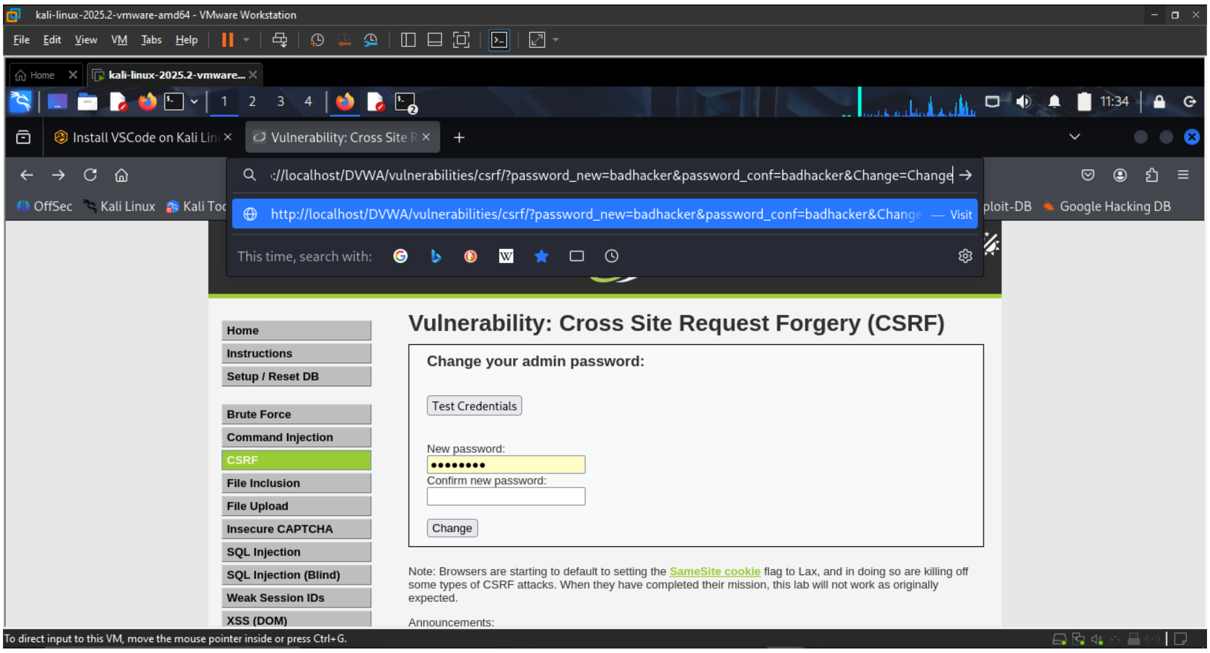
CSRF Source

vulnerabilities/csrf/source/low.php

```
<?php

if( isset( $_GET[ 'Change' ] ) ) {
    // Get input
    $pass_new  = $_GET[ 'password_new' ];
    $pass_conf = $_GET[ 'password_conf' ];

    // Do the passwords match?
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? m
```

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

This is the PHP (backend source code) for the web application and from that, we can see that the web app uses the 'GET' method or parameters without CSRF tokens which means that we can trigger a password change just by visiting a malicious link.



://localhost/DVWA/vulnerabilities/csrf/?password_new=badhacker&password_conf=badhacker&Change=Change

http://localhost/DVWA/vulnerabilities/csrf/?password_new=badhacker&password_conf=badhacker&Change — Visit

This time, search with:

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

Test Credentials

New password: ••••••••

Confirm new password:

Change

Note: Browsers are starting to default to setting the SameSite cookie flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.

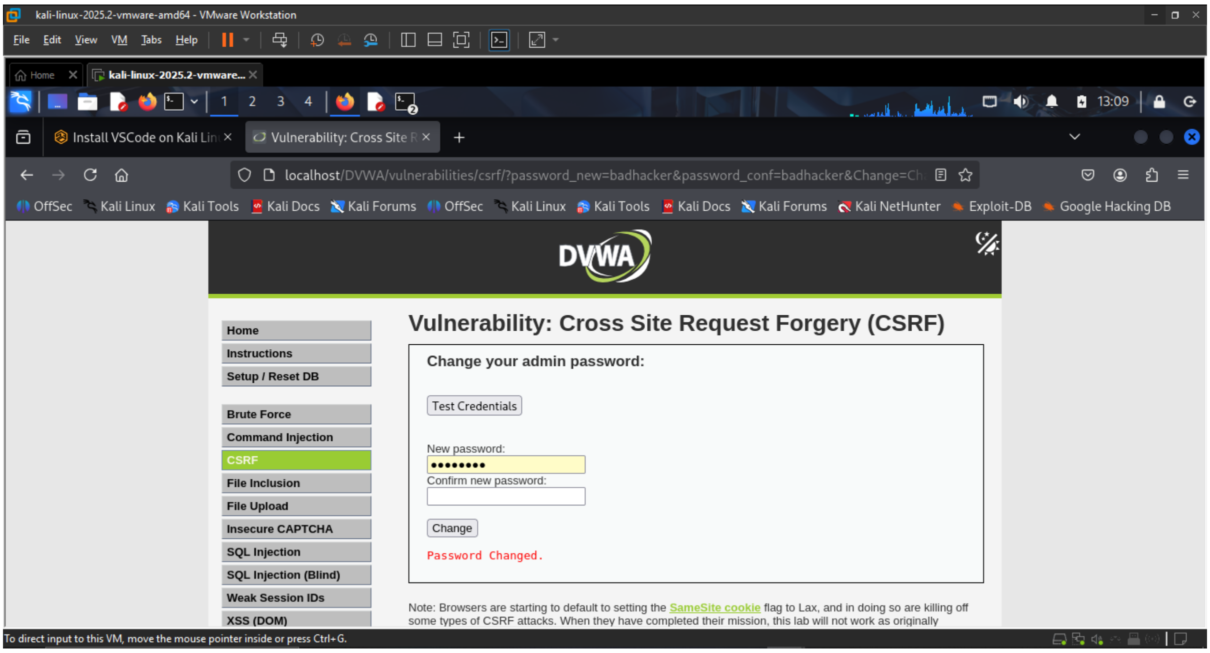
Announcements:

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

This is malicious link entered:

Payload(s):

- http://localhost/DVWA/vulnerabilities/csrf/?password_new=badhacker&password_conf=badhacker&Change=Change ➔ This is the link for the password change.
- <html>
  <body>
  <h1>You've just won a free trip to any country of your choice and an iPhone 16 Pro Max! 🎁</h1>
  <img src="http://localhost/DVWA/vulnerabilities/csrf/?password_new=badhacker&password_conf=badhacker&Change=Change" style="display:none">
  </body>
  </html> ➔ This is the HTML file we created that can be run in the victim's website and browser.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
13:09
Install VSCode on Kali Lin
Vulnerability: Cross Site R
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
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)
Test Credentials
Change
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

localhost/DVWA/vulnerabilities/csrf/?password_new=badhacker&password_conf=badhacker&Change=Ch

Vulnerability: Cross Site Request Forgery (CSRF)

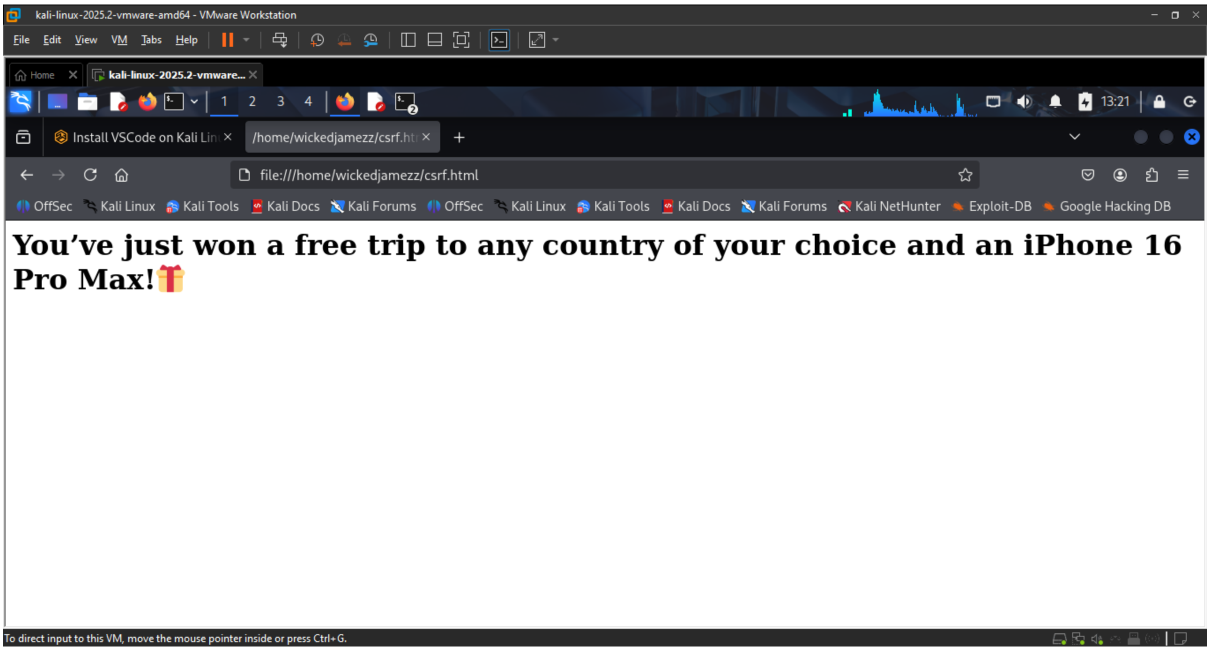
Change your admin password:

New password: ••••••••

Confirm new password:

Password Changed.

Note: Browsers are starting to default to setting the SameSite cookie flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
13:21
Install VSCode on Kali Lin
/home/wickedjamezz/csrf.ht
OffSec Kali Linux Kali Tools Kali Docs Kali Forums OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

file:///home/wickedjamezz/csrf.html

You’ve just won a free trip to any country of your choice and an iPhone 16 Pro Max!🎁

Mitigations recommended:

- Use CSRF tokens in forms.
- Require POST requests for sensitive actions.
- Check the ‘referrer’ or ‘Origin’ header.