

Practical :- 6

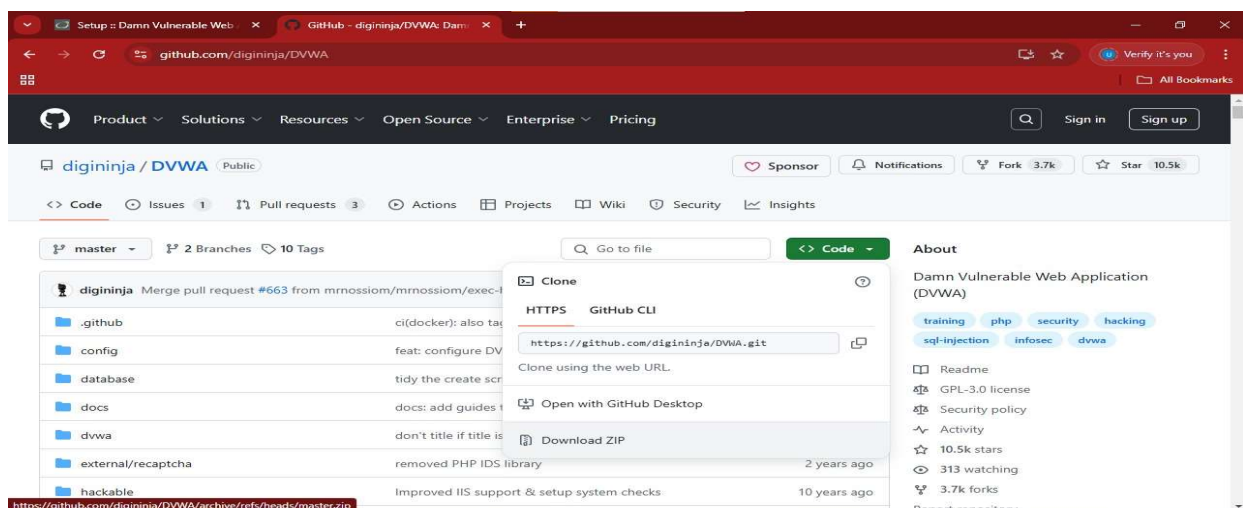
Aim :- Persistent Cross-Site Scripting Attack

- 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.

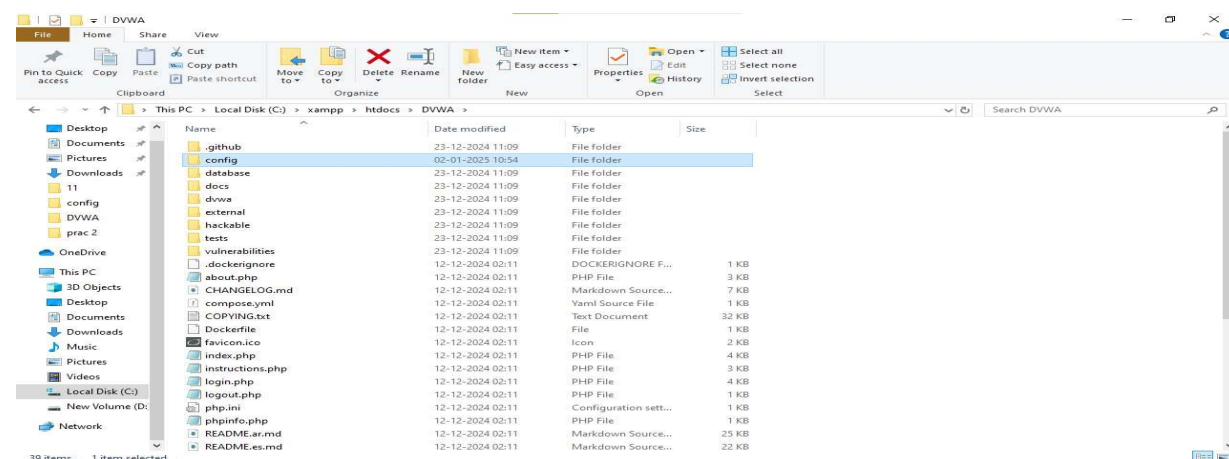
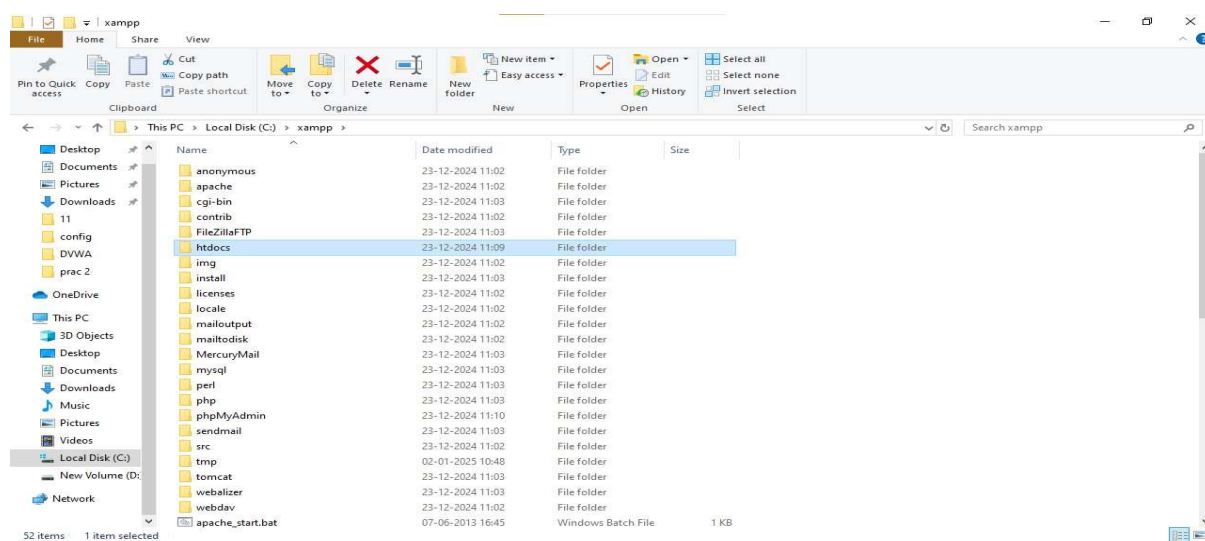
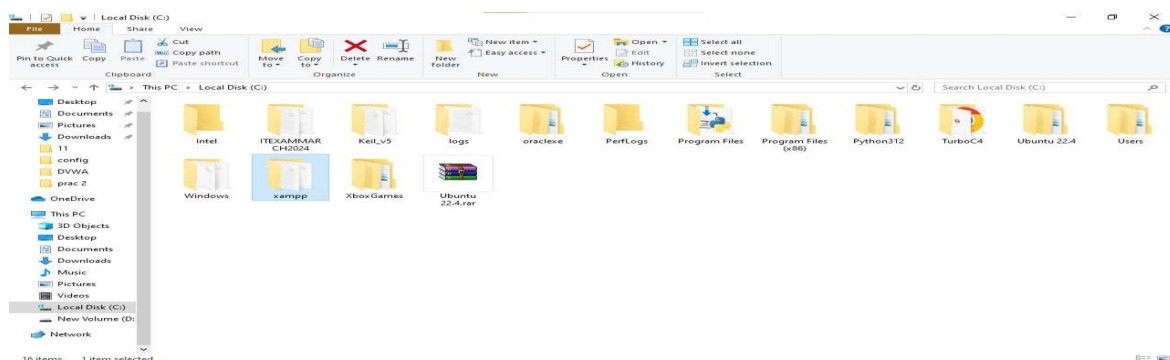
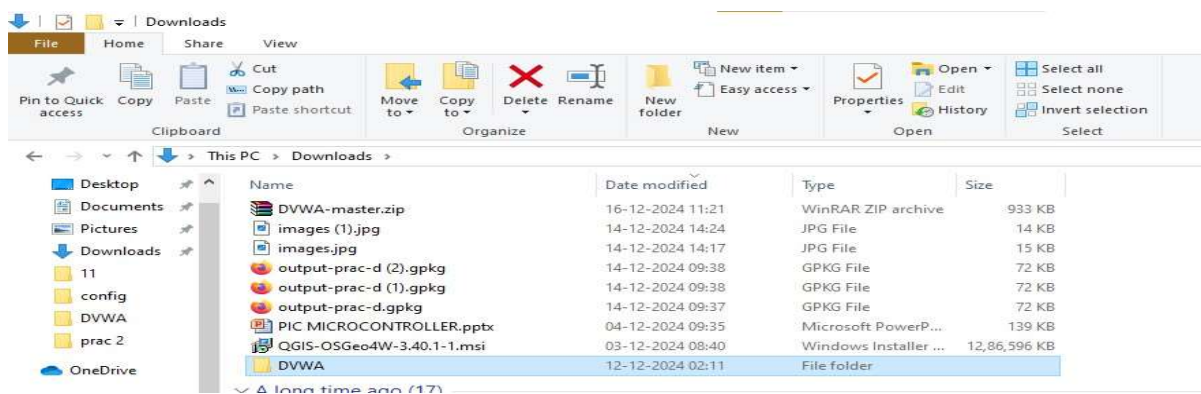
Cross Site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client side scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access controls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



```

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';

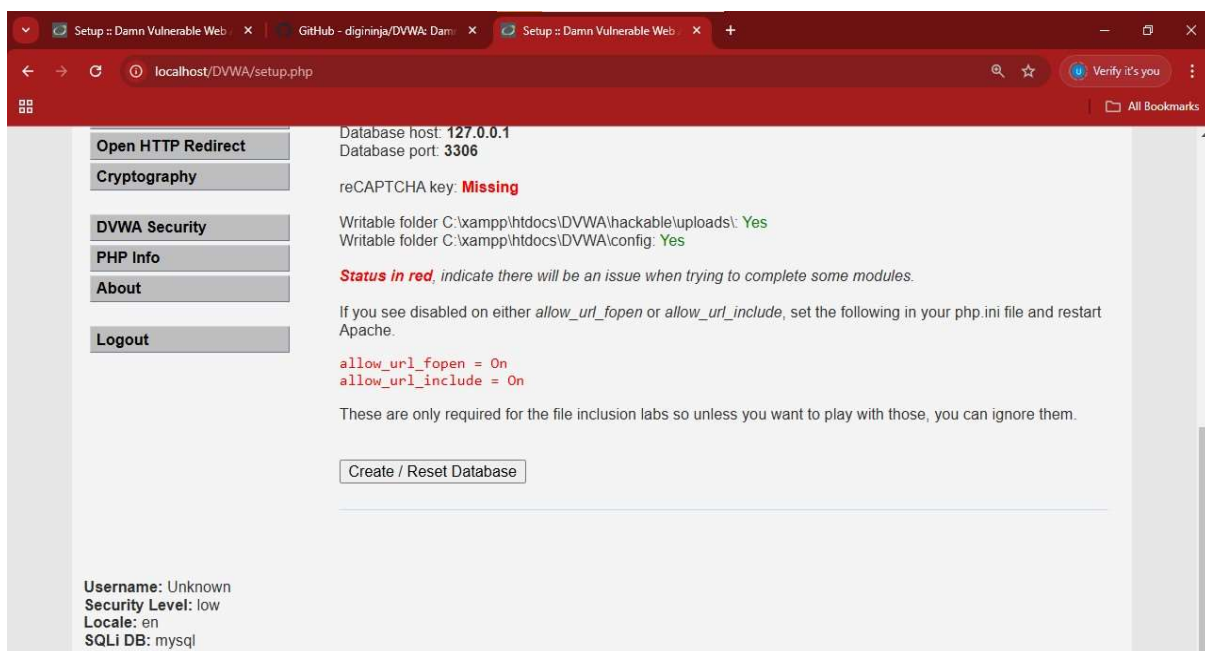
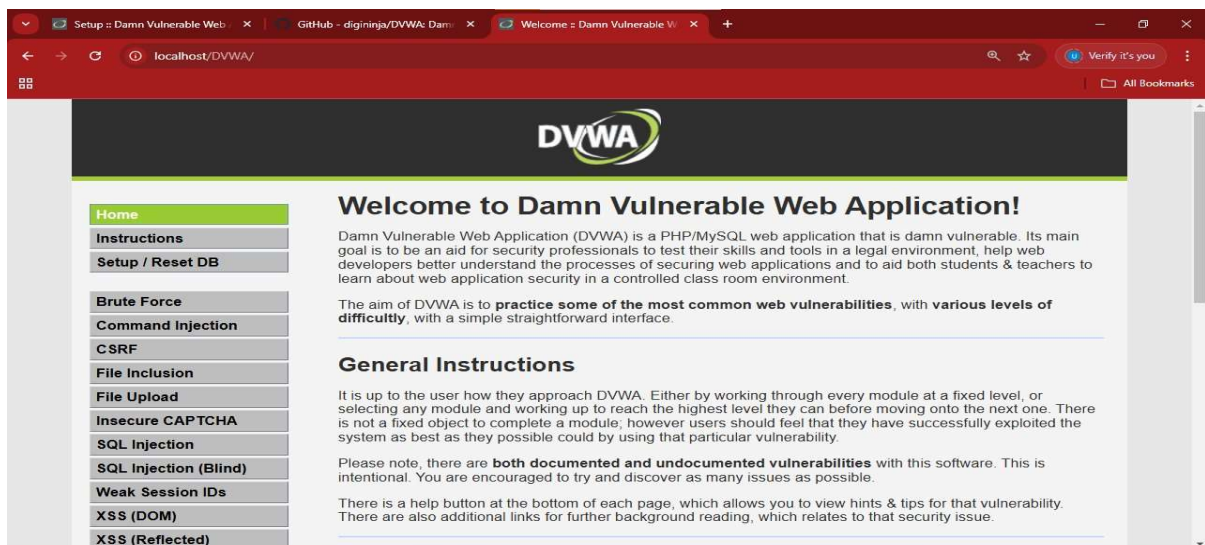
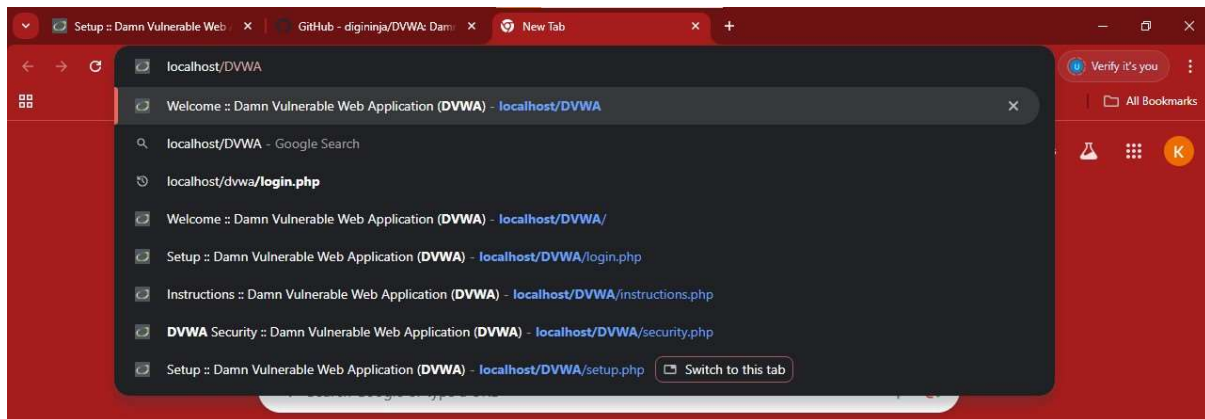
# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$ _DVWA[ 'default_locale' ] = getenv('DEFAULT_LOCALE') ?: 'en';

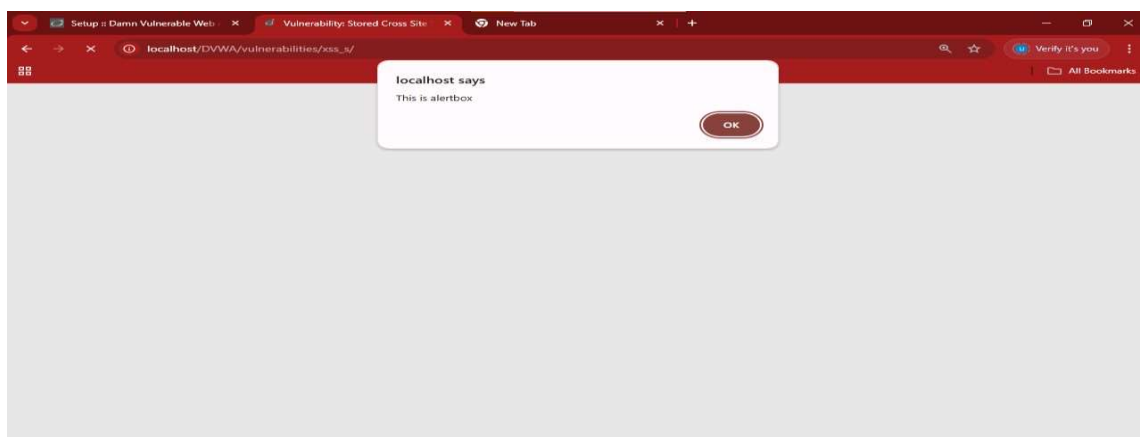
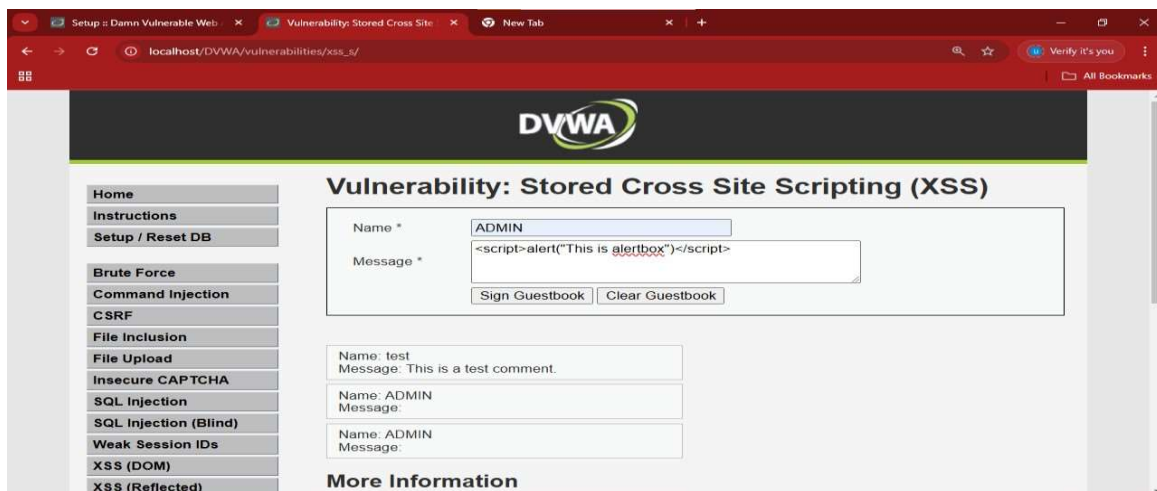
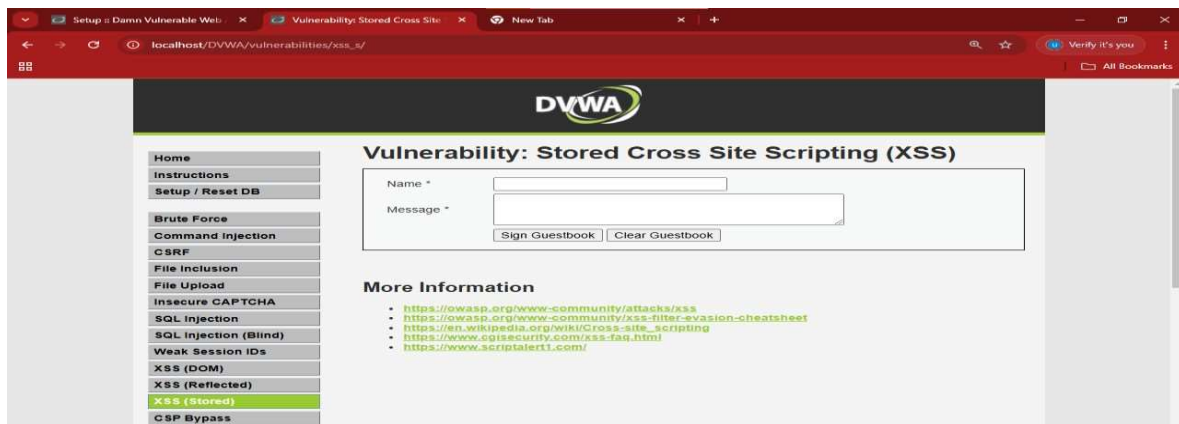
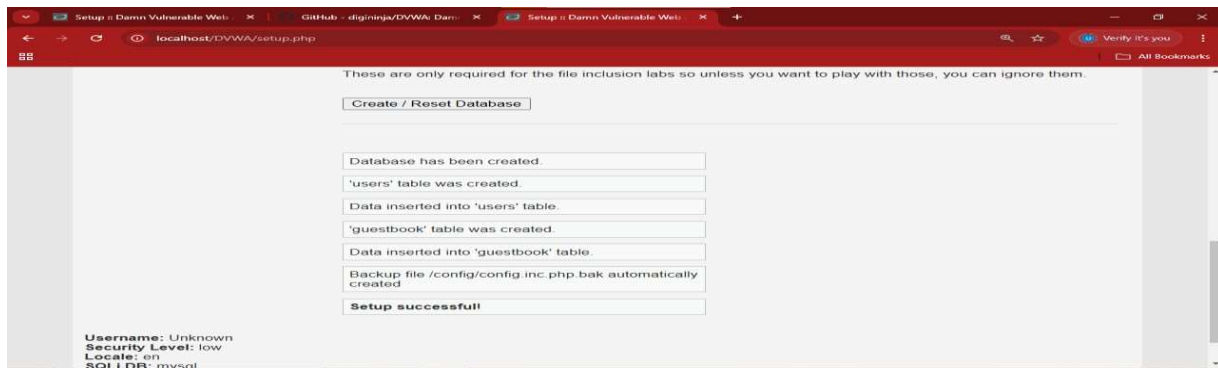
# Disable authentication
# Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$ _DVWA[ 'disable_authentication' ] = getenv('DISABLE_AUTHENTICATION') ?: true;

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

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

```



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