

Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 4

```
File Actions Edit View Help
kali@kali:~/var/www/html$
$ sudo su
[sudo] password for kali:
kali@kali:~/var/www/html$
kali@kali:~/var/www/html$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 4710, done.
remote: Counting objects: 100% (260/260), done.
remote: Compressing objects: 100% (163/163), done.
remote: Total 4710 (delta 133), reused 198 (delta 92), pack-reused 4450 (from 1)
Receiving objects: 100% (4710/4710), 2.17 MiB | 9.39 MiB/s, done.
Resolving deltas: 100% (2228/2228), done.
kali@kali:~/var/www/html$
$ mv DVWA dvwa
mv: cannot move 'DVWA' to 'dvwa/DVWA': Directory not empty
kali@kali:~/var/www/html$
$ rm DVWA
rm: cannot remove 'dvwa': Is a directory
kali@kali:~/var/www/html$
$ rmdir dvwa
rmdir: failed to remove 'dvwa': Directory not empty
kali@kali:~/var/www/html$
$ ls dvwa
about.php  CHANGELOG.md  compose.yml  COPYING.txt  Dockerfile  favicon.ico  index.php  instructions.php  login.php  logout.php  php.ini  README.es.md  README.fr.md  README.pt.md  README.zh.md  SECURITY.md  security.txt  setup.php
kali@kali:~/var/www/html$
$ cd dvwa
$ ls
about.php  CHANGELOG.md  compose.yml  COPYING.txt  Dockerfile  favicon.ico  index.php  instructions.php  login.php  logout.php  php.ini  README.es.md  README.fr.md  README.pt.md  README.zh.md  SECURITY.md  security.txt  setup.php
kali@kali:~/var/www/html/dvwa$
$ cd -config
cd: no such file or directory: -config
kali@kali:~/var/www/html/dvwa$
$ cd /config
cd: no such file or directory: /config
kali@kali:~/var/www/html/dvwa$
$ cd config
$ ls
config.inc.php  config.inc.php.bak  config.php.dist  config.inc.php.save
kali@kali:~/var/www/html/dvwa/config$
```

```
# 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 = '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'] = 'dvwa';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';
$_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'] = '';

# 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'] = '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'] = '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'] = false;

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

# SQLite DB Backend
# Use this to switch the backend database used in the SQLite and Blind SQLite 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.
$_DVWA['SQLI_DB'] = MYSQL;
$_DVWA['SQLI_DB'] = SQLITE;

# Read 56 Lines (Converted from DOS f...
```

Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 4

```
#!/usr/bin/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 = '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'] = 'dvwa';
$DVWA['db_user'] = 'user';
$DVWA['db_password'] = 'pass';
$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'] = '';

# 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'.
# Only an issue if you want to play with exploits
$DVWA['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'] = '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'] = 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.
$DVWA['SQLI_DB'] = MYSQL;
$DVWA['SQLI_DB'] = SQLITE;

# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# M-A Set Mark
# M-E Copy
# M-T To Bracket
# M-C Previous
# M-W Next
# B-B
# F-F
```

```
(root@kali)~# cd /var/www/html/dvwa
cd: no such file or directory: /config

(root@kali)~# cd /var/www/html/dvwa/config
ls
config.inc.php  config.inc.php.bak  config.inc.php.dist  config.inc.php.save

(root@kali)~# cp config.inc.php.dist config.inc.php
(root@kali)~# nano config.inc.php
(root@kali)~# service mysql restart
(root@kali)~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.9-MariaDB-1 Debian build-1 unstable

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

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

MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye

(root@kali)~# service apache2 start
(root@kali)~# cd /etc/php/7.4/apache2
(root@kali)~# service apache2 start
(root@kali)~#
```

Welcome to Damn Vulnerable Web

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is intended to be used for testing web security concepts and to help you learn about web application security in a controlled and safe environment.

The aim of DVWA is to practice some of the most common web vulnerabilities in a safe and controlled environment.

General Instructions

It is up to the user to try and exploit DVWA. Either by looking through the source code and working up to reach the highest level they can, or by using a third party tool to compromise a module. However, there should be no exploit as such as there should be no way to exploit the application.

Please note that we both documented and undocumented vulnerabilities. You are encouraged to try and discover as many as you can.

There is a help button at the bottom of each page which shows you the help for that module. There are also additional links for further background reading, which may be useful.

WARNING!

Damn Vulnerable Web Application is damn vulnerable. Do not upload to the Internet or any other public server, as they will be compromised. Please do not use DVWA on any production system. It is not a security tool. It is a training tool. It is not a security tool. It is a training tool.

Disclaimer

We do not take responsibility for the way in which any one uses this application. The authors of this application take no responsibility for any damage or loss of data. We do not take responsibility for any damage or loss of data. We do not take responsibility for any damage or loss of data.

More Training Resources

DVWA aims to cover the most commonly used vulnerabilities found in web applications. It is not a security tool. It is a training tool. It is not a security tool. It is a training tool.

Welcome :: Damn Vulne: X +

127.0.0.1/dvwa/

http://127.0.0.1/dvwa/ — Visit


- Login :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/login.php
- Vulnerability: DOM Based Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_d/default=youarehacked
- Vulnerability: DOM Based Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_d/default=you are hacked
- Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)</script>#
- Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_r/
- Vulnerability: Stored Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/xss_s/
- Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/sql/?id=%'+or+0=union+select+null+user()&Submit=Submit#
- Setup :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/setup.php
- Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) — http://127.0.0.1/dvwa/vulnerabilities/sql/

This time, search with:

Weak Session IDs

There is a hint button at the bottom of each page, which allows you to view hints & tips for that vulnerability

Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 4



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

DVWA Security

PHP Info

About

Logout

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 difficulty**, 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 vulnerability** 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.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

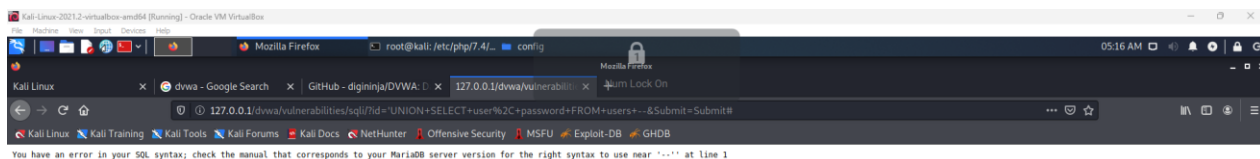
Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

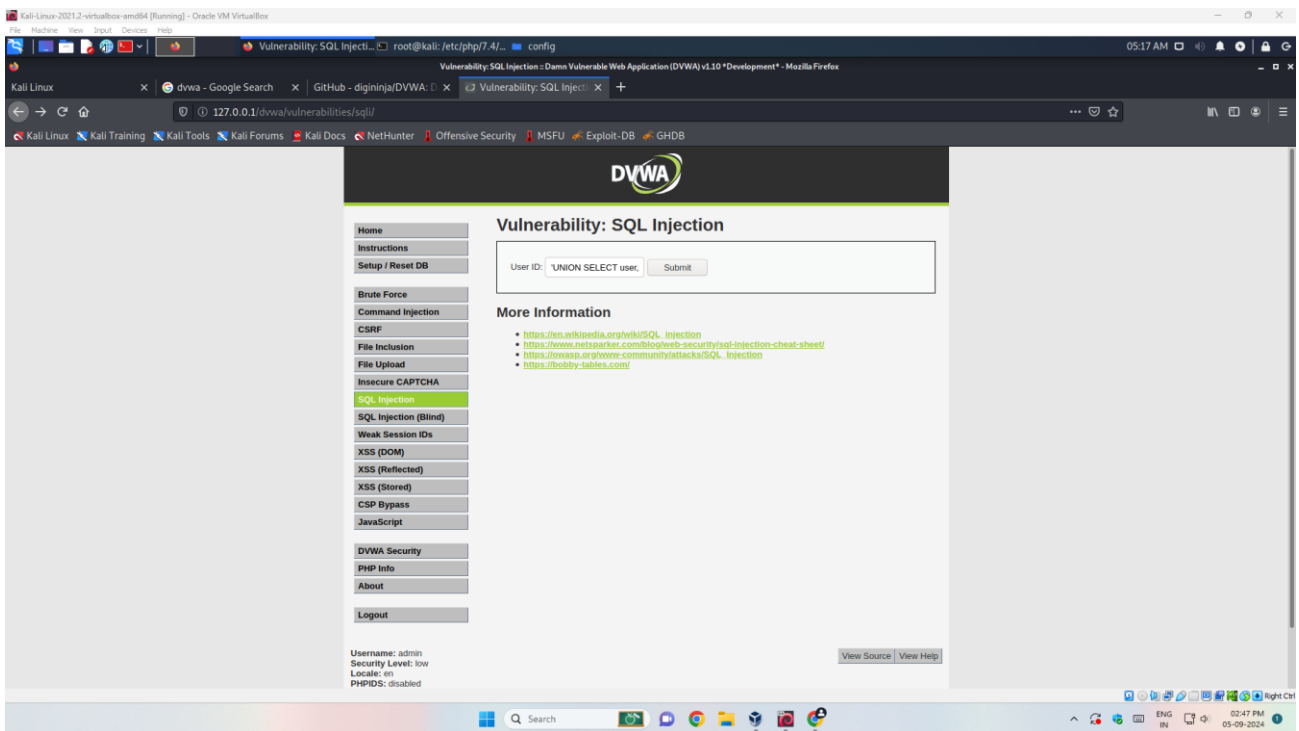
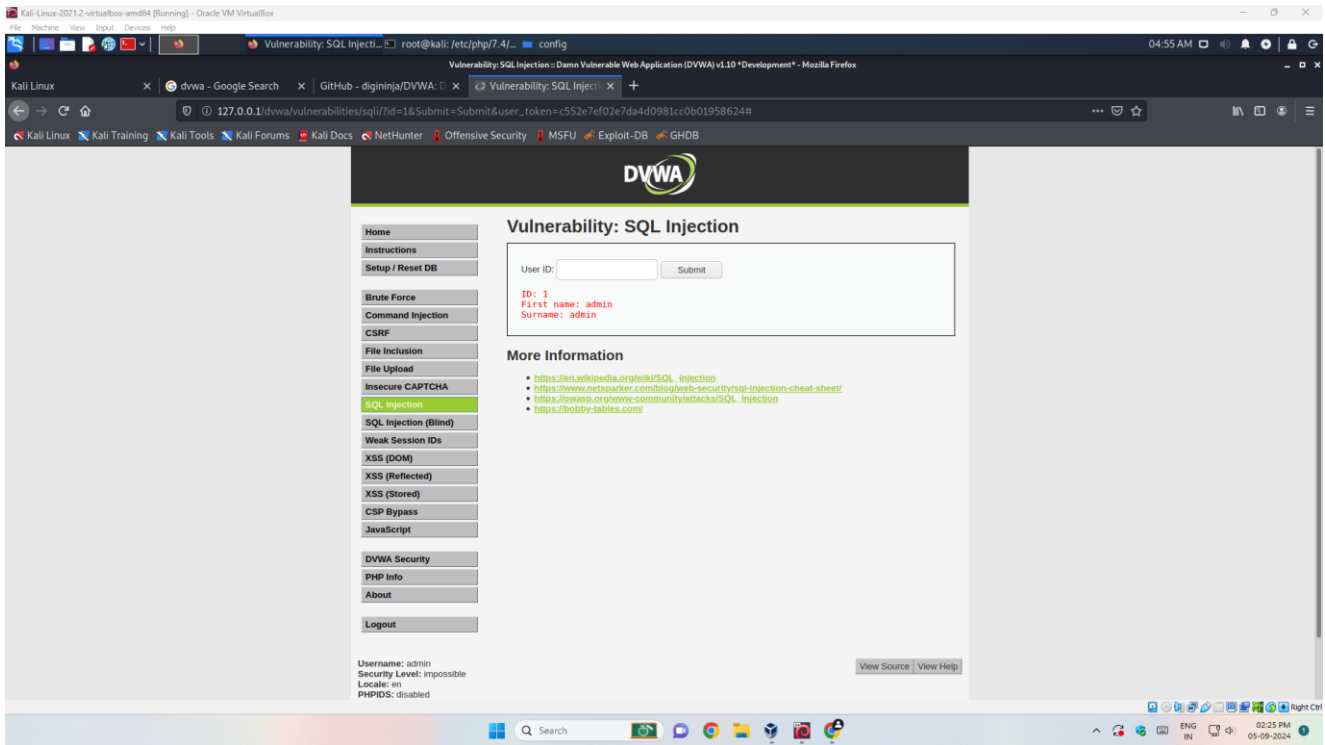
More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

[Mitillirao](#)



Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 4



Suraj S. Kaduvetti M.Sc.ComputerScience F015 Practical 4

