

<?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' ] = 'kali';
$_DVWA[ 'db_user' ] = 'kali';
$_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';
```

```
root@kali: /var/log

(root@kali)-[/var/log]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.11.5-MariaDB-3 Debian n/a

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 USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
ERROR 1396 (HY000): Operation CREATE USER failed for 'kali'@'127.0.0.1'
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.001 sec)
```



DVWA Security

Security Level

Security level is currently: low.

You can set the security level to low, medium, high

1. Low - This security level is completely vulnerable



- 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

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Security level set to low

Request to http://127.0.0.1:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty Raw Hex

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=h5pontuo9ht4rs5lulprd8vamr
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=73eefad2bbb744426a5e3b7ec57ade63
```

Request

PrettyRawHex

⌵

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

GET /DVWA/index.php HTTP/1.1

Host: 127.0.0.1

Cache-Control: max-age=0

sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Linux"

Upgrade-Insecure-Requests: 1

Origin: http://127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si

gned-exchange;v=b3;q=0.7

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Referer: http://127.0.0.1/DVWA/login.php

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: security=impossible; PHPSESSID=h5pontuo9ht4rs5lulprd8vavr

Connection: close

0 highlights

Response

PrettyRawHexRender

⌵

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

HTTP/1.1 200 OK

Date: Wed, 06 Dec 2023 10:16:22 GMT

Server: Apache/2.4.58 (Debian)

Expires: Tue, 23 Jun 2009 12:00:00 GMT

Cache-Control: no-cache, must-revalidate

Pragma: no-cache

Vary: Accept-Encoding

Content-Length: 6159

Connection: close

Content-Type: text/html; charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>

Welcome :: Damn Vulnerable Web Application (DVWA)

</title>

<link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />

<link rel="icon" type="image/ico" href="favicon.ico" />

<script type="text/javascript" src="dvwa/js/dvwaPage.js">

</script>

</head>

<body class="home">

<div id="container">

<div id="header">

</div>

<div id="main_menu">

<div id="main_menu_padded">

<ul class="menuBlocks">

<li class="selected">

Home

0 highlights