

```
# 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 @diginiinja for the fix.
```

```
# 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.
```

```
# 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.
```


File Azioni Modifica Visualizza Aiuto

GNU nano 6.4

config.inc.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
$DBMS = 'MySQL';
#$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' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_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.
```

^G Help

^O Salva

^W Cerca

^K Cut

^T Execute

^C Location

M-U Annulla

M-A Set Mark

M-] Parentesi

M-Q Precedente

^X Esci

^R Inserisci

^_ Sostituisci

^U Paste

^J Giustifica

^/ Vai a riga

M-E Ripeti

M-6 Copy

^Q Cerca Ind.

M-W Successiva

File Azioni Modifica Visualizza Aiuto

^C

— www.google.com ping statistics —

15 packets transmitted, 15 received, 0% packet loss, time 14030ms

rtt min/avg/max/mdev = 9.371/10.149/11.886/0.679 ms

(mattiadesimeï@kali)-[~]

\$ sudo su

(root@kali)-[/home/mattiadesimeï]

cd /var/www/html

File system

(root@kali)-[/var/www/html]

git clone https://github.com/digininja/DVWA

Clone in 'DVWA' in corso ...

remote: Enumerating objects: 4221, done.

remote: Total 4221 (delta 0), reused 0 (delta 0), pack-reused 4221

Ricezione degli oggetti: 100% (4221/4221), 1.87 MiB | 736.00 KiB/s, fatto.

Risoluzione dei delta: 100% (1999/1999), fatto.

home

(root@kali)-[/var/www/html]

chmod -R 777 DVWA/

(root@kali)-[/var/www/html]

cd DVWA/config

(root@kali)-[/var/www/html/DVWA/config]

cp config.inc.php.dist config.inc.php

(root@kali)-[/var/www/html/DVWA/config]

nano config.inc.php

(root@kali)-[/var/www/html/DVWA/config]

service mysql start

(root@kali)-[/var/www/html/DVWA/config]

mysql -u root -p

File Azioni Modifica Visualizza Aiuto

```
(root@kali)-[/var/www/html/DVWA/config]
# service mysql start
```

```
(root@kali)-[/var/www/html/DVWA/config]
# mysql -u root -p
```

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 32

Server version: 10.6.10-MariaDB-1+b1 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 (0,087 sec)

MariaDB [(none)]> exit

Bye

```
(root@kali)-[/var/www/html/DVWA/config]
# service apache2 start
```

```
(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php/8.1/apache2
```

```
(root@kali)-[/etc/php/8.1/apache2]
# cd /etc/php
```

```
(root@kali)-[/etc/php]
# ls
```

8.1

127.0.0.1/DVWA/setup.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

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)

DVWA

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: ***nix**

PHP version: **8.1.12**

PHP function display_errors: **Disabled**

PHP function safe_mode: **Disabled**

PHP function allow_url_include: **Disabled**

PHP function allow_url_fopen: **Enabled**

PHP function magic_quotes_gpc: **Disabled**

PHP module gd: **Missing - Only an issue if you want to play with captchas**

PHP module mysql: **Installed**

PHP module pdo_mysql: **Installed**

CTRL (DESTRA)

127.0.0.1/DVWA/setup.php

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: **Missing**

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: **Yes**

[User: root] Writable folder /var/www/html/DVWA/config: **Yes**

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.

`allow_url_fopen = 0n`
`allow_url_include = 0n`

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.


Create / Reset Database

Username: Unknown
Security Level: impossible
Locale: en
SQLi DB: mysql

Damn Vulnerable Web Application (DVWA)

CTRL (DESTRA)

 Request to http://127.0.0.1:80

[Forward](#)
[Drop](#)
[Intercept is on](#)
[Action](#)
[Open Browser](#)
[Comment this item](#)

[HTTP/1](#)


Pretty
Raw
Hex
Inspector

1 POST /DWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 87

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium";v="107", "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/107.0.5304.107 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=0.9

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

19 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

20 Cookie: security=impossible; PHPSESSID=0tmu2ra5lcp3mis2gmoar8ih2j

21 Connection: close

22

23 username=kali&password=password&Login=Login&user_token=97b645674674ded564704effd29e36d0

Request Attributes2

Request Query Parameters0

Request Body Parameters4

Request Cookies2

Request Headers20






0 matches

⚡

Burp Suite Community Edition v2022.9.6 - Temporary Project

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearn

1 x2 x+

Send⚙️Cancel< >

Target: http://127.0.0.1HTTP/1

Request

RawHex

1 POST /DWWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 87

4 Cache-Control: max-age=0

5 sec-ch-ua: "Chromium"; v="107", "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/107.0.5304.107 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=0.9

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/DWWA/login.php

18 Accept-Encoding: gzip, deflate

19 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

20 Cookie: security=impossible; PHPSESSID=0tmu2ra5lcp3mis2gmoar8ih2j

21 Connection: close

22

23 username=kali&password=password&Login=Login&user_token=97b645674674ded564704effd29e36d0

0 matches

Response

PrettyRawHexRender

0 matches

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters4

Request Cookies2

Request Headers20

Ready

Burp Suite Community Edition v2022.9.6 - Temporary Project

BurpProjectIntruderRepeaterWindowHelp

DashbaordTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearn

1 x2 x+

Send

Cancel

<>

Follow redirection

Target: http://127.0.0.1HTTP/1

Request

P

Raw

Hex

1

POST /DWWA/login.php HTTP/1.1

2

Host: 127.0.0.1

3

Content-Length: 87

4

Cache-Control: max-age=0

5

sec-ch-ua: "Chromium";v="107", "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/107.0.5304.107 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=0.9

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/DWWA/login.php

18

Accept-Encoding: gzip, deflate

19

Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

20

Cookie: security=impossible; PHPSESSID=0tmu2ra5lcp3mis2gmoar8ih2j

21

Connection: close

22

23

username=kali&password=password&Login=Login&user_token=97b645674674ded564704effd29e36d0

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 Found

2

Date: Wed, 12 Apr 2023 19:22:46 GMT

3

Server: Apache/2.4.54 (Debian)

4

Expires: Thu, 19 Nov 1981 08:52:00 GMT

5

Cache-Control: no-store, no-cache, must-revalidate

6

Pragma: no-cache

7

Location: login.php

8

Content-Length: 0

9

Connection: close

10

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

11

12

Inspector

Request Attributes

2

Request Query Parameters

0

Request Body Parameters

4

Request Cookies

2

Request Headers

20

Response Headers

9

?

Search...

0 matches

?

Search...

0 matches

Done300 bytes | 18 millis

1 x2 x+

SendCancel<>

Target: http://127.0.0.1HTTP/1

Request

PrettyRawHex

1 GET /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Cache-Control: max-age=0

4 sec-ch-ua: "Chromium";v="107", "Not=A?Brand";v="24"

5 sec-ch-ua-mobile: ?0

6 sec-ch-ua-platform: "Linux"

7 Upgrade-Insecure-Requests: 1

8 Origin: http://127.0.0.1

9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36

10 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=0.9

11 Sec-Fetch-Site: same-origin

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-User: ?1

14 Sec-Fetch-Dest: document

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

16 Accept-Encoding: gzip, deflate

17 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

18 Cookie: security=impossible; PHPSESSID=0tmu2ra5lcp3mis2gmoar8ih2j

19 Connection: close

20

21

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Wed, 12 Apr 2023 19:23:38 GMT

3 Server: Apache/2.4.54 (Debian)

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

5 Cache-Control: no-cache, must-revalidate

6 Pragma: no-cache

7 Vary: Accept-Encoding

8 Content-Length: 1434

9 Connection: close

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

11

12 <!DOCTYPE html>

13

14 <html lang="en-GB">

15

16 <head>

17

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

19

20 <title>

21 Login :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

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

25

26 <body>

27

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters0

Request Cookies2

Request Headers18

Response Headers9

Done

1.725 bytes | 2 millis