

Per **installare** il DVWA dobbiamo installare il database **MariaDB**, **mysql** e **web server apache**

MARIADB:

```
(kali@kali)-[~]  
$ sudo apt install mariadb-server
```

MYSQL:

```
(kali@kali)-[~]  
$ sudo apt update
```

```
(kali@kali)-[~]  
$ sudo apt install *mysql*
```

restart mysql e verifica

```
(kali@kali)-[~]  
$ service mysql restart  
  
(kali@kali)-[~]  
$ service mysql status  
mariadb.service - MariaDB 10.11.6 database server  
  Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: disabled)  
  Active: active (running) since Tue 2024-01-30 09:33:28 EST; 23s ago  
    Docs: man:mariadb(8)  
           https://mariadb.com/kb/en/library/systemd/  
Process: 7907 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)  
Process: 7911 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)  
Process: 7914 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/..; /usr/bin/galera_>  
Process: 7987 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)  
Process: 7990 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)  
Main PID: 7975 (mariabdb)  
  Status: "Taking your SQL requests now..."  
    Tasks: 13 (limit: 2265)  
  Memory: 91.3M  
    CPU: 241ms  
CGroup: /system.slice/mariadb.service  
└─7975 /usr/sbin/mariabdb
```

APACHE:

```
(kali@kali)-[~]  
$ sudo apt-get install apache2
```

2)

Eseguo i comandi di creazione e spostamento file/cartelle

```
(kali㉿kali)-[~]
$ cd /var/www/html

(kali㉿kali)-[/var/www/html]
$ git clone https://github.com/digininja/DVWA
fatal: could not create work tree dir 'DVWA': Permission denied

(kali㉿kali)-[/var/www/html]
$ sudo su
(root㉿kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 4494 (delta 15), reused 31 (delta 9), packed 0 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (4494/4494), 2.29 MiB | 1.72 MiB/s, done.
Resolving deltas: 100% (2110/2110), done.

(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]
# nano config.inc.php
```

3)

Modifico user e password

```
See README.md for more information
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER');
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port' ] = '3306';
```

4)

avviamento mysql e connessione al database

```
(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 33
Server version: 10.11.6-MariaDB-1 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)]> █
```

5)

Creazione nuovo utente e assegnazione privilegi

```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali'
Query OK, 0 rows affected (0.005 sec)
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON DVWA.* TO 'kali'@'127.0.0.1' identified by 'kali'
Query OK, 0 rows affected (0.003 sec)
```

6)

Configurazione servizio Apache

AVVIO (root@kali)-[/home/kali]
service apache2 start

SPOSTAMENTO DIRECTORY

```
(root@kali)-[~]
# cd /etc/php/8.2/apache2
```

MODIFICA FILE PHP.INI

```
(root@kali)-[/etc/php/8.2/apache2]
# nano php.ini
```

RESTART

```
(root@kali)-[/etc/php/8.2/apache2]  
# service apache2 restart
```

7)

Setup DVWA

inserire nel Browser l'indirizzo

127.0.0.1/DVWA/setup.php

Creare un nuovo Database
effettuare il login

Create / Reset Database

ed

8)

Aprire Burpsuite, scegliamo un progetto temporaneo, proxy, attiviamo l'intercettazione e apriamo il browser inserendo l'indirizzo 127.0.0.1/DVWA

loggando noteremo che i parametri di login sono stati catturati:

Request to http://127.0.0.1:80

Forward... Drop Intercept... Action Open... Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /DVWA/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:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
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/115.0.5790.171 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/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=
oh7a4mqunft696ldlrvtpq7gp7
21 Connection: close
22
23 username=admin&password=password&Login=Login&
user_token=130c98ae4a0dbd688b52e224dacdb5d5
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 4

Request cookies 2

Request headers 20

Search... 0 highlights

Login :: Damn Vulnerable x

127.0.0.1/DVWA/login.php



Username

admin

Password

Login

You have logged out

[Damn Vulnerable Web Application \(DVWA\)](#)

9)

Modifica dei parametri di accesso sostituendo con login errato

The screenshot shows the Burp Suite interface. On the left, the 'HTTP history' pane displays a request to `http://127.0.0.1/DVWA/login.php`. The request body contains a login attempt with the username `mortadella` and password `mozzarella&Login&user_token=d260e3004fbe63dfa9a3b8466d589652`. On the right, the 'Request query parameters' pane is open, showing a list of actions. The 'Send to Repeater' option is highlighted, which is used to send the selected request to the Repeater tool for further manipulation.

Request query parameters	
Scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Send to Organizer	Ctrl+O
Insert Collaborator payload	
Request in browser	
Engagement tools [Pro version only]	
Change request method	
Change body encoding	
Copy URL	
Copy as curl command (bash)	
Copy to file	
Paste from file	
Save item	
Don't intercept requests	
Do intercept	
Convert selection	

10)

Per inviare alla vittima il login con il cambio di dati procede con il menu repeater, send, follow redirection

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Repeater' pane displays a list of requests. The first request is selected, and the 'Send' button is highlighted. The 'Follow redirection' button is also visible, which is used to follow the redirection in the current response. The target URL is `http://127.0.0.1`.

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer
Decoder	Comparer	Logger	Organizer	Extensions	Learn	

1 x 2 x +

Send [Settings] Cancel < > Follow redirection Target: http://127.0.0.1

Follow the redirection in the current response

11)

Verifica login failed

The image displays two screenshots from a Burp Suite and a web browser interface, illustrating a login attempt on the DVWA (Damn Vulnerable Web Application).

Top Screenshot: The Burp Suite interface shows a request to `http://127.0.0.1:80` intercepted. The request is a POST to `/DVWA/login.php` with the following details:

- Host: `127.0.0.1`
- Content-Length: `88`
- Cache-Control: `max-age=0`
- sec-ch-ua: `sec-ch-ua-mobile: ?0`
- sec-ch-ua-platform: `""`
- Upgrade-Insecure-Requests: `1`
- Origin: `http://127.0.0.1`
- Content-Type: `application/x-www-form-urlencoded`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36`
- 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`
- Sec-Fetch-Site: `same-origin`
- Sec-Fetch-Mode: `navigate`
- Sec-Fetch-User: `??`
- Sec-Fetch-Dest: `document`
- Referer: `http://127.0.0.1/DVWA/login.php`
- Accept-Encoding: `gzip, deflate`
- Accept-Language: `en-US,en;q=0.9`
- Cookie: `security=impossible; PHPSESSID=rn0tar3qlipr3j8g0d2sbi9hlg`
- Connection: `close`
- Request body parameters: `username=panino&password=connortadella&Login=Login&user_token=e3fc8b44336251ba5e5c940de17f6929`

The browser window shows the DVWA login page with the username `admin` and password `*****` entered. The `Login` button is visible.

Bottom Screenshot: The Burp Suite interface shows the `Intercept` tab. The `Intercept` button is disabled, and the status is `Intercept is off`. The browser window shows the DVWA login page with the username `admin` and password `*****` entered. The `Login` button is visible, and the message `Login failed` is displayed below the password field.