

# DVWA

abbiamo aperto mariaDB e il database

File Actions Edit View Help

(kali@kali)-[~]

\$ mysql -u root -p

Enter password:

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

Your MariaDB connection id is 31

Server version: 10.11.4-MariaDB-1 Debian 12

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' ;

Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.\*TO'kali'@'127.0.0.1' IDENTIFIED BY 'kali';

Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit

Bye

(kali@kali)-[~]

\$

# andando su burp abbiamo cercato 127.0.0.1 e abbiamo intercettato i pacchetti

The screenshot displays the Burp Suite interface with the 'Intercept' tab selected. A request to `http://127.0.0.1:80` is shown, and the 'Intercept is on' button is active. The request is displayed in 'Pretty' format, showing an `HTTP/1.1` POST to `/DVWA/login.php`. The request body contains the following data:

```
username=admin&password=password&Login=Login&user_token=e43545432b13ebb2a99ffc7f630560b8
```

The right-hand pane shows the 'Inspector' tab, which is currently empty. The bottom status bar indicates '0 highlights'.

# notiamo che all interno abbiamo username e password

Burp Project Intruder Repeater View Help

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

1 x +

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

### Request

Pretty Raw Hex

```
1 GET /DVWA/index.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: ""
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)
10 Chrome/115.0.5790.171 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
12 ned-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=4fk9q8tch092kl18552j412vup
21 Connection: close
```

### Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Wed, 06 Dec 2023 11:32:14 GMT
3 Server: Apache/2.4.57 (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: 6103
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 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
18
19 <title>
20 Welcome :: Damn Vulnerable Web Application (DVWA)
21 </title>
22
23 <link rel="stylesheet" type="text/css" href="dvwa/css/main.css" />
24
25 <link rel="icon" type="image/ico" href="favicon.ico" />
26
27 <script type="text/javascript" src="dvwa/js/dvwaPage.js">
28 </script>
29
30 </head>
31
32 <body class="home">
33 <div id="container">
34
35 <div id="header">
36
37 
38
39 </div>
40
41 <div id="main_menu">
```

### Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

0 highlights

6,394 bytes | 11 millis