

## Esercizio 08-02

Utilizzo di Burpsuite per intercettare una richiesta di login e modificarne le credenziali per farla fallire

```
(kali㉿kali)-[~]
└─$ sudo apt install mysql -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package mysql

(kali㉿kali)-[~]
└─$ sudo su
(root㉿kali)-[/home/kali]
# service mysql start

(kali㉿kali)-[~]
└─$ sudo su
(root㉿kali)-[/home/kali]
# service mysql status
● mariadb.service - MariaDB 10.6.11 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Wed 2023-02-08 12:06:04 EST; 27s ago
     Docs: man:mariabdb(8)
           https://mariadb.com/kb/en/library/systemd/
  Process: 128467 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, st>
  Process: 128468 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, s>
  Process: 128470 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/.>
  Process: 128514 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, >
  Process: 128516 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 128500 (mariabdb)
   Status: "Taking your SQL requests now..."
    Tasks: 15 (limit: 2287)
  Memory: 91.0M
     CPU: 755ms
  CGroup: /system.slice/mariadb.service
          └─128500 /usr/sbin/mariabdb

Feb 08 12:06:04 kali mariabdb[128500]: 2023-02-08 12:06:04 0 [Note] InnoDB: Loading buffer pool(s) from /var/>
Feb 08 12:06:04 kali mariabdb[128500]: 2023-02-08 12:06:04 0 [Warning] You need to use --log-bin to make --ex>
Feb 08 12:06:04 kali mariabdb[128500]: 2023-02-08 12:06:04 0 [Note] InnoDB: Buffer pool(s) load completed at >
Feb 08 12:06:04 kali mariabdb[128500]: 2023-02-08 12:06:04 0 [Note] Server socket created on IP: '127.0.0.1'.
Feb 08 12:06:04 kali mariabdb[128500]: 2023-02-08 12:06:04 0 [Note] /usr/sbin/mariabdb: ready for connections.
Feb 08 12:06:04 kali mariabdb[128500]: Version: '10.6.11-MariaDB-2' socket: '/run/mysqld/mysqld.sock' port:>
Feb 08 12:06:04 kali systemd[1]: Started mariadb.service - MariaDB 10.6.11 database server.
Feb 08 12:06:04 kali /etc/mysql/debian-start[128518]: Upgrading MySQL tables if necessary.
Feb 08 12:06:05 kali /etc/mysql/debian-start[128530]: Checking for insecure root accounts.
Feb 08 12:06:05 kali /etc/mysql/debian-start[128534]: Triggering myisam-recover for all MyISAM tables and ari>
```

```
(root@kali)-[/home/kali]
# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.55-1).
The following packages were automatically installed and are no longer required:
  catfish dh-elpa-helper docutils-common gir1.2-xfconf-0 libcfitsio9 libgdal31 libpoppler123 libprotobuf23
  libzxcvbn python-pastedeploy-tpl python3-alabaster python3-docutils python3-imagesize python3-roman
  python3-snowballstemmer python3-speaklater python3-sphinx ruby3.0 ruby3.0-dev ruby3.0-doc sphinx-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Avviamento servizio Apache2

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

E verifica stato

```
(root@kali)-[/home/kali]
# service apache2 status
```

```
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Wed 2023-02-08 12:10:07 EST; 9s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 130673 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 130677 (apache2)
    Tasks: 6 (limit: 2287)
   Memory: 23.6M
      CPU: 142ms
   CGroup: /system.slice/apache2.service
           └─130677 /usr/sbin/apache2 -k start
             130679 /usr/sbin/apache2 -k start
             130680 /usr/sbin/apache2 -k start
             130681 /usr/sbin/apache2 -k start
             130682 /usr/sbin/apache2 -k start
             130683 /usr/sbin/apache2 -k start
```

```
Feb 08 12:10:06 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Feb 08 12:10:07 kali apachectl[130676]: AH00558: apache2: Could not reliably determine the server's fully qua>
Feb 08 12:10:07 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

```
(root@kali)-[/home/kali]
# cd /var/www/html
```

```
(root@kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
git: 'remote-https' is not a git command. See 'git --help'.
```

The most similar command is  
remote-https

```
(root@kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4112, done.
remote: Counting objects: 100% (126/126), done.
remote: Compressing objects: 100% (71/71), done.
remote: Total 4112 (delta 62), reused 114 (delta 54), pack-reused 3986
Receiving objects: 100% (4112/4112), 1.86 MiB | 831.00 KiB/s, done.
Resolving deltas: 100% (1920/1920), 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
```

Copia di un file su GitHub in  
“html” con modifica dei  
permessi per modificarlo

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

Connessione al db  
con utenza di root

```
(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 31
Server version: 10.6.11-MariaDB-2 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)]>
```

```
(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 31
Server version: 10.6.11-MariaDB-2 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'@'120.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.022 sec)
```

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.020 sec)
```

```
MariaDB [(none)]> exit
Bye
```

Creazione di una utenza  
“kali” con tutti i privilegi

```
(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 ..

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

(root@kali)-[/etc/php]
# ls
8.1 8.2

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

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

Spostamento in apache2  
passando per php 8.2  
(versione più recente)



Username

admin

Password

\*\*\*\*\*

Login

You have logged out

Intercettazione tentativo di login  
da web server di Burpsuite

Forward Drop Intercept is on Action Open Bro

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: "Not?A_Brand";v="8", "Chromium";v="108"
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.
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,:
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: PHPSESSID=bb0nosjjh426vd5t0odufta565; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=7d9ed64e0
```

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/108.0.5359.125 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/DVWA/login.php

18 Accept-Encoding: gzip, deflate

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

20 Cookie: PHPSESSID=bb0nosjjh426vd5t0odufta565; security=impossible

21 Connection: close

22

23 username=ciao&password=ciao&Login=Login&user\_token=7d9ed64e0c01a406a43e984dfd4b8df9

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Insert Collaborator payload

Request in browser >

Engagement tools [Pro version only] >

Change request method

Change body encoding

Copy URL

Copy as curl command

...

KHTML, image

dfd4b8df9

Modifica delle credenziali di accesso e invio pacchetto al ripetitore

PrettyRawHex

1 POST /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 Content-Length: 83

4 Cache-Control: max-age=0

5 sec-ch-ua: "Not?A\_Brand";v="8", "Chromium";v="108"

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/108.0.5359.125 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/DVWA/login.php

18 Accept-Encoding: gzip, deflate

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

20 Cookie: PHPSESSID=bb0nosjjh426vd5t0odufta565; security=impossible

21 Connection: close

22

23 username=ciao&password=ciao&Login=Login&user\_token=7d9ed64e0c01a406a43e984dfd4b8df9

PrettyRawHexRender

1 HTTP/1.1 302 Found

2 Date: Thu, 09 Feb 2023 15:30:39 GMT

3 Server: Apache/2.4.55 (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

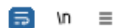
12

Pacchetto inviato al ripetitore e cliccato "send". A seguire clic su "follow redirection"



## Request

Pretty Raw Hex



```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
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/108.0.5359.125
  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: en-US,en;q=0.9
18 Cookie: PHPSESSID=bb0nosjjh426vd5t0odufta565; security=impossible
19 Connection: close
20
21
```

## Response

Pretty Raw Hex Render



```
1 HTTP/1.1 200 OK
2 Date: Thu, 09 Feb 2023 15:31:58 GMT
3 Server: Apache/2.4.55 (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: 1454
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>
  Login :: Damn Vulnerable Web Application (DVWA) v1.10
  *Development*
</title>
21
22 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
23
24 </head>
25
26 <body>
27
28 <div id="wrapper">
29
30 <div id="header">
31
32 <br />
33
34 <p>
  

```

Simulazione della  
richiesta di login

```
0
1 <br />
2
3 <div class="message">
  Login failed
</div>
4
5 <br />
6 <br />
7 <br />
```

Fallita perchè abbiamo  
sostituito le credenziali