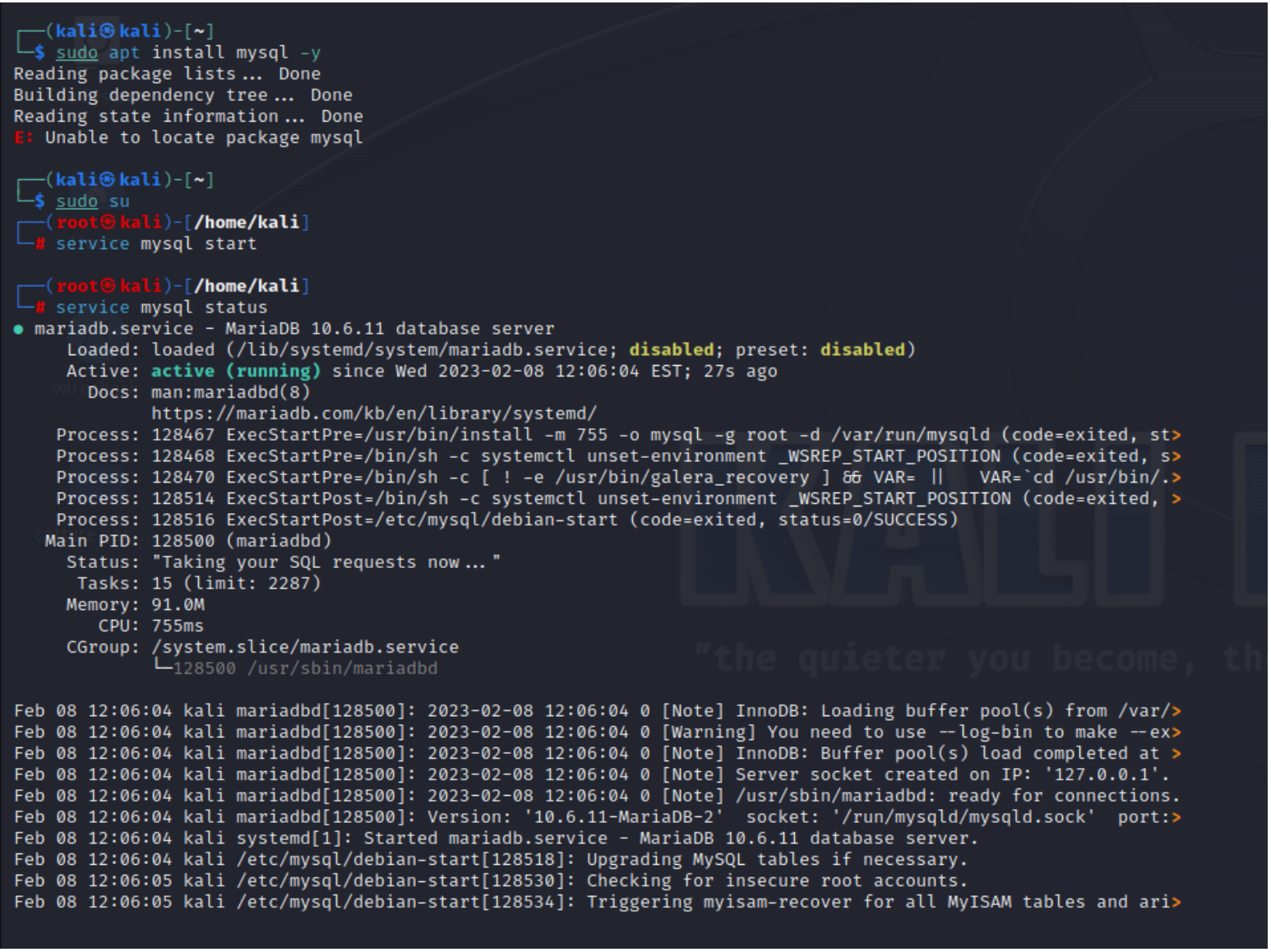
Esercizio 08-02

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



```
┌──(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
  libzxingcore1 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.

┌──(root㉿kali)-[/home/kali]
└─# service apache2 start

┌──(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.
```

Avviamento servizio Apache2

E verifica stato

```
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone hhtps://github.com/digininja/DVWA
Cloning into 'DVWA' ...
git: 'remote-hhtps' 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

┌──(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)]>
```

Connessione al db con utenza di root

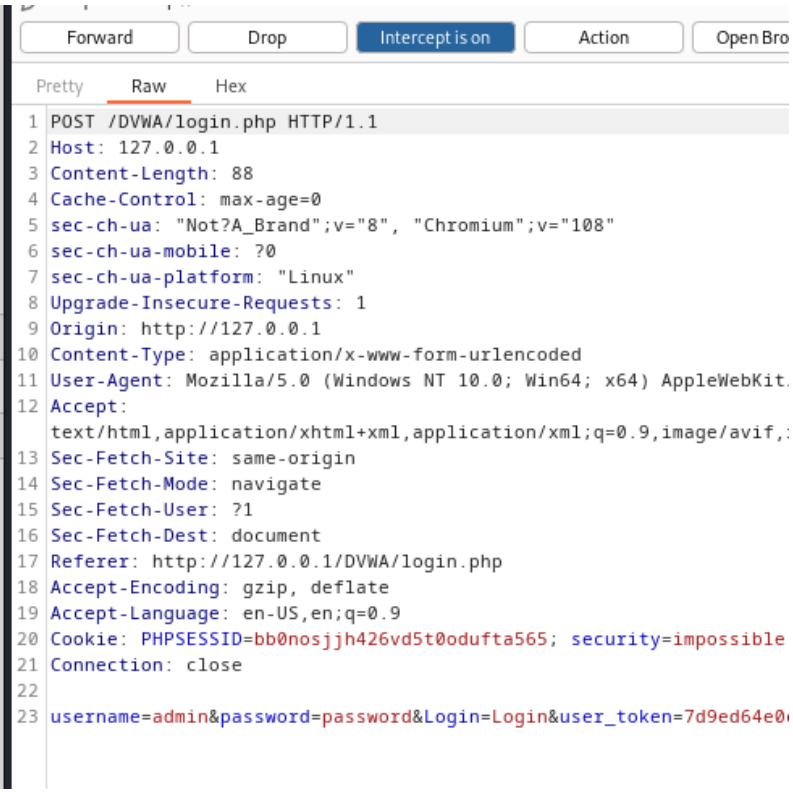
```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.11-MariaDB-2 Debian n/a

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)]> 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)

Intercettazione tentativo di login da web server di Burpsuite



```
9  Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlen
11 User-Agent: Mozilla/5.0 (Windows NT 10.0;
12 Accept:
   text/html,application/xhtml+xml,applicatio
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=bb0nosjjh426vd5t0odufta5
21 Connection: close
22
23 username=ciao&password=ciao&Login=Login&us
```

```
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,
p,imag
dfd4b8
```

Modifica delle credenziali di accesso e invio pacchetto al ripetitore

Pretty Raw Hex

```
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,im
   age/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
```

Pretty Raw Hex Render

```
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

```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
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/108.0.5359.125
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
9
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
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=bb0nosjjh426vd5t0odufta565; security=impossible
Connection: close
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Thu, 09 Feb 2023 15:31:58 GMT
Server: Apache/2.4.55 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1454
Connection: close
Content-Type: text/html;charset=utf-

<!DOCTYPE html>

<html lang="en-GB">

  <head>

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

    <title>
      Login :: Damn Vulnerable Web Application (DVWA) v1.10
      *Development*
    </title>

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

  </head>

  <body>

    <div id="wrapper">

      <div id="header">

        <br />

        <p>
          <img src="dvwa/images/login_logo.png" />
```

Simulazione della richiesta di login

```
        <br />

        <div class="message">
          Login failed
        </div>

        <br />
        <br />
        <br />
```

Fallita perchè abbiamo sostituito le credenziali