

BurpSuite

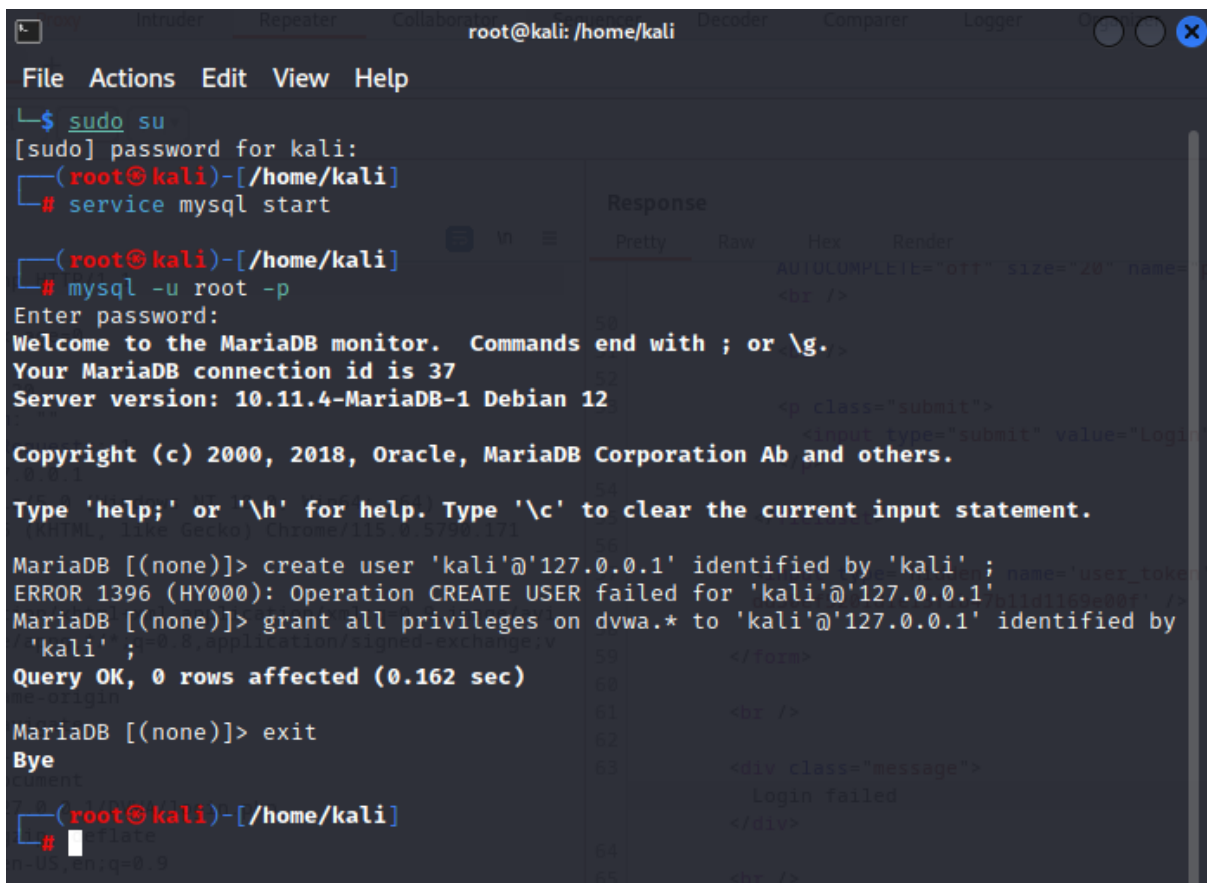
Oggi abbiamo fatto pratica installando programmi e inserendo comandi vari come qui sotto nelle foto.

Qui abbiamo scaricato dei servizi obbligatori e necessari per il nostro lavoro.

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

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

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



```
File Actions Edit View Help
root@kali: /home/kali

$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# service mysql start

(root@kali)-[/home/kali]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 37
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';
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 (0.162 sec)

MariaDB [(none)]> exit
Bye

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

Adesso apriamo burp suite che lo utilizzerò come un proxy per intercettare il sito di DVWA, e modifichiamo username e password

in ciao.

The screenshot displays the Burp Suite Community Edition v2023.9.1 interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below the menu, a tabbed interface shows Dashboard, Target, Proxy (selected), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, and Logger. The Proxy tab is active, showing a list of intercepted requests. The first request is selected, and its details are shown in the main pane. The request is a POST to /DVWA/login.php. The raw view is selected, showing the full HTTP request including headers and body. The body contains a login attempt with username=admin and password=password.

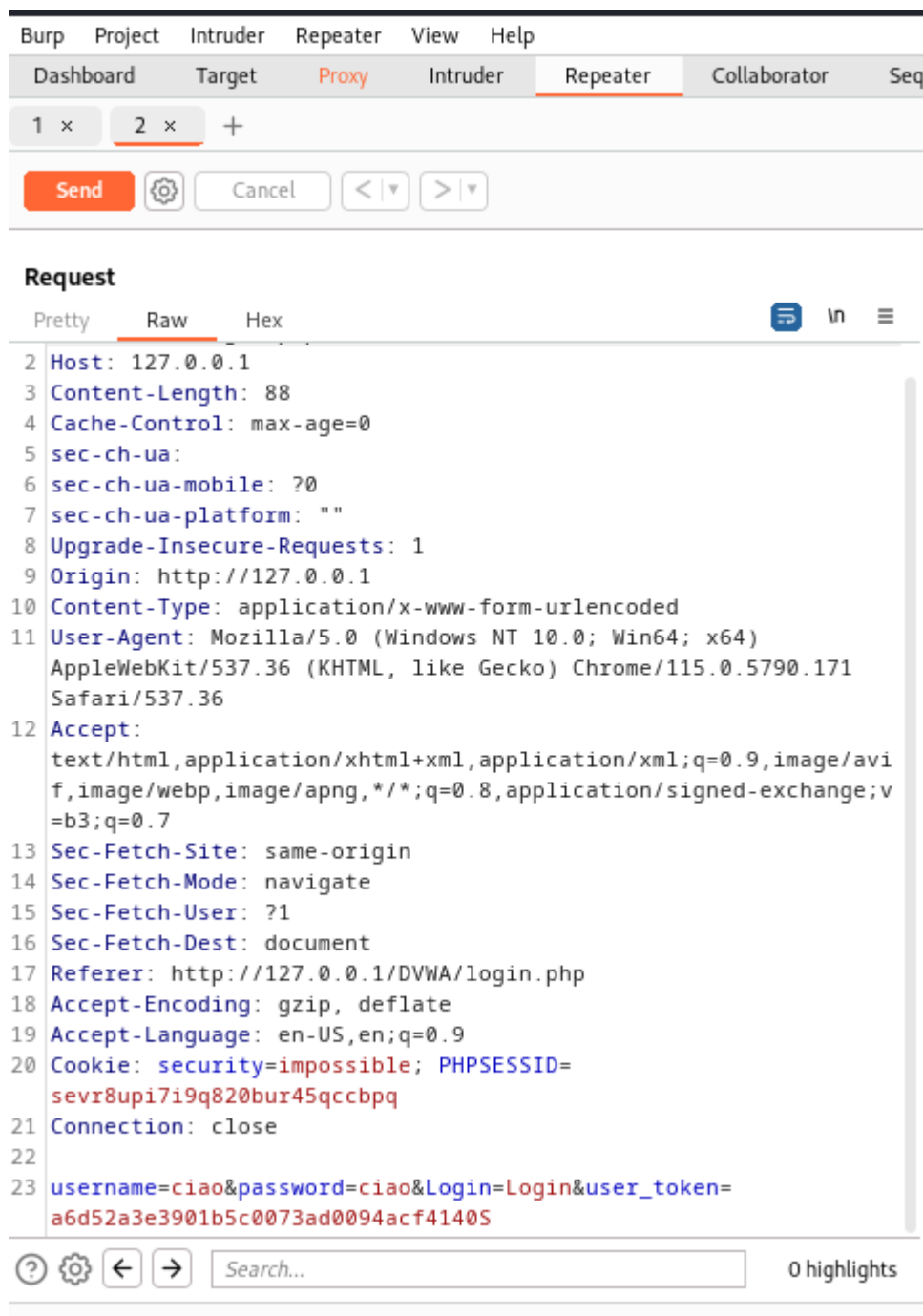
Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

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
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
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=sevr8upi7i9q820bur45qccbpq
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=a6d52a3e3901b5c0073ad0094acf41405
```

Dopodiché andiamo col tasto destro e mandalo sul repeater, e spostiamoci dalla tabella Proxy alla tabella Intruder.



Ora facciamo Send e poi poco a destra comparirà follow direction



Ed arriviamo al punto finale dell'esercizio dove ovviamente ci sarà **login failed** perchè abbiamo modificato le nostre credenziali prima.

⚙️

Burp Suite Community Edition v2023.9.1 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

1 x2 x3 x+

Send⚙️Cancel<>

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:

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) Chrome/115.0.5790.171 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=0.7

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: security=impossible; PHPSESSID=sevr8upi7i9q820bur45qccbpq

19 Connection: close

20

21

Response

PrettyRawHexRender

50 AUTOCOMPLETE="off" size="20" name="password">

51

52

53 <p class="submit">

54 <input type="submit" value="Login" name="Login">

55 </p>

56 </fieldset>

57 <input type='hidden' name='user_token' value='dd30ef5201d1e13f1b47b11d1169e00f' />

58 </form>

59

60

61

62 <div class="message">

63 Login failed

64 </div>

65

66

67

68

69

70

71

72

⚙️⏪⏩Search...0 highlights

⚙️⏪⏩Search...0 highlights

🔍🔊📄🔗📁🖨️🌐📶