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

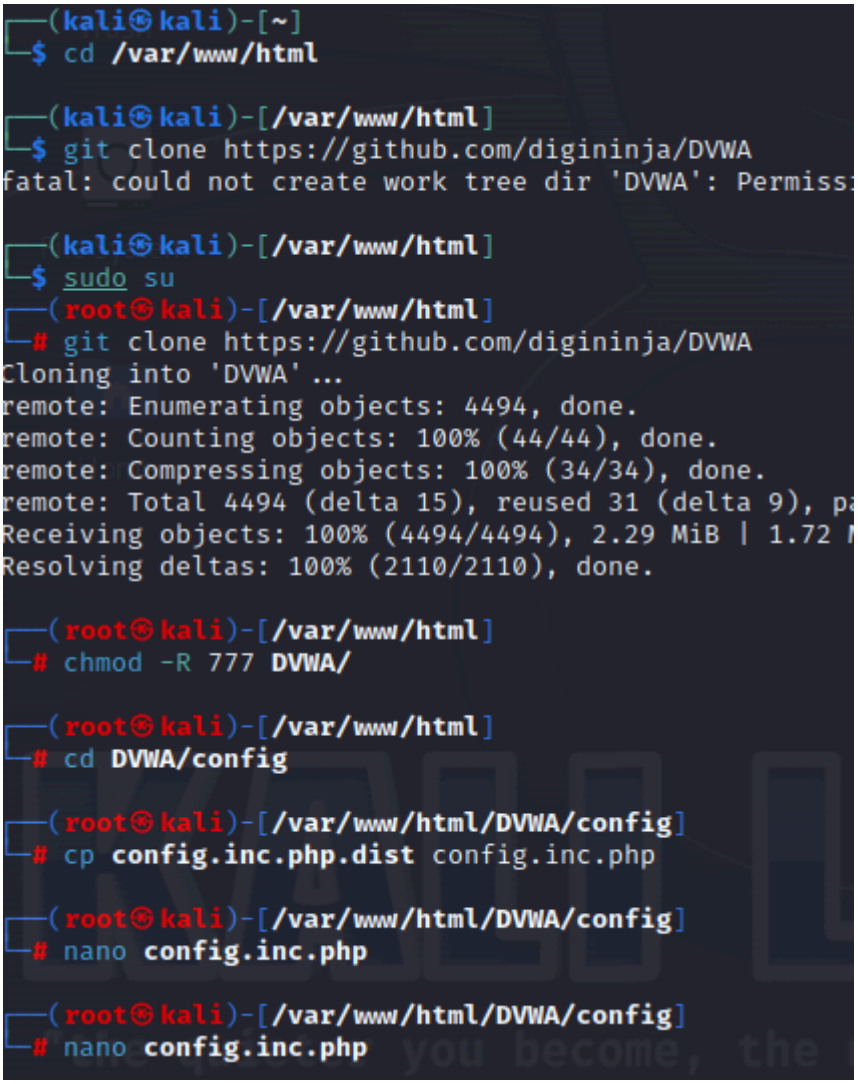
```
┌──(kali㉿kali)-[~]
└─$ service mysql restart

┌──(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:mariadbd(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 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 13 (limit: 2265)
     Memory: 91.3M
        CPU: 241ms
     CGroup: /system.slice/mariadb.service
             └─7975 /usr/sbin/mariadbd
```

APACHE:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install apache2
```

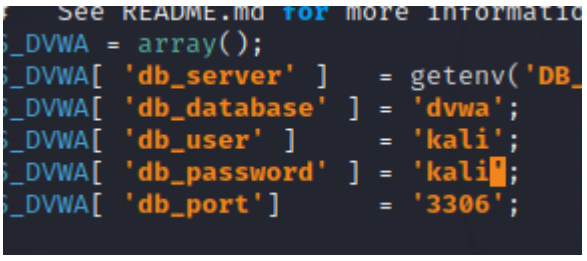
2)

Eseguo i comandi di creazione e spostamento file/cartelle



3)

Modifico user e password



4)

avviamento mysql e connessione al dagabase

```
┌──(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

7)

Setup DVWA

inserire nel Browser l’indirizzo

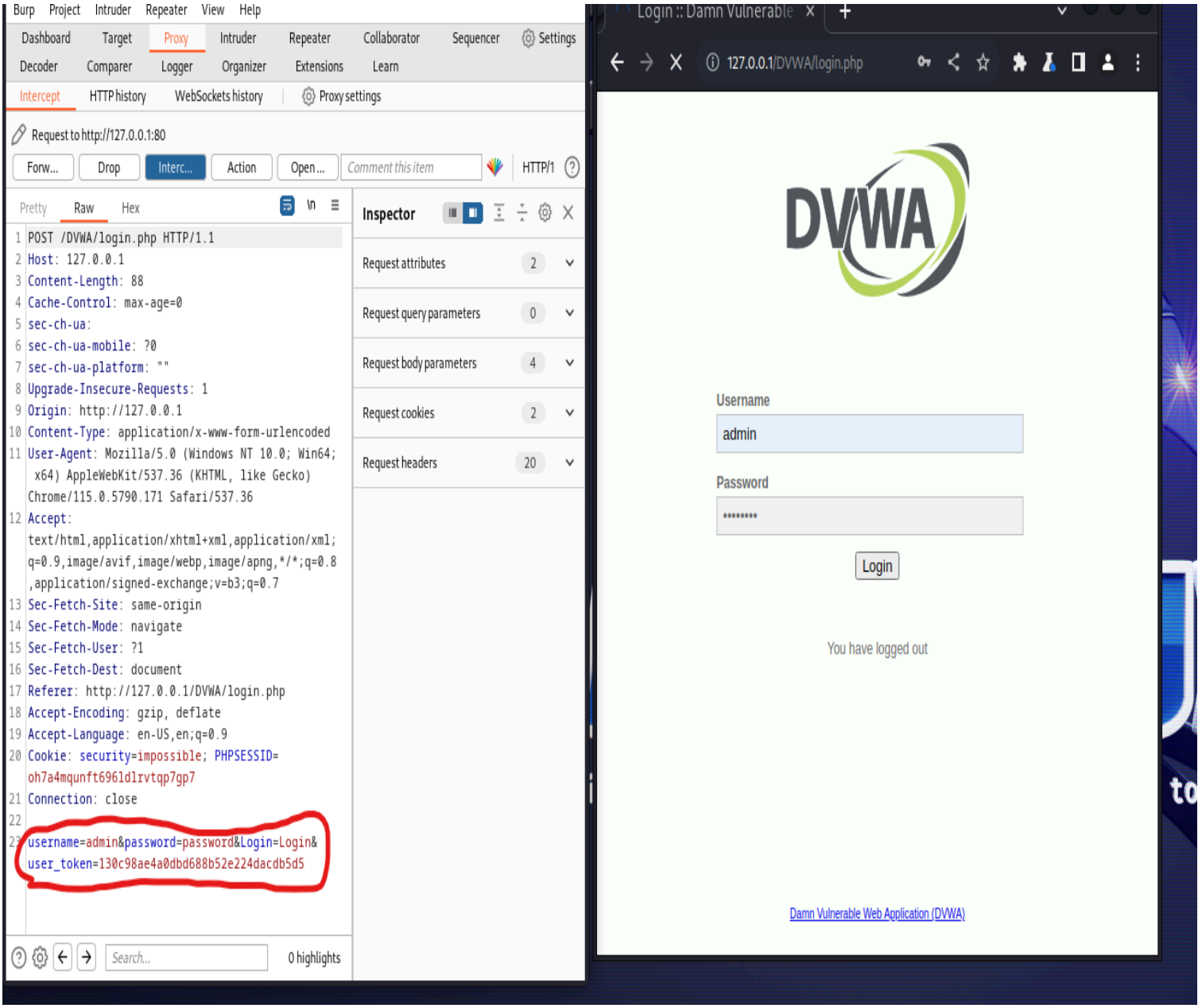
Creare un nuovo Database 

ed effettuare il login

8)

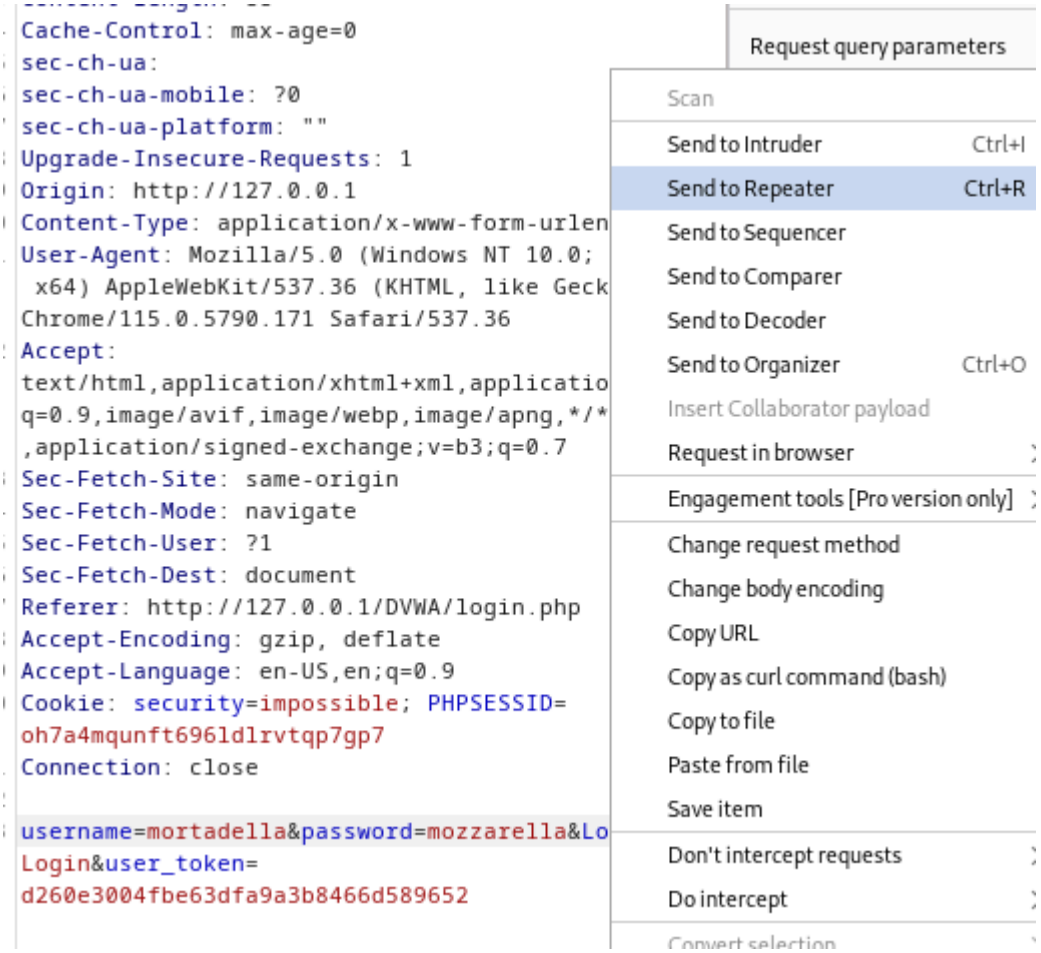
Aprire Burpsuite, scegliamo un progetto temporaneo, proxy, attiviamo l’intercettazione e apriamo il browser inserendo l’indirizzo 127.0.0.1/DVWA

loggando noteremo che i parametri di login sono stati catturati:


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Settings
Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forw... Drop Interc... 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=oh7a4mqunft696ldlrvtqp7gp7
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=130c98ae4a0dbd688b52e224dacdb5d5
Search... 0 highlights
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 20
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
admin
Password
Login
You have logged out
Damn Vulnerable Web Application (DVWA)

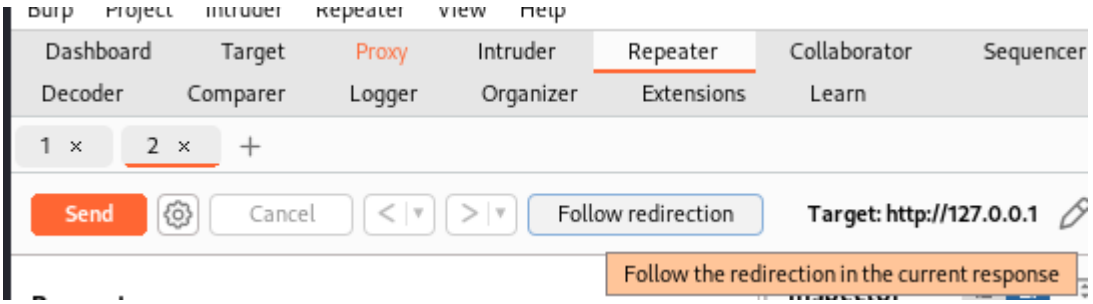
9)

Modifica dei parametri di accesso sostituendo con login errato



10)

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



11)

Verifica login failed