ENTRANDO SUI SITE DAI BURPSUITE

Inizio configurando il mio kali in bridge, impostando sul etc/network/interfaces in Lo e loopback.

Dopo entro in modo root, usando sudo su, faccio tutti gli update di kali, installo mysql, mariadb server e il server apache.

Parto con il creare il mio DVWA come segue nelle immagini:

1.

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

@ git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'....
remote: Enumerating objects: 4494, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 4494 (delta 15), reused [31 (delta 9), pack-reused 4450 Receiving objects: 100% (4494/4494), $2.29 MiB | 1.82 MiB/s, done.
Resolving deltas: 100% (2110/2110), done.
```

2.

```
(ront@ 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
```

Dopo eseguo il comando nano config.inc.php e modifico le credenziali di user e password con kali e kali

Dopo avvio il mio mysgl e modifico mariadb come su immagine:

```
(rost@ Wali)-[/home/kali]
service mysql start

(rost@ Wali)-[/home/kali]
service mysql status

mariadb.service - MariaOB 10.11.6 database server
Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
Active: active (running) since Wed 2024-01-31 12:55:19 EST; 8s ago
Docs: man:mariadbd(8)
https://mariadb.com/kb/en/library/systemd/
Process: 2332 ExecStartPre-/usr/bin/sntall -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
Process: 2331 ExecStartPre-/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
Process: 2421 ExecStartPre-/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
Process: 2423 ExecStartPre-/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
Main PID: 2933 (mariadbd)
Status: "Taking your SQL requests now..."
Tasks: 12 (limit: 2274)
Memory: 207.9M (peak: 211.0M)
CPU: 1.905S
CGroup: /system.slice/mariadb.service
__2393 /usr/sbin/mariadbd
```

```
(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 32
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)]> create user 'kali'@'1270.0.1' identified by 'kali';
Query OK, 0 rows affected (0.014 sec)
```

```
(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 34
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)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.021 sec)
MariaDB [(none)]> exit
Bye
```

Dopo avvio apache2

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

Entro sul mio browser e vado in cerca del sito 127.0.0.1/DWA/setup-php. e li dico di creare il "server"

Dopo entro con le credenziali "admin" "password" sul sito e cambio il livello di sicurezza come in immagine:



dopo inizio a rintracciare con Burpsuite il sito:

