Esercizio S3L3

Gianluca Barella

SCOPO: Configurare una DVWA su Kali Linux

Per prima cosa serve collegarsi alla rete internet da kali e per farlo è necessario attivare la scheda di rete di tipo “bridge” dalle impostazioni. Una volta fatto questo si apre il terminale e si esegue il comando “sudo su” per attivare l’utenza di root, dopodiché si eseguono una serie di comandi:

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.42 MiB | 1.26 MiB/s, done.
Resolving deltas: 100% (2420/2420), done.

┌──(root㉿kali)-[/var/www/html]
└─# chmod <89>R 777 DVWA/
chmod: invalid mode: ‘\211R’
Try 'chmod --help' for more information.

┌──(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
```

Una volta fatto questo si imposta nel file copiato utente e password:

```
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'kali';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'kali';
```

Ora si eseguono dei comandi per far partire il servizio e connetterci al data base

```
┌──(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: 11.4.2-MariaDB-4 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Ora creiamo un utente e gli assegniamo i privilegi, il messaggio di errore è dovuto al fatto che l'utente era già stato creato

```
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)]> 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 (0.044 sec)

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

Ora che abbiamo configurato il servizio facciamo partire il web server e dopo aver cercato il file php.ini andiamo a cambiare delle impostazioni:

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

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# nano php.ini
```

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Ora dal browser di Kali scriviamo sulla barra degli indirizzi 127,0,0,1/DVWA/setup.php e clicchiamo “Create Database”, una volta fatto questo si apre una pagina di login dove bisogna inserire le credenziali: “admin” e “password” da qui potremo entrare nell’app e scegliere la scheda DVWA.
Una volta fatto tutto questo proviamo ad intercettare il traffico con Burpsuite cambiando il livello di difficoltà della DVWA