

Pratica S3/L3

Esercizio Web Application – preparazione ambiente

Traccia:

Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test sia durante la build week 1 che durante lo sviluppo del modulo 2, dove vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

```
(kali@kali)-[~]
$ cd /var/www/html

(kali@kali)-[/var/www/html]
$ git clone https://github.com/digininja/DVWA
fatal: impossibile creare la directory dell'albero di lavoro 'DVWA': Permesso negato

(kali@kali)-[/var/www/html]
$ sudo su
(root@kali)-[/var/www/html]
# git clone https://github.com/digininja/DVWA
Clone in 'DVWA' in corso...
remote: Enumerating objects: 4436, done.
remote: Counting objects: 100% (211/211), done.
remote: Compressing objects: 100% (145/145), done.
remote: Total 4436 (delta 97), reused 145 (delta 63), pack-reused 4225
Ricezione degli oggetti: 100% (4436/4436), 2.17 MiB | 1.76 MiB/s, fatto.
Risoluzione dei delta: 100% (2099/2099), fatto.

(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

(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 37
Server version: 10.11.5-MariaDB-3 Debian n/a

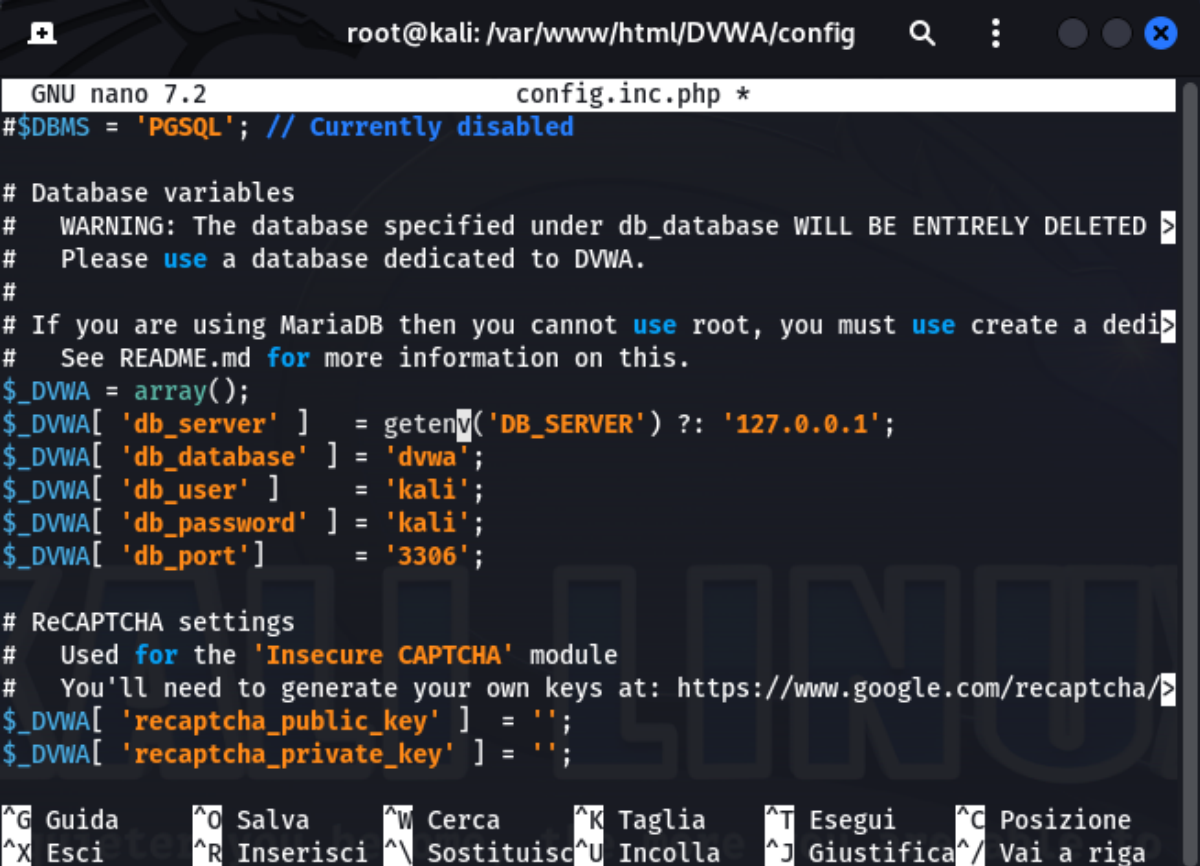
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> |
```

Comandi utilizzati per la creazione del server sql:

```
-cd /var/www/html
-git clone https://github.com/digininja/DVWA-chmod
-R 777 DVWA/
-cd DVWA/config-cp config.inc.php.dist config.inc.php
-nano config.inc.php
-service mysql start
```



```
root@kali: /var/www/html/DVWA/config
GNU nano 7.2 config.inc.php *
# $DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedi
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'kali';
$_DVWA['db_password'] = 'kali';
$_DVWA['db_port'] = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/
$_DVWA['recaptcha_public_key'] = '';
$_DVWA['recaptcha_private_key'] = '';

^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^T Esegui      ^C Posizione
^X Esci      ^R Inserisci  ^\ Sostituisci ^U Incolla     ^J Giustifica ^_ Vai a riga
```

Modifica nel nano 'db_user' e 'db_password' entrambi in kali

dopo la modifica nel nano :

```
-mysql -u root -p
-create user 'kali'@'127.0.0.1' identified by 'kali'
-grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by
'kali' ;
```

```

(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 38
Server version: 10.11.5-MariaDB-3 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'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
Bye

(root@kali)-[/var/www/html/DVWA/config]
# service apache2 start

(root@kali)-[/var/www/html/DVWA/config]
# 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]
# service apache2 start

(root@kali)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini

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

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

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

```

Comandi usati per creazione server apache2:

- service apache2 start
- cd /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

```

Una volta entrati nel file si deve settare 'allow_url_include = On'

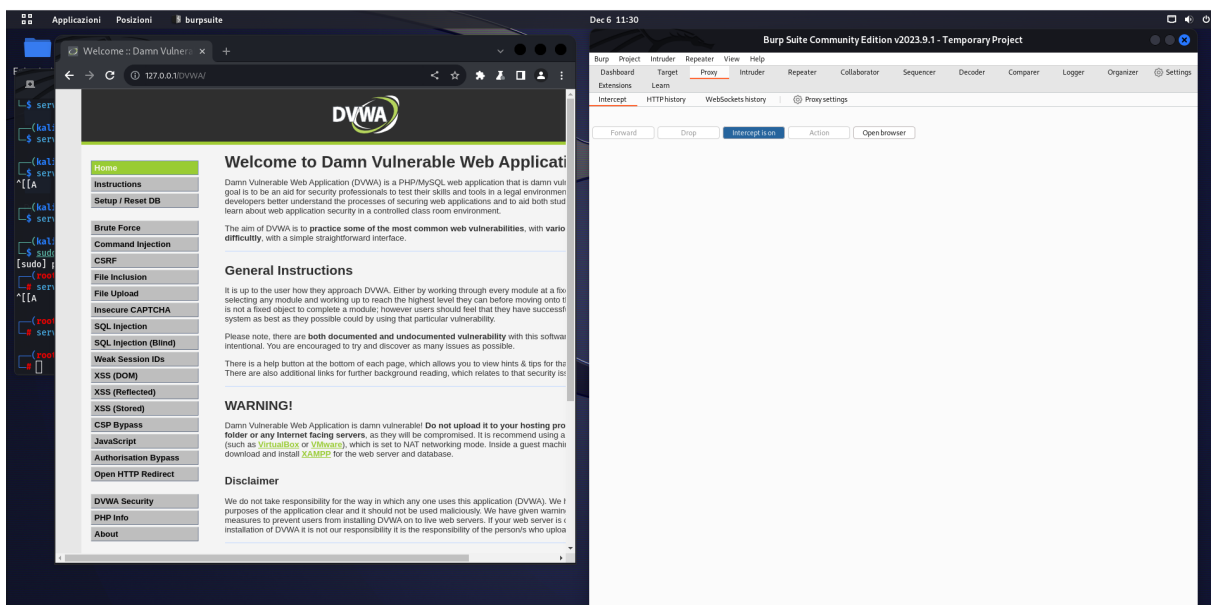
Una volta creati gli server si entra nel sito '127.0.0.1/DVWA/' entrati con le credenziali :

User : admin

password : password

alla schermata home in basso c'è il pulsante crea/reset database , una volta creato si va in basso a sinistra c'è l'opzione DVWA Secure , lì si può modificare il livello di sicurezza del server.

Fatto tutto ciò si può avviare Burpsuite



Creare un nuovo file in ascolto , andare nella voce Proxy e verificare che Intercept sia in on poi cliccare il bottone blue open Browser , ti si aprirà una finestra (in figura la finestra a sinistra) inserire l'indirizzo del sito (in questo caso l'indirizzo del database creato prima 127.0.0.1/DVWA/login) .

Dopo di che tornare su Burpsuite cliccare il pulsante forward per far caricare la pagina del sito e nel Burpsuite ti apparirà l'informazione che ha catturato di quella pagina web