Cyber Security Analyst

PROJECT REPORT

BURPSUITE DI KALI

In risposta all'esercizio sulla Burpsuite di Kali

Prepared by

Fulvio Zalateu

Security Rookies

Consegna:

In questa lezione pratica vedremo come configurare una DVWA – ovvero *damn vulnerable web application* in Kali Linux. La DVWA ci sarà molto utile per i nostri test, in cui vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

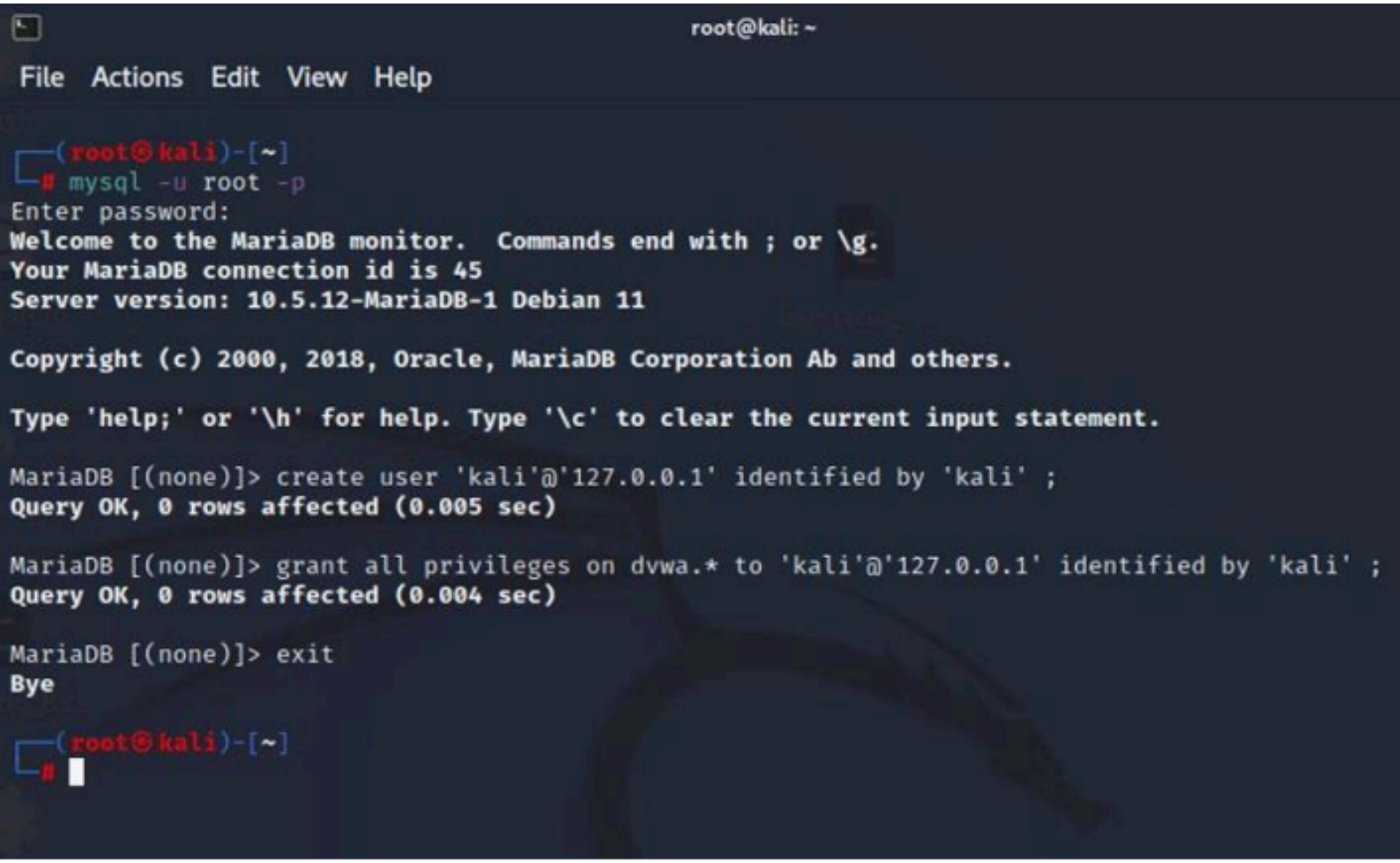
Procedimento

Installazione Database MySQL Eseguire i seguenti comandi da terminale di Kali in utenza di root.

1. Dal terminale inserire comando sudo su per ottenere i privilegi di amministratore. Recarsi alla cartella html da terminale con cd /var/www/html
2. Copiare/ scaricare la cartella DVWA dal link fornito dalla traccia dell'esercizio, comando git clone https://github.com/digininja/DVWA .

3.Cambiare I pri
vilegi della cartella DVWA in
R(4)+W(2)+X(1) = 7 per ogni gruppo
quindi 777, comando chmod -R 777
DVWA/ -R è usato per la modifica dei
permessi valida anche per i file all’interno
della cartella.
4. Recarsi nella cartella config, comando
cd DVWA/config .
5. Copiare i contenuti, comando cp
config.inc.php.dist config.inc.php .
6. Modificare il file tramite nano, comando
nano config.inc.php . Attraverso i comandi
nano, modificare username e password in
kali

7. Avviare il servizio mysql, comando service mysql start . 8. Connettere il database all’utenza di root, comando mysql –u root –p . 9. Creare l’utenza e i privilegi sul database, comandi create user 'kali'@'127.0.0.1' identified by 'kali' ; e grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali’;
10. Uscire con exit


root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 45
Server version: 10.5.12-MariaDB-1 Debian 11
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 (0.005 sec)
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.004 sec)
MariaDB [(none)]> exit
Bye
(root㉿kali)-[~]
#

Configurazione Apache service

Sempre da terminale in modalità utente root sudo su

1. Avviare il servizio apache, comando service apache2 start

2. Recarsi nella cartella di apache 2, comando cd /etc/php/x/apache2 (x è il numero della versione) In questo caso con il comando ls si scopre che la versione è la 8.2.

3. Aprire il file php.ini, comando nano php.ini

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

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# ls
conf.d  php.ini

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

4. Modificare la voce “allow_url_include” in On e assicurarsi che “allow_url_fopen” sia anch’esso On

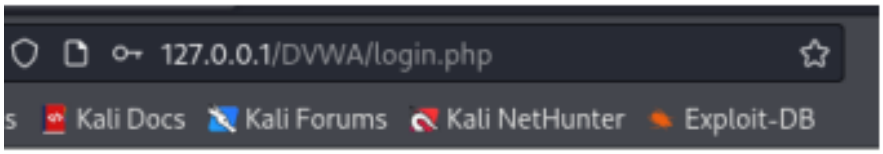
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

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

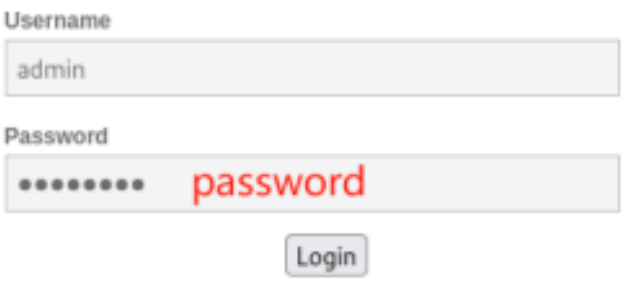
Per aiutarsi a trovarlo si può usare la funzione di nano CTRL+F per usare la funzione di ricerca. Per salvare CTRL+O invio e CTRL+X invio

5. Avviare il servizio, comando service apache2 start 6. Aprire un browser di Kali e scrivere l’indirizzo per il Setup del Web Server. Link http://127.0.0.1/DVWA/setup.php 7. Cliccate su «Create / Reset Database» nella parte bassa della pagina

Configurazione Web Server DVWA

Le credenziali di default sono admin e password.





Impostare la sicurezza di DVWA su livello basso dopodiché cercare Burpsuite tra le app di Kali ed avviare un “Temporary project in memory”. Nella sezione “Proxy” attivare “Intercept is on”, poi attivare il browser.

Nel browser di Burp Suite recarsi all’indirizzo http://127.0.0.1/DVWA/ ed effettuare anche in questo caso la modifica al livello di sicurezza su basso. Per caricare la pagina premere Forward su Burpsuit fintantoché il browser non carichi la pagina web.

Test con Burp e DVWA

Inserire una qualsiasi credenziale non corretta come in immagine e intercettarla con Burp. Premere Ctrl+R oppure tasto destro Send to Repeater per inviare alla sezione Repeater il cookie intercettato. Correggere la password con quella corretta “password” e inviare una richiesta al server. Se necessario premere Follow redirection, se il server lo prevedesse. L’esercizio si conclude con l’avvenuto login nel server tramite il cookie con la password corretta. Il tentativo di rubare la sessione tramite il cookie intercettato è riuscito.

Cosa abbiamo fatto nella pratica?

1 Inserimento delle credenziali non corrette:

- Viene inserita una combinazione di username e password errata nella pagina di login di DVWA. L'obiettivo è simulare un tentativo di accesso fallito.
  -

2 Intercettazione della richiesta HTTP:

- Utilizzando Burp Suite, si attiva l'intercettazione del traffico tra il browser e il server DVWA. Questo permette di catturare tutte le richieste HTTP inviate dal browser, inclusi i cookie, le credenziali, e altre informazioni sensibili.
- Quando viene inviata la richiesta di login, Burp Suite cattura il traffico, inclusa la richiesta con le credenziali errate e qualsiasi cookie associato alla sessione di quella richiesta.

3 Invio della richiesta a Burp Repeater:

Utilizzando la funzione "Send to Repeater" di Burp Suite, la richiesta intercettata viene inviata al modulo Repeater. Questo modulo consente di modificare e reinviare la richiesta quante volte si vuole, manipolando i dati per osservare le risposte del server.

4 Correzione della password:

All'interno del modulo Repeater, viene corretta la password nella richiesta HTTP, sostituendo quella errata con la password corretta, ad esempio "password". In questo modo si simula un tentativo di accesso fraudolento con credenziali corrette.

5 Inoltro della richiesta modificata:

- La richiesta modificata viene inviata nuovamente al server con Burp Suite. Se il server è configurato per gestire correttamente i reindirizzamenti, è possibile seguire questi reindirizzamenti utilizzando l'opzione "Follow redirection".
- Se tutto va a buon fine, si ottiene l'accesso al server come se il login fosse stato eseguito correttamente, anche se le credenziali originali inserite dall'utente nel browser erano errate.

Intercettazione del cookie

- Il cookie è un'informazione che il server invia al browser e che viene spesso utilizzata per gestire la sessione dell'utente. Durante il login, il server potrebbe generare un cookie di sessione che identifica in modo univoco l'utente e lo associa a una sessione specifica.
- In questo caso, Burp Suite ha intercettato il cookie associato alla richiesta di login errata.
- Manipolando i dati, come la password, e inviando nuovamente la richiesta con il cookie originale, è possibile ottenere l'accesso alla sessione dell'utente come se il login fosse stato eseguito correttamente.

Come si riferisce al furto di cookie nella vita reale:

- Il furto di cookie (cookie hijacking) è una tecnica utilizzata dagli attaccanti per rubare i cookie di sessione di un utente, che permettono di autenticarsi senza dover reinserire le credenziali. Un attaccante potrebbe intercettare i cookie attraverso diversi metodi, come:
- Man-in-the-middle attack: L'attaccante intercetta il traffico tra il browser dell'utente e il server, proprio come viene fatto con Burp Suite.
- XSS (Cross-Site Scripting): L'attaccante inietta uno script dannoso in una pagina web vulnerabile che ruba i cookie della vittima.

- Una volta ottenuto il cookie di sessione, l'attaccante può usarlo per accedere all'account della vittima senza conoscere le credenziali, fintanto che la sessione è valida.
- L'esercizio mostra quanto sia vulnerabile una sessione se un attaccante riesce a intercettare il traffico o ottenere i cookie, il che rende fondamentale implementare misure di sicurezza come HTTPS, SameSite cookie policy, e tecniche di validazione lato server per proteggere le sessioni degli utenti.

GRAZIE