Esercizio Barpsuite

Data 06/12/23

Guglielmo Carratello

L'obiettivo di oggi consiste nella configurazione di DVWA (Damn Vulnerable Web Application) su Kali Linux.

Configurazione di DVWA:

-Clonazione del repository DVWA:

Nel terminale di Kali, abbiamo eseguito i comandi "cd /var/www/html" per raggiungere la cartella html, clonare il repository DVWA con il comando " git clone https://github.com/digininja/DVWA" e impostare i permessi correttamente con "chmod –R 777 DVWA/".

-Configurazione di MySQL:

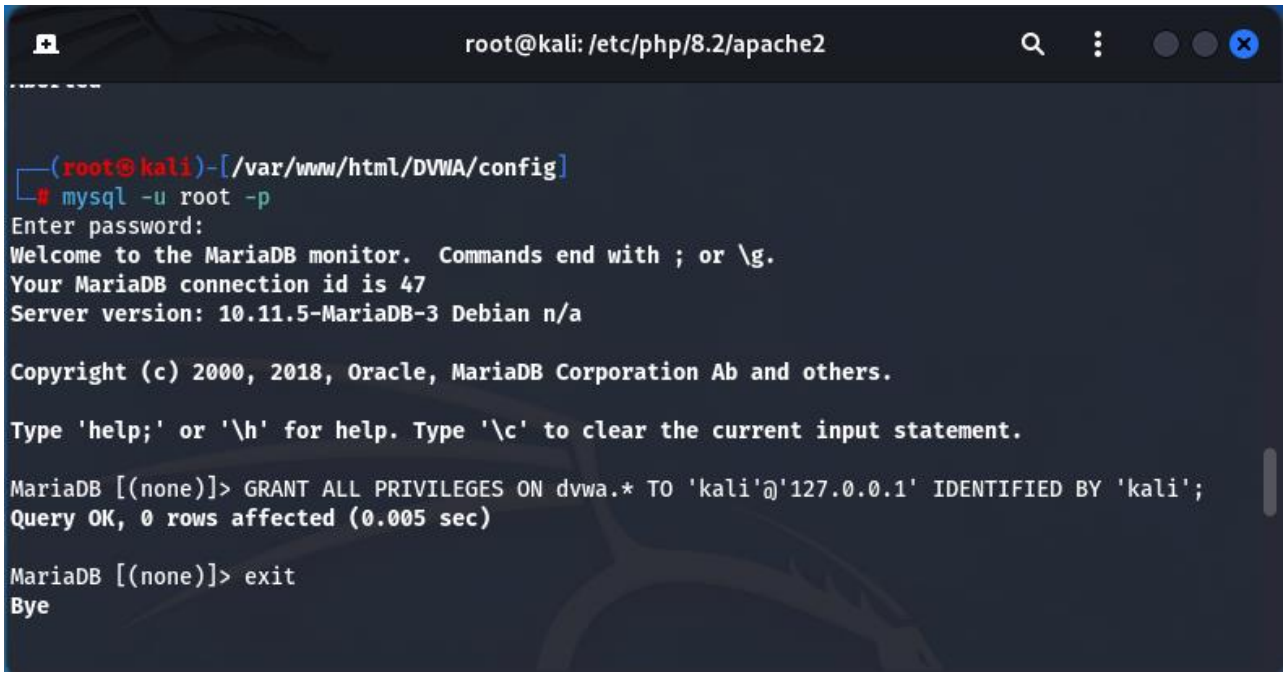
Successivamente, abbiamo configurato il servizio MySQL, modificando il file di configurazione e creando un nuovo utente. Abbiamo raggiungo la cartella DVWA con il comando "cd DVWA/config", copiato il file .config che dobbiamo modificare ed infine modificato con il comando "nano config.inc.php". In questo file modifichiamo le credenziali standard con id:kali e psw: kali utilizzate per l'avvio di mysql.

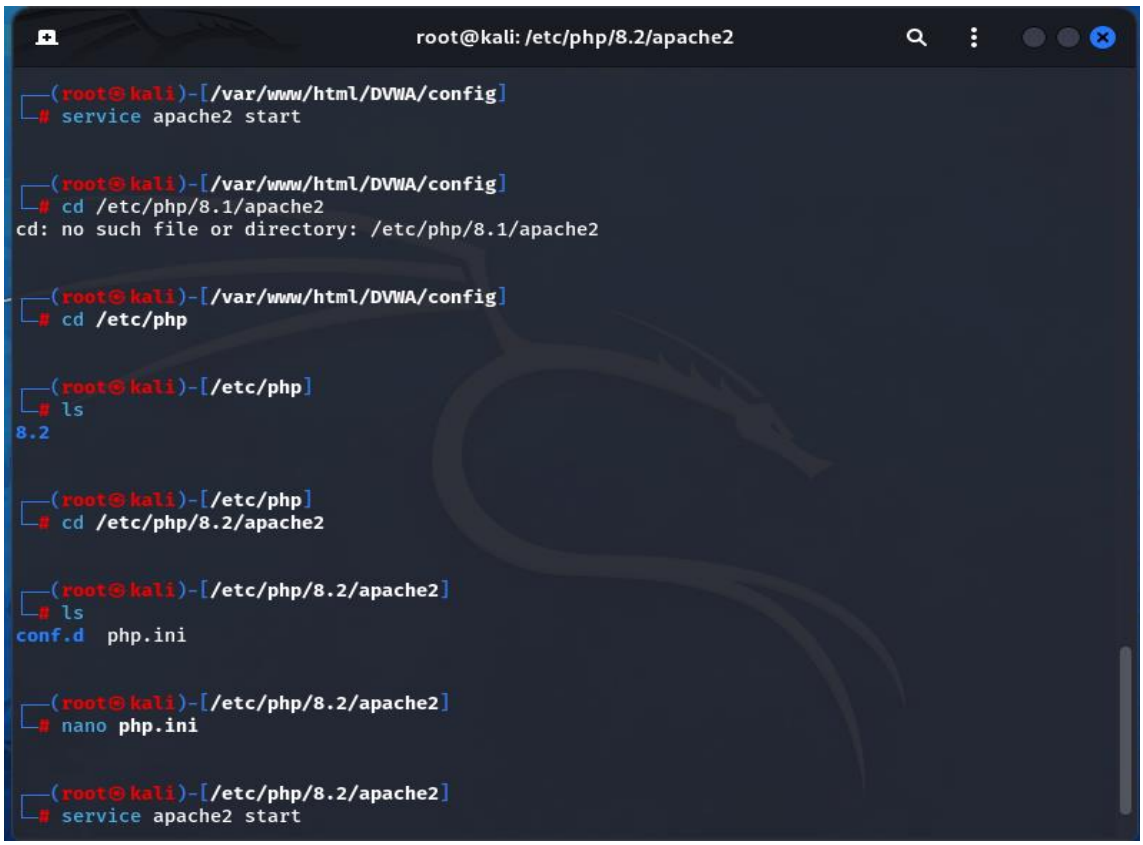
-Configurazione di Apache:

Abbiamo avviato il servizio Apache e navigato nella directory di configurazione di PHP andando a cercare prima la cartella corrispondente in questo caso l'8.2 (è riferita alla versione) e successivamente modificato il file php.ini con il comando di editor nano. Abbiamo impostato su "On" i due servivi allow_url_fopen e allow_url_include.

-Inizializzazione di DVWA:

Infine, abbiamo aperto una sessione del browser e visitato 127.0.0.1/DVWA/setup.php per inizializzare il database e configurare DVWA impostando la sicurezza del database su low ovvero la più bassa.





Pratica con Burpsuite:

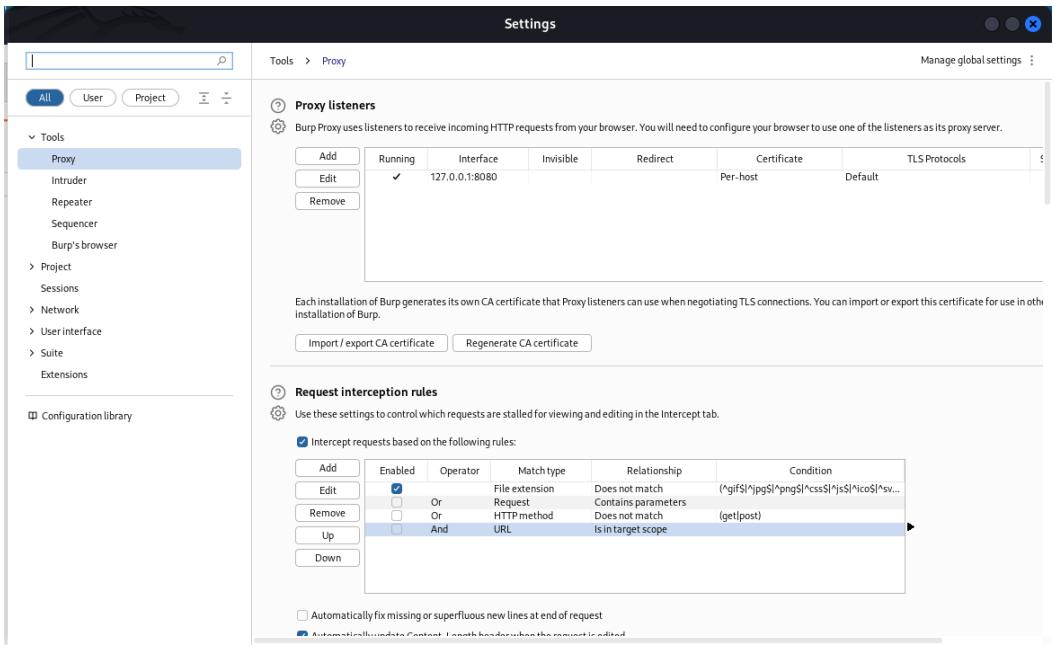
Dopo aver configurato DVWA, ci siamo concentrati su un'esercitazione pratica con Burpsuite.

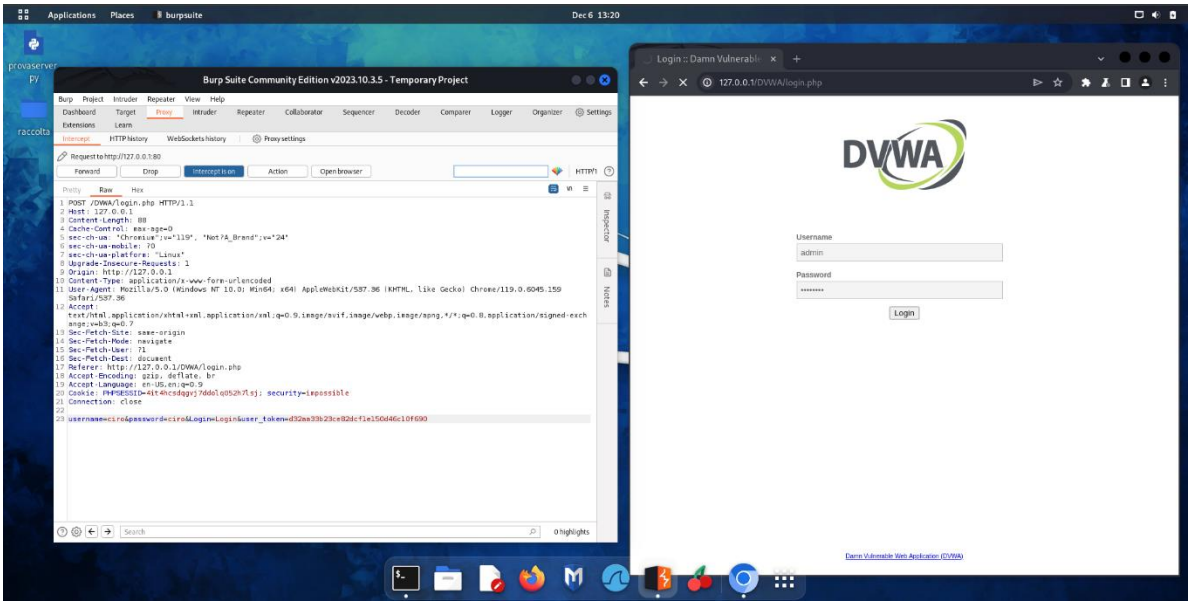
Abbiamo lanciato Burpsuite, creato un progetto temporaneo e aperto un browser per accedere a DVWA.

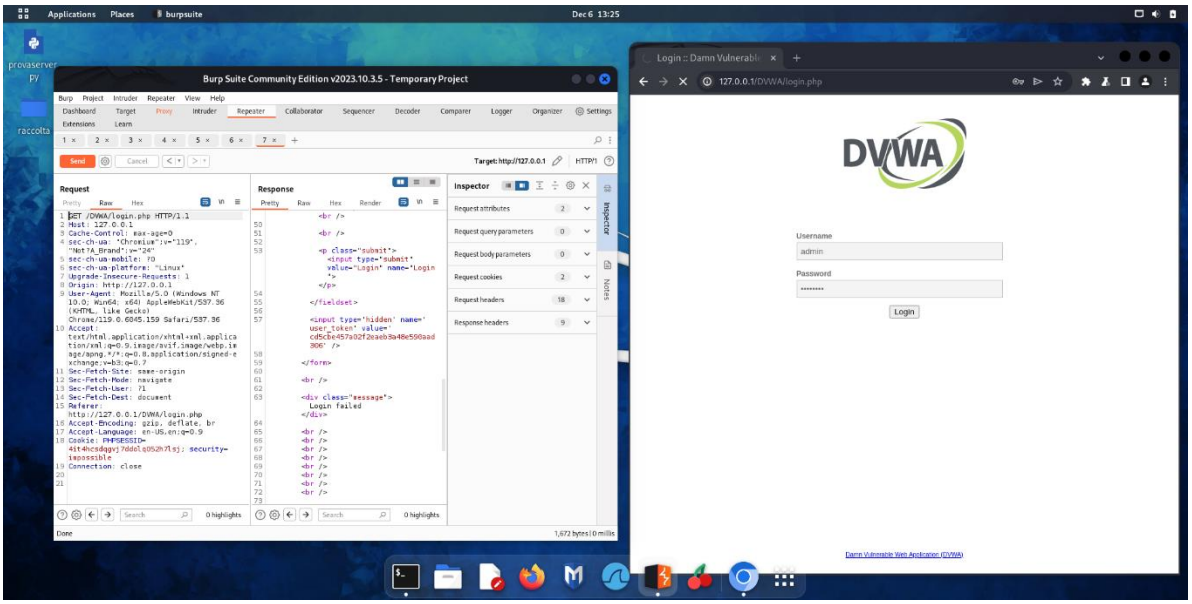
Con Burpsuite, abbiamo intercettato una richiesta di login e ne abbiamo esaminato i parametri.

Modificando i campi delle credenziali prima di inviare la richiesta, abbiamo dimostrato come sia possibile alterare i dati inviati all'applicazione. Abbiamo sostituito le credenziali di accesso fornite dal programma ovvero id: admin e psw: password con ciro sia per l'id che per la password.

Da notare come una volta sostituiti ed inviato la richiesta al repeater e mandata nuovamente tra i messaggi di risposta della pagina viene visualizzato "Login failed".






Applications
Places
burpsuite
Dec 6 13:25
provaserver FV
raccolta
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Request
Response
Inspector
Login :: Damn Vulnerable
127.0.0.1/DVWA/login.php
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)