S6 LEZIONE 5

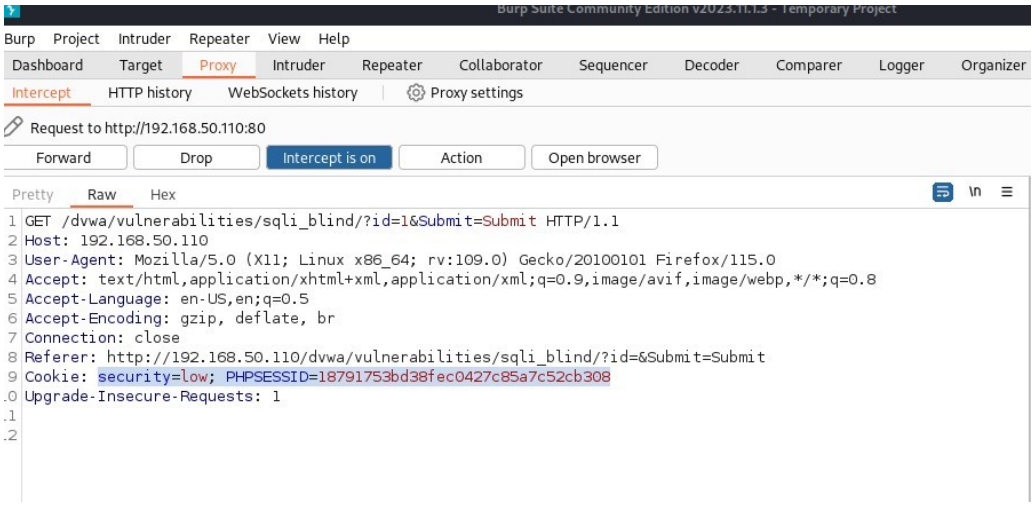
Traccia:
Nell’esercizio di oggi, viene richiesto di exploitare le vulnerabilità:
-SQL injection (blind).
-XSS stored.
Presenti sull’applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=LOW.

Scopo dell’esercizio:
-Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).
-Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell’attaccante.

SQL injection (blind):

Lo scopo è recuperare le password presenti sul database dvwa attraverso sql injection, per fare ciò mi sono servito del tool **sqlmap** presente su kali linux.

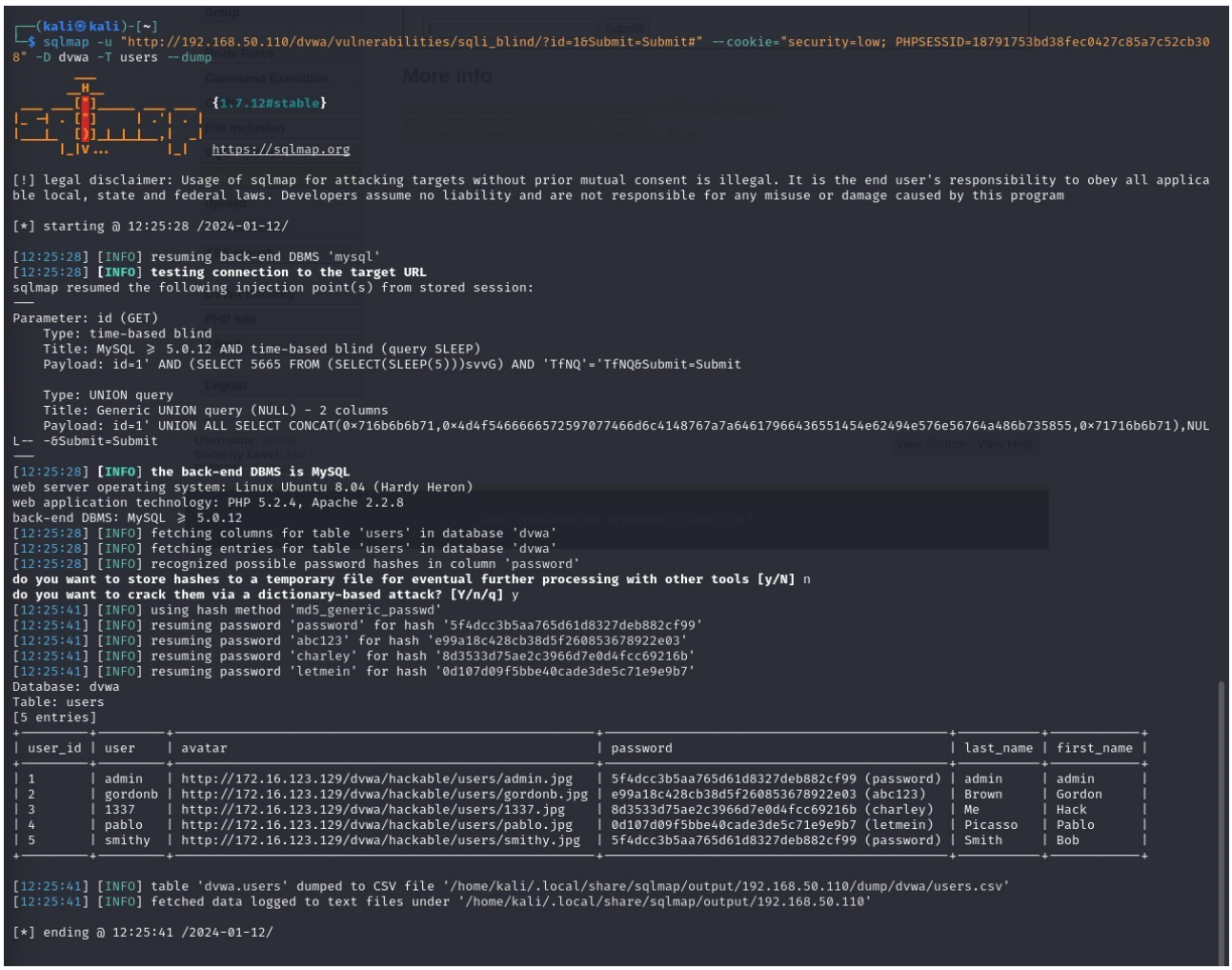
Prima di tutto viene fatta una scansione con burpsuite per scovare il livello di sicurezza del sito e il SESSID da attaccare.



Dopodiché sapendo che il database è dvwa, con il comando

sqlmap -u *<indirizzo><cookie>* **-d dvwa –tables –columns**

si può capire la struttura del database, subito salta all’occhio la tabella **users;**
qui sono presenti sia gli user che le password per accedere al sito. Sarà li che punteremo il nostro attacco.

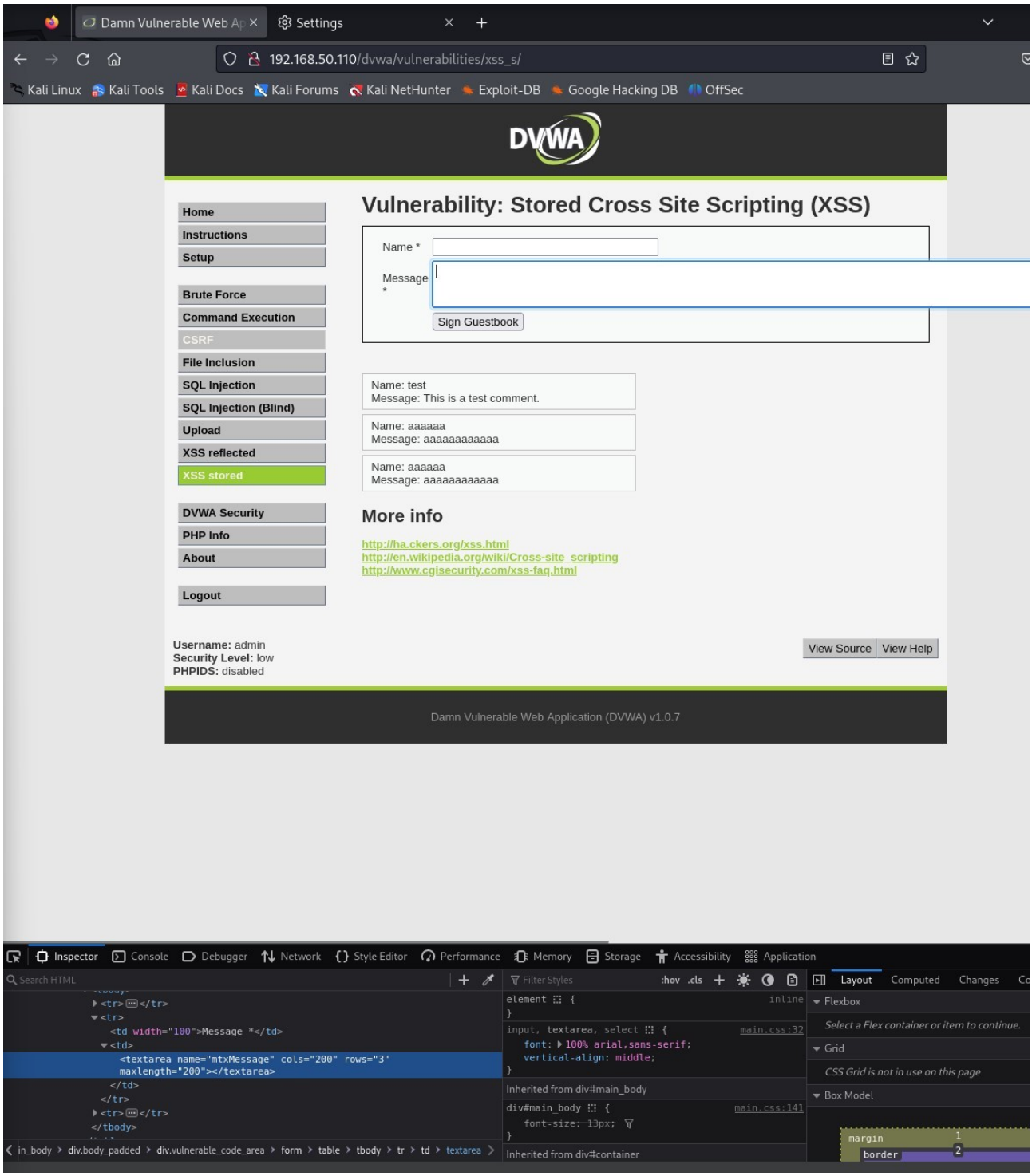


con il comando sopra è possibile scoprire le password crittografate on hash per ogni user e con un attacco a dizionario è possibile decrittarle e scoprire le password reali collegate ad ogni user (es: admin , password).

XSS (stored)

Lo scopo di questo attacco è recuperare i cookie di sessione ed inviarli ad un server sotto il nostro controllo.

Per prima cosa nel capo messaggio aggiorniamo la lunghezza massima di caratteri da “50” a “200” per poter eseguire lo script:



Ora con il comando **python -m http.server 1337** si va a creare un server python dove sarà possibile visualizzare i cookie di sessione delle vittime.

Spostandoci sulla pagina di dvwa andiamo a scrivere lo script che ci permetterà di visualizzare il cookie di sessione della vittima