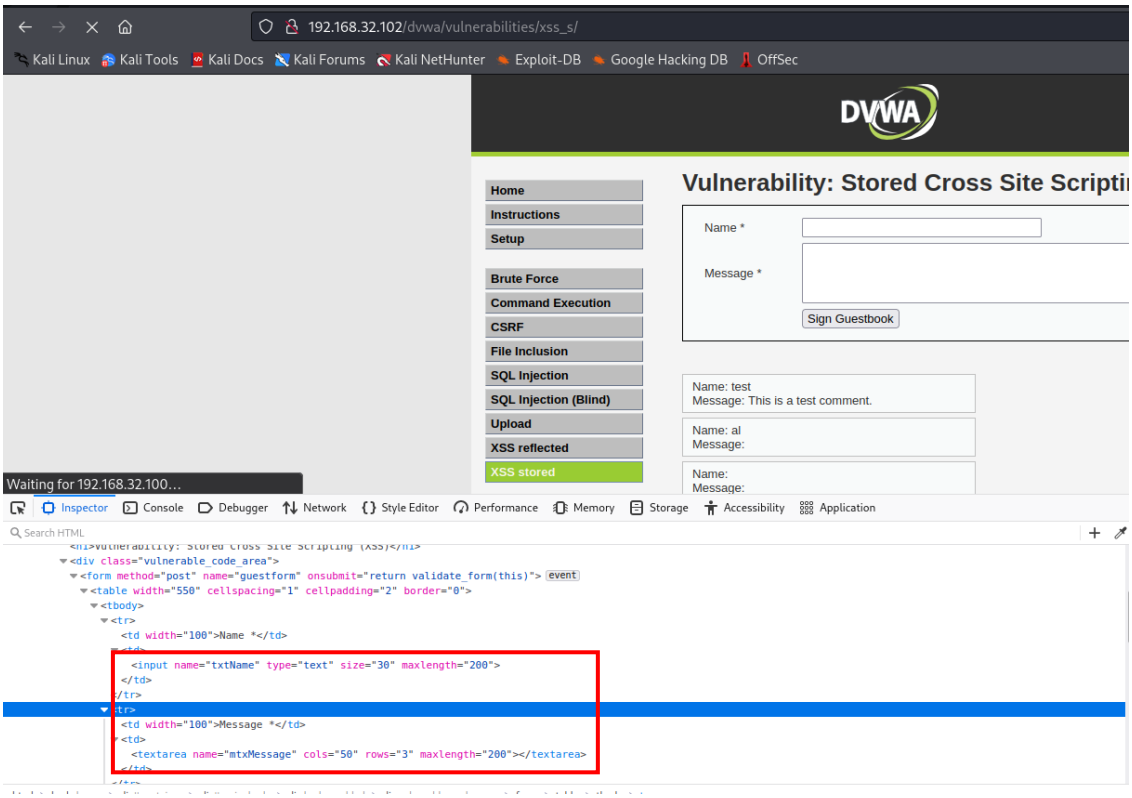
EXPLOIT VULNERABILITA' DVWA

Nell'esercizio di oggi andremo a sfruttare le vulnerabilità del DVWA della macchina Metasploitable; in particolare andremo a fare attacchi di Cross site scripting e SQL injection.

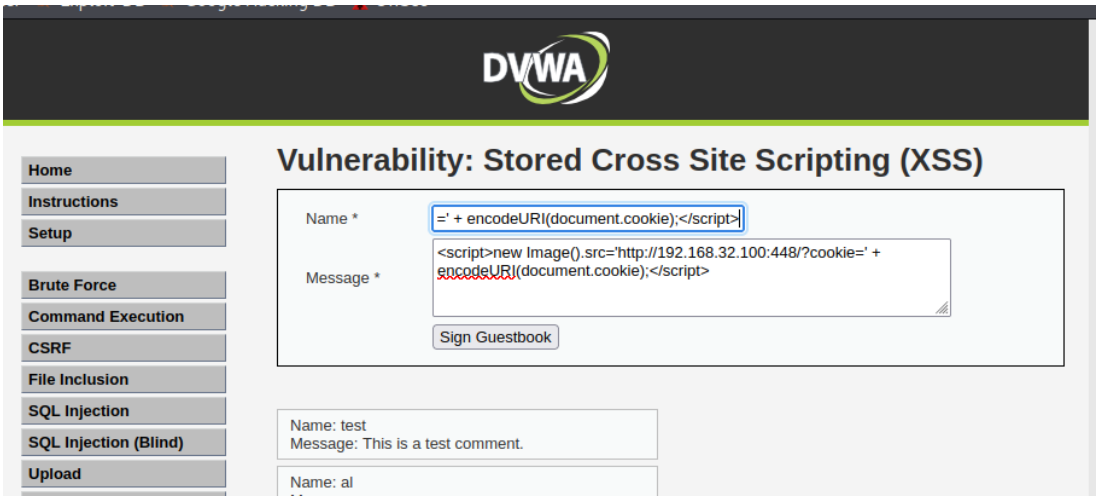
Per prima cosa andiamo a provare un attacco di Cross Site Scripting, che consiste nell'iniettare dello script malevolo nel campo dell'input utente con lo scopo di prendere possesso della web app; quello che andremo a fare noi sarà di tipo stored, cioè l'injection di codice malevolo nel sito web che agisce in maniera persistente e che viene quindi attivato quando un web browser avvia la pagina infettata

Effettuiamo il login sul DVWA di Metasploitable, impostiamo la sicurezza su "low" come richiestoci, e nel menù laterale clicchiamo su "XSS stored":

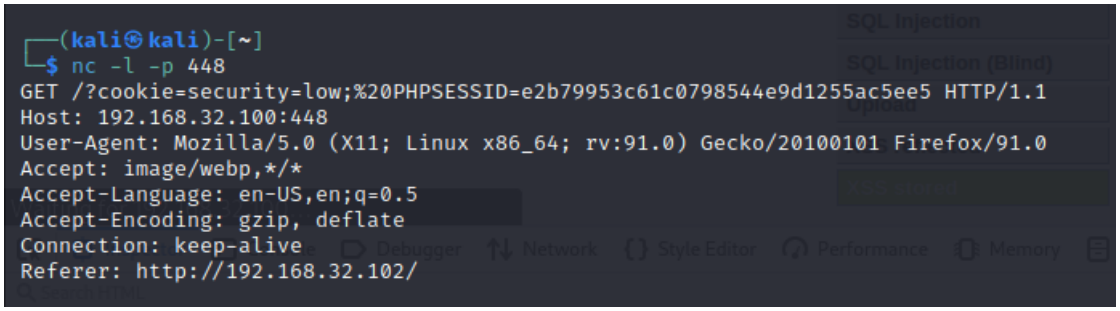


Per inserire lo script che a me serviva, ho dovuto modificare il campo max length, come mostrato sopra;

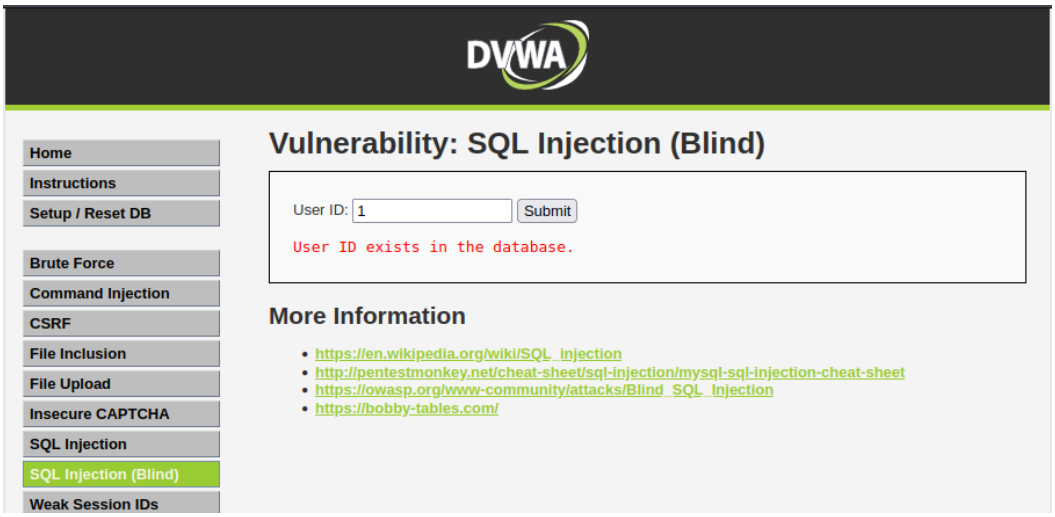
Dopodiché ho iniettato il codice che mi servirà per inviare il cookie di sessione al mio web server, che in questo caso è Kali 192.168.32.100:

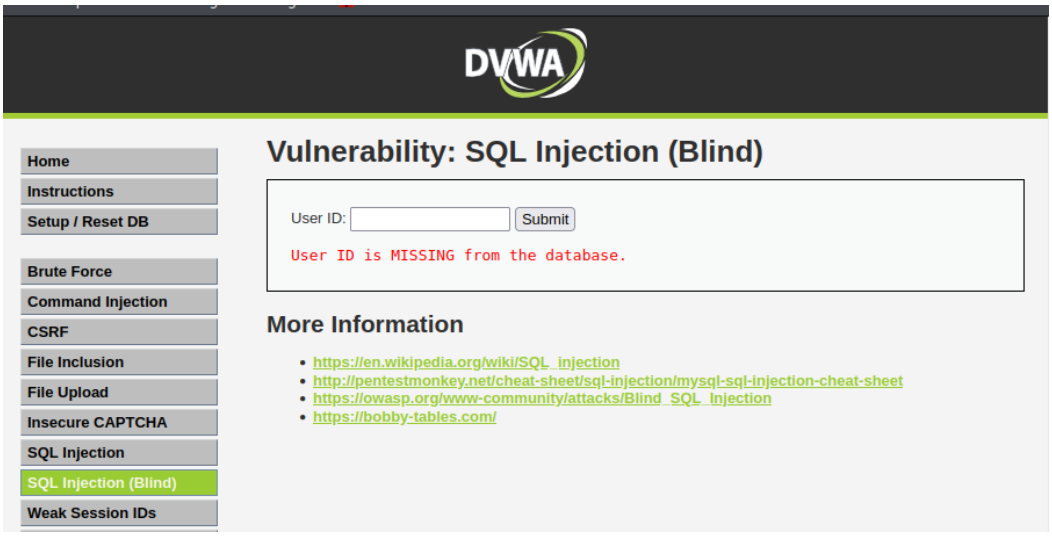


Nell'immagine in basso possiamo vedere che, mettendoci in ascolto sulla porta scelta con netcat, riceviamo il cookie sul nostro pc:



Per quanto riguarda l'altro attacco richiesto, il SQL injection blind, ho riscontrato che c'è un errore di programmazione sul server Metasploitable in quanto inserendo in input un qualsiasi comando SQL, il messaggio in rosso appare uguale a quello non blind, appaiono quindi in chiaro gli username e gli hash delle password; l'attacco l'ho fatto sul localhost di Kali (127.0.0.1); provando ad inserire un comando qualsiasi all'interno dell'input, compaiono solamente i messaggi "User ID exists in the database" e "User ID is MISSING from the database", cioè ci appare se il record è esistente o meno nel database:





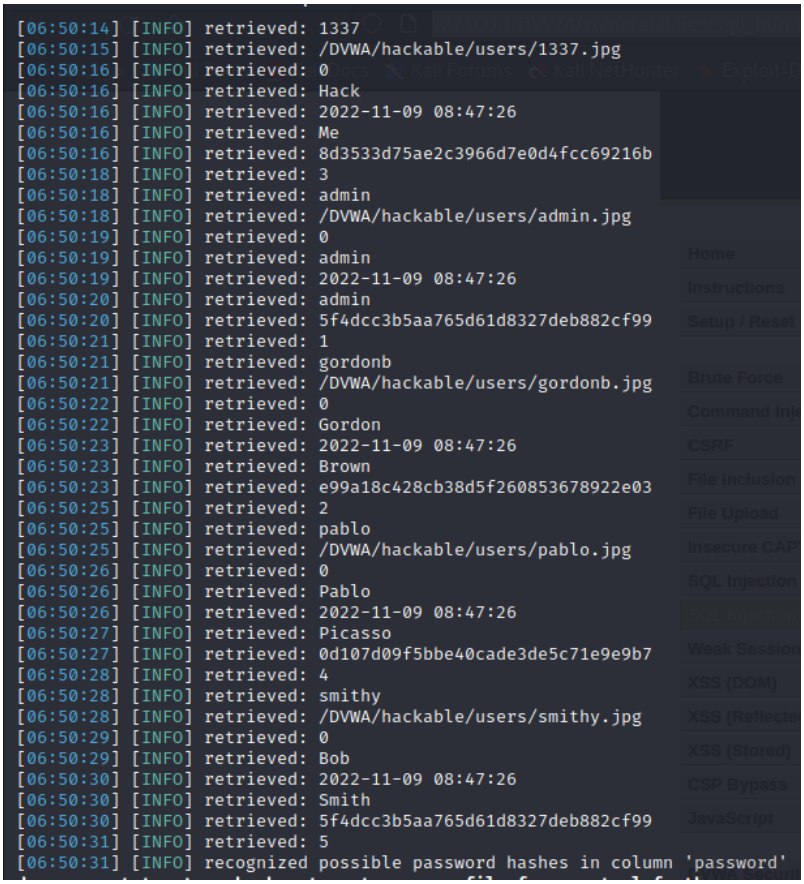
Per riuscire a carpire le informazioni che vogliamo, le password degli utenti in chiaro, usiamo sqlmap, un tool che ci permette di automatizzare il rilevamento e lo sfruttamento di difetti nella SQL injection e di prendere il controllo del server DBMS.

Lanciamolo dal terminale di Kali con il comando:

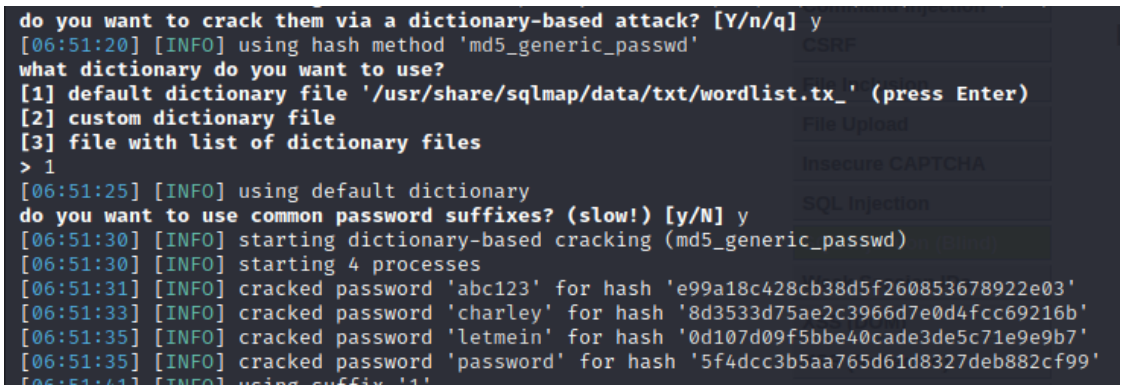
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u 'http://127.0.0.1/DVWA/vulnerabilities/sqli_blind/?id=1&Submit=Submit' -cookie="security=low; PHPSESSID=8sl7subpppt0v42ua1a4meq5g9" --dump
```

N.B.: il cookie di sessione l’abbiamo recuperato tramite un attacco XSS reflected

Qui possiamo già vedere tra le info che ha trovato i nomi utenti e gli hash delle password:



Lo stesso sqlmap ci chiede se vogliamo crackare gli hash attraverso un attacco a dizionario, diciamogli di sì e avremo le password in chiaro:



Effettuando poi il login con, ad esempio, Pablo e la relativa password “letmein”, possiamo vedere nell’immagine sotto che siamo entrati come l’utente scelto: