Simulazione 09/06

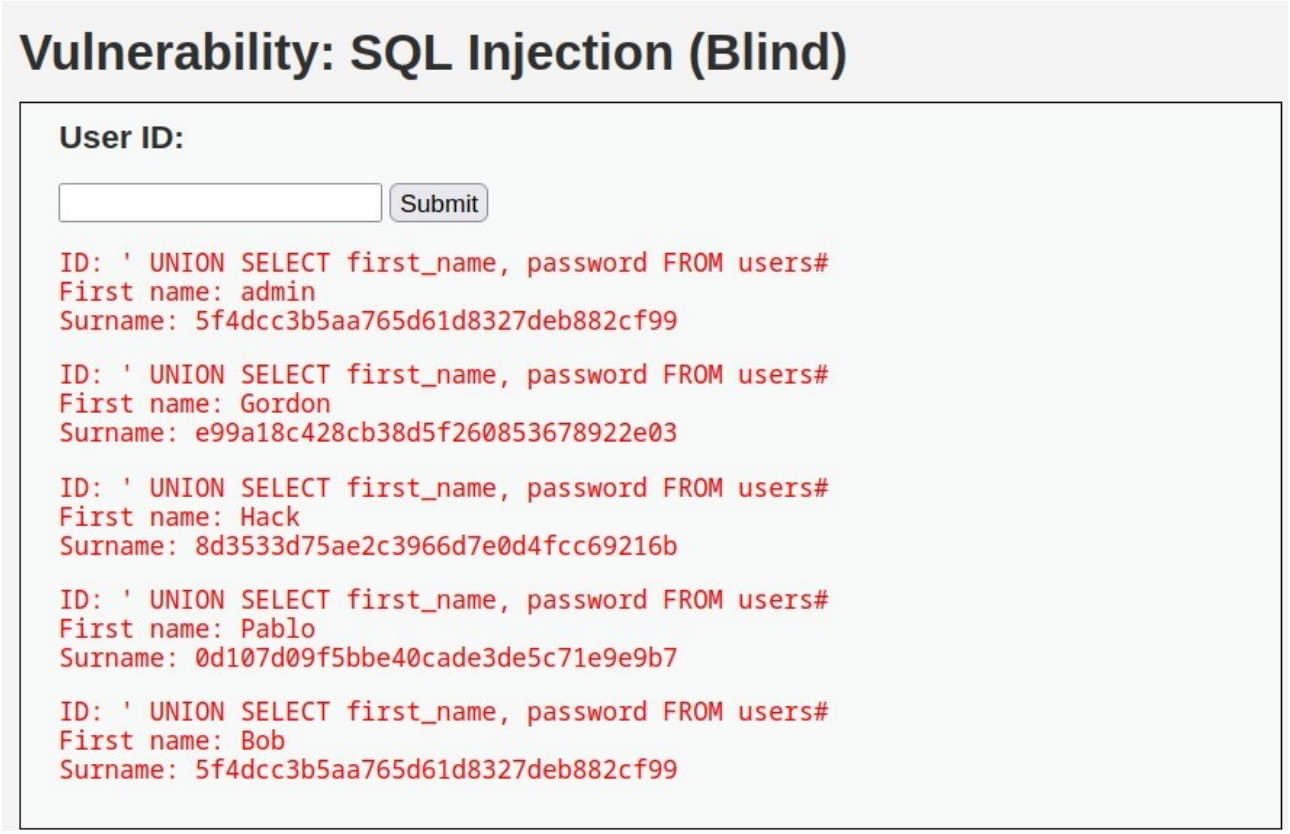
Nella simulazione di oggi andremo a simulare sulla nostra web app DVWA con gli attacchi:

SQL Injection (blind)

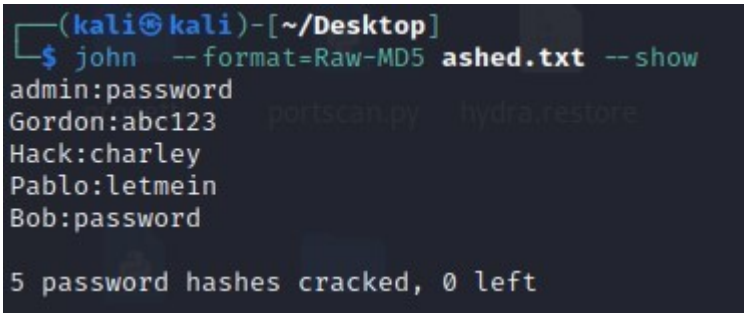
XSS stored (persistente)

SQL Injection (Blind)

Dentro a DVWA siamo andati nella categoria SQL Injection (blind),dove con la nostra query nell'immagine abbiamo ottenuto gli hash degli utenti.
A differenza di un SQL Injection tradizionale ,la variante blind non invia messaggi di errore e di conseguenza non mostra la presenza di vulnerabilità.

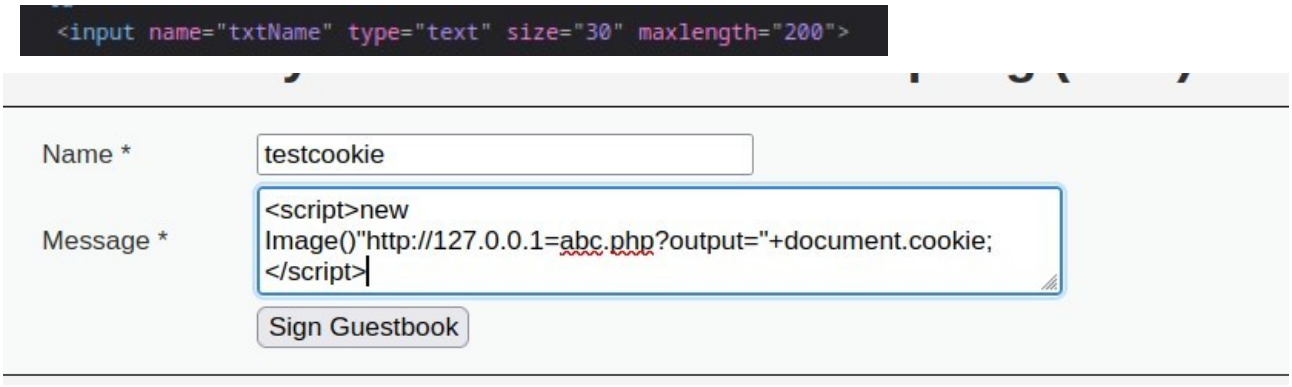


Successivamente da terminale grazie a JTR abbiamo ottenuto le password dei nostri utenti dopo averle trascritte nel file che vediamo dentro all'immagine.

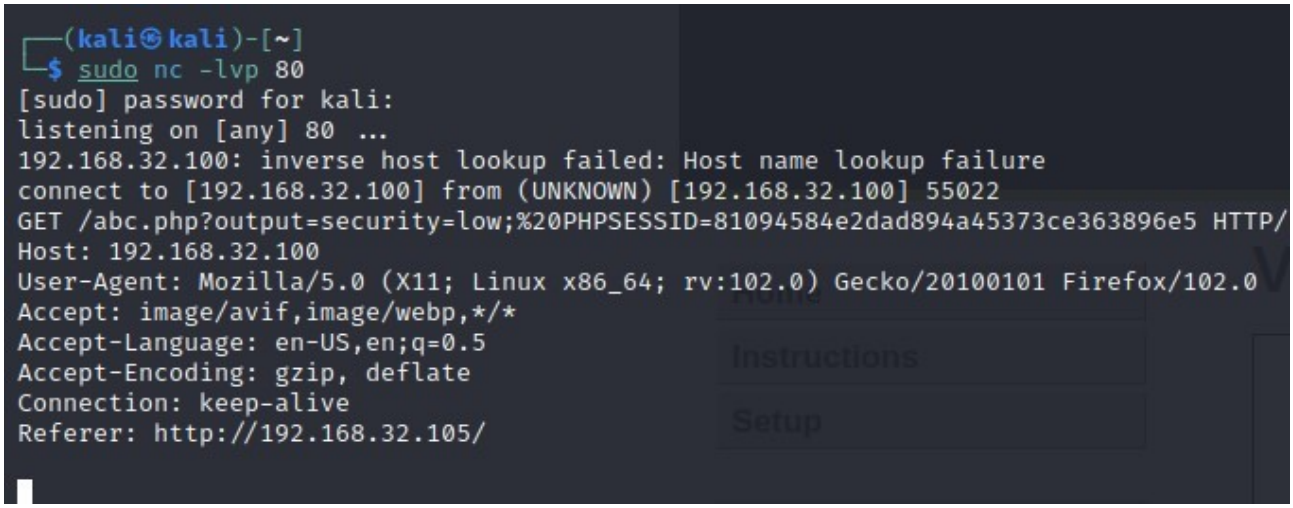


XSS Stored

Per quanto riguarda XSS Stored abbiamo inserito la query che vediamo nell'immagine modificando la quantità massima di caratteri,prima impostata su 50 e abbiamo inserito un max lenght 200.

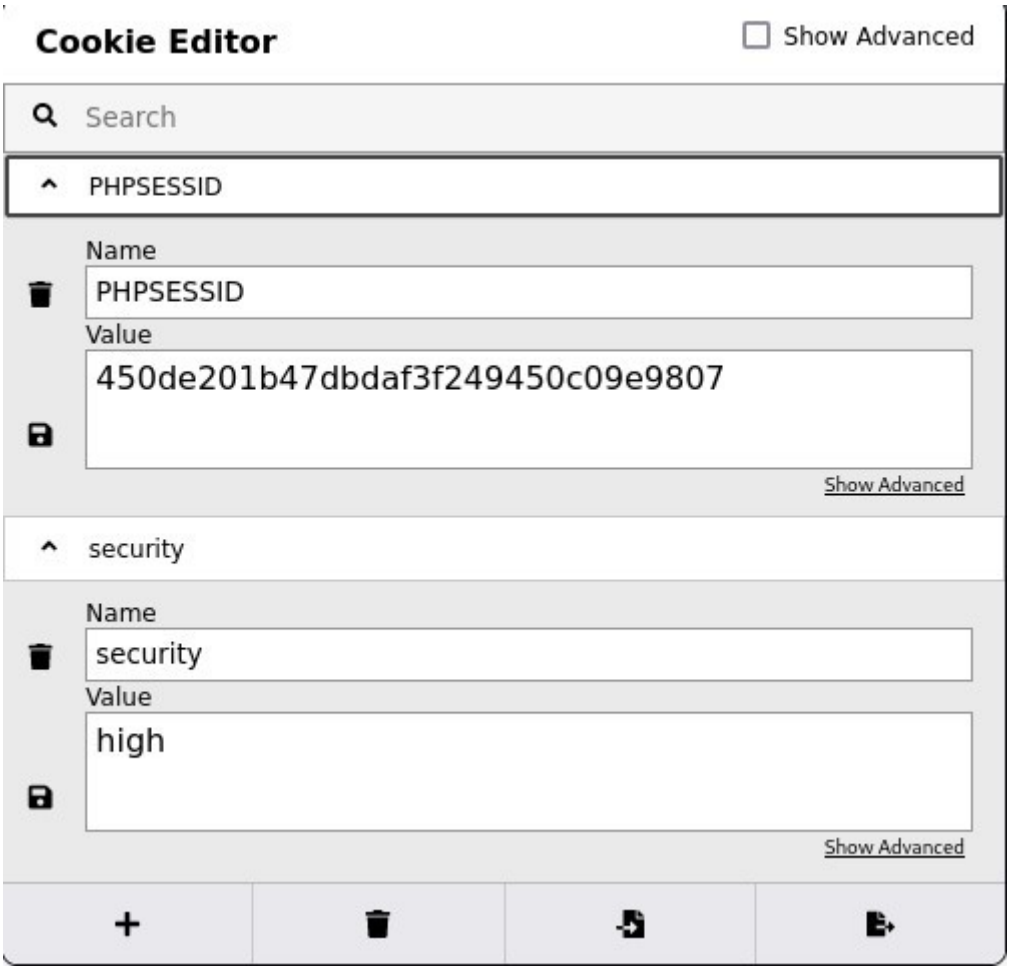


da terminale abbiamo avviato netcat e messo in ascolto sulla porta 80 ottenendo il nostro PHPSESSID,dentro DVWA abbiamo impostato una security low.

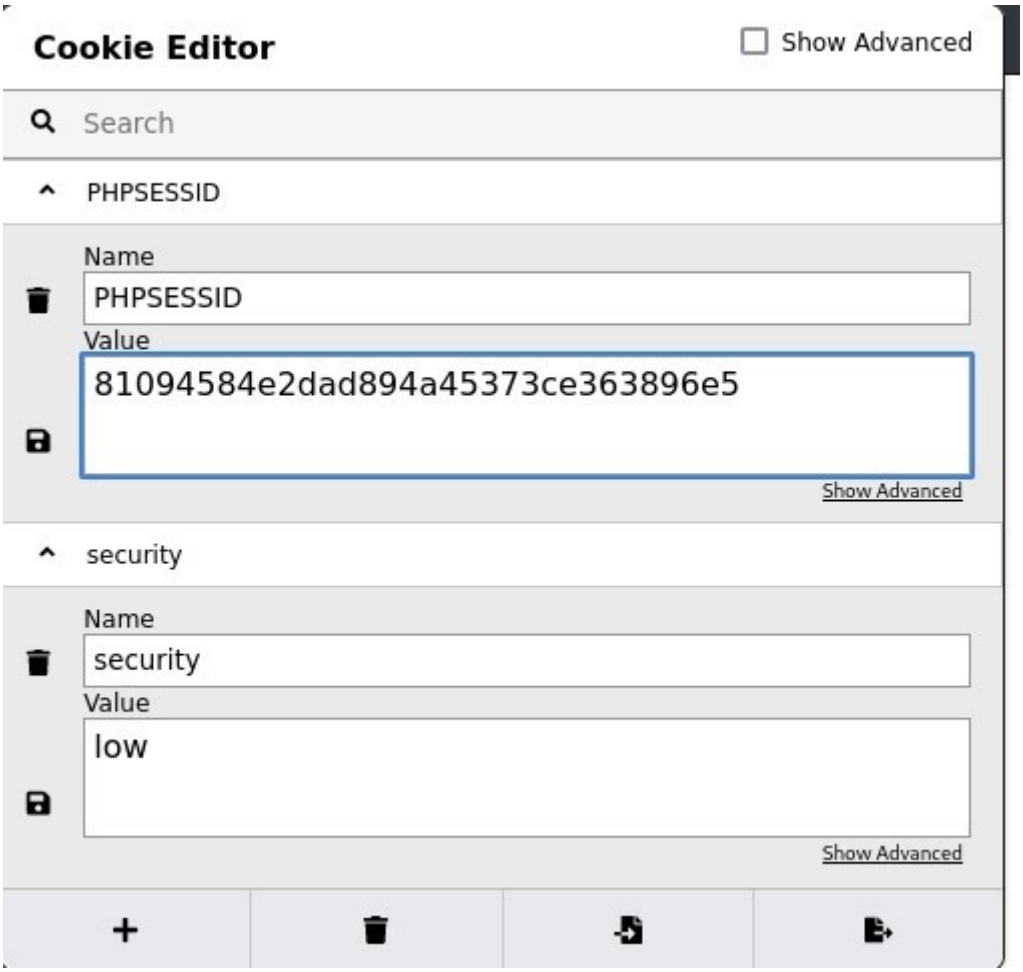


Successivamente abbiamo scaricato l'estensione di Firefox ,Cookie Manager impostando una security low e il cookie dello sniff di netcat precedentemente ottenuto.

Cookie prima della modifica



Cookie post modifica



Grazie al cookie ottenuto riusciamo ad entrare dentro DVWA senza che ci richieda login rubando di fatto la sessione.