**PRATICA 05 NOVEMBRE 2024**

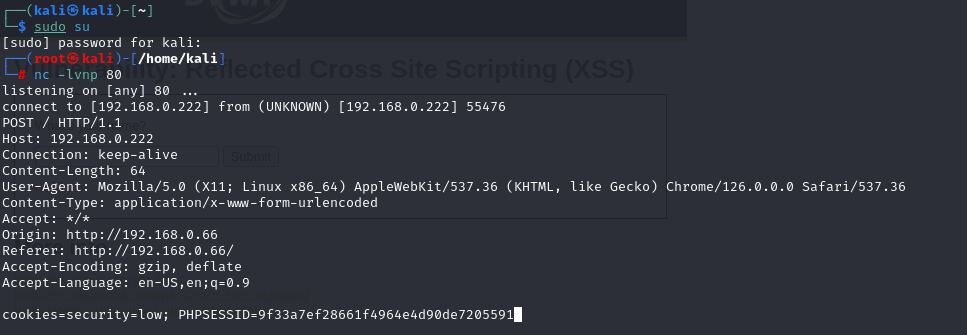
**Exploit DVWA - XSS e SQL injection**

Gli obiettivi di oggi consistono nell’usare una vulnerabilità XSS Reflected e SQL Injection per rubare il cookie di sessione della vittima (con XSS) e rubare i dati dal database (con SQL Injection).

**XSS REFLECTED**

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamentePer prima cosa bisogna utilizzare netcat per mettere in ascolto tutti i movimenti sulla porta 80. Una volta fatto ciò, si procede ad effettuare il login sulla DVWA e selezionare l’opzione XSS Reflected, dove andremo ad inserire il nostro script malevolo che andrà a rubare il cookie della sessione.

Una volta cliccato Submit netcat intercetterà l’operazione, rubando di conseguenza il cookie della sessione attiva.  


**SQL INJECTION**

Con questa tipologia di attacco, ormai obsoleto, andremo a estrapolare i dati degli utenti dal database di DVWA. Utilizzeremo un script in SQL per ottenere il risultato desiderato.  
  
Lo script che utilizzeremo sarà:   
  
**%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password)**

**from users #**

Di seguito il risultato dell’operazione:



Come da immagine, tramite lo script SQL abbiamo estrapolato i dati sensibili di tutti gli utenti registrati sul database.   
  
**Conclusione**

Difendersi contro questi attacchi è essenziale per garantire la sicurezza e l'integrità delle applicazioni e dei dati. L’implementazione di pratiche di sicurezza, come la convalida dell'input oltre a una revisione regolare della sicurezza del codice, rappresentano strategie efficaci per limitare i rischi. Una solida difesa contro le vulnerabilità XSS e SQL Injection non solo protegge i dati degli utenti, ma rafforza anche la fiducia verso l’applicazione e l’azienda stessa.