S6/L2

Nell'esercizio di oggi ci viene chiesto di raggiungere la DVWA e settare il livello di sicurezza a «LOW». Scegliere una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

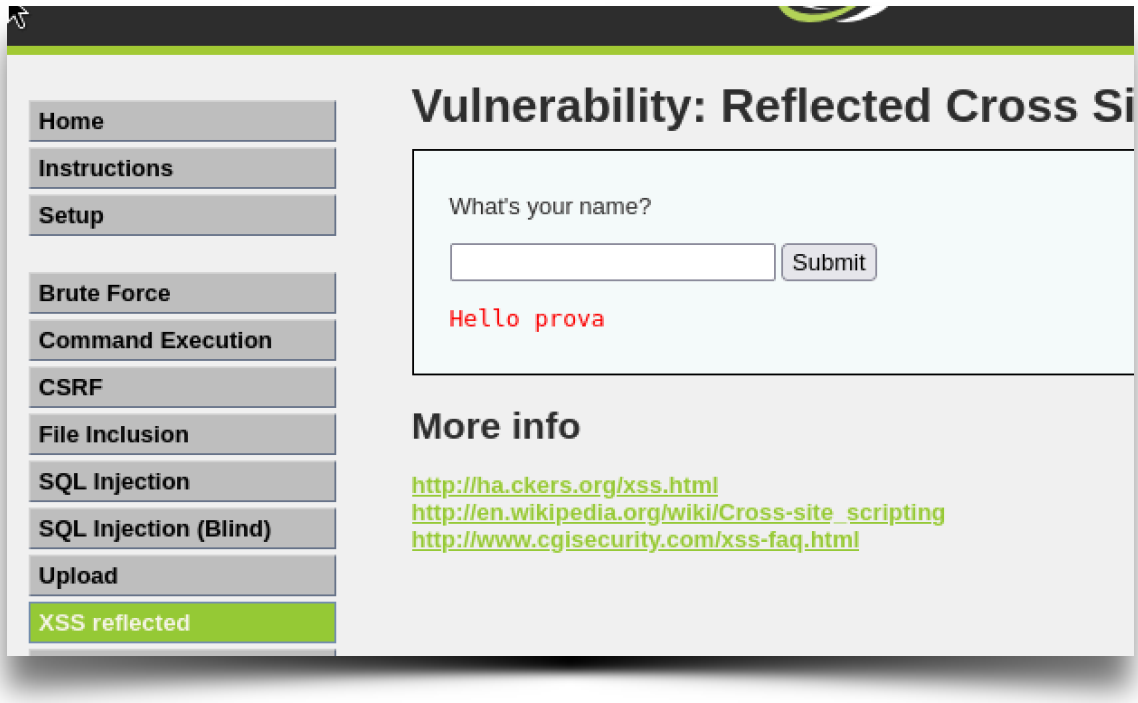
La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

- XSS reflected.
- SQL Injection (non blind).

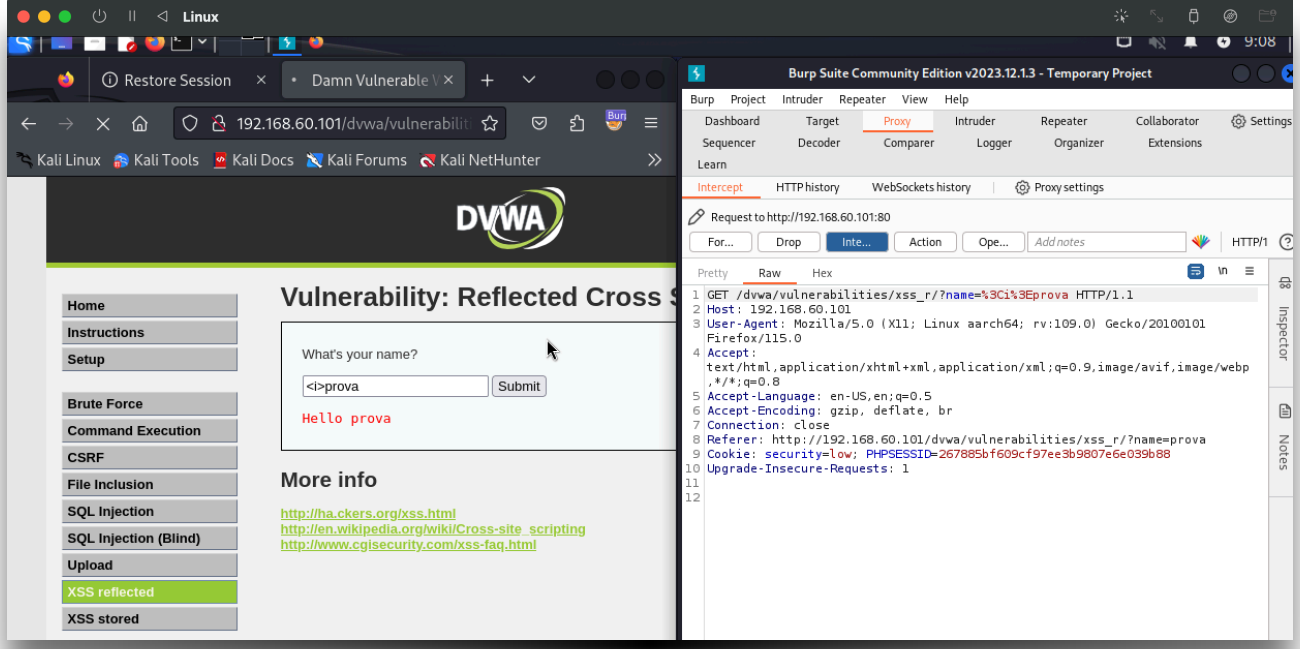
XSS reflected

Il Cross-Site Scripting (XSS) reflected è una vulnerabilità web in cui script dannosi vendono iniettati in un sito web e poi riflessi agli utenti. Questo accade quanto l'input dell'utente non viene adeguatamente sanificato (nel senso che le informazioni fornite dall'utente non vengono filtrate correttamente prima di essere utilizzate).

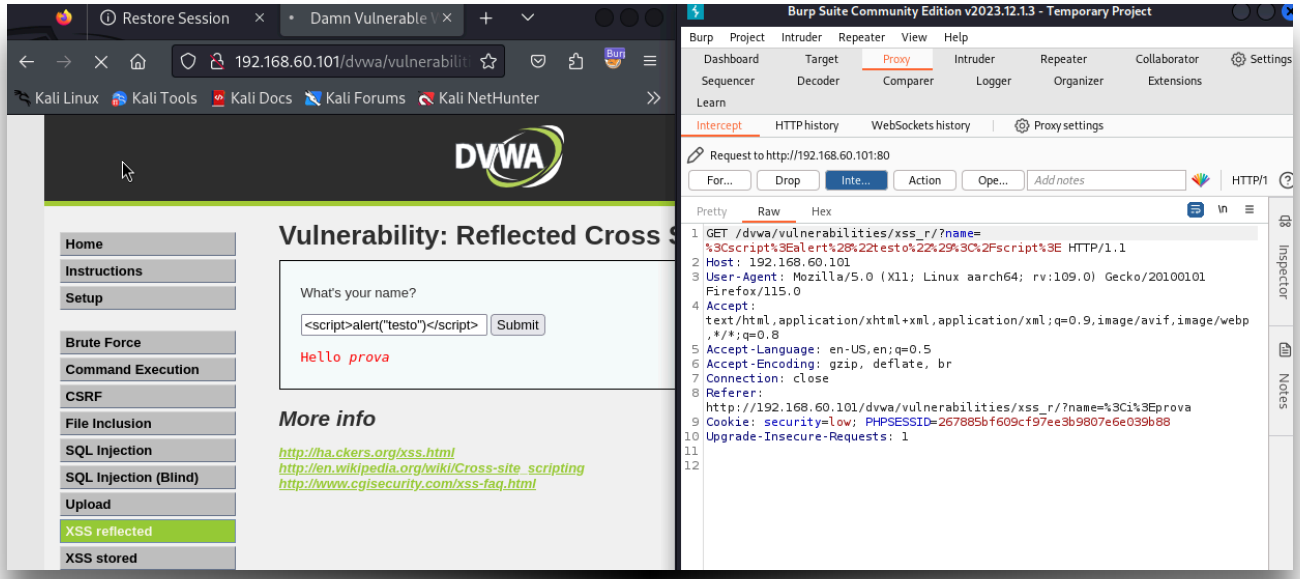
Eseguendo alcune prove si può notare che questa vulnerabilità è presente

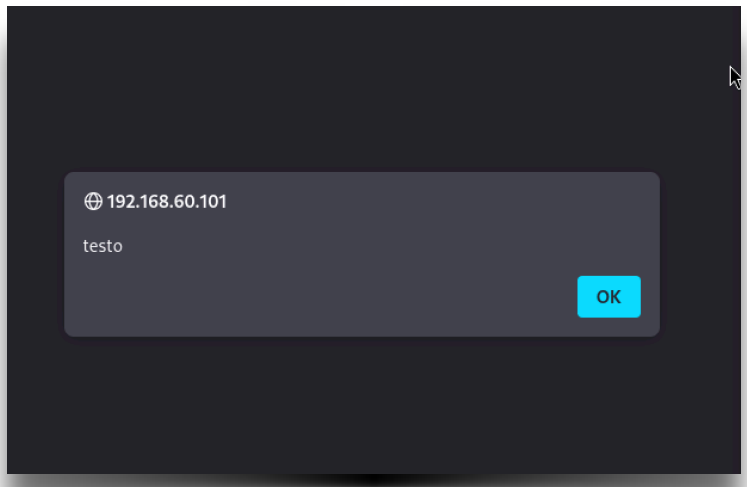


Inserendo un tag HTML si può notare che l'output viene modificato ciò vuol dire che i tag HTML vengono eseguiti



Lo stesso inserendo il codice Javascript *<script>alert("testo")</script>*. Come si può notare anche questo codice viene eseguito aprendo una finestra pop-up

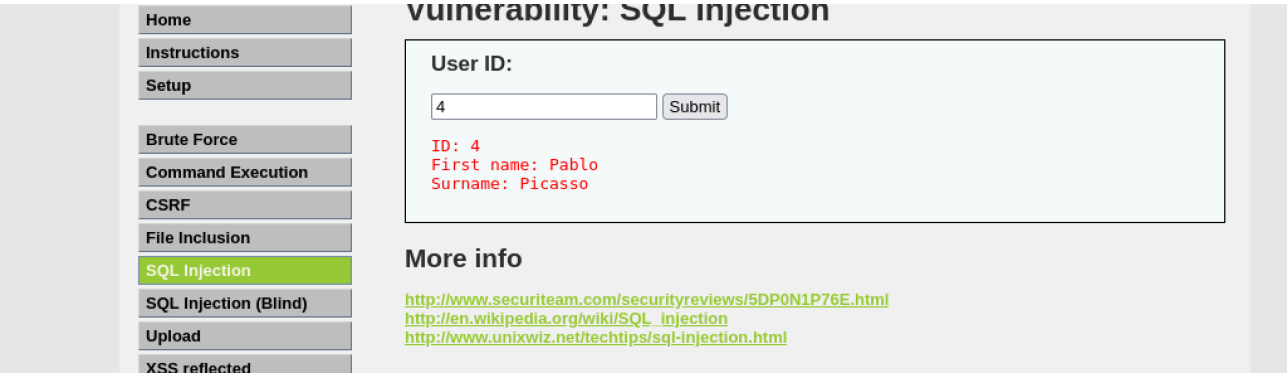




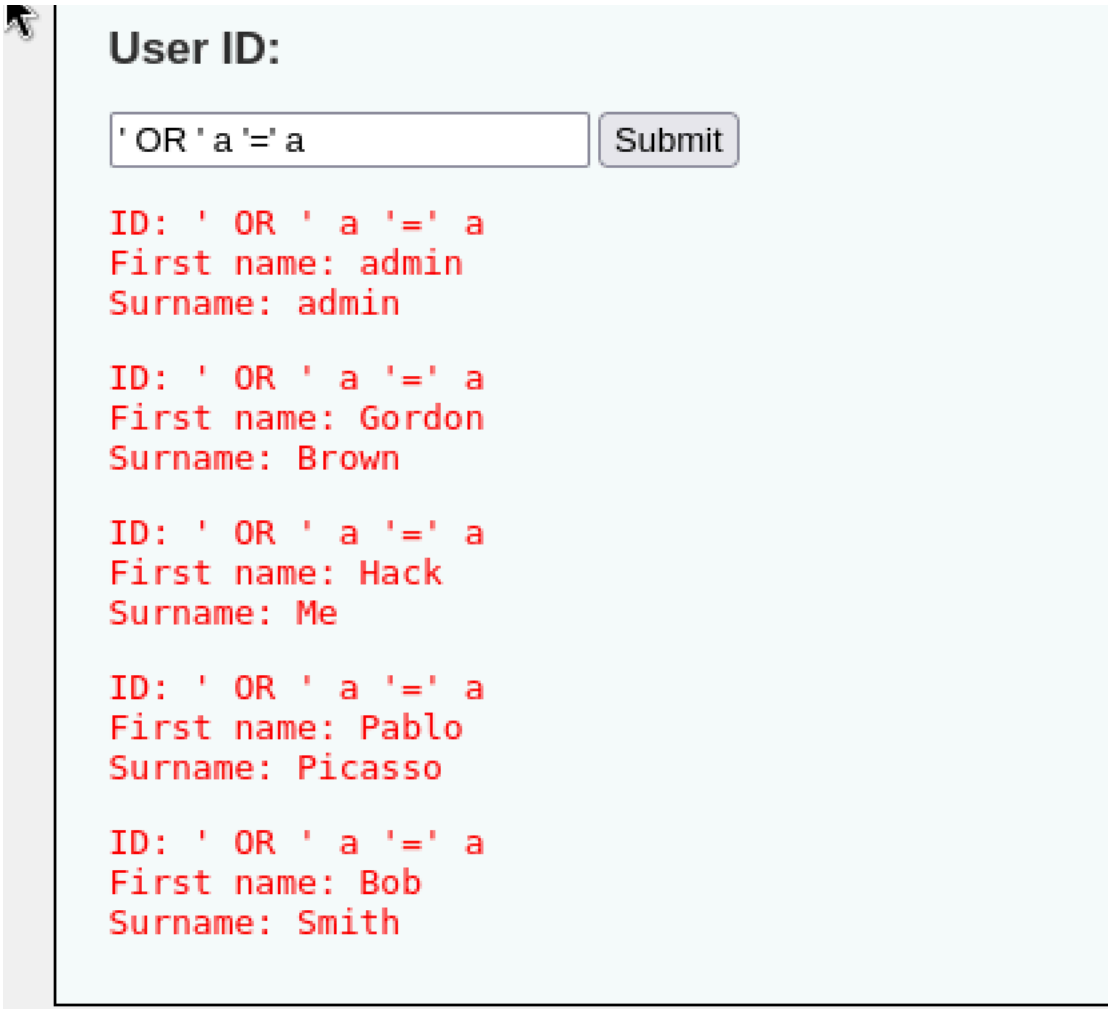
Questo consente all'attaccante di poter inserire ed eseguire uno script dannoso nella Web App.

SQL Injection

Si inserisce il valore che rappresenta un ID



Con la variabile (*' OR ' a ' = ' a)* si annulla il filtro e avere tutti i risultati possibili.



Il comando UNION, esegue un’unione tra due risultati (per esempio tra due SELECT)