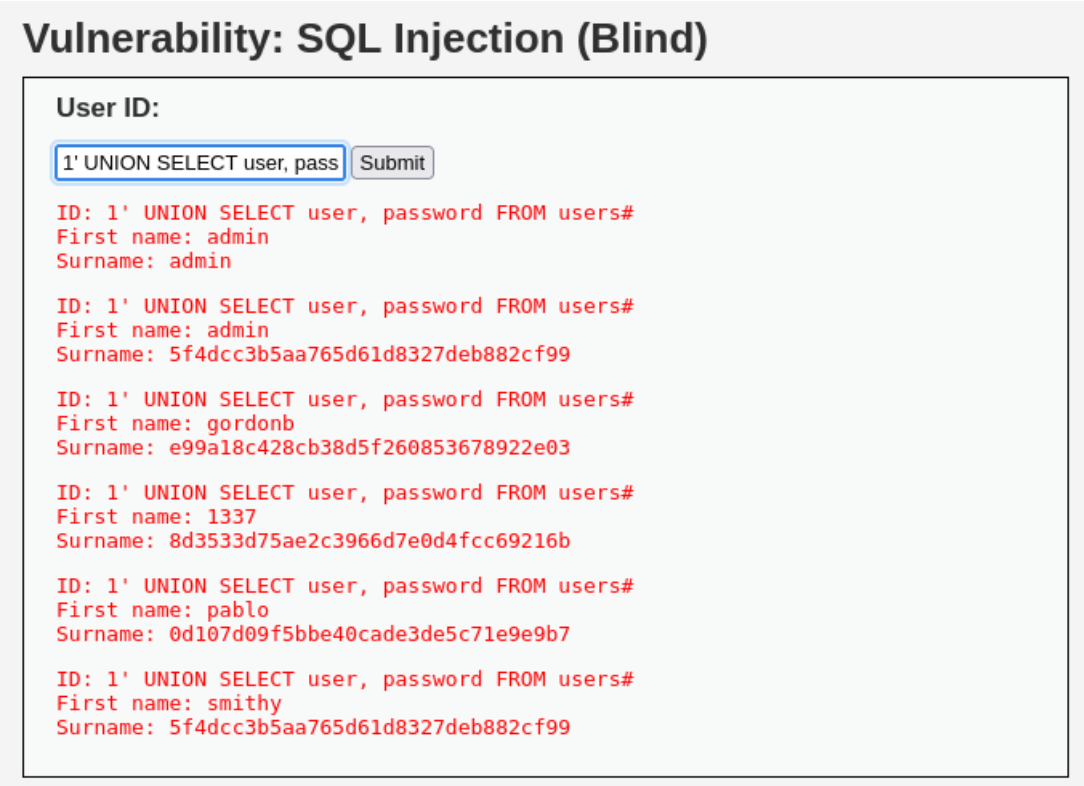
Vulnerability report

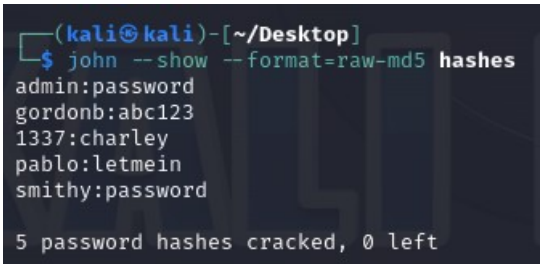
Nel corso dell'exploit delle vulnerabilità riscontrate ho potuto sfruttare due particolari vulnerabilità sulla pagina DVWA, tramite SQL injection e Cross Site Script Stored.

SQL Injection

Ho approcciato per prima la SQL Injection. Inserendo nel campo di ricerca una query che risultasse sempre vera ho potuto recuperare la lista degli utenti con nomi e soprannomi. Ho quindi proceduto a recuperare le password tramite un'altra query UNION based, sfruttando il linguaggio SQL che con il comando UNION permette di unire più ricerche ed ottenere in output le informazioni rilevate con le ricerche stesse.



Le password ottenute sono criptate tramite codice hash (le password nei database non sono mai salvate in chiaro). Per ottenere le password in chiaro ho ricorso allo strumento John the Ripper, un programma che porta avanti attacchi a dizionario sfruttando liste di password e di codici hash delle password.



Come possiamo vedere, la vulnerabilità riscontraa permetta ad un eventuale black hat di infiltrare il database del server web di DVWA e sottrarre dati ivi contenuti, anche importanti come le password.

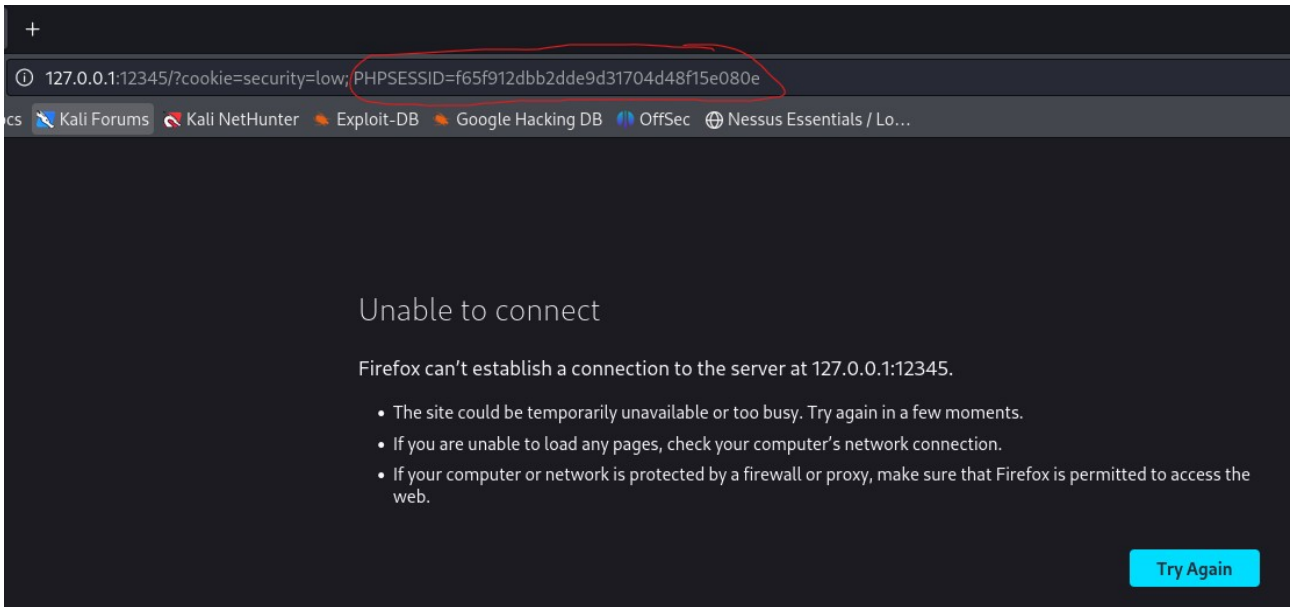
A differenza di una normale SQL injection, nella versione "blind" non verremmo reindirizzati ad una pagina di errore qualora inserissimo una injection non valida, quindi non potremmo sapere se l'attacco è andato a buon fine a meno di testarlo.

Si consiglia di sanitizzare il codice della pagina in modo da filtrare l'input utente, permettendo solo caratteri specifici (lettere) ed evitando espressioni booleane o che sfruttino linguaggio SQL.

XSS stored

Nel caso dell'attacco XSS (Cross Site Script) reflected andiamo a sfruttare un'altra vulnerabilità della pagina web, sempre tramite un input utente. In questo caso possiamo vedere che dato un input, il messaggio apparirà a schermo e verrà salvato nel database del server, così che chiunque arrivi su questa pagina possa ritrovarlo anche in futuro, finché non viene cancellato dal database. In sostanza è una minaccia duratura nel tempo.

Inizialmente ho testato la pagina per confermare che i messaggi venissero effettivamente salvati e che oltretutto la pagina potesse eseguire del codice; l'ultimo messaggio salvato lo prova, essendo scitto in corsivo.
Usando un comando che mi reindirizzasse ad un altro sito web ho potuto recuperare il cookie di sessione dell'utente target su DVWA. Questa può essere una situazione molto pericolosa, in quanto io attaccante potrei spacciarmi per l'utente legittimo (avendo il suo cookie di sessione) e andare a sottrarre dati e informazioni, fare acquisti o pagamenti (se si tratta di un e-commerce o di un sito bancario, per esmepio), cambiare la password, accedere al numero di carta di credito...



Come soluzione a questo problema si consiglia anche in questo caso di filtrare l'input utente e, per quanto riguarda il cookie di sessione, implementare un doppio fattore di autenticazione, associando per esempio l'ID di sessione ad un unico indirizzo IP (l'indirizzo IP dell'attacante e quello dell'utente legittimo saranno necessariamente diversi.