Esercitazione S6/L2

In questa esercitazione ho testato le vulnerabilità del server DVWA provando un attacco di SQL Injection e XSS Reflected.

Dispositivi e software utilizzati:

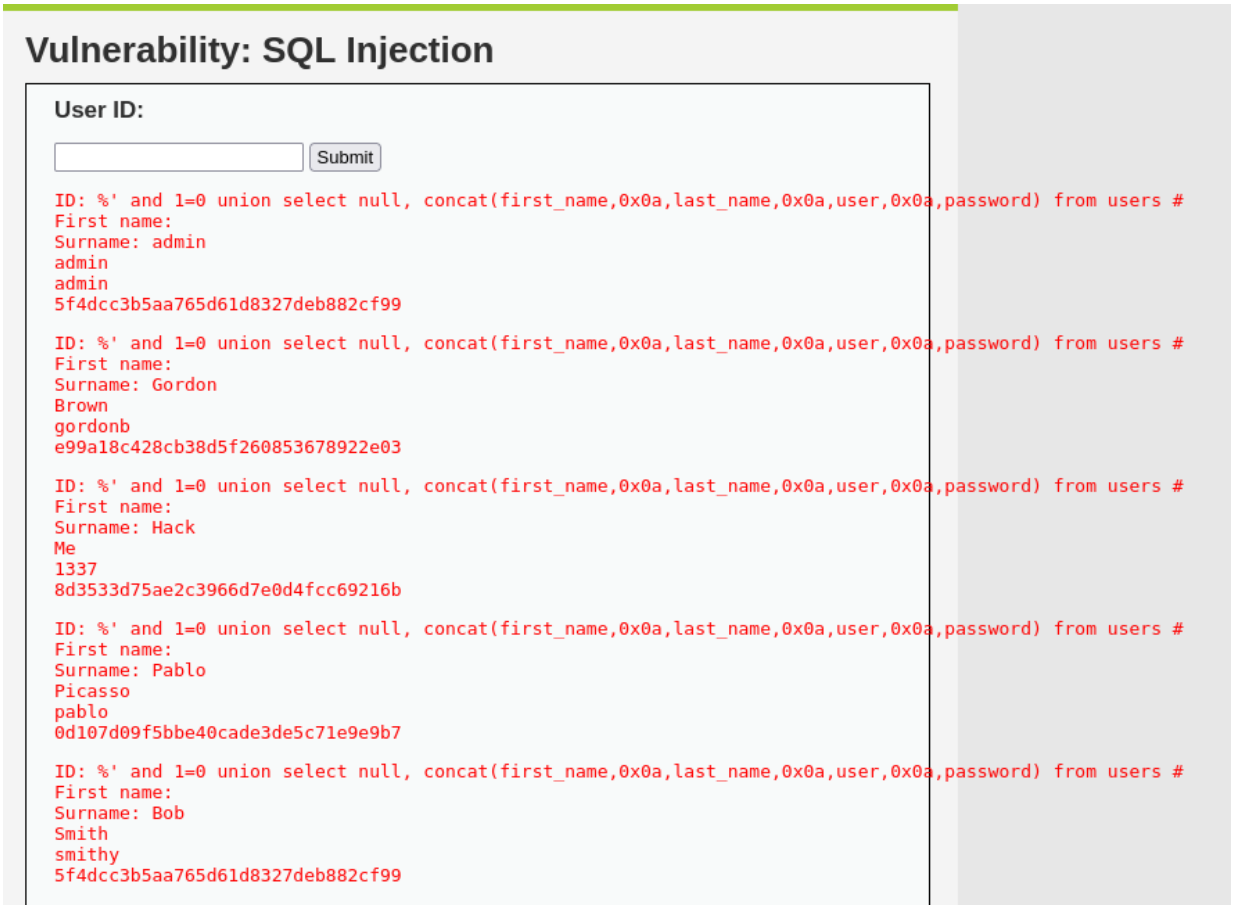
- Metaspoitable (DVWA)
- Kali
- Netcat

SQL Injection:

Questo tipo di attacco mira a ricavare informazioni e e dati richiedendo al database determinate informazioni.
SQL è un linguaggio di programmazione ideato per creare o manpolare dati nel database. Il web server e il database comunicano in SQL per richiedere i dati inseriti da un utente.
Se il web server non è impostato per filtrare gli input degli utenti, utilizzando comandi specifici (la giusta query) si possono ricavare i tutti i dati che un attaccante vuole ricavare, ad esempio: ID, password o carte di credito.

Svolgimento:

Dopo aver messo in comunicazione Metaspoitable e Kali ho provato a inserire una query per ricavare username e password degli utenti salvati nel database di DVWA



Ho utilizzato questa query per procedere con l'attacco SQL Injection:
%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
Ecco una spiegazione dettagliata di come funziona:

1. **`%' and 1=0`**: la query inizia con `%'`, che chiude una condizione di ricerca, presumibilmente in una query che sta cercando un valore come `%termine%`. Subito dopo troviamo `and 1=0`, che aggiunge una condizione sempre falsa, per garantire che i risultati della query originale siano nulli (cioè, non restituiscano dati significativi).
2. **`union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`**:
    - **`union select`** è utilizzato per combinare il risultato di una query aggiuntiva con il risultato originale. In questo caso, si prova ad aggiungere una query che estrae informazioni sensibili dalla tabella `users`.
    - **`null`**: il primo valore è `null`, probabilmente per allineare il numero di colonne della query iniettata con quella originale, permettendo così alla query di funzionare correttamente.
    - **`concat(first_name,0x0a,last_name,0x0a,user,0x0a,password)`** : questa parte concatena (unisce) vari campi dalla tabella `users`, separandoli con `0x0a`, che rappresenta un carattere di nuova riga (`\n` in esadecimale).
        - Vengono estratti `first_name`, `last_name`, `user`, e `password`.
    - `#`: il simbolo # in SQL è utilizzato per commentare il resto della query. Questo significa che qualsiasi cosa segua verrà ignorata dal database, isolando e rendendo efficace l'iniezione.

XSS Reflected

Con questo tipo di attacco ho ricavato il cookie di sessione del server DVWA.
Ricavando il cookie di sessione si può accedere alla sessione di un altro utente e rubare ovviamente dati e informazioni.
Andando a sfruttare sempre il mancato filtro degli input degli utenti sul web server si può inserire uno script.Utilizzando Netcat, mettendolo in ascolto sulla porta 80, andiamo a intercettare le comunicazioni tra Kali e il server DVWA.
Come si può vedere dall'immagine abbiamo ricavato il cookie con la sessione e il codice di riferimento.
Più varie informazioni legate alla pagina.
Avendo queste informazioni un attaccante può svolgere un attacco CSRF ed avere accesso alle informazioni legate all'account dela vittima.