**EXPLOIT DVWA - XSS E SQL INJECTION**

**INTRODUZIONE TEORICA**

Abbiamo visto tre tipi di attacchi MITM alle webapp eseguibili tramite degli script:

- XSS (Cross Site Scripting)  
- CSRF (Cross Site Request Forge)  
- SQL Injection

L’attacco XSS si verifica quando l’attaccante può inserire codice malevolo nei campi di input dell’applicazione web, come campi di ricerca o di commento, che poi verranno visualizzati agli utenti che accedono alla stessa pagina web.

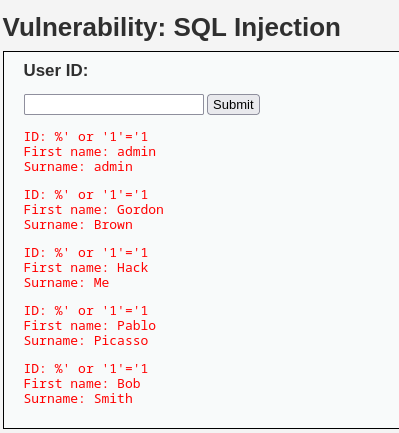
Esistono tre tipi di attacchi XSS:  
- Stored XSS: in cui il codice malevolo permane su un server/database e viene eseguito ogni volta che un utente accede alla pagina web in cui è stato inserito.  
- Reflected XSS: in cui il codice malevolo viene inserito nell’URL della pagina web e viene eseguito quando l’utente accede a tale URL.  
- DOM-based XSS: in cui il codice malevolo viene eseguito sulla struttura della pagina e permette allo script di modificarne contenuto, la struttura e lo stile del documento.

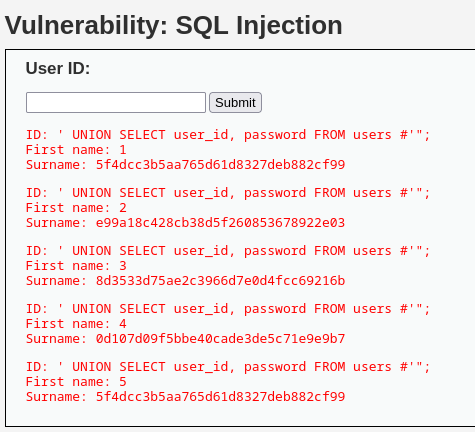
L’attacco CSRF sfrutta l’architettura di base del protocollo HTTP e della comunicazione di dati in Internet, ovvero le sessioni di autenticazione e i cookie inviati ai browser. In pratica, l’attaccante non inganna l’utente vero e proprio, ma il suo browser, facendogli inviare una richiesta a un’applicazione web in cui si è precedentemente autenticato e per cui non ha fatto il logout.

L’attacco SQL Injection permette ad un utente non autorizzato di prendere il controllo sui comandi SQL utilizzati da un’applicazione Web. Questa tipologia di attacco ha impatti negativi enormi sui siti web.

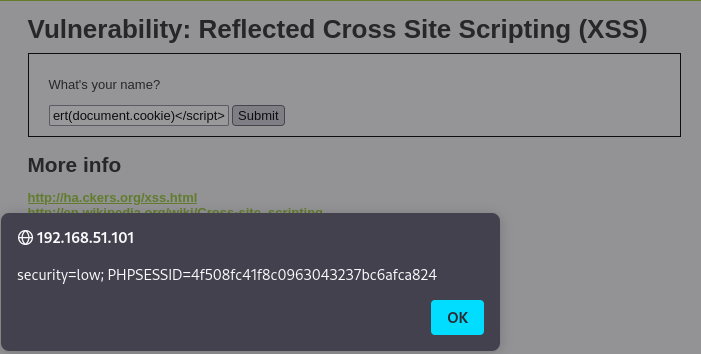
Andiamo ora ad eseguire due attacchi su DVWA:  
- SQL Injection  
- XSS Reflected

**1) SQL Injection**

Abbiamo utilizzato la query “%' or '0'='0'” per fare in modo che ci vengano visualizzate le info riguardanti tutti gli user\_id (a seguito della condizione 0=0 che è sempre vera).

Successivamente andiamo ad utilizzare un’altra query “' UNION SELECT user\_id, password FROM users #” che ci visualizzi lo user\_id e le password (in hash) di tutti gli utenti registrati nel database.

**2) XSS REFLECTED**

Abbiamo utilizzato uno script “<script>alert(document.cookie)</script>” che ci visualizza l’IP della macchina vittima ed il SessionID contenuto nel cookie.