Corso Epicode
XSS E SQL INJECTION

Report a cura di Valentino Pizzi
5 ottobre, 2025

Obbiettivo:
- Sfruttare XSS reflected e sql injection in DVWA su metasploitable IP ‘192.168.50.101

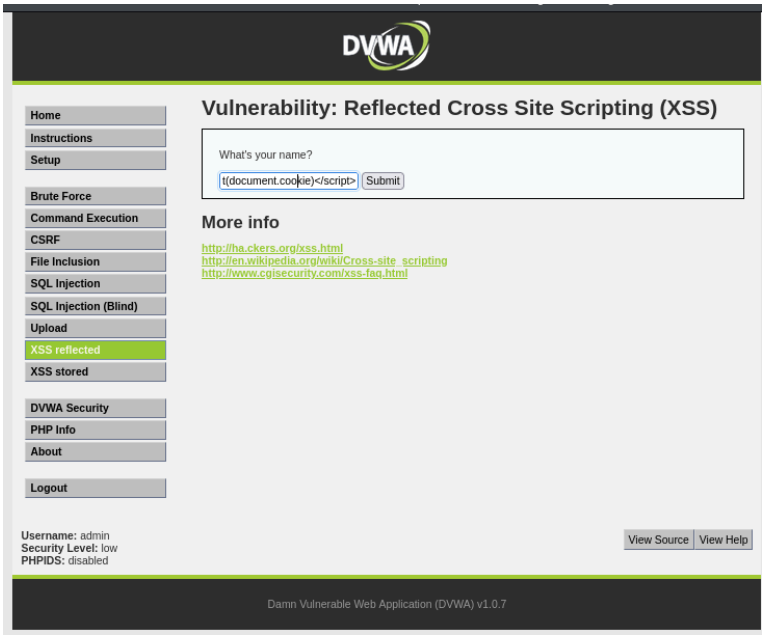
Contenuti:
- XSS reflected
- SQL injection

Obbiettivo:
- Recuperare i cookie di sessione sfruttando xss
- Sfruttare Union in sql injection

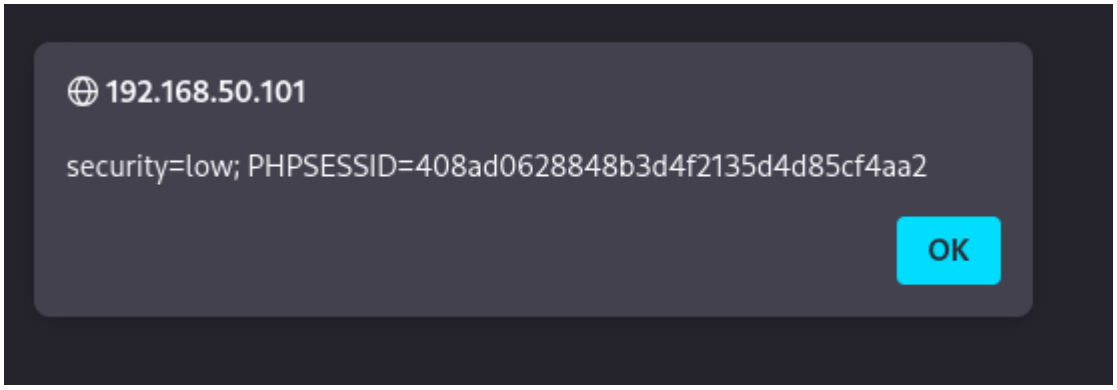
Xss reflected

Dopo aver aperto DVWA ed aver fatto l’accesso, selezioniamo il livello di security ‘low’, apriamo la sezione xss reflected e testiamo come funziona, iniziando con provare ad inserire del corsivo nella casella per l’inserimento del nome scriviamo:” **Ciao** “ ed inviamo, vediamo che ci risponde scrivendo ciao in corsivo.

Proviamo allora a reperire i cookie di sessione con uno script “ <script>alert(document.cookie)</script>” come in figura sotto.

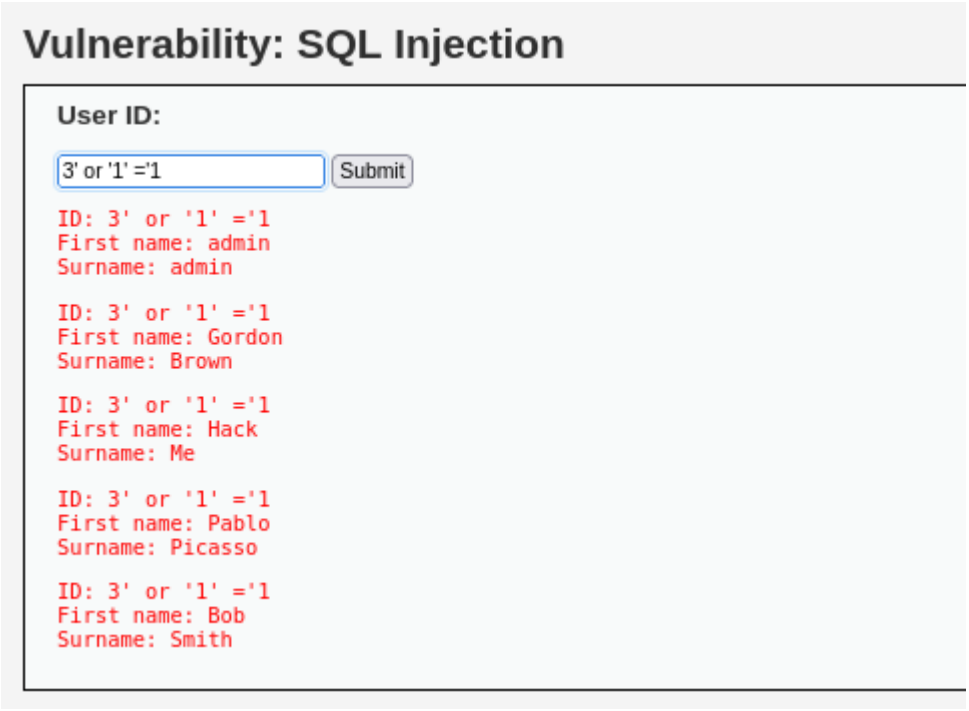


Appuriamo che restituisce esattamente quello che volevamo con un piccolo pop-up creato dal comando alert.

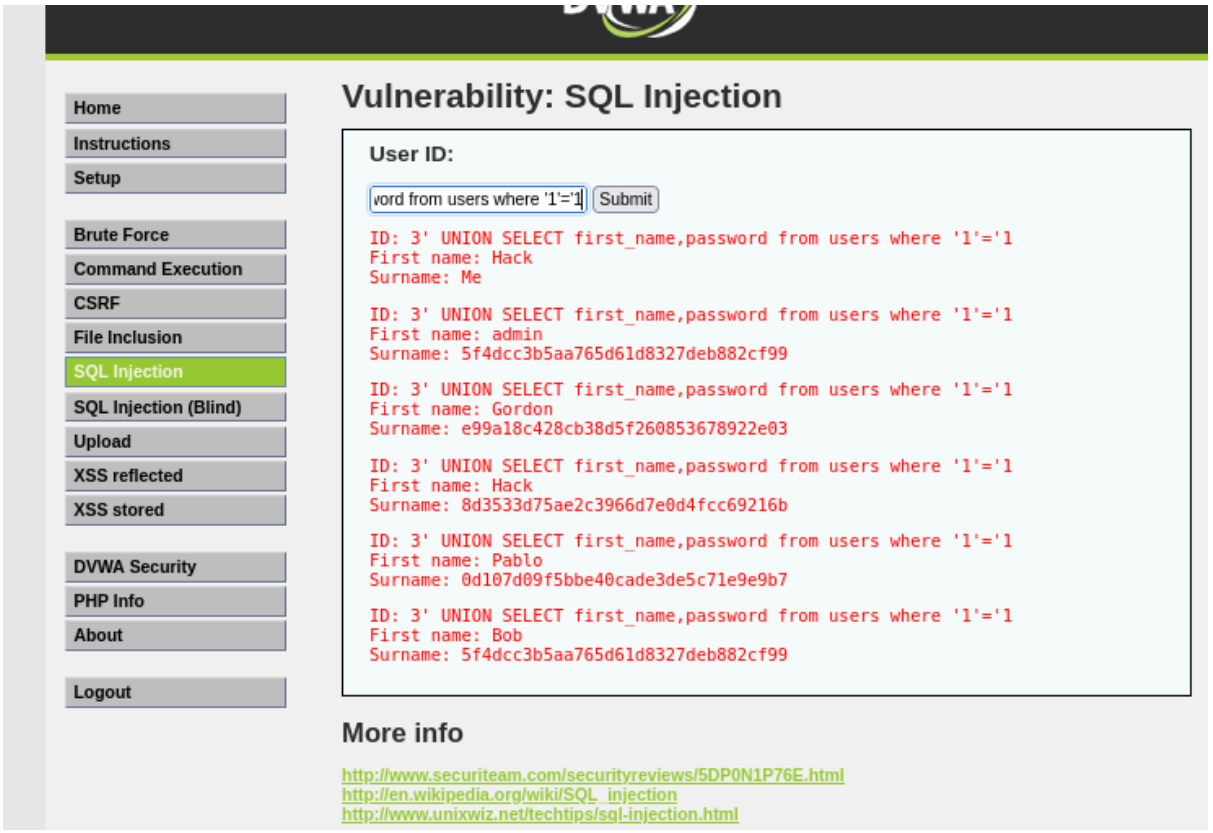


SQL Injection

Testiamo ora l'SQL injection di DVWA, come prima con security low, iniziamo capendo come funziona, inseriamo un numero (3), vediamo che ci vengono restituiti delle informazioni di una tabella, vediamo se inserendo un piccolo payload riusciamo ad avere piu' informazioni, proviamo con: 3' or '1'='1



Vediamo che ci restituisce tutti le informazioni di quella tabella, proviamo quindi con altri payload: 3' UNION SELECT first_name,password from users where '1'='1



Possiamo vedere che ci ha restituito i nomi e le password delle persone iscritte nella tabella, cerchiamo ora di recuperare gli username di queste persone usando lo stesso payload ma modificandolo per ricevere gli user e non i nomi.
3' UNION SELECT user,password from users where '1'='1