Exploit DVWA XSS – SQL INJECTION

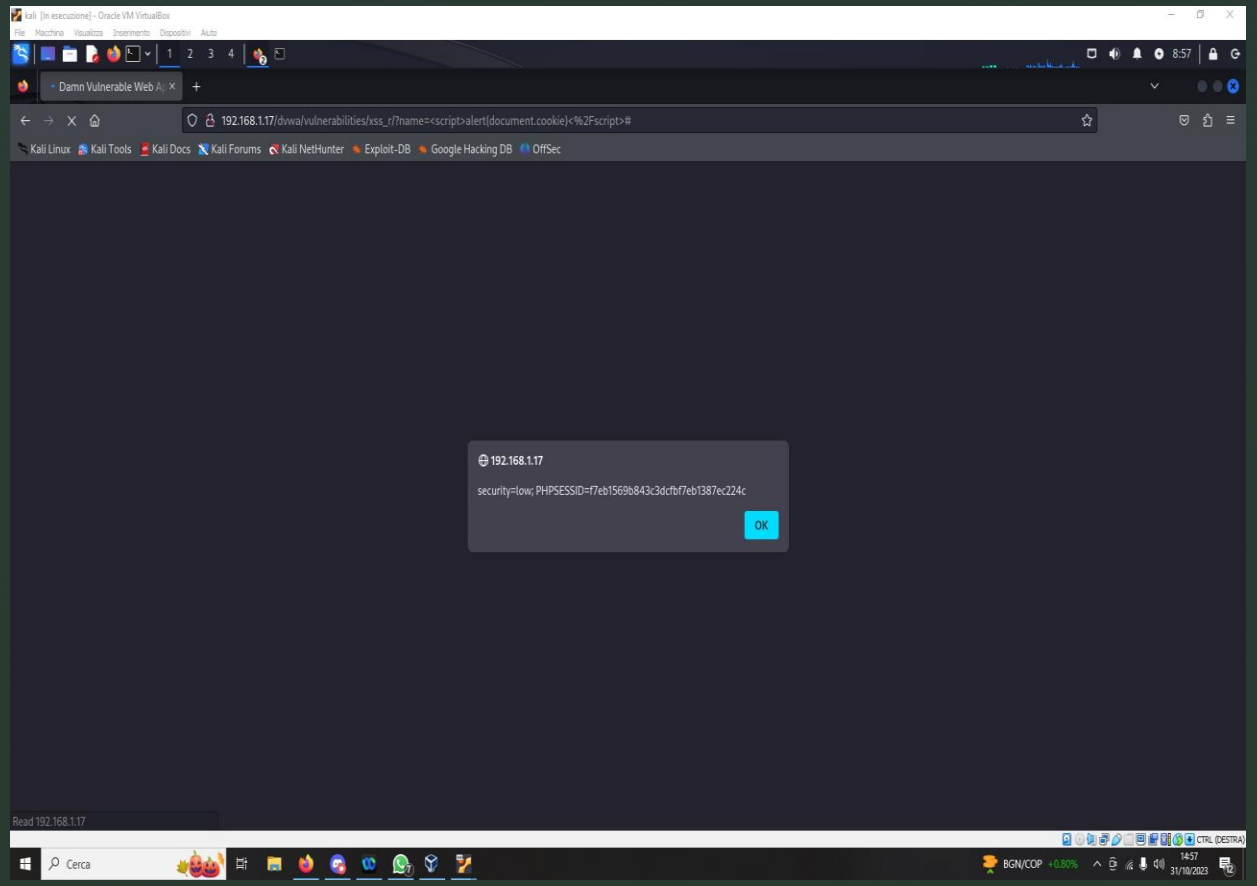
- L'esercizio di oggi ci invita ad eseguirere due tipi di attacchi sulla DVWA dalla macchina Kali:

  - XSS REFLECTED
  - SQL INJECTION

Attacco XSS Reflected:

- Gli XSS (Cross site scripting) sono una famiglia di vulnerabilità con cui il black hat puo sfruttare per prendere controllo su una Web App.
- L'esercizio di oggi richiedeva di usare un specifico tipo di XSS, ovvero XSS reflected:
- Avviene quando il Payload malevolo dell'attaccante sara trasportato dalla richiesta che il browser del client invierà al sito vulnerabile

Andando su DVWA nella sezione XSS reflected, abbiamo inserito un codice HTML in cui abbiamo chiesto di mostrarci il coockie di sessione

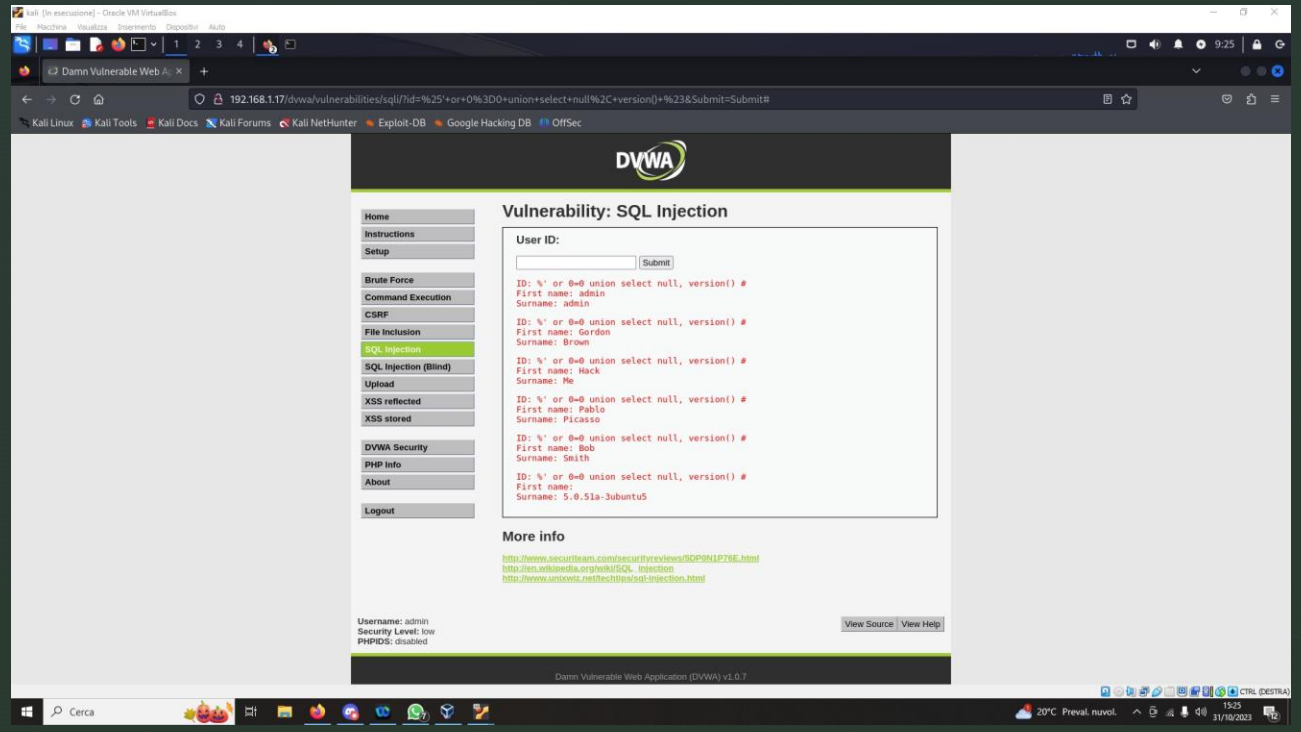


<script>alert(document.coockie)</script>

SQL INJECTION

- L'attacco SQL Injection permette all'attaccante di prendere il controllo sui comandi SQL utilizzati da una Web App
- Avere il controllo dei comandi SQL significa poter chiedere ai database qualsiasi cosa.

Con questo comando SQL chiediamo al DB i First Name e Surname che sono presenti in tabella e la versione dell'applicazione DVWA con cui sta operando




```
%' or 0=0 union select null,
version() #
```