M4-W13D4-Pratica

DATA

Cybersecurity Analyst

Studente:
Andrea Scarmagnani
Docente:
Federico Daidone

Exploit DVWA - XSS e 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**)

Consegna:

XSS
1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

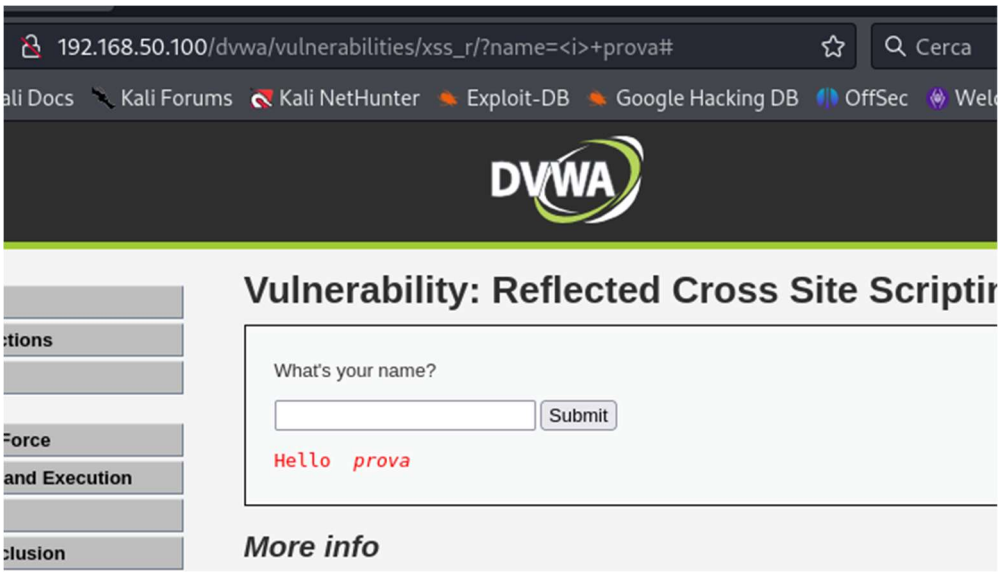
SQL
1. Controllo di injection
2. Esempi
3. Union

Screenshot/spiegazione in un report di PDF

XSS reflected

Scrivendo nel campo nome il testo → <i>prova ← Ci troviamo il testo di risposta scritto in corsivo. Significa che la macchina è vulnerabile agli attacchi XSS.

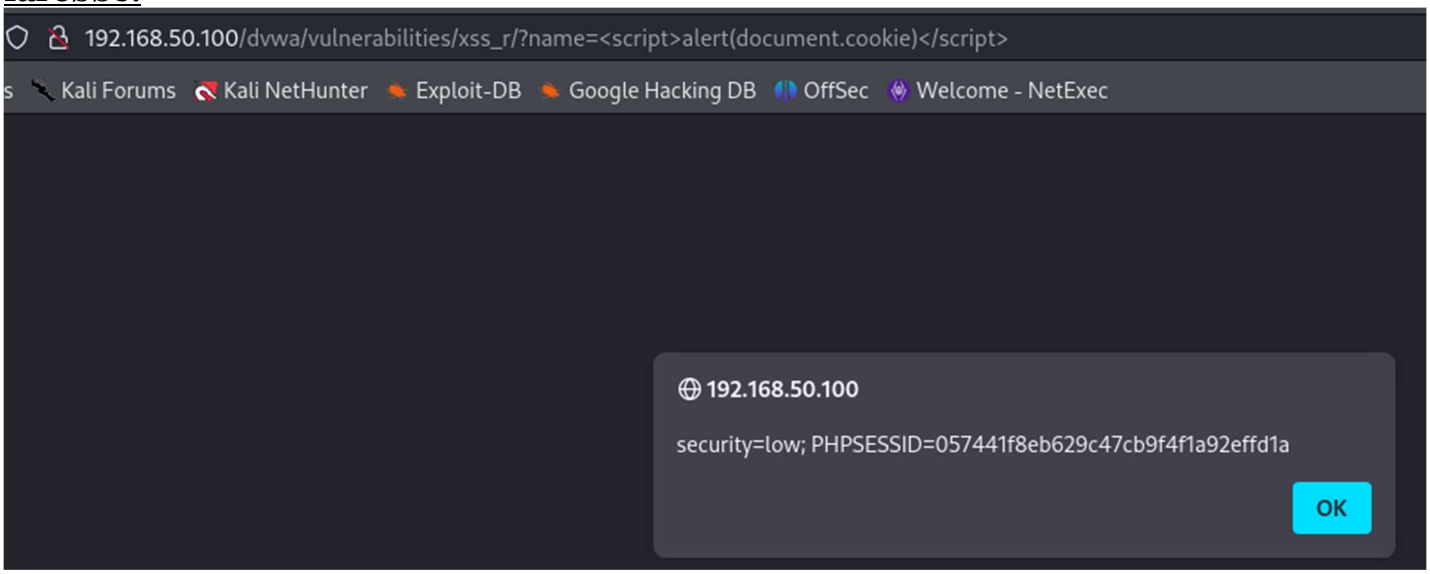
http://192.168.50.100/dvwa/vulnerabilities/xss_r/?name=**%3Ci%3E+prova#**



Ora si tenta qualcosa di più complesso: **<script>alert(document.cookie)</script>**
Passando questo comando ci restituisce il cockie, quindi il livello di sicurezza e la sessione php:

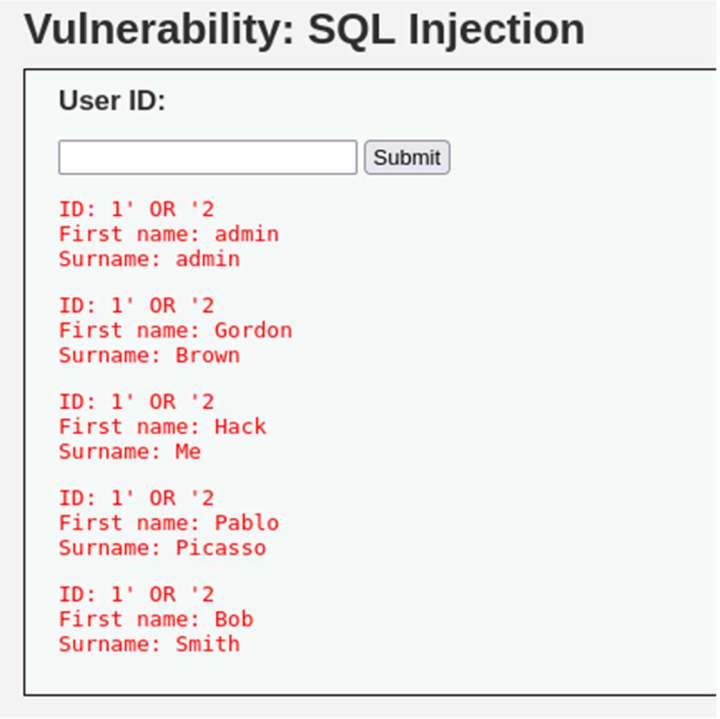
http://192.168.50.100/dvwa/vulnerabilities/xss_r/?name=**%3Cscript%3Ealert(document.cookie)%3C/script%3E**

Ho fatto comparire nel messaggio di Allert il cookie. Solo a scopo didattico, non si farebbe.



SQL
1. Controllo di injection
2. Esempi
3. Union

Qui ho inserito il comando 1’ or ‘2 e ha restituito tutti i gli utenti…



Esempio fatto con union:

Cybersecurity Analyst 2023