

Consegna BW 2

Consegna BW II: Web Application Exploit e Metasploit

🔖 Tag: [#SQLi](#) [#XSS](#) [#metasploit](#) [#hacking](#)

Traccia Giorno 1: SQL Injection

Obiettivo: Utilizzando le tecniche SQL Injection apprese, sfruttare la vulnerabilità sulla Web Application DVWA per recuperare in chiaro la password dell'utente **Pablo Picasso**. È richiesto:

1. Recuperare la password in chiaro senza l'uso di strumenti automatizzati come sqlmap (è ammesso l'uso di **Burp Suite Repeater**).

Requisiti laboratorio Giorno 1

- Livello difficoltà DVWA: **LOW**.
- IP Kali Linux: **192.168.13.100/24**.
- IP Metasploitable: **192.168.13.150/24**.

Bonus:

- Replicare tutto a livello **medium**.
- Recuperare informazioni vitali da altri database collegati.
- Creare una guida illustrata per spiegare ad un utente medio come replicare l'attacco.

Traccia Giorno 2: Cross-Site Scripting (XSS)

Obiettivo: Sfruttare una vulnerabilità di **XSS persistente** in DVWA per simulare il furto di una sessione utente inoltrando i cookie a un Web Server sotto controllo.

Requisiti laboratorio Giorno 2

- Livello difficoltà DVWA: **LOW**.
- IP Kali Linux: **192.168.104.100/24**.
- IP Metasploitable: **192.168.104.150/24**.
- **Web Server** in ascolto sulla porta **4444**.

Extra facoltativi:

- Replicare tutto a livello **medium**.
 - Ottenere dump completi di dati come cookie, versione browser, IP.
 - Creare una guida illustrata per spiegare ad un utente medio come replicare l'attacco.
-

Traccia Giorno 3: Buffer Overflow

Obiettivo:

1. Descrivere il funzionamento del programma prima dell'esecuzione.
2. Riprodurre ed eseguire il programma, verificando le ipotesi sul suo funzionamento.
3. Modificare il programma per generare un **errore di segmentazione**.

Suggerimento: Concentrarsi sull'assenza di controlli nell'input.

Bonus:

- Inserire controlli di input.
- Creare un menù interattivo per decidere se il programma debba generare un errore o eseguire correttamente.

Traccia Giorno 4: Exploit Metasploitable

Obiettivo: Utilizzando Metasploit:

1. Eseguire uno scan con Nessus.
2. Sfruttare il servizio Samba sulla porta **445 TCP**.
3. Ottenere l'indirizzo IP della macchina compromessa con `ifconfig`.

Requisiti laboratorio Giorno 4

- IP Kali Linux: **192.168.50.100**.
 - IP Metasploitable: **192.168.50.150**.
 - Listen port (opzioni payload): **5555**.
 - **Exploit Path:** `exploit/multi/samba/usermap_script`.
-

Traccia Giorno 5: Exploit su Windows 10

Obiettivo:

1. Avviare i servizi vulnerabili su Windows.
2. Eseguire un **basic scan** con Nessus.
3. Exploitare il servizio **Tomcat** con Metasploit.


Requisiti laboratorio Giorno 5

- IP Kali Linux: **192.168.200.100**.
- IP Windows: **192.168.200.200**.
- Listen port (payload): **7777**.

Evidenze:

- Identificare la macchina (virtuale o fisica).

- Ottenere impostazioni di rete e verificare la presenza di webcam attive.
 - Acquisire uno screenshot del desktop.
-

 **Chiavi:** [SQLi, XSS, metasploit, hacking]