Web Application Exploit SQLi

Traccia 1

Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare in chiaro la password dell'utente Pablo Picasso.
NB: non usare tool automatici come sqlmap. È ammesso l'uso di repeater burp suite.

Requisiti laboratorio

- 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 db collegati
-Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco

Web Application Exploit XSS

Traccia 2

Utilizzando le nozioni viste a lezione, sfruttare la vulnerabilità **XSS persistente** presente sulla Web Application DVWA al fine simulare il furto di una sessione di un utente lecito del sito, inoltrando i cookie «rubati» ad Web server sotto il vostro controllo. Spiegare il significato dello script utilizzato.

Requisiti laboratorio:

- Livello difficoltà DVWA: LOW
- IP Kali Linux: 192.168.104.100/24
- IP Metasploitable: 192.168.104.150/24
- I cookie dovranno essere ricevuti su un Web Server in ascolto sulla porta 4444

Bonus

-Replicare tutto a livello medium
-Fare il dump completo, cookie, versione browser, ip, data
-Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco

System exploit BOF

Traccia 3

https://drive.google.com/file/d/1nEM_FV5zFHj4hw9_Ya1PUP_xf5bLGy0I/view
Leggete attentamente il programma in allegato. Viene richiesto di:

- Descrivere il funzionamento del programma prima dell´esecuzione.
- Riprodurre ed eseguire il programma nel laboratorio - le vostre ipotesi sul funzionamento erano corrette?
- Modificare il programma affinché si verifichi un errore di segmentazione.

Bonus

-Inserire controlli di input.

-Creare un menù per far decidere all'utente se avere il programma che va in errore oppure quello corretto.

Exploit Metasploitable con Metasploit

Traccia 4

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable.
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento).
- Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l´indirizzo di rete della macchina vittima.

Requisiti laboratorio:

- IP Kali Linux: 192.168.50.100
- IP Metasploitable: 192.168.50.150
- Listen port (nelle opzioni del payload): 5555

Exploit Windows con Metasploit

Traccia 5

Sulla macchina Windows 10 ci possono essere dei servizi che potrebbero causare degli exploit. Si richiede allo studente di:

- Avviare questi servizi
- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows 10
- Aprire una sessione con metasploit, exploitando il servizio TomCat.

Requisiti laboratorio

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

Evidenze laboratorio:

Una volta ottenuta una sessione Meterpreter, eseguite una fase di test per confermare di essere sulla macchina target. Recuperate le seguenti informazioni:

1. Se la macchina target è una macchina virtuale oppure una macchina fisica

2. le impostazioni di rete della macchine target

3. se la macchina target ha a disposizione delle webcam attive. Infine, recuperate uno screenshot del desktop

Bonus: Jangow 01 CTF Facile

Scaricare ed importare la macchina virtuale da questo link:
https://download.vulnhub.com/jangow/jangow-011.0.1.ova

Effettuare gli attacchi necessari per diventare root. Studiare a fondo la macchina per scoprire tutti i segreti. L’ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall’interno dell’azienda, di cui non sappiamo nulla, per questo è test di BlackBox puro.

Bonus: Empire Lupin One - CTF Media difficoltà

Scaricare ed importare la macchina virtuale da questo link:
https://download.vulnhub.com/empire/01Empire-Lupin-One.zip

Questa box è stata creata per essere di media difficoltà, ma può trasformarsi in un'impresa ardua se ti smarrisci nel suo labirinto.
Suggerimento: dovrai enumerare tutto ciò che è possibile.

Bonus: BlackBox Epicode Harry P - CTF difficile

Scaricare ed importare la macchina virtuale da questo link:
https://drive.google.com/file/d/1vLIieF2HBgCCI76hqopUW3j98wFjflM/view?usp=drive_link

In questa immagine OVA di una macchina compromessa, un dipendente infedele di nome Luca ha deliberatamente sabotato il server, cambiando le password e alterando i servizi. Da una breve indagine OSINT, scopriamo che Luca ha intrecciato una relazione con Milena, anch'ella operante presso Theta. La tua missione è di riprendere il controllo del server compromesso e restaurare l'ordine perduto