Raul Pastor

XSS e SQLInjection

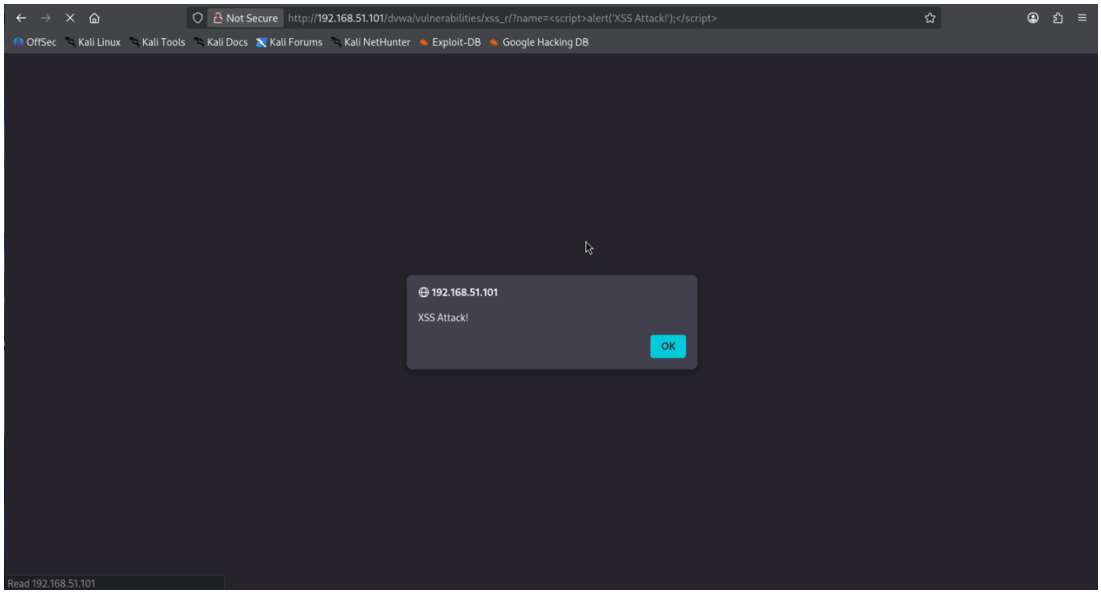
Nell'esercizio di oggi viene richiesto di utilizzare la vulnerabilità della DVWA di meta per effettuare attacchi XSS e SQLinjection attraverso la macchina Kali..

La prima cosa fatta è stata mettere in collegamento le due macchine, dopodiché mi sono collegato alla DVWA di Meta.

Ho Settato la sicurezza a Low.

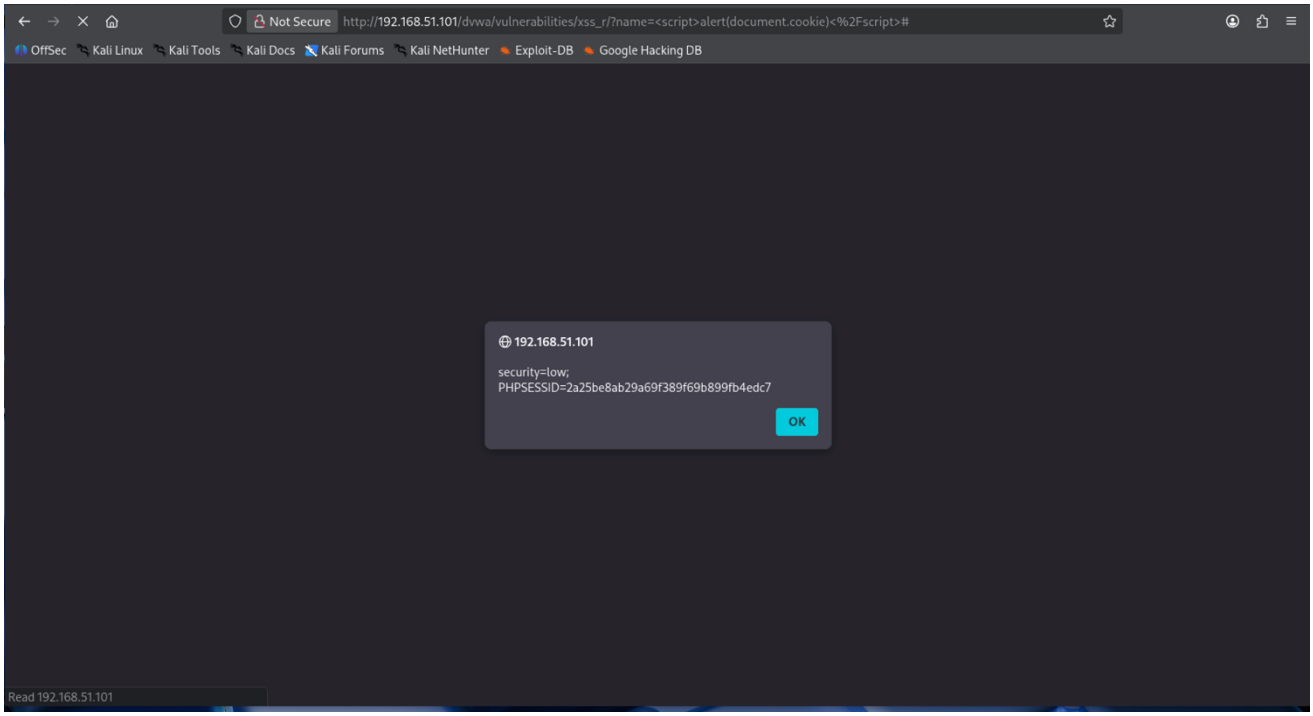
Per la parte di XSS ho fatto qualche test per verificare che la submit leggesse testo html quindi ho scritto '<I> hi' ed effettivamente mi ha cambiato il testo in corsivo.

Subito dopo ho laciato un alert con <script>alert('XSS Attack!')</script>

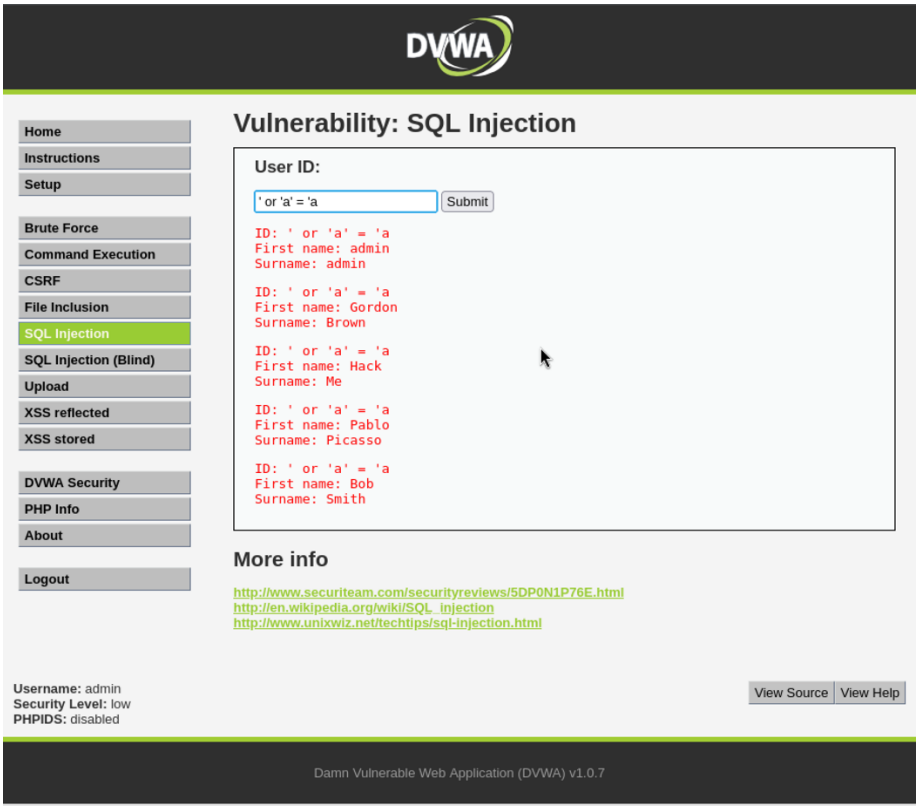


Raul Pastor

Ho continuato l'attacco cercando il con '<script>alert(document.cookie)</script>' ritrovando il cookie della sessione:



Per la parte di SQL Injection ho utilizzato il metodo boolean based per cercare tutti gli username e password:



Raul Pastor

Ho utilizzato sia il metodo Union based injection per ricevere tutte le informazioni possibili dalla tabella users: