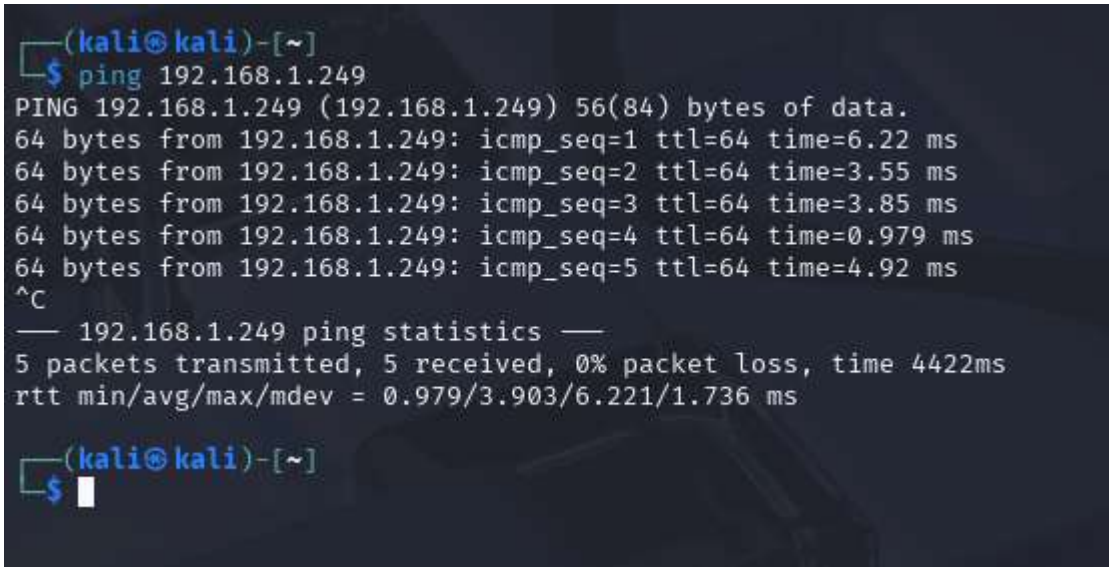
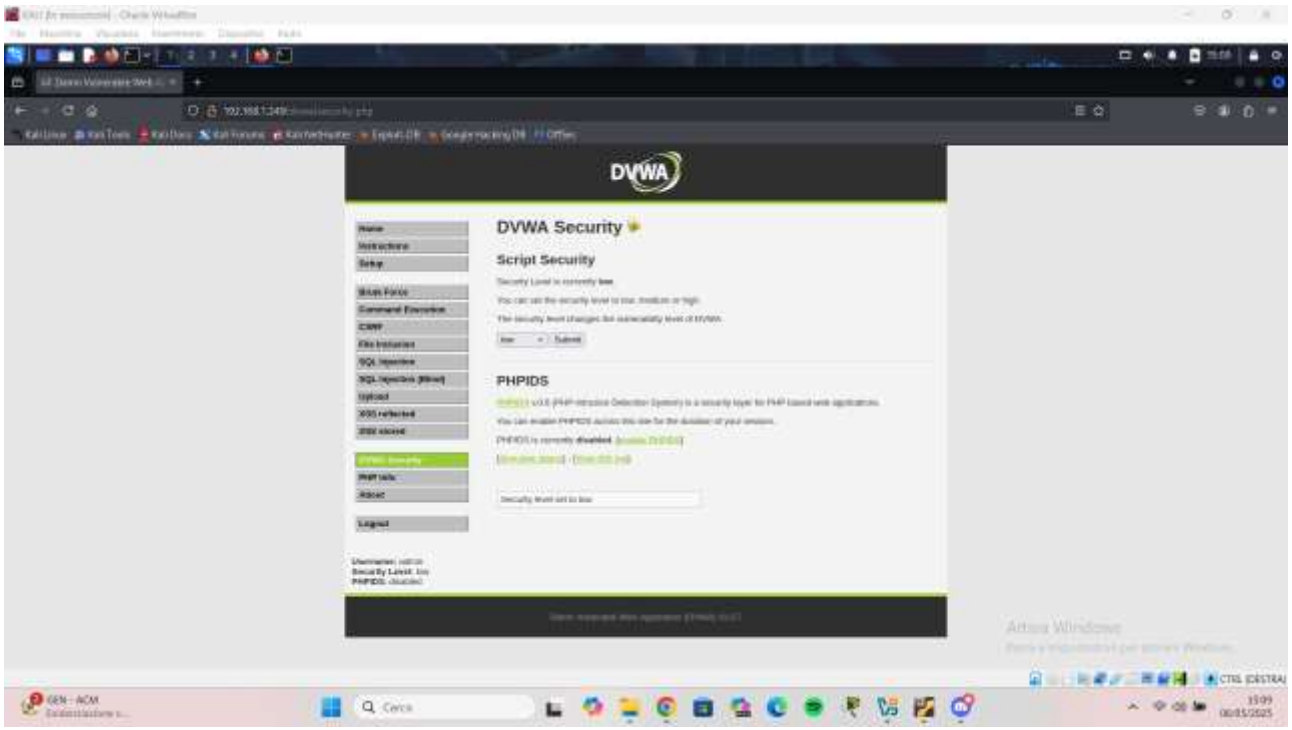
S6L2:ESERCIZIO

- Configurazione del Laboratorio: ○ Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante). ○ Verificate la comunicazione tra le due macchine utilizzando il comando ping.

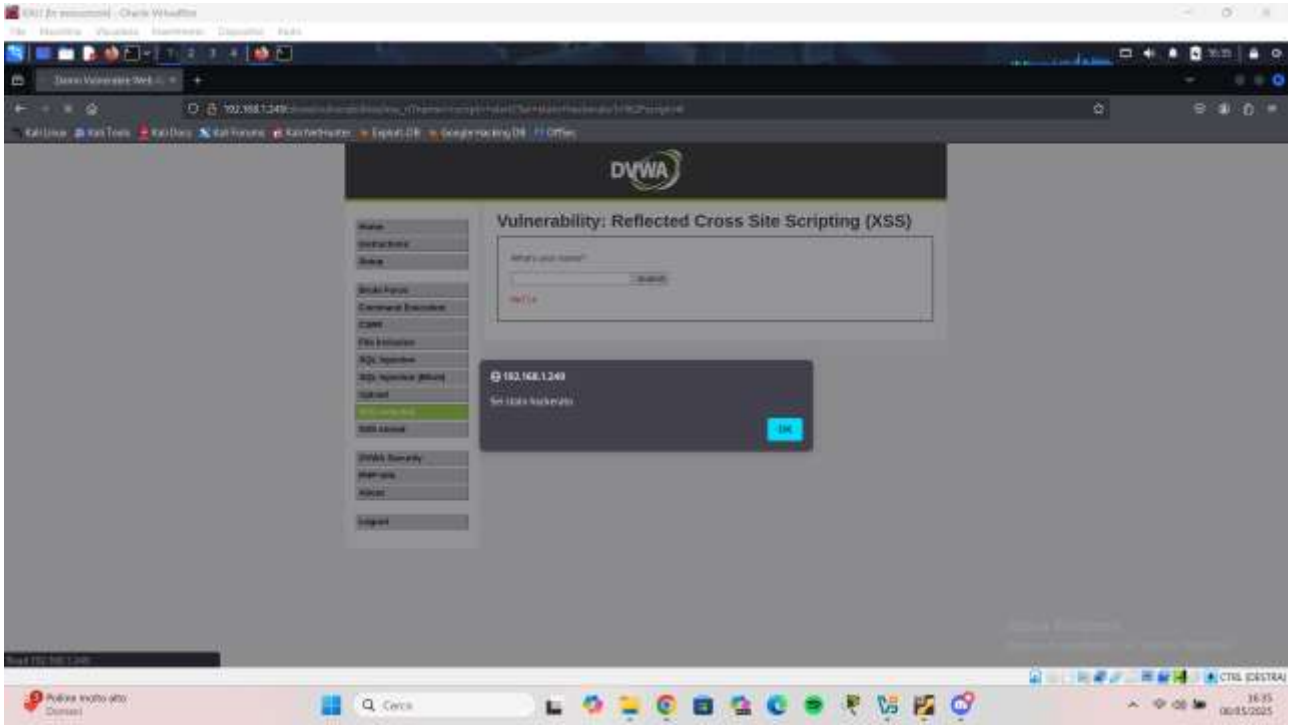


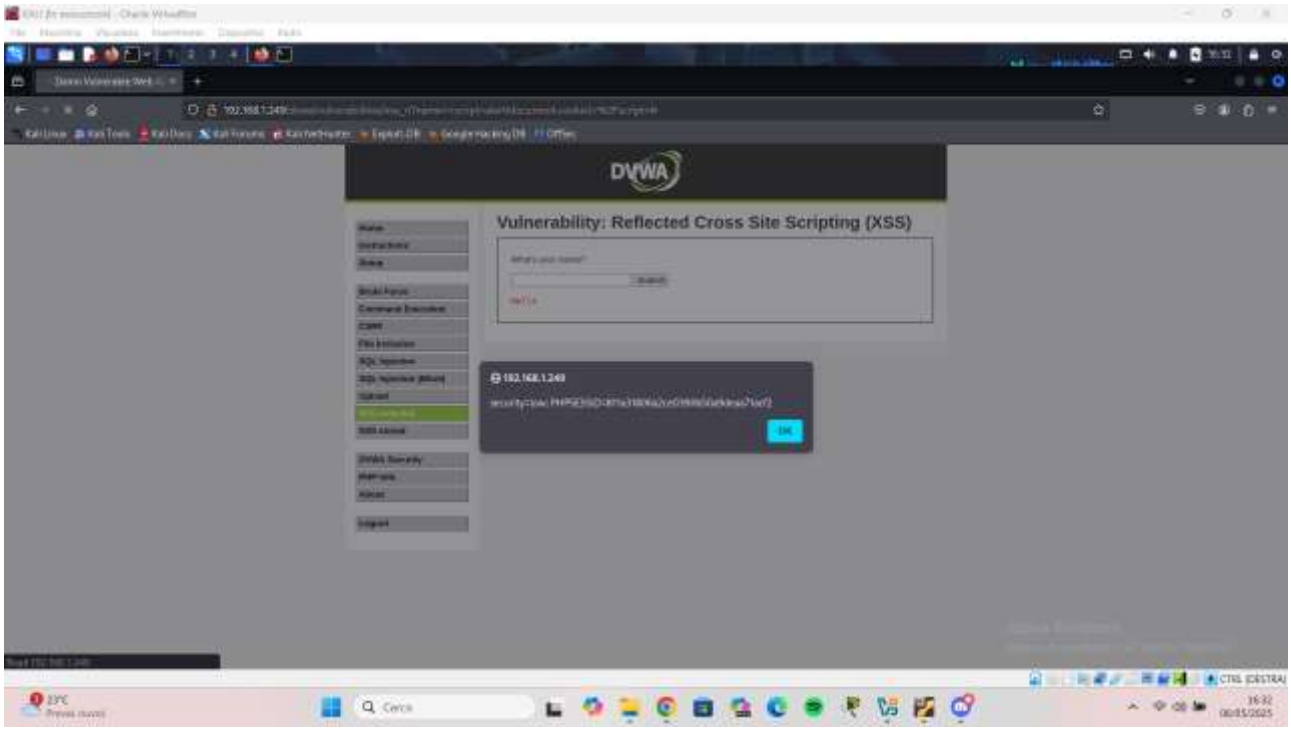
- Impostazione della DVWA↵ ○ Accedete alla DVWA dalla macchina Kali Linux tramite il browser. ○ Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.



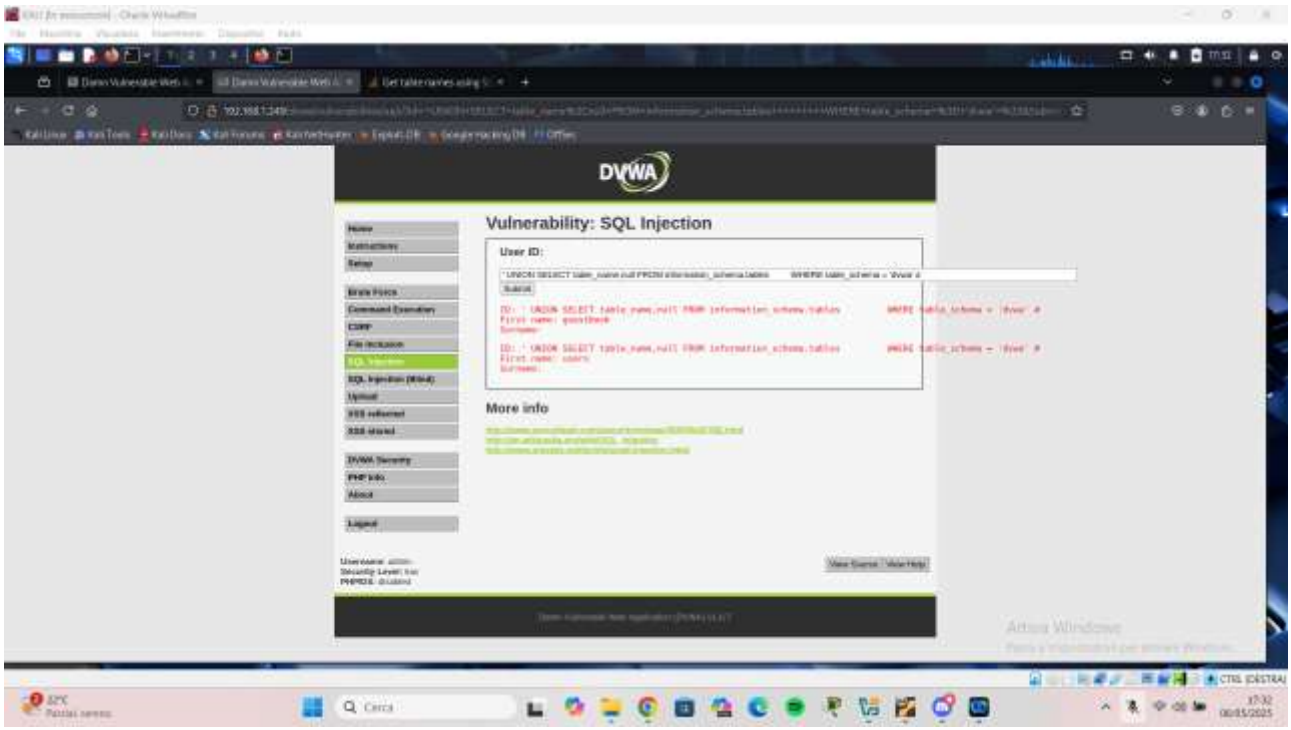
- Sfruttamento delle Vulnerabilità: ○ Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind). Sfruttamento delle Vulnerabilità: ○ Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind).

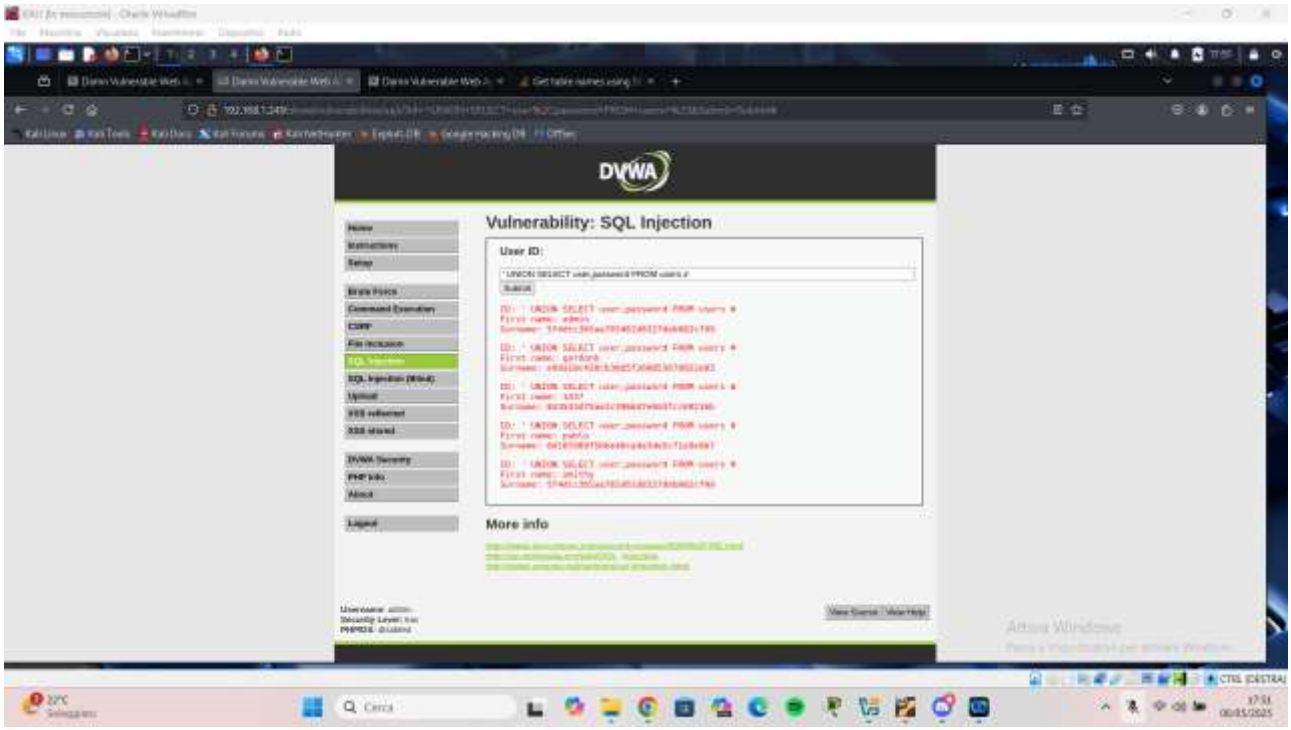
XSS REFLECTED:

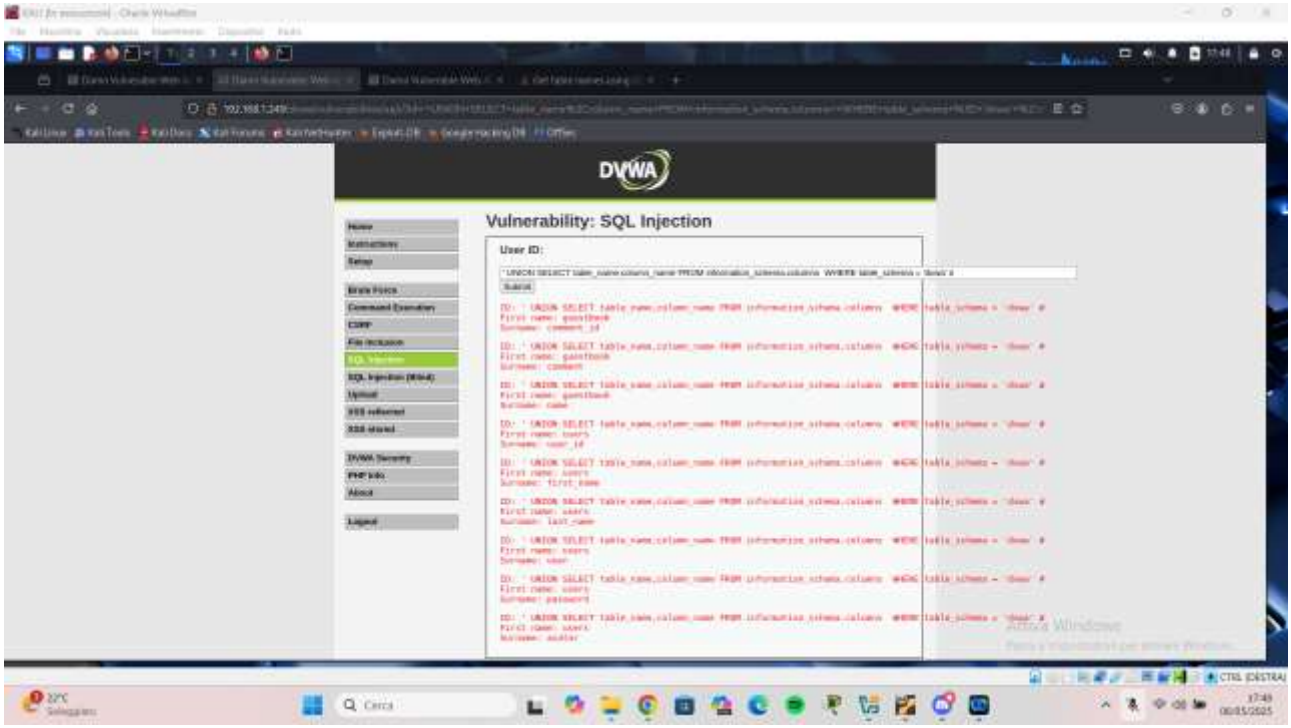


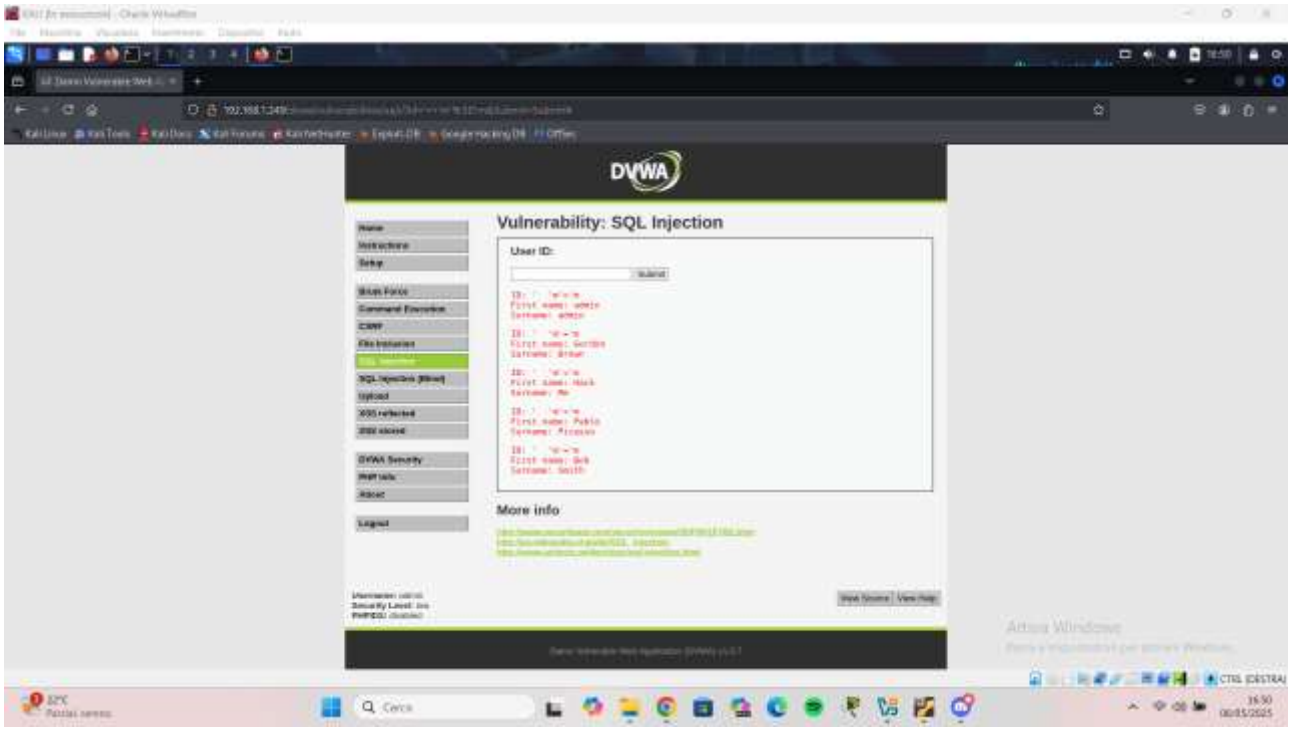


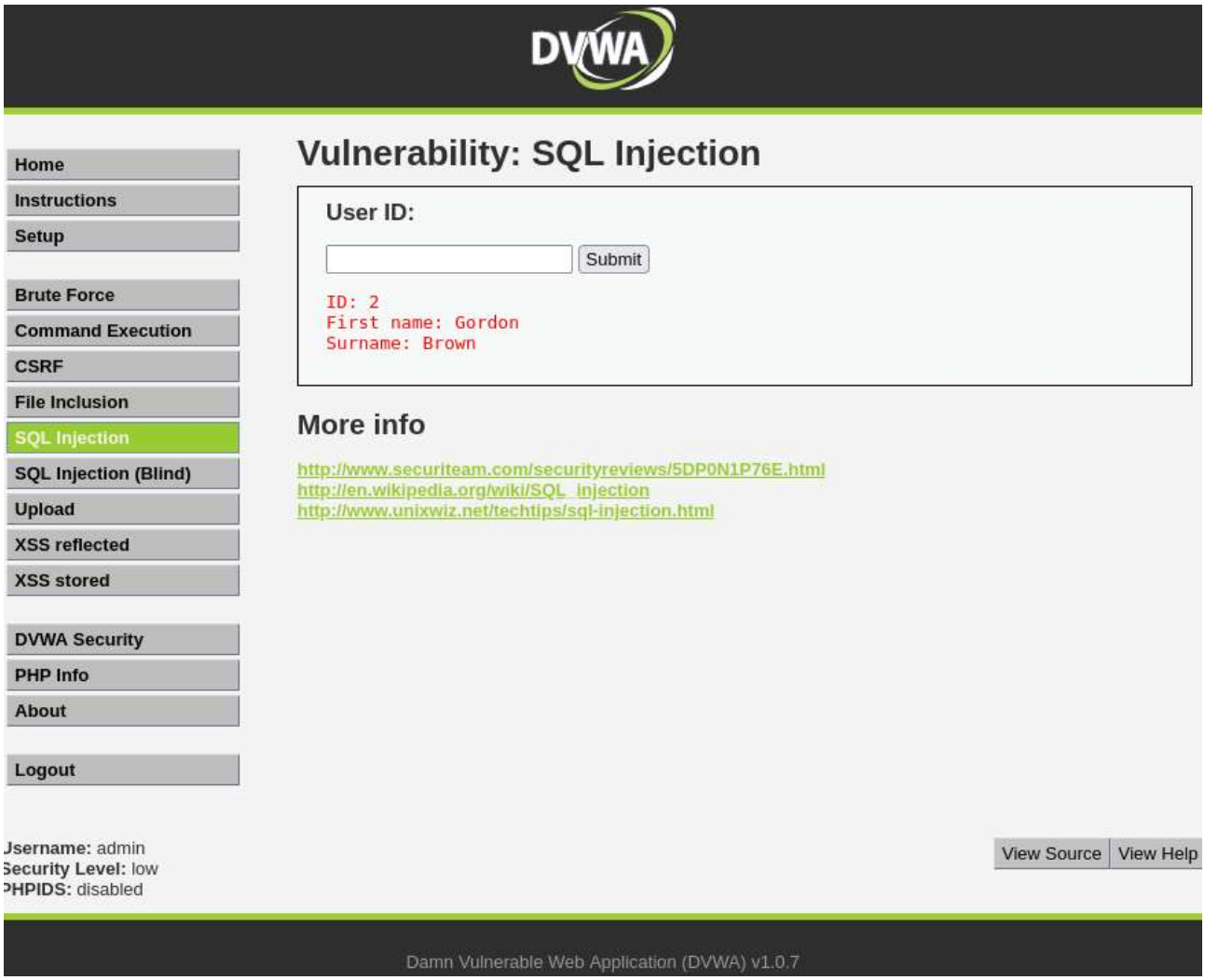
SQL INJECTION:


DVWA
Vulnerability: SQL Injection
User ID:
Submit
More info


DVWA
Vulnerability: SQL Injection
User ID:
Submit
More info


DVWA
Vulnerability: SQL Injection
User ID:
Submit


DVWA
Vulnerability: SQL Injection
User ID:
Submit
More info


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
About
Logout
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
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7