



---

# PUESTA EN PRODUCCIÓN SEGURA

---

Unidad 4. Actividad 14



15 DE FEBRERO DE 2024  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

Enunciado.....	2
Ejercicio.....	2

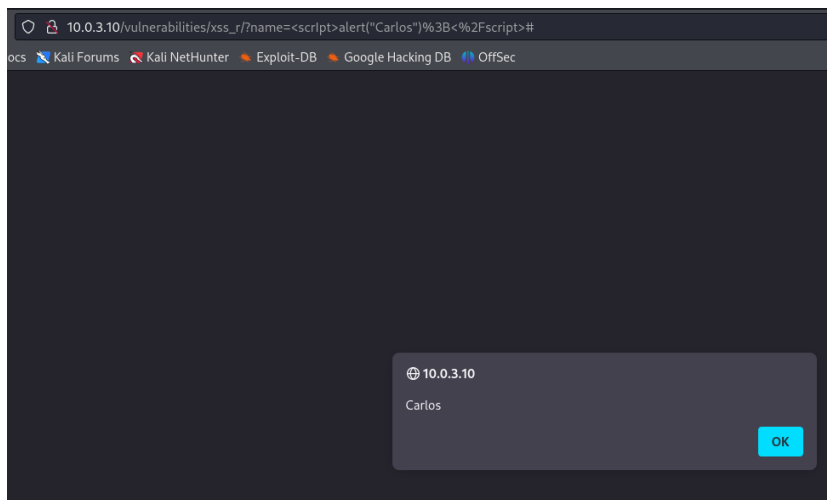
## Enunciado

En la página XSS Reflected, con un nivel de seguridad media, repita los pasos y capture imágenes de los resultados.

## Ejercicio.

## En medio

**<script>alert("Carlos");</script>**



**<img src="" alt="Cuadro" />**

**<IMG SRC="https://4.bp.blogspot.com/-g2ZBNT7yLN8/XI-9Z-pQiPI/AAAAAAAAKyk/8\_1vpw5oczgEVXIKnpGK9NM4GrRWNXAOWCLcBGAs/s1600/Frikis%2Bde%2Blos%2Bordenadores%2Ben%2Blos%2B80%2B6.jpg" />**

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

### 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>

Username: admin

Security Level: medium

View Source

View Help

`<a href="http://iescelia.org">IES Celia</a>`

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello IES Celia

### 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>