

Pentest Web basado en topten de OWASP

[Sun Club](#)[News](#)[Sport](#)[Fabulous](#)

NURSERY HACK Hackers steal pictures, names and address of 8,000 children from nursery chain and post on the dark web

The hackers are attempting to extort money from the nursery

Jordan Farrell

Published: 20:48, 25 Sep 2025 | **Updated:** 1:26, 26 Sep 2025



Método que utilizan los equipos de seguridad para **simular ciberataques** dirigidos contra un sistema basado en web, descubriendo posibles debilidades que un atacante podría **explotar** para robar datos u obtener acceso no autorizado.



Top 10 Vulnerabilities

1 Broken Access Control

10 Server-Side Request Forgery (SSRF)

2 Cryptographic Failures

9 Security Logging and Monitoring Failures

3 Injection

8 Software and Data Integrity Failures

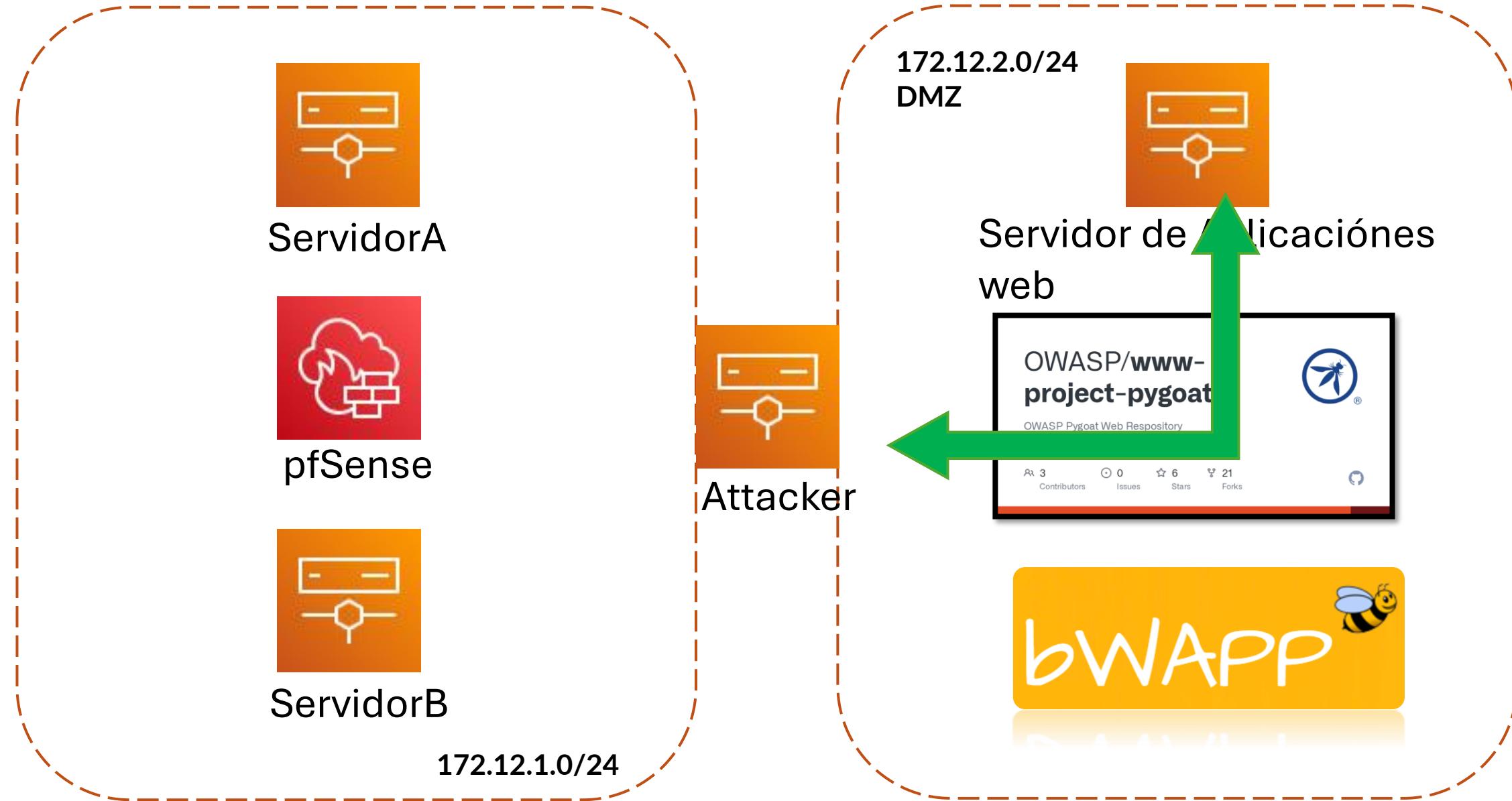
4 Insecure Design

7 Identification and Authentication Failures

5 Security Misconfiguration

6 Vulnerable and Outdated Components

Laboratorio & **Herramientas**



Código

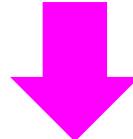
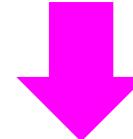
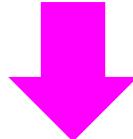
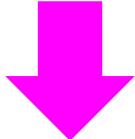
#Instalación

```
git clone  
https://github.com/adeyosemanputra/pygoat  
.git  
docker build -f Dockerfile -t pygoat .  
docker run --rm -p 8000:8000  
pygoat:latest
```

```
#/install.sh
```

1. Mapear el contenido de la aplicación

2. Analizar la aplicación



3 Client-side controls

Logic Flaws 9

4 Authentication

5 session management

Access Controls

7 Fuzz all parameters

Issues with specific functionality 8

10

Shared hosting issues

Test the web server

11

Lógica de la aplicación

Manejo de Acceso

Manejo de Entradas

Hosting de la aplicación

Miscellaneos check

Information Leakage

Recomendaciones para remediación o prevención

- **Implementar una autenticación robusta**
- **Cifrar datos confidenciales en reposo**
- **Utilizar variables de entorno, bóvedas o gestión segura de la configuración**
- **Evitar el acceso directo al almacenamiento o a los recursos a nivel del sistema desde el código orientado al usuario.**

