

Pentest Web basado en top ten de OWASP

THE Sun

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.**

Broken Access Control

1

Server-Side Request
Forgery (SSRF)

10

Cryptographic Failures

2

Security Logging
and Monitoring Failures

9

Injection

3

Software and Data
Integrity Failures

8

Insecure Design

4

Identification and
Authentication Failures

7

Security Misconfiguration

5

Vulnerable and Outdated
Components

6



Laboratorio & Herramientas



ServidorA



pfSense



ServidorB

172.12.1.0/24

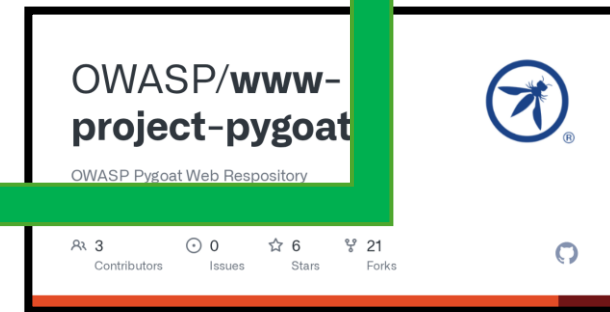


Attacker

172.12.2.0/24
DMZ



Servidor de Aplicaciones
web



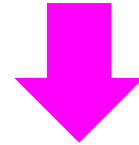
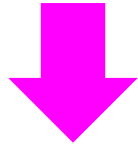
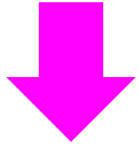
Código

#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

Lógica de la aplicación

4 Authentication

5 session management

Access Controls

Manejo de Acceso

7 Fuzz all parameters

8 Issues with specific functionality

Manejo de Entradas

10 Shared hosting issues

Test the web server

Hosting de la aplicación

Miscellaneous check

Information Leakage

11

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.**

