informe Resultados De Pruebas Seguridad -   
WebGoat

Índice

[0. Registro de Cambios 2](#_Toc77180302)

[1. Objeto 2](#_Toc77180303)

[2. Documentación 2](#_Toc77180304)

[3. Descripción General 2](#_Toc77180305)

[**3.1.** **Entorno** 2](#_Toc77180306)

[**3.2.** **Versiones Probadas** 2](#_Toc77180307)

[**3.3.** **Requisitos** 2](#_Toc77180308)

[**3.4.** **Pruebas Realizadas** 4](#_Toc77180309)

[**3.5.** **Resultado de las pruebas** 4](#_Toc77180310)

[**3.6.** **Conclusiones** 5](#_Toc77180311)

[4. Anexos 6](#_Toc77180312)

# Registro de Cambios

|  |  |  |  |
| --- | --- | --- | --- |
| **Autor (iniciales)** | **Versión** | **Fecha Registro** | **Cambio Realizado respecto a la versión anterior** |
| EJRN | 1 | 03/05/2021 | Versión inicial |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Objeto

Este documento recoge los resultados obtenidos en las pruebas de seguridad que se han llevado a cabo en la aplicación [WebGoat](https://github.com/WebGoat/WebGoat) con el objetivo de verificar que se cumplen los requisitos estipulados en el nivel 2 del [OWASP Application Security Verification Standard](https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf)

# Documentación

* Plan de pruebas de seguridad: [PPR WebGoat - Plan de Pruebas de Seguridad.docx](https://github.com/M0l1n3ta/PFG/blob/master/Reportes/PPR%20-%20Plan%20de%20pruebas/PPR%20WebGoat%20-%20Plan%20Pruebas%20de%20Seguridad.docx)
* Reporte análisis estático de código: [ReporteAnalisisestatico\_WebGoat.docx](https://github.com/M0l1n3ta/PFG/blob/master/Reportes/02%20-%20An%C3%A1lisis%20estatico%20de%20c%C3%B3digo/ReporteAnalisisestatico_WebGoat.docx)
* Reporte análisis dinámico de código: [WebGoat- ReporteAnalisisDinamico.html](https://github.com/M0l1n3ta/PFG/blob/master/Reportes/03%20-%20An%C3%A1lisis%20din%C3%A1mico%20de%20c%C3%B3digo/WebGoat-%20ReporteAnalisisDinamico.html)
* Requisitos de seguridad para la portal eSTILA y web services OWASP Nivel 2: [OWASP Application Security Verification Standard 4.0-en](https://github.com/M0l1n3ta/PFG/blob/master/Reportes/Requisitos%20Seguridad%20-%20OWASP%20ASVS_v4.xlsx)

# Descripción General

## **Entorno**

La aplicación debe estar desplegada en el entorno de pruebas, en nuestro caso se ejecutará a través del siguiente docker compose:

## **Versiones Probadas**

La versión analizada fue la “[vtest10](https://github.com/WebGoat/WebGoat/releases/tag/vtest10)”

## **Requisitos**

Se han establecido los siguientes requisitos de seguridad basados en el Nivel 2 de [OWASP Application Security Verification Standard 4.0](https://github.com/M0l1n3ta/PFG/blob/master/Reportes/Requisitos%20Seguridad%20-%20OWASP%20ASVS_v4.xlsx)

## **Pruebas Realizadas**

Las pruebas se han realizado de forma automática cuando el requisito bajo prueba lo permitía, asistidas con OWASP ZAP o de forma manual si era necesario ampliar la ejecución automática o el requisito no permitía otra opción.

La herramienta utilizada ha sido SonarQube, para los análisis estáticos y AppScan para los análisis dinámicos.

## **Resultado de las pruebas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID defecto** | **Título** | **Severidad** | **Proyecto** | **Estado** |
|  | Credentials should not be hard-coded | Muy Alta | WebGoat | Abierta |
|  | Command-injection | Muy Alta | WebGoat | Abierta |
|  | SQL Injection | Muy Alta | WebGoat | Abierta |
|  | Denial of Service (DOS) | Muy Alta | WebGoat | Abierta |
|  | Weak-cryptography | Muy Alta | WebGoat | Abierta |
|  | Object-injection | Muy Alta | WebGoat | Abierta |
|  | Make sure that environment variables are used safely | Muy Alta | WebGoat | Abierta |
|  | Throwable.printStackTrace(...) should not be called | Alta | WebGoat | Abierta |
|  | Mutable fields should not be "public static" | Alta | WebGoat | Abierta |
|  | Return values should not be ignored when they contain the operation status code. | Alta | WebGoat | Abierta |
|  | XML parsers should not be vulnerable to XXE attacks | Alta | WebGoat | Abierta |
|  | Links with "target=\_blank" should prevent phishing attacks | Alta | WebGoat | Abierta |

## **Conclusiones**

La aplicación WebGoat es una aplicación insegura para poder ponerla en un sistema de producción debe de corregir los errores que se han detectado durante el proceso de pruebas de seguridad ejecutados.

# Anexos

N.A.