informe Resultados De Pruebas Seguridad -   
WebGoat

Índice

[0. Registro de Cambios 2](#_Toc73618711)

[1. Objeto 2](#_Toc73618712)

[2. Documentación 3](#_Toc73618713)

[3. Definiciones 3](#_Toc73618714)

[4. Descripción General 4](#_Toc73618715)

[**4.1.** **Dentro del alcance de las pruebas** 4](#_Toc73618716)

[**4.2.** **Fuera del alcance de las pruebas** 4](#_Toc73618717)

[**4.3.** **Objetivos** 4](#_Toc73618718)

[**4.4.** **Metodología de Pruebas** 5](#_Toc73618719)

[**4.5.** **Prerequisitos** 6](#_Toc73618720)

[4.5.1. Damn Vulnerable Web Application (DVWA) 6](#_Toc73618721)

[5. Herramientas e infraestructura de pruebas 7](#_Toc73618722)

[**5.1.** **Herramientas** 7](#_Toc73618723)

[**5.2.** **Infraestructura de pruebas** 7](#_Toc73618724)

[6. Seguimiento de defectos 7](#_Toc73618725)

[7. Entregables 8](#_Toc73618726)

[**7.1.** **Reporte Análisis estático** 8](#_Toc73618727)

[**7.2.** **Reporte análisis dinámico** 8](#_Toc73618728)

[**7.3.** **Informe resultado ejecución pruebas de seguridad** 8](#_Toc73618729)

# 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)
* 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** |
|  | Se permite la obtención de datos a partir de la modificación de la url de una aplicación | Alta | WebGoat | Abierta |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **Conclusiones**

# Anexos

N.A.