TIPO DE REPORTE

Informe técnico de auditoría web

CLIENTE

Yoseyomo SL

REFERENCIA

EZDAUD25PW0076

CONTACTO

pentest@zerod.io

Atributos del Documento

Nombre del documento	Informe técnico de auditoría web
Referencia del cliente	Yoseyomo SL
Nombre del cliente	Álvaro
Código del documento	EZDAUD25PW0076
Versión	2
Estado	Final
Fecha	Nov 3, 2025
Autor	Zer0D

Tabla de Contenidos

1 - Introducción	4
2 - Información confidencial y propietaria	5
3 - Metodología de pruebas de red y aplicaciones	6
4 - Alcance	8
5 - Manual del usuario	9
6 - Criterio de clasificación de riesgo	11
7 - Resumen ejecutivo	13
8 - Ocurrencias detectadas	14

Introducción

El presente documento muestra los resultados de las pruebas realizadas en el alcance asignado. La información contenida se divide en las siguientes secciones:

• **Introducción:** explicación de la distribución de la información proporcionada en el informe.

• **Información confidencial y propietaria:** en esta sección se detalla el conjunto de consideraciones relativas a la distribución y confidencialidad del documento.

• **Alcance:** en esta sección se detallan los sistemas o aplicaciones Web que han sido auditados y la ventana de tiempo en la que fueron probados.

• **Manual del usuario:** en esta sección se ofrecen un conjunto de recomendaciones a los usuarios para este informe.

• **Criterio de clasificación de riesgos:** explica el criterio de clasificación de riesgos según el estándar CVSS (Common Vulnerability Scoring System) y la clasificación del nivel de severidad.

• **Ocurrencias detectadas:** presenta una lista de vulnerabilidades identificadas en lugares específicos. El concepto de ocurrencia está asociado a un problema de seguridad en una ubicación específica.

• **Vulnerabilidades: descripción y recomendaciones:** contiene una lista de los problemas de seguridad genéricos encontrados en la infraestructura analizada y la información sobre los mismos.

En resumen, este reporte enumera las incidencias de seguridad detectadas, define su nivel de riesgo y propone soluciones que mitigarán o eliminarán el riesgo.

Información Confidencial y Propietaria

La información proporcionada en este documento contiene datos de naturaleza privilegiada y/o confidencial. La copia o divulgación de esta información a cualquier persona u organización que no sean sus destinatarios autorizados está totalmente prohibida, a menos que se realice con la autorización expresa requerida.

Metodología de Pruebas de Red y Aplicaciones

Zer0D utilizó una combinación del Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) v3.0 de ISECOM y la Guía de Pruebas V4 del Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) para llevar a cabo Evaluaciones de Vulnerabilidad y Pruebas de Penetración en la red y aplicaciones basadas en la web.

La prueba de penetración se realizó siguiendo uno de los enfoques de evaluación estándar, en función del nivel de información proporcionada sobre el activo objetivo. En este caso, se aplicó la metodología **Grey Box** alineada con los objetivos de la prueba de penetración.

Los dominios funcionales de OSSTMM en línea con el alcance de este compromiso se enumeran a continuación:

- Recopilación de información y revisión de postura.
- Exploración y enumeración de la eed.
- Verificación de servicios de sistemas y escaneo de puertos.
- Pruebas de aplicaciones.
- Investigación y verificación de vulnerabilidades.

Para la aplicación web y los servicios en línea, la lista de las diez principales de OWASP sirvió como guía y los dominios probados se enumeran a continuación:

- Control de acceso roto.
- Fallos criptográficos.
- Inyección.
- Diseño inseguro.
- Mala configuración de seguridad.
- Componentes vulnerables y desactualizados.
- Fallos en identificación y autenticación.
- Fallos en la integridad del software y los datos.
- Fallos en el registro y monitoreo de seguridad.
- Falsificación de solicitudes del servidor.

El proceso general se puede resumir de la siguiente manera:

Después de definir el alcance y los objetivos, el siguiente paso es recopilar la información necesaria para llevar a cabo la evaluación. Esto implica recoger datos proporcionados por el cliente, realizar un análisis automático de la aplicación, inspeccionar manualmente la aplicación, familiarizarse con las características ofrecidas y buscar inteligencia adicional en fuentes públicas. En esta etapa, nuestro objetivo es obtener la máxima información para identificar vulnerabilidades y priorizar el uso del tiempo o la funcionalidad disponible. El objetivo es identificar todas las vulnerabilidades con un nivel de riesgo elevado en términos de importancia o exposición.

Una vez que hemos reunido toda la información posible sobre la aplicación objetivo, planificamos y realizamos pruebas técnicas para descubrir, identificar y explotar vulnerabilidades.

En la fase de Escaneo de Vulnerabilidades de Aplicaciones Web, se utilizan diversas herramientas automáticas para analizar las posibles vulnerabilidades en la aplicación objetivo. Desplegamos tanto herramientas comerciales de escaneo (Qualys, Acunetix, Netsparker...) como, cuando es posible, herramientas específicas de código abierto y semi-automáticas de Zer0D, dependiendo del entorno en estudio.

La fase siguiente implica una revisión manual de los riesgos típicos en plataformas web, tales como filtraciones de información (contenido no protegido, listado de directorios, listado de contenido, etc.), inyecciones de código (XSS, SQLi, LDAPi, etc.), así como una evaluación del uso adecuado de mecanismos de seguridad (autenticación, gestión de sesiones, SSL, etc.).

Con las vulnerabilidades identificadas en las fases anteriores, procedemos a realizar tareas de análisis e informes. Estas tareas incluyen identificar y descartar falsos positivos/vulnerabilidades irrelevantes para el entorno, explotar vulnerabilidades aplicables (obtención de información, acceso remoto, escalación de privilegios) y, en algunos casos, intentar intrusión en sistemas controlados remotamente.

Alcance

El objetivo de la auditoría es medir el nivel de seguridad de la aplicación web:

URL	**https://dev.inheritans.com**

Limitaciones del alcance

Esta auditoría es un análisis de la seguridad de los sistemas descritos en la sección anterior y en la ventana de tiempo especificada, por lo que Zer0D no es responsable de las implicaciones de seguridad relacionadas con los cambios en el entorno después de la fase de recopilación de datos / pruebas.

Manual de Usuario

Esta sección proporciona un conjunto de indicaciones generales para facilitar la interpretación de este informe.

La información proporcionada en la sección 9 sobre las Ocurrencias Detectadas incluye una tabla que enumera las vulnerabilidades identificadas en lugares específicos. El nombre de la ocurrencia está asociado con un problema de seguridad en un lugar específico.

La información ofrecida en la sección citada para cada una de las ocurrencias es la siguiente:

- **Riesgo:** identifica y describe las posibles consecuencias adversas que podrían surgir de una vulnerabilidad que un atacante pueda explotar o acción insegura. Detalla la gravedad y naturaleza de la amenaza, ayudando a evaluar y priorizar.

- **ID de ocurrencia:** representa un identificador único para cada ocurrencia. Este identificador permite al usuario monitorear esta ocurrencia a lo largo del tiempo.

- **Tipo de vulnerabilidad:** refleja el problema de seguridad en el que se incluye la ocurrencia. La sección 9, Ocurrencias Detectadas, incluye una descripción general del problema de seguridad y un conjunto de recomendaciones generales destinadas a corregir la vulnerabilidad. Cuando corresponda, estas recomendaciones se complementarán en la sección que describe la ocurrencia.

- **Base CVSS:** en esta sección se incluye la información relacionada con el riesgo basado en el estándar CVSS. Utilizamos estas tres métricas: riesgo base, riesgo que variará según el tiempo y riesgo asociado al entorno. El detalle sobre el uso de CVSS y cómo afecta al presente informe se muestra en la sección 6.

- **Descripción:** el segmento de descripción de cada ocurrencia presenta la información específica sobre el problema detectado en un lugar específico. La descripción incluye toda la información relacionada con el problema específico. Si se necesita alguna indicación particular sobre su corrección, también se incluirá aquí.

- **Referencias:** esta sección incluye, cuando sea necesario, una serie de enlaces web donde se puede encontrar información adicional que ayudará a complementar la información presentada sobre la ocurrencia.

- **Evidencias:** cuando sea necesario, se incluirán una o más capturas de pantalla u otro tipo de documento, que se ofrecerán como evidencia gráfica del problema identificado; si no se requiere tal evidencia, no se incluirá en esta sección de la ocurrencia.

Criterio de Clasificación de Riesgo

Al clasificar las vulnerabilidades detectadas, se considera la versión 3.0 del CVSS (Sistema Común de Puntuación de Vulnerabilidades).

La dirección del sitio web oficial del estándar es: **https://www.first.org/cvss/calculator/3.0**

Los siguientes párrafos proporcionan un breve resumen del estándar y cómo afecta la evaluación de riesgos reflejada en este documento:

CVSS se compone de un conjunto de tres grupos de métricas: Base, Temporal y Entorno. Cada uno de estos grupos está compuesto por un grupo de métricas:

- **Base:** representa las características fundamentales e intrínsecas de una vulnerabilidad, características que son constantes en el tiempo y en el entorno del usuario; comprenden:
  - o Vector de Acceso: Local, Red Adyacente o Red
  - o Complejidad de Acceso: Alta, Media o Baja
  - o Autenticación: Múltiple, Única o Ninguna
  - o Impacto en Confidencialidad, Integridad y Disponibilidad: Cómo la vulnerabilidad afecta cada uno de estos aspectos, expresado en los siguientes valores: Completo, Parcial o Ninguno.
  - o Balance de Impacto: Esta métrica nos permite dar mayor énfasis a uno de los aspectos del impacto. Sus valores pueden incluir Confidencialidad, Integridad, Disponibilidad o Normal; el valor Normal se utiliza cuando el impacto es igual en importancia en los tres aspectos.
- **Temporal:** representa las características de una vulnerabilidad que cambian con el tiempo pero que no se ven afectadas por cambios en el entorno del usuario. Está compuesto por:
  - o Explotabilidad: No Comprobada, Prueba de Concepto, Funcional, Alta o No Definida
  - o Nivel de Solución: Oficial, Temporal, Alternativa, No Disponible o No Definida
  - o Fiabilidad de la Detección: No Confirmada, No Corroborada, Confirmada o No Definida
- **Entorno:** este grupo de métricas comprende las características de la vulnerabilidad que son importantes y únicas en un entorno de usuario específico. Está compuesto por:

o Potencial de Daño Colateral: Ninguno, Bajo, Bajo-Medio, Medio-Alto, Alto o No Definido

o Objetivo de Distribución: Ninguno, Bajo, Medio, Alto o No Definido, relacionado con los requisitos de Confidencialidad, Integridad y Disponibilidad.

Al combinar este conjunto de métricas, se obtienen una serie de valores que dan lugar a los valores finales de Riesgo Base, Riesgo Temporal y Riesgo Ambiental.

Zer0D proporciona clasificaciones de severidad de "Informativo", "Bajo", "Medio", "Alto" y "Crítico" además de las puntuaciones numéricas del CVSS, estas métricas están en consonancia con NIST NVD.

Las clasificaciones cualitativas simplemente se mapean a partir de las puntuaciones numéricas de CVSS:

- Las vulnerabilidades se etiquetan con severidad "Informativo" si tienen una puntuación base de CVSS de 0.0.
- Las vulnerabilidades se etiquetan con severidad "Bajo" si tienen una puntuación base de CVSS de 0.1-3.9.
- Las vulnerabilidades se etiquetarán con severidad "Medio" si tienen una puntuación base de CVSS de 4.0-6.9.
- Las vulnerabilidades se etiquetarán con severidad "Alto" si tienen una puntuación base de CVSS de 7.0-8.9.
- Las vulnerabilidades se etiquetarán con severidad "Crítico" si tienen una puntuación base de CVSS de 9.0-10.0.

Resumen Ejecutivo

El nivel de seguridad de esta aplicación es Suficiente

El nivel de seguridad de esta aplicación es **Suficiente** para garantizar la confidencialidad, disponibilidad e integridad de los datos. Existen algunas vulnerabilidades que a largo plazo pueden provocar impactos en el portal.

Se han identificado **0** vulnerabilidades distribuidas de la siguiente manera:

- **0** vulnerabilidades asociadas a un riesgo crítico.
- **0** vulnerabilidades asociadas a un riesgo alto.
- **0** vulnerabilidades asociadas a un riesgo medio.
- **0** vulnerabilidades asociadas a un riesgo bajo.
- **0** vulnerabilidades asociadas a un riesgo informativo.

Métricas del proyecto

Durante el proyecto se midieron tres indicadores clave de desempeño:

- **TTK (Tiempo hasta el inicio):** Las pruebas comenzaron el Oct 18, 2025, la misma fecha de autorización del cliente.
- **TTFF (Tiempo hasta la primera vulnerabilidad):** La primera vulnerabilidad se identificó el Invalid Date.
- **TTR (Tiempo hasta el informe):** El informe final se entregó el Oct 31, 2025.

Ocurrencias Detectadas

Hasta el momento, no se han identificado vulnerabilidades abiertas o sin resolver. Todos los hallazgos se han abordado o mitigado según el plan de remediación.