



Informe Técnico-Ejecutivo

Empresa **NOMBRE EMPRESA
AUDITADA**

LOGO EMPRESA
AUDITADA

Este documento es confidencial y contiene información sensible.
No debería ser impreso o compartido con terceras entidades.

[Fecha Auditoría]

Índice

1. Antecedentes	2
2. Objetivos	2
2.1. Alcance	2
2.2. Impedimentos y Limitaciones	2
3. Resumen Ejecutivo	3
4. Resultados Obtenidos	4
4.1. Objetivo 1 - [DIRECCIÓN URL DEL OBEJTIVO 1]	4
4.2. Objetivo 2 - https://ejemplo.com	4
4.3. Objetivo 3 - https://subdominio.ejemplo.com	5
5. Tabla de Criticidad	6
6. Conclusiones	7

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría a la empresa **NOMBRE EMPRESA AUDITADA**, dedicada a [DEDICACIÓN DE LA EMPRESA].

Durante las pruebas se simulan las actividades que realizaría un atacante real, descubriendo las vulnerabilidades, su nivel de riesgo, y generando recomendaciones que permitan al cliente realizar la remediación de estas. En cada sección de este informe se detallan los aspectos importantes de la forma en que un atacante podría utilizar la vulnerabilidad para comprometer y obtener acceso no autorizado a información sensible. Se incluyen además directrices que al ser aplicadas mejoraran los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

Dirección URL

Dirección URL de Partida

[INSERTAR IMAGEN]

2. Objetivos

Los objetivos de la presente auditoría de seguridad se enfocan, primeramente, en la identificación de posibles vulnerabilidades y debilidades de la página web de la empresa **NOMBRE EMPRESA AUDITADA** para su posterior explotación, con el propósito de garantizar la integridad y confidencialidad de la información almacenada en él.

[AÑADIR INFORMACIÓN ADICIONAL SI ES NECESARIO]

2.1. Alcance

La evaluación se ha centrado en los siguientes objetivos establecidos en el alcance. Aquí quedan representados los **dominios, subdominios y enpoints** que han conllevado alguna incidencia en la auditoría:

Nº	Objetivo
Cliente	NOMBRE EMPRESA AUDITADA
1	[DIRECCIÓN IP]
2	ejemplo.com
3	subdominio.ejemplo.com

Cuadro 1: Definición del Alcance y Objetivos de la auditoría

2.2. Impedimentos y Limitaciones

Aquí quedan reflejados los impedimentos y limitaciones que deberá llevar la auditoría. Todas las acciones aquí especificadas están **totalmente prohibidas llevarlas a cabo bajo ningún concepto**:

- **Impedimento 1**
- **Impedimento 2**
- **Impedimento 3**

3. Resumen Ejecutivo

Este es un resumen ejecutivo de manera general donde se pueden observar mediante tablas y gráficos las vulnerabilidades y problemas encontrados junto con su severidad durante la auditoría.

Al final de este documento se han especificado las **Contramedidas** a llevar a cabo para la mitigación de estas vulnerabilidades.

[AÑADIR INFORMACIÓN ADICIONAL SI ES NECESARIO]

Vulnerabilidad	Severidad
SQL Injection en login	Crítica
XSS Reflejado	Alta
Credenciales por defecto	Alta
Enumeración de usuarios	Media
Información sensible expuesta	Baja

Cuadro: Resumen de Vulnerabilidades

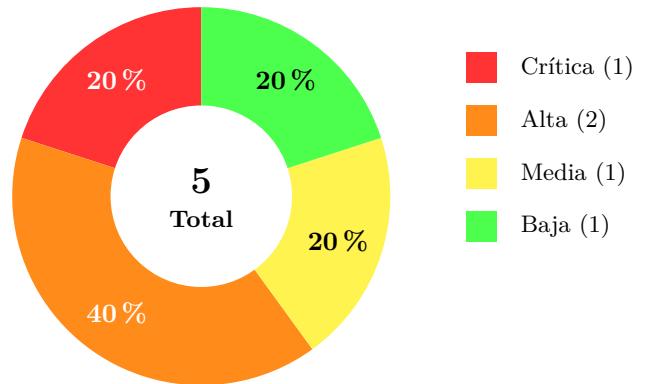


Imagen: Distribución de Vulnerabilidades

4. Resultados Obtenidos

En este apartado se documentan los resultados de las pruebas llevadas a cabo en los diferentes objetivos establecidos más arriba.

Se reflejan los pasos ejecutados en cada objetivo, además de una descripción de la vulnerabilidad encontrada junto con su nivel de criticidad.

4.1. Objetivo 1 - [DIRECCIÓN URL DEL OBJETIVO 1]

Vulnerabilidad: [VULNERABILIDAD]

Criticidad: Alta

Descripción

[DESCRIPCIÓN DE LA VULNERABILIDAD]

Estas son las pruebas realizadas:

[WRITE UP DE LA EXPLOTACIÓN DE LA VULNERABILIDAD]

Recomendaciones y Contramedidas: [RECOMENDACIONES QUE ARREGLEN LA VULNERABILIDAD ENCONTRADA]

4.2. Objetivo 2 - <https://ejemplo.com>

Vulnerabilidad: XSS Almacenado

Criticidad: Alta

Descripción

El **Cross-Site Scripting (XSS) Almacenado**, también conocido como **Stored XSS o Persistent XSS**, es una vulnerabilidad de seguridad web que ocurre cuando una aplicación permite almacenar datos maliciosos proporcionados por un usuario y posteriormente los muestra a otros usuarios sin realizar una correcta validación o sanitización.

A diferencia del **XSS reflejado**, el payload malicioso no se envía directamente en la petición y respuesta inmediata, sino que queda persistido en el servidor (por ejemplo, en una base de datos, sistema de comentarios, perfiles de usuario o foros). Cuando otro usuario accede al contenido afectado, el navegador ejecuta automáticamente el código malicioso.

Estas son las pruebas realizadas:

[WRITE UP DE LA EXPLOTACIÓN DE LA VULNERABILIDAD]

Recomendaciones y Contramedidas: [RECOMENDACIONES QUE ARREGLEN LA VULNERABILIDAD ENCONTRADA]

4.3. Objetivo 3 - <https://subdominio.ejemplo.com>

Vulnerabilidad: CSRF (Cross-Site Request Forgery)

Criticidad: Alta

Descripción

El **Cross-Site Request Forgery (CSRF)**, o falsificación de petición en sitios cruzados, es una vulnerabilidad que permite a un atacante inducir a un usuario autenticado a realizar acciones no deseadas en una aplicación web en la que tiene sesión activa.

Esta vulnerabilidad se produce cuando una aplicación no verifica adecuadamente que una solicitud enviada al servidor ha sido iniciada de forma legítima por el propio usuario, sino que confía únicamente en el hecho de que la petición incluye las credenciales de sesión válidas (como cookies).

Estas son las pruebas realizadas:

[WRITE UP DE LA EXPLOTACIÓN DE LA VULNERABILIDAD]

Recomendaciones y Contramedidas: [RECOMENDACIONES QUE ARREGLEN LA VULNERABILIDAD ENCONTRADA]

5. Tabla de Criticidad

En la siguiente tabla se ven reflejadas las diferentes vulnerabilidades encontradas junto con su **Nivel de Criticidad y Puntuación CVSS**

ID	Vulnerabilidad	Severidad	CVSS	Estado
V-01	SQL Injection en login	Crítica	9.8	Abierta
V-02	XSS Reflejado	Alta	7.4	Abierta
V-03	Credenciales por defecto	Alta	8.1	Abierta
V-04	Enumeración de usuarios	Media	5.3	Abierta
V-05	Información sensible expuesta	Baja	3.1	Abierta

Cuadro 2: Resumen de Vulnerabilidades Identificadas

Definición

La **puntuación CVSS (Common Vulnerability Scoring System)** es un estándar abierto y marco de referencia utilizado en ciberseguridad para calificar la gravedad de las vulnerabilidades de software y hardware, asignándoles un valor numérico del 1 al 10. Ayuda a priorizar la respuesta ante amenazas, clasificándolas en niveles bajo, medio, alto o crítico.

6. Conclusiones

[REDACCIÓN DE LAS CONCLUSIONES DE LA AUDITORÍA LLEVADA A CABO]