

***Informe de Auditoría de Seguridad***

http://example.com

***Grupo COFARES***

*Versión: 1.1*

23/04/2025

|  |  |  |  |
| --- | --- | --- | --- |
| **Título** | **Informe de Auditoría de Seguridad** | | |
| **Elaborado** | Ciberseguridad | | |
| **Responsable** | Pedro Iván Montes | | |
| **Fecha de elaboración** | 23/04/2025 | | |
| **Metodología** | OWASP | | |
| Control de Versiones | | | |
| **Ver.** | **Fecha** | **Autor** | **Modificaciones** |
| 1.0 | 23/04/2025 | Ciberseguridad | Creación de informe |

**Índice**

[1. Alcance 3](#_p4oemcyod1zt)

[2. Metodología 3](#_dacxzmujloap)

[3. Resumen Ejecutivo 4](#_1as8lml38neq)

[4. Resumen de vulnerabilidades 5](#_hhrdc86cfmqi)

[5. Análisis de Vulnerabilidades 6](#_8w3sct9ttwb9)

[6. Checklist Requerimientos de Seguridad Web 14](#_zfy2iuy1adz0)

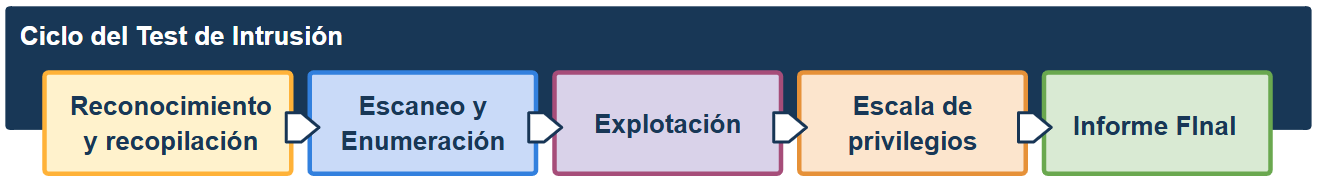
|  |
| --- |
| **1. Alcance** |

La presente auditoría tiene como alcance la evaluación de vulnerabilidades y requisitos de seguridad de la plataforma web http://example.com. Con el objetivo de no causar interrupciones de servicio en la plataforma de producción, la auditoría se ha llevado a cabo en el entorno de preproducción que corresponde con http://example.com

Se ha seguido una modalidad de auditoría de caja gris, en la que se ha facilitado información acerca de los activos a auditar incluyendo información técnica, servicios instalados, usuarios y contraseñas para acceder a la plataforma.

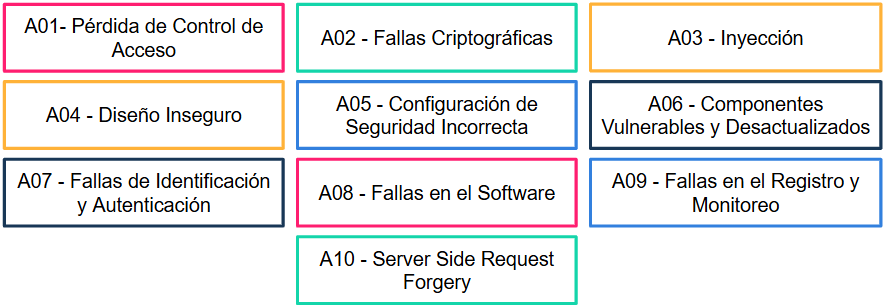
|  |
| --- |
| **2. Metodología** |

Las acciones y tareas realizadas en la auditoría se han llevado a cabo siguiendo una metodología propia de un ciclo de test de intrusión, junto con la metodología de auditoría web dictada por el estándar de seguridad OWASP, siguiendo las siguientes fases y actividades:



Adicionalmente, se han llevado a cabo pruebas manuales para identificar problemas de flujo de datos, lógica empresarial y control de acceso, todo ello recogido en el checklist de requerimientos de seguridad web.

En cuanto a la metodología OWASP, se ha clasificado las vulnerabilidades siguiendo la guía OWASP Top 10, en las que se enumeran los riesgos más críticos para la seguridad de las aplicaciones web:



Adicionalmente, para cada vulnerabilidad identificada se ha detallado proporcionando las evidencias correspondientes, el riesgo que supone, propuestas de solución y/o mitigación y enlaces de interés; junto con la calificación de la criticidad del impacto de la vulnerabilidad siguiendo la siguiente tabla:

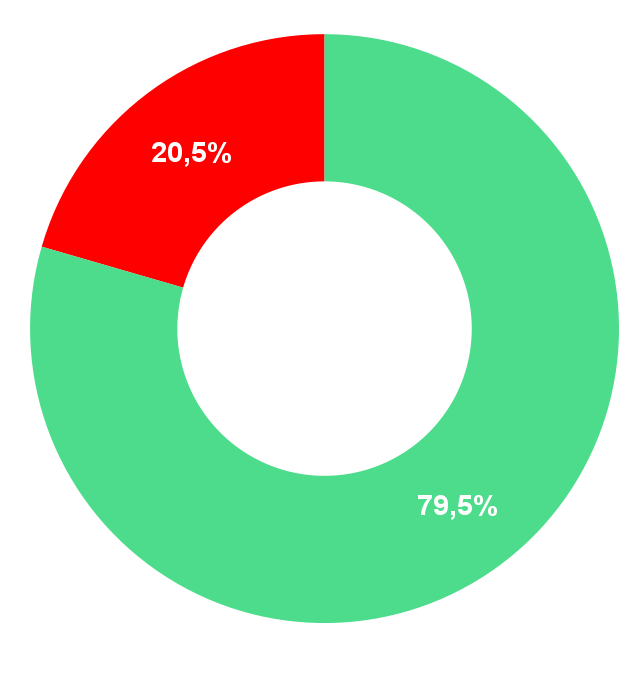
|  |  |
| --- | --- |
| **Impacto** | **Definición** |
| **Alta** | Vulnerabilidad crítica que permite comprometer completamente el sistema, acceder a datos sensibles, realizar cambios no autorizados o interrumpir servicios esenciales. |
| **Media** | Vulnerabilidad significativa que puede ser explotada para obtener ventajas parciales o causar daños moderados. |
| **Baja** | Vulnerabilidad de bajo riesgo que puede ser explotada, pero requiere condiciones muy específicas o tiene un impacto limitado. |
| **Informativa** | Hallazgos que no representan una amenaza directa, pero pueden proporcionar información útil para un atacante o ser considerados buenas prácticas de remediación. |

|  |
| --- |
| **3. Resumen Ejecutivo** |

La auditoría de seguridad en example.com reveló áreas de mejora en la protección del sitio web. Se detectaron vulnerabilidades relacionadas con la configuración de las cabeceras HTTP, lo que podría exponer a los usuarios a ataques. Específicamente, la ausencia de una cabecera Content Security Policy (CSP) dificulta la protección contra ataques de cross-site scripting (XSS), donde un atacante podría inyectar código malicioso en el sitio y afectar a los usuarios.  
  
La falta de una cabecera Anti-Clickjacking incrementa el riesgo de que los usuarios sean engañados para realizar acciones no deseadas, como hacer clic en enlaces o botones maliciosos sin saberlo. Adicionalmente, la ausencia del encabezado X-Content-Type-Options podría permitir que el navegador interprete incorrectamente los archivos, lo que también facilitaría ataques.  
  
Para mitigar estos riesgos, se recomienda implementar las cabeceras HTTP faltantes. Al hacerlo, se fortalecerá significativamente la seguridad del sitio web y se protegerá mejor a los usuarios contra posibles ataques. La implementación de estas cabeceras es un paso fundamental para mejorar la postura de seguridad general del sitio.

|  |
| --- |
| **4. Resumen de vulnerabilidades** |
|  |

**Evaluación de Requerimientos de Seguridad Web**

**Cumple / No cumple**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerabilidad** | **Nº Alertas** | **Categoría**  **OWASP** | **Criticidad** | **Estado** |
| [VUL 01] Cabecera Content Security Policy (CSP) no configurada | 1 | A05 | Medio | Detectada |
| [VUL 02] Falta de cabecera Anti-Clickjacking | 1 | A05 | Medio | Detectada |
| [VUL 03] Falta encabezado X-Content-Type-Options | 1 | A05 | Bajo | Detectada |

|  |
| --- |
| **5. Análisis de Vulnerabilidades** |
| A continuación, se detallan las vulnerabilidades identificadas durante la auditoría de seguridad. Para cada vulnerabilidad, se incluye una descripción del problema, el riesgo asociado, así como recomendaciones y medidas correctoras. Además, se proporcionan enlaces de interés con recursos adicionales que permiten profundizar en la comprensión de cada vulnerabilidad y en las mejores prácticas para su remediación. |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-01] Cabecera Content Security Policy (CSP) no configurada** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 693 | http://example.com |
| **Detalles** |  | | |
| La falta de configuración del encabezado Content Security Policy (CSP) expone a la aplicación a ataques XSS e inyección de datos. CSP define las fuentes de contenido válidas (scripts, CSS, imágenes, etc.) que el navegador puede cargar, mitigando la ejecución de código malicioso proveniente de fuentes no confiables y reduciendo el riesgo de robo de datos y malware. | | | |
| **Riesgo** |  | | |
| La ausencia de CSP permite a los atacantes inyectar código malicioso en el sitio web, comprometiendo la integridad de la aplicación y la seguridad de los usuarios. Esto puede resultar en el robo de credenciales, la desfiguración del sitio web, la redirección a sitios maliciosos y la propagación de malware, dañando la reputación y generando pérdidas económicas. | | | |
| **Solución** |  | | |
| Implementar una política CSP robusta y restrictiva, definiendo explícitamente las fuentes de contenido permitidas para cada tipo de recurso. Validar y probar la política CSP en un entorno de pruebas antes de implementarla en producción. Monitorear y actualizar la política CSP regularmente para adaptarse a las necesidades cambiantes de la aplicación y abordar nuevas vulnerabilidades. | | | |
| **Referencias** |  | | |
| <p>https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\_Content\_Security\_Policy</p><p>https://cheatsheetseries.owasp.org/cheatsheets/Content\_Security\_Policy\_Cheat\_Sheet.html</p><p>https://www.w3.org/TR/CSP/</p><p>https://w3c.github.io/webappsec-csp/</p><p>https://web.dev/articles/csp</p><p>https://caniuse.com/#feat=contentsecuritypolicy</p><p>https://content-security-policy.com/</p> | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-02] Falta de cabecera Anti-Clickjacking** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | http://example.com |
| **Detalles** |  | | |
| La alerta notifica la ausencia de medidas de protección contra ataques de Clickjacking. La falta de cabeceras HTTP como Content-Security-Policy (con la directiva 'frame-ancestors') o X-Frame-Options permite que un atacante encubra un sitio web legítimo dentro de un iframe, engañando a los usuarios para que realicen acciones no deseadas. Esto compromete la integridad de la interfaz de usuario. | | | |
| **Riesgo** |  | | |
| El principal riesgo es el Clickjacking, donde un atacante superpone capas invisibles sobre una página web legítima para engañar a los usuarios y hacer que realicen acciones sin su consentimiento, como cambiar contraseñas, realizar transacciones o revelar información confidencial. Esto puede resultar en robo de identidad, pérdidas financieras y daño a la reputación de la organización. | | | |
| **Solución** |  | | |
| Implementar la cabecera Content-Security-Policy (CSP) con la directiva 'frame-ancestors' para especificar los dominios que pueden incrustar la página en un iframe. Como alternativa, utilizar la cabecera X-Frame-Options con valores como 'DENY' o 'SAMEORIGIN'. Validar que la configuración se aplica correctamente y que no interfiere con la funcionalidad legítima de la aplicación. | | | |
| **Referencias** |  | | |
| <p>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</p> | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-03] Falta encabezado X-Content-Type-Options** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Bajo** | A05 | 693 | http://example.com |
| **Detalles** |  | | |
| La alerta indica la ausencia del encabezado 'X-Content-Type-Options: nosniff' en la respuesta HTTP. Este encabezado previene que navegadores como Internet Explorer y Chrome realicen 'MIME-sniffing', una técnica que intenta adivinar el tipo de contenido de un archivo basándose en su contenido en lugar de en la cabecera 'Content-Type'. Su ausencia puede llevar a interpretaciones erróneas del contenido. | | | |
| **Riesgo** |  | | |
| La principal vulnerabilidad es la posibilidad de que el navegador interprete incorrectamente el contenido, lo que podría permitir la ejecución de código malicioso disfrazado de un tipo de archivo diferente. Por ejemplo, un archivo HTML malicioso podría ser interpretado como una imagen, llevando a un ataque de Cross-Site Scripting (XSS) si se incluye código JavaScript. | | | |
| **Solución** |  | | |
| La solución consiste en configurar el servidor web para que incluya el encabezado 'X-Content-Type-Options: nosniff' en todas las respuestas HTTP. Esto indica al navegador que debe confiar únicamente en la cabecera 'Content-Type' proporcionada por el servidor y evitar el 'MIME-sniffing'. La configuración específica dependerá del tipo de servidor web utilizado (Apache, Nginx, IIS, etc.). | | | |
| **Referencias** |  | | |
| <p>https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</p><p>https://owasp.org/www-community/Security\_Headers</p> | | | |

|  |
| --- |
| **6. Checklist Requerimientos de Seguridad Web** |

En este apartado se detalla un checklist de requerimientos que contempla los principales controles y buenas prácticas que deben ser evaluados para garantizar un entorno seguro y robusto frente a posibles amenazas.

Se estructura en categorías clave que cubren aspectos críticos de la aplicación, tales como el control de acceso y autenticación, la gestión de sesiones y cookies, la configuración adecuada de cabeceras HTTP, el manejo seguro de transacciones y entradas de datos, así como mecanismos de protección activa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Tipo**  **Requerimiento** | **Requisito de Seguridad** | **Cumple** | **Criticidad** |
| 1 | **Control de acceso y autenticación** | Autenticación total para todos los recursos/páginas | **SI** | **Baja** |
| Es necesario estar autenticado para acceder a cada uno de los recursos y/o página de la plataforma. | | |
| 2 | Doble verificación para el registro o alta | **SI** | **Media** |
| Se solicita un código OTP en el primer inicio de sesión tras el registro de un nuevo usuario. | | |
| 3 | Política de complejidad de contraseña | **SI** | **Alta** |
| La política de contraseña establecida es: 5-8 caracteres de longitud, donde se debe incluir como mínimo una letra mayúscula, una letra minúscula y un número. | | |
| 4 | Renovación periódica de contraseña | **NO** | **Media** |
| No hay un mecanismo para la renovación periódica de contraseñas. | | |
| 5 | Autenticación Multifactor opcional para cuentas de usuarios | **NO** | **Media** |
| No existe autenticación multifactor para el inicio de sesión de los usuarios en la plataforma. | | |
| 6 | Autenticación Multifactor para cuentas administrador | **NO** | **Crítica** |
| No existe autenticación multifactor para el inicio de sesión de los administradores en la plataforma. | | |
| 7 | Autenticación Multifactor en zonas con información sensible o datos bancarios | **SI** | **Crítica** |
| transferencias, reseteo. consulta. | | |
| 8 | Mecanismo Captcha para la autenticación | **SI** | **Baja** |
| En caso de introducir incorrectamente la contraseña, en el siguiente inicio de sesión se solicita completar un mecanismo captcha. | | |
| 9 | Mecanismo Captcha para el registro/alta | **SI** | **Baja** |
| El registro debe validarse mediante el envío de un código OTP. | | |
| 10 | Bloqueo de cuenta tras intentos fallidos | **SI** | **Media** |
| Se ha comprobado que tras varios intentos fallidos de autenticación, la cuenta de usuario es bloqueada. | | |
| 11 | Función de recordatorio/olvido de contraseña válido | **SI** | **Media** |
| El mecanismo de reseteo de contraseña es lo suficientemente seguro, incluyendo un mecanismo multifactor de autenticación OTP para validar la acción. | | |
| 12 | Doble verificación para el cambio/reseteo de contraseña | **SI** | **Alta** |
| Se solicita un código OTP para validar el cambio/reseteo de contraseña. | | |
| 13 | Contraseña temporal o link temporal para el cambio de contraseña | **N/A** | **Alta** |
| No aplica. El cambio de contraseña se lleva a cabo en el mismo portal de Sección de Crédito tras ser validado por el código OTP. | | |
| 14 | Histórico de 3 o más contraseñas para el cambio/reseteo de contraseña | **NO** | **Media** |
| Únicamente te prohíbe establecer la misma contraseña igual a la última. | | |
| 15 | Respuestas de error genéricas en la autenticación | **SI** | **Baja** |
| La respuesta de error tras un intento de inicio de sesión fallido es genérica. *“La autenticación ha fallado. Por favor inténtelo otra vez”* | | |
| 16 | Respuestas de error genéricas en el servicio de cambio de contraseña | **SI** | **Baja** |
|  | | |
| 17 | Almacenamiento y cifrado seguro de contraseñas | **SI** | **Media** |
|  | | |
| 18 | Registro de eventos de seguridad | **SI** | **Media** |
|  | | |
| 19 | **Gestión de sesión y cookies** | El cierre de sesión termina con la sesión/conexión asociada | **SI** | **Alta** |
| Se ha comprobado que el cierre de sesión se completa correctamente y la sesión se destruye. | | |
| 20 | Tiempo de vida de sesión | **SI** | **Media** |
|  | | |
| 21 | Cierre de sesión automático tras expiración de sesión | **SI** | **Media** |
|  | | |
| 22 | Generación de nuevos identificadores por sesión | **SI** | **Baja** |
|  | | |
| 23 | Tokens CSRF | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-03]. | | |
| 24 | No existe información sensible o confidencial en cookies | **SI** | **Baja** |
|  | | |
| 25 | Cookies con atributo Secure configurado | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-04]. | | |
| 26 | Cookies con atributo HttpOnly configurado | **SI** | **Baja** |
|  | | |
| 27 | Cookies con attribute SameSite Flag | **NO** | **Baja** |
| Se detalla en la vulnerabilidad [VULN-05]. | | |
| 28 | **Gestión y configuración de cabeceras HTTP** | HTTP Strict Transport Security (HSTS) | **SI** | **Baja** |
|  | | |
| 29 | X-XSS-Protection | **NO** | **Media** |
| Se detalla en la vulnerabilidad [VULN-01] | | |
| 30 | X-Content-Type-Options | **SI** | **Baja** |
|  | | |
| 31 | X-Frame-Options | **SI** | **Media** |
|  | | |
| 32 | Content Security Policy (CSP) | **SI** | **Baja** |
|  | | |
| 33 | Cache Control | **SI** | **Baja** |
|  | | |
| 34 | Cross-Origin-Resource-Policy (CORP) | **SI** | **Baja** |
|  | | |
| 35 | **Transacción y entrada de datos** | Protocolo HTTPS TLS seguro (TLSv1.3 o TLSv1.2) | **SI** | **Alta** |
| https://www.ssllabs.com/analyze.html?d=sdc30.cofares.es&latest | | |
| 36 | Certificado SSL válido y bien configurado | **SI** | **Media** |
| La calificación otorgada por el escaner ssllabs es de A+. | | |
| 37 | Validación de entrada de datos | **SI** | **Media** |
| Parcialmente. Revisar vulnerabilidad [VULN-01] | | |
| 38 | Validación de subida/carga de ficheros | **N/C** | **Media** |
| No existe la carga o subida de ficheros a la plataforma. | | |
| 39 | Mensaje de error tras la entrada de datos ilegítimas o malformadas | **SI** | **Baja** |
|  | | |
| 40 | Límite de transacciones/peticiones en un periodo de tiempo | **SI** | **Media** |
| Es posible configurar un límite de transacciones web por usuario. | | |
| 42 | **Protección Activa** | Protección WAF | **SI** | **Media** |
|  | | |