

***Informe de Auditoría de Seguridad***

http://example.com

***Grupo COFARES***

*Versión: 1.1*

16/04/2025

|  |  |  |  |
| --- | --- | --- | --- |
| **Título** | **Informe de Auditoría de Seguridad** | | |
| **Elaborado** | Ciberseguridad | | |
| **Responsable** | Pedro Iván Montes | | |
| **Fecha de elaboración** | 16/04/2025 | | |
| **Metodología** | OWASP | | |
| Control de Versiones | | | |
| **Ver.** | **Fecha** | **Autor** | **Modificaciones** |
| 1.0 | 16/04/2025 | 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)

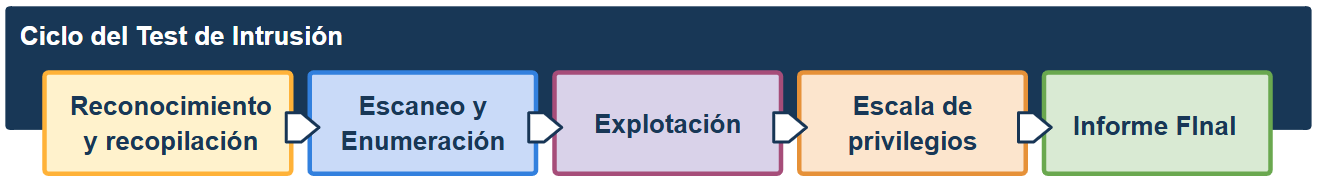
|  |
| --- |
| **1. Alcance** |

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.

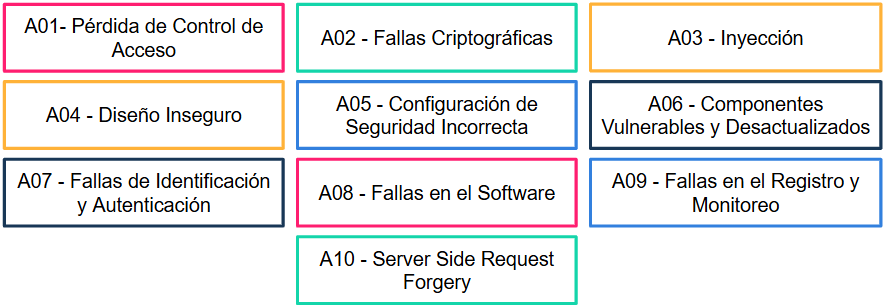
|  |
| --- |
| **2. Metodología** |

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:

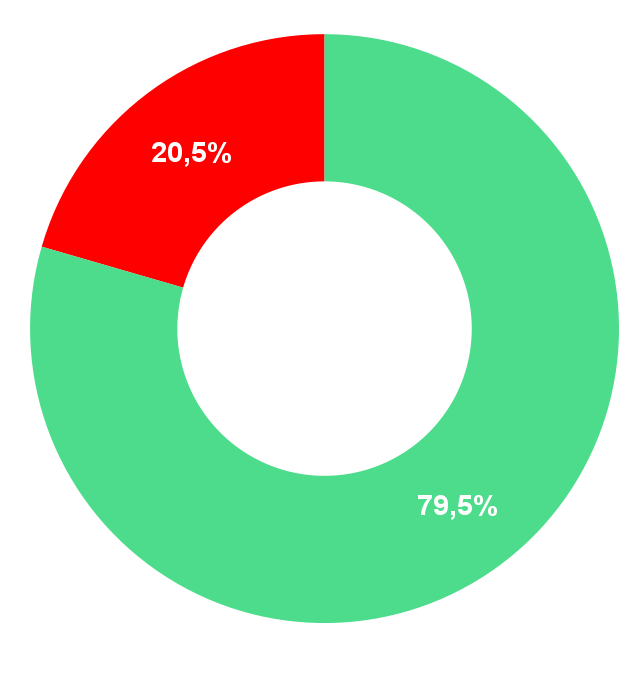
|  |  |
| --- | --- |
| **Impacto** | **Definición** |
| **Alta** | Vulnerabilidad crítica que permite comprometer completamente el sistema, acceder a datos sensibles, realizar cambios no autorizados o interrumpir servicios esenciales. |
| **Media** | Vulnerabilidad significativa que puede ser explotada 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 reciente auditoría de seguridad en http://example.com reveló áreas de mejora que, aunque no representan un riesgo inmediato crítico, requieren atención para fortalecer la postura general de seguridad. Específicamente, se detectó la ausencia de la cabecera Content Security Policy (CSP). Esto significa que el navegador no está recibiendo instrucciones claras sobre de dónde debe cargar los recursos, abriendo la puerta a posibles ataques de inyección de contenido malicioso.  
  
Asimismo, se identificó la falta de una cabecera anti-clickjacking, lo que podría permitir que un atacante engañe a los usuarios para que realicen acciones sin su consentimiento. Finalmente, la ausencia de la cabecera X-Content-Type-Options podría permitir que el navegador interprete archivos de manera incorrecta, exponiendo a los usuarios a posibles ataques de cross-site scripting.  
  
Se recomienda implementar estas cabeceras de seguridad para robustecer la protección contra estas amenazas y seguir las mejores prácticas de seguridad web. Si bien la plataforma no se considera en alto riesgo, aplicar estas correcciones contribuirá significativamente a una mayor seguridad y protección del usuario.

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

**Evaluación de Requerimientos de Seguridad Web**

**Cumple / No cumple**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerabilidad** | **Nº Alertas** | **Categoría**  **OWASP** | **Criticidad** | **Estado** |
| [VUL 01] Missing Anti-clickjacking Header | 1 | A05 | Medio | Detectada |
| [VUL 02] Content Security Policy (CSP) Header Not Set | 1 | A05 | Medio | Detectada |
| [VUL 03] X-Content-Type-Options Header Missing | 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] Missing Anti-clickjacking Header** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 1021 | http://example.com |
| **Detalles** |  | | |
| La alerta 'Missing Anti-clickjacking Header' indica que el servidor web no está enviando la cabecera HTTP 'X-Frame-Options' o 'Content-Security-Policy: frame-ancestors'. Esta omisión permite que atacantes incrusten el sitio web en un iframe dentro de un sitio malicioso, engañando a los usuarios para que realicen acciones no deseadas. | | | |
| **Riesgo** |  | | |
| El principal riesgo es el 'clickjacking', donde un atacante superpone capas invisibles sobre el sitio web legítimo. Los usuarios, creyendo que están interactuando con el sitio original, son inducidos a hacer clic en elementos ocultos, como cambiar contraseñas, realizar transacciones o conceder permisos. Esto puede resultar en robo de credenciales, fraude financiero o manipulación de datos. | | | |
| **Solución** |  | | |
| La solución es configurar el servidor web para enviar la cabecera 'X-Frame-Options'. Se recomienda establecerla a 'SAMEORIGIN' para permitir el enmarcado solo desde el mismo dominio, o 'DENY' para evitar el enmarcado por completo. Alternativamente, se puede usar 'Content-Security-Policy: frame-ancestors' para un control más granular, especificando qué dominios pueden enmarcar el sitio. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-02] Content Security Policy (CSP) Header Not Set** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Medio** | A05 | 693 | http://example.com |
| **Detalles** |  | | |
| La falta de una cabecera Content Security Policy (CSP) permite la ejecución de contenido malicioso inyectado en la página web, como scripts cross-site scripting (XSS). Sin una CSP definida, el navegador ejecuta cualquier script proveniente de cualquier origen, aumentando la superficie de ataque y facilitando la explotación de vulnerabilidades XSS. | | | |
| **Riesgo** |  | | |
| La ausencia de CSP facilita ataques XSS, permitiendo a atacantes ejecutar código malicioso en el contexto del usuario. Esto puede resultar en robo de cookies, redirección a sitios web maliciosos, alteración de la página web y la captura de información sensible del usuario. La reputación del sitio web también puede verse comprometida. | | | |
| **Solución** |  | | |
| Implementar una cabecera CSP robusta que defina explícitamente los orígenes válidos para cargar recursos como scripts, estilos e imágenes. Utilizar 'nonce' o 'hash' para permitir scripts inline específicos. Revisar y actualizar la CSP regularmente para adaptarla a los cambios en la aplicación y asegurar una protección continua. | | | |
| **Referencias** |  | | |
| https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing\_Content\_Security\_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content\_Security\_Policy\_Cheat\_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/ | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **[VULN-03] X-Content-Type-Options Header Missing** | | | |
| **Criticidad** | **Categoría** | **CWE** | **Fuente** |
| **Bajo** | A05 | 693 | http://example.com |
| **Detalles** |  | | |
| La alerta 'X-Content-Type-Options Header Missing' indica la ausencia de esta cabecera de seguridad en la respuesta HTTP. Esta cabecera previene que el navegador interprete incorrectamente los tipos MIME declarados, lo que podría llevar a la ejecución de código malicioso si un archivo se sirve con un tipo MIME incorrecto. | | | |
| **Riesgo** |  | | |
| La principal amenaza es el 'MIME sniffing', donde el navegador intenta adivinar el tipo de contenido del archivo, ignorando el tipo MIME declarado. Esto puede permitir a un atacante inyectar código malicioso (e.g., JavaScript) en un archivo aparentemente inofensivo (e.g., una imagen) y lograr que el navegador lo ejecute, conduciendo a XSS u otros ataques. | | | |
| **Solución** |  | | |
| La solución es configurar el servidor web para que incluya la cabecera 'X-Content-Type-Options: nosniff' en todas las respuestas HTTP. Esto instruye al navegador a no realizar 'MIME sniffing' y a adherirse estrictamente al tipo MIME declarado en la cabecera 'Content-Type'. Verificar la configuración del servidor web es crucial. | | | |
| **Referencias** |  | | |
| https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security\_Headers | | | |

|  |
| --- |
| **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** |
|  | | |