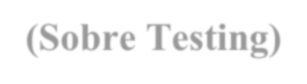
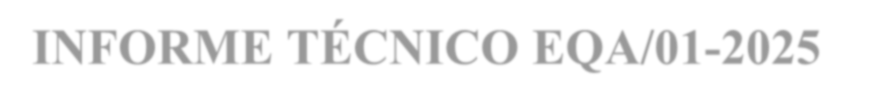
**INFORME TÉCNICO EQA/02-2025**



**(Sobre Testing)**



|  |  |
| --- | --- |
| **Dirigido a:** | M. Sc. Ing. Juan Regis Muñez Sirpa  **JEFE DE UNIDAD**  **DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (UTIC)**  **UNIVERSIDAD PÚBLICA DE EL ALTO (UPEA)** |
| **Vía:** | Ing. Gabriela Luque Arteaga  **TÉC. TESTER Y SEGURIDAD DE SOFTWARE UTIC - UPEA** |
| **De:**  **Ref.:** | Univ. Vanesa Ramirez Callisaya  Univ. Mariluz Huanca Mamani    **Informe de testing realizado al Sistema de Administración de Tesoro Universitario**  **– Universidad Pública de El Alto** |
| **Lugar y fecha:** | **El Alto de 30 de agosto de 2025** |

# CONSIDERACIONES GENERALES

En este informe se presentan los resultados obtenidos del Testing de seguridad que se realizó mediante la herramienta Owasp Zap, al Sistema de Administración de Tesoro Universitario, en fecha 30 de agosto de 2025, con el propósito de identificar las vulnerabilidades de seguridad en el sistema de información web y proporcionar recomendaciones para mitigar estas vulnerabilidades.

**Cuadro 1.** *Datos generales de testeo*

|  |  |  |  |
| --- | --- | --- | --- |
| **Testeo realizado a:** | **Fecha del testeo:** | **Tiempo de**  **Duración del Testeo** | **Observaciones** |
| Página Web de Tesorería | 22/08/2025 | 25 minutos | Owasp Zap |
|  |  |  |  |

*Nota*. Elaboración propia.

El testeo se realizará tomando parámetros de evaluación: nivel de riesgo y confianza. La conclusión de la auditoría de seguridad de la aplicación web se puede resumir como lo siguiente:

**Figura 1**. *Resumen de seguridad de aplicación web (Los porcentajes entre paréntesis representan el recuento como porcentaje del número total de alertas incluidas en el informe, redondeadas a un decimal.)*

Tabla

Descripción generada automáticamente

1. **ALCANCE**

Estos hallazgos son críticos para garantizar la seguridad de la aplicación frente a ataques comunes, como la manipulación de datos o la ejecución de scripts maliciosos en el navegador del usuario.

Los resultados del escaneo se clasificaron según su severidad e impacto potencial, proporcionando descripciones detalladas de cada vulnerabilidad, identificadores CVE correspondientes (cuando aplicable) y recomendaciones específicas para su mitigación.

# OBJETIVO

El objetivo principal de este análisis fue realizar un escaneo de detección de vulnerabilidades en el Sistema de proyecto, utilizando la herramienta OWASP ZAP. A partir de los resultados obtenidos, se brindaron recomendaciones para la mitigación de las vulnerabilidades identificadas, con el fin de fortalecer la seguridad del sistema.

# HERRAMIENTAS UTILIZADAS

OWASP ZAP es una herramienta de análisis de vulnerabilidades que permite a los usuarios identificar y evaluar las vulnerabilidades de seguridad en aplicaciones web y sistemas informáticos. Utiliza un conjunto de plugins y scripts para realizar pruebas de seguridad exhaustivas, enfocándose en riesgos comunes como inyecciones SQL (SQLi), Cross-Site Scripting (XSS), fallos de configuración y problemas de autenticación. Además, OWASP ZAP incluye un sistema de gestión de vulnerabilidades que facilita el seguimiento de los hallazgos, permitiendo a los usuarios priorizar y corregir los riesgos identificados de manera eficiente.

Esta herramienta es especialmente útil para equipos de desarrollo y seguridad, ya que ofrece la flexibilidad de realizar pruebas automatizadas y manuales, adaptándose a las necesidades específicas del proyecto. Su enfoque en aplicaciones web lo convierte en una opción ideal para garantizar la seguridad de sistemas basados en navegadores y servicios en línea.

OWASP ZAP es una solución robusta y de código abierto, diseñada para integrarse fácilmente en flujos de trabajo de seguridad, lo que la convierte en una herramienta esencial para la identificación, gestión y mitigación de vulnerabilidades en aplicaciones web.

**Cuadro 2.** *Datos generales de testeo*

|  |  |  |
| --- | --- | --- |
| **Nombre de la herramienta informática** | **Versión** | **Breve descripción de funciones** |
| OWASP ZAP | 2.16.1 | 1. **Detección de Inyecciones SQL (SQLi):** Identifica vulnerabilidades que permiten la manipulación de bases de datos mediante consultas maliciosas. |
|  |  | 1. **Escaneo de Cross-Site Scripting (XSS):** Detecta puntos débiles donde se pueden inyectar scripts maliciosos en aplicaciones web. 2. **Análisis de Fallos de Configuración**: Busca configuraciones inseguras en servidores y aplicaciones, como directorios expuestos o permisos incorrectos. 3. **Pruebas de Autenticación y Sesiones**: Evalúa la seguridad en la autenticación y el manejo de sesiones, como contraseñas débiles o tokens inseguros. 4. **Detección de CSRF (Cross-Site Request**   **Forgery):** Identifica vulnerabilidades que permiten realizar acciones no autorizadas en nombre de usuarios autenticados.   1. **Escaneo Automatizado y Manual**: Ofrece opciones para realizar pruebas automatizadas o manuales, adaptándose a las necesidades del usuario. 2. **Gestión de Vulnerabilidades:** Incluye un sistema para rastrear y gestionar las vulnerabilidades identificadas, facilitando su resolución. |

*Nota*. Elaboración propia.

# METODOLOGÍA

Para realizar el testeo de seguridad en el sistema bajo prueba, se siguió la metodología del **OWASP Testing Guide versión 2.16.1**, utilizando la herramienta **OWASP ZAP** como principal solución para evaluar la seguridad de la aplicación web. A continuación, se detallan las fases del proceso:

# Identificación

Se identificaron los activos críticos de la página web, incluyendo servidores, bases de datos y componentes de la aplicación web. Se realizó una evaluación de riesgos asociados con cada activo, considerando factores como la exposición a internet, la sensibilidad de los datos manejados y la criticidad de los servicios proporcionados.

# 2. Configuración

Se configuró **OWASP ZAP** para realizar pruebas de seguridad en la aplicación web. Se establecieron criterios de aceptación, incluyendo la identificación de vulnerabilidades críticas y la validación de la seguridad de los componentes clave. La herramienta se ajustó para realizar escaneos automatizados y pruebas manuales, dependiendo de las necesidades del sistema.

# 3. Revisión de Requisitos de Seguridad

Se revisaron los requisitos de seguridad específicos de la página web, incluyendo políticas de autenticación, autorización y cifrado de datos. Además, se identificaron vulnerabilidades conocidas asociadas con los componentes de la página web, utilizando bases de datos de vulnerabilidades y documentación de seguridad.

# 4. Prueba de Seguridad

Se realizaron pruebas de seguridad en la aplicación web utilizando **OWASP ZAP**, enfocándose en los siguientes aspectos:

* **Inyecciones SQL (SQLi)**: Detección de vulnerabilidades que permiten la manipulación de bases de datos.
* **Cross-Site Scripting (XSS)**: Identificación de puntos débiles donde se pueden inyectar scripts maliciosos.
* **Fallos de Configuración**: Búsqueda de configuraciones inseguras en servidores y aplicaciones.
* **Autenticación y Gestión de Sesiones**: Evaluación de debilidades en la autenticación de usuarios y el manejo de sesiones.

Las pruebas se realizaron en el **nivel de aplicación**, centrándose en las vulnerabilidades web y los riesgos asociados con la interacción del usuario.

# 5. Evaluación de Resultados

Gráfico, Gráfico de proyección solar

Descripción generada automáticamenteSe evaluaron los resultados de las pruebas de seguridad realizadas con **OWASP ZAP**, identificando vulnerabilidades y configuraciones inseguras. Los hallazgos se clasificaron en función de su gravedad y prioridad, utilizando un sistema de clasificación de riesgos. Además, se realizó una evaluación de los riesgos asociados con cada hallazgo, considerando el impacto potencial y la probabilidad de explotación.

# 6. Documentación de Hallazgos

Se documentaron los hallazgos de las pruebas de seguridad, incluyendo descripciones detalladas de las vulnerabilidades y configuraciones inseguras identificadas por **OWASP ZAP**. Se creó un informe de pruebas de seguridad que incluye los resultados de las pruebas, las recomendaciones para mitigar las vulnerabilidades y las conclusiones generales sobre el estado de seguridad de la página web.

# 7. Seguimiento y Revisión

Se realizarán seguimientos de los hallazgos para asegurarse de que se abordan adecuadamente, incluyendo la implementación de parches y configuraciones de seguridad. Además, se llevará a cabo una revisión de los resultados de las pruebas de seguridad para identificar posibles mejoras en el proceso de pruebas y en la seguridad general de la página web.

# RESUMEN DE RESULTADOS OBTENIDOS POR NIVELES DE CRITICIDAD

En este apartado del informe se enumeran los hallazgos que presentan un mayor potencial de riesgo. Cabe destacar que se presentan secuencialmente a medida que se descubren, y no están ordenados por importancia o impacto.

**Cuadro 3.** Información del anfitrión ambiente de pruebas:

|  |  |
| --- | --- |
| Nombre DNS: | S/N |
| IP: | 127.0.0.1 |
| Puerto: | 8000 |

*Nota*. Elaboración propia.

## NIVEL ALTO

En el análisis realizado, no se encontró ninguna vulnerabilidad clasificada como de nivel crítico.

## NIVEL MEDIO

### Cabecera Content Security Policy (CSP) no configurada (1)

**Salida del testeo:**

**Tabla 1.** *Salida del complemento (Cabecera Content Security Policy (CSP)no configurada (1))*

|  |  |
| --- | --- |
| Riesgo=Medio, Confianza=Alta (1) | |
| *http://127.0.0.1:8000 (1)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1 host: 127.0.0.1:8000 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache  **Response**  HTTP/1.1 200 OK Host: 127.0.0.1:8000 Connection: close X-Powered-By: PHP/8.4.1 Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private Date: Fri, 22 Aug 2025 15:36:49 GMT Content-Type: text/html; charset=UTF-8 Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **Solución:** | Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy. |

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

***Nota***: Datos obtenidos del resultado del escaneo del complemento " Cabecera Content Security Policy (CSP) no configurada (1)",utilizando la herramienta Owasp Zap

### Falta de cabecera Anti-Clickjacking (1)

**Salida del testeo:**

**Tabla 2.** *Salida del complemento Falta de cabecera Anti-Clickjacking (1)*

|  |  |
| --- | --- |
| Riesgo=Medio, Confianza=Media (1) | |
| *http://127.0.0.1:8000 (1)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1 host: 127.0.0.1:8000 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache  **Response**  HTTP/1.1 200 OK Host: 127.0.0.1:8000 Connection: close X-Powered-By: PHP/8.4.1 Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private Date: Fri, 22 Aug 2025 15:36:49 GMT Content-Type: text/html; charset=UTF-8 Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax  **Parametro:**  x-frame-options |
| **solución** | Los navegadores web modernos admiten las cabeceras HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que una de ellas está configurada en todas las páginas web devueltas por su sitio/aplicación.  Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, si forma parte de un FRAMESET), utilice SAMEORIGIN; de lo contrario, si no espera que la página esté enmarcada, utilice DENY. Alternativamente, considere implementar la directiva "frame-ancestors" de la Política de Seguridad de Contenidos. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento " Falta de cabecera Anti-Clickjacking (1)",utilizando la herramienta Owasp Zap

### Ausencia de tokens anti-CSRF

**Salida del testeo:**

**Tabla 3.** *Salida del complemento Ausencia de tokens anti-CSFR*

|  |  |
| --- | --- |
| Riesgo=Medio, Confianza=Baja (1) | |
| *http://127.0.0.1:8000 (1)* | |
| GET http://127.0.001:8000/admin/login/ | |
| **Descripción** | No se encontraron tokens Anti-CSRF en formulario de envío HTML.  Una solicutud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo. La falsificación de las solicitudes ente los sitios también se conoce como CSRF, XSRG, ataques con un solo clic, montaje de sesión, diputado confundido y navegación en alta mar.  Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:  \*La victima tiene una sesión activa en el sitio de destino.  \*La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.  \*La víctima se encuentra en la misma red local que el sitio de destino.  CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.  **Otra información**  No se ha encontrado ningún token Anti-CSRF [anticsrf, CSRFToken, \_\_RequestVerificationToken, csrfmiddlewaretoken, authenticity\_token, OWASP\_CSRFTOKEN, anoncsrf, csrf\_token, \_csrf, \_csrfSecret, \_\_csrf\_magic, CSRF, \_token, \_csrf\_token, \_csrfToken] conocido en el siguiente formulario HTML: [Form 1: "data.email" "data.password" "data.remember" ].  **Evidencia**  <form  method="post"  x-data="{ isProcessing: false }"  x-on:submit="if (isProcessing) $event.preventDefault()"  x-on:form-processing-started="isProcessing = true"  x-on:form-processing-finished="isProcessing = false"  class="fi-form grid gap-y-6" id="form" wire:submit="authenticate"  >  **Request**  GET http://127.0.0.1:8000/admin/login HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  referer: http://127.0.0.1:8000/  Cookie: XSRF-TOKEN=eyJpdiI6Ikt5OGQ1TW5HNUNLQXJsenRhcVhXOWc9PSIsInZhbHVlIjoiQjJMTG44enlLeU5iQTBsSTNEamZXRXNKeFBnUzdXcElGbDF3dU51WHRlSER0aDVNcUhLTlpPZDJDZkhWWGNZM2Z6M3BMclhkMWlIcG50Snk5NnJJU2NQSW95RXoyV1JNUXhhSDljakl4VWVLQm04SDMyRGZiQjRrQk5GU2NlQnAiLCJtYWMiOiI3M2Y3YWZiODc4NjI5OTA2NmRlZmJlMGI5NGJiNGU5N2Q5NjQ4Mzg1N2RiNTYwYzk2Y2FjZjdlZDBlODRkYTk3IiwidGFnIjoiIn0%3D; trayecto\_u\_session=eyJpdiI6InlhZlBOajlwVUc4K3lCYkM5bFhZckE9PSIsInZhbHVlIjoiUHBOQXNudE9lakdGUURXMWxkeURUdVIrUXV6NXp6eVBROXUwN2xPb29aTXhMZmt4aUtISWlwZmZnTkUzNVpyYW5XUHJiMkFMR3VYUmZhM1BBeWREejJ6UGJSOUpFc2xyWDRrSmthbFh6RFg4eVlRUWlhR3BtdWx2TVUyU2lSSjUiLCJtYWMiOiI2ZTU4MmVjMGI2OWZlY2MwOTVmMjk3YjhlYjVkNmNjMzBiODRlMDM4ZmNlZTRkODY4Yjg3NDU4NzJlY2MxZTM2IiwidGFnIjoiIn0%3D    **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:50 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6InhTaGh0eG1VMnFjTU42QXJzUVRocFE9PSIsInZhbHVlIjoiOCtKekMvVG9IOVlRb2p4SFNFZDFqNUFSVllGeUgrNGRDdlJzKzhlbWw4MDRuYUxFcVFFWFV2d2JnMWRUUVRuUE9uN1ZvaXhiTThDTGtzN1JOV1BLT3d1bTllWWg4eG1EWW8yQkNqK1dsMkZMT1pOQ1FSV3FWUm1acXpOM2s2ZzkiLCJtYWMiOiI0YjA2MmU4ZjBmODYxNWIxOTVhN2NlNjgxOWZiM2ZiOGJjOGRmODY2MDBiMjc3MmY5ZTY3NzZkZTdmNzI0YjkyIiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:50 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6InRVemNNaVp1ZVV1dk9BNS9qVGx0a0E9PSIsInZhbHVlIjoiZGtxdU96UVZWZTNEWHFDTGJaWW9HYmhPbkdIRWNQb3B1L0Q2U3hFZFpsdjRkMlNpemphWVJBeXNaS2tOOUgzRUR6YmdaYVFBbWYzNGVYUjV2d2syaVBrUGFJbFhlUXRpcFNpTkhweEg4N2toYyswa0ZQZUY3bnU5Qm1yVWJNNGwiLCJtYWMiOiI3OWU4NTE2MTU0MGIzMmJjNzkyNTY2ZWMyNGFlOTFkY2I0NDQwNDA3NDZiZDUzNzEyZGEzY2EzZWVmMGZjZjkwIiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:50 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Fase: Arquitectura y Diseño  Utilizar una biblioteca o framework verificado y confiable que evite esta vulnerabilidad o proporcione elementos que faciliten evitarla.  Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de OWASP.  Fase: Implementación  Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.  Fase: Arquitectura y Diseño  Origina un nonce único para cada uno de los formularios, coloque el nonce en el formulario y confirme la independencia al obtener el formulario. Asegúrese de que el nonce no sea predecible (CWE-330).  Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.  Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíe una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.  Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.  Utilice el control de gestión de la sesión de ESAPI.  Este control introduce un elemento para CSRF.  No utilice el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.  Fase: Implementación  Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad auténtica, ya que los usuarios o los representantes puede ser que hayan desactivado el envío de Referir por motivos de privacidad. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Ausencia de Tokens Anti-CRSF",utilizando la herramienta Owasp Zap

## NIVEL BAJO

### *El servidor filtra información de versión a través del campo “server” del encabezado de respuesta HTTP (1)*

**Salida del testeo:**

**Tabla 1.** *Salida del complemento (El servidor filtra información de versión a través del campo “server” del encabezado de respuesta HTTP(1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Alta (2) | |
| https://tracking-protection.cdn.mozilla.net (2) | |
| GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396 | |
| **Descripción** | El servidor web/aplicación está filtrando información de versión a través de la cabecera de respuesta HTTP "Server". El acceso a dicha información puede facilitar a los atacantes la identificación de otras vulnerabilidades a las que está sujeto su servidor web/aplicación.  **Evidenicia**  AmazonS3  **Request**  GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396 HTTP/1.1  host: tracking-protection.cdn.mozilla.net  User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  Accept: \*/\*  Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3  Connection: close  Sec-Fetch-Dest: empty  Sec-Fetch-Mode: no-cors  Sec-Fetch-Site: none  Priority: u=4  Pragma: no-cache  Cache-Control: no-cache  **Response**  HTTP/1.1 200 OK  X-Amz-Id-2: KSmDsDpsbuLODWJ+mRdxmjEm94qE2GnOhKLsr5J3Tmm6NxU5BygiMyW1h4IiboUlEPAU0L02B53VNNbKI7i6zA==  X-Amz-Request-Id: 15BNN8GYFP4ZCGPQ  X-Amz-Server-Side-Encryption: AES256  Accept-Ranges: bytes  Content-Length: 74102  Server: AmazonS3  Via: 1.1 google  Date: Thu, 21 Aug 2025 09:29:24 GMT  Last-Modified: Fri, 08 Aug 2025 11:30:43 GMT  ETag: "5b95dc24328d20fc6490357b6c3dc37c"  Content-Type: application/octet-stream  Age: 108467  Cache-Control: public,max-age=86400  Alt-Svc: clear  Connection: close |
| **solución** | Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para suprimir la cabecera "Server" o proporcionar detalles genéricos. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento " El Servidor filtra información de version a través del campo “Server” del encabezado de respuesta HTTP (1) ,utilizando la herramienta Owasp Zap

### El Servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP “X-Powered-By” (1)

**Salida del testeo:**

**Tabla 2.** *Salida del complemento(Strict-Transport-Security Header No Establecido(1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Alta (2) | |
| *http://tracking-protection.cdn.mozilla.net (2)* | |
| GET http://tracking-protection.cdn.mozilla.neads-track-digest256.0/1754651396 | |
| **Descripción** | HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797  **Request**  GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396 HTTP/1.1  host: tracking-protection.cdn.mozilla.net  User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  Accept: \*/\*  Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3  Connection: close  Sec-Fetch-Dest: empty  Sec-Fetch-Mode: no-cors  Sec-Fetch-Site: none  Priority: u=4  Pragma: no-cache  Cache-Control: no-cache    **Response**  HTTP/1.1 200 OK  X-Amz-Id-2: KSmDsDpsbuLODWJ+mRdxmjEm94qE2GnOhKLsr5J3Tmm6NxU5BygiMyW1h4IiboUlEPAU0L02B53VNNbKI7i6zA==  X-Amz-Request-Id: 15BNN8GYFP4ZCGPQ  X-Amz-Server-Side-Encryption: AES256  Accept-Ranges: bytes  Content-Length: 74102  Server: AmazonS3  Via: 1.1 google  Date: Thu, 21 Aug 2025 09:29:24 GMT  Last-Modified: Fri, 08 Aug 2025 11:30:43 GMT  ETag: "5b95dc24328d20fc6490357b6c3dc37c"  Content-Type: application/octet-stream  Age: 108467  Cache-Control: public,max-age=86400  Alt-Svc: clear  Connection: close |
| **solución** | Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para aplicar Strict-Transport-Security. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Strick-Transport-Security Header No Establecida(1),utilizando la herramienta Owasp Zap

### *Cookie Sin Flag HttpOnly (1)*

**Salida del testeo:**

**Tabla 3.** *Salida del complemento (Cookie Sin Flag HttpOnly (1)*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Media (4) | |
| *http://127.0.0.1:8000 (4)* | |
| GET http://127.0.0.1:8000 | |
| **Descripción** | Se ha establecido una cookie sin el flag HttpOnly, lo que significa que JavaScript puede acceder a la cookie. Si un script malicioso puede ser ejecutado en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión, el secuestro de sesión puede ser posible.  **Evidencia**  XSRF-TOKEN  **Parámetro**  Set-Cookie: XSRF-TOKEN  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache    **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:49 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Asegúrese de que la flag HttpOnly está establecida para todas las cookies. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Cookie Sin Flag HttpOnly(1),utilizando la herramienta Owasp Zap

### El servidor divulga informacion mediante un campo(s) de encabezado de respuesta HTTP ““X-Powered-By”” (1)

**Salida del testeo:**

**Tabla 4.** *Salida del complemento (El servidor divulga informacion mediante un campo(s) de encabezado de respuesta HTTP ““X-Powered-By”” (1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Media (4) | |
| *http://127.0.0.1:8000 (4)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | El servidor de la web/aplicación está divulgando información mediante uno o más encabezados de respuesta HTTP ''''X-Powered-By''''. El acceso a tal información podría facilitarle a los atacantes la identificación de otros marcos/componentes de los que su aplicación web depende y las vulnerabilidades a las que pueden estar sujetos tales componentes.  **Request**  X-Powered-By: PHP/80401  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache    **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:49 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para suprimir las cabeceras "X-Powered-By". |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "El servidor divulga informacion mediante un campo(s) de encabezado de respuesta HTTP ““X-Powered-By”” (1)",utilizando la herramienta Owasp Zap

### Falta encabezado X-Content-Type-Options (1)

**Salida del testeo:**

**Tabla 5.** *Salida del complemento (Falta encabezado X-Content-Type-Options(1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Media (4) | |
| *http://127.0.0.1:8000 (4)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo dé la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.  **Otra información**  Este problema aún se aplica a las páginas de tipo error (401, 403, 500, etc.), ya que esas páginas a menudo se ven afectadas por problemas de inyección, en cuyo caso aún existe la preocupación de que los navegadores husmeen las páginas lejos de su tipo de contenido real.  En el umbral «Alto» esta regla de análisis no alertará sobre respuestas de error del cliente o servidor.  **parámetro**  x-content-type-options  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:49 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Asegúrese de que la aplicación/servidor web establece el encabezado Content-Type adecuadamente, y que establece el encabezado X-Content-Type-Options a 'nosniff' para todas las páginas web.  Si es posible, asegúrese de que el usuario final utiliza un navegador web moderno y compatible con los estándares que no realiza MIME-sniffing en absoluto, o que puede ser dirigido por la aplicación web/servidor web para que no realice MIME-sniffing. |

### *Nota*: Datos obtenidos del resultado del escaneo del complemento "Falta encabezado X-Content-Type-Options (1) ",utilizando la herramienta Owasp Zap

### inclusión de archivos fuente JavaScript entre dominios (1)

**Salida del testeo:**

**Tabla 5.** *Salida del complemento (inclusión de archivos fuente JavaScript entre dominios (1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Media (4) | |
| *http://127.0.0.1:8000 (4)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | La página incluye uno o más archivos de script de un dominio de terceros.  **parámetro**  http://[::1]:5173/@vite/client  **parámetro**  <script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:49 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Asegúrese de que los archivos fuente JavaScript se cargan solo desde fuentes de confianza, y que las fuentes no pueden ser controladas por los usuarios finales de la aplicación. |

### *Nota*: Datos obtenidos del resultado del escaneo del complemento "Inclusion de archivos fuente JavaScript entre dominios (1) ",utilizando la herramienta Owasp Zap

### Divulgación de Marcas de Tiempo-Unix (1)

**Salida del testeo:**

**Tabla 5.** *Salida del complemento (Divulgación de Tiempo-Unix (1))*

|  |  |
| --- | --- |
| Riesgo=Bajo, Confianza=Baja (1) | |
| *http://127.0.0.1:8000 (4)* | |
| GET http://127.0.0.1:8000/js/filament/support/support.js?v=3.3.14.0 | |
| **Descripción** | Una marca de tiempo fue revelada por la aolicacion/servidor web. -Unix  **Otra información**  1732584194, que se evalua como: 2024-11-25 21.23:14.  **Evidencia**  1732584194  **Request**  GET http://127.0.0.1:8000/js/filament/support/support.js?v=3.3.14.0 HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  referer: http://127.0.0.1:8000/admin/login  Cookie: XSRF-TOKEN=eyJpdiI6IkNqOHRVR2NpamNwZXU1NFpRdVFDU2c9PSIsInZhbHVlIjoicityblBlRGNZcUpDVnpxZGRESnA2cnQxNnREUFI2VEJwazlDckcvVUtmbVZnM08xVUk3cVArUldNcUc5ajlVeWtudnoweERidGdkMGMzYWpOSXRyU1AxWU9BbnBId0M4ZmpQY2Q4YmZ4SVpUbm1lSFFUamtYd2wrZW5nT2hkMEMiLCJtYWMiOiJlZTU1OGVkNWYzMmYxN2YwYTkzZGU5MDRkODcwMzMxYmRlNjllZmIwOTkwYmUyNDBlOWYzNTQ0NWNjYzExM2I5IiwidGFnIjoiIn0%3D; trayecto\_u\_session=eyJpdiI6Ik9ET0pTOTFPZUpWaEZNUVV6eTBJaHc9PSIsInZhbHVlIjoid3I4eFN1Qk5zZUl1dFg1NUVOdmQweDBWNGlaT3RXeUdreEJzd2dGM0ROUGE5d1dOVXROc0ZodkVCbnp2NnVRdnY0b0tIeHFXakVkMk5VaXMvOFRDUWpzaDVTbVJTTUZwOGRHUzN0QXJMcFdMMUU0cUJZRzZZQU1CMDVYWEp2eVgiLCJtYWMiOiI3ZDVhNGráfico, Gráfico de proyección solar  Descripción generada automáticamenteTg0YWNjODk1M2NlZGY5MDA1MmM3ZDJhYzcxNzNlOGUwMDQ2Y2VkNDJlY2Q5YmIzMWU1ODM5YWMyOWFmIiwidGFnIjoiIn0%3D  **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Date: Fri, 22 Aug 2025 15:37:03 GMT  Connection: close  Content-Type: application/javascript  Content-Length: 136387 |
| **solución** | Confirmar que los datos encontrados de información sobre la marca de tiempo no son sensibles, ni se pueden usar en patrones explotables de divulgación. |

### *Nota*: Datos obtenidos del resultado del escaneo del complemento "Divulgación de Marcas de Tiempo – Unix (1) ",utilizando la herramienta Owasp Zap

## NIVEL INFORMATIVO

### Recuperado de la Cache (1)

**Salida del testeo:**

**Tabla 1.** *Salida del complemento (Recuperado de la Cache (1))*

|  |  |
| --- | --- |
| Riesgo=Informativo, Confianza=media (3) | |
| *http://tracking-protection.cdn.mozilla.net (1)* | |
| GET http://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396 | |
| **Descripción** | El contenido se ha recuperado de una caché compartida. Si los datos de respuesta son sensibles, personales o específicos del usuario, esto puede resultar en la filtración de información sensible. En algunos casos, esto puede incluso resultar en que un usuario obtenga el control completo de la sesión de otro usuario, dependiendo de la configuración de los componentes de caché en uso en su entorno. Este problema se produce principalmente cuando los servidores de caché, como los "proxy", están configurados en la red local. Esta configuración se encuentra típicamente en entornos corporativos o educativos, por ejemplo.  **Otra información**  La presencia de la cabecera 'Age' indica que se está utilizando un servidor de caché compatible con HTTP/1.1.  **Evidencia**  Age: 105467  **Request**  GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/128.0/1754651396 HTTP/1.1  host: tracking-protection.cdn.mozilla.net  User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  Accept: \*/\*  Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3  Connection: close  Sec-Fetch-Dest: empty  Sec-Fetch-Mode: no-cors  Sec-Fetch-Site: none  Priority: u=4  Pragma: no-cache  Cache-Control: no-cache  **Response**  HTTP/1.1 200 OK  X-Amz-Id-2: KSmDsDpsbuLODWJ+mRdxmjEm94qE2GnOhKLsr5J3Tmm6NxU5BygiMyW1h4IiboUlEPAU0L02B53VNNbKI7i6zA==  X-Amz-Request-Id: 15BNN8GYFP4ZCGPQ  X-Amz-Server-Side-Encryption: AES256  Accept-Ranges: bytes  Content-Length: 74102  Server: AmazonS3  Via: 1.1 google  Date: Thu, 21 Aug 2025 09:29:24 GMT  Last-Modified: Fri, 08 Aug 2025 11:30:43 GMT  ETag: "5b95dc24328d20fc6490357b6c3dc37c"  Content-Type: application/octet-stream  Age: 108467  Cache-Control: public,max-age=86400  Alt-Svc: clear  Connection: close |
| **solución** | Válida que la respuesta no contenga información confidencial, personal o específica del usuario. Si es así, considere el uso de los siguientes encabezados de respuesta HTTP para limitar o evitar que otro usuario almacene y recupere el contenido de la memoria caché:  Cache-Control: no-cache, no-store, must-revalidate, private  Pragma: no-cache  Expires: 0  Esta configuración indica a los servidores de almacenamiento en caché compatibles con HTTP 1.0 y HTTP 1.1 que no almacenen la respuesta ni la recuperen (sin validación) de la memoria caché en respuesta a una solicitud similar. |

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente***Nota***: Datos obtenidos del resultado del escaneo del complemento "Recuperando el cache (1) ",utilizando la herramienta Owasp Zap

### Aplicación Web Moderna (1)

**Salida del testeo:**

**Tabla 2.** *Salida del complemento (Aplicación Web Moderna (1))*

|  |  |
| --- | --- |
| Riesgo=Informativo, Confianza=Media (3) | |
| *http://localhost:8000 (2)* | |
| GET http://127.0.0.1:8000/admin/login | |
| **Descripción** | La aplicación parece ser una aplicación web moderna. Si necesita explorarla automáticamente, el Ajax Spider puede ser más eficaz que el estándar.  **Otra información**  No se han encontrado enlaces, aunque sí scripts, lo que indica que se trata de una aplicación web moderna.  **Evidencia**  <script>  (function () {  const darkStyles = document.querySelector('style[data-theme="dark"]')?.textContent  const lightStyles = document.querySelector('style[data-theme="light"]')?.textContent  const removeStyles = () => {  document.querySelector('style[data-theme="dark"]')?.remove()  document.querySelector('style[data-theme="light"]')?.remove()  }  removeStyles()  setDarkClass = () => {  removeStyles()    const isDark = localStorage.theme === 'dark' || (!('theme' in localStorage) && window.matchMedia('(prefers-color-scheme: dark)').matches)  isDark ? document.documentElement.classList.add('dark') : document.documentElement.classList.remove('dark')  if (isDark) {  document.head.insertAdjacentHTML('beforeend', `<style data-theme="dark">${darkStyles}</style>`)  } else {  document.head.insertAdjacentHTML('beforeend', `<style data-theme="light">${lightStyles}</style>`)  }  }  setDarkClass()  window.matchMedia('(prefers-color-scheme: dark)').addEventListener('change', setDarkClass)  })();  </script>  **Request**  POST http://127.0.0.1:8000/admin/login HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  content-type: application/x-www-form-urlencoded  referer: http://127.0.0.1:8000/admin/login  content-length: 0  Cookie: XSRF-TOKEN=eyJpdiI6IkY4TDVtZ3N2bjVkZTJJaG5aOEpCT2c9PSIsInZhbHVlIjoiQlpldENBeGFuNE80djhCaXJybEtJUFIxQ3pMb1J5aVhFMlJVMGVacHBQcVN5aEwydjJnM2NTOXk2M1o0QlhTbWV4UU4wV0FlMzNVM2QwdUYwU1dNbGRLL0ZYcmJkR0lZRllkSFg1aElPZmdvNCtrU1hteWlKWWVhZGVqWCs2VUMiLCJtYWMiOiIwMmJlNGVhZWE4NzMyMjNiYTRkOWYyZGFjNDFmNmNiOGJhMGU2NjQwMzMwNDc0ODBjMThiMzUwNzUyMWNiMGU4IiwidGFnIjoiIn0%3D; trayecto\_u\_session=eyJpdiI6InpaZng3YXpvR1VBeDM5NXJZaGhjTGc9PSIsInZhbHVlIjoiMEgyUmZ2cERFYy9qRHJFVTBrMTk2U3JwbkJseXdaTDk0dW5Xa1Z5a2xLN0JiT1VHUy8wZ2VETmFVdTdsaUJwN016MGdoR1kwY3lXUHV3S0hjZ2taVnBjVVl1Z00ySnpGSVorYWJsV2hIOXdXcEoveVZHcjE1Y0NneXF3dkgxQmsiLCJtYWMiOiJlMWU2NzM5MGU3MDI1NWUyMGZmOTY2ZDljNmE1NWVhMjA3Yjc1ZDJjMzhiYWRhN2E2OThiODg5YmI0YWI0MWM4IiwidGFnIjoiIn0%3D  **Response**  HTTP/1.1 405 Method Not Allowed  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  allow: GET, HEAD  Cache-Control: no-cache, private  date: Fri, 22 Aug 2025 15:37:04 GMT  Content-Type: text/html; charset=UTF-8 |
| **solución** | se trata de una alerta informativa, por lo que no es necesario realizar ningún cambio. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Aplicación Web Moderna (1) ",utilizando la herramienta Owasp Zap

### Respuesta de Gestión de Sesión Identificada (1)

**Salida del testeo:**

**Tabla 3.** *Salida del complemento (Respuesta de Gestión de Sesión Identificada (1))*

|  |  |
| --- | --- |
| Riesgo=Informativo, Confianza=media (3) | |
| *http://127.0.0.1.8000 (2)* | |
| GET http://127.0.0.1:8000/ | |
| **Descripción** | Se ha identificado que la respuesta dada contiene un token de gestión de sesión. El campo 'Other Info' contiene un conjunto de tokens de cabecera que pueden utilizarse en el método Header Based Session Management (gestión de sesión basado en cabecera). Si la petición se encuentra en un contexto que tiene un método Session Management establecido en "Auto-Detect", esta regla cambiará la gestión de sesión para utilizar los tokens identificados.  **Otra información**  cookie:trayecto\_u\_session  cookie:XSRF-TOKEN  **Parametro**  Trayecto\_u\_session  **Evidencia**  Trayecto\_u\_session  **Request**  GET http://127.0.0.1:8000/ HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Connection: close  X-Powered-By: PHP/8.4.1  Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private  Date: Fri, 22 Aug 2025 15:36:49 GMT  Content-Type: text/html; charset=UTF-8  Pragma: no-cache  Expires: Fri, 01 Jan 1990 00:00:00 GMT  Set-Cookie: XSRF-TOKEN=eyJpdiI6IkQvWDF1eXdIQytJb3BROTNnQXhjNkE9PSIsInZhbHVlIjoiRnhoUVpGTlFiTU5aREdKYWhyN09lWlBINVBPbVN2NnZGUDdIeVF0TVNERFhrL1plaG82NUxHTWJ5dlplY1NXdUVqTVRaeEhyc2pKK0lBd0lJSG14Z3djcHpkUWw3cWphZFV1UDQxdGFTTE8zb0UvRU0wZ29CZkMvY3ZiWWNkQXIiLCJtYWMiOiI4YmQ4NzZiNjY3ZTc3ZjQwOTYzZGIzNzhkMTMwZWMxY2NlMTJiNTMzOWFiNjgyMjkxODIwYzk3YWZkYTNmYTY2IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; samesite=lax  Set-Cookie: trayecto\_u\_session=eyJpdiI6IjdnVDFmOU1iQ1JEWit0UnJodHowL1E9PSIsInZhbHVlIjoiTFBnd2JmbFMxcnRrVW5PYzMyYjg3TGlvK3VJS3NxLzN4eVFiL0JURTc0bFRWbURtUXVleU9YUThEdkE1YTNLTmp3b2cwNjA3T0d2NEczL3dWK1JjVkZnNkRrbmF0UWNIL2ZQWHovdkJTNGNsTnBmK3ExcGlIVUUxd25zdHpBUEMiLCJtYWMiOiI1Mjk0YWRjM2Q1OWZjMWYzZDZiZmUzNjU1NzBmNGI4OTIyYjJkOTVlZTRkNzIyNWYzOTM0NWUzZTNiMDE0YzY3IiwidGFnIjoiIn0%3D; expires=Fri, 22 Aug 2025 17:36:49 GMT; Max-Age=7200; path=/; httponly; samesite=lax |
| **solución** | Se trata de una alerta informativa y no de una vulnerabilidad, por lo que no hay nada que corregir. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Respuesta de Gestión de sesión Identificada (1) ",utilizando la herramienta Owasp Zap

### Divulgación de información-Comentarios sospechosos (1)

**Salida del testeo:**

**Tabla 4.** *Salida del complemento (Divulgación de información – Comentarios sospechosos (1))*

|  |  |
| --- | --- |
| Riesgo=Informativo, Confianza=Baja (1) | |
| *http://127.0.0.1:8000 (1)* | |
| GET http://127.0.0.1:8000/js/filament/filament/echo.js?v=3.3.14.0 | |
| **Descripción** | The response appears to contain suspicious comments which may help an attacker.  **Otra información**  The following pattern was used: \bUSER\b and was detected in likely comment: "//js.pusher.com",cdn\_https:"https://js.pusher.com",dependency\_suffix:""},d=f,N=function(){function e(t){this.options=t,this.rece", see evidence field for the suspicious comment/snippet.  **Evidencia**  user  **Request**  GET http://127.0.0.1:8000/js/filament/filament/echo.js?v=3.3.14.0 HTTP/1.1  host: 127.0.0.1:8000  user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36  pragma: no-cache  cache-control: no-cache  referer: http://127.0.0.1:8000/admin/login  Cookie: XSRF-TOKEN=eyJpdiI6IkVSWHVGd0RhcTJkVlhqbHV0TllPUXc9PSIsInZhbHVlIjoiUE44eVN2SXVvN1V6cnJsMS94M3R1TFhuRHlCazZKU2Mzc2dhMy9ldjU5S1FLN2VZZGt1SHY2N3RvU3Jkb0NmM0Z2b2JPbE5kdEZwS3dHZ2RvSmV4MTR3dVBxOHVGdlRSbkc2WmhxLzc4OVhwYmEvU1U4Q01SdEdSQzhHdTVNZCsiLCJtYWMiOiI3MDdjZGZlMDQxNTdjMTdmNTI5ZTRkYzljYzUwYzdjNDdjZDI1OGVhNTFlNGU3YzdkNGI0MmYyNjE1YTdiOTMwIiwidGFnIjoiIn0%3D; trayecto\_u\_session=eyJpdiI6IkZSQTJmNytYZ0JHMVdGOGxONGJvRFE9PSIsInZhbHVlIjoiU0orU1hublo0REF4RElVUXhUS2NYT0ZFanhmRW83T3ZoOVZmcTJzRFR3c1l6ajRZTnNhZmp6K0gweVF3RU1POGswRUZFQkRWRDBpSFVNS2xBdVpydTM0ZUpCSGVid0Z6Tis5QkNnWGZtM3VuMzRJK0JVS3Y3Q2JBemM5L2dmTHEiLCJtYWMiOiI3MmY1NTA4ZmI3NzQ1NGUyZjZhN2UxN2ZjMmVmMjk5NTU0NDU2NzhmMjc1YmQ3MzQwYTY4MjFjNTM0OWNiNDExIiwidGFnIjoiIn0%3D  **Response**  HTTP/1.1 200 OK  Host: 127.0.0.1:8000  Date: Fri, 22 Aug 2025 15:37:03 GMT  Connection: close  Content-Type: application/javascript  Content-Length: 91742 |
| **solución** | Eliminar todos los comentarios que muestren información que pueda ayudar a un atacante y solucionar el problema al que se refieren. |

***Nota***: Datos obtenidos del resultado del escaneo del complemento "Divulgación de información – Comentarios sospechosos (1) ",utilizando la herramienta Owasp Zap

## ANÁLISIS DE RESULTADOS

El análisis de seguridad realizado al Sistema de Administración de Tesoro Universitario el 22 de agosto de 2025, mediante OWASP ZAP, reveló varias vulnerabilidades críticas, principalmente relacionadas con la ausencia y mala configuración de las cabeceras de seguridad, destacando la falta de una Content Security Policy (CSP) no configurada (314.0%) una vulnerabilidad crítica que expone el sistema a ataques de inyección y Cross-Site Scripting (XSS). Este hallazgo representa un de las vulnerabilidades identificadas en el sistema, la ausencia de protección Anti-Clickjacking (300.0%), lo que expone el sistema a ataques como XSS, clickjacking y secuestro de datos, se hallo la ausencia de Tokens Anti-CSRF(7,1%) representa una vulnerabilidad de ataques Cross-Site Request Forgery (CSRF),que pueden forzar al usuario a realizar acciones no deseadas si su consentimiento. Además, se identificaron vulnerabilidades de riesgo bajo y hallazgos informativos, como ser la inclusión de archivos fuente de JavaScript entre dominios(592,9%) aunque sea de nivel bajo por depender en gran medida de archivos externos se podría convertir en un riesgo si alguno de los archivos se ve comprometido, también la falta de de encabezado X-Content-Type-Options(414,3%) se podría interpretar por archivos de manera maliciosa, también el servidor divulga informacion mediante el campo “X-Powered-By”(321,4%) permite a los atacantes identificar tecnologías subyacentes eso facilita la búsqueda de vulnerabilidades conocidas, también las Cookie Sin Flag HttpOnly(300,0%) es decir que las cookies np están protegidas contra robos a través de ataques XSS, la Divulgación de Marcas de Tiempo-Unix(150,0%) esto expone que el servido rexpone con frecuencia información que puede ser utilizada para realizar ataque de ingeniería socia lo de fuerza bruta, también se hallo que el Servidor filtrainformacion de version a través del campo “server” (7,1%) y Strict-Transport-Security Heder no Establecida (7,1%) ambos son riesgos

que suman una gran cantidad de puntos de riesgo la Divulgación de Marcas de Tiempo - Unix (200.0%), un problema de divulgación de información que facilita la correlación de eventos por parte de un atacante. También se encontró el servidor divulga información sensible en el encabezado de respuesta X-Powered-By (40.0%), lo que expone la tecnología subyacente y puede ser utilizado para ataques dirigidos. Además, la omisión del encabezado X-Content-Type-Options (130.0%) aumenta el riesgo de ataques de *sniffing* de contenido, también la falta de la bandera HttpOnly en las cookies (20.0%) expone las cookies a un posible robo a través de scripts maliciosos. Además, se detectó una gran redirección (10.0%), que podría ser un indicio de una posible fuga de información confidencial a través de la URL. También, se encontraron Divulgación de información - Comentarios sospechosos (20.0%), clasificados como informativos, que pueden proporcionar pistas a los atacantes sobre la estructura interna de la aplicación.

## CONCLUSIONES

El análisis de seguridad realizado en el sistema de Kardex-infraestructura, mediante la herramienta OWASP ZAP en un tiempo de 25 minutos donde presenta vulnerabilidades significativas que se distribuyen en alertas de nivel crítico donde no se detectó alertas, en alertas de nivel medio se identificaron 3 alertas, las que corresponden a ausencia de Content Security Policy(CSP), también ausencia de tokens Anti-CSRF y la falta de protección Anti-Clickjacking. Estas vulnerabilidades son las más críticas y deben ser abordadas con máxima prioridad, en alertas de nivel bajo se identificaron 5 alertas, estas incluyen la omisión de la bandera HttpOnly en las cookies, la divulgación de información del servidor, la falta del encabezado X-Content-Type-Options, la divulgación de marcas de tiempo y una gran redirección, en alertas de nivel informativo se registró 2 alerta, relacionada con la divulgación de información en comentarios sospechosos y respuestas de gestión de sesión identificadas.

## RECOMENDACIONES

Se debe configurar una política de seguridad de contenido (CSP) para restringir la ejecución de scripts maliciosos y reducir el riesgo de ataques XSS, utilizando reglas adecuadas como default-src 'self' y limitando fuentes externas de contenido. Para evitar ataques de Clickjacking, es fundamental implementar la cabecera X-Frame-Options con valores como DENY o SAMEORIGIN, asegurando que la aplicación no pueda ser incrustada en sitios no autorizados. La eliminación o modificación del encabezado XPowered-By es recomendable para ocultar detalles sobre la tecnología del servidor y reducir el riesgo de ataques dirigidos; esto se puede hacer mediante configuraciones en Apache o Nginx. También se debe agregar la cabecera X-Content-Type-Options: nosniff para evitar que los navegadores interpreten archivos con un tipo de contenido diferente al esperado, mitigando riesgos de ejecución no controlada. También asegúrese de que todas las cookies de sesión se configuren con la bandera HttpOnly. Esto impide que los scripts del lado del cliente (como JavaScript) accedan a las cookies, mitigando el riesgo de robo de sesión en caso de un ataque de XSS. Se recomienda realizar una auditoría del código fuente para eliminar comentarios sospechosos que puedan revelar información interna de la aplicación. Finalmente, es esencial establecer un plan de pruebas de seguridad periódicas con herramientas como OWASP ZAP para identificar y mitigar vulnerabilidades de manera proactiva.

|  |  |  |
| --- | --- | --- |
| **Informe realizado por:** | **Informe revisado por:** | **Informe aprobado por:** |
| ------------------------------------ | ------------------------------------------- | ---------------------------------------- |

## 

## ANEXO

**ANEXO 1**

**Sistema de Presentación de Tesorería Universitaria**

Interfaz de usuario gráfica

Descripción generada automáticamente



# ANEXO 2 Resumen de los resultados del escaneo de la herramienta Owasp Zap al Sistema de Administración de Tesoro Universitario

Tabla

Descripción generada automáticamente

Tabla

Descripción generada automáticamente

Gráfico, Gráfico de proyección solar

Descripción generada automáticamente

# ANEXO 3 Tabla de contenidos de Owasp Zap

**Vulnerabilidades por host del escaneo al Sistema de Administración de Tesoro Universitario**

**Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente**