ZAP por Informe de Escaneo Checkmarx

Sitio: http://127.0.0.1:8000

Generado a mié, 16 jul 2025 23:19:05

ZAP Versión: 2.16.1

ZAP by Checkmarx

Sumario de Alertas

Nivel de riesgo	Número de Alertas
Alto	0
Medio	2
Bajo	5
Informativo	3

Alertas

Nombre	Nivel de riesgo	Número de Instancias
Cabecera Content Security Policy (CSP) no configurada	Medio	9
Falta de cabecera Anti-Clickjacking	Medio	8
Cookie Sin Flag HttpOnly	Bajo	8
El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""	Bajo	11
Falta encabezado X-Content-Type-Options	Bajo	15
Gran redirección detectada (posible fuga de información confidencial)	Bajo	1
Inclusión de archivos fuente JavaScript entre dominios	Bajo	16
Divulgación de Información - Información sensible en URL	Informativo	6
Petición de Autenticación Identificada	Informativo	1
Respuesta de Gestión de Sesión Identificada	Informativo	10

Detalles de la Alerta

Medio	Cabecera Content Security Policy (CSP) no configurada
	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

Descripción	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.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	

Otra información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/sitemap.xml
Método	GET
Ataque	
Evidencia	
Otra información	
Instancia	9
Solución	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.
Referencia	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/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medio	**Falta de cabecera Anti-Clickjacking**
Descripción	La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET

Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	
Otra información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	
Otra información	
Instancia	8
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.
Referencia	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15

Plugin Id	10020

Bajo	**Cookie Sin Flag HttpOnly**
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.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET

Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	Set-Cookie: XSRF-TOKEN
Otra información	
Instancia	8
Solución	Asegúrese de que la flag HttpOnly está establecida para todas las cookies.
Referencia	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Bajo	**El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""**
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.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/flux/flux.js?id=77364176
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	

Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/livewire/livewire.js?id=df3a17f2
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4
Otra información	
URL	http://127.0.0.1:8000/sitemap.xml
Método	GET
Ataque	
Evidencia	X-Powered-By: PHP/8.2.4

Otra información	
Instancia	11
Solución	Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para suprimir las cabeceras "X-Powered-By".
Referencia	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	497
WASC Id	13
Plugin Id	10037

Bajo	**Falta encabezado X-Content-Type-Options**
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.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/apple-touch-icon.png
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/favicon.ico
Método	GET
Ataque	

Evidencia	
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.
URL	http://127.0.0.1:8000/favicon.svg
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/flux/flux.js?id=77364176
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/img/logos.png
Método	GET
Ataque	
Evidencia	
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.

URL	http://127.0.0.1:8000/livewire/livewire.js?id=df3a17f2
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	
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.
URL	http://127.0.0.1:8000/robots.txt
Método	GET
Ataque	
Evidencia	

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.
Instancia	15
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.
Referencia	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
CWE Id	693
WASC Id	15
Plugin Id	10021

Bajo	**Gran redirección detectada (posible fuga de información confidencial)**
Descripción	El servidor ha respondido con una redirección que parece proporcionar una respuesta larga. Esto puede indicar que aunque el servidor envió una redirección, también respondió con el contenido del cuerpo (que puede incluir detalles confidenciales, PII, etc.).
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	
Otra información	Longitud URI de la cabecera de ubicación: 27 [http://127.0.0.1:8000/login]. Tamaño previsto de la respuesta: 327. Longitud del cuerpo de la respuesta: 354.
Instancia	1
Solución	Asegúrese de que no se filtre información confidencial a través de las respuestas de redirección. Las respuestas de redireccionamiento casi no deben tener contenido.
Referencia	
CWE Id	201
WASC Id	13
Plugin Id	10044

Bajo	**Inclusión de archivos fuente JavaScript entre dominios**
Descripción	La página incluye uno o más archivos de script de un dominio de terceros.
URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	<script src="https://cdn.tailwindcss.com"></script>
Otra información	
URL	http://127.0.0.1:8000/
Método	GET
Ataque	

Evidencia	<script src="https://unpkg.com/aos@2.3.1/dist/aos.js"></script>
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET

Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="reload"></script>
Otra información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/@vite/client" data-navigate-track="reload"></script>
Otra	

información	
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	<script type="module" src="http://[::1]:5173/resources/js/app.js" data-navigate-track="" reload"></script>
Otra información	
Instancia	16
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.
Referencia	
CWE Id	829
WASC Id	15
Plugin Id	10017

Informativo	**Divulgación de Información - Información sensible en URL**
Descripción	La solicitud parecía contener información sensible filtrada en la URL. Esto puede violar las políticas de cumplimiento de PCI y de la mayoría de las organizaciones. Puede configurar la lista de cadenas de esta comprobación para añadir o eliminar valores específicos de su entorno.
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	zaproxy@example.com
Otra información	El URL contiene dirección(es) de correo electrónico.
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	zaproxy@example.com
Otra información	El URL contiene dirección(es) de correo electrónico.
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	password
Otra información	La URL contiene información potencialmente sensible. La siguiente cadena fue encontrada a través del patrón: pass password
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	zaproxy@example.com
Otra	

información	El URL contiene dirección(es) de correo electrónico.
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	password
Otra información	La URL contiene información potencialmente sensible. La siguiente cadena fue encontrada a través del patrón: pass password
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP
Método	GET
Ataque	
Evidencia	password_confirmation
Otra información	La URL contiene información potencialmente sensible. La siguiente cadena fue encontrada a través del patrón: pass password_confirmation
Instancia	6
Solución	No pase información sensible en URIs.
Referencia	
CWE Id	598
WASC Id	13
Plugin Id	10024

Informativo	**Petición de Autenticación Identificada**
Descripción	La petición en cuestión se ha identificado como una petición de autenticación. El campo "Otra información" contiene un conjunto de líneas key=vvalue que identifican cualquier campo relevante. Si la solicitud está en un contexto que tiene un método de autenticación configurado como "Detección automática", esta regla cambiará la autenticación para que coincida con la petición identificada.
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	password
Otra información	userParam=email userValue=zaproxy@example.com passwordParam=password referer=http://127.0.0.1:8000/login
Instancia	1
Solución	Se trata de una alerta informativa y no de una vulnerabilidad, por lo que no hay nada que corregir.
Referencia	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informativo	**Respuesta de Gestión de Sesión Identificada**
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.

URL	http://127.0.0.1:8000/
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/forgot-password
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/forgot-password?email=zaproxy%40example.com
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login?email=zaproxy%40example.com&password=ZAP
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/register
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/register?email=zaproxy%40example.com&name=ZAP&password=ZAP&password_confirmation=ZAP

Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/dashboard
Método	GET
Ataque	
Evidencia	laravel_session
Otra información	cookie:laravel_session
URL	http://127.0.0.1:8000/login
Método	GET
Ataque	
Evidencia	XSRF-TOKEN
Otra información	cookie:XSRF-TOKEN
Instancia	10
Solución	Se trata de una alerta informativa y no de una vulnerabilidad, por lo que no hay nada que corregir.
Referencia	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112