Servidor OAuth2

Sitio: http://localhost:9000

Generado a mar, 4 mar 2025 20:11:35

ZAP Versión: 2.16.0

ZAP by Checkmarx

Sumario de Alertas

Nivel de riesgo	Número de Alertas
Alto	0
Medio	2
Bajo	1
Informativo	2

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alertas

Nombre	Nivel de riesgo	Número de Instancias
Ausencia de Tokens Anti-CSRF	Medio	3
Cabecera Content Security Policy (CSP) no configurada	Medio	3
Cookie sin el atributo SameSite	Bajo	3
Petición de Autenticación Identificada	Informativo	1
Respuesta de Gestión de Sesión Identificada	Informativo	3

Detalles de la Alerta

Medio	Ausencia de Tokens Anti-CSRF
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 líites de la misma política de origen.
URL	http://localhost:9000
Método	GET
Parámetros	
Ataque	
Evidencia	<form class="login-form" method="post" action="/login">
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] conocido en el siguiente formulario HTML: [Form 1: "password" "username"].
URL	http://localhost:9000/login
Método	GET
Parámetros	
Ataque	
Evidencia	<form class="login-form" method="post" action="/login">
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] conocido en el siguiente formulario HTML: [Form 1: "password" "username"].
URL	http://localhost:9000/login?error
Método	GET
Parámetros	
Ataque	
Evidencia	<form class="login-form" method="post" action="/login">
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] conocido en el siguiente formulario HTML: [Form 1: "password" "username"].
Instancia	3
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 formularo 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 Referer por motivos de privacidad.
Referencia	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202
Medio	**Cabecera Content Security Policy (CSP) no configurada**
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.
URL	http://localhost:9000
Método	GET
Parámetros	
Ataque	
Evidencia	
Otra información	
URL	http://localhost:9000/login
Método	GET
Parámetros	
Ataque	

Evidencia	
Otra información	
URL	http://localhost:9000/login?error
Método	GET
Parámetros	
Ataque	
Evidencia	
Otra información	
Instancia	3
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

Bajo	**Cookie sin el atributo SameSite**
Descripción	Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de peticiones entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.
URL	http://localhost:9000
Método	GET
Parámetros	JSESSIONID
Ataque	
Evidencia	Set-Cookie: JSESSIONID
Otra información	
URL	http://localhost:9000/robots.txt
Método	GET
Parámetros	JSESSIONID
Ataque	
Evidencia	Set-Cookie: JSESSIONID
Otra información	

URL	http://localhost:9000/sitemap.xml
Método	GET
Parámetros	JSESSIONID
Ataque	
Evidencia	Set-Cookie: JSESSIONID
Otra información	
Instancia	3
Solución	Asegúrese que el atributo SameSite está establecido como 'lax' o idealmente 'strict' para todas las cookies.
Referencia	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

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://localhost:9000/login
Método	POST
Parámetros	username
Ataque	
Evidencia	password
Otra información	userParam=username userValue=ZAP passwordParam=password referer=http://localhost:9000/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://localhost:9000
Método	GET
Parámetros	JSESSIONID

Ataque	
Evidencia	9948817A598884126980739D75C231AE
Otra información	cookie:JSESSIONID
URL	http://localhost:9000/robots.txt
Método	GET
Parámetros	JSESSIONID
Ataque	
Evidencia	F0FA106B3150515ECBB21CA698C2DF2E
Otra información	cookie:JSESSIONID
URL	http://localhost:9000/sitemap.xml
Método	GET
Parámetros	JSESSIONID
Ataque	
Evidencia	A9EFA28F6F6DE994D9C0B39CEE7B4B33
Otra información	cookie:JSESSIONID
Instancia	3
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

Sequence Details

With the associated active scan results.