Engineer

SSRF

Hacer que el servidor pida una URL elegida por el atacante

Qué es

SSRF, abreviatura de server-side request forgery, es el ataque en el que alguien entrega una URL a un servidor y este la descarga en su nombre, desde el lugar de la red donde se encuentre. El catálogo Common Weakness Enumeration lo registra como CWE-918 y describe el fallo por lo que el código no hace: recibe una URL de un componente anterior, obtiene aquello a lo que apunta y nunca comprueba que la petición vaya al destino previsto. El atacante no cambia nada del código del servidor. Proporciona una dirección y la posición del servidor en la red hace el resto.

Esa posición es precisamente lo importante. Un servidor en un centro de datos o en una cuenta en la nube suele poder acceder a cosas que un visitante de internet no alcanza: un panel de administración vinculado a una dirección interna, un puerto de base de datos, un panel de supervisión o un servicio de metadatos. La entrada de CWE detalla las consecuencias. El servidor se convierte en un proxy para el atacante, se le puede hacer explorar puertos de equipos de la red interna, y esquemas de URL como `file://`, `gopher://` y `tftp://` pueden leer documentos de la propia máquina o dar al atacante más control sobre el contenido de la petición. CWE sitúa SSRF bajo una debilidad más amplia, CWE-441, el proxy involuntario o «delegado confundido»: un componente con privilegios que trabaja para alguien que no los tiene.

La función que abre la puerta suele ser corriente. La guía de prevención de OWASP menciona dos casos habituales: una imagen de avatar que la aplicación descarga desde una URL escrita por el usuario, y URL de webhooks o de retorno de llamada que los usuarios registran para que la aplicación las invoque después. Las vistas previas de enlaces y los botones para importar desde una URL pertenecen a la misma familia, al igual que cualquier función en la que el servidor

siga una dirección escrita por otra persona. El título de la propia entrada de CWE escribe el término como Server-Side Request Forgery, con mayúsculas, y recoge un nombre anterior para lo mismo: XSPA, abreviatura de Cross Site Port Attack.

Utilice el concepto en una decisión

Aplique «¿Qué es SSRF?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Cuentas, contraseñas y permisos organizados para que cada persona tenga exactamente el acceso que necesita y lo pierda el mismo día que deja la empresa.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 1.000 reglas RBAC para servidores Linux — 1,000 reglas de acceso escritas para cerrar una brecha de seguridad

1.000 reglas RBAC para servidores Linux Póngase en contacto →

Por qué importa

OWASP incorporó SSRF a su Top 10 de 2021 como A10, y no por su volumen. Sus datos mostraban una incidencia relativamente baja, pero la categoría fue la más elegida en la encuesta de la comunidad, y sus valoraciones de explotación e impacto superaban la media. OWASP lo explica por la normalización de la descarga de URL como función de las aplicaciones web y porque los servicios en la nube y las arquitecturas más complejas agravan las consecuencias. En la edición de 2025, SSRF ya no tiene una categoría propia: CWE-918 aparece entre las debilidades destacadas de A01:2025, Broken Access Control, la categoría que encabeza la lista. La clasificación de MITRE apunta en la misma dirección: CWE-918 figura en el CWE Top 25 Most Dangerous Software Weaknesses todos los años de 2021 a 2025.

El motivo es que SSRF atraviesa directamente las defensas en las que más se apoyan los equipos. La descripción de OWASP destaca que el ataque funciona incluso cuando la aplicación está detrás de un cortafuegos, una VPN o una lista de control de acceso de red, porque la petición sale desde dentro. Sus ejemplos recorren lo que hay tras ese perímetro: localizar hosts internos y puertos abiertos a partir del resultado o del tiempo de las conexiones, leer archivos locales como `file:///etc/passwd`, comunicarse con servicios internos como `http://localhost:28017/` y aprovecharlos para ir más lejos, hasta ejecutar código remoto o provocar una denegación de servicio.

Los metadatos de la nube son el caso que convierte una molestia en una intrusión. OWASP señala que la mayoría de los proveedores mantienen los metadatos de las instancias en `http://169.254.169.254/`, una dirección del bloque

169.254.0.0/16 que el registro de usos especiales de IANA clasifica como de enlace local. En Amazon EC2, el servicio de metadatos de esa dirección también proporciona al software de la instancia las credenciales de seguridad de AWS correspondientes al rol que tiene asociado. Si un servidor descarga cualquier URL para cualquiera, se le puede pedir que descargue esas credenciales.

El patrón sigue apareciendo en lugares nuevos. Entre los ejemplos recientes de CWE hay un conjunto de herramientas para LLM que descargaba URL de imágenes arbitrarias, un fallo que ya se utilizaba para explorar puertos en abril de 2026 (CVE-2026-33626) y un entorno de aplicaciones LLM cuyo recuperador de URL podía dirigirse a direcciones locales mediante una cabecera `Location` preparada para ello (CVE-2024-3095). Desde el punto de vista de la red, un agente que navega por la web para un usuario es un servidor que descarga URL elegidas por otra persona.

Cómo se aplica en la práctica

Considere una aplicación de chat en `app.example.com` que muestra una tarjeta de vista previa cuando alguien pega un enlace. El navegador envía la URL al servidor y este descarga la página para leer su título y su imagen:

```
POST /api/link-preview HTTP/1.1
Host: app.example.com
Content-Type: application/json

{"url": "https://news.example.org/2026/10/harbour-reopens"}
```

Ese es el funcionamiento previsto. Ahora se envía la misma petición con otra URL, la que utiliza la documentación de AWS para enumerar los metadatos de la instancia:

```
POST /api/link-preview HTTP/1.1
Host: app.example.com
Content-Type: application/json

{"url": "http://169.254.169.254/latest/meta-data/"}
```

Si el servidor se ejecuta en EC2 y todavía permite la versión antigua IMDSv1, envía la petición desde dentro de la instancia, el servicio de metadatos responde y todo lo que devuelva el código de vista previa acaba en manos del atacante. No se ha inyectado nada ni se ha producido una caída. El servidor ha hecho exactamente aquello para lo que se construyó, pero con la dirección equivocada.

La comprobación del destino parte de adónde iría realmente la petición una vez resuelto el nombre, en lugar de fijarse en el texto de la URL. En Python, el módulo `ipaddress` de la biblioteca estándar utiliza los registros de usos especiales de IANA para clasificar si una dirección es global, excluyendo las direcciones directas de bucle local, privadas, de enlace local, compartidas y de documentación. La siguiente función auxiliar ilustra esa clasificación; no constituye una defensa completa contra SSRF. Un despliegue también debe limitar las peticiones a destinos unicast admisibles y tener en cuenta la traducción de direcciones, como NAT64: en una red con una pasarela de traducción, una dirección clasificada como global todavía puede alcanzar un destino IPv4 incrustado que esté bloqueado. La prueba de clasificación de la función auxiliar es esta:

```
import ipaddress
import socket
from urllib.parse import urlsplit

ALLOWED_SCHEMES = {"http", "https"}


def resolve_public(url: str) -> tuple[str, int, list[str]]:
    parts = urlsplit(url)
    if parts.scheme not in ALLOWED_SCHEMES or not parts.hostname:
        raise ValueError("scheme or host not allowed")
    port = parts.port or (443 if parts.scheme == "https" else 80)
    infos = socket.getaddrinfo(parts.hostname, port, type=socket.SOCK_STREAM)
    addresses = sorted({info[4][0] for info in infos})
    for address in addresses:
        if not ipaddress.ip_address(address).is_global:
            raise ValueError(f"{address} is not a public address")
    return parts.hostname, port, addresses
```

Todas las direcciones a las que resuelva el nombre deben superar la prueba, no solo la primera. Después, el cliente se conecta a una de esas direcciones validadas y sigue enviando el nombre de host original en la cabecera `Host` y utilizándolo para comprobar el certificado TLS, con las redirecciones desactivadas. Permitir que el cliente HTTP resuelva el nombre una segunda vez anularía la

comprobación. Ese es el enfoque que describe la guía de OWASP para el caso difícil, los webhooks, donde los usuarios eligen los destinos y ninguna lista de permitidos puede enumerarlos de antemano. Cuando los destinos se conocen, una lista de nombres de host exactos reduce aún más el alcance, aunque la guía deja claro que las direcciones resueltas siguen necesitando la misma prueba.

Las comprobaciones de aplicación son una capa. La descripción de la implementación de correo con conmutación ante fallos y registro de entregas señala que la ruta de envío pasa por un cliente protegido contra SSRF con un tiempo de espera de 30 segundos. Detrás de la aplicación sigue siendo pertinente el consejo de OWASP para la red: sitúe el código que obtiene recursos remotos en su propio segmento de red y aplique reglas de cortafuegos que denieguen por defecto, para que una comprobación omitida se encuentre con una puerta cerrada.

Dónde surgen los problemas

Listas de denegación y coincidencias de patrones. Un filtro que rechaza URL que contengan `127.0.0.1`, `localhost` o `169.254.169.254` ya ha perdido. La función POSIX `inet_addr()` acepta una dirección IPv4 con entre una y cuatro partes, cada una en decimal, octal o hexadecimal, por lo que, para cualquier analizador que siga esas reglas, tanto `2852039166` como `0xa9.0xfe.0xa9.0xfe` representan la dirección de metadatos. La entrada de CWE recoge una CVE en la que las formas octales y hexadecimales eludían una comprobación escrita para decimal y anulaban una protección contra SSRF (CVE-2016-4029). La entrada del Top 10 de OWASP lo dice sin rodeos: «No mitigue SSRF mediante una lista de denegación ni una expresión regular». Decida según la dirección resuelta, como antes, y permita de forma explícita en lugar de denegar casos concretos.

Comprobar una vez y conectar después. Validar el nombre de host y dejar después que el cliente HTTP vuelva a resolverlo abre una brecha. Con DNS rebinding, el nombre del atacante responde con una dirección pública durante la comprobación y con una interna para la conexión. Conéctese a la dirección exacta que haya validado y aplique la misma política a los reintentos y a las conexiones alternativas, que la guía de OWASP menciona expresamente.

Seguir redirecciones. La URL validada responde con una redirección a `http://169.254.169.254/` o a una URL `file://`, y el cliente la sigue sin preguntar. Los ejemplos de CWE incluyen una biblioteca de descarga de URL que seguía

redirecciones a URL `file://` y `scp://` (CVE-2009-0037). Desactive las redirecciones o trate cada salto como una URL nueva que debe volver a superar toda la comprobación.

Permitir todos los esquemas. Un cliente que también admita `file`, `gopher` o `dict` entrega al atacante archivos locales o mucho más control sobre lo que llega a un servicio interno del que permite una petición HTTP. La guía de OWASP incluye esos esquemas entre los que puede utilizar una segunda petición. Permita únicamente `http` y `https`, en los puertos que necesite la función.

Dos analizadores, dos hosts. La guía de OWASP muestra cómo una cadena puede identificar dos hosts distintos. En `http://good.example\@bad.example`, un analizador que siga WHATWG URL Standard trata la barra inversa como una barra normal, por lo que la ruta empieza ahí y el host es `good.example`, mientras que `urlsplit` de Python interpreta todo lo anterior al último `@` como información del usuario y devuelve `bad.example`. Cuando un componente valida y otro descarga, pueden discrepar sobre adónde va la petición. Analice una sola vez y rechace cualquier URL cuyo host no sea interpretado de la misma forma por todos los analizadores por los que pase.

Devolver la respuesta sin filtrar. Un endpoint de vista previa que devuelve al solicitante el cuerpo descargado transforma un ataque que solo podía deducir qué había dentro a partir de errores y tiempos en uno que puede leerlo. Devuelva únicamente lo que necesite la función, como un título y una referencia a una imagen, nunca la respuesta sin filtrar, tal como aconseja la lista de OWASP.

Dejar IMDSv1 activado. La documentación de AWS indica que, por defecto, se pueden utilizar ambas versiones del servicio de metadatos de instancias. IMDSv2 exige primero un token de sesión, solicitado con un `PUT` a `/latest/api/token` y enviado después en la cabecera `X-aws-ec2-metadata-token`; cuando se exige IMDSv2 (`httpTokens=required`), IMDSv1 deja de funcionar. La guía de OWASP describe IMDSv2 como un mecanismo de defensa en profundidad que mitiga algunos casos de SSRF, no todos. Exija IMDSv2 en cada instancia y corrija también la aplicación.

Una red plana. Si el servicio que descarga puede alcanzar la base de datos, el panel de administración y el servicio de metadatos, cada comprobación omitida deja todo al alcance. Aplique los controles de red de OWASP: segmentación, reglas de cortafuegos que denieguen por defecto el tráfico interno y registros de flujos aceptados y bloqueados para que una exploración deje rastro.

Lecturas adicionales

- CWE-918: Server-Side Request Forgery (SSRF) — la entrada de la debilidad: consecuencias, categoría superior del delegado confundido y CVE observadas.
- OWASP Top 10:2021: A10 Server Side Request Forgery (SSRF) — por qué se añadió la categoría, controles de red y aplicación y cuatro escenarios de ataque.
- OWASP Cheat Sheet Series: Server Side Request Forgery Prevention — listas de permitidos, conexión solo a direcciones validadas, discrepancias entre analizadores y el caso de los webhooks.
- OWASP Top 10:2025: A01 Broken Access Control — dónde se sitúa CWE-918 en la edición de 2025.
- Amazon EC2: Access instance metadata for an EC2 instance — IMDSv1 e IMDSv2, la petición del token y cómo saber si se exige IMDSv2.
- Python documentation: ipaddress — `is_global` y los registros de IANA que sigue.

Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es SSRF?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/ssrf/