Tipo de artículo: Artículo de revisión

Tendencias en las vulnerabilidades y ataques SSRF

Trends is SSRF vulnerabilities and attacks

Fernando Gonzalez Martinez [1*] **https://orcid.org/0009-0002-6604-4359**
Arnol Stiven Meneses Ruiz[2] **https://orcid.org/0009-0008-8965-0021**
Henry Raúl González Brito [3] **https://orcid.org/0000-0002-3226-9210**
Yaimí Trujillo Casañola[4] **https://orcid.org/0000-0002-3138-011X**

[1] Facultad de Ingeniería, Universidad Santiago de Cali. Colombia. Correo: fernando.gonzalez00@usc.edu.co
[2] Facultad de Ingeniería, Universidad Santiago de Cali. Colombia. Correo: arnol.meneses00@usc.edu.co
[3] Dirección de Seguridad Informática, Universidad de las Ciencias Informáticas. Cuba. Correo: henryraul@uci.cu
[4] Facultad de Tecnologías Interactivas, Universidad de las Ciencias Informáticas. Cuba. Correo: yaimi@uci.cu

*** Autor para correspondencia: fernando.gonzalez00@usc.edu.co**

Resumen

El objetivo de la investigación fue explorar sobre las vulnerabilidades de ataques *Server-Side Request Forgery* (SSRF), visto desde las temáticas trabajadas en investigaciones recientes y los reportes internacionales. Se realizó una revisión sistemática que permite conocer el estado actual de los ataques de SSRF, abordada a partir de las siguientes interrogantes: ¿Cuál es la tendencia en detecciones de ataques SSFR? ¿Cuáles son las principales técnicas para identificar este tipo de vulnerabilidad? ¿Cómo se manifiestan los ataques SSFR? ¿Qué herramientas se emplean para identificar este tipo de vulnerabilidad? ¿Cuáles son las medidas para mitigar que se explote este tipo de vulnerabilidad? Las bases de datos utilizadas fueron IEEE, ACM, Elsevier, tomando como período de recuperación desde el año 2020 al 2024. Los resultados muestran que anualmente se reporta un incremento en los ataques SSRF, con un aumento significativo año por año. Las principales técnicas para identificar las vulnerabilidades de SSRF son: el análisis estático y dinámico de código, las pruebas de penetración y la revisión de configuraciones y políticas de seguridad. Estas vulnerabilidades se manifiestan comúnmente a través de la exfiltración de datos y la evasión de controles de seguridad. Para la detección de vulnerabilidades SSRF se utilizan herramientas como: Burp Suite, OWASP Zap y Nikto. Las medidas para mitigar la explotación de vulnerabilidades SSRF incluyen la validación y análisis de entradas; la segregación de redes y servicios; el uso de listas blancas y negras; y el monitoreo continuo. Se concluye que las vulnerabilidades de ataques SSRF son una amenaza para la transformación digital.

Palabras clave: vulnerabilidades; seguridad web; SSRF; ataques; exfiltración.

Abstract

The objective of the research was to explore Server-Side Request Forgery (SSRF) attack vulnerabilities, seen from the topics worked on in recent research and international reports. A systematic review was carried out that allows us to know the current state of SSRF attacks, addressed from the following questions: What is the trend in SSFR attack detections? What are the main techniques to identify this type of vulnerability? How do SSFR attacks manifest themselves? What tools are used to identify this type of vulnerability? What are the measures to mitigate the exploitation of this type of vulnerability? The databases used were IEEE, ACM, Elsevier, taking the recovery period from 2020 to 2024. The results show that an increase in SSRF attacks is reported annually, with a significant increase year by year. The main techniques to identify SSRF vulnerabilities are: static and dynamic code analysis, penetration testing, and review of security configurations and policies. These vulnerabilities are commonly manifested through data exfiltration and the evasion of security controls. Tools such as Burp Suite, OWASP Zap, and Nikto are used to detect SSRF vulnerabilities. Measures to mitigate the exploitation of SSRF vulnerabilities include input validation and

analysis; network and service segregation; the use of white and black lists; and continuous monitoring. It is concluded that SSRF attack vulnerabilities are a threat to digital transformation.

Keywords: *vulnerabilities; web security; SSRF; attacks; exfiltration.*

Recibido: 01/07/2024
Aceptado: 12/07/2024
En línea: 18/07/2024

Introducción

En la era de la transformación digital, la ciberseguridad se ha convertido en una prioridad estratégica dentro de las organizaciones debido al crecimiento exponencial de amenazas que ponen en riesgo la integridad y disponibilidad de sus activos digitales. La Web, como infraestructura fundamental para la comunicación global y el intercambio de datos, está expuesta a una variedad de ciberataques que pueden comprometer desde la privacidad de los usuarios hasta la estabilidad de sistemas críticos (Saeed et al., 2023).

Los marcos de desarrollo de tecnologías web, como Node.js, Ruby on Rails y Django, facilitan la creación de aplicaciones robustas, pero también introducen vulnerabilidades potenciales. Entre estas vulnerabilidades, destacan los ataques como *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF) y *Server-Side Request Forgery* (SSRF) (Faisal Fadlalla & Elshoush, 2023). Estos últimos, específicamente SSRF, representan una amenaza significativa al permitir que un atacante manipule peticiones desde un servidor vulnerable hacia recursos internos o externos de una red (Wang et al., 2024).

El presente artículo tiene como objetivo identificar y analizar las tendencias actuales en las vulnerabilidades y ataques SSRF, las principales técnicas para identificar dichas vulnerabilidades, las manifestaciones de estos ataques, las herramientas empleadas en su detección y las medidas eficaces para mitigar su explotación. De acuerdo a los datos suministrados en CVEdetails.com se puede identificar una tendencia de crecimiento en los ataques de este tipo. A través de un análisis a la literatura científica y estudios de caso recientes, se busca proporcionar una visión integral de las prácticas actuales y emergentes en la prevención y mitigación de vulnerabilidades SSRF, con especial énfasis en publicaciones posteriores al 2020. Al abordar estas preocupaciones, se suministra un marco teórico referencial para comprender y enfrentar los desafíos emergentes en ciberseguridad.

Materiales y métodos

Para el desarrollo de la presente investigación se emplearon métodos combinados que proporcionan una base para el análisis de tendencias en vulnerabilidades y ataques SSRF. Entre los métodos de trabajos científicos utilizados en la

investigación se destacan los que se mencionan a continuación. Además, se brinda una breve explicación de los fines para los que fueron utilizados.

- Histórico - lógico: para realizar un análisis de tendencia de las vulnerabilidades y ciberataques desde el 2020 al 2024 a través de investigaciones recientes y los reportes internacionales.
- Analítico - sintético: para analizar los conceptos de ciberseguridad, vulnerabilidades y ataques SSRF como antecedentes de la investigación y resumir las principales amenazas para el desarrollo de aplicaciones Web para identificar patrones comunes, avances tecnológicos y brechas en la investigación actual.

Revisión sistemática de la bibliografía

Para reunir evidencia que demuestre la necesidad de la investigación, a partir de la revisión de las vulnerabilidades y ataques recogidos entre el 2020 y el 2024 en bases de datos científicas como IEEE Xplore, ACM Digital Library, y Elsevier, enfocándose en publicaciones desde 2020 en adelante. Los términos de búsqueda incluyeron "*SSRF vulnerabilities*", "*SSRF attacks*", "*SSRF detection techniques*", "*SSRF mitigation*", y "*SSRF tools*".

Preguntas de la investigación (RQ):

RQ 1. ¿Cuál es la tendencia en detecciones de ataques SSFR?

RQ 2. ¿Cuáles son las principales técnicas para identificar este tipo de vulnerabilidad?

RQ 3. ¿Cómo se manifiestan los ataques SSFR?

RQ 4. ¿Qué herramientas se emplean para identificar este tipo de vulnerabilidad?

RQ 5. ¿Cuáles son las medidas para mitigar que se explote este tipo de vulnerabilidad?

Criterios de inclusión y exclusión

De acuerdo con las preguntas de investigación definidas, fueron identificados los siguientes criterios de inclusión para este estudio:

- Artículos publicados entre 2020 y 2024.
- La publicación se centra en ataques SSFR.
- La publicación fue arbitrada por pares.
- Artículos donde se realice experimentación y/o simulación sobre ataques SSFR.
- Artículos con texto completo disponible sobre el objeto de estudio.
- Escritos en idioma Español o Inglés.

No se tendrán en cuenta aquellas publicaciones que cumplan con uno o más de los siguientes criterios de exclusión:

- Artículos publicados antes de 2020.
- La publicación no está escrita en inglés o español.

- El texto completo de la publicación no es de acceso público.
- La publicación es un estudio secundario.
- Cartas al editor, notas cortas, solamente el resumen.
- Publicaciones donde no se describe el escenario de experimentación.
- Estudios que no discuten un caso real implementado.

Resultados y discusión

En el entorno de transformación digital, la ciberseguridad se define como la práctica de proteger sistemas, redes y programas de ataques digitales, que tienen como objetivo acceder, alterar o destruir información sensible, extorsionar a los usuarios o interrumpir procesos comerciales normales. La ciberseguridad se utiliza en una variedad de contextos, incluida la seguridad informática y la protección de infraestructuras críticas (Marselis et al., 2020).

En ciberseguridad, una vulnerabilidad es una debilidad que una amenaza puede explotar para acceder, dañar o interrumpir el funcionamiento normal de un sistema o red. Las vulnerabilidades pueden existir en el hardware, el software, el personal o los procesos (Marselis et al., 2020).

Una de las vulnerabilidades emergentes en el panorama de la ciberseguridad es el *Server-Side Request Forgery* (SSRF) que es una vulnerabilidad web que se manifiesta cuando un atacante puede hacer peticiones HTTP del lado del servidor a una aplicación web como se refleja en la figura 1. Estas vulnerabilidades permiten al atacante acceder a servicios internos donde se aloja el sitio web, como bases de datos accesibles a través de peticiones habilitadas para HTTP o solicitudes POST y así hacen infiltración y extracción de información, los ataques SSRF pueden explotar estos servicios a través de envíos de correos no deseados o ejecución de comandos de forma remota (Jabiyev et al., 2021).

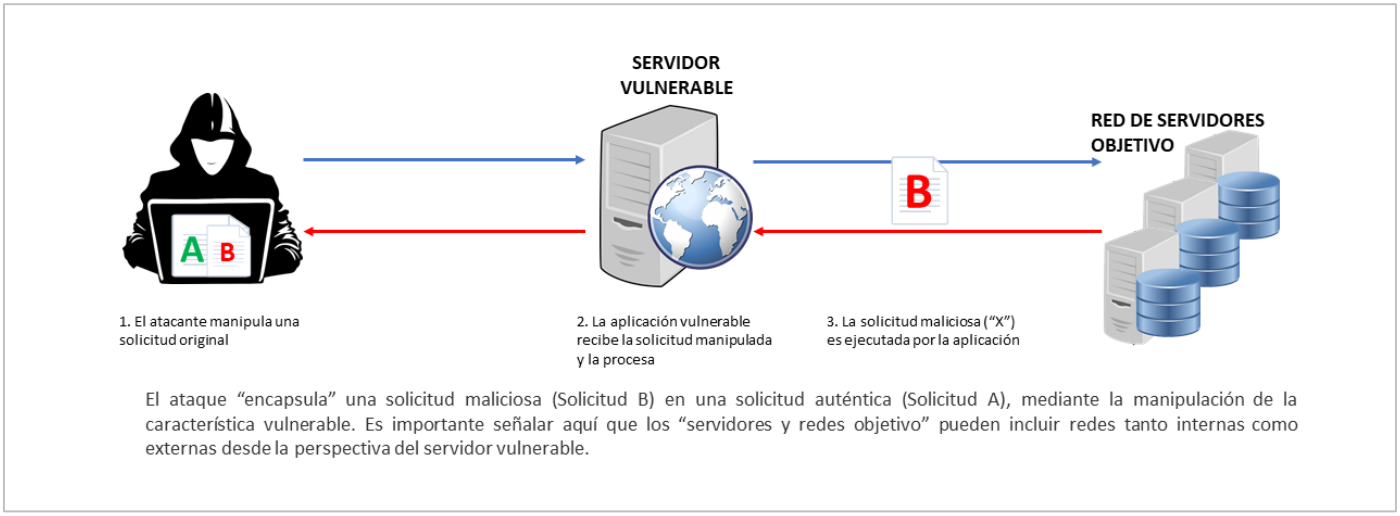

Figura 1. Funcionamiento ataque SSRF.

Fuente: Elaboración propia.

Debido a su capacidad para evadir las defensas tradicionales y acceder a recursos internos, la vulnerabilidad SSRF son un riesgo significativo en el panorama actual de la ciberseguridad. La necesidad de crear e implementar medidas de seguridad más sólidas y sofisticadas se ve reforzada por la sofisticación de las técnicas empleadas por los atacantes. Se sugiere que las organizaciones adopten un enfoque proactivo en la detección y mitigación de vulnerabilidades SSRF, utilicen herramientas de seguridad actuales y colaboren con el intercambio de información sobre amenazas emergentes (Jabiyev et al., 2021; Marselis et al., 2020).

Tendencias en la detección de ataques SSRF

Según los estudios y reportes más recientes de varias organizaciones de ciberseguridad, la detección de ataques SSRF, impulsado por la creciente adopción de servicios web y la interconectividad de sistemas, está aumentando constantemente (Cao et al., 2023). Las tres tendencias principales en este campo, respaldadas por varias fuentes son:

Aumento de la sofisticación en ataques (Técnicas avanzadas): los atacantes están utilizando métodos más avanzados para superar las defensas convencionales, como el uso de redes de bots y ataques dirigidos diseñados para explotar vulnerabilidades específicas. Los atacantes se aprovechan de los protocolos y manipulan los encabezados HTTP utilizando técnicas complejas para superar los firewalls y otras medidas de seguridad convencionales (Cao et al., 2023).

Mayor enfoque en la detección proactiva (Sistemas de detección temprana): la inversión en sistemas de detección temprana y soluciones de monitoreo continuo se ha centrado en la detección de patrones de comportamiento anómalos

que pueden indicar ataques SSRF. Esto incluye el uso de sistemas de detección de anomalías y algoritmos de aprendizaje automático para detectar y responder a actividades sospechosas (Cao et al., 2023).

Colaboración y compartición de información (Intercambio de inteligencia sobre amenazas): se ha vuelto fundamental que las organizaciones compartan información sobre amenazas entre sí y dentro de la comunidad de ciberseguridad. OWASP y otras organizaciones de ciberseguridad han destacado la importancia de difundir información sobre métodos de ataque, indicadores de compromiso (IOCs) y estrategias de mitigación para mejorar las defensas colectivas contra SSRF (Cao et al., 2023).

Al analizar estas tendencias, respaldadas por investigaciones y reportes recientes, las organizaciones pueden prepararse mejor y adaptar sus estrategias de seguridad para abordar el panorama de amenazas en evolución que presentan los ataques SSRF. Invertir en tecnologías de detección avanzadas, fomentar una cultura de seguridad proactiva y participar en esfuerzos colaborativos son pasos esenciales para mitigar los riesgos asociados con las vulnerabilidades SSRF. Se destaca la efectividad de las medidas de detección proactiva y el impacto del intercambio de inteligencia colaborativa ilustrando el aumento anual en las detecciones de ataques SSRF desde 2014 hasta 2024 Figura 2 (*CVE Security Vulnerabilities By Types/Categories*, 2021).

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	831	627	304	1099	207	3	266	67	10	48	534
2015	1066	1104	221	776	152	6	249	50	8	46	380
2016	1209	1174	97	497	99	12	87	41	16	33	530
2017	2489	1551	505	1500	283	155	334	109	57	97	963
2018	2099	1746	504	2042	572	112	479	189	118	85	1274
2019	1209	2038	554	2389	491	126	560	137	103	122	918
2020	1222	1900	466	2203	441	110	416	119	132	101	831
2021	1675	2561	744	2725	560	92	520	126	197	133	698
2022	1886	3414	1790	3407	733	100	769	127	235	147	815
2023	1756	2788	2157	5177	806	137	1398	138	246	186	788
2024	1257	1682	1394	3957	570	158	860	57	243	81	272
Total	16699	20585	8736	25772	4914	1011	5938	1160	1365	1079	8003

Figura 2. Vulnerabilidades por tipo/categoría.

Tomado de: cvdetails.com

De acuerdo a los datos suministrados en CVEdetails.com en la columna 9 de la figura 2 se puede identificar una tendencia de crecimiento en los ataques SSRF como tipo de vulnerabilidad emergente. Pese a que no es la vulnerabilidad más explotada se ha ubicado como una de las de mayor riesgo en los últimos años.

Técnicas para identificar vulnerabilidades SSRF

Varias técnicas, como el análisis estático y dinámico de código, las pruebas de penetración y la revisión de configuraciones y políticas de seguridad, se pueden utilizar para abordar la identificación de vulnerabilidades SSRF. Las pruebas de penetración simulan ataques reales para evaluar la seguridad de la aplicación, mientras que el análisis de código utiliza herramientas automatizadas para detectar patrones vulnerables (Wang et al., 2024). A continuación, se desglosa con más detalle en qué consiste cada una de estas técnicas:

- Análisis estático y dinámico de código: una práctica fundamental en la seguridad del software es identificar vulnerabilidades SSRF a través del análisis estático y dinámico de código. El análisis estático requiere el uso de herramientas automatizadas que escanean el código fuente para encontrar patrones de código potencialmente explotables (Wang et al., 2024).
- Pruebas de penetración: estas pruebas, que pueden ser manuales o automatizadas, simulan ataques reales para evaluar la seguridad de una aplicación y son esenciales para la identificación de vulnerabilidades SSRF. Esta estrategia no solo ayuda a identificar vulnerabilidades, sino que también permite comprender las posibles consecuencias de un ataque exitoso y mejorar las medidas de mitigación (Ravindran & Potukuchi, 2022).
- Revisión de configuraciones y políticas de seguridad: una auditoría regular de las configuraciones y políticas de seguridad de la red es otra técnica importante para identificar vulnerabilidades SSRF. Una revisión completa de las políticas de acceso, las reglas del firewall y las configuraciones del servidor puede ayudar a identificar y corregir estos problemas antes de que sean explotados (Rahmawati et al., 2023).

La combinación de análisis estático y dinámico de código, pruebas de penetración y revisiones de configuraciones y políticas de seguridad proporciona un enfoque integral para identificar vulnerabilidades SSRF. Estas técnicas permiten detectar y mitigar puntos débiles antes de que sean explotados, mejorando la seguridad general de las aplicaciones. Al implementar estas prácticas de manera regular, se puede mantener una postura de seguridad robusta y proteger mejor los sistemas contra ataques (Ravindran & Potukuchi, 2022; Wang et al., 2024).

Manifestaciones de los ataques SSRF

Los ataques SSRF se manifiestan de una variedad de maneras, lo que permite a los atacantes explotar las vulnerabilidades de seguridad en los servidores. La exfiltración de datos es una de las manifestaciones más frecuentes en las que los atacantes pueden acceder a datos sensibles internos mediante solicitudes maliciosas, aprovechando la capacidad de un servidor para comunicarse con otras partes internas de la red. Estos ataques pueden afectar interfaces de gestión internas, como bases de datos NoSQL, que permiten extraer datos no expuestos a Internet (Khodayari et al., 2024).

La evasión de controles de seguridad es otra manifestación significativa en la que los atacantes utilizan SSRF para eludir firewalls y otras medidas de seguridad. Los atacantes pueden manipular las solicitudes del servidor para identificar servicios internos vulnerables y obtener información crítica sobre la infraestructura interna de la red mediante escaneos de puertos o ataques de escaneo de puertos (Ravindran & Potukuchi, 2022).

Debido a su capacidad para acceder a datos confidenciales, evadir controles de seguridad y manipular los servicios internos, los ataques SSRF son una amenaza significativa. Es fundamental comprender estas manifestaciones para crear métodos efectivos de mitigación y protección en entornos vulnerables. Las investigaciones recientes sobre seguridad en la computación en la nube y la mitigación de vulnerabilidades SSRF son referencias importantes (Al-talak & Abbass, 2021).

Herramientas para la detección de vulnerabilidades SSRF

Burp Suite, OWASP ZAP y Nikto son las herramientas de detección de vulnerabilidades SSRF más utilizadas. Burp Suite, que se utiliza ampliamente en pruebas de penetración, incluye módulos SSRF específicos y permite la creación de reglas personalizadas. OWASP ZAP, por otro lado, es una herramienta configurable de análisis de seguridad que identifica SSRF y se integra en los procesos de desarrollo continuo. Aunque no fue creado para SSRF, Nikto realiza análisis exhaustivos de servidores web para encontrar configuraciones inseguras y otros problemas de seguridad (Ravindran & Potukuchi, 2022).

La identificación efectiva de vulnerabilidades SSRF requiere el uso de herramientas como Burp Suite, OWASP ZAP y Nikto. Las capacidades avanzadas de análisis y prueba que ofrecen estas herramientas permiten a los profesionales de la seguridad detectar y mitigar riesgos potenciales de manera proactiva. Para proteger la integridad y seguridad de los sistemas web frente a amenazas emergentes, es esencial incorporar estas herramientas en los procesos de seguridad (Ravindran & Potukuchi, 2022).

Medidas de mitigación

Para mitigar efectivamente la explotación de las vulnerabilidades SSRF, es esencial implementar una combinación de medidas de seguridad sólidas, cada una respaldada por investigaciones y prácticas recomendadas en ciberseguridad. En la bibliografía consultada se identifican las siguientes medidas:

- **Validación y análisis de entradas**: es esencial aplicar controles rigurosos para validar y sanear las entradas de usuarios. Esto implica asegurarse de que todos los datos del cliente sean verificados antes de que el servidor los procese. La mayoría de los ataques de inyección, incluido el SSRF, pueden ser prevenidos mediante la validación y análisis de las entradas (*OWASP Top Ten Proactive Controls 2018 | C5*, 2018). Se recomienda, en particular, utilizar listas blancas para determinar qué entradas son aceptables y usar funciones de análisis para limpiar las entradas de datos que no sean confiables.
- **Segregación de redes y servicios:** aislar servicios internos críticos y separar las redes puede minimizar el impacto de un ataque SSRF. Esta medida reduce la superficie de ataque y limita el acceso que un atacante podría obtener si logra explotar una vulnerabilidad SSRF. Investigaciones de la Universidad de Stanford han demostrado que la segregación de redes puede reducir significativamente el riesgo de propagación de ataques dentro de una infraestructura de TI. El uso de entornos virtualizados y segmentación de red son prácticas comunes y efectivas en la mitigación de ataques (Basta et al., 2022).
- **Uso de listas blancas y negras:** configurar listas blancas y negras para controlar las solicitudes de red permitidas es otra medida efectiva. Las listas blancas permiten únicamente las solicitudes de red a destinos aprobados, mientras que las listas negras bloquean destinos conocidos por ser maliciosos. Según IEEE, la implementación de listas blancas y negras es una práctica recomendada para proteger contra una variedad de ataques, incluidos SSRF. La efectividad de estas listas depende de la actualización continua basada en inteligencia de amenazas (Pant, 2022).
- **Monitoreo continuo y actualización de seguridad:** la implementación de sistemas de monitoreo continuo y la aplicación regular de actualizaciones de seguridad son esenciales para identificar y mitigar amenazas de manera proactiva. Se destaca la importancia del monitoreo continuo y las actualizaciones de seguridad en la detección temprana y prevención de ataques SSRF. Las herramientas de información de seguridad y gestión de eventos conocidas como SIEM (por sus siglas en inglés de Security Information and Event Management) son particularmente efectivas en este ámbito (Rahmawati et al., 2023).

La combinación de medidas de mitigación como la validación y análisis de entradas, la segregación de redes, el uso de listas blancas y negras, y el monitoreo continuo es fundamental para proteger los sistemas contra vulnerabilidades SSRF.

Estas prácticas, respaldadas por investigaciones y recomendaciones de la industria de ciberseguridad, permiten una defensa proactiva y efectiva contra este tipo de ataques.

Conclusiones

En el presente artículo de revisión se abordan las tendencias actuales en las vulnerabilidades y ataques SSRF, así como las técnicas de detección y las medidas de mitigación. A través del análisis de estudios recientes y reportes internacionales, se han obtenido varios hallazgos clave.

La detección de ataques SSRF ha mostrado un incremento significativo desde 2020, impulsado por la creciente adopción de servicios web y la interconectividad de sistemas. Los datos indican un aumento constante año tras año, este aumento se debe en parte a la sofisticación creciente de los atacantes, que emplean técnicas avanzadas como redes de bots y ataques dirigidos para evadir las defensas tradicionales. Los ataques SSRF se manifiestan comúnmente a través de la exfiltración de datos y la evasión de controles de seguridad.

Las técnicas de identificación de vulnerabilidades SSRF como el análisis estático y dinámico de código, las pruebas de penetración y la revisión de configuraciones y políticas de seguridad, han demostrado ser cruciales para identificar patrones anómalos y prevenir ataques. Las medidas para mitigar la explotación de vulnerabilidades SSRF incluyen la validación y análisis de entradas, la segregación de redes y servicios, el uso de listas blancas y negras, y el monitoreo continuo. Estas prácticas no solo ayudan a prevenir los ataques, sino que también limitan su impacto en caso de ocurrir.

Este trabajo contribuye al campo de la ciberseguridad al proporcionar un análisis de las tendencias actuales en la detección y mitigación de ataques SSRF. Los hallazgos presentados ofrecen una base para mejorar las prácticas de seguridad en el desarrollo y mantenimiento de aplicaciones web. Además, este artículo destaca la importancia de la colaboración y el intercambio de información en la comunidad de ciberseguridad para enfrentar las amenazas emergentes de manera efectiva.

Se recomienda el desarrollo y perfeccionamiento de herramientas basadas en inteligencia artificial y aprendizaje automático que puedan detectar vulnerabilidades SSRF con mayor precisión y rapidez. Investigaciones futuras podrían enfocarse en la integración de las herramientas como Burp Suite, OWASP ZAP y Nikto con plataformas de monitoreo de seguridad en tiempo real, que podrían examinar con mayor profundidad el impacto de la colaboración y el intercambio de información entre organizaciones en la efectividad de la detección y mitigación de ataques SSRF. Esto incluye el análisis de redes de intercambio de inteligencia sobre amenazas y su papel en la mejora de la seguridad global. Así mismo, es crucial continuar evaluando y desarrollando nuevas técnicas de mitigación que puedan adaptarse a las

tácticas cada vez más sofisticadas de los atacantes. Esto incluye la exploración de enfoques innovadores en la segregación de redes, el uso de listas blancas y negras, y la implementación de soluciones de seguridad basadas en blockchain.

Agradecimientos

Se agradece a la Universidad de las Ciencias Informáticas (UCI) y la Universidad Santiago de Cali (USC) que proporcionaron las facilidades para la realización de la investigación.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola.
2. Análisis formal: Fernando Gonzalez Martinez y Arnol Stiven Meneses Ruiz
3. Investigación: Fernando Gonzalez Martinez y Arnol Stiven Meneses Ruiz
4. Metodología: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola
5. Administración del proyecto: Fernando Gonzalez Martinez y Arnol Stiven Meneses Ruiz
6. Recursos: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola
7. Supervisión: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola
8. Visualización: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola
9. Redacción – borrador original: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola
10. Redacción – revisión y edición: Fernando Gonzalez Martinez, Arnol Stiven Meneses Ruiz, Henry Raúl González Brito y Yaimí Trujillo Casañola

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Al-talak, K., & Abbass, O. (2021). Detecting server-side request forgery (SSRF) attack by using deep learning techniques. International Journal of Advanced Computer Science and Applications, 12(12), 12.

Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). Towards a zero-trust micro-segmentation network security strategy: An evaluation framework. 1-7.

Cao, Y., Li, S., Lv, C., Wang, D., Sun, H., Jiang, J., Meng, F., Xu, L., & Cheng, X. (2023). Towards cyber security for low-carbon transportation: Overview, challenges and future directions. Renewable and Sustainable Energy Reviews, 183, 113401. https://doi.org/10.1016/j.rser.2023.113401

CVE security vulnerabilities By Types/Categories. (2021, julio 17). Vulnerabilities By Types/Categories. https://www.cvedetails.com/vulnerabilities-by-types.php

Jabiyev, B., Mirzaei, O., Kharraz, A., & Kirda, E. (2021). Preventing server-side request forgery attacks. 1626-1635.

Khodayari, S., Barber, T., & Pellegrino, G. (2024). The Great Request Robbery: An Empirical Study of Client-side Request Hijacking Vulnerabilities on the Web. Proceedings of 45th IEEE Symposium on Security and Privacy.

Marselis, R., Veenendaal, B. van, Geurts, D., & Ruigrok, W. (2020). Quality for DevOps teams. Sogeti.

OWASP Top Ten Proactive Controls 2018 | C5: Validate All Inputs | OWASP Foundation. (2018, julio 17). https://owasp.org/www-project-proactive-controls/v3/en/c5-validate-inputs.html

Pant, P. (2022). Secure web development.

Rahmawati, T., Shiddiq, R. W., Sumpena, M. R., Setiawan, S., Karna, N., & Hertiana, S. N. (2023). Web Application Firewall Using Proxy and Security Information and Event Management (SIEM) for OWASP Cyber Attack Detection. 280-285.

Ravindran, U., & Potukuchi, R. V. (2022). A Review on Web Application Vulnerability Assessment and Penetration Testing. Review of Computer Engineering Studies, 9(1).

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

Wang, E., Chen, J., Xie, W., Wang, C., Gao, Y., Wang, Z., Duan, H., Liu, Y., & Wang, B. (2024). Where URLs Become Weapons: Automated Discovery of SSRF Vulnerabilities in Web Applications. 2024 IEEE Symposium on Security and Privacy (SP), 216-216.