Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

Sección de alumnos: artículo original

Explotación de la vulnerabilidad SSRF

Exploiting the SSRF vulnerability

Darian Morales
Ingeniería Informática - Universidad Nacional de La Matanza
darmorales@alumno.unlam.edu.ar

Agustín Ignacio Contreras
Ingeniería Informática - Universidad Nacional de La Matanza
agucontreras@alumno.unlam.edu.ar

Maximiliano Leonel Morales
Ingeniería En Informática. Universidad Nacional de La Matanza
maxmorales@alumno.unlam.edu.ar

Nicolas Castellino
Ingeniería En Informática - Universidad Nacional de La Matanza
ncastellino@alumno.unlam.edu.ar

Mariano Toloza
Ingeniería En Informática - Universidad Nacional de La Matanza
mariatoloza@alumno.unlam.edu.ar

Referentes Institucionales:

Mg. Jorge Eterovic
Universidad Nacional de La Matanza
eterovic@unlam.edu.ar

Resumen:

Este artículo explora la vulnerabilidad Server-Side Request Forgery (SSRF), una de las principales amenazas en ciberseguridad debido a su capacidad de comprometer redes internas. SSRF permite a un atacante manipular al servidor para que realice solicitudes HTTP hacia recursos no autorizados, lo que puede derivar en acceso a datos confidenciales, exfiltración de información y evasión de controles de seguridad. Se describe el funcionamiento de esta vulnerabilidad, sus variantes, el impacto que puede tener en las empresas y los métodos comunes de explotación. Además, el artículo presenta técnicas de detección y medidas de mitigación que incluyen

validación de entradas, segregación de redes, y monitoreo de tráfico. Concluye destacando la importancia de prácticas de desarrollo seguro y del uso de herramientas de detección como Burp Suite y OWASP Zap para prevenir ataques SSRF.

Abstract:

This article explores the Server-Side Request Forgery (SSRF) vulnerability, one of the main threats in cybersecurity due to its ability to compromise internal networks. SSRF allows an attacker to manipulate the server to make HTTP requests to unauthorized resources, which can result in access to confidential data, exfiltration of information and evasion of security controls. It is described the operation of this vulnerability, its variants, the impact it may have on enterprises and common exploitation methods. In addition, the article presents detection techniques and mitigation measures that include input validation, network segregation, and traffic monitoring. Concludes by highlighting the importance of safe development practices and the use of detection tools such as Burp Suite and OWASP Zap to prevent SSRF attacks.

Palabras Clave: *SSRF, exfiltración de datos, ciberseguridad, mitigación de ataques, validación de entradas*

Key Words: *SSRF, data exfiltration, cybersecurity, attack mitigation, input validation*

Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

I. CONTEXTO

Área del Conocimiento: Seguridad en Redes y Ciberseguridad.
Temática: Este proyecto se centra en el estudio de la vulnerabilidad SSRF (Server-Side Request Forgery), una amenaza que afecta la seguridad de servidores y aplicaciones web, permitiendo a los atacantes manipular peticiones desde el servidor hacia recursos internos o externos no autorizados. La investigación aborda la detección, explotación y mitigación de esta vulnerabilidad, con un enfoque en la protección de redes y datos sensibles dentro de la infraestructura de TI.
Institución que Coordina el Proyecto: Universidad Nacional de La Matanza

II. INTRODUCCIÓN

La vulnerabilidad SSRF (Server-Side Request Forgery) es una amenaza crítica en el ámbito de la ciberseguridad. Permite a los atacantes manipular un servidor para realizar solicitudes HTTP en su nombre, accediendo así a recursos internos de la red que, normalmente, están fuera del alcance del usuario. SSRF se presenta como una debilidad que puede comprometer la confidencialidad e integridad de sistemas internos y externos, especialmente en aplicaciones web conectadas a múltiples servicios [1] [2].

Las principales manifestaciones de ataques SSRF incluyen la exfiltración de datos y la evasión de controles de seguridad, utilizando técnicas avanzadas para evadir medidas de protección como firewalls o listas de control de acceso [3] [4]. Para la detección de esta vulnerabilidad, se emplean técnicas como el análisis de código estático y dinámico, pruebas de penetración y revisión de políticas de seguridad [5]. Herramientas como Burp Suite y OWASP Zap son recomendadas para la detección y mitigación de SSRF, ya que permiten analizar vulnerabilidades en profundidad y realizar pruebas de explotación controladas.

III. MÉTODOS

Para comprender y analizar la recientemente identificada vulnerabilidad Server-Side Request Forgery (SSRF), se aplicarán métodos diseñados para explorar su funcionamiento, impacto y posibles estrategias de mitigación. A continuación, se detallan los enfoques que se emplearán para este estudio inicial.

Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

OBSERVACIÓN Y DOCUMENTACIÓN DE CASOS DE EXPLOTACIÓN

Dado que se trata de una vulnerabilidad recientemente identificada, el primer paso es observar y documentar cómo se manifiesta SSRF en aplicaciones web y sistemas de servidor. Para esto:

- Se realizarán análisis de tráfico en aplicaciones sospechosas, observando patrones de solicitudes HTTP que parecen originarse desde el servidor hacia otros recursos internos o externos.
- Se documentarán instancias en las que el servidor reacciona inesperadamente a entradas manipuladas, identificando cómo los atacantes pueden redirigir estas solicitudes.
- El propósito de este paso es construir un conjunto de casos de uso reales que ejemplifiquen los escenarios en los que SSRF se presenta, ayudando a desarrollar un entendimiento más claro de su potencial de explotación.

ANÁLISIS DEL CÓDIGO FUENTE AFECTADO

Una vez identificados los casos de SSRF, el siguiente paso es analizar el código fuente de las aplicaciones en busca de los puntos de vulnerabilidad:

- Identificación de Entradas y Procesamiento de Solicitudes: Se examinará dónde y cómo las aplicaciones procesan las entradas del usuario, en especial en los puntos donde se permite el ingreso de URLs o direcciones IP.
- Inspección de Validaciones y Filtros: Se revisará si el código incluye validaciones para restringir las solicitudes permitidas. La falta de filtros adecuados en las entradas es un indicador de vulnerabilidad.
- Análisis de las Llamadas HTTP: Este paso implica analizar cómo se configuran y ejecutan las solicitudes HTTP del servidor a otros recursos, permitiendo determinar si un atacante puede influir en el destino de estas solicitudes. Esto ayudará a mapear el flujo de información y a identificar el punto exacto de explotación en el código.

SIMULACIÓN DE ATAQUES CONTROLADOS

Para comprender mejor el alcance de SSRF, se realizarán simulaciones de ataques en un entorno controlado que imiten un intento de explotación:

- Preparación del Entorno: Se creará un entorno de pruebas que simule los recursos internos y externos que el servidor podría acceder bajo condiciones de vulnerabilidad.

Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

- Ejecución de Solicitudes Maliciosas: Mediante herramientas como Burp Suite y OWASP Zap, se generarán solicitudes dirigidas a los puntos de entrada previamente identificados. Las solicitudes incluirán URLs internas y externas para ver si el servidor permite el acceso.
- Observación de Respuestas y Documentación de Resultados: Se documentará cómo responde el servidor a las solicitudes maliciosas, registrando cualquier indicio de acceso no autorizado. Esto ayudará a comprender el impacto potencial de un ataque SSRF exitoso.

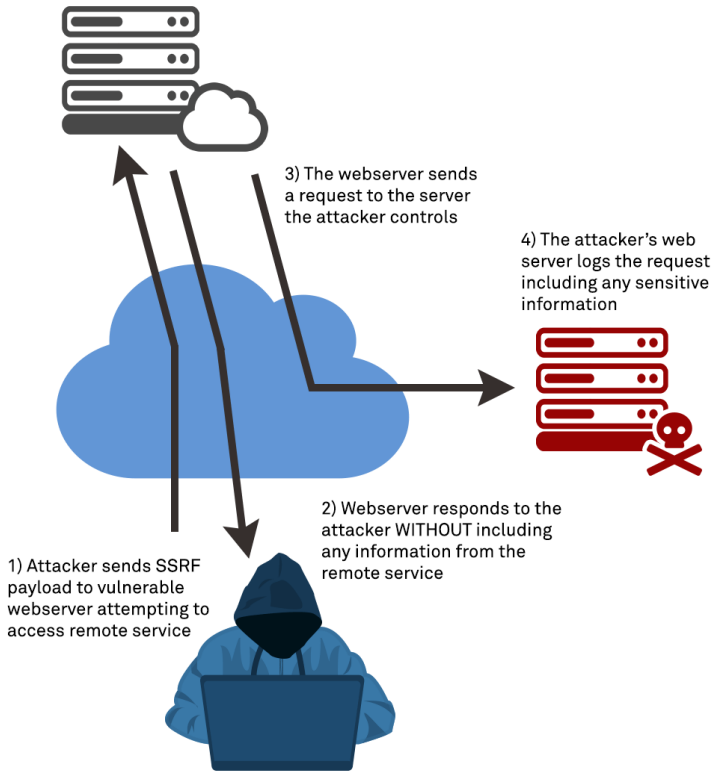

Fig1. Ejemplo de ataque por SSRF

ESTUDIO DE CONFIGURACIONES DE SEGURIDAD EN EL ENTORNO DE PRUEBA

Este paso examina las configuraciones de red y servidor en busca de vulnerabilidades de seguridad que faciliten SSRF:

- Análisis de Configuraciones de Firewalls: Se evaluará la efectividad de los firewalls en el bloqueo de solicitudes externas e internas potencialmente peligrosas.
- Revisión de Listas de Control de Acceso: Las políticas de control de acceso serán auditadas para garantizar que no se permitan solicitudes de recursos no autorizados.

Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

- Políticas de Red y Segmentación de Recursos: Se revisará si los recursos internos están segmentados de manera adecuada para evitar accesos no autorizados. Este análisis es crucial para limitar el impacto de SSRF en caso de explotación.

PROPUESTAS DE MITIGACIÓN

Finalmente, se explorarán y documentarán medidas potenciales para mitigar el impacto de SSRF, tales como restricciones en las solicitudes HTTP generadas por el servidor, validación de entradas, y limitación de acceso a recursos internos. Dado que se trata de un estudio exploratorio, estas medidas se evaluarán inicialmente en un entorno de prueba para determinar su efectividad.

IV. RESULTADOS Y OBJETIVOS

Resultados Alcanzados

1. **Identificación de Patrones de Explotación**: Se logró identificar y documentar los patrones iniciales de explotación de SSRF, incluyendo los flujos de ataque más comunes y los recursos internos comprometidos. Estos resultados son cruciales para crear una base de conocimiento sobre cómo y dónde puede manifestarse esta vulnerabilidad en sistemas reales.
2. **Análisis de Código Fuente y Descubrimiento de Vulnerabilidades**: A través del análisis de código fuente, se identificaron estructuras comunes de desarrollo que permiten la explotación de SSRF. Se demostró que la ausencia de validación y control en los puntos de entrada es una de las principales causas de esta vulnerabilidad, aportando información valiosa para su detección temprana en auditorías de código.
3. **Simulación de Ataques y Evaluación de Impacto**: Las simulaciones de ataques permitieron observar en un entorno controlado los impactos potenciales de SSRF, como la exfiltración de datos y el acceso no autorizado a redes internas. La documentación detallada de estos efectos proporciona un marco de referencia para entender la gravedad de SSRF y su potencial de explotación.
4. **Propuestas de Mitigación Efectivas**: A partir de los estudios realizados, se formularon y probaron estrategias de mitigación que resultaron eficaces en la contención de SSRF. Estas medidas incluyen la validación de entradas, la segregación de redes y la implementación de listas blancas. Los resultados de esta evaluación proporcionan una guía para la implementación de protecciones contra SSRF en entornos similares.

Revista Digital del Departamento de
Ingeniería e Investigaciones Tecnológicas
de la Universidad Nacional de La Matanza
ISSN: 2525-1333

Vol.: 9 - Nro. 2 (Diciembre - 2024)

Objetivos en Curso o Futuros del Proyecto

1. **Desarrollo de Herramientas de Detección Automática de SSRF**: Continuar con el desarrollo de herramientas que automatizan la detección de patrones de SSRF en aplicaciones y redes, utilizando técnicas de análisis estático y dinámico. Estas herramientas podrán integrarse en procesos de desarrollo seguro para detectar SSRF de forma preventiva.
2. **Estudio de SSRF en Nuevas Tecnologías y Aplicaciones**: Ampliar el estudio de SSRF hacia tecnologías emergentes, como microservicios y entornos de computación en la nube, donde las interacciones entre servicios pueden incrementar los riesgos. Este objetivo incluye el análisis de las configuraciones específicas de estas tecnologías y su vulnerabilidad ante SSRF.
3. **Capacitación y Concientización en Desarrollo Seguro**: Desarrollar programas de capacitación para ingenieros de software y profesionales de seguridad en prácticas de desarrollo seguro y detección de SSRF. Esta capacitación estará orientada a prevenir la introducción de vulnerabilidades SSRF desde las etapas iniciales de desarrollo.
4. **Colaboración y Difusión de los Resultados**: Establecer colaboraciones con otras instituciones académicas y empresas para compartir los hallazgos sobre SSRF, promoviendo una respuesta colectiva y el desarrollo de estándares de seguridad más rigurosos en la comunidad de ciberseguridad.
5. **Implementación de Monitoreo Continuo y Respuesta Temprana**: Desarrollar sistemas de monitoreo en tiempo real que detecten patrones de tráfico inusuales y posibles intentos de explotación de SSRF, permitiendo una respuesta rápida ante incidentes. Estos sistemas se basarán en inteligencia de amenazas y aprenderán de intentos previos de ataque.

V. CONCLUSIONES

El presente estudio sobre la vulnerabilidad Server-Side Request Forgery (SSRF) ha permitido entender sus manifestaciones, impacto y métodos de mitigación. A través de la identificación de patrones de explotación y simulaciones en entornos controlados, se evidenció el riesgo significativo que representa SSRF para la confidencialidad y seguridad de los recursos internos de una organización. La validación de entradas y la configuración segura de servidores se identificaron como medidas preventivas clave, junto con la necesidad de herramientas automatizadas para la detección temprana de SSRF en aplicaciones. Los objetivos futuros incluyen el desarrollo de estas herramientas, la capacitación en prácticas de desarrollo seguro y la colaboración interinstitucional en ciberseguridad. En conclusión, SSRF presenta desafíos críticos en la

seguridad de redes, y una respuesta proactiva, combinada con monitoreo continuo y una cultura de desarrollo seguro, será clave para su prevención efectiva en el panorama tecnológico actual.

VI. REFERENCIAS Y BIBLIOGRAFÍA

[1] E. Wang, J. Chen, W. Xie, *et al.*, "Where URLs Become Weapons: Automated Discovery of SSRF Vulnerabilities in Web Applications," en *IEEE Symposium on Security and Privacy*, 2024.

[2] Y. Cao, S. Li, C. Lv, *et al.*, "Towards Cyber Security for Low-Carbon Transportation: Overview, Challenges and Future Directions," *Renewable and Sustainable Energy Reviews*, 2023.

[3] B. Jabiyev, O. Mirzaei, A. Kharraz, y E. Kirda, "Preventing Server-Side Request Forgery Attacks," 2021.

[4] S. Khodayari, T. Barber, y G. Pellegrino, "The Great Request Robbery: An Empirical Study of Client-side Request Hijacking Vulnerabilities on the Web," en *IEEE Symposium on Security and Privacy*, 2024.

[5] U. Ravindran y R. V. Potukuchi, "A Review on Web Application Vulnerability Assessment and Penetration Testing," *Review of Computer Engineering Studies*, 2022.

[6] F. González Martínez, A. S. Meneses Ruiz, H. R. González Brito, y Y. Trujillo Casañola, "Tendencias en las vulnerabilidades y ataques SSRF," *Serie Científica de la Universidad de las Ciencias Informáticas*, julio 2024. [En línea]. Disponible en: https://publicaciones.uci.cu/index.php/serie/article/view/1626/1331.

[7] Baehost, "Vulnerabilidad Blind SSRF en WordPress," *Baehost Blog*, enero 2024. [En línea]. Disponible en: https://blog.baehost.com/vulnerabilidad-blind-ssrf-en-wordpress/.

[8] OWASP, "OWASP Top 10: 2021. A10:2021 – Falsificación de Solicitudes del Lado del Servidor (SSRF)." [En línea]. Disponible en: https://owasp.org/Top10/es/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/.

Recibido: 2024-09-10
Aprobado: 2024-12-02
Hipervínculo Permanente: https://doi.org/10.54789/reddi.9.2.6
Datos de edición: Vol. 9 -Nro. 2 - SA. 2
Fecha de edición: 2024-12-30