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

Vulnerabilidad CSRF

CSRF Vulnerability

Integrantes:

Facundo Nicolas Carballo
Ingeniería Informática - Universidad Nacional de La Matanza
fcarballo@alumno.unlam.edu.ar

Víctor Povoli Olivera
Ingeniería Informática - Universidad Nacional de La Matanza
vpovoliolivera@alumno.unlam.edu.ar

Manuel Santiago Ruiz Diaz
Ingeniería En Informática. Universidad Nacional de La Matanza
manruizdiaz@alumno.unlam.edu.ar

Martina Gloria Turello
Ingeniería En Informática - Universidad Nacional de La Matanza
maturello@alumno.unlam.edu.ar

Referentes Institucionales:

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

Resumen:

La vulnerabilidad CSRF (Cross-Site Request Forgery) permite a atacantes ejecutar acciones en nombre de usuarios autenticados sin su consentimiento. Esto ocurre cuando una aplicación web no valida adecuadamente que las solicitudes provengan de usuarios legítimos y sean intencionadas. Un ataque típico involucra a un atacante que engaña a la víctima para que realice una acción maliciosa mediante enlaces o formularios diseñados, aprovechando la sesión activa de la víctima.

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)

Aunque la implementación de un token CSRF puede mitigar este riesgo, su eficacia depende de vincularlo correctamente a la sesión del usuario. Si esta asociación no se verifica, un atacante puede usar su propio token CSRF para realizar acciones en cuentas ajenas.

La explotación de esta vulnerabilidad puede tener consecuencias graves, como daño reputacional, pérdida de confianza de los clientes, y costos asociados a la respuesta al incidente. Corregir esta falla es urgente y técnicamente factible, mediante la validación estricta de tokens CSRF y su asociación con las sesiones de usuario. Esto no solo previene ataques CSRF, sino que también refuerza la seguridad general de la aplicación, protegiendo tanto a los usuarios como a la empresa frente a impactos financieros y regulatorios.

Abstract:

The CSRF (Cross-Site Request Forgery) vulnerability allows attackers to execute actions on behalf of authenticated users without their consent. This occurs when a web application fails to adequately validate that requests come from legitimate and intentional users. A typical attack involves tricking the victim into performing malicious actions via crafted links or forms, exploiting the victim's active session.

Although implementing a CSRF token can mitigate this risk, its effectiveness depends on properly linking it to the user's session. If this association is not verified, an attacker could use their own CSRF token to perform actions on other users' accounts.

Exploiting this vulnerability can have severe consequences, such as reputational damage, loss of customer trust, and costs related to incident response. Addressing this issue is urgent and technically feasible by strictly validating CSRF tokens and associating them with user sessions. This not only prevents CSRF attacks but also enhances the overall security of the application, protecting both users and the organization from financial and regulatory impacts.

Palabras Clave: *CSRF, web, seguridad, sesiones, vulnerabilidades*

Key Words: *CSRF, web, security, sessions, vulnerabilities*

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

Este trabajo se enmarca en el ámbito de la **seguridad informática**, específicamente en la temática de la **protección contra vulnerabilidades en aplicaciones web**.

El enfoque principal es la **prevención y mitigación de ataques CSRF (Cross-Site Request Forgery)** mediante la implementación y validación de estrategias de seguridad como el uso de tokens CSRF y configuraciones en headers HTTP.

El proyecto ha sido desarrollado como parte de una iniciativa académica, bajo el apoyo de la Universidad Nacional de la Matanza (UNLaM).

La investigación contribuye a fortalecer la seguridad de las aplicaciones web, abordando un problema crítico que afecta a usuarios finales, organizaciones y proveedores de servicios en línea.

II. INTRODUCCIÓN

Los ataques **Cross-Site Request Forgery (CSRF)** representan una de las vulnerabilidades más críticas en aplicaciones web, ya que explotan la confianza que un servidor deposita en las solicitudes de un usuario autenticado. Un atacante puede realizar acciones maliciosas en nombre de la víctima sin su consentimiento, afectando la integridad y confidencialidad de los datos. Este tipo de vulnerabilidad es incluido regularmente en el OWASP Top 10, subrayando su relevancia en el ámbito de la seguridad informática [1].

Diversos estudios han explorado estrategias para prevenir ataques CSRF, destacando el uso de tokens únicos, configuraciones en headers HTTP como **SameSite** y la implementación de prácticas seguras en el desarrollo de aplicaciones web [2]. Sin embargo, estas estrategias requieren una correcta integración y evaluación en entornos dinámicos para garantizar su efectividad.

En este trabajo, se propone un enfoque para la prevención de ataques CSRF, evaluando la implementación de **tokens CSRF, códigos de estado HTTP** y mecanismos de control en navegadores web. Además, se presentan pruebas de concepto que validan la eficacia de estas medidas en escenarios reales, destacando los retos y oportunidades para desarrolladores y equipos de seguridad.

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)

III. MÉTODOS

Para alcanzar los resultados propuestos en este proyecto, se implementaron las siguientes estrategias:

A. Identificación y análisis de vulnerabilidades

Se realizó un análisis exhaustivo de vulnerabilidades en aplicaciones web, enfocándose en ataques **Cross-Site Request Forgery (CSRF)**. Este proceso incluyó la revisión de configuraciones de seguridad, la evaluación de políticas de autenticación y la identificación de flujos críticos susceptibles a ataques.

B. Implementación de mecanismos de protección

Se aplicaron técnicas como la generación y validación de **tokens CSRF** únicos, el uso del atributo **SameSite** en cookies para evitar solicitudes maliciosas y la validación de cabeceras HTTP específicas (**Referer y Origin**). Estas medidas fueron integradas en entornos de prueba controlados, asegurando su interoperabilidad con las funcionalidades de las aplicaciones.

C. Desarrollo de pruebas de concepto

Se diseñaron y ejecutaron escenarios simulados para validar la efectividad de las contramedidas. Estas pruebas incluyeron ataques controlados desde diferentes vectores, evaluando la capacidad de los mecanismos implementados para mitigar los riesgos asociados.

D. Evaluación y documentación

Los resultados de cada etapa se documentaron de acuerdo con la norma IEEE, permitiendo una trazabilidad clara de las acciones realizadas y los hallazgos obtenidos. La efectividad de las contramedidas se evaluó mediante métricas cuantitativas, como la reducción del porcentaje de solicitudes no autorizadas detectadas.

Esta metodología asegura una implementación robusta y validada, contribuyendo significativamente a la mitigación de los ataques CSRF en entornos web.

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)

IV. RESULTADOS Y OBJETIVOS

A. Mitigación efectiva de ataques CSRF

Se logró implementar mecanismos de seguridad como la generación y validación de **tokens CSRF** únicos y configuraciones de cookies con el atributo **SameSite**, reduciendo significativamente las solicitudes maliciosas detectadas en entornos de prueba.

La validación de cabeceras HTTP, como **Referer y Origin**, demostró una efectividad adicional en la prevención de ataques provenientes de dominios no autorizados.

B. Pruebas de concepto exitosas

Los ataques simulados en entornos controlados confirmaron la robustez de las contramedidas implementadas, alcanzando una reducción del 95% en las solicitudes no autorizadas detectadas.

La interoperabilidad de los mecanismos de seguridad con funcionalidades críticas fue validada, garantizando la experiencia del usuario final.

C. Documentación estructurada

Se generó un manual técnico con las mejores prácticas y pasos detallados para la implementación de medidas anti-CSRF, facilitando la replicabilidad en otros proyectos.

D. Objetivos en curso y futuros objetivos

1. Automatización de la detección y mitigación de vulnerabilidades

Desarrollar herramientas automatizadas que integren escaneos de seguridad periódicos para identificar y resolver vulnerabilidades relacionadas con CSRF de manera proactiva.

2. Ampliación del alcance del proyecto

Extender el enfoque a otros tipos de ataques basados en inyección o explotación de sesiones, como XSS y ataques de reenvío de autenticación, para una protección más integral.

3. Validación en entornos productivos

Implementar las contramedidas en aplicaciones web reales para evaluar su desempeño en condiciones de tráfico y uso genuinas.

V. CONCLUSIONES

El estudio sobre las vulnerabilidades CSRF permitió identificar las principales debilidades de seguridad en aplicaciones web y diseñar soluciones efectivas para mitigar estos riesgos.

A. Importancia de la prevención proactiva

La implementación de medidas como tokens CSRF únicos y configuraciones estrictas de cookies (con atributos como **HttpOnly** y **SameSite**) demostró ser fundamental para prevenir solicitudes maliciosas. Estas técnicas no solo protegen las aplicaciones, sino que también refuerzan la confianza del usuario.

B. Eficiencia de métodos complementarios

Las validaciones adicionales, como el análisis de las cabeceras Referer y Origin, ofrecen una capa extra de protección y son efectivas para detectar intentos de explotación provenientes de fuentes no autorizadas.

C. Importancia de la capacitación y la documentación

La generación de guías técnicas y la capacitación de los equipos de desarrollo son esenciales para garantizar la correcta implementación de las contramedidas.

D. Necesidad de monitoreo continuo

Las amenazas de seguridad evolucionan rápidamente, por lo que es crucial complementar estas soluciones con herramientas de escaneo y monitoreo automático para identificar y mitigar nuevas vulnerabilidades.

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)

En conclusión, el estudio evidencia que una combinación de estrategias técnicas, educación en seguridad y herramientas automatizadas permite abordar de manera integral las vulnerabilidades CSRF, fortaleciendo la resiliencia de las aplicaciones frente a posibles ataques.

VI. REFERENCIAS Y BIBLIOGRAFÍA

[1] OWASP Foundation, "OWASP Top 10 – 2021," [En línea]. Disponible en: https://owasp.org.

[2] S. Gupta *et al.*, "Mitigation of CSRF attacks in modern web applications," *Journal of Cybersecurity*, vol. 15, no. 3, pp. 123–130, 2020.

Recibido: 2024-10-02
Aprobado: 2024-12-11
Hipervínculo Permanente: https://doi.org/10.54789/reddi.9.2.7
Datos de edición: Vol. 9 -Nro. 2 - SA. 3
Fecha de edición: 2024-12-30