Tipo de artículo: Artículo de revisión

Tendencia en las vulnerabilidades CSRF entre 2018 y 2024

Trend in CSRF vulnerabilities between 2018 and 2024

Daniel Bonilla Mosquera[1*], https://orcid.org/0009-0004-9967-8168
Juan Fernando Gonzalez Lopez[2], https://orcid.org/0009-0009-6465-6993
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. daniel.bonilla@usc.edu.co
[2] Facultad de Ingeniería, Universidad Santiago de Cali. Colombia. juan.gonzalez08@usc.edu.co
[3] Dirección de Seguridad Informática, Universidad de las Ciencias Informáticas. Cuba. henryraul@uci.cu
[4] Facultad de Tecnologías Interactivas, Universidad de las Ciencias Informáticas. Cuba. yaimi@uci.cu

*** Autor para correspondencia: daniel.bonilla@usc.edu.co**

Resumen

El objetivo de la investigación fue analizar las vulnerabilidades de ataques *Cross-site Request Forgery* (CSRF), se revisó datos estadísticos recientes y reportes internacionales. Se llevó a cabo una revisión sistemática basada en las siguientes preguntas: ¿Cuál es la tendencia en detecciones de ataques CSRF? ¿Qué son y cómo se manifiestan los ataques CSRF? ¿Cuáles son las principales técnicas para identificar este tipo de vulnerabilidad? ¿Qué herramientas se emplean para identificar este tipo de vulnerabilidad? Las bases de datos utilizadas fueron IEEE, ACM, Elsevier, y Springer Link, abarcando el período de 2018 a 2024, con el objetivo de identificar medidas y herramientas para mitigar las vulnerabilidades de ataques CSRF. Los resultados indican que anualmente se reporta una media de 690,33 ataques CSRF, con un incremento notable cada año. Las principales técnicas para identificar ataques CSRF incluyen la verificación de las solicitudes provengan de fuentes legítimas y la validación de tokens anti-CSRF antes de realizar cualquier acción. Las herramientas más utilizadas para identificar estas vulnerabilidades son ZAP, Burp Suite, Acunetix y PhishTank. Las medidas identificadas para mitigar estas vulnerabilidades se centran en la correcta configuración de las aplicaciones web y el uso de tokens CSRF en las peticiones a la base de datos. Se concluye que las vulnerabilidades de ataques CSRF son una amenaza significativa para la transformación digital, destacando la necesidad de implementar métodos preventivos robustos.

Palabras clave: vulnerabilidades; ciberseguridad; ataques web; CSRF; ataques CSRF

Abstract

The objective of the research was to analyze the vulnerabilities of Cross-site Request Forgery (CSRF) attacks, reviewing recent statistical data and international reports. A systematic review was carried out based on the following questions: What is the trend in CSRF attack detections? What are CSRF attacks and how do they manifest themselves? What are the main techniques for identifying this type of vulnerability? What tools are used to identify this type of vulnerability? The databases used were IEEE, ACM, Elsevier, and Springer Link, covering the period from 2018 to 2024, with the objective of identifying measures and tools to mitigate CSRF attack vulnerabilities. The results indicate that an average of 690.33 CSRF attacks are reported annually, with a notable increase each year. The main techniques for identifying CSRF attacks include verifying that requests come from legitimate sources and validating anti-CSRF tokens before taking any action. The most commonly used tools to identify these vulnerabilities are ZAP, Burp Suite, Acunetix and PhishTank. The measures identified to mitigate these vulnerabilities focus on the correct configuration of web applications and the use of CSRF tokens in database requests. It is concluded that CSRF attack vulnerabilities are a significant threat to digital transformation, highlighting the need to implement robust preventative methods.

Keywords: *vulnerabilities; cybersecurity; Web attacks; CSRF; CSRF attacks*

Recibido: 01/07/2024
Aceptado: 14/07/2024
En línea: 19/07/2024

Introducción

En la actualidad, el panorama digital de la ciberseguridad se encuentra en cambio constante. Los ciberdelincuentes se encuentran al acecho, diseñando nuevas estrategias con el fin de vulnerar los sistemas que utilizan a diario, ya sean aplicaciones web o móviles. La conexión a internet, como la principal herramienta de interacción a nivel global, y su crecimiento exponencial han aumentado de manera considerable los ciberataques, que en muchos casos han dejado graves consecuencias no solo para personas naturales sino también para empresas y organizaciones (Sessions, 2019).

Para enfrentar dichos retos, los profesionales del área de las tecnologías de la información y las comunicaciones (TIC) deben contar habilidades para salvaguardar la confidencialidad, integridad y disponibilidad de la información (Howard *et al.*, 2023). Estos profesionales deben supervisar los entornos que los usuarios emplean en su día a día, prevenir el acceso no autorizado y, sobre todo, proteger la información confidencial de las personas u organizaciones (Yadav and Parekh, 2017).

Varias son las tecnologías para el desarrollo integrado de aplicaciones web que facilitan la labor de los profesionales: Django, Ruby, Spring o Laravel. Estas tecnologías han enfrentado ataques de tipo *Cross-Site Request Forgery* (CSRF) (Swacha and Kulpa, 2023). Una de las causas de los ataques del tipo CSRF a las aplicaciones web se debe a vulnerabilidades halladas en las cookies, principalmente por deficiencia en las configuraciones (Squarcina *et al.*, 2023).

Un ataque CSRF es una vulnerabilidad de seguridad en aplicaciones web que permite a un atacante diseñar solicitudes maliciosas en nombre de un usuario autenticado (Yadav and Parekh, 2017). En este tipo de ataque, el atacante induce al usuario a realizar acciones no deseadas en una aplicación en la que el usuario está autenticado, sin que el usuario sea consciente de ello. Esto ocurre debido a que el usuario se encuentra autenticado en un sitio de confianza pero realizando acciones no deseadas sin que se dé cuenta (Sitohang, Asnar and Saptawati, 2024).

El objetivo de la presente investigación es analizar los ataques de tipo CSRF a través de una revisión sistemática de la bibliografía entre los años 2018 a 2024 teniendo en cuenta las siguientes preguntas científicas:

- ¿Cuál es la tendencia en detecciones de ataques CSRF?

- ¿Qué es y cómo se manifiestan los ataques de inyección CSRF?
- ¿Cuáles son las principales técnicas para identificar este tipo de vulnerabilidad?
- ¿Qué herramientas se emplean para identificar este tipo de vulnerabilidad?

Después de responder estas preguntas se realizó un análisis de la información obtenida evaluando las estrategias más efectivas al momento de proteger los portales web de ataques de este tipo y a los usuarios; así como también cuales son las herramientas utilizadas para identificar y mitigar este tipo de vulnerabilidad.

Materiales y métodos

Entre los métodos de trabajo científico 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: Este método se utilizó para realizar un análisis de tendencia de las vulnerabilidades y ciberataques desde el 2018 al 2024. Se revisaron investigaciones recientes y reportes internacionales para identificar patrones y cambios en la naturaleza de los ataques CSRF. El objetivo fue entender con qué frecuencia se ejecutan estos ataques, y cómo las medidas de mitigación han sido implementadas y adaptadas en respuesta.
- Analítico - sintético: Se empleó este método para analizar y sintetizar los conceptos clave relacionados con la ciberseguridad, las vulnerabilidades y los ataques CSRF. Este análisis permitió identificar y resumir las principales amenazas que enfrentan las aplicaciones web, destacando las similitudes y diferencias entre distintos tipos de ataques y sus impactos en la seguridad de las aplicaciones.
- Revisión sistemática a la bibliografía: Se llevó a cabo una revisión sistemática de la literatura para reunir evidencia que demuestre la necesidad de investigar los ataques CSRF. Se revisaron artículos académicos y científicos e informes de seguridad y bases de datos de vulnerabilidades que documentaron incidentes y tendencias de ataques entre 2018 y 2024. Este enfoque permitió identificar las áreas más críticas y las brechas en el conocimiento actual sobre las vulnerabilidades CSRF.

Estos métodos se combinaron para dar guía a la presente investigación.

Resultados y discusión

En el presente artículo se describen los resultados obtenidos de la investigación, con el objetivo de identificar las principales técnicas para detectar vulnerabilidades asociadas a los ataques de tipo CSRF, cómo se manifiestan estos

ataques, las herramientas utilizadas para su identificación, las medidas de mitigación y las tendencias en detección de ataques CSRF.

¿Cuál es la tendencia en detecciones de ataques CSRF?

Los ataques *Cross-Site Request Forgery* son una amenaza importante para las aplicaciones web debido a que se van adaptando nuevas tecnologías y métodos para conseguir aprovecharse de las vulnerabilidades de las aplicaciones web, utilizando técnicas de ingeniería social o *phishing* para afectar a usuarios específicos (M, 2024). Las redes sociales también se han convertido en una fuente recurrente para realizar ataques CSRF mediante diferentes formatos como links anexados a imágenes, vídeos, contenidos multimedia, entre otros. Revisando la información de las vulnerabilidades reportadas en el portal CVEdetails.com dentro de los años 2018 y 2024, se evidencia que hay un crecimiento exponencial, estos datos se muestran en la Tabla 1.

Tabla 1. Registro de reportes de diferentes vulnerabilidades descubiertas en aplicaciones web desde el año 2018 hasta el 2023.

Año	Numero de Reportes
2018	479
2019	560
2020	416
2021	520
2022	769
2023	1398
Total	4142
Media	**690,33**

Fuente: Elaborado a partir de www.cvedetails.com.

Los datos reflejados en la Tabla 1 se analizan en la Figura 1, y se toma una media para definir el promedio de ataques entre los años 2018 y 2023. A partir de 2021, se observa una marcada tendencia al alza, alcanzando un pico significativo en 2023 con 1398 reportes. Este aumento destaca la creciente exposición de los usuarios debido a la mayor cantidad de aplicaciones que requieren autenticación por inicios de sesión. El análisis de comportamiento de estos datos permite establecer una línea de tendencia que pronostica el crecimiento constante en el número de vulnerabilidades de tipo CSRF en los próximos años.

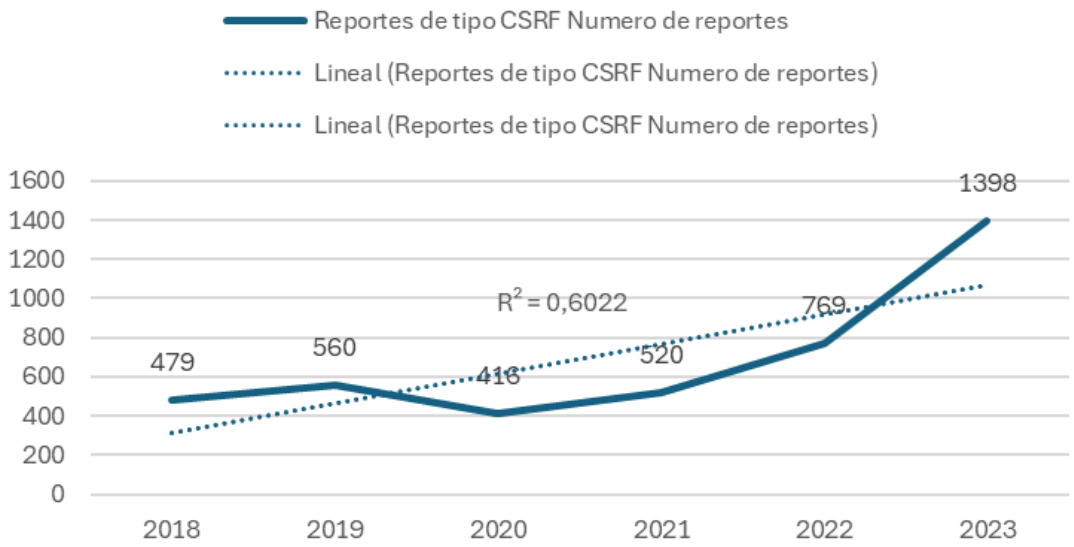

Figura 1. Análisis de tendencia en los reportes de vulnerabilidades CSRF en aplicaciones web.

Fuente: Elaboración propia a partir de CVDetails.com.

¿Qué son y cómo se manifiestan los ataques CSRF?

Un ataque CSRF es un tipo de ataque enfocado a aplicaciones web donde un adversario engaña a un usuario autenticado dentro de un sitio web seguro (Nagpal, Chauhan and Singh, 2017). Este tipo de ataque es peligroso debido a que induce al usuario a que realice acciones no deseadas en la aplicación en la que está autenticado, de manera que se explota la confianza que la aplicación web otorga al navegador del usuario (Ranimäki, 2023).

En la Figura 2 se representa el escenario de un ataque básico CSRF. En esta el ataques se manifiestan por la vulnerabilidad en las transacciones web, donde el contenido de una aplicación maliciosa A inicia solicitudes en la aplicación sitio de confianza B, dentro de la sesión de confianza por medio de una autenticación iniciada por el usuario, donde el navegador tratará estas peticiones como parte de la sesión en curso con B. Dichas solicitudes pueden ser transacciones bancarias o la explotación del buzón de correo o la libreta de la víctima sin que el usuario se percate de estas peticiones maliciosas (Alex *et al.*, 2004).

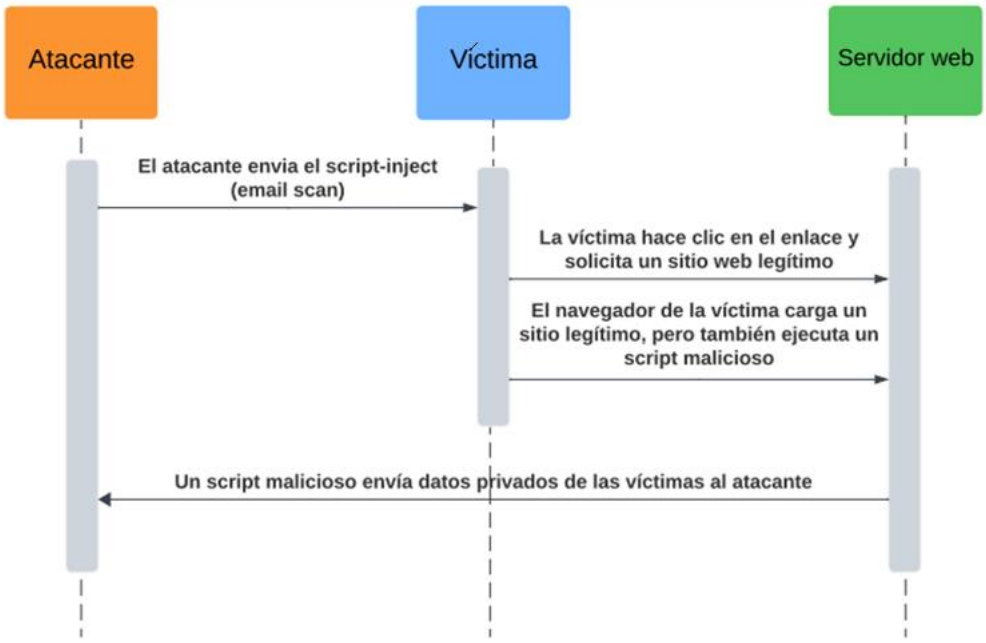

Figura 2. Escenario de ataque CSRF básico.

Fuente: Elaboración propia a partir de (Kshetri *et al.*, 2024).

¿Qué técnicas se emplean para mitigar la vulnerabilidad CSRF?

Existen diferentes técnicas para identificar si una aplicación web es vulnerable a estos ataques, las más básicas incluyen realizar una revisión del código de la aplicación web en busca de secciones de formularios o entradas de datos donde falte la validación de tokens anti-CSRF (Siahaan *et al.*, 2023). La información consultada sobre los ataques CSRF sugiere que, la técnica de protección más efectiva contra este tipo de ataques se realiza en el servidor mediante tokens de validación únicos aplicados a los formularios web, los cuales, al ser enviados, el servidor verifica la validez del token antes de ejecutar la acción solicitada por el usuario.

Un token CSRF es un valor único que se incluye en los formularios y solicitudes sensibles, cuando el servidor recibe una solicitud verifica que el token proporcionado por la solicitud coincida con el token esperado antes de ser procesada la solicitud. En la Figura 3 se muestra fragmento de código que ejemplifica una manera de incluir un campo oculto con el token. Cuando el usuario envía el formulario, el navegador incluye el token CSRF junto con los otros datos en la solicitud al servidor. Al recibir la solicitud, el servidor recupera el token y lo compara con el token almacenado en la sesión del usuario, si los tokens coinciden, la solicitud se considera valida, de lo contrario se rechaza y se protege contra un ataque de este tipo.

```
<form action="/transferir" method="POST">
  <input type="hidden" name="csrf_token" value="TOKEN_GENERADO">
  <input type="text" name="cuenta_destino">
  <input type="number" name="cantidad">
  <input type="submit" value="Transferir">
</form>
```

Figura 3. Fragmento de código que incluye un campo oculto con token.

Fuente: Elaboración Propia.

¿Qué herramientas se emplean para identificar vulnerabilidades de tipo CSRF?

Entre las herramientas más empleadas para identificar vulnerabilidades CSRF se encuentran:

- ZAP: Es una herramienta gratuita y de código abierto mantenida por OWASP que escanea aplicaciones web en busca de diversas vulnerabilidades, que incluyen CSRF. Proporciona análisis automatizados y manuales, es fácil de usar y altamente configurable (Shah and Lad, 2021).
- Burp Suite: Conjunto de herramientas de pruebas de seguridad web ampliamente utilizado que permite la detección y explotación de vulnerabilidades. Ofrece un proxy interceptor, un escáner de vulnerabilidades, y herramientas de explotación avanzadas (Thaqi, Vishi and Rexha, 2022).
- Acunetix: herramienta comercial de análisis de seguridad web que identifica y reporta vulnerabilidades CSRF junto con otras fallas de seguridad. Brinda un escaneo automatizado, informes detallados e integración con entornos de desarrollo CI/C (Hadavi and Sadeghi, 2021).
- PhishTank Database: Base de datos que contiene una lista negra de correos no deseados y sitios usados frecuentemente por atacantes para secuestrar sesiones de usuarios. Ayuda a identificar sitios maliciosos que podrían estar involucrados en ataques de este tipo.(Shah, Varshney and Mehrotra, 2024).

El uso de estas herramientas es crucial para identificar y mitigar vulnerabilidades de tipo CSRF en aplicaciones web. Estas proporcionan una combinación de escaneo automatizado, análisis manual y explotación avanzada, lo que permite una cobertura adecuada para la detección de vulnerabilidades de seguridad. La utilización de múltiples herramientas es beneficioso porque cada una ofrece capacidades únicas y enfoques complementarios para detectar y analizar vulnerabilidades, con el fin de asegurar así una protección más robusta y completa contra estos ataques.

Conclusiones

De acuerdo con los datos revisados de los reportes de vulnerabilidades entre los años 2018 a 2023 existe una tendencia al aumento de estos ataques con un pico considerable en el 2023 con relación a los años anteriores. Para dar solución a este tipo de vulnerabilidades, es necesario que los desarrolladores implementen tokens únicos para cada cliente y para cada transacción HTTP. Durante la investigación se identificaron herramientas para el escaneo activo como ZAProxy, Burp Suite entre otras que permiten detectar la presencia de esta vulnerabilidad mediante auditorias de seguridad.

Esta investigación se propone como trabajo futuro el estudio de casos de reales y experimentos para analizar la puesta en práctica de las herramientas y medidas recomendadas en esta investigación. Otra línea de trabajo sería abordar nuevas técnicas para detección de vulnerabilidades de tipo CSRF desde etapas tempranas del desarrollo de software que incluyan la realización de pruebas estáticas al código fuente generado.

Agradecimientos

Agradecemos a la Universidad Santiago de Cali por brindarnos una sólida formación durante nuestro pregrado. Sus docentes y compañeros fueron una fuente constante de inspiración y apoyo; También a la Universidad de las Ciencias Informáticas de Cuba por permitirnos cursar el diplomado que amplió nuestros conocimientos y perspectivas en ciberseguridad y en calidad de software. Los profesionales, expertos y compañeros con los que interactuamos a lo largo de nuestro proceso académico los cuales fueron fundamentales para nuestro crecimiento académico.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.
2. Análisis formal: Juan Fernando Gonzalez Lopez y Daniel Bonilla Mosquera.
3. Investigación: Juan Fernando Gonzalez Lopez y Daniel Bonilla Mosquera.
4. Metodología: Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.

5. Administración del proyecto: Juan Fernando Gonzalez Lopez y Daniel Bonilla Mosquera.
6. Recursos: Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.
7. Supervisión: Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.
8. Visualización: Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.
9. Redacción – Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.
10. Redacción – Juan Fernando Gonzalez Lopez, Daniel Bonilla Mosquera, Henry Raul Gonzalez Brito y Yaimi Trujillo Casañola.

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Alex, B. et al. (2004) 'Spring security reference', URL https://docs. spring. io/springsecurity/site/docs/current/reference/htmlsingle/.[utoljára megtekintve: 2017. 04. 21.], 12. Available at: https://docs.spring.io/spring-security/site/docs/5.2.1.RELEASE/reference/pdf/spring-security-reference.pdf (Accessed: 18 July 2024).

Hadavi, M.A. and Sadeghi, S. (2021) 'Automatic Black-Box Detection of Resistance Against CSRF Vulnerabilities in Web Applications', Journal of Computing and Security, 8(1), pp. 19–32.

Howard, H. et al. (2023) 'Confidential Consortium Framework: Secure Multiparty Applications with Confidentiality, Integrity, and High Availability'. arXiv. Available at: http://arxiv.org/abs/2310.11559 (Accessed: 17 July 2024).

Kshetri, N. et al. (2024) 'algoXSSF: Detection and analysis of cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks via Machine learning algorithms', in 2024 12th International Symposium on Digital Forensics and Security (ISDFS). IEEE, pp. 1–8. Available at: https://ieeexplore.ieee.org/abstract/document/10527278/ (Accessed: 17 July 2024).

M, B. (2024) 'Mitigating Cross-Site Request Forgery Vulnerabilities: Evaluating Current Strategies and Proposing Defense Mechanisms'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.4783867.

Nagpal, B., Chauhan, N. and Singh, N. (2017) 'SECSIX: security engine for CSRF, SQL injection and XSS attacks', International Journal of System Assurance Engineering and Management, 8(S2), pp. 631–644. Available at: https://doi.org/10.1007/s13198-016-0489-0.

Ranimäki, M. (2023) Web security and hacking. Master's Thesis. Itä-Suomen yliopisto. Available at: https://erepo.uef.fi/bitstream/handle/123456789/30146/urn_nbn_fi_uef-20230812.pdf?sequence=1 (Accessed: 18 July 2024).

Sessions, C.L. (2019) Exploring Personal Protection Strategies of Cybersecurity Specialists in Social Media. PhD Thesis. Colorado Technical University. Available at: https://search.proquest.com/openview/b144ea60bdc59ce1f00225034ce9dfb9/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 16 July 2024).

Shah, A., Varshney, S. and Mehrotra, M. (2024) 'Threats on online social network platforms: classification, detection, and prevention techniques', Multimedia Tools and Applications, pp. 1–33. Available at: https://doi.org/10.1007/s11042-024-19724-5.

Shah, M. and Lad, H. (2021) 'Efficient Classification of True Positive and False Positive XSS and CSRF Vulnerabilities Reported by the Testing Tool', in Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Springer, Singapore, pp. 871–884. Available at: https://doi.org/10.1007/978-981-16-0733-2_62.

Siahaan, C.N. et al. (2023) 'Study of Cross-Site Request Forgery on Web-Based Application: Exploitations and Preventions', Procedia Computer Science, 227, pp. 92–100.

Sitohang, B., Asnar, Y.D.W. and Saptawati, G.A.P. (2024) 'Securing Cross-Site Request Forgery Vulnerabilities in Web Applications Using Mutation Analysis', in 2024 2nd International Conference on Software Engineering and Information Technology (ICoSEIT). IEEE, pp. 227–232. Available at: https://ieeexplore.ieee.org/abstract/document/10497499/ (Accessed: 18 July 2024).

Squarcina, M. et al. (2023) 'Cookie crumbles: breaking and fixing web session integrity', in 32nd USENIX Security Symposium (USENIX Security 23), pp. 5539–5556. Available at: https://www.usenix.org/conference/usenixsecurity23/presentation/squarcina (Accessed: 17 July 2024).

Swacha, J. and Kulpa, A. (2023) 'Evolution of popularity and multiaspectual comparison of widely used web development frameworks', Electronics, 12(17), p. 3563.

Thaqi, R., Vishi, K. and Rexha, B. (2022) 'Enhancing Burp Suite with Machine Learning Extension for Vulnerability Assessment of Web Applications', Journal of Applied Security Research, pp. 1–19. Available at: https://doi.org/10.1080/19361610.2022.2096387.

Yadav, P. and Parekh, C.D. (2017) 'A report on CSRF security challenges & prevention techniques', in 2017 international conference on innovations in information, embedded and communication systems (ICIIECS). IEEE, pp. 1–4. Available at: https://ieeexplore.ieee.org/abstract/document/8275852/ (Accessed: 18 July 2024).