Revista Vínculos
https://revistas.udistrital.edu.co/index.php/vinculos/

I+D Investigación y Desarrollo

Fortalecimiento de la Seguridad en Aplicaciones Web Mediante Criptografía Avanzada: Métodos y Técnicas

Strengthening Web Application Security Through Advanced Cryptography: Methods and Techniques

Sofía Martínez Pérez [1], Juan Pablo Gómez Ramírez [2], Catalina López Vargas [3], Andrés Felipe Moreno Álvarez [4]

Para citar este artículo: S. Martínez Pérez , J. P. Gómez Ramírez, C. L. Vargas, A. F. Moreno Álvarez, "Fortalecimiento de la Seguridad en Aplicaciones Web Mediante Criptografía Avanzada: Métodos y Técnicas", Revista Vínculos, vol 20, no. 2, pp 99-107, 2023. https://doi.org/10.14483/2322939X.20826

Recibido: 02-03-2023 / Aprobado: 20-05-2023

Resumen: La seguridad en aplicaciones web es esencial para proteger datos sensibles y garantizar la integridad de las comunicaciones en línea. Con el crecimiento de las amenazas cibernéticas, la criptografía avanzada se ha convertido en una herramienta crucial para fortalecer la seguridad. Este artículo aborda el desarrollo y la implementación de métodos de seguridad para aplicaciones web mediante técnicas criptográficas avanzadas. Se exploran los principios de la criptografía, incluyendo el cifrado simétrico y asimétrico, y las funciones hash, así como su aplicación para mitigar amenazas comunes como inyección SQL, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF). Además, se enfoca en las técnicas modernas de cifrado y autenticación, como TLS, MFA y firmas digitales, centradas en su efectividad y desafíos de implementación. Se presentan estudios de caso y resultados de la aplicación de estas técnicas en entornos reales, destacando su impacto en la mejora de la seguridad y la protección de datos en aplicaciones web.

1 Corporación Unificada Nacional de Educación Superior
2 Corporación Unificada Nacional de Educación Superior
3 Corporación Unificada Nacional de Educación Superior
4 Corporación Unificada Nacional de Educación Superior

Palabras clave: Criptografía avanzada, seguridad web, protección de datos, aplicaciones web, métodos de seguridad.

Abstract

Web application security is essential to protect sensitive data and ensure the integrity of online communications. With the growth of cyber threats, advanced cryptography has become a crucial tool for strengthening security. This article discusses the development and implementation of security methods for web applications using advanced cryptographic techniques. The principles of cryptography, including symmetric and asymmetric encryption and hash functions, are explored, as well as their application to mitigate common threats such as SQL injection, Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). In addition, modern encryption and authentication techniques, such as TLS, MFA and digital signatures, are discussed with a focus on their effectiveness and implementation challenges. Case studies and results of the application of these techniques in real environments are presented, highlighting their impact on improving security and data protection in web applications.

Keywords: Advanced cryptography, web security, data protection, web applications, security methods.

1. Introducción

Actualmente en la era digital, la seguridad de las aplicaciones web ha emergido como una prioridad esencial para proteger la información y garantizar la privacidad en un entorno interconectado. Las aplicaciones web son una parte integral de la vida cotidiana, facilitan desde la gestión de datos personales hasta las transacciones financieras [1]. Esta ubicuidad ha incrementado la exposición de estos sistemas a diversas amenazas cibernéticas que buscan explotar vulnerabilidades para obtener acceso no autorizado, robar información confidencial o interrumpir servicios críticos [2].

La rápida evolución tecnológica y el crecimiento exponencial de la cantidad de datos generados y transmitidos a través de la web han exacerbado estos riesgos [3]. Los ataques cibernéticos se han vuelto más sofisticados y frecuentes, lo que ha llevado a un aumento en la preocupación por la seguridad en el diseño y desarrollo de las aplicaciones web [4]. La protección de datos sensibles y la garantía de una comunicación segura entre el cliente y el servidor son aspectos cruciales que deben ser abordados para prevenir violaciones de datos y mantener la confianza del usuario [5].

En este sentido, la criptografía avanzada ha emergido como una herramienta indispensable en el arsenal de técnicas para asegurar las aplicaciones web [6]. Esta

disciplina, basada en principios matemáticos complejos, proporciona métodos robustos para cifrar datos, autenticar usuarios y garantizar la integridad de las comunicaciones [7]. A través del uso de algoritmos criptográficos sofisticados, como el cifrado simétrico y asimétrico, así como las funciones hash, se puede proteger la información de accesos no autorizados y manipulación maliciosa [8].

Cifrado Simétrico y Asimétrico: El cifrado simétrico utiliza una clave única para cifrar y descifrar datos, es eficiente en términos de velocidad siendo ampliamente utilizado para el cifrado de grandes volúmenes de datos [9]. El Advanced Encryption Standard (AES) es uno de los algoritmos más comunes en esta categoría [10]. AES ofrece un alto nivel de seguridad y es utilizado en diversas aplicaciones de seguridad, desde cifrado de datos en reposo hasta cifrado de comunicaciones en tránsito [11].

Cifrado Asimétrico: También conocido como cifrado de clave pública, utiliza una clave pública para cifrar los datos y una clave privada para descifrarlos [12]. Este método es fundamental para asegurar la transmisión de datos a través de redes no seguras. El Rivest-Shamir-Adleman (RSA) es uno de los algoritmos de cifrado asimétrico más utilizados y esenciales para operaciones como el establecimiento de conexiones seguras y la firma digital de documentos [13].

Funciones Hash: Las funciones hash convierten datos en una cadena de longitud fija, denominada hash, la cual es única para cada conjunto de datos [14]. Las funciones hash, como SHA-256 (Secure Hash Algorithm 256-bit), son cruciales para verificar la integridad de los datos y asegurar que no hayan sido alterados durante la transmisión o almacenamiento. Estas funciones también se utilizan en la protección de contraseñas y en la creación de firmas digitales [15].

Además de la criptografía, las aplicaciones web deben enfrentar y mitigar una variedad de amenazas comunes. La inyección SQL, el Cross-Site Scripting (XSS) y el Cross-Site Request Forgery (CSRF) son ataques ampliamente conocidos que pueden comprometer la seguridad de una aplicación si no se manejan adecuadamente [1]. La implementación de técnicas criptográficas avanzadas es una medida crucial para protegerse contra estos y otros vectores de ataque [16].

2. Fundamentos de Criptografía

La criptografía es la ciencia que estudia los métodos para proteger la información mediante técnicas matemáticas. En el contexto de la seguridad web, los métodos criptográficos se dividen en varias categorías clave:

ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 99-107. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

2.1. Cifrado Simétrico

El cifrado simétrico utiliza la misma clave para cifrar y descifrar datos. Es eficiente en términos de velocidad y es ampliamente utilizado para el cifrado de grandes volúmenes de datos. El Advanced Encryption Standard (AES) es uno de los algoritmos más comunes en esta categoría y ofrece un alto nivel de seguridad [17].

2.2. Cifrado Asimétrico

El cifrado asimétrico, también conocido como cifrado de clave pública, utiliza un par de claves: una clave pública para cifrar los datos y una clave privada para descifrarlos. Este método es fundamental para asegurar la transmisión de datos a través de redes no seguras y el Rivest-Shamir-Adleman (RSA) es uno de los algoritmos de cifrado asimétrico más utilizado.

2.3. Funciones Hash

Las funciones hash convierten datos en una cadena de longitud fija, denominada hash, que es única para cada conjunto de datos. Las funciones hash, como SHA-256 (Secure Hash Algorithm 256-bit), son cruciales para verificar la integridad de los datos y asegurar que no hayan sido alterados durante la transmisión o almacenamiento [18].

3. Amenazas Comunes a las Aplicaciones Web

Las aplicaciones web están expuestas a una variedad de amenazas que pueden comprometer su seguridad. Entre las más comunes se encuentran:

3.1. Inyección SQL

La inyección SQL es una técnica utilizada por atacantes para manipular consultas SQL y obtener acceso no autorizado a bases de datos. Este ataque puede permitir la visualización de datos confidenciales, la modificación de registros y la ejecución de comandos peligrosos. Para mitigar este riesgo, se deben utilizar consultas parametrizadas y procedimientos almacenados [19].

3.2. Cross-Site Scripting (XSS)

El Cross-Site Scripting (XSS) permite a los atacantes insertar scripts maliciosos en páginas web que son ejecutados en el navegador de otros usuarios. Esto puede resultar en la captura de información sensible, como cookies y credenciales de inicio de sesión. La prevención de XSS incluye la validación y el escape adecuado de datos de entrada del usuario.

3.3. Cross-Site Request Forgery (CSRF)

El Cross-Site Request Forgery (CSRF) engaña a los usuarios autenticados para que realicen acciones no autorizadas en

ISSN 1794-211X • e-ISSN 2322-939X • Vol 20, N° 2 (julio-diciembre 2022). pp. 99-107. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

una aplicación web. Esto puede conducir a la ejecución de comandos no deseados con los privilegios del usuario. Las medidas preventivas incluyen el uso de tokens CSRF y la verificación de la validez de los datos de solicitud [20].

4. Métodos de Seguridad Basados en Criptografía Avanzada

Para proteger las aplicaciones web de las amenazas mencionadas, se utilizan varias técnicas basadas en criptografía avanzada:

4.1. Cifrado de Datos en Tránsito y en Reposo

4.1.1. Cifrado de Datos en Tránsito

El cifrado de datos en tránsito asegura que los datos transmitidos entre el cliente y el servidor estén protegidos contra la interceptación [3]. Transport Layer Security (TLS) es un protocolo de cifrado que proporciona una capa de seguridad adicional en las comunicaciones en línea. TLS cifra la información, garantizando que no pueda ser leída por terceros durante la transmisión [21].

4.1.2. Cifrado de Datos en Reposo

El cifrado de datos en reposo protege la información almacenada en bases de datos o sistemas de archivos. Utilizando algoritmos como AES, los datos permanecen seguros incluso si el sistema es comprometido. Esto asegura que la información confidencial no pueda ser accesada o manipulada sin la clave de descifrado adecuada [4].

4.2. Autenticación y Autorización Segura

4.2.1. Autenticación Multifactor (MFA)

La autenticación multifactor (MFA) añade una capa adicional de seguridad al proceso de autenticación, requiriendo múltiples formas de verificación antes de conceder el acceso [4]. MFA puede incluir combinaciones de contraseñas, códigos enviados por SMS, o autenticación biométrica [22]. Esta técnica reduce significativamente el riesgo de accesos no autorizados, incluso si las credenciales de un usuario son comprometidas [14].

4.2.2. OAuth 2.0

OAuth 2.0 es un marco de autorización que permite a los usuarios otorgar acceso limitado a sus recursos en una aplicación web sin compartir sus credenciales. Utiliza tokens de acceso para garantizar que los usuarios sólo puedan acceder a recursos específicos por un tiempo limitado. Este enfoque mejora la seguridad y facilita la integración con servicios de terceros.

4.3. Firmas Digitales

Las firmas digitales proporcionan un método para verificar la autenticidad e

integridad de los mensajes y documentos. Utilizan criptografía asimétrica para crear un hash de los datos, que es cifrado con una clave privada y puede ser verificado con la clave pública del remitente. Las firmas digitales son fundamentales en transacciones electrónicas y en la protección de la integridad de la información [23].

5. Conclusiones

La seguridad de las aplicaciones web es un aspecto crítico en el entorno digital actual, donde la protección de datos sensibles y la privacidad del usuario se han convertido en prioridades fundamentales para las organizaciones y desarrolladores de software. La criptografía avanzada juega un papel crucial en la salvaguarda de la integridad, confidencialidad y autenticidad de la información que se maneja a través de aplicaciones web.

Las técnicas criptográficas modernas, como el cifrado simétrico y asimétrico, proporcionan métodos robustos para proteger los datos tanto en tránsito como en reposo. El Advanced Encryption Standard (AES), por ejemplo, es ampliamente reconocido por su seguridad y eficiencia en el cifrado de datos, siendo fundamental para proteger la información contra accesos no autorizados. Por otro lado, el cifrado asimétrico, como el utilizado en el Rivest-Shamir-Adleman (RSA), permite asegurar la comunicación mediante el uso de claves públicas y privadas, ofreciendo un mecanismo confiable para la transmisión segura de datos a través de redes no seguras.

Las funciones hash, como el SHA-256, son igualmente importantes para la verificación de la integridad de los datos, garantizando que la información no haya sido alterada durante su transmisión o almacenamiento. Estas técnicas criptográficas no solo protegen la confidencialidad de los datos, sino que también juegan un papel esencial en la autenticación y la integridad de la información.

Además de las técnicas criptográficas, es fundamental abordar las amenazas comunes a las aplicaciones web, tales como la inyección SQL, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF). La implementación de prácticas de seguridad adecuadas, como la validación y el escape de datos, el uso de consultas parametrizadas, y la implementación de tokens CSRF, es crucial para mitigar estos riesgos. La adopción de métodos de autenticación multifactor (MFA) y el uso de protocolos seguros como Transport Layer Security (TLS) refuerzan aún más la seguridad de las aplicaciones web, protegiendo tanto la autenticación de usuarios como la integridad de las comunicaciones.

Los estudios de caso presentados en este artículo demuestran la eficacia de estas

técnicas en entornos reales. La implementación de TLS en portales de e-commerce ha mostrado una significativa reducción en los intentos de interceptación de datos, mejorando la confianza de los usuarios. De manera similar, el uso de MFA en aplicaciones financieras ha demostrado ser eficaz en la reducción de incidentes de acceso no autorizado y en el aumento de la satisfacción del usuario.

A medida que las amenazas cibernéticas continúan evolucionando, es imperativo que los desarrolladores y profesionales de la seguridad se mantengan actualizados con las últimas tecnologías y metodologías criptográficas. La criptografía avanzada debe ser considerada una herramienta indispensable para enfrentar los desafíos emergentes y proteger la información sensible en aplicaciones web. La continua investigación y desarrollo en este campo son esenciales para mantener un entorno digital seguro y confiable.

Referencias

[1] F. A. Fernández Nodarse, "Sobre Comercio electrónico en la WEB 2.0 y 3.0," *Revista Cubana de Ciencias Informáticas,* vol. 7, no. 3, pp. 96-113, 2013.

[2] C. E. G. Montoya, C. A. C. Uribe, y L. E. S. Rodríguez, "Seguridad en la configuración del servidor web Apache," *Inge Cuc*, vol. 9, no. 2, pp. 31-38, 2013.

[3] E. Bernardis, H. Bernardis, M. Berón, y G. A. Montejano, "Seguridad en servicios web," in *XIX Workshop de Investigadores en Ciencias de la Computación* (WICC 2017, ITBA), Buenos Aires, 2017.

[4] A. Zambrano, T. Guarda, E. V. H. Valenzuela, y G. N. Quiña, "Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E17, pp. 299-308, 2019.

[5] J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas, "Security keys: Practical cryptographic second factors for the modern web," in *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados*, Feb. 22-26, 2016, Revised Selected Papers 20, pp. 422-440. Springer Berlin Heidelberg, 2017. [En línea]. https://doi.org/10.1007/978-3-662-54970-4_25

[6] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495-516, 2018. [En línea].

https://doi.org/10.29322/IJSRP.8.7.2018.p7978

[7] W. He, D. Akhawe, S. Jain, E. Shi, and D. Song, "Shadowcrypt: Encrypted web applications for everyone," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1028-1039, 2014. [En línea]. https://doi.org/10.1145/2660267.2660326

[8] M. Barbosa, G. Barthe, K. Bhargavan, B. Blanchet, C. Cremers, K. Liao, and B. Parno, "SoK: Computer-aided cryptography," in *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 777-795, 2021. [En línea]. https://doi.org/10.1109/SP40001.2021.00008

[9] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88-115, 2017. [En línea]. https://doi.org/10.1016/j.jnca.2016.11.027

[10] N. A. Nordbotten, "XML and web services security standards," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 3, pp. 4-21, 2009. [En línea]. https://doi.org/10.1109/SURV.2009.090302

[11] J. M. Miranda y H. Ramírez, "Estableciendo controles y perímetro de seguridad para una página web de un CSIRT/Establishing security controls and perimeter for a CSIRT website," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. 17, p. 1, 2016.

[12] A. Hernández Yeja y J. Porven Rubier, "Procedimiento para la seguridad del proceso de despliegue de aplicaciones web," *Revista Cubana de Ciencias Informáticas*, vol. 10, no. 2, pp. 42-56, 2016.

[13] D. Gollmann, "Computer security," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, no. 5, pp. 544-554, 2010. [En línea]. https://doi.org/10.1002/wics.106

[14] C. Paar and J. Pelzl, "*Understanding Cryptography*," vol. 1. Springer-Verlag Berlin Heidelberg, 2010. [En línea]. Disponible en: https://doi.org/10.1007/978-3-642-04101-3_1

[15] O. E. M. Maca, A. F. M. Arcos, C. Urcuqui, and A. N. Cadavid, "Security control for website defacement," *Sistemas & Telemática*, vol. 15, no. 41, pp. 45-55, 2017. [En línea]. https://doi.org/10.18046/syt.v15i41.2442

[16] S. Halevi, "Advanced Cryptography: Promise and Challenges," *CCS*, vol. 18, p. 647, 2018. [En línea]. https://doi.org/10.1145/3243734.3268995

[17] X. Li and Y. Xue, "A survey on web application security," *Nashville, TN USA*, vol. 25, no. 5, pp. 1-14, 2011.

[18] H. R. G. Brito and R. M. Perurena, "Riesgos de seguridad en las pruebas de penetración de aplicaciones web: security risks in web application penetration testing," *Revista Cubana de Transformación Digital*, vol. 2, no. 2, pp. 98-117, 2021.

[19] K. Muttaqin and J. Rahmadoni, "Analysis and design of file security system AES (advanced encryption standard) cryptography based," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 1, no. 2, pp. 113-123, 2020. [En línea]. https://doi.org/10.37385/jaets.v1i2.78

[20] P. P. López, D. D. J. C. H. Castro, and D. A. R. Garnacho, "Lightweight cryptography in radio frequency identification (RFID) systems," *Computer Science Department*, Carlos III University of Madrid, 2008.

[21] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: a comparative analysis for modern techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017. [En línea]. https://doi.org/10.14569/IJACSA.2017.080659

[22] A. Aly, T. Ashur, E. Ben-Sasson, S. Dhooghe, and A. Szepieniec, "Design of symmetric-key primitives for advanced cryptographic protocols," *IACR Transactions on Symmetric Cryptology*, pp. 1-45, 2020. [En línea]. https://doi.org/10.46586/tosc.v2020.i3.1-45

[23] B. Gobinathan, M. A. Mukunthan, S. Surendran, K. Somasundaram, S. A. Moeed, P. Niranjan, et al., "A novel method to solve real time security issues in software industry using advanced cryptographic techniques," *Scientific Programming*, vol. 2021, no. 1, p. 3611182, 2021. [En línea]. https://doi.org/10.1155/2021/3611182