https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 108 - 117

Aplicación de pruebas de seguridad informática para sitios web institucionales

Application of cybersecurity testing for institutional websites

Información del reporte:

Para citar este reporte técnico:

Aguilar Domínguez, A. (2026). Aplicación de pruebas de seguridad informática para sitios web institucionales. *Cuadernos Técnicos Universitarios de la DGTIC, 4* (1), páginas (108 - 117). https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157

Angie Aguilar Domínguez
Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México
angie.aguilar@comunidad.unam.mx
ORCID: 0009-0007-7590-0678

Resumen

Como parte de los servicios institucionales proporcionados por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación hacia la comunidad de TI universitaria, se cuenta con el servicio de realización de pruebas de penetración web, que forman parte de las medidas de seguridad que ayudan a robustecer la protección tanto de los sitios y los usuarios finales, como de la información que se maneja. La metodología empleada para la realización de las pruebas es una adecuación a partir de las metodologías existentes en la industria, en la que se combina la ejecución de herramientas automatizadas que se sumaron a la revisión manual por parte del equipo de trabajo. Los resultados obtenidos son ponderados de acuerdo con la calculadora *Common Vulnerability Scoring System* del *Forum of Incident Response and Security Teams*, para establecer su nivel de criticidad. Como resultado de la prestación de este servicio, se apoya a distintas áreas universitarias a reforzar la seguridad no sólo de sus aplicaciones web, sino también del entorno en el que se despliegan y de la información que manejan. La importancia de la realización de las pruebas de seguridad web puede verse en el aumento de revisiones realizadas en el periodo 2024-2025, sobre todo en las de seguimiento. Se destaca el interés por parte de las áreas universitarias en mejorar este aspecto de la infraestructura tecnológica que gestionan para beneficio de la comunidad universitaria.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 109 - 117

Palabras clave: Despliegue de aplicaciones web institucionales, *pentest* de aplicaciones web, seguridad informática en aplicaciones web, vulnerabilidades en aplicaciones web.

Abstract

As part of the institutional services provided by the Dirección General de Cómputo y de Tecnologías de Información y Comunicación to the university's IT community, a web penetration testing service is offered. These tests are part of the security measures that help strengthen the protection of websites, end users, and the information they handle. The methodology used for conducting the tests is an adaptation of existing industry methodologies, combining the execution of automated tools with manual review by the team. The results obtained are weighted according to the Common Vulnerability Scoring System calculator of the Forum of Incident Response and Security Teams to establish their level of criticality. As a result of providing this service, various university areas are supported in strengthening the security not only of their web applications but also of the environment in which they are deployed and the information they handle. The importance of conducting web security tests can be seen in the increase in reviews carried out in the 2024-2025 period, especially in follow-up reviews, highlighting the interest on the part of university areas in improving this aspect of the technological infrastructure they manage for the benefit of the university community.

Keywords: *Computer security in web applications, deployment of institutional web applications, pentest of web applications, vulnerabilities in web applications.*

1. INTRODUCCIÓN

El propósito de la prestación del servicio de pruebas de seguridad web para la UNAM es "fortalecer la seguridad de las redes sociales y las páginas oficiales de la Universidad" (Universidad Nacional Autónoma de México, Dirección General de Cómputo y de Tecnologías de Información y Comunicación, 2022). Por ello se debe entender que la revisión en materia de seguridad informática para los sitios web de la Universidad es una medida preventiva necesaria, ya que busca disminuir la exposición de vulnerabilidades una vez que los sitios sean publicados, las cuales, si no son atendidas de forma preventiva, pueden derivar en incidentes de seguridad.

Adicionalmente, en el entorno de la seguridad en aplicaciones web, es importante tener presente que "el proceso de aplicación de pruebas de penetración puede ser una forma de evaluar el nivel de seguridad de un sistema. Cuanto más potente sea la prueba de penetración, más completa será la evaluación de las debilidades/fortalezas del sistema" (Bertoglio y Zorzo, 2017, p.2).

Dado lo anterior, el servicio proporcionado se fundamenta en marcos de referencia como el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) y el *Forum of Incident Response and Security Teams* (FIRST), que son empleados en la industria para la realización de las pruebas. Esto permite sistematizar su ejecución y entregar resultados ordenados por nivel de criticidad para su atención.

Finalmente, es relevante recordar que, aunque las pruebas podrían aplicarse a sitios que ya se encuentran en un entorno productivo, en este caso se abordan sólo aquellos que se encuentran próximos a su publicación.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 110 - 117

El objetivo de este reporte técnico es describir y comparar el servicio de realización de las pruebas de penetración en aplicaciones web durante el periodo 2024-2025, con el fin de dar a conocer un servicio institucional, así como evidenciar su contribución al interior de la Universidad en el reforzamiento de aspectos de seguridad informática en sitios web antes de su publicación.

2. DESARROLLO TÉCNICO

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) proporciona el servicio de Pruebas de penetración y análisis de vulnerabilidades en aplicaciones web, el cual ayuda al adecuado despliegue de aplicaciones web mediante la revisión de seguridad informática, para lo cual se sigue la metodología de *pentest* establecida en la industria.

De acuerdo con Tudosi, Graur, Balan y Potorac (2023): "La principal diferencia entre un ataque informático y una prueba de penetración es que los hackers irrumpen para robar y causar daños, mientras que los pentesters alertan sobre vulnerabilidades de seguridad explotables y ayudan a corregirlas". Así pues, las pruebas de penetración que se llevan a cabo por parte de los revisores se encuentran limitadas al objetivo previamente establecido, se realizan en entornos controlados, en ventanas de tiempo que han sido acordadas y, sobre todo, cuentan con la autorización de los responsables del sitio.

Cuando una entidad o dependencia busca publicar un sitio web, requiere cubrir una serie de requisitos a nivel técnico. Al solicitar el servicio, lo primero que debe realizarse es un respaldo del sitio web y su base de datos, así como evitar modificar el sitio durante el periodo de revisión. Posteriormente, se debe agendar la fecha para llevar a cabo las pruebas de seguridad necesarias. Actualmente, la solicitud puede realizarse mediante un ticket en la plataforma de Gestión de Servicios TIC o mediante la Oficina Central de Correspondencia. En ambos casos se deben proporcionar los datos solicitados para dar inicio al proceso de revisión.

Lo anterior, junto con la autorización para la realización de las pruebas, permite su desarrollo de manera coordinada entre el solicitante y el equipo de revisores, lo que habilita una comunicación constante para lograr el seguimiento adecuado de posibles complicaciones como, por ejemplo, la pérdida de conectividad hacia el sitio.

De esta forma, la revisión de seguridad se lleva a cabo considerando que: "Mediante la ejecución de pruebas que simulan ataques activos, imitando el comportamiento real de un actor malicioso, se pueden evaluar las vulnerabilidades en diversos activos de información, ya sea de forma manual o automática. Este proceso, en última instancia, facilita la identificación de las estrategias de defensa y respuesta más eficaces" (Moreno et al., 2025, p. 2).

Esto es de gran ayuda para identificar cuáles son los puntos débiles que pueden ser aprovechados por usuarios maliciosos, así como para determinar las medidas de mitigación y recomendaciones de seguridad que serán entregadas a los responsables de las aplicaciones para solventar los hallazgos reportados.

A partir de lo anterior, se genera un reporte con los hallazgos derivados de la revisión, los cuales se ponderan de acuerdo con el impacto que pueden tener y cómo éste afecta la confidencialidad, disponibilidad e integridad del sitio web, así como la información que contiene, los usuarios y la infraestructura tecnológica relacionada.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 111 - 117

El documento contiene una serie de recomendaciones que se apoyan en los estándares y buenas prácticas realizadas por autoridades en materia de seguridad informática como, por ejemplo, el *National Institute of Standards and Technology* (NIST), MITRE, el top 10 de vulnerabilidades web publicado por OWASP, así como referencias a la documentación oficial en el rubro de seguridad de CMS, lenguajes de programación como PHP o Java, bibliotecas de terceros, *frameworks*, repositorios, entre otros.

Una vez entregado el reporte a los responsables de la aplicación web para su atención, se espera la implementación de medidas que ayuden a solventar los puntos señalados en el documento. Cuando el equipo responsable de solventar las vulnerabilidades indica que han sido atendidas, es necesario llevar a cabo una revisión de seguimiento para verificar la adecuada implementación de las configuraciones de seguridad. No se define un periodo de tiempo específico para la atención de los hallazgos, debido a que cada entidad o dependencia universitaria gestiona sus actividades de acuerdo con su carga de trabajo, infraestructura y prioridades institucionales, por lo que son los responsables de atender el reporte tomando en consideración lo anterior.

Durante la revisión de seguimiento, no se realiza nuevamente un escaneo en busca de vulnerabilidades, sino que el trabajo se centra en verificar la solución de los hallazgos reportados. En caso de existir hallazgos persistentes debido a que no se tomaron medidas o a que su aplicación no fue adecuada, se entrega un segundo reporte de seguimiento, el cual contiene tanto los hallazgos que no fueron atendidos como los nuevos que se encuentren durante la verificación y que pueden afectar la seguridad del sitio web.

Adicionalmente, se comunica a los responsables de la aplicación que, en caso de llevar a cabo una migración de sistema operativo o una versión mayor en cuanto a los componentes empleados (por ejemplo, el *framework* de desarrollo o bibliotecas de terceros), es necesario llevar a cabo una nueva prueba de seguridad debido a los cambios realizados.

Finalmente, en caso de que los hallazgos del primer o segundo reporte sean solventados favorablemente, el sitio revisado puede continuar con su proceso de liberación en el entorno productivo.

2.1 METODOLOGÍA

La metodología empleada obedece a una propuesta de adaptación propia de acuerdo con las necesidades de seguridad de la comunidad de TI de la Universidad, la cual es una versión modificada de la metodología empleada en la industria para las pruebas de penetración (*pentest*). Se tomó como referencia la información proporcionada por OWASP en su apartado referente al *Web Application Security Testing* (OWASP, s. f.), así como las 7 fases propuestas por el *Penetration Testing Execution Standard* (PTES) (Penetration Testing Execution Standard, s. f.).

Se realizan pruebas de caja negra que "consisten en imitar las acciones de un atacante que no tiene información sobre la empresa ni su red corporativa. Así es precisamente como la gran mayoría de los hackers se ven obligados a actuar: utilizando todas las herramientas disponibles para identificar y explotar vulnerabilidades en el sistema de seguridad. En la mayoría de los casos, encuentran fallos de seguridad" (Khamdamov y Ibrokhimov, 2021, p.1). Por lo anterior, se desarrollan las siguientes etapas:

- Planificación y determinación del alcance: Se notifica que se lleva a cabo una revisión de caja negra. Adicionalmente, se establece de común acuerdo qué otros elementos descubiertos durante la revisión quedarán fuera del alcance.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 112 - 117

- Reconocimiento: Acercamiento al sitio web, información pública (si existe), posibles usuarios, entre otros.
- Análisis y escaneo: Revisión con distintas herramientas (manuales y automatizadas).
- Explotación: En ocasiones, se trabaja con pruebas de concepto para evitar afectaciones mayores o a otros elementos fuera del alcance.
- Generación del reporte: Se documentan las vulnerabilidades y se emite un reporte técnico.

Las etapas anteriores evitan directamente la explotación de la vulnerabilidad; tampoco se mantiene el acceso en caso de lograrse. Esto obedece a que la revisión debe mantenerse dentro del alcance acordado con la entidad o dependencia universitaria, y descartar otros elementos que puedan encontrarse durante la revisión.

En cuanto a las herramientas empleadas para llevar a cabo el proceso de revisión de seguridad, se emplea Acunetix, en conjunto con la suite de Kali, para tener un entorno controlado durante la realización de las pruebas. De la suite de Kali, se emplean aquellas herramientas que puedan reportar con mayor precisión algún hallazgo, por ejemplo, si se revisa un sitio en WordPress, entonces se hace uso de WPScan.

En la Tabla 1, se pueden observar las características que permitieron la selección de Acunetix como una de las herramientas que se emplean en la etapa automatizada y que se complementan con otras de la suite de Kali y la revisión manual:

Tabla 1

Elementos considerados para la selección de Acunetix

	Acunetix	Burp Suite Professional	OWASP ZAP
Tiempo de respuesta	Rápido y automatizado	Depende de la configuración	Lento en aplicaciones grandes
Capacidad de procesar múltiples sitios	Alto	Medio (depende de la capacidad de procesamiento del equipo donde está instalado)	Limitado-Medio (depende de la capacidad de procesamiento del equipo donde está instalado)
Soporte y mantenimiento	Soporte del fabricante (de acuerdo con lo contratado)	Soporte del fabricante y comunidad amplia	Comunidad *open source*
Falsos positivos	Bajo	Bajo-Moderado (requiere configuración adicional)	Moderado

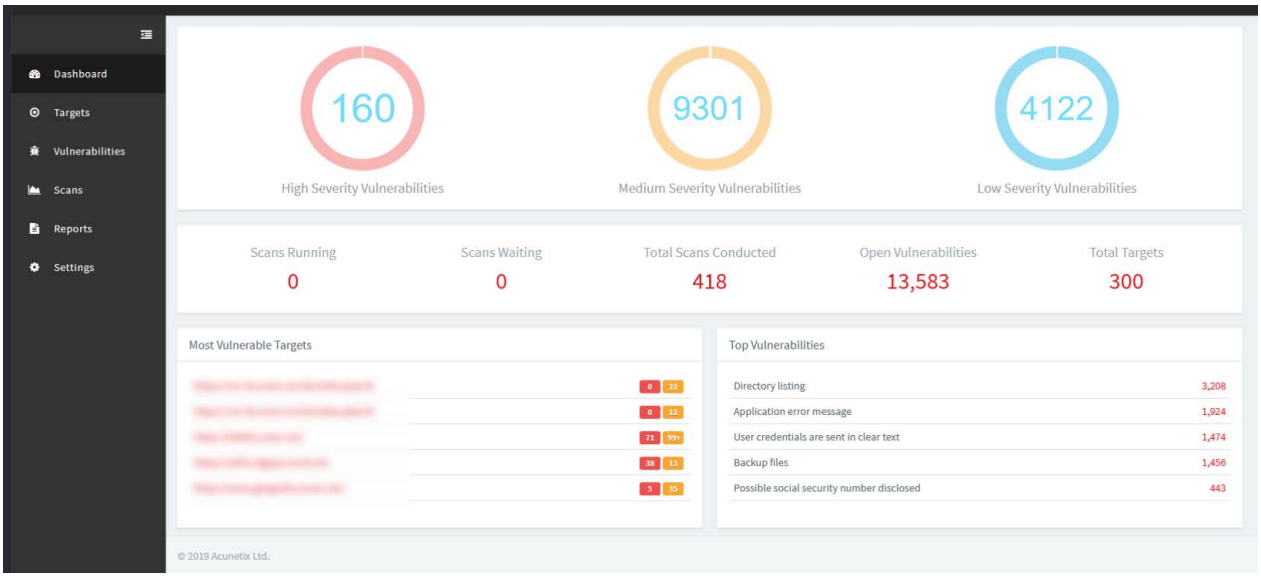
Nota. La tabla se elaboró tomando en consideración la experiencia en el uso de las herramientas durante la realización de las revisiones.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 113 - 117

En la Figura 1 se puede observar el tablero con el resumen de la ejecución de la herramienta automatizada empleada durante la revisión.

Figura 1

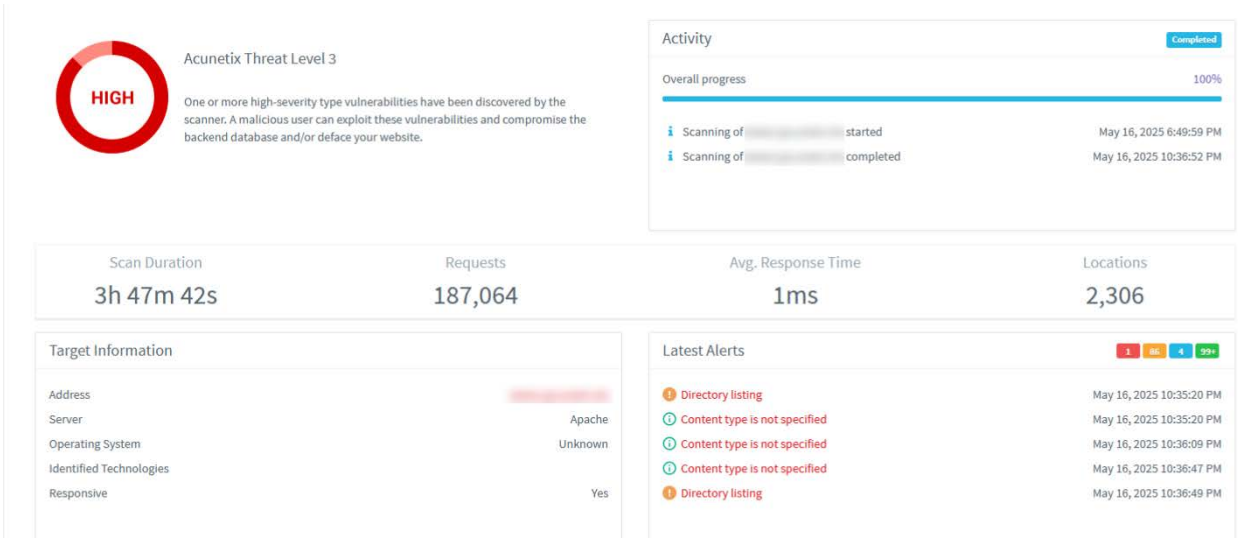
Salida proporcionada por la herramienta Acunetix durante la realización de las pruebas



En la Figura 2 puede observarse el detalle de la ejecución de la herramienta para la búsqueda de vulnerabilidades en un sitio web institucional.

Figura 2

Salida de la ejecución de la herramienta Acunetix para un sitio web



https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 114 - 117

Para aprobar una revisión de seguridad se requiere que el reporte emitido (primera revisión o de seguimiento) no cuente con hallazgos ponderados como Críticos, Altos o Medios de acuerdo con las calificaciones proporcionadas por la calculadora *Common Vulnerability Scoring System (CVSS)* de FIRST en su versión 3.1 (FIRST, 2025).

Las recomendaciones de seguridad buscan la implementación de configuraciones que ayuden a proteger no sólo al código fuente, sino también al manejador de bases de datos, al sistema operativo, a los usuarios y a los privilegios asignados, así como al software empleado como servidor de aplicaciones web.

Las pruebas despliegan un conjunto de herramientas automatizadas que se deben configurar y poner en marcha sólo para el objetivo previamente establecido; la salida proporcionada debe ser verificada para descartar falsos positivos, así como para obtener la evidencia correspondiente.

3. RESULTADOS

La realización de pruebas de caja negra permite llevar a cabo una exploración de sitio web sin conocer su contexto, lo que evita tener un sesgo al conocer previamente el funcionamiento, apartados, tipos de usuarios o tecnologías empleadas en su implementación. Los resultados mostrados corresponden sólo a las pruebas realizadas para los sitios web institucionales que solicitaron el servicio. Adicionalmente, es mandatorio para aquellos que se alojan en el Centro de Datos de la DGTIC y, en todos los casos, se llevan a cabo antes de su publicación.

Si bien el servicio se ha proporcionado con anterioridad, este reporte se centra en el periodo 2024-2025 debido al aumento en su demanda. Se presentó un incremento cercano al 11% en las revisiones solicitadas por primera vez y otro de aproximadamente 14% en las revisiones de seguimiento, lo que refleja un mayor interés por parte de las áreas universitarias por solventar temas de seguridad en los sitios web antes de su publicación. De esta manera, a lo largo del periodo que abarca tanto el año 2024 como el año 2025, se obtuvieron los resultados de la Tabla 2.

Tabla 2

Comparativa del número de revisiones realizadas entre 2024 y 2025

	2024	2025 (enero - octubre)
Primera revisión	74	81
Revisión de seguimiento	41	57

Derivado de los datos proporcionados en la Tabla 2, se puede observar que se ha presentado un incremento del número de revisiones realizadas, las cuales reflejan el interés no sólo en cubrir el requisito institucional de llevar a cabo la verificación correspondiente, sino en fortalecer las implementaciones realizadas a los sitios.

Este proceso representa un beneficio real para la Universidad, ya que las correcciones y mejoras pueden ser asimiladas y, posteriormente, aplicadas por los responsables en otras aplicaciones web que pertenecen a las mismas áreas, lo que contribuye a aumentar la seguridad de la infraestructura tecnológica.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 115 - 117

Todas las aplicaciones revisadas se encontraban próximas a su publicación en entornos productivos y las cifras proporcionadas corresponden a la totalidad de solicitudes de revisión recibidas y atendidas.

Por otra parte, a pesar de que los sitios web institucionales son heterogéneos, ya que cada uno soluciona una necesidad en particular, en la Tabla 3 se pueden observar los porcentajes de las tecnologías más empleadas para su implementación:

Tabla 3

Tecnologías más empleadas en los sitios web institucionales

Lenguaje de programación	Servidor de aplicaciones	CMS empleado
PHP 80%	Apache 90%	Wordpress 70%
Java 15%	NginX 5%	OJS 15%
Otras soluciones 5%	Otras soluciones 5%	Drupal 10%
		Otras soluciones 5%

El uso de estas tecnologías se encuentra orientado a proporcionar soluciones a las necesidades de sitios web de la comunidad universitaria, por lo que se puede notar una preferencia por herramientas de distribución libre, que además cuentan con soporte, actualizaciones constantes y módulos o complementos de seguridad por parte de los desarrolladores y la comunidad que les da seguimiento.

Se ha observado que las pruebas de caja negra se pueden fortalecer con una visión integral de seguridad donde se complementen con otras tecnologías y prácticas de seguridad como el análisis estático de código fuente (SAST) y la implementación de defensa en profundidad. Asimismo, es importante el uso de un *firewall* como elemento adicional de seguridad, pues aporta información relevante para el monitoreo y análisis posterior a la revisión realizada, lo que permite dar seguimiento a los hallazgos reportados que no pudieron ser atendidos.

De esta manera, "Una función esencial de un firewall es registrar los detalles de cada intento de conexión, como quién lo realizó y cuándo. Estos datos son valiosos para la resolución de problemas, el análisis de seguridad y otras aplicaciones" (Tudosi et al., 2023, p.11). Esta información, al ser analizada, es de ayuda para fortalecer los resultados de las revisiones y mejorar de manera continua la seguridad web.

Cabe destacar que todas las solicitudes recibidas fueron atendidas. Los únicos retrasos registrados en el inicio de las pruebas corresponden a las aplicaciones que presentaron complicaciones en su despliegue, situación que, una vez solventada, permitió iniciar con el proceso de revisión sin mayores afectaciones.

Adicionalmente, las aplicaciones web que fueron revisadas, en su mayoría, cumplieron con las medidas de seguridad que ayudan no sólo a protegerlas, sino también a evitar afectaciones en los otros sitios que están coubicados en la misma infraestructura.

Finalmente, al considerar la incorporación de las pruebas de *pentest* como parte del ciclo de vida del desarrollo seguro de software (SSDLC), se obtienen elementos para entender el incremento observado en las revisiones solicitadas, ya que su adopción favorece una "mayor eficiencia del proceso de seguridad del software, mejor rendimiento en las métricas de seguridad del software y seguridad general de los productos de software" (Umeugo et al., 2023, p.2).

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 Vol. 4, Núm. 1. enero-marzo 2026, págs. 116 - 117

4. CONCLUSIONES

Las revisiones de seguridad realizadas durante el periodo 2024-2025 contribuyeron a mitigar la exposición de vulnerabilidades de los sitios web antes de su liberación y uso por parte de la comunidad universitaria, lo que se refleja en la protección de la información y la continuidad de los servicios institucionales.

El análisis del periodo permitió identificar un incremento en la realización de pruebas de seguimiento respecto a años anteriores, lo que refleja una mayor comprensión y compromiso por parte de los responsables de los sitios respecto a los hallazgos reportados y las medidas a implementar orientadas al fortalecimiento de la seguridad de sus aplicaciones web.

No obstante, los resultados obtenidos pueden optimizarse, ya que el escenario deseable sería que cada revisión inicial cuente con una revisión de seguimiento en donde se corrobore la mitigación total de los hallazgos reportados en el primer reporte, ayudando así a un cierre efectivo de las pruebas de seguridad web.

Resulta fundamental considerar a futuro la necesidad de impulsar el servicio para otras entidades y dependencias de la Universidad, con el fin de fortalecer la postura institucional que promueve la seguridad en aplicaciones web, así como promover una cultura de la seguridad que apoye acciones preventivas que beneficien tanto a los sitios web como a los usuarios.

AGRADECIMIENTOS

Por su apoyo, al Ing. Sergio Anduin Tovar Balderas, al Dr. Manuel I. Quintero Martínez y al Mtro. Juan López Morales.

REFERENCIAS

Bertoglio, D. D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society, 23*(1), 2. https://doi.org/10.1186/s13173-017-0051-1

Forum of Incident Response and Security Teams. (2025). *Common Vulnerability Scoring System Version 3.1 Calculator*. Recuperado de https://www.first.org/cvss/calculator/3-1/

Khamdamov, R. K., & Ibrokhimov, A. (2021). Techniques and methods of black box identifying vulnerabilities in web servers. En *2021 International Conference on Information Science and Communications Technologies (ICISCT)* (Vol. 00, pp. 1–4). IEEE. https://doi.org/10.1109/ICISCT52966.2021.9670263

Moreno, A. C., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Portillo-Portillo, J., Olivares-Mercado, J., & García Villalba, L. J. (2025). Analysis of Autonomous Penetration Testing Through Reinforcement Learning and Recommender Systems. *Sensors, 25*(1), 211. https://doi.org/10.3390/s25010211

Open Web Application Security Project. (s. f.). *OWASP Web Security Testing Guide*. OWASP. https://owasp.org/www-project-web-security-testing-guide/

Penetration Testing Execution Standard. (s. f.). *Penetration Testing Execution Standard (PTES)*. https://www.

https://doi.org/10.22201/dgtic.30618096e.2026.4.1.157 **Vol. 4, Núm. 1.** enero-marzo 2026, págs. 117 - 117

pentest-standard.org/index.php/Main_Page

Tudosi, A.-D., Graur, A., Balan, D. G., & Potorac, A. D. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. *Sensors*, *23*(5), 2683. https://doi.org/10.3390/s23052683

Umeugo, W., Lowrey, K., & Pandya, S. Y. (2023). Factors affecting the adoption of secure software practices in small and medium enterprises that build software in-house. *International Journal of Advanced Research in Computer Science, 14*(2), 1–8. https://doi.org/10.26483/ijarcs.v14i2.6955

Universidad Nacional Autónoma de México, Dirección General de Cómputo y de Tecnologías de Información y Comunicación. (2022). *Lineamientos de seguridad de la información en sitios web de la UNAM*. Red de responsables TIC. https://www.red-tic.unam.mx/recursos/2022/2022_Lineamientos_DGTIC_02.pdf