Revisión de vulnerabilidades en sitios web de Instituciones de Educación Superior en Colombia: Identificación y recomendaciones para prevención y mitigación de ataques

Review of vulnerabilities in websites of Higher Education Institutions in Colombia: Identification and recommendations for prevention and attacks mitigation

Santiago Alzate Romero[1]
santiago.alzate00@usc.edu.co

Manuel Alejandro Paredes[1]
manuel.paredes00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (1)

Resumen

Por su amplia extensión y diversidad que posee, la ciberseguridad se ha convertido en un concepto bastante complejo de controlar, ya sea por las diferentes técnicas de hackeo o alguna vulnerabilidad encontrada en el sistema. Este artículo tiene como objetivo presentar las vulnerabilidades más comunes que puedan ocurrir junto con las herramientas de monitoreo más comunes para las páginas web. Se investigaron aleatoriamente Instituciones de educación superior que cuenten con un sistema de Información para interactuar con los estudiantes por motivos académicos y/o administrativos a las cuales se estudió acerca de sus herramientas empleadas en el desarrollo de sus plataformas, para así poder presentar las vulnerabilidades a las que se puedan encontrar por su estructura interna. Los resultados indicaron que la mayoría de los sitios web están elaborados bajo el lenguaje de programación PHP junto con la herramienta DRUPAL, las cuales demostraron potenciales vulnerabilidades que los ciber atacantes puedan utilizar para tener acceso al sistema que, en muchos casos, no se cuenta con un plan de prevención o reacción frente a estas situaciones. Por tal motivo, se concluye que se necesita reforzar en el concepto de ciberseguridad tanto en buenas prácticas o estándares como en capacitación para todos los puestos de la organización, incluyendo también al usuario final, que en este caso sería el estudiante

Palabras Clave: Ciberseguridad, institución de educación superior, vulnerabilidades de software, ataque cibernético, desarrollo web, lenguajes de programación, buenas prácticas, PHP, malware

Abstract

Given its wide extension and diversity, cybersecurity has become a rather complex concept to control in its entirety, either because of the different hacking techniques or some vulnerability found within the system. This article aims to present the most common vulnerabilities that may occur along with the most common monitoring tools for web pages. We randomly investigated higher education institutions that have an information system to interact with students for academic and/or administrative purposes and studied their tools used in the development of their platforms, in order to present the vulnerabilities that can be found in their internal structure. The results indicated that most of the websites are developed under the PHP programming language together with the DRUPAL tool, which showed potential vulnerabilities that cyber attackers can use to gain access to the system and that, in many cases, there is no prevention or reaction plan for these situations. For this reason, it is concluded that it is necessary to reinforce the concept of cybersecurity both in good practices or standards and in training for all positions in the organization, including the end user, which in this case would be the student.

Keywords: cybersecurity, higher education, vulnerabilities software, cyber-attack, web development, programming languages, good practices, PHP, malware

I. INTRODUCCIÓN

El avance tecnológico ha transformado radicalmente la forma en que vivimos, interactuamos y realizamos diversas actividades cotidianas. Desde la comunicación instantánea con personas en cualquier parte del mundo hasta la posibilidad de acceder a vastas cantidades de información en dispositivos móviles, la tecnología ha permeado casi todos los aspectos de la sociedad. Uno de los impactos más significativos de la tecnología se ha dado en el ámbito de la comunicación. La internet ha revolucionado la forma en que nos conectamos con los demás, permitiendo la comunicación instantánea a través de plataformas como redes sociales, mensajería instantánea y videollamadas. Esto ha facilitado la colaboración, el intercambio de ideas y la construcción de relaciones a nivel global.

En el ámbito del desarrollo web, la tecnología ha dado lugar a nuevas herramientas y librerías que optimizan el trabajo de los programadores. Estas herramientas permiten crear páginas web más estructuradas, estéticas y eficientes, utilizando menos recursos y generando mejores resultados. Según un estudio de (Plaw et al., n.d.), el uso de internet se ha convertido en la principal actividad social en Latinoamérica. Esto refleja la profunda integración de la tecnología en la vida cotidiana de las personas y su papel fundamental en la sociedad actual.

En la era digital, donde la información es un tesoro y las transacciones se realizan en línea, la ciberseguridad se ha vuelto una necesidad imperiosa. Este concepto, que surge de la intersección entre internet y la programación, busca proteger a las aplicaciones y plataformas web que manejan información sensible de los usuarios, estableciendo protocolos preventivos tanto físicos como virtuales contra ataques cibernéticos.

Los ciberdelincuentes, expertos en explotar vulnerabilidades, emplean diversos métodos para obtener información personal, desde malware hasta phishing y ransomware. Afortunadamente, la ciberseguridad, entendida como un estado logrado mediante la aplicación de medidas organizativas, normativas, técnicas, educativas, políticas y diplomáticas, está cobrando cada vez más fuerza. Su objetivo primordial es garantizar la protección y el uso legítimo del ciberespacio, un espacio cada vez más vital en nuestras vidas.

En el desafío de la ciberseguridad, es casi imposible afirmar que un sistema pueda contar con una seguridad total ante cualquier ciberataque o vulnerabilidad, interna y externa, y es una situación que ha perdurado con los años en distintas organizaciones de cualquier ámbito, incluso las Instituciones de Educación Superior (IES) son un objetivo potencial para estos criminales. En el Reino Unido se hizo una encuesta generada por el gobierno indicando que semanalmente, un 62% de IES fueron vulneradas o sufrieron algún tipo de violación a la seguridad (Prümmer et al., 2024).

Lo que parece destacar es que la mayoría de los ciberataques generados se deben a vulnerabilidades relacionadas con el factor humano dentro de las organizaciones, más específicamente hablando a temas de phishing, el cual es una manera de ciber ataque que ha sido tendencia desde los años 90, en el que el ciber atacante obtiene información sensible y/o financiera del usuario mediante una suplantación de identidad, aparentando ser alguien distinto o una organización reconocida solicitando un cambio de información mediante un enlace a una página web que parece verídica, pero resulta ser una imitación maliciosa y controlada por éste, (Chaudhry et al., 2016). Por lo general se utilizan las plataformas de correo electrónico, a través de mensajes de texto (SMS) o chat personal (P.E WhatsApp) incluso por medio de llamadas telefónicas y cada vez tiende a ser más elaborado el método de suplantación de identidad y la gente está menos preparada, lo cual facilita en gran manera el hurto a la información del usuario

Todos estos daños y filtración de información personal o sensible de los usuarios dentro de las organizaciones generan fuertes consecuencias internas en varios aspectos, tanto pérdidas económicas, en términos de productividad, pero lo más importante de todo, termina afectando uno de los tres pilares fundamentales de la seguridad de la información: Confidencialidad, previene el acceso no autorizado a la información (Burgos Salazar & Campos, n.d.), lo que ocasiona una pérdida masiva de confianza y credibilidad de la organización

Es de esperarse que la educación se modernice y use distintas tecnologías, por eso es crucial que los organismos de educación superior den prioridad a la ciberseguridad. Además, en un estudio realizado por (Ulven & Wangen, 2021), se demostró que la investigación empírica sobre los riesgos de ciberseguridad en la educación superior es escasa, y hay grandes lagunas en la literatura. Esto es especialmente importante con el incrementado número de ciber atacantes que buscan robar información valiosa. Por lo tanto, es vital reforzar las medidas de seguridad en estos lugares.

En este contexto, se investigaron las herramientas y enfoques recomendados para evaluar y fortalecer la ciberseguridad

en instituciones de educación superior que muestren una tendencia hacia cierto lenguaje de programación. Desde auditorías de seguridad y pruebas de penetración hasta la implementación de buenas prácticas de codificación segura. Adicionalmente, se examinaron las mejores estrategias para mitigar riesgos y garantizar un entorno digital seguro en el ámbito educativo.

Existen herramientas para identificar y analizar vulnerabilidades en las aplicaciones web. Estas herramientas escanean la aplicación web en busca de inseguridades conocidas y proporcionan informes detallados sobre los resultados encontrados. Estas son algunas de las tecnologías más populares que cuentan con una versión gratuita:

- Nessus: Se utiliza para escanear redes y sistemas en busca de vulnerabilidades conocidas.
- OpenVAS: Se utiliza para escanear redes y sistemas en busca de vulnerabilidades conocidas.
- Nikto: Se utiliza para escanear servidores web en busca de vulnerabilidades conocidas.
- RecurScan: Se utiliza para escanear y se enfoca en vulnerabilidades basadas en inyección está en prototipo por ahora.

(Devi & Kumar, 2020; Ravindran & Potukuchi, 2022; Shi et al., 2024)

Adicional a eso, también se encuentran las herramientas para pruebas de penetración, las cuales simulan ataques cibernéticos y evaluar la capacidad en las aplicaciones web para resistir ataques cibernéticos. Estas son algunas de las tecnologías más populares que cuentan con una versión gratuita:

- **Metasploit**: Se utiliza para simular ataques cibernéticos en las aplicaciones web
- **Burp Suite**: Simular ataques cibernéticos en las aplicaciones web.
- **OWASP ZAP**: Se utiliza para simular ataques cibernéticos en las aplicaciones web.

(Amankwah et al., 2020; Ravindran & Potukuchi, 2022)

Una de las contribuciones más destacadas de OWASP es el proyecto Top 10 (Jorge, n.d.), que identifica y documenta las diez vulnerabilidades de seguridad más críticas que afectan a las aplicaciones web. El objetivo principal de este proyecto consiste en actualizarse periódicamente para reflejar las nuevas amenazas y tendencias en el panorama de la ciberseguridad. Esta herramienta está basada en los principios de transparencia, colaboración y compartición de conocimientos. La organización promueve la concientización sobre la importancia de la seguridad desde las etapas iniciales del ciclo de vida del desarrollo de software, fomentando la integración de prácticas de seguridad en todos los aspectos del proceso de desarrollo.

Finalmente, se exponen las herramientas de monitoreo, destinadas a monitorear la seguridad de las aplicaciones web, y así detectar y alertar sobre posibles ataques cibernéticos para una reacción oportuna. Estas son algunas de las tecnologías para monitoreo más populares que cuentan con una versión gratuita:

- **Snort**: Se utiliza para detectar y alertar sobre posibles ataques cibernéticos. Snort es una herramienta de código abierto y es gratuita.
- **OSSEC**: Se utiliza para detectar y alertar sobre posibles ataques cibernéticos

(Liu et al., 2019)

Sin embargo, También es necesario mencionar los escenarios en los que las políticas de ciberseguridad adoptadas por las instituciones que tuvieron un resultado positivo ante los potenciales ciberataques.

Aunque el enfoque no va orientado principalmente hacia la Inteligencia Artificial (IA), una posible solución a la problemática sería el concepto de XAI, o Inteligencia Artificial Explicable, que en la actualidad se ha convertido en un punto crucial en la defensa contra ciberataques, abordando áreas clave como la detección de programa maligno, el filtrado de spam, la identificación de botnets, la prevención de fraudes, la detección de phishing y la intrusión en redes. Al utilizar

técnicas como SHAP y LIME, los sistemas de defensa basados en IA pueden ofrecer transparencia y explicabilidad, lo que aumenta la confianza y la comprensión de sus decisiones (Deng et al., 2019)

II. METODOLOGÍA

Para la investigación se recolectó la información acerca de las páginas web institucionales de catorce (14) IES nacionales que cumplieran con las siguientes condiciones: (1) que cuente con un Sistema de Información el cual el estudiante interactúe frecuentemente, (2) que maneje información sensible del mismo, (3) que el enfoque de la plataforma sea más administrativo que académico. Por motivos de alcance del proyecto y tiempo estimado, se considera que la muestra recolectada cumple con los requisitos mínimos para el estudio de ésta.

Luego de la selección de las páginas web, a cada plataforma se le realizó un análisis de su estructura técnica y las tecnologías utilizadas para su elaboración a través de la herramienta Wappalyzer, en su formato de extensión para navegador, el cual es una herramienta *open source* (código abierto, que cualquiera tiene acceso a este) que permite al usuario conocer algunas tecnologías utilizadas en la página web de las universidades elegidas

Dicha revisión se enfocó en dar a conocer las potenciales vulnerabilidades que estén en dichas tecnologías. Por motivos de alcance de la investigación y elementos en común, se optó por trabajar con el lenguaje de programación para el desarrollo y el gestor de contenido, dado que la herramienta generaba más contenido para algunos sitios web que para otros

Se examinaron los mejores métodos para comprobar y mejorar la seguridad en línea, con tal de proteger los sistemas digitales de las Instituciones de Educación Superior y así, mantenerlas fiables, seguras y con gran credibilidad respecto a la información personal y académica de los estudiantes y procesos administrativos.

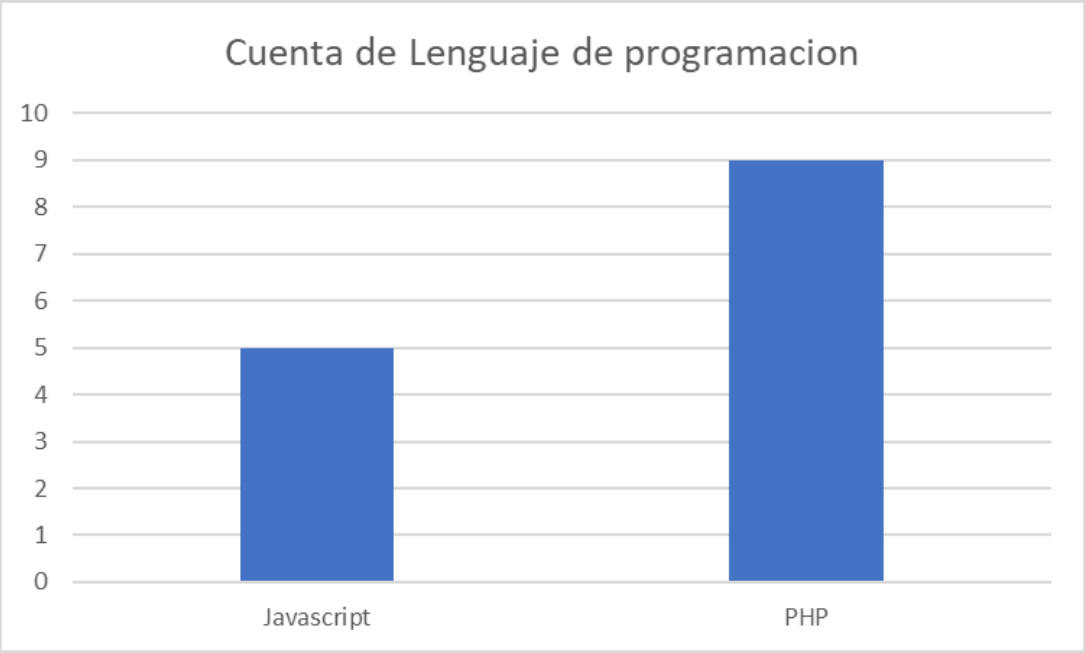
Toda la información obtenida se almacenó y ordenó en una tabla de Excel donde el análisis estadístico se representó mediante la generación de diversos gráficos y visualizaciones. Estas representaciones gráficas de los resultados permitieron un examen más exhaustivo y detallado de la información obtenida durante el estudio, identificando tendencias, patrones y hallazgos clave relacionados con el estado de las IES en cuanto a ciberseguridad.

Ante la limitada disponibilidad de literatura en español pertinente al estudio, la búsqueda de referencias bibliográficas se extendió al idioma inglés, utilizando para ello diversas bases de datos, tanto institucionales como públicas. Esta estrategia posibilitó la obtención de información más completa y reciente sobre la temática abordada, enriqueciendo el análisis y la discusión de los resultados.

III. RESULTADOS

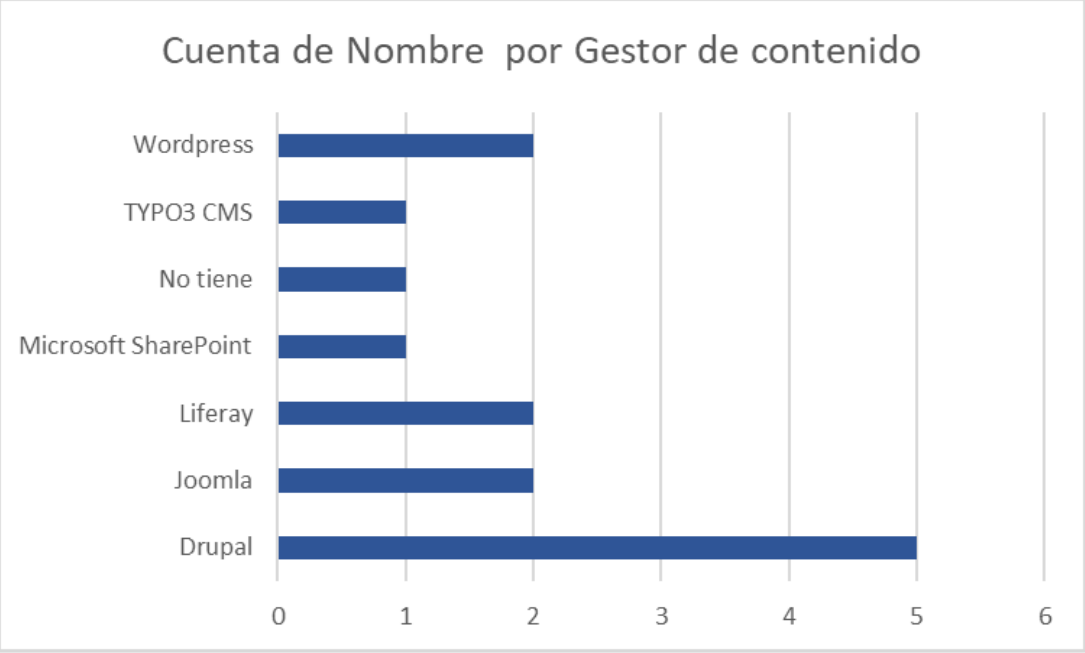
Esta sección abarca los resultados de la investigación realizada, mostrados de forma gráfica. Se abarcaron los puntos de fortalezas y debilidades, abordando de menor a mayor detalle los hallazgos obtenidos. Este análisis contribuyó a entender los desafíos y riesgos inherentes al uso de ciertas tecnologías y plataformas en el ámbito de la seguridad informática. La información recolectada se organizó en las siguientes gráficas (Figura 1, Figura 2)

Figura 1. Lenguajes de programación usados



Fuente: Autoría propia

Figura 2. Gestores de contenido



Fuente: Autoría propia

De las instituciones investigadas se encontró que nueve (9) de ellas presentan una familiaridad o tendencia más elevada hacia PHP como lenguaje principal para el desarrollo de aplicaciones web. Sin embargo, este lenguaje plantea desafíos específicos en cuanto a seguridad. (Yenduri & Al-khassaweneh, 2022) A razón de este descubrimiento, predomina la necesidad crítica de abordar unas consideraciones de seguridad específicas, y de implementar estrategias robustas para proteger la integridad y confidencialidad de los datos en estos establecimientos.

Esta sección se ha abordado los resultados obtenidos de la investigación, ofreciendo un análisis detallado de los hallazgos relacionados con la preferencia hacia PHP, dado que su facilidad de integración con bases de datos relacionales, lo ha

convertido en una opción distinguida para la creación de sitios web dinámicos y aplicaciones web. Sin embargo, la creciente competencia de otros lenguajes de programación y *frameworks*, que ofrecen funcionalidades y enfoques más modernos y estrictos, ha desafiado la posición dominante de PHP. A pesar de eso, la gran comunidad de desarrolladores que utilizan este lenguaje, así como la amplia documentación y librerías, garantizan su relevancia en el mercado laboral y su continuidad en el desarrollo de proyectos web, (Islam et al., 2024).

Además, otro de los motivos por el cual las IES optaron por PHP como su lenguaje de programación, es que presenta un comportamiento bastante estable frente a pequeñas peticiones con relación al tiempo requerido, (X. Liu et al., n.d.), por eso es una buena opción para proyectos de pequeña y mediana escala, tales como las respectivas páginas web trabajadas

Por otro lado, se demostró que el gestor de contenido Drupal fue el más utilizado por el equipo al desarrollar las plataformas, que suele trabajar con el lenguaje analizado anteriormente por su ayuda en la mitigación de riesgos, del que se encontraron y estudiaron debilidades. Por motivos de investigación, los demás gestores de contenidos fueron descartados

FORTALEZAS DE USAR DRUPAL:

- Flexibilidad y Personalización: La arquitectura modular de Drupal permite una amplia personalización, adecuada para una variedad de tipos de sitios web, desde blogs simples hasta portales complejos.
- Escalabilidad: Drupal es altamente escalable y puede manejar grandes cantidades de tráfico y contenido, siendo utilizado por sitios web de alto tráfico como portales gubernamentales y grandes empresas.
- Seguridad: Conocido por sus robustas características de seguridad, Drupal es una opción preferida para sitios que requieren medidas de seguridad estrictas. Cuenta con un equipo de seguridad dedicado y un proceso riguroso para abordar vulnerabilidades.
- Soporte de la Comunidad: Drupal tiene una gran y activa comunidad que contribuye con una gran cantidad de módulos, temas y documentación. Este apoyo comunitario puede ser invaluable para solucionar problemas y encontrar soluciones.
- Capacidades Multilingües: Drupal ofrece un fuerte soporte multilingüe desde el principio, lo que lo hace ideal para sitios web que necesitan operar en múltiples idiomas.

DEBILIDADES DE USAR DRUPAL:

- Curva de Aprendizaje Pronunciada: Drupal tiene una curva de aprendizaje más pronunciada en comparación con otras plataformas CMS como WordPress. Requiere un buen entendimiento de su arquitectura y puede necesitar la contratación de desarrolladores experimentados para proyectos complejos.
- Complejidad en la Configuración y Mantenimiento: Configurar y mantener un sitio Drupal puede ser más complejo y llevar más tiempo, especialmente para aquellos sin experiencia técnica. Las actualizaciones regulares y la gestión de módulos también pueden ser desafiantes.
- Sobrecargas de Rendimiento: Aunque Drupal es escalable, a veces puede sufrir problemas de rendimiento si no se optimiza adecuadamente. Puede ser necesario realizar ajustes de rendimiento y mecanismos de almacenamiento en caché adicionales para un rendimiento óptimo.
- Menos Temas y Plugins: En comparación con WordPress, Drupal tiene menos temas y plugins listos para usar, lo que puede requerir más desarrollo personalizado para lograr la funcionalidad y apariencia deseada.
- Consumo de Recursos: Ejecutar un sitio en Drupal puede ser intensivo en recursos, requiriendo soluciones de hosting más potentes para asegurar un rendimiento fluido, particularmente para sitios más grandes con tráfico y contenido significativos.

(Khalil et al., 2024)

VULNERABILIDADES DE PHP:

- **Inyección de código SQL**: Permite a los ciber atacantes ejecutar comandos maliciosos en la base de datos con la cual la plataforma web trabaja, se han presentado casos en los que los delincuentes obtienen control total vía remota del servidor, permitiéndoles realizar acciones indebidas como modificar o eliminar datos, instalar software malicioso o incluso interrumpir el funcionamiento del sistema.
- **Cross-Site Scripting (XSS)**: Le da la facilidad a los ciber atacantes de ejecutar scripts maliciosos en el propio navegador del usuario lo que podría permitir el robo de cookies, redirección a sitios web malignos y/o control del navegador.
- **Cross-Site Request Forgery (CSRF)**: Permite a los ciber atacantes realizar acciones maliciosas en nombre del usuario sin su conocimiento. Para solucionar esta vulnerabilidad, se deben utilizar tokens CSRF y validar todas las solicitudes entrantes.
- **Vulnerabilidades de autenticación y autorización**: Permiten acceder a recursos protegidos sin la debida autorización. Para solucionar estas vulnerabilidades, se deben implementar mecanismos de autenticación y autorización adecuados.
- **Vulnerabilidades de manejo de archivos**: Permiten a los atacantes cibernéticos cargar archivos maliciosos en el servidor web. Para solucionar estas vulnerabilidades, se deben validar y filtrar todas las entradas de usuario.

(Kareem et al., 2021; Liu et al., 2019; Ravindran & Potukuchi, 2022; Ulven & Wangen, 2021; Yerram et al., 2014)

Una vulnerabilidad que más llamó la atención es que presenta una apertura de seguridad al momento de hacer peticiones GET o POST, donde un usuario inocentemente accede a un enlace falsificado mientras que el atacante sencillamente tiende a modificar las cookies del sitio web para acceder a la información de acceso del usuario, (Backes et al., 2017). Sin embargo, este factor se ha podido evidenciar en otras plataformas desarrolladas en distintos lenguajes de programación, y resulta ser una problemática más enfocada hacia el navegador de preferencia y al fácil acceso que se le da a un usuario con mínimo manejo de la herramienta a las cookies de la página web

ANÁLISIS DE LAS VULNERABILIDADES:

De acuerdo con (Yerram et al., 2014), una solución que se le puede dar en el caso de la Inyección de código SQL es que se deben utilizar consultas preparadas, evitar la concatenación de cadenas de consulta. Además de eso, limitar el ingreso de caracteres especiales dentro del campo del formulario podría favorecer a la protección del sistema. Ahora, en el caso de XSS, es indispensable que se validen y cierren todas las entradas de usuario en el sistema posterior a su uso

En un estudio de (Oyemade et al., 2015) encontró que, de 170 profesionales en TI de distintas organizaciones e instituciones en Nigeria, 75 encuestados afirmaron que las vulnerabilidades más comunes que pueden surgir en el desarrollo con PHP son la inyección de código SQL y la revelación de código fuente. Lo que genera sus respectivas consecuencias para la aplicación web. Una de ellas es el hackeo de la base de datos y la otra es que el sitio web resulte infectado por código o scripts maliciosos por el lado del cliente (frontEnd)

En la investigación realizada por (Smith & Dissertation, 2023), se encontró que muchos de los ciberataques ejecutados en la mayoría IES son ocurridos durante los primeros semestres académicos, y esto se debe a que los estudiantes no cuentan con una capacitación apropiada desde el inicio de su ciclo para el buen uso de las plataformas, pero también es debido al cambio de metodología utilizada en los colegios, donde en algunos casos no se utiliza algún sistema de Información o gestión sino que todo termina siendo aterrizado a lo manual y presencial. Esto representa una alta problemática dado que, con un mal uso del programa, puede ser una potencial vulnerabilidad explotable por parte de los ciberatacantes

Un estudio realizado por (Ulven & Wangen, 2021) recopiló los resultados acerca de las vulnerabilidades más comunes que pueden ocurrir en las IES, sus respectivas descripciones y la probabilidad de ocurrencia, donde cerca de 3000 casos investigados sirvieron para realizar la información de la siguiente tabla (tabla 1)

Amenaza o incidente	Descripción	Probabilidad
Intrusión, malware y compromiso	Entrada electrónica por parte de un tercero; pérdida de datos a través de malware, spyware y hacking.	29%
Activos vulnerables y exploración	Propiedad de la organización que es vulnerable a ataques externos e internos, o adversarios que buscan vulnerabilidades.	28.6%
Ingeniería social y ataques selectivos	Los fraudes se intentan principalmente a través de estafas de phishing, ataques dirigidos e intentos de intrusión en la organización.	10.9%
Divulgación involuntaria y errores	Información sensible publicada en un sitio web, mal manejada o enviada a la parte equivocada por correo electrónico, fax o correo postal.	10.4%
Pérdida o robo de dispositivos o documentos	Dispositivos perdidos, desechados o robados (por ejemplo, portátil, PDA, PC, smartphone, dispositivo de memoria portátil, CD, disco duro). o registros no electrónicos robados, como documentos en papel.	6.2%
Secuestro de cuenta/usuario comprometido	Un usuario comprometido es cuando el nombre de usuario y la contraseña de una cuenta se ven comprometidos.	5.5%
Abuso y uso indebido	Infracciones de la ley o de la política por abuso y mal uso de la infraestructura por infracción de derechos de autor, alojamiento ilegal, minería de criptomonedas, etc.	4.8%
Ataques internos	Violación intencionada de la información por parte de alguien con acceso legítimo.	3.9%
DoS/DDoS	La denegación de servicio (DoS) se produce cuando un servicio o activo deja de estar disponible.	0.6%
Desconocidos u otros	Infracciones que no encajan en las otras categorías o cuya causa principal no se ha determinado.	0.2%

Tabla 1, vulnerabilidades más comunes. Autoría (Ulven & Wangen, 2021)

En el ámbito legal se realizó un estudio para implementar un modelo dinámico de ciberseguridad basado en los estándares ISO en unas IES de Colombia, (Varona Taborda, 2021).Click or tap here to enter text. Dicho estudio agrupó distintos estándares (ISO / IEC: 20000-1, ISO / IEC 27001, ISO / IEC 27002, ISO / IEC 29119: 2013, ISO 19770-1), donde cada uno abarcaba un factor importante, que van desde la gestión eficiente de servicios hasta el establecimiento de un marco versátil y de fácil aplicación dentro del software para las técnicas de gestión de activos de TI. Todo este contenido dio como resultado un modelo demasiado robusto, de fácil implementación en cualquier organización y, si es implementado correcta y rigurosamente, se estaría hablando de un producto muy estable en cuestión de ciberseguridad

Como se menciona en (Senarak, 2021), que siempre habrá una relación muy estrecha entre los factores humano, infraestructura y procedimiento en lo que respecta a una ciberseguridad "saludable". Lo que significa es que todos los eslabones deben estar alineados porque de lo contrario, si un solo elemento no funciona correctamente o presenta debilidades, toda la cadena se verá afectada. Afirma también que la falta de conocimientos y competencias que van desde los altos ejecutivos hasta los empleados para aplicar las medidas de ciberseguridad podría ocasionar el fracaso en el desarrollo de una limpieza de puertos de ciberseguridad satisfactoria. Es importante que todo el personal, sin importar el cargo o la posición, se encuentre bien capacitado y se concientice de la importancia del problema, para aplicar medidas eficaces de ciberseguridad y constancia en ellas en todos los niveles de la organización.

También se encontró un proyecto que vincula la Inteligencia Artificial con las vulnerabilidades potenciales que tenga

PHP, VulEye representa un avance significativo en el campo de la seguridad informática, especialmente en lo que respecta a la detección de vulnerabilidades en el código en PHP, (Lin et al., 2023). Los resultados de este estudio evaluaron su rendimiento en comparación con otras herramientas y modelos existentes, posicionándola como una alternativa bastante favorable. Algo que caracteriza esta herramienta es la capacidad de VulEye para detectar una amplia variedad de vulnerabilidades con una precisión excepcional y su capacidad de generalización.

Un software nunca se podrá encontrar seguro en su totalidad, ya que se implementen buenas prácticas en el desarrollo, como un tipado fuerte de las variables, realizar un mantenimiento frecuente del producto, evitar caracteres especiales en los campos de los formularios, utilizar un proceso de autenticación de 2 pasos, ya sea por confirmación o con una clave única (OTP), o, mantener un control robusto de las cookies utilizadas en el navegador, (Yang, 2023), ahí solo se abarcaría a una parte del problema. Se tiene que establecer una capacitación sobre el uso seguro y constante de la plataforma con los usuarios finales, (Seguridad+en+desarrollo+web+mejores+prácticas+para+proteger+aplicaciones+y+datos, n.d.), aquellos usuarios que utilizarán constantemente el producto, y establecer unos estándares de seguridad rigurosos que deben ser empleados, tales como el uso de y cambio cada cierto peridodo de contraseñas robustas que contengan caracteres especiales y que no sean de fácil acceso, realizar una limpieza de cookies regularmente, entre otros. Solo así se podría hablar de una plataforma relativamente segura de forma momentánea.

IV. CONCLUSIÓN

Pese a la diversidad que cuentan los lenguajes de programación en la actualidad, y sin importar qué tan modernos puedan llegar a ser y las tecnologías y librerías que tengan para mejorar el rendimiento de desarrollo, la preferencia por parte de las instituciones investigadas hacia PHP resulta ser causante de atención, ya sea por la experiencia y práctica que los desarrolladores tengan o por la robustez y la estabilidad que maneje, se opta trabajar con este lenguaje y sus respectivas tecnologías.

Se debe aclarar que, referente al contenido y la información investigada sobre las IES nacionales, no se encontró alguna documentación relevante sobre el tema, aparte de lo obtenido por mérito propio, lo que da a entender que, aunque las instituciones puedan sufrir algún ciberataque, no muestran una actitud preventiva para contrarrestar dichas amenazas. Esto puede surgir por distintas razones, una, no cuentan con una capacitación adecuada referente al tema o, dos, el equipo de desarrollo encargado encuentra el sitio web en cuestión relativamente estable que no ve necesario realizar su respectivo mantenimiento referente a las vulnerabilidades

Dados los cambios en tecnologías y/o requerimientos por implementar en las páginas web, es recomendable generar espacios de capacitación enfocados a la ciberseguridad que abarque todos los puestos jerárquicos de la compañía, desde los directivos conscientes de las potenciales ciber amenazas en las que se puedan ver involucrados; como el equipo de desarrollo tomando una posición proactiva para prevenir alguna vulnerabilidad de los atacantes para cumplir con su objetivo; y, finalmente, el usuario final, dándole recomendaciones de cómo mantener su acceso relativamente seguro.

Finalmente y, como se ha mencionado anteriormente, la integridad de un sistema nunca se encontrará intacta por completo ni por mucho tiempo, sin embargo, siempre se le puede dificultar el acceso indeseado de los atacantes haciendo un riguroso monitoreo y mantenimiento de manera frecuente que, con el tiempo, se irán implementando constantemente algunas de las buenas prácticas preventivas mencionadas anteriormente, organizándolas y adecuándolas de tal forma para, de esta forma, llegar a generar un sistema estandarizado de ciberseguridad a nivel empresarial, lo que permitirá a la institución definir una metodología de acción y control en el momento de que se generen los posibles ciber ataques.

V. REFERENCIAS

Amankwah, R., Chen, J., Kudjo, P. K., & Towey, D. (2020). An empirical comparison of commercial and open-source web vulnerability scanners. *Software - Practice and Experience*, *50*(9), 1842–1857. https://doi.org/10.1002/spe.2870

Backes, M., Rieck, K., Skoruppa, M., Stock, B., & Yamaguchi, F. (2017). Efficient and Flexible Discovery of PHP Application Vulnerabilities. *Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017*, 334–349. https://doi.org/10.1109/EuroSP.2017.14

Burgos Salazar, J., & Campos, P. G. (n.d.). Modelo Para Seguridad de la Información en TIC. https://ceur-ws.org/Vol-488/paper13.pdf

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247–256. https://doi.org/10.14257/ijsia.2016.10.1.23

Deng, T., Kanthawala, S., Meng, J., Peng, W., Kononova, A., Hao, Q., Zhang, Q., & David, P. (2019). Measuring smartphone usage and task switching with log tracking and self-reports. *Mobile Media and Communication*, *7*(1), 3–23. https://doi.org/10.1177/2050157918761491

Devi, R. S., & Kumar, M. M. (2020). Testing for Security Weakness of Web Applications using Ethical Hacking. *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, 354–361. https://doi.org/10.1109/ICOEI48184.2020.9143018

Islam, M. T., Islam, M. R., Jhilik, R. A., Islam, M. A., Raihan, P. M. S., Faruque, M. S., & Shahjahan, A. M. (2024). A Comparative Analysis of Programming Language Preferences Among Computer Science and Non-Computer Science Students. *European Journal of Theoretical and Applied Sciences*, *2*(3), 900–912. https://doi.org/10.59324/ejtas.2024.2(3).70

Jorge, R. (n.d.). *VULNERABILIDADES DE APLICACIONES WEB SEGÚN OWASP*. http://polux.unipiloto.edu.co:8080/00004801.pdf

Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., Ibrahim, I. M., Ahmed, A. M., Rashid, Z. N., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. *Asian Journal of Research in Computer Science*, 13–32. https://doi.org/10.9734/ajrcos/2021/v10i330242

Khalil, M. M., Ghazi, H. M., Habib, M. I., Shahzad, F., Elahi, A. I., Saher, N., & Qadri, S. (2024). *Guideline for Selecting the Right Content Management System (RCMS) for Web Development: A Comprehensive Approach*.

Lin, C., Xu, Y., Fang, Y., & Liu, Z. (2023). VulEye: A Novel Graph Neural Network Vulnerability Detection Approach for PHP Application. *Applied Sciences (Switzerland)*, *13*(2). https://doi.org/10.3390/app13020825

Liu, M., Zhang, B., Chen, W., & Zhang, X. (2019). A Survey of Exploitation and Detection Methods of XSS Vulnerabilities. *IEEE Access*, *7*, 182004–182016. https://doi.org/10.1109/ACCESS.2019.2960449

Liu, X., IEEE Computer Society, IEEE International Conference on Ubiquitous Computing and Communications (13th : 2014 : Chengdu, C., International Symposium on Pervasive Systems, A., & International Conference on Frontier of Computer Science and Technology (8th : 2014 : Chengdu, C. (n.d.). *CSE 2014 : the 17th IEEE International Conference on Computational Science and Engineering : jointly with the 13th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2014), the 13th International Symposium on Pervasive Systems, Algorithms, and Networks (I-SPAN 2014), the 8th International Conference on Frontier of Computer Science and Technology (FCST 2014) : proceedings: 19-21 December 2014, Chengdu, China*.

Oyemade, O., Odiagbe, J. O., & Buhari, B. A. (2015). A Survey of Security Vulnerabilities in PHP Applications among IT Professionals in Nigeria. In *African Journal of Computing & ICT African Journal of Computing & ICT Reference Format* (Vol. 8, Issue 3). https://www.researchgate.net/publication/307702595_A_Survey_of_Security_Vulnerabilities_in_PHP_Applications_among_IT_Professionals_in_Nigeria

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Ramadevi, Y., and Mahmood, A. "PHP: Vulnerabilities and Solutions," (2022) 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 2022, pp. 391-396, doi: https://doi.org/10.1109/MIUCC55081.2022.9781790 .

Ravindran, U., & Potukuchi, R. V. (2022). A Review on Web Application Vulnerability Assessment and Penetration Testing. *Review of Computer Engineering Studies*, *9*(1), 1–22. https://doi.org/10.18280/rces.090101

Seguridad+en+desarrollo+web+mejores+prácticas+para+proteger+aplicaciones+y+datos. (n.d.). https://doi.org/10.23857/dc.v9i3.3552

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Shi, Y., Zhang, Y., Bai, T., Zhang, L., Tan, X., & Yang, M. (2024). *RecurScan: Detecting Recurring Vulnerabilities in PHP Web Applications*. 1746–1755. https://doi.org/10.1145/3589334.3645530

Smith, S., & Dissertation, A. (2023). *INVESTIGATING FACTORS THAT INCREASE VULNERABILITY TO CYBER-ATTACKS DURING THE FIRST YEAR COLLEGE TRANSITION*. https://www.proquest.com/docview/2866350662

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. In *Future Internet* (Vol. 13, Issue 2, pp. 1–40). MDPI AG. https://doi.org/10.3390/fi13020039

Varona Taborda, M. A. (2021). Dynamic Cybersecurity Model based on ISO standards for Higher Education Institutions in Colombia. *Ingeniería Solidaria*, *17*(3), 1–21. https://doi.org/10.16925/2357-6014.2021.03.05

Yerram, V., Venkat, G., & Reddy, R. (2014). *A SOLUTION TO PHP CODE INJECTION ATTACKS AND WEB VULNERABILITIES*. https://doi.org/10.9734/ajrcos/2021/v10i330242