Plan Estratégico

Centro de enseñanza técnica industrial CETI Colomos

Ingeniería en Desarrollo de Software

Desarrollo de Software Seguro

Maestra: Guadalupe Ortega Tirado

Equipo

Nombre: Rogelio Reynaga Salazar	Registro: 20310015
Nombre: Jorge Ibarra Peña	Registro: 20310025
Nombre: Angel Gabriel Munguia	Registro: 20310041
Nombre: Rubén Valdivia Pérez	Registro: 20310014
Nombre: Iván Alexander Luce	Registro: 20310017

04 Octubre, 2023

ceti

CENTRO DE ENSEÑANZA TÉCNICA INDUSTRIAL

1. Análisis de Riesgos

Vulnerabilidad	Probabilidad	Impacto	Acción Preventiva	Color
Cross-Site Scripting (XSS)	4/10	Robo de sesiones de usuario Robo de datos sensibles Distribución de malware Manipulación del contenido del sitio	Validación de entrada de usuario Uso de encabezados de seguridad del navegador Escapar datos de salida	AMARILLO
Falta de validación del lado del servidor	2/10	Manipulación del contenido del sitio. Ejecución de código malicioso en el servidor.	Implementar una sólida validación en el lado del servidor para todas las entradas de usuario. Aplicar buenas prácticas de desarrollo seguro, como la utilización de parámetros preparados en consultas de bases de datos para evitar inyección de SQL.	VERDE
Cross-Site Request Forgery (CSRF)	6/10	Realizar acciones no autorizadas en nombre de un usuario autenticado. Cambiar la configuración del perfil del usuario. Realizar transacciones	Implementar tokens de solicitud (CSRF tokens) en formularios y solicitudes importantes. Limitar las acciones críticas a través de solicitudes	AMARILLO

Cross-Site Request Forgery (CSRF)	6/10	financieras no deseadas. Modificar datos del usuario.	POST en lugar de GET. Educar al personal sobre las mejores prácticas de seguridad y realizar auditorías de seguridad de manera regular.	
Falta de Captcha	10/10	Envío masivo de spam a través de formularios. Creación automatizada de cuentas de usuario falsas. Ataques de fuerza bruta en contraseñas.	Implementar Captcha o soluciones equivalentes en formularios y áreas críticas para verificar la humanidad del usuario. Actualizar y mejorar las soluciones de Captcha a medida que evolucionen las amenazas y los desafíos de seguridad. Educar al personal sobre las mejores prácticas de seguridad en el desarrollo web y realizar auditorías de seguridad de manera regular.	ROJO
Vulnerabilidades en plugins y extensiones	3/10	Exposición de datos sensibles de los usuarios. Ejecución de código malicioso en el servidor. Ataques de inyección de SQL.	Utilizar extensiones y plugins solo de fuentes confiables y verificadas. Realizar actualizaciones regulares de	VERDE

		Compromiso de cuentas de usuario. Modificación del contenido del sitio.	todos los plugins y extensiones. Implementar una política de revisión y aprobación antes de agregar nuevas extensiones o plugins al sitio.	
Inyección de código en el lado del servidor	1/3	Ejecución de comandos maliciosos en el servidor. Exposición de datos confidenciales o robo de datos. Manipulación y degradación del rendimiento del sitio. Compromiso de cuentas de usuario y la seguridad del sistema.	Validación y desinfección de entrada de usuario en todos los formularios y campos de entrada. Utilizar consultas parametrizadas en las bases de datos en lugar de concatenación de cadenas. Implementar restricciones de seguridad en la configuración del servidor y el sistema operativo.	VERDE

1. Desarrollar políticas de seguridad
    a. Registrar las IP necesarias para los desarrolladores.
    b. Tener un apartado que contenga la autenticación y autorización de los usuarios que intentan acceder a recursos de la página web.
    c. Tener un control de acceso para los usuarios y para los desarrolladores o dueños de la página para acceder a distintas áreas que contiene la página.
    d. Tener una encriptación de datos para mejor seguridad del usuario.
    e. Constantemente actualizar y poner parches a la página web para mayor seguridad de la página anti hackeos.

2. Seguridad en Redes (LAN, WAN, WIFI)

La página cuenta con un certificado SSL, mediante el protocolo HTTPS, por lo que la seguridad en redes está cubierta.

3. Seguridad en Servidores

Está alojada en un servidor virtual en Oracle, el cuál tiene una instalación en Docker con los puertos asegurados, es decir, que tiene una white list de Ip's permitidas, esto es, que solamente esas Ip's pueden acceder al login de administración de la página.

4. Seguridad en Aplicación

Dentro de la página no existen campos con los que el usuario pueda subir o descargar información, por lo que el usuario promedio de la página no puede verse afectado por terceros que quieran interceptar su sesión para extraer información, ni ellos mismos pueden afectar la página.

5. Seguridad de Usuarios

La página abierta al público, NO cuenta con sesiones para el usuario promedio, más sin embargo si los hay para la administración de la página (que no está abierta para el público).

No solamente el login para la parte de administración está oculta, lo que le da seguridad a los usuarios administradores de entrada al dificultar la entrada a hackers y personas maliciosas, sino que también cuentan con encriptación para su contraseña.

6. Conclusiones

La página web ha demostrado un compromiso sólido con la seguridad al implementar una serie de medidas preventivas y de control. Esto incluye la adopción de políticas de seguridad, autenticación de usuarios y control de acceso, así como la encriptación de datos y actualizaciones regulares. Además, la seguridad en redes y servidores está respaldada por un certificado SSL, una infraestructura alojada en Oracle con una white list de IP's autorizadas, y una configuración segura en Docker. La seguridad de la aplicación está garantizada al evitar campos de carga y descarga, lo que reduce significativamente el riesgo para los usuarios. En general, estas prácticas sólidas disminuyen la probabilidad de vulnerabilidades y amenazas en múltiples niveles.

La página también se preocupa por la seguridad de los usuarios administradores al ocultar el acceso a la administración y al encriptar las contraseñas. Este enfoque proactivo crea un entorno más seguro para las personas con roles administrativos y protege la página web contra intrusiones no deseadas. En resumen, la combinación de medidas de seguridad en políticas, redes, servidores, aplicaciones y usuarios fortalece la defensa de la página web y garantiza una experiencia segura tanto para los usuarios como para los responsables de su administración.