ALLISSON KATHERINE TAPIA MEDINA

ID NAO: 3080

CONSULTOR DE CIBERSEGURIDAD

PROTOCOLOS DE SEGURIDAD CON PENTESTING Y CRIPTOGRAFÍA

SPRINT 2

DOMINGO 19 DE SEPTIEMBRE DEL 2024

Contenido

Sprint 3

Desarrolla

Sigue estas instrucciones para desarrollar el tercer avance de tu proyecto.

1. Elabora un reporte con los hallazgos derivados de la evaluación de riesgos, para su resolución acorde con las buenas prácticas de seguridad.

Evaluación de Riesgos y Resolución acorde a las Buenas Prácticas de Seguridad

1. Introducción

La seguridad de las aplicaciones web y las pasarelas de pago es crítica para garantizar la protección de datos sensibles y mantener la confianza del cliente. Este informe presenta los resultados de una evaluación de riesgos realizada en [nombre del sitio web] y su pasarela de pagos. A través de esta evaluación, se identifican vulnerabilidades que podrían comprometer la integridad, confidencialidad y disponibilidad de la plataforma. A continuación, se detallan los hallazgos, el análisis de riesgos y las recomendaciones para mitigar las amenazas encontradas, siguiendo las mejores prácticas de seguridad.

2. Metodología

El análisis de riesgos se llevó a cabo mediante un enfoque basado en las buenas prácticas de ciberseguridad, utilizando herramientas de escaneo automatizado y pruebas manuales. El proceso incluyó los siguientes pasos:

- **Identificación de activos críticos**

Se evaluaron el sitio web y la pasarela de pagos como los principales puntos de riesgo.

- **Identificación de amenazas**

Se revisaron posibles amenazas como inyección de código, ataques de fuerza bruta, vulnerabilidades en el procesamiento de pagos y errores de configuración.

- **Evaluación de impacto**

Se analizó el impacto potencial de las vulnerabilidades en términos de pérdida de datos, fraude, interrupción del servicio y daños a la reputación.

- **Evaluación de probabilidad**

Se evaluó la probabilidad de que cada vulnerabilidad fuera explotada con éxito.

- **Propuesta de mitigación**

Se presentan medidas correctivas basadas en las mejores prácticas de seguridad.

2.1. Evaluación de Seguridad del Sitio Web

La evaluación de seguridad del sitio web se llevó a cabo con herramientas como OWASP ZAP, escaneos de seguridad basados en plugins como Wordfence Security y Sucuri Security, así como pruebas manuales de las siguientes vulnerabilidades:

- **Inyección SQL y XSS (Cross-Site Scripting)**

Se realizaron pruebas automatizadas y manuales para identificar cualquier posible vulnerabilidad que pudiera comprometer la base de datos o permitir la ejecución de scripts maliciosos en el navegador de los usuarios.

- **Fuerza bruta y autenticación**

Se probaron los mecanismos de autenticación, con especial atención a la protección contra ataques de fuerza bruta mediante el uso de plugins como Limit Login Attempts Reloaded y reCAPTCHA by BestWebSoft.

- **Protección de datos sensibles**

Se revisó el cifrado de datos sensibles durante el tránsito y el almacenamiento.

2.2. Evaluación de Seguridad de la Pasarela de Pagos

Para la pasarela de pagos, se evaluaron tanto la lógica del proceso de pago como las medidas de seguridad implementadas. Esto incluyó:

- **Validación de transacciones**

Se revisó cómo se procesan y validan las transacciones, asegurándose de que no haya brechas de seguridad en el flujo de pago.

- **Cifrado de datos de pago**

Se verificó que los datos de las tarjetas de crédito y otra información financiera estén debidamente cifrados durante su tránsito y no se almacenen de manera insegura.

- **Pruebas de simulación de ataques**

Se realizaron simulaciones de ataques comunes, como la suplantación de identidad y la manipulación de pagos, para evaluar la robustez del sistema.

3. Hallazgos y Análisis

3.1. Sitio Web

Inyección SQL

No se detectan vulnerabilidades críticas de inyección SQL, ya que todas las entradas del usuario pasan por validaciones estrictas y están debidamente parametrizadas. Sin embargo, es necesario mejorar la documentación de seguridad para futuros desarrollos.

XSS (Cross-Site Scripting)

Se detectan puntos vulnerables en algunas páginas de perfil de usuario, donde los inputs no estaban siendo completamente sanitizados. Esto podría permitir que un atacante inyecte scripts maliciosos en los navegadores de otros usuarios.

Ataques de Fuerza Bruta

Se verificó que el plugin Limit Login Attempts Reloaded está debidamente configurado, bloqueando correctamente las IP después de varios intentos fallidos. Sin embargo, se recomienda aumentar la complejidad de las contraseñas y habilitar la autenticación multifactor (MFA).

3.2. Pasarela de Pagos

Validación de transacciones

No se encontraron errores significativos en el flujo de validación de las transacciones. Los datos se cifran correctamente durante su tránsito, y no se almacenan datos sensibles en la base de datos del sitio.

Suplantación de identidad (phishing)

Se identificó una falta de protección contra posibles intentos de phishing. Aunque los datos están cifrados, la interfaz de usuario no advierte adecuadamente a los usuarios sobre posibles correos electrónicos fraudulentos.

Pruebas de manipulación de pagos

No se encontraron vulnerabilidades que permitieran la alteración de montos o detalles de la transacción durante el proceso de pago. El sistema de pago cuenta con medidas robustas para evitar este tipo de ataques.

4. Recomendaciones

Con base en los resultados anteriores, las siguientes recomendaciones están alineadas con las mejores prácticas de seguridad y tienen como objetivo mitigar los riesgos identificados:

4.1. Sitio Web

Sanitización de inputs

Se recomienda reforzar la sanitización de todos los inputs de usuario para mitigar cualquier riesgo de XSS. Además, se debe implementar un sistema de validación en todas las entradas, especialmente en las áreas de perfil y comentarios.

Autenticación multifactor (MFA)

Implementar MFA para todos los usuarios, especialmente aquellos con roles administrativos, para mejorar la seguridad en el acceso.

Cifrado adicional

Asegurarse de que todos los datos sensibles estén cifrados tanto en tránsito como en reposo, incluso aquellos considerados de bajo riesgo.

4.2. Pasarela de Pagos

Protección contra phishing

Se recomienda habilitar advertencias claras y visibles para los usuarios sobre la posibilidad de correos fraudulentos. Además, se debe agregar la validación de los dominios de correos electrónicos de comunicación oficial.

Auditoría de seguridad regular

Realizar auditorías de seguridad regulares para detectar posibles vulnerabilidades que puedan surgir con el tiempo, especialmente después de cada cambio o actualización en la pasarela de pagos.

5. Conclusiones

La evaluación de riesgos realizada en el sitio web y la pasarela de pagos identificó varias áreas de mejora relacionadas con la seguridad de la plataforma. Aunque no se encontraron vulnerabilidades críticas que pongan en riesgo los datos de los usuarios de inmediato, existen aspectos a reforzar, particularmente en la sanitización de inputs, la protección contra ataques de phishing y la autenticación multifactor. Implementar las recomendaciones sugeridas fortalecerá la seguridad de la plataforma y reducirá significativamente la posibilidad de incidentes en el futuro.