CONTENIDO

1. Objetivo

Establecer un procedimiento para el desarrollo seguro de la aplicación y la plataforma web de Plus + Restaurant, esto basándose en los estándares internacionales de OWASP top 10, con las cuales se busca reducir la probabilidad de la materialización de un incidente de seguridad que pueda ocurrir o no, externa o internamente.
El OWASP Top 10 es un documento para desarrolladores y concientizando acerca de los estándares de seguridad de aplicaciones web. Representa un amplio concepto sobre los riesgos de seguridad más críticos para las aplicaciones web.
Así mismo se busca el Implementar buenas prácticas en el desarrollo de estos 2 sistemas de información, pues siguiendo estándares se reduce el riesgo ante ataques externos o internos y que estos puedan comprometer la confidencialidad, integridad y disponibilidad de la información de estos sistemas.

2. Alcance

Aplica a todos los sistemas tanto a la aplicación como a la plataforma web de la empresa las cuales se pueden desarrollar internamente o externamente dentro de la organización.

3. Propuesta OWASP TOP 10

A continuación, se presentan los controles estándar de seguridad que se deberán implementar en el proceso de desarrollo y lanzamiento a producción tanto de la aplicación como de la plataforma web de Plus + Restaurant.

1. Checar que todos los componentes de la aplicación sean requeridos y asegurar que son realmente necesarios. Para no instalar o tener librerías que no se encuentren en uso.
2. Validar que todos los componentes como bibliotecas, módulos y sistemas externos, que no son parte de la de la plataforma y de la aplicación principal, pero que sean necesarios para el correcto funcionamiento estén identificados.
3. Verificar que los datos sensibles del sistema estén siempre de manera encriptada Usando el protocolo de seguridad de HTTP y HSTS ya que este

último al colocar sus headers es de mucha ayuda para prevenir ataques de tipo SSL.

4. Realizar un modelo de amenazas para la aplicación y la plataforma y que este cubra los riesgos asociados con suplantación de identidad, manipulación, revelación de información y elevación de privilegios de usuarios.
5. Validar que el sistema cuente con que los controles de autenticación se encuentren de forma segura para evitar que los atacantes o cualquier tercero no puedan iniciar sesión de manera no autorizada, que todas las credenciales de autenticación para acceder a servicios externos a la aplicación se encuentran altamente cifradas y almacenadas en un lugar protegido así como que los campos de contraseña permitan o fomenten el uso de frases como contraseñas así como el uso de caracteres sin limitar el uso de gestores de contraseñas, por medio de contraseñas largas o altamente complejas.
6. Verificar que no existan puertos abiertos al público que no sean necesarios, mucho menos los puertos importantes, para así evitar cualquier tipo de taque que se pueda efectuar por medio de los puertos en un futuro.
7. Validar que los datos secretos o sensibles como llaves de un API y contraseñas no se incluyen en el código fuente o en los repositorios que se encuentren directamente en la nube, así como las interfaces administrativas de la organización no sean accesibles a intrusos. Para validar todo esto es necesario realizar testings antes de la lanzar la plataforma y la aplicación a producción para probar que todo funcione correctamente.
8. Deben de existir historiales o bitácoras con la información completa de la base de datos de la aplicación y de la plataforma para poder identificar por anticipado alguna actividad sospechosa y así evitar ataques de seguridad.
9. Tanto la aplicación como la plataforma al estar en producción se debe de estar al tanto de que usuario actualice todas sus versiones y tener la versión más reciente para que estas puedan utilizarse de manera totalmente segura.
10. Tener en cuenta de que es necesario analizar la plataforma y la aplicación de manera concurrente para validar que esta no se encuentre en estado vulnerable para un ataque, para realizar el análisis de vulnerabilidad podemos usar la herramienta de Nessus, ya que usando esta herramienta podemos observar si nuestro sistema tiene algún punto vulnerable y así al detectarlo a tiempo es posible resolver el punto vulnerable.

4. Elaboración y aprobación

Nombre y Cargo	Fecha	Rol
Hanna Siddharttha Lizarraga Ceballos Encargada de Seguridad	13-11-2021	Creación del documento

5. Historial de cambios

Revisión	Descripción del cambio	Responsable	Fecha
01	Creación del documento	Hanna Siddharttha Lizarraga Ceballos	13-11-2021