OWAS Top-10
Symetrix marine

Heyner Fernando Cruz Guzmán
UNIVERSIDAD MODELO

CONTENIDO

1. Objetivo

Elaborar un plan de seguridad de software para la página de *Symetrix marine* basándose en el documento de los 10 registros de seguridad más importante en aplicaciones web que sería OWASP Top-10.

2. Plan para OWAS Top-10

OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la Open Web Application Security Project, un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. A continuación, se mostrarán 11 puntos que ayudarán a tener una mejor seguridad de software en base a los 10 puntos de OWASP.

1. Se deberá tener un buen control de acceso, implementar mecanismos de control de acceso y usarlos en toda la aplicación, incluida la minimización del uso del intercambio de recursos entre orígenes (CORS), de este modo se tiene un estándar con el cual trabajar. De igual forma se deberá limitar el acceso a la API, de esta forma se evitará accesos a la API no autorizados y evitaremos la manipulación de parámetros o navegación forzada.
2. Se deberá invalidar los indicadores de sesión con estado después de cerrar la sesión, esto evitará que se forcé a la página y puedan navegar como usuarios privilegiados cuando deberían ser estándar.
3. Para evitar eventos o incidentes con Inyecciones se deberá Implementar un API segura, la cual evita el uso del interprete y obteniendo una interfaz parametrizada. Combinándolo con validación de entrada del lado de servido positiva podemos proteger de mejor forma nuestros datos.
4. Para asegurar los registros se utilizará LIMIT y otros controles de SQL para evitar la divulgación masiva de estos.
5. Se deberá tener un diseño seguro el cual nos ayudará a tener una metodología que nos permita evaluar constantemente las amenazas y garantizar que el código este diseñado y probado de manera sólida.

Determinar el flujo correcto de los usuarios al igual que analizar los flujos esperados y de falla.

6. Los entornos de desarrollo, control de calidad y producción deben configurarse de forma idéntica, con diferentes credenciales utilizadas en cada entorno. Este proceso se debe automatizarse para minimizar el esfuerzo necesario para configurar un nuevo entorno seguro. Al igual que tener una plataforma sin funciones, componentes y documentación innecesaria.
7. Tener una Arquitectura de aplicaciones segmentada para una separación efectiva y segura entre componentes, con segmentación, con el uso de contenedores o grupos de seguridad de la nueve (ACL)
8. Implementar la autentificación de múltiples factores para evitar el relleno automatizado de credenciales, la fuerza bruta y los ataques de reutilización de credenciales robadas. AL igual que asegurar de que las rutas de registro, recuperación de credenciales y API estén reforzados contra los ataques de enumeración de cuentas.
9. Asegúrese de que todas las fallas de validación de entrada, control de acceso y del lado del servidor puedan registrarse con suficiente contexto de usuario para identificar cuentas sospechosas o maliciosas y mantenerse durante el tiempo suficiente para permitir un análisis forense retrasado.
10. Establecer o adoptar un plan de recuperación y respuesta a incidentes, como el Instituto Nacional de Estándares y Tecnología (NIST) 800-61r2 o posterior. De esta forma podremos tener una correcta respuesta a cualquier incidente de seguridad.
11. Realizar un inventario continuo de las versiones de los componentes del lado del cliente y del lado del servidor y sus dependencias utilizando herramientas de versiones o *OWASP Dependency Check*. Utilice herramientas de análisis de composición de software como *Benchmark ESG* | *Gensuite* para automatizar el proceso.

3. Elaboración y creación

Nombre y Cargo	Fecha	Rol
Heyner Fernando Cruz Guzmán ***Director de Seguridad***	13/11/21	Agregó contenido, revisó la redacción y la ortografía

4. Historial de cambios

Revisión	Descripción del cambio	Responsable	Fecha
01	Creación de documento	Heyner Fernando Cruz Guzmán	13/11/21