Sistemas de Gestión de Seguridad de la Información 2023/2024

Entrega 2 – Auditoría Sistema Web

Fecha de entrega: 26 de noviembre de 2023 a las 23:55.

Alcance y Objetivos

El objetivo principal de esta entrega es realizar una auditoría de seguridad a vuestro trabajo 1 usando una de las herramientas de pentesting más conocidas (ZAP[1]) y solucionar las vulnerabilidades del informe OWASP 2021 visto en clase.

ZAP es una herramienta que sirve para analizar sitios web en búsqueda de vulnerabilidades. Para ello, actúa como si fuera un proxy y trabaja con todas las peticiones que se hacen al sitio web y así analiza tanto las peticiones como las respuestas en busca de posibles agujeros de seguridad.

El trabajo consiste en realizar dos auditorías sobre la seguridad de la aplicación web que elaborásteis en el trabajo 1 utilizando ZAP. La primera auditoría debéis realizarla en base a la aplicación tal y como la entregásteis. La segunda auditoría debéis realizarla una vez solucionadas, como mínimo, las vulnerabilidades que se describen en este enunciado.

El uso de ZAP es recomendable pero no obligatorio. Podéis usar cualquier otra herramienta de pentesting, siempre que se documente su uso.

Forma de entrega

Se debe crear un rama adicional en GitHub, llamada **entrega_2**, con las modificaciones necesarias para arreglar las vulnerabilidades. Además, se debe entregar a través de eGela un fichero comprimido (.zip) que contenga un informe con el resultado de las auditorías, con el siguiente contenido:

- URL de Github del proyecto auditado.
- Cómo se han realizado las auditorías (explicación en forma de tutorial).
- Análisis sobre el resultado de ambas auditorías.
- Explicación de los cambios realizados en el código para solucionar las vulnerabilidades indicadas. Tenéis que explicar cómo habéis solucionado la vulnerabilidad, y en caso de que la aplicación no fuera vulnerable, qué habíais hecho en el código original para que el sistema no fuera vulnerable. En caso de que uséis funciones desarrolladas por terceros o busquéis información extra de cómo solucionar las vulnerabilidades, recordad indicarlo en el informe con su correspondiente referencia bibliográfica.
- Conclusiones sobre las diferencias entre ambas auditorías.

1 https://www.zaproxy.org/

Evaluación

El informe se evaluará sobre 10 puntos. Este trabajo supondrá un 50% de la nota del apartado “Trabajos” de la asignatura. Se valorará especialmente vuestras reflexiones y conclusiones sobre las vulnerabilidades detectadas.

Vulnerabilidades a solucionar

Las vulnerabilidades a solucionar son, como mínimo, las vistas en clase:

- Rotura de control de acceso.
- Fallos criptográficos.
- Inyección.
- Diseño inseguro.
- Configuración de seguridad insuficiente.
- Componentes vulnerables y obsoletos.
- Fallos de identificación y autenticación.
- Fallos en la integridad de datos y software.
- Fallos en la monitorización de la seguridad.

Si el sistema no es vulnerable a una de las vulnerabilidades vistas en clase, hay que documentar la comprobación y la causa de que no sea vulnerable.

Si se descubren vulnerabilidades no vistas en clase y se incluyen en la auditoría, también se tendrán en cuenta para mejorar la nota.