UNIVERSIDAD DE COLIMA

Facultad de Telemática – Ingeniería de Software

Actividad 11.- Auditoria de Código Fuente

Desarrollo de Software Seguro

Daniel Hernández Ascencio

6°K

Prof. José Nabor Ramírez Morfín

Villa de Álvarez, Colima

Martes, 27 de abril de 2021

Introducción

Es bien sabido que una auditoria es un proceso sistemático, documentado e independiente que permite obtener evidencia de auditoría, como registros o evaluaciones fácticas o cualquier información relacionada. El propósito es realizar una evaluación objetiva basada en políticas, procedimientos o requisitos para determinar el grado de cumplimiento, llamado estándar de auditoría.

Ahora bien, una auditoría informática es un proceso formal, objetivo e independiente de productos de software, cuyo objetivo es evaluar el cumplimiento de especificaciones, controles, procedimientos y estrategias para determinar la integridad, confiabilidad y efectividad de los sistemas de información o la información de la red.

¿Qué es auditoria de código fuente?

La auditoría del código fuente es parte de la integración de la seguridad en el ciclo de vida del desarrollo de software y es una estrategia complementaria para las pruebas de penetración o la revisión de seguridad.

La revisión del código de una aplicación se puede realizar en diferentes etapas del proceso de desarrollo. Idealmente, cada nueva iteración de desarrollo dará como resultado la verificación de la seguridad y la calidad del software, pero la mayoría de las empresas consideran integrar revisiones cada primavera de la aplicación.

En la auditoria del código fuente, las búsquedas se realizan dentro del código de la aplicación en sí, con el objetivo de descubrir fragmentos de código potencialmente vulnerables con problemas conocidos. Para realizar estas búsquedas se utilizan algunas herramientas para automatizar el proceso y realizar la verificación manual.

Cabe señalar que la programación modular y estructurada ayuda a revisar el código, por lo que el equipo de desarrollo necesita trabajar con el equipo de revisión porque conocen la estructura de la aplicación y pueden facilitar la revisión del código a evaluar.

Una revisión de seguridad de código fuente permite identificar aquellas debilidades que afectan a la confidencialidad, disponibilidad o integridad de la información gestionada por la aplicación, ayudando a la protección de la información de negocio.

¿Como se realiza una auditoria de código fuente?

Para encontrar fragmentos vulnerables en el de código fuente y mejorar la calidad del código se realizará análisis estático, dinámico y de seguridad del código.

Análisis estático

El análisis estático consiste en evaluar el código sin tener la necesidad de ejecutar la aplicación, un aspecto importante a considerar es conocer el lenguaje de programación con el que se desarrolló la aplicación.

El análisis estático permite detectar entre el 30% y 70% de defectos en el código, haciendo que la corrección del código sea más fácil y menos costosa con relación a la fase del análisis dinámico del código.

Los defectos que se busca evaluar mediante el análisis estático son los siguientes:

- Corrección: El código evaluado no debe contener errores.
- Compleción: El código evaluado debe estar completo.
- Consistencia: No debe haber contradicciones entre 2 o más sentencias.

Técnicas de evaluación estáticas:

- Revisiones: Verifica la correcta transición entre fases del ciclo de desarrollo de software.
- Análisis de flujo de control: Detecta defectos causados por desarrollo anómalo del código.
- Análisis de flujo de datos: Detecta anomalías en el flujo de datos tomando como estrada diagramas de control de flujo de datos.

Análisis dinámico

El análisis dinámico consiste en la evaluación del código ejecutando la aplicación o un de sus componentes dentro de un entorno controlado, se compara los resultados obtenidos con los resultados esperados con el propósito de encontrar fallas en la aplicación para identificar el defecto asociado a esa falla y corregirlo.

Técnicas de evaluación dinámicas:

- Caja Blanca o Estructurales: Se requiere conocer la lógica del programa.
- Caja Negra o Funcionales: Se requiere conocer el objetivo o funcionalidad del código

Análisis de vulnerabilidades

El análisis de vulnerabilidades tiene como objetivo identificar vulnerabilidades que exponen a las aplicaciones de posibles ataques informáticos, perjudicando a la organización en sus actividades, el propósito de este análisis es de gestionar y mitigar los riesgos ligados a las vulnerabilidades encontradas. La enumeración de vulnerabilidades se realiza con ayuda de herramientas automáticas y revisiones manuales y posteriormente se realiza un inventario de vulnerabilidades descartando falsos positivos y priorizando vulnerabilidades de alto impacto para la organización

Referencias

Santacruz, C. D. (2020). Auditoría de Código Fuente Utilizando la Norma ISO-19011 y el Estándar IEEE-1028 (Bachelor's thesis, Quito, 2020.).