TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 2 – UNIDAD 3

Universidad Tecnológica de Pereira | faceIT

Desarrollo desde un Enfoque Seguro

El desarrollo de software con un enfoque seguro es fundamental para proteger aplicaciones y datos sensibles de posibles ataques. En un entorno digital donde las amenazas están en constante evolución, incorporar prácticas de seguridad desde las etapas iniciales del ciclo de vida del desarrollo ayuda a minimizar riesgos, reducir costos de correcciones tardías y garantizar la confianza de los usuarios en el producto final. OWASP, con sus proyectos y herramientas, desempeña un papel esencial en promover y facilitar un desarrollo seguro.

Algunas herramientas que ayudan en el ciclo de desarrollo y de mantenimiento de software son:
Herramientas de análisis estático y dinámico de código

Las herramientas de análisis estático (SAST) y dinámico (DAST) son fundamentales para identificar vulnerabilidades en el código.

.

SAST: Analiza el código fuente, identificando problemas de seguridad antes de que la aplicación se ejecute. Este tipo de herramientas permite detectar vulnerabilidades como inyecciones de SQL, errores de configuración y malas prácticas de programación. Este tipo de soluciones se integran en los ciclos de vida del software para que las aplicaciones no sean desplegadas ni se reciban cambios por parte de los desarrolladores si se encuentra que, al menos uno de los cambios genera brechas de seguridad.

Incluso se pueden crear reglas personalizadas para validar también estilos de programación y buenas prácticas de escritura de código.

DAST: Evalúa la seguridad de una aplicación en tiempo de ejecución, simulando ataques reales para identificar fallas en la lógica o configuraciones inseguras. DAST se enfoca en la interacción con la aplicación desde una perspectiva externa, sin necesidad de acceso al código fuente.
Ambas herramientas son complementarias y su uso conjunto fortalece significativamente la postura de seguridad de las aplicaciones. Siempre es recomendado que en el ciclo de vida de software se incluyan ambas categorías de herramientas y se estén generando informes periódicamente.
También es recomendado que se estén actualizando las herramientas para cubrir exploits de día cero y vulnerabilidades que se descubran que pueden afectar al software existente.