Seguridad en el software: en fase de codificación, pruebas y depuración

- **¿Entrada?**
  - Requerimientos de seguridad
  - Casos de abuso
  - Análisis de riesgo: modelado de amenazas.

- **Prácticas importantes:**
  - Buenas prácticas de desarrollo
  - **Revisión de código**
  - **Test de penetración**

Pruebas de seguridad

¿Con base a qué se realizan las pruebas?

Con base al análisis de riesgos.

Luego de identificar los riesgos del sistema-aplicativo y de haber diseñado las pruebas con base a ellos, bajo la perspectiva de un atacante.

"PRUEBAS CON BASE A RIESGOS"

Objetivos: operación bajo estrés, fiabilidad, falta de defectos, capacidad de supervivencia.

No olvidar, las dos perspectivas de pruebas seguridad: Funcionales y perspectiva del atacante

¿Las pruebas de seguridad deberían comenzar antes de las pruebas de Integración?

¿Qué se debe utilizar en las pruebas de seguridad?

- Modelos de ataque
- Casos de abuso
- Análisis de riesgo

Desde la perspectiva del ATACANTE, las pruebas realizadas se pueden clasificar en:

- Caja negra
- Caja blanca
- Caja grises

Fases generales de las pruebas de seguridad:

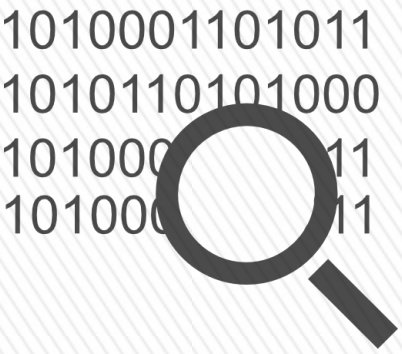
- Descomponer el sistema en sus componentes
- Identificar y clasificar las interfaces de los componentes
- Encontrar problemas de seguridad

Análisis estático (SAST)

¿Cuáles son las dos causas principales de errores en el código por parte del programador?

Razones para hacer SAST:

- Comprueban a fondo
- Podrían indicar el origen
- Previo a ejecución-lanzamiento
- Comprobar “nuevas vulnerabilidades”



Desde la perspectiva del atacante, ¿qué tipo de prueba será (caja negra, blanca…)?

Existen herramientas (SW) para hacer análisis estático. Para hacer "White box testing". Son conocidas como herramientas SAST.

Principal desventaja: **producen mucho falsos positivos**. (mucho ruido, como se conoce)

¿Qué pasa con los **falsos negativos** en estas herramientas?

"Sentido falso de seguridad"

Proceso:

SAST Tool

Falso positivo

Falso negativo

¿Son estas herramientas automáticas?

Análisis dinámico (DAST) – Black box testing

Se debe hacer en la fase previo a producción.

¿De qué trata? Verificar cómo el SW se comporta y resiste ante diferentes tipos de ataques. *¿Por qué cajas negras?*

Importante trabajar con base a **escenarios**. Incluyendo los peores escenarios.

Si el resultado de una prueba DAST no revela defecto, ¿qué significa?

No olvidar: políticas de seguridad, secuencia de ataques, amenazas y riesgos.

Pasos:

- Revisar inf. de casos de abusos, patrones de ataque, modelado de amenazas.
- Identificar vulnerabilidades
- Buscar exploit
- Ejecutar exploit
- Realizar pruebas DAST y Fuzzing

El test de penetración es una prueba de tipo DAST. Y claro que existen herramientas (SW) que realizan test de penetración a SW, además de otros tipos de pruebas DAST.