ANEXO IV: DOCUMENTACIÓN ANÁLISIS DE SEGURIDAD

Análisis de Seguridad

VERSIÓN 1.0 – FECHA 19/04/2021

Municipalidad de Córdoba

INDICE

Introducción

El presente documento tiene como propósito indicar como se realizará el proceso de 'Análisis de Seguridad' necesario y solicitado por la Municipalidad de Córdoba para cualquier sistema que se utilice para gestiones municipales (aplicaciones Web/Mobile). El correspondiente análisis esta dispuesto tanto para desarrollos propios como de terceros.

Hoy en día las aplicaciones están expuestas a diferentes amenazas creadas para extraer información organizacional o personal y con esto realizar ataques dañinos que vulneran la seguridad de las operaciones.

Por lo tanto el análisis de seguridad es un servicio por medio del cual se comprueban a través de herramientas de software y servicios de consultoría la debilidad o fortaleza de un sistema ante posibles amenazas que pueden atentar contra la seguridad de un sistema de información.

En los siguientes puntos se detalla objetivo, alcance, definiciones, equipo de trabajo y procedimiento que se ejecutarán cada vez que se realiza el correspondiente análisis de seguridad.

Objetivo

El objetivo del correspondiente 'Análisis de Seguridad es detectar las vulnerabilidades (debilidades o fallos) que ponen en riesgo la seguridad de la información de la Municipalidad de Córdoba.

Alcance

Este análisis de seguridad tendrá como resultado un informe técnico donde se indicarán las vulnerabilidades detectadas junto con el proceso que se utilizo para encontrarlas y de ser necesario un informe ejecutivo.

Equipo y Herramientas

El 'equipo de seguridad' que ejecutará el correspondiente análisis está formado por personal del laboratorio de sistemas LabSis-CIDS perteneciente a la UTN_FRC.

El correspondiente 'equipo de seguridad' emplea metodologías y buenas prácticas sugeridas por OWASP y SANS en los procesos de análisis de seguridad, poniendo también énfasis en pruebas de experiencia acumulada durante los análisis realizados en los últimos años.

Las herramientas utilizadas son de código abierto y aplicaciones de desarrollo propio adaptadas a cada uno de los proyectos de desarrollo en análisis. Las pruebas desarrolladas son automáticas y manuales.

Referencias

Para diagnosticar los riesgos se utilizan los estándares asociados a vulnerabilidades encontradas, en este caso se usa el Sistema Común de Puntuación de Vulnerabilidad (CVSS). Se utilizará la Base Score, por lo que el riesgo en el negocio, entre otras cosas, no está contemplado.

Las categorías son extraídas del listado de vulnerabilidades del sitio oficial de OWASP.

Sistema Común de Puntuación de Vulnerabilidad: https://www.first.org/cvss.

Sitio oficial OWASP: https://www.owasp.org/index.php/Category:Vulnerability

Sitio oficial SANS: https://www.sans.org

Definiciones

CVSS: Common Vulnerability Scoring System
OWASP: Open Web Application Security Project
SANS: SysAdmin Audit, Networking and Security Institute

UTN-FRC: Universidad Tecnologica Nacional – Facultad Regional Córdoba
LabSis-CIDS: Laboratorio de Sistemas – Centro de Investigación y Desarrollo de Software

Proceso utilizado

El proceso del análisis de seguridad comienza con una reunión entre las partes, el propósito es definir objetivos y características del análisis a ejecutar. De allí surge la posibilidad de una inducción por parte del proveedor del sistema para poder dimensionar el alcance específico del 'análisis de seguridad' que se realizará a la aplicación.

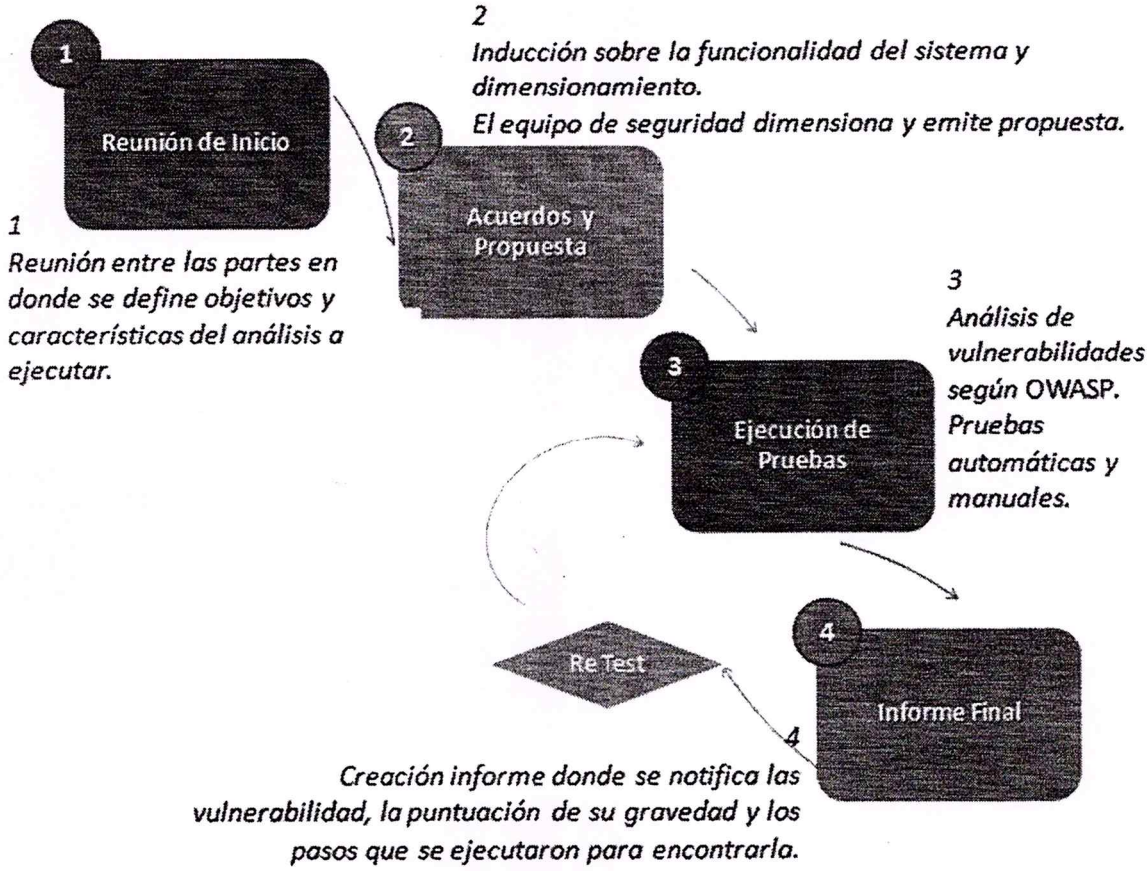
De los datos recolectados en esta primera reunión el equipo de seguridad, realiza la propuesta donde se definen los objetivos generales y específicos, descripción del alcance, tipos de análisis técnicos de seguridad, visibilidad, posicionamiento del test de penetración, etapas del análisis de seguridad, generalidades y los requerimientos para llevar a cabo el análisis.

En la propuesta también se detalla el comienzo del análisis con fecha de fin estimada, supeditada al avance normal que requieren las pruebas.

Se recomienda el uso de un canal de comunicación de mensajería instantánea para sortear los problemas funcionales o de disponibilidad en el transcurso de la ejecución de las pruebas.

Culminadas las pruebas en las fechas acordadas, se lleva a cabo la realización de informes que se entregan a la Municipalidad de Córdoba.

Posterior al análisis del mismo y de la aplicación del plan de ejecución que lleve a cabo el proveedor, puede surgir la necesidad de la realización de un rechequeo de los hallazgos informados previamente, en ese caso solo se lleva cabo el recheck de los hallazgos y se genera otro informe donde se notifica si las vulnerabilidades fueron resueltas o no.



Requerimientos para el proceso

Estos requerimientos dependen de cada proyecto, de la disponibilidad de los mismos por parte de los proveedores y algunos tienen carácter de obligatorios dependiendo del tipo análisis que se lleve a cabo, los cuales se definen en cada proyecto de acuerdo al alcance.

1. Video llamada para inducción al sistema en análisis.
2. Entorno donde se realiza la prueba (recomendación preproducción)
3. Métodos de acceso y links de acceso.
4. Un usuario por cada perfil y por cada rol.
5. Listado de Funcionalidades.
6. Base de datos con suficiente información registrada por funcionalidad.
7. Acceso a repositorio de código fuente para análisis estático.
8. Documentación (Principalmente funcionalidades de cada acceso al sistema existente).

9. Contacto para evacuar dudas funcionales o informar sobre problemas que surgen para la continuidad del análisis. (Generación de un grupo para canal de comunicación instantánea).