SESION 8 1ER PARCIAL

Desarrollo de aplicaciones seguras

OBJETIVO: al finalizar la sesión el alumno configurara y realizara pruebas en desarrollo de aplicaciones Java Web

Consideraciones teóricas.

OWAS Open Web Aplication Security Proyect

Es un proyecto de código abierto dedicado a determinar, combatir las causas que hacen que el software, aplicaciones, sistemas, programas sean seguros. Organismo internacional con las mejores prácticas, gestión de calidad de proyectos de software, enfocados principalmente al desarrollo web multiplataforma.

Para la administración de la seguridad informática determina los riesgos recabados en las sig. Áreas:

1.- Inyección. Los ataques de inyección ocurren cuando se envían datos desde formularios, archivos digitales con diversos formatos y con procesos ETL (explotación, transportación y carga de datos). Sobre bases de datos SQL (Oracle, Mysql, MarioBD, Infomix, SQL Server, PostgreSQL, BD2, BD1 BD2) relacionales y NO SQL (PostgreSQL, MondoBD, FireBird) Json OWASP minimiza los ataques de inyección.

2.- Autenticación rota. Fuga de datos, métodos inseguros GET

3.- exposición de datos duros, confidenciales

Exposición de información en el frond end de la aplicación y su almacenamiento visible en base de datos

4.- XXE Entidades XML Internas y externas

Referencia a códigos de etiquetas compuestas y simples de lenguaje extendido marcado

5.- pedidas de control de acceso

Validación desde base de datos vulnerables sin métodos criptográficos, contraseñas inseguras

6.- mala configuración de la seguridad

Excesivos controles, listas negras sin configuración y funcionamiento

7.- Scripting enter sites

Microcódigos, scripts añadidos por URL o inyección SQL, envíos de correos electrónicos, actividades de tareas del usuario

8.- deserialización no segura

Descargar datos de fuentes no confiables generando ataques DDOS ataques de inyecciones remotas, apis y platillas web

9.- componentes con vulnerabilidades

Código redundante no protegido, parches de seguridad, códigos no comprobados

10.- registro, supervisiones insuficientes

Mejoras no continuas, 3er día, actualizaciones sin verificación, análisis técnicos de profundo plan de mantenimiento en el ambiente de producción

Se implementarán para las áreas también de

infraestructura de TI

Análisis de datos

Administración de proyectos seguros

Redes y comunicaciones seguras

Desarrollo 1. Descargue NetBeans web y genere un proyecto bajo servidor de aplicativos TomCat con

Usuario: Alejandroowsap

Password: Encriptado shai >java1

455765d5eed19715f100e22ca54016e3034f8820031