UTT
UNIVERSIDAD TECNOLÓGICA DE TIJUANA
GOBIERNO DE BAJA CALIFORNIA

TEMA:

Puntos de vulnerabilidad de las aplicaciones móviles

PRESENTADO POR:

Pliego Cortes Giovanni

GRUPO:

10 ° B

MATERIA:

Desarrollo móvil integral

CARRERA:

TI. Desarrollo de software multiplataforma

Docente:

Ray Brunett Parra Galaviz

Tijuana, Baja California, 22 de enero del 2025

1. **Almacenamiento de Datos Inseguro**

Guardar datos sensibles (como contraseñas, tokens de sesión o información personal) en almacenamiento local sin cifrado adecuado.

2. **Fallas en la Comunicación de Red**

Transmitir datos sensibles a través de canales inseguros, como HTTP no cifrado.

3. **Inyección de Código**

Permitir que usuarios maliciosos inyecten código (como SQL, JavaScript o comandos del sistema) debido a una validación deficiente de las entradas.

4. **Autenticación y Autorización Débil**

Implementaciones incorrectas de autenticación o autorización que permitan accesos no autorizados.

5. **Fallas en el Manejo de Sesiones**

Manejo incorrecto de tokens de sesión o cookies, como almacenarlos sin cifrar o no invalidarlos tras cerrar sesión.

6. **Vulnerabilidades de Bibliotecas de Terceros**

Usar bibliotecas desactualizadas o de fuentes no confiables.

7. **Reversión de Ingeniería y Modificación de Código**

El código de la aplicación móvil puede ser descompilado, lo que permite que atacantes extraigan claves, lógica empresarial o encuentren vulnerabilidades.

8. **Falta de Validación en el Lado del Servidor**

Confiar completamente en la validación del lado del cliente.

9. **Permisos Excesivos**

Solicitar permisos que no son necesarios, lo que puede ser explotado por atacantes si se compromete la aplicación.

10. **Actualizaciones y Parcheo Insuficientes**

No abordar vulnerabilidades descubiertas en versiones anteriores de la aplicación.

11. **Uso de APIs Inseguras**

Exponer APIs con controles de seguridad insuficientes o datos sensibles

12. **Falta de Protección Contra Malware**

Las aplicaciones pueden ser objetivo de malware que manipula el entorno de ejecución.