Reporte de Vulnerabilidades

Pruebas de Vulnerabilidad

1. Herramientas Utilizadas:

- OWASP ZAP: Para análisis de vulnerabilidades web.

- MobSF (Mobile Security Framework): Para análisis de seguridad de aplicaciones móviles.

- Herramienta adicional: Cualquier otra herramienta de seguridad que se considere necesaria para complementar el análisis.

2. Pasos para Realizar las Pruebas:

1. Configuración del Entorno:

- Asegurarse de que la aplicación esté configurada correctamente para ser analizada en un entorno seguro.

- Habilitar los permisos necesarios en el dispositivo o emulador.

2. Escaneo con OWASP ZAP:

- Ejecutar OWASP ZAP para escanear la comunicación de la aplicación y detectar posibles vulnerabilidades como:

- Inyección de código (SQL, XSS).

- Fuga de información en las respuestas HTTP.

- Falta de autenticación o autorización adecuada.

- Guardar los resultados en formato PDF.

3. Escaneo con MobSF:

- Cargar el APK de la aplicación en MobSF para analizar el código fuente y buscar vulnerabilidades comunes en aplicaciones móviles como:

- Permisos no seguros.

- Exposición de datos sensibles.

- Configuración insegura en el manifiesto de la aplicación.
- Generar el reporte en formato PDF.

4. Revisión Manual:

- Revisar el código fuente y la configuración de la aplicación para detectar posibles puntos débiles no detectados por las herramientas automáticas, como el uso de claves duras en el código o configuraciones inseguras.

5. Reporte Detallado:

- Unificar los resultados obtenidos por ambas herramientas y el análisis manual.
- Documentar cada vulnerabilidad encontrada, su impacto y las posibles soluciones en un informe detallado.

3. Generación del Reporte:

- Nombre del archivo: `vulnerability_report.pdf`
- Ubicación: Guardar el archivo en el repositorio GitHub, en la carpeta raíz o en una carpeta dedicada a la documentación.
- Contenido del Reporte:
  - Descripción de las herramientas y métodos utilizados.
  - Listado de vulnerabilidades encontradas, organizadas por nivel de severidad (alta, media, baja).
  - Impacto de cada vulnerabilidad en la seguridad de la aplicación.
  - Recomendaciones para corregir cada vulnerabilidad.
  - Evidencia (capturas de pantalla o logs) de las pruebas realizadas.