Proyecto: Simulación y Explotación de Vulnerabilidades de Software

Objetivo:

Desarrollar una aplicación (API y/o Frontend) que contenga vulnerabilidades de seguridad predefinidas, con el fin de simular y explotar ataques reales. El proyecto busca demostrar el impacto de fallos críticos y reforzar la concienciación en ciberseguridad mediante pruebas prácticas.

Alcance:

Implementación de Vulnerabilidades en una Aplicación (Escoger dos):

- Inyección de Comandos al Sistema Operativo (OS Command Injection): Permitir la ejecución arbitraria de comandos del SO mediante entradas no validadas.
- Inyección de Código JavaScript (XSS/Code Injection): Crear un vector de ataque para ejecutar scripts maliciosos en el lado del cliente.
- Ataque de Denegación de Servicio (DoS): Simular un colapso del sistema mediante sobrecarga de recursos.
- Hombre en el Medio (Man-in-the-Middle/MitM): Interceptar o manipular comunicaciones entre cliente y servidor.
- (Otras vulnerabilidades como SQLi, CSRF, etc.)

Simulación de Ataques:

Explotar cada vulnerabilidad implementada, documentando el proceso paso a paso.

Validar el impacto en tiempo real (ej. acceso no autorizado, pérdida de datos, interrupción del servicio).

Entregables:

Código Fuente:

- Aplicación funcional con las vulnerabilidades integradas (versión 1 para revisión inicial y versión final corregida).
- Scripts o herramientas utilizadas para los ataques.

Informe Ejecutivo:

- Identificación de Vulnerabilidades: Descripción técnica de cada fallo y su ubicación en el código.
- Metodología de Ataque: Pasos detallados para explotar cada vulnerabilidad, evidencias (capturas, logs).
- Recomendaciones de Mitigación: Soluciones para corregir los fallos (ej. sanitización de entradas, rate-limiting, uso de HTTPS).

Cronograma:

Versión 1 (Viernes, 30 de mayo):

- Aplicación básica funcional con al meno 1 vulnerabilidad implementada.
- Avance parcial del informe (estructura y hallazgos iniciales).

Versión Final (Lunes, 3 de junio):

- Aplicación completa con todas las vulnerabilidades requeridas.
- Informe ejecutivo finalizado y ataques documentados.
- Versión "parcheada" con las mitigaciones aplicadas.