Simulación y Análisis de Vulnerabilidades en Aplicaciones Web

Objetivo:

El objetivo de este trabajo es aplicar los conocimientos adquiridos sobre vulnerabilidades en aplicaciones web mediante el análisis y la resolución de problemas hipotéticos. Los estudiantes deberán identificar, describir y proponer soluciones para diversas vulnerabilidades en escenarios proporcionados. Además, deberán reflexionar sobre las implicaciones de seguridad de cada escenario.
Organizarse en grupos de al menos 3 personas en lo posible o más.

Instrucciones:

1. **Presentación**: asignatura, docente, consigna elegida, estudiantes que colaboraron en el trabajo.
2. **Desarrollo**:
    - Escenarios de Vulnerabilidad:
        - Se proporcionan siete escenarios hipotéticos, cada uno relacionado con una de las vulnerabilidades estudiadas (SQL Injection, Cross Site Scripting (XSS), Business Logic Abuse, Open Redirect, Path Traversal, CSRF y NoSQL Injection). Deben seleccionar al menos tres.
        - Para cada escenario, los estudiantes deben realizar las siguientes tareas:
            - Identificación y Descripción de la Vulnerabilidad:
                - Identificar la vulnerabilidad presente en el escenario.
                - Describir cómo se manifiesta la vulnerabilidad y qué la causa.
            - Impacto Potencial:
                - Analizar el impacto que podría tener la explotación de la vulnerabilidad en la aplicación y en los usuarios.
            - Explotación Hipotética:
                - Describir paso a paso cómo un atacante podría explotar la vulnerabilidad, incluyendo cualquier técnica o herramienta que utilizaría.
            - Propuesta de Mitigación:
                - Proponer medidas específicas para mitigar la vulnerabilidad y evitar futuras explotaciones (en el lenguaje de programación que trabajen).
                - Explicar cómo las soluciones propuestas previenen la vulnerabilidad.

Escenarios Proporcionados:

- **Escenario 1: SQL Injection**
  - Descripción: Un formulario de inicio de sesión en un sitio de comercio electrónico que no valida adecuadamente las entradas del usuario.
- **Escenario 2: Cross Site Scripting (XSS)**
  - Descripción: Un campo de comentarios en un blog que permite a los usuarios insertar scripts sin validación.
- **Escenario 3: Business Logic Abuse**
  - Descripción: Un sistema de descuentos en una tienda en línea que permite aplicar múltiples códigos de descuento en una sola transacción.
- **Escenario 4: Open Redirect**
  - Descripción: Un enlace de redirección en un correo electrónico de confirmación que no valida la URL de destino.
- **Escenario 5: Path Traversal**
  - Descripción: Un sistema de gestión de archivos en un sitio web que permite a los usuarios descargar archivos especificando rutas de directorio relativas.
- **Escenario 6: CSRF (Cross-Site Request Forgery)**
  - Descripción: Un formulario de cambio de contraseña en una aplicación de banca en línea vulnerable a solicitudes no autorizadas de otros sitios web.
- **Escenario 7: NoSQL Injection**
  - Descripción: Una aplicación de búsqueda en una tienda en línea que no valida las entradas del usuario, permitiendo la inyección de código en consultas NoSQL.

3. Conclusión:

- Resumen de los puntos clave discutidos en cada escenario.
- Importancia de la implementación de buenas prácticas de seguridad en el desarrollo de aplicaciones web y sobre el rol de los desarrolladores y administradores en la prevención de vulnerabilidades.

Fecha de primer entrega: 17 de junio
Fecha de segunda entrega: hasta el 30 junio

Entregar al mail fernando.gianni@ort.edu.ar