Proyecto Final de Curso
Curso: Optativa
Periodo: 2610

Análisis, Explotación y Mitigación de Vulnerabilidades en Software

Contexto general

Una organización ha identificado riesgos de seguridad en una de sus aplicaciones web o APIs, derivados de prácticas inseguras de diseño, implementación y configuración. Dichas vulnerabilidades pueden comprometer la confidencialidad, integridad y disponibilidad de la información, así como la confianza de los usuarios y la responsabilidad legal de la empresa.

El equipo de ingeniería de software ha sido asignado para **analizar el sistema, identificar vulnerabilidades, relacionarlas con estándares de seguridad reconocidos y proponer soluciones técnicas que mitiguen el riesgo**, documentando todo el proceso y justificando cada decisión desde una perspectiva técnica, normativa y ética.

El proyecto debe reflejar un escenario realista de desarrollo de software seguro, integrando análisis de código, estándares OWASP, refactorización y argumentación técnica, alineados con las competencias **SABER – HACER – SER** del curso.

Enfoque del proyecto

El proyecto se desarrolla desde un enfoque **aplicado e integrador**, donde el estudiante asume el rol de **ingeniero de software responsable de la seguridad del sistema**, evidenciando:

- Comprensión del riesgo asociado a vulnerabilidades de software.
- Capacidad de relacionar prácticas inseguras con estándares OWASP.
- Propuesta y aplicación de mecanismos de mitigación.
- Reflexión ética sobre el impacto de un desarrollo inseguro.

Actividades obligatorias del proyecto

Cada equipo deberá desarrollar, como mínimo, las siguientes actividades:

1. **Selección del sistema vulnerable**
    - Aplicación web o API (propuesta por el equipo o suministrada como entorno de práctica).
    - Descripción general del sistema y su propósito.
2. **Identificación y caracterización de vulnerabilidades**
   Para cada vulnerabilidad analizada se debe documentar claramente:

   - Descripción de la vulnerabilidad.
   - Riesgo de seguridad asociado.
   - Categoría correspondiente del **OWASP Web Top 10 o OWASP API Security Top 10**.
   - Impacto potencial sobre el sistema y los usuarios.
3. **Análisis técnico y ético**
   - Análisis del origen de la vulnerabilidad (diseño, implementación o configuración).
   - Reflexión sobre la responsabilidad del ingeniero de software frente a dicha práctica insegura.
4. **Propuesta y aplicación de mitigación**
   - Refactorización de código o ajustes de configuración.
   - Aplicación de controles de seguridad (validación, autenticación, autorización, manejo de errores, etc.).
   - Justificación técnica de la solución adoptada.
5. **Validación de la solución**
   - Evidencia del antes y después de la mitigación.
   - Verificación de que la vulnerabilidad fue corregida o reducida.

Publicación y evidencia escrita del proceso (obligatoria)

Como parte fundamental del proyecto, **cada equipo deberá publicar el proceso de desarrollo y análisis** en **al menos una de las siguientes plataformas**:

- Repositorio **GitHub** (README técnico detallado).
- Artículo técnico en **Medium**.
- Blog técnico personal o institucional.
- Plataforma equivalente aprobada por el docente.

La publicación debe incluir:

- Contexto del problema.
- Vulnerabilidades analizadas.
- Riesgos OWASP asociados.
- Soluciones propuestas y aplicadas.
- Reflexión técnica y ética del equipo.

Esta actividad busca **fortalecer la competencia de escritura técnica, argumentación y comunicación profesional**, propia del ejercicio del ingeniero de software.

Seguimiento del proyecto – Revisión intermedia

- **Semana 9**: revisión parcial del proyecto.
- Cada equipo deberá evidenciar:

  - Vulnerabilidad seleccionada.
  - Riesgo OWASP relacionado.
  - Propuesta inicial de mitigación.
- La revisión tiene carácter **formativo** y orienta el desarrollo del proyecto final.

Trabajo colaborativo

- Equipos de **máximo 4 estudiantes**.
- Se debe evidenciar claramente el **trabajo en equipo**, tanto en:
  - Repositorio / publicación.
  - Desarrollo del proyecto.
  - Sustentación final.
- Cada integrante debe tener una responsabilidad claramente definida y defendible.

Sustentación final

- Sustentación **oral y técnica** del proyecto.
- **Duración máxima: 20 minutos por equipo**.
- Todos los integrantes deben participar activamente.
- Cada estudiante debe demostrar dominio del problema, la solución y las decisiones tomadas.

Evaluación

El proyecto será evaluado mediante la **rúbrica institucional del curso**, alineada con la **Taxonomía SOLO** y las competencias **SABER – HACER – SER**.

Distribución general de la calificación:

- **Entrega del proyecto (documentación, código y publicación): 37,5 %**
- **Sustentación y justificación técnica: 62,5 %**

Enfoque de la evaluación

La evaluación prioriza:

- La comprensión del problema de seguridad.
- La correcta relación vulnerabilidad – riesgo – estándar OWASP – mitigación.
- La justificación técnica y ética de las decisiones adoptadas.
- La coherencia entre análisis, solución implementada y defensa oral.
- La capacidad de comunicar técnicamente el proceso, tanto de forma escrita como oral.