Atalanta

Módulo 4

07/01/2026

Ejercicio 1

Realizar un análisis sobre el proyecto Pygoat (https://github.com/adeyosemanputra/pygoat) con Bandit y remediar de 3 a 5 (3 obligatorias, 2 opcionales) vulnerabilidades de entre los siguientes CWEs

- CWE-502, CWE-78, CWE-20, 400, CWE-259, CWE-330, CWE-327.
- Buscar información sobre cada vulnerabilidad y su remediación (revisar la documentación que ofrece Bandit)
- Mapear con OWASP Top 10 e investigar el CWE al que pertenece.

Ejercicio 2

Realizar una integración con el mismo proyecto Pygoat en un pipeline de Jenkins, en el cual haya que integrar:

- Un stage para análisis SAST con la herramienta Bandit.
- Un stage para análisis SCA con la herramienta Dependency-Track.
- Un stage para análisis de secretos con gitleaks.
- Integrarlo todo con DefectDojo (tenéis libertad para modelar con sus respectivos productos y engagements).
- Especificar security gates para vulnerabilidades críticas y/o altas en bandit y Dependency-Track.
- Aplicar el hook precommit sobre git en local de gitleaks (opcional).

Ejercicio 3

Realizar una actividad de threat modeling mediante la herramienta Threat Dragon (opcional Microsoft Threat Modeling Tool/Iriusk Risk community version) en el cual aparezca la siguiente arquitectura:

- Aplicación de banco que realiza las siguientes funcionalidades:
  - Autenticación
  - Cobro
  - Gestión externa
- 3 tipos de actores:
  - Usuario anónimo
  - Usuario autenticado
  - Administrador
- Frontend, backend, base de datos y proxy asíncrono hacia otro sistema de terceros.

Ejercicio 3

Sobre la actividad anterior, identificar lo siguiente:

- 3 (1 como opcional) amenazas que mapeen con CIA.
- 3 (1 como opcional) amenazas que mapeen con STRIDE.
- 4 (1 como opcional) contramedidas para cualquiera de las amenazas.

Explicar en la documentación las amenazas elegidas y sus contramedidas.

Ejercicio 4 - Opcional

Realizar una integración terragoat (https://github.com/bridgecrewio/terragoat) con Terrascan en un pipeline de Jenkins en el cual se remedien 2 vulnerabilidades y se explique los detalles de porqué se produce la vulnerabilidad y como se remedia. (Opcional)

Notas

- Incluir evidencias con capturas, código del pipeline y de los proyectos (pygoat y terragoat, con las vulnerabilidades ya remediadas) y memoria con la explicación de los ejercicios propuestos.
- La puntuación necesaria para aprobar es del **70%.**
- **La fecha límite de entrega será el 4 de febrero a las 23:59.**
- El formato de entrega será un zip que contenga todos los archivos requeridos y la memoria en formato PDF.
- Nombre del archivo: número de CI_Nombre del alumno.zip
- La entrega de notas será la semana del 2-6 de marzo.
- Se habilitará un espacio en el foro para dudas sobre el enunciado o problemas técnicos, pero no se permitirán preguntas sobre la resolución del propio ejercicio.


Atalanta