



## EVALUACIÓN DEL CURSO INTRODUCCIÓN A LA PROGRAMACIÓN SEGURA

### Objetivo

El objetivo de esta evaluación es que los alumnos demuestren su comprensión y aplicación de metodologías de desarrollo seguro y buenas prácticas de programación, así como su capacidad para identificar y abordar vulnerabilidades de seguridad en el código fuente proporcionado. Los alumnos deberán aplicar sus conocimientos en integridad, confidencialidad y disponibilidad de datos para analizar el código fuente en Python, identificar posibles problemas de seguridad y proponer soluciones adecuadas.

### Instrucciones

#### 1. Entrega del Código Fuente:

- Descargue el directorio Evaluación Final del repositorio del curso.
- En el directorio descargado encontrara un archivo llamado ejercicio\_prueba.py
- Este archivo contendrá el código fuente que deben analizar en busca de posibles problemas de seguridad.

#### 2. Análisis del Código:

- Los equipos deben revisar el código proporcionado en busca de posibles vulnerabilidades de seguridad.
- Se espera que apliquen sus conocimientos en metodologías de desarrollo seguro y buenas prácticas de programación para identificar posibles problemas en cuanto a integridad, confidencialidad y disponibilidad de datos.

#### 3. Elaboración del Informe:

- Los equipos deberán redactar un informe que contenga los siguientes elementos:

- i. Un análisis detallado del código fuente proporcionado, destacando las vulnerabilidades de seguridad identificadas:
  - Los equipos deben proporcionar un análisis exhaustivo del código fuente proporcionado, destacando cualquier vulnerabilidad de seguridad identificada. Esto incluirá la identificación de áreas problemáticas en el código que puedan afectar la integridad, confidencialidad o disponibilidad de datos.
- ii. Una descripción de las prácticas inseguras y las posibles consecuencias para la integridad, confidencialidad y disponibilidad de datos:
  - Deben describir claramente las prácticas inseguras presentes en el código y explicar cómo estas pueden comprometer la seguridad de la aplicación. Esto implica identificar las posibles consecuencias para la integridad, confidencialidad y disponibilidad de datos si las vulnerabilidades no se abordan adecuadamente.
- iii. Propuestas claras y fundamentadas para corregir las vulnerabilidades identificadas, aplicando metodologías de desarrollo seguro y buenas prácticas de programación:
  - Los equipos deben proponer soluciones concretas y fundamentadas para corregir las vulnerabilidades identificadas en el código. Estas propuestas deben aplicar metodologías de desarrollo seguro y buenas prácticas de programación, y explicar cómo abordan específicamente cada uno de los problemas de seguridad identificados.
- iv. Justificación de las soluciones propuestas, incluyendo cómo abordan cada uno de los problemas de seguridad identificados:
  - Deben justificar por qué las soluciones propuestas son adecuadas para abordar las vulnerabilidades identificadas. Esto puede incluir explicaciones sobre cómo las soluciones mitigarán los riesgos de seguridad y mejorarán la integridad, confidencialidad y disponibilidad de los datos.
- v. Reflexión sobre el proceso de evaluación de scripts y la importancia de la seguridad en el desarrollo de software:
  - Finalmente, los equipos deben reflexionar sobre el proceso de evaluación de scripts y la importancia de la seguridad en el desarrollo de software. Deben considerar cómo esta experiencia ha mejorado su comprensión de

la programación segura y cómo aplicarán estos conocimientos en el futuro.

**4. Formato del Informe:**

- a. El informe debe presentarse en formato digital.
- b. El informe debe presentarse en formato Microsoft Word o PDF.
- c. Debe incluir una portada con el nombre de los integrantes del equipo, el título de la evaluación, nombre de la asignatura, código de la sección y la fecha de entrega.

**5. Plazo de Entrega:**

- a. El plazo máximo de entrega corresponde al domingo 30 de abril a las 23:59 horas.

**6. Medio de entrega:**

- a. La entrega debe ser realizada a través correo electrónico a la casilla del docente [ruben.valencia05@inacapmail.cl](mailto:ruben.valencia05@inacapmail.cl) indicando en el asunto “evaluación final introducción a la programación segura”.

**Entregables**

Informe de aplicación de prácticas de seguridad en scripts.

**Instrumento de Evaluación**

En el directorio descargado encontrara un archivo llamado “Rubrica Evaluación.xlsx” correspondiente a la rúbrica de la evaluación del curso.