Benyahir Y. Martínez Hermina R00624824 12/noviembre/2025

Asignación 3 - Validación y Corrección de Código Inseguro

Parte A — Detección (8 pts)

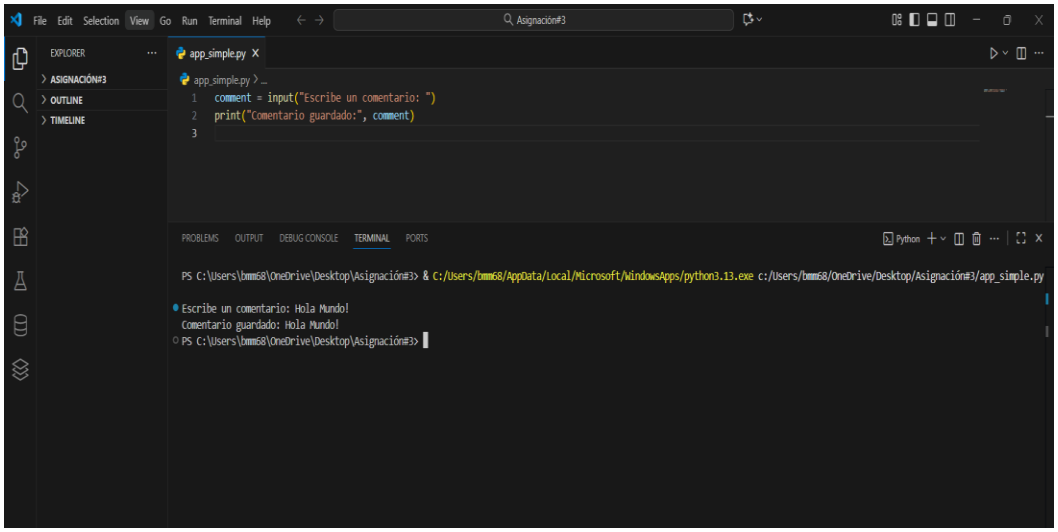
1. Lee el código y responde:
   a) ¿Por qué es inseguro aceptar cualquier texto sin validación?

   Porque esto le permite a un atacante introducir código o datos maliciosos que la aplicación procesará y potencialmente ejecutará sin control. También puede permitir accesos no autorizados o la manipulación de los datos del sistema, afectando la integridad y privacidad.

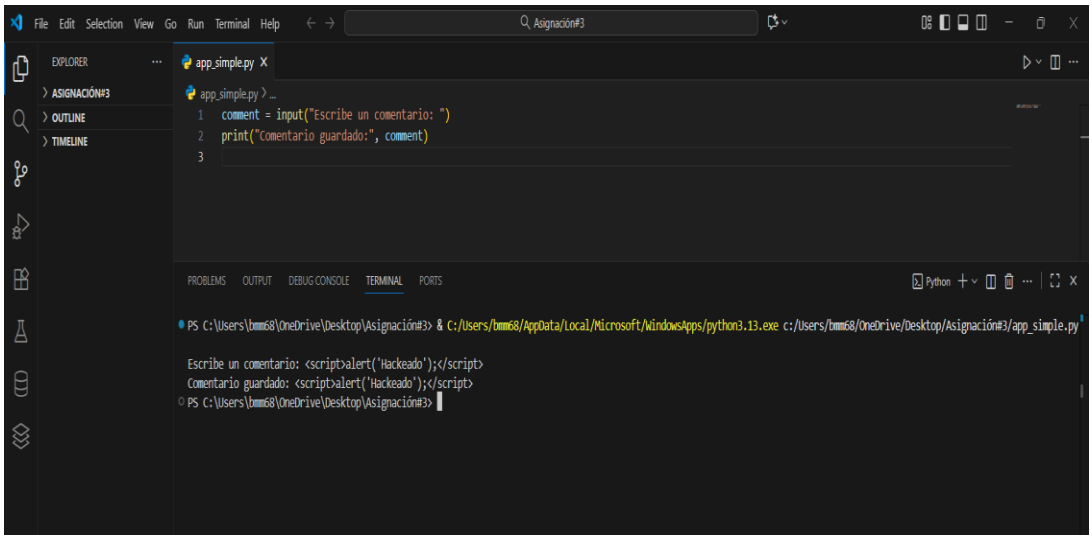
   b) ¿Qué tipo de ataque podría aprovechar esto?

   El ataque critico que se beneficia de esta vulnerabilidad es la inyección de código (Code injection). Donde un atacante inserta comandos o código malicioso por una entrada que la aplicación no valido antes de procesarla.

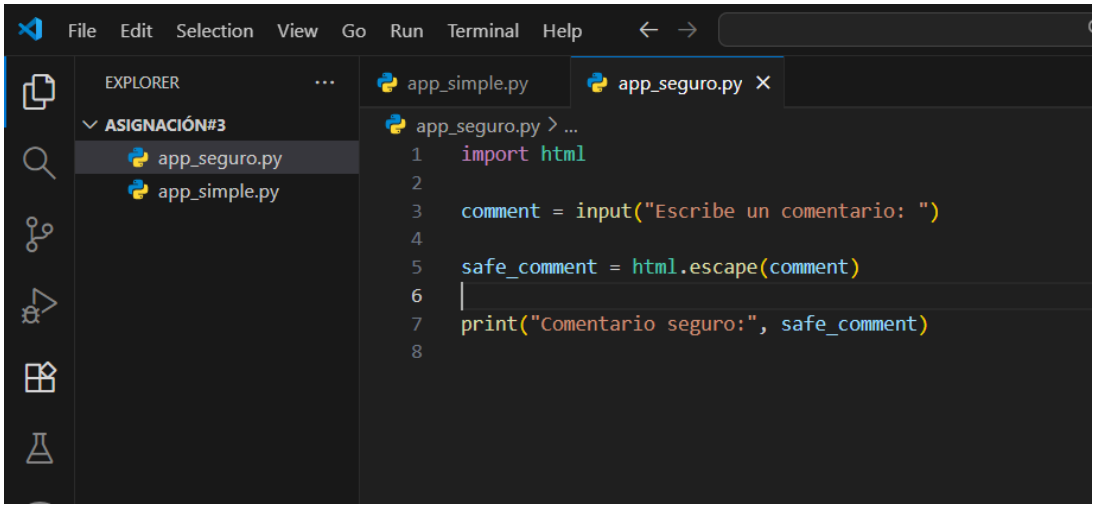
2. Ejecuta el programa y prueba introducir:
   - Texto normal (ejemplo: *Hola mundo*).



- Texto con etiquetas HTML o comandos sospechosos (ejemplo: <script>)

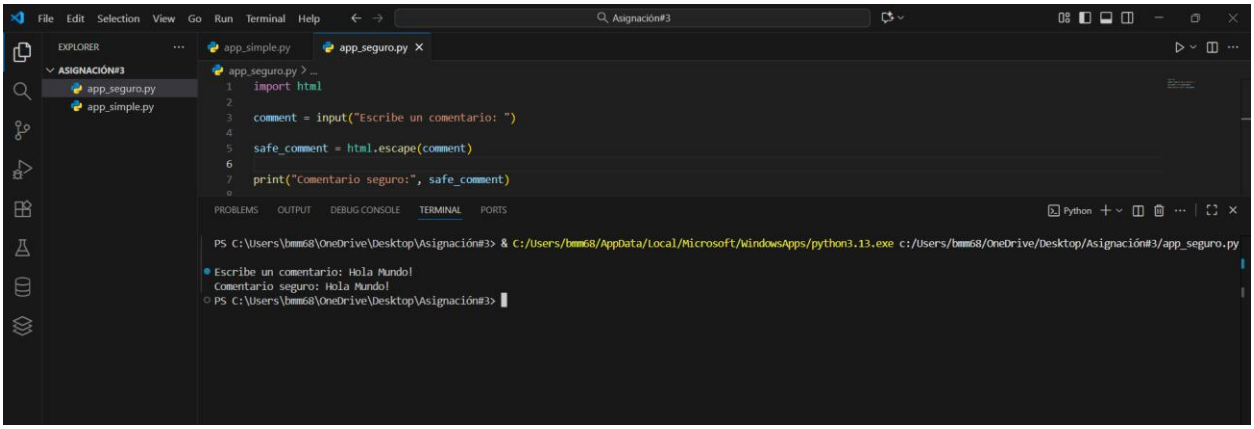


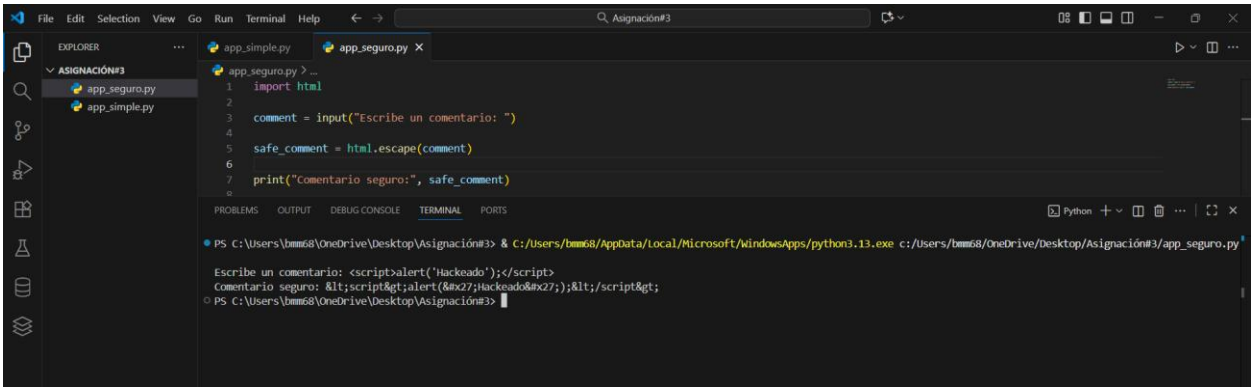
Parte B — Corrección (10 pts)



- En Python la función de html.escape() es la de convertir caracteres especiales de una cadena de texto hacia equivalentes en entidades HTML. Tiene como propósito prevenir vulnerabilidades de seguridad y asegurar que el texto se muestre de manera correcta en un navegador web.

Parte C — Verificación (5 pts)





Preguntas Teóricas (2 pts)

1. ¿Qué principio de la seguridad del software se está aplicando al validar la entrada del usuario?

   El principio que se esta utilizando es el de la validación robusta de entradas. En donde el programa limpia y verifica los datos que se están entrando para evitar datos maliciosos antes de procesarlo.

2. ¿Qué impacto tendría no sanitizar los datos en la Confidencialidad y la Integridad del sistema?

   El impacto en la Confidencialidad se podría notar por parte que podrían ocurrir fugas de datos, permitiendo la extracción o monitoreo de información personal, credenciales y datos almacenados. Cuanto a la Integridad del sistema se puede ver afectado por atacantes que pueden inyectar código que altere el funcionamiento normal de la aplicación, manipule registros o bases de datos.