EVALUACIÓN SUMATIVA 4 - UNIDAD 4 - 30%

Informe de aplicación de prácticas de seguridad en scripts

SEDE	**VALPARAÍSO**		**FECHA:**
ÁREA	**INFORMÁTICA Y TELECOMUNICACIONES**		**PUNTAJE TOTAL: 40 puntos**
ASIGNATURA	**Introducción a la Programación Segura**		**Duración:**
SECCIÓN	**TI3011/D**		**NOTA:**
DOCENTE	**Francisco Jara Bernal**	**EXIGENCIA: 60%**	
ALUMNOS			

INSTRUCCIONES GENERALES

Lea cuidadosamente estas instrucciones antes de realizar el informe:

- La nota 4,0 se obtiene logrando 24 puntos.
- Preocúpese de la redacción, ortografía y legibilidad de sus respuestas. Se penalizará en puntaje el no cumplimiento de lo anterior.
- El nombre del archivo debe ser ES4-IAPS-SusApellidos.docx o ES4-IAPS-SusApellidos.pdf
- Los criterios de evaluación son los siguientes: Explica las metodologías de desarrollo seguro SAMM, de acuerdo con la integridad, confidencialidad y disponibilidad. Explica metodología de desarrollo seguro SDL, de acuerdo con de acuerdo con la integridad, confidencialidad y disponibilidad. Distingue buenas prácticas de desarrollo seguro, considerando la sanitización de variables, estructuras de datos, anonimización y seudonimización. Evalúa script de desarrollo seguro, considerando las metodologías SDL, SAMM y las librerías Python de repositorios oficiales.
- El medio de envío de esta Evaluación es solamente el Ambiente de Aprendizaje de Inacap (AAI) y dentro del plazo establecido. NO se recibirán ni calificarán archivos fuera de plazo ni vía mail u por otro medio.
- Ante plagio y/o copia, será calificado con la nota mínima.
- El docente se reserva el derecho de interrogación sobre cualquier aspecto del informe presentado, en caso de dudas sobre la autoría.

INSTRUCCIONES

1. **Entrega del Código Fuente:**
   a. Descargue desde el Ambiente de Aprendizaje de Inacap (AAI) el archivo llamado Código Informe Evaluación 4 (30%): ejercicio_prueba.py
   b. Este archivo contendrá el código fuente que deben analizar en busca de posibles problemas de seguridad.

2. **Análisis del Código:**
   a. El docente en el rol de cliente hará una demostración del código en funcionamiento, Usted y su equipo bajo el rol de equipo de asesores informáticos deben permanecer en silencio y tomar nota de los evidentes problemas de seguridad al momento de ejecutar el código.
   b. Los equipos deben revisar el código proporcionado en busca de posibles vulnerabilidades de seguridad.
   c. 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, de acuerdo con el material de estudio aportado en el AAI.

3. **Elaboración del Informe:**
   Los equipos deberán redactar un informe que contenga los siguientes elementos:
   a. **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.

   b. **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.

   c. **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.

d. **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.

e. **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 y la fecha de entrega.
d. Debe contar con un apartado de Bibliografía, indicando claramente y en formato APA las fuentes consultadas y utilizadas en el desarrollo del informe.

5. Plazo de Entrega:

a. El plazo de entrega corresponde a la **fecha indicada en el Ambiente de Aprendizaje de Inacap (AAI)** para la Evaluación Sumativa 4 (30%).

6. Medio de entrega:

a. La entrega debe ser realizada a través del Ambiente de Aprendizaje de Inacap (AAI) por uno de los integrantes del grupo en el acceso que se indicará. Solamente se aceptarán entregas realizadas dentro del plazo y por este medio. Debe tener en cuenta que el no presentarse a clases el día de la entrega del Informe, queda ausente a una evaluación y con la nota mínima, debiendo justificar vía Intranet de alumno en el Módulo de solicitudes académicas, ingresando la Solicitud de justificación de inasistencia a una evaluación, con el documento de respaldo correspondiente.
b. Los documentos que debe considerar para la carga en AAI es el entregable Informe.

ESCALA DE NOTAS

Puntaje	Nota	Puntaje	Nota	Puntaje	Nota	Puntaje	Nota	Puntaje	Nota
0.0	1.0	10.0	2.3	20.0	3.5	30.0	5.1	40.0	7.0
1.0	1.1	11.0	2.4	21.0	3.6	31.0	5.3		
2.0	1.3	12.0	2.5	22.0	3.8	32.0	5.5		
3.0	1.4	13.0	2.6	23.0	3.9	33.0	5.7		
4.0	1.5	14.0	2.8	24.0	4.0	34.0	5.9		
5.0	1.6	15.0	2.9	25.0	4.2	35.0	6.1		
6.0	1.8	16.0	3.0	26.0	4.4	36.0	6.3		
7.0	1.9	17.0	3.1	27.0	4.6	37.0	6.4		
8.0	2.0	18.0	3.3	28.0	4.8	38.0	6.6		
9.0	2.1	19.0	3.4	29.0	4.9	39.0	6.8		

PAUTA DE CORRECCIÓN

Criterio de Evaluación	Destacado (5 puntos)	Habilitado (4 puntos)	En Desarrollo (3 puntos)	No logrado (2 puntos)	No presente (1 puntos)	Puntaje Obtenido
Explica la metodología de desarrollo seguro SAMM, de acuerdo con la integridad, confidencialidad y disponibilidad.	El estudiante ofrece una explicación clara y detallada de la metodología SAMM, destacando cómo abordan la integridad, confidencialidad y disponibilidad de los datos.	El estudiante proporciona una explicación adecuada de la metodología SAMM y su relación con la integridad, confidencialidad y disponibilidad, aunque podría haber más profundidad en algunos aspectos.	El estudiante presenta una explicación básica de la metodología SAMM y su relación con la integridad, confidencialidad y disponibilidad, pero con algunas omisiones o imprecisiones.	La explicación de la metodología SAMM y su relación con la integridad, confidencialidad y disponibilidad es limitada o confusa, mostrando falta de comprensión.	No se proporciona ninguna explicación sobre la metodología SAMM.	
	La explicación incluye ejemplos concretos que ilustran cómo la metodología SAMM pueden mejorar la integridad, confidencialidad y disponibilidad de los datos.	La explicación demuestra comprensión de la metodología SAMM, pero carece de ejemplos específicos para respaldar las afirmaciones.	La explicación menciona la metodología SAMM de manera general, sin proporcionar ejemplos concretos o aplicaciones prácticas.	La explicación carece de ejemplos y detalles específicos sobre cómo la metodología SAMM se relacionan con la integridad, confidencialidad y disponibilidad de los datos.	La explicación no menciona la metodología SAMM ni su relación con la seguridad de los datos.	
Explica la metodología de desarrollo seguro SDL, de acuerdo con la integridad, confidencialidad y disponibilidad.	El estudiante ofrece una explicación completa y precisa de la metodología SDL, mostrando cómo se relaciona con la integridad, confidencialidad y disponibilidad de los datos.	El estudiante proporciona una explicación sólida de la metodología SDL y su relación con la integridad, confidencialidad y disponibilidad, aunque podría haber más detalle en algunos aspectos.	El estudiante presenta una explicación básica de la metodología SDL y su relación con la integridad, confidencialidad y disponibilidad, con algunas carencias o imprecisiones.	La explicación de la metodología SDL y su relación con la integridad, confidencialidad y disponibilidad es superficial o incorrecta, mostrando falta de comprensión.	No se proporciona ninguna explicación sobre la metodología SDL.	
	La explicación destaca cómo la metodología SDL puede mitigar riesgos de seguridad específicos y mejorar la integridad, confidencialidad y disponibilidad de los datos en el desarrollo de software.	La explicación demuestra comprensión de la metodología SDL, pero no ofrece ejemplos o aplicaciones prácticas que ilustren su impacto en la seguridad de los datos.	La explicación menciona la metodología SDL de manera general, sin proporcionar detalles específicos sobre cómo se relaciona con la seguridad de los datos.	La explicación carece de ejemplos y detalles específicos sobre la metodología SDL y su aplicación en el desarrollo seguro de software.	La explicación no menciona la metodología SDL ni su relación con la seguridad de los datos.	
Distingue buenas prácticas de desarrollo seguro, considerando la sanitización de variables, estructuras de datos, Anonimización y Seudonimización.	El estudiante demuestra una comprensión completa de las buenas prácticas de desarrollo seguro, distinguiendo claramente entre la sanitización de variables, estructuras de datos, anonimización y seudonimización.	El estudiante demuestra una comprensión sólida de las buenas prácticas de desarrollo seguro y es capaz de distinguir entre la sanitización de variables, estructuras de datos, anonimización y seudonimización, aunque podría haber algunas omisiones o imprecisiones.	El estudiante presenta una comprensión básica de las buenas prácticas de desarrollo seguro, identificando la sanitización de variables, estructuras de datos, anonimización y seudonimización, pero con algunas carencias o imprecisiones.	La distinción entre las buenas prácticas de desarrollo seguro es limitada o confusa, mostrando falta de comprensión.	No se proporciona ninguna distinción clara entre las buenas prácticas de desarrollo seguro.	
	El estudiante ofrece ejemplos concretos de cada una de las buenas prácticas mencionadas, ilustrando cómo se aplican en diferentes contextos de desarrollo de software.	El estudiante menciona las buenas prácticas de desarrollo seguro, pero no proporciona ejemplos específicos o aplicaciones prácticas que demuestren su comprensión.	El estudiante identifica las buenas prácticas de desarrollo seguro, pero no ofrece ejemplos ni detalles adicionales sobre cómo se aplican en el desarrollo de software.	La distinción entre las buenas prácticas de desarrollo seguro es limitada y carece de ejemplos o detalles específicos sobre su aplicación en el desarrollo de software.	El estudiante no menciona ni distingue las buenas prácticas de desarrollo seguro.	
Evalúa script de desarrollo seguro, considerando las metodologías SDL y SAMM y las librerías de Python de repositorios oficiales.	El estudiante realiza una evaluación exhaustiva del script de desarrollo seguro, aplicando correctamente las metodologías SDL y SAMM y utilizando librerías de Python de repositorios oficiales para mejorar la seguridad.	El estudiante realiza una evaluación sólida del script de desarrollo seguro, aplicando adecuadamente las metodologías SDL y SAMM y utilizando algunas librerías de Python de repositorios oficiales para mejorar la seguridad, aunque podría haber algunas áreas de mejora.	El estudiante realiza una evaluación básica del script de desarrollo seguro, aplicando parcialmente las metodologías SDL y SAMM y utilizando algunas librerías de Python de repositorios oficiales, con algunas carencias o imprecisiones.	La evaluación del script de desarrollo seguro es limitada o confusa, mostrando falta de comprensión en la aplicación de las metodologías y las librerías de Python.	No se proporciona ninguna evaluación del script de desarrollo seguro.	
	La evaluación identifica con precisión las vulnerabilidades de seguridad presentes en el script y propone soluciones claras y efectivas para abordarlas, utilizando metodologías de desarrollo seguro y librerías de Python de repositorios oficiales.	La evaluación identifica adecuadamente algunas vulnerabilidades de seguridad en el script y propone soluciones para abordarlas, aunque podría haber más detalles o justificación en algunas áreas.	La evaluación identifica algunas vulnerabilidades de seguridad en el script y propone soluciones básicas para abordarlas, con algunas carencias o imprecisiones en la aplicación de metodologías de desarrollo seguro y librerías de Python.	La evaluación de seguridad es superficial o incorrecta, mostrando falta de comprensión en la identificación y mitigación de vulnerabilidades en el script.	No se proporciona ninguna evaluación del script de desarrollo seguro.	
					NOTA	**0,0**