

**CURSO** : 2414 – Seguridad de Aplicaciones  
**PROFESOR** : Wilman Vasquez  
**SEMESTRE** : 2026  
**CICLO** : Quinto  
**SECCIÓN** : T5HO  
**GRUPO** : 01  
**FECHA** : 29 de enero de 2026  
**DURACIÓN** : 60 minutos

NOTA

**ALUMNO (A)** :JOSE MONTERO VILCAS

### PRIMERA EVALUACIÓN T1

#### Logro

Tenga presente que el logro de esta evaluación, es que usted aplique de manera correcta y eficiente el manejo de las herramientas OWASP

#### Consideraciones generales:

- Tomar en cuenta de realizar la evaluación con orden, limpieza y claridad en las respuestas.
- Capturar pantalla completa para evidenciar el sustento de su respuesta.

#### Consolidado

Pregunta	Puntaje		Llenar solo en caso de Recalificación justificada	
	Máximo	Obtenido	Sustento	Puntaje
1	07			
2	07			
3	06			
Nota Recalificada				

### Pregunta 01

La empresa “**TecnoSmart**”, dedicada a la venta online de equipos electrónicos (celulares, laptops y accesorios), desea implementar una tienda virtual con pasarela de pagos para atender pedidos a nivel nacional. Debido al manejo de información sensible de clientes y transacciones económicas, la empresa solicita identificar mecanismos de defensa para proteger su plataforma.

Rúbrica				
Puntos	Excelente: 7 puntos	Bueno: 5 puntos	Regular: 3 puntos	Deficiente: 0 puntos
7 puntos	Nombra 3 mecanismos y logra justificar correctamente.	Nombra 2 mecanismos, Justificando correctamente	Nombra 1 mecanismo, Justificando correctamente	No nombra ningún mecanismo

- **WAF (Web Application Firewall):** Este es el componente más crítico para una tienda virtual. A diferencia de un firewall de red, el WAF filtra el contenido específico de las aplicaciones web. Es capaz de bloquear ataques como SQL Injection, XSS (Cross Site Scripting) y Denegación de Servicio (DoS), protegiendo así la pasarela de pagos y los datos de los clientes,.
- **DMZ (Zona Desmilitarizada):** Se debe ubicar el servidor web de la tienda en una DMZ. Esto lo sitúa entre la red interna y la externa (Internet), aislando los servicios públicos para que, si son comprometidos, no expongan la red interna de la empresa.
- **Firewall de Red: Actúa como la primera línea** de defensa estableciendo una barrera entre redes seguras y no seguras, controlando el tráfico basado en puertos y protocolos,.
- **IDS/IPS (Sistemas de Detección/Prevención de Intrusos):** Implementar estos sistemas permite generar alertas anticipadas y prevenir accesos no autorizados mediante análisis de firmas y comportamiento.
- **Protección de Datos en Tránsito (HTTPS/TLS):** Para la información sensible (tarjetas, datos personales), es obligatorio usar TLS en todas partes. No se deben mezclar contenidos cifrados y no cifrados, y se debe utilizar la bandera de cookie "segura" para evitar el robo de sesiones y la exposición de datos

### Pregunta 02

OWASP A1: La empresa “SaludPlus Online”, dedicada a la gestión de citas médicas y venta de productos farmacéuticos vía web, utiliza un servidor de pruebas basado en DVWA (Damn Vulnerable Web Application) para evaluar la seguridad de su plataforma antes de pasarla a producción. Durante la auditoría de seguridad se detecta una vulnerabilidad relacionada con OWASP A1: Inyección SQL, específicamente en el módulo SQL Injection Blind, configurado con nivel de seguridad medio.

Evidenciar con capturas de pantalla completa del procedimiento

Rúbrica				
Puntos	Excelente: 7 puntos	Bueno: 4 puntos	Regular: 2 puntos	Deficiente: 0 punto
7 puntos	Evidencia el nombre de la base de datos, el usuario conectado y brinda medidas de seguridad	Evidencia el nombre de la base de datos y/o usuario conectado al servidor	Logra determinar cuál es el parámetro vulnerable	No logra implementar el servidor

### Pregunta 03

OWASP A3: La empresa “NovaMarket”, dedicada a la venta de productos al por menor vía web, cuenta con un portal informativo y de compras en línea accesible a través de una página web cuyo nombre inicia con la letra “R”, correspondiente al apellido paterno del evaluador. Durante el análisis de seguridad, se identifica que el sitio opera únicamente bajo el protocolo HTTP, el cual corresponde a una capa de transporte insegura, ya que no implementa mecanismos de cifrado.

<b>Rúbrica</b>				
<b>Puntos</b>	<b>Excelente: 6 puntos</b>	<b>Bueno: 4 puntos</b>	<b>Regular: 3 puntos</b>	<b>Deficiente: 0 punto</b>
<b>6 puntos</b>	<b>Logra encontrar la página web, evidencia de la información sensible y brinda 3 mejoras de seguridad</b>	<b>Logra encontrar la página web y evidencia la información sensible</b>	<b>Logra encontrar la página web</b>	<b>No entrega nada</b>