

Simulacro de Examen - Puesta en Producción Segura

**Selecciona la opción correcta para cada una de las siguientes preguntas. Solo hay una respuesta válida por pregunta.**

1. **¿Qué es un IDE en programación?**

A) Editor de texto simple

B) Compilador

C) Entorno de Desarrollo Integrado

D) Navegador web

1. **¿Cuál es una ventaja de los lenguajes interpretados?**

A) Menor seguridad

B) Multiplataforma

C) Mayor rendimiento

D) Necesidad de compilador

1. **¿Qué tipo de prueba se enfoca en validar bloques de código individuales?**

A) Pruebas Funcionales

B) Pruebas de Carga

C) Pruebas Unitarias

D) Pruebas de Integración

1. **¿Para qué se utiliza un sandbox en programación?**

A) Mejorar la velocidad de red

B) Aislar procesos

C) Gestionar usuarios

D) Crear interfaces gráficas

1. **¿Qué desventaja tienen los lenguajes interpretados frente a los compilados?**

A) Mayor seguridad

B) Menor velocidad

C) Requieren hardware específico

D) Mayor complejidad

1. **¿Cuál es el propósito del modelado de amenazas?**

A) Mejorar la interfaz de usuario

B) Aumentar el rendimiento

C) Identificar riesgos

D) Probar la conexión a la red

1. **¿Qué herramienta se usa para pruebas de penetración?**

A) TeamViewer

B) Metasploit

C) Photoshop

D) Wireshark

1. **¿Qué tipo de prueba simula el comportamiento de un atacante?**

A) Pruebas Unitarias

B) Pruebas de Carga

C) Pentesting

D) Pruebas Funcionales

1. **¿Qué es el STRIDE en ciberseguridad?**

A) Herramienta de análisis de red

B) Lenguaje de programación

C) Metodología de modelado de amenazas

D) Protocolo de comunicación

1. **¿Qué vulnerabilidad se produce al no validar correctamente los datos de entrada?**

A) Pérdida de autenticación

B) Exposición de datos sensibles

C) Inyección

D) Cross-site Scripting (XSS)

1. **¿Qué significa ASVS en seguridad de aplicaciones?**

A) Advanced Security Verification Standard

B) Application Standard Verification

C) Application Security Verification Standard

D) Automatic Security Validation

1. **¿Qué herramienta se sugiere para análisis de dependencias en ASVS?**

A) Burp Suite

B) Nessus

C) Snyk

D) Wireshark

1. **¿Qué nivel de ASVS se recomienda para aplicaciones con transacciones B2B?**

A) Oportunista

B) Avanzado

C) Mínimo

D) Standard

1. **¿Qué framework se utiliza para pruebas de seguridad en aplicaciones web?**

A) ASVS

B) SAST

C) WSTG

D) OWASP

1. **¿Qué acción ayuda a evitar ataques de XSS en WSTG?**

A) Desactivar el firewall

B) Uso de HTTP plano

C) Habilitar JavaScript automático

D) Codificación de caracteres especiales

1. **¿Qué es una inyección SQL?**

A) Un tipo de firewall

B) Herramienta de análisis de red

C) Vulnerabilidad que permite ejecutar comandos en la base de datos

D) Protocolo de autenticación

1. **¿Qué contramedida ayuda a proteger contra ataques XSS?**

A) Usar contraseñas débiles

B) Permitir scripts sin validación

C) Desactivar la autenticación

D) Content Security Policy (CSP)

1. **¿Qué estándar de autenticación se basa en tokens?**

A) OAuth2

B) OpenID

C) JSON Web Token (JWT)

D) TLS

1. **¿Qué herramienta permite la integración continua en DevOps?**

A) Git

B) Docker

C) Jenkins

D) Ansible

1. **¿Qué significa DevSecOps?**

A) Automatizar tareas administrativas

B) Crear redes privadas virtuales

C) Integrar la seguridad en todas las etapas del pipeline

D) Optimizar la memoria del sistema

1. **¿Qué es un contenedor en DevOps?**

A) Un antivirus especializado

B) Una unidad estandarizada de software

C) Un tipo de firewall

D) Una herramienta de diseño gráfico

1. **¿Qué herramienta se utiliza para la monitorización en DevOps?**

A) Photoshop

B) ELK Stack

C) Illustrator

D) Windows Media Player

1. **¿Qué herramienta ayuda a automatizar la gestión de contenedores?**

A) Word

B) Kubernetes

C) Excel

D) PowerPoint

1. **¿Qué componente de Kubernetes almacena la configuración del clúster?**

A) kubelet

B) etcd

C) kube-proxy

D) Pod

# Caso Práctico: Seguridad en el despliegue de una nueva aplicación web

**La empresa TechSolutions va a lanzar una nueva aplicación web para la gestión de proyectos internos. El equipo de desarrollo ha usado DevOps con integración continua (CI/CD), empleando contenedores Docker y Kubernetes para el despliegue. Antes de salir a producción, se realiza un análisis de seguridad que revela riesgos de inyección SQL, falta de políticas CSP y ausencia de autenticación basada en tokens. Se recomienda aplicar medidas correctivas y configurar herramientas que aseguren la disponibilidad, integridad y confidencialidad del sistema.**

1. **¿Qué medida mitigaría el riesgo de inyección SQL?**

A) Desactivar el firewall

B) No validar entradas

C) Uso de consultas preparadas

D) Permitir comandos dinámicos

1. **¿Qué política se debe aplicar para evitar ataques XSS?**

A) Activar root en contenedores

B) Desactivar autenticación

C) Permitir JavaScript externo sin revisión

D) Implementar CSP

1. **¿Qué estándar de autenticación se recomienda para esta aplicación?**

A) OpenID

B) OAuth1

C) JSON Web Token (JWT)

D) Captcha

1. **¿Qué ventaja aporta Kubernetes en este despliegue?**

A) Editar gráficos vectoriales

B) Enviar correos automáticos

C) Orquestación de contenedores

D) Validación de formularios

1. **¿Qué herramienta permite integrar seguridad en el ciclo CI/CD?**

A) Wireshark

B) Metasploit

C) DevSecOps

D) Photoshop

1. **¿Qué tipo de prueba es más útil en esta fase final?**

A) Carga

B) Unitaria

C) Funcional

D) Pentesting