

Preguntas de Desarrollo para el supuesto práctico (5 puntos por pregunta).

Desarrollo Supuesto práctico 1

En la auditoría de seguridad realizada en la Diputación de Pontevedra por la AMTEGA (Xunta de Galicia), se identificaron varias vulnerabilidades en sus sistemas. A continuación, se muestra una tabla con el nombre de las vulnerabilidades y el número de ocurrencias.

Nombre de vulnerabilidad	Activo	Número de ocurrencias
Múltiples vulnerabilidades Moodle	formacioncontinua.depo.es	8
Vulnerabilidad librería Moments.js	www.depo.gal	3
HTTP Parameter Pollution	formacioncontinua.depo.es	14
	boppo.depo.gal	
Múltiples vulnerabilidades JQuery	boppo.depo.gal	20
	revitaliza.depo.gal	
No configurado HTTP Strict Transport Security Policy	www.depo.gal	25
	ovt.depo.gal	
No soportado SSL/TLS Forward Secrecy Cipher Suites	www.depo.gal	6
	sede.depo.gal	
Política permisiva de HTTP Strict Transport Security Policy	boppo.depo.gal	6
	revitaliza.depo.gal	
Detectadas dependencias de paquetes	formacioncontinua.depo.es	1
Inyección HTML/CSS	revitaliza.depo.gal	3
Detectado configuración de fichero travis.yml	formacioncontinua.depo.es	1
Vulnerabilidad librería YUI	boppo.depo.gal	4
	revitaliza.depo.gal	
Versión Bootstrap vulnerable	revitaliza.depo.gal	8
	museo.depo.gal	
	boppo.depo.gal	
	www.depo.gal	

Indique las recomendaciones de seguridad que deben implementarse para mitigar estas vulnerabilidades. Estas vulnerabilidades hacen uso del protocolo HTTP/HTTPS, por lo que también explique el funcionamiento básico de este protocolo.

Desarrollo Supuesto práctico 2

Los usuarios de la Diputación de Pontevedra están informando de una lentitud extrema en el acceso a los ficheros ubicados en las unidades departamentales de los distintos servicios, indican que el problema solo ocurre al acceder a estos recursos en particular. En el sistema de monitorización también informa que uno de los servidores de ficheros está funcionando de forma extremadamente lenta desde una actualización reciente mediante las métricas de acceso al disco. El sistema operativo que ejecuta este servidor es un Windows Server 2022, el servidor cumple con los requisitos de hardware recomendados y el espacio en disco es suficiente. Se ha comprobado que el origen del problema es el servidor, y el funcionamiento de los pcs clientes y la red es correcto, por lo tanto:

- A. Detalla los pasos que seguirías para identificar si el problema proviene de la actualización del sistema operativo o de otra causa.
- B. Explica qué herramientas usarías para verificar el uso de CPU, memoria, disco y red en Windows Server 2022, y cómo interpretarías los resultados para detectar la causa del rendimiento lento.
- C. Describe una posible solución que incluya tanto la optimización del rendimiento como la implementación de medidas preventivas para evitar futuros problemas después de actualizaciones.