Apartado 1. (Puntuación: 2 puntos).

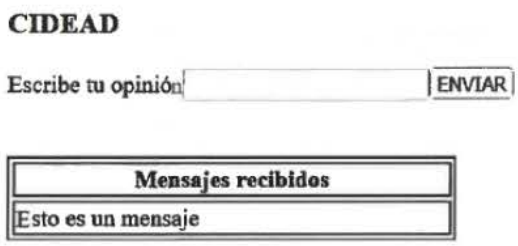
1.1. (1 pto). Rellena la siguiente tabla indicando la línea de comandos a ejecutar para realizar la tarea solicitada

Eliminar un contenedor de nombre **miexamen**	docker -rm -f miexamen
Ver los contenedores en ejecución	docker ps
Lanzar un contenedor con la imagen **alpine** pasándole la variable de entorno **STATUS** con el valor **open**	docker run -e STATUS=open alpine

1.2. (1 pto). Indica las diferencias entre el archivo *docker-compose.yml* y el archivo *Dockerfile.* Debes centrarte en para qué se utilizan, qué contenido tienen y los comandos de Docker que los utilizan

Apartado 2. (2 ptos)

Dada una aplicación web que tiene el siguiente formulario, responde a las siguientes preguntas:



2.1. (0.5 puntos). Si el formulario fuese vulnerable a inyección SQL, indica si esta vulnerabilidad se puede mitigar con CSP y justifica tu respuesta.

En resumen, para mitigar una vulnerabilidad de inyección SQL en un formulario, es necesario implementar medidas de seguridad en el lado del servidor, como la validación de entradas y el uso de consultas parametrizadas, y no depender de CSP, que es una política de seguridad del lado del cliente e nfocada principalmente en la prevención de XS

2.2. (0.5 puntos). Si el formulario fuese vulnerable a XSS indica si esta vulnerabilidad se puede mitigar con HSTS y justifica tu respuesta.

En resumen, HSTS mejora la seguridad de la conexión al forzar el uso de HTTPS, pero no tiene la capacidad de inspeccionar o bloquear código malicioso inyectado a través de una vulnerabilidad XSS en un formulario. Para mitigar el XSS, se deben implementar medidas específicas en el lado del servidor para procesar las entradas del usuario de forma s egura y considerar el uso de CSP en el lado del cliente para controlar los recursos permitidos en la página.

2.3. (0,5 puntos). Si el formulario fuese vulnerable a XSS indica si esta vulnerabilidad se puede mitigar con un CAPTCHA y justifica tu respuesta

En resumen, un CAPTCHA no aborda la vulnerabilidad fundamental que permite los ataques de XSS, que es la falta de un procesamiento seguro de las entradas del usuario en el servidor. Para mitigar el XSS, se deben implementar medidas de seguridad específicas en el lado del servidor y considerar el uso de CSP en el lado del cliente

2.4. (0,5 puntos). Si el formulario fuese vulnerable a inyección sql indica si esta vulnerabilidad se puede mitigar con un WAF y justifica tu respuesta.

un WAF analiza el contenido del tráfico web en el lado del servidor y puede bloquear activamente las solicitudes que contengan código SQL malicioso, proporcionando una mitigación directa contra la vulnerabilidad de inyección SQL

Apartado 3. (Puntuación: 6 puntos). Test.

Cada pregunta sólo tiene una única respuesta correcta. Una respuesta correcta se valorará positivamente con **0,30** puntos. Una respuesta incorrecta se valorará negativamente con **0,10** puntos. Una respuesta no contestada ni sumará ni restará puntos. **Contestar las respuestas en la siguiente tabla** (toda respuesta fuera de esta tabla no se tendrá en cuenta):

1.- En general, ¿qué ventaja tiene un lenguaje de programación compilado frente a uno interpretado?

a) Es más seguro
b) Es menos complejo de programar
c) Tiene un mayor rendimiento
d) Todos los anteriores

2.- A los entornos controlados, no influenciados por otras piezas de software o hardware y donde todos los programadores pueden tener las mismas condiciones, y por tanto, poder medir y probar el software de manera eficaz y eficiente se les conoce como

a) isolateenv
b) sandtrust
c) securebox
d) Ninguna de las anteriores

3.- El lenguaje Scala

a) No necesita un compilador
b) No necesita ser ejecutado en un entorno controlado o máquina virtual
c) Es un lenguaje intermedio
d) Todos los anteriores

4.- ¿Qué tipo de prueba verifica si el código introducido rompe o degrada la funcionalidad del software original?

a) Pruebas de integración
b) Pruebas de rendimiento
c) Pruebas de estrés
d) Ninguna de las anteriores

Regresión

5.- Las pruebas de seguridad que analizan el código fuente o binario de una aplicación en busca de vulnerabilidades potenciales sin ejecutar el programa son las

a) Pruebas de Análisis Dinámico
b) Pruebas de Penetración –
c) Pruebas unitarias
d) Pruebas de Análisis Estático

6.- Dada la siguiente línea de código

```
$query = "SELECT nombre_usuario FROM usuarios WHERE  clave=$clave ";
```

¿Qué debería contener la variable $clave para que la consulta devuelva registros?

a) ' OR '1'='1
b) 1 OR '1'='1'
c) 1' OR 1=1
d) 1 OR 1=1'

7.- ¿Cuál de las siguientes no es una vulnerabilidad del Top 10 de OWASP en entornos web?

a) Componentes Vulnerables y Obsoletos
b) Problemas de configuración a nivel de Seguridad
c) Fallos de Autenticación e Identificación
d) Protecciones binarias insuficientes

8.- El listado de controles generales en la versión 4.0.3 de ASVS no incluye

a) Archivos y recursos
b) Gestión de sesión
c) Comunicaciones
d) Plataforma móvil

9.- ¿Cuál de los siguientes no es un estándar de autenticación?

a) VCS
b) OAuth
c) Con certificados
d) Ninguno de los anteriores

10.- ¿Cuál de los siguientes es un ataque Server Side Inyection?

a) HTML Inyection
b) Session Hijacking
c) XSS
d) Ninguna de las anteriores

11.- La herramienta Frida

a) Se utiliza para ofuscar el código de una aplicación móvil
b) Protege las comunicaciones en aplicaciones móviles
c) Permite la manipulación y el análisis dinámico de aplicaciones móviles
d) Todas las anteriores

12.- La herramienta ProGuard

a) es una herramienta de optimización y ofuscación de código para aplicaciones Java y Android.
b) es una herramienta que permite realizar ingeniería inversa de aplicaciones móviles.
c) es una herramienta que permite realizar el tampering en aplicaciones Java y Android.
d) Ninguna de las anteriores.

13.- La herramienta que proporciona iOS para generar y almacenar de forma segura las claves usadas en los algoritmos de cifrado de la información, es

a) Keychain
b) Keystore
c) KeyTrust
d) Ninguna de las anteriores

14.- El proceso de compras a través de las aplicaciones móviles sigue determinados mecanismos de protección, entre los que se incluye

a) Criptografía y Firma Digital
b) GDPR
c) Autenticación UniFactor
d) Todos los anteriores

15.- Tanto en iOS como en Android

a) Todas las aplicaciones se ejecutan en su propio entorno aislado
b) Cada aplicación está funcionando con un usuario específico que se crea para ella
c) Cada aplicación tiene un directorio de inicio único para sus archivos, que se asigna aleatoriamente cuando se instala la aplicación
d) Todas las opciones son correctas

16.- Kubernetes es

a) Una plataforma de provisión y gestión de recursos de infraestructura en la nube, como servidores virtuales, redes, bases de datos y otros servicios.
b) Una plataforma de orquestación de repositorios de Git.
c) Una plataforma que proporciona una capa de abstracción sobre los recursos físicos, permitiendo la definición y gestión de la infraestructura como código
d) Ninguna de las anteriores

17.- ¿Cuál de las siguientes no es una herramienta para pruebas automatizadas de seguridad?

a) OWASP Zap
b) PHPUnit
c) Acunetix
d) Ninguna de las anteriores

18.- Ansible permite a los usuarios especificar cómo deberían estar configurados los sistemas y servicios, y luego aplicar esas configuraciones de manera consistente a través de todos los nodos del sistema. ¿Qué protocolo utiliza?

a) HTTPS
b) SSH
c) SMTP
d) IMAP

19.- Git

a) Es una plataforma basada en la web donde los usuarios pueden alojar repositorios
b) Permite clonar un repositorio
c) Permite realizar pruebas de sistemas de pago en aplicaciones móviles
d) Ninguna de las anteriores

20.- ¿Cuál de las siguientes es una herramienta de gestión automatizada de configuración de sistemas?

a) Puppet
b) Cypress
c) Cucumber
d) Todas las anteriores