Prepara tu examen de PPS

Introducción

Cada centro, cada año y cada docente, puede plantear al alumnado un modelo de examen concreto que, a su criterio, pueda servir como una correcta evaluación del módulo.

Para ayudar a preparar las evaluaciones, he pensado que podría ser de ayuda crear un archivo único para cada módulo, que pueda crecer cada año con el feedback y apoyo de la comunidad, con cuestionarios de todo tipo, con solucionario o solo los enunciados, pues la intención primera es poder ofrecer una idea de lo que podemos encontrarnos a la hora de una evaluación, poder aprender con ello, y no algo que una persona acabe memorizando, y esperando, sin comprender ni ahondar en la materia, que aparezca mágicamente en el examen.

Este documento, por tanto, no pretende ser una guía única y veraz de exámenes pasados o futuros, pero si una fuente de información sobre la que basar vuestros estudios.

Posibles modelos.

Modelo 1.

Ejemplo para preparación.

Apartado 1. (Puntuación: 2 puntos)

(1 pto) Indica la línea de comandos a ejecutar para **lanzar un contenedor de nombre mysql-db1** basado en la imagen del servidor de base de datos **mysql** (la imagen se llama mysql), mapeando el puerto 3306 del contenedor al puerto 33060 del equipo donde va a lanzar el contenedor y ejecutándose en segundo plano.

Dado el siguiente archivo

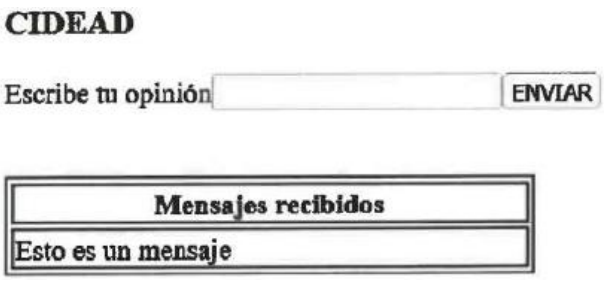
```
FROM ubuntu
#
EXPOSE 80
ADD ["index.html","/var/www/html/"]
ENTRYPOINT ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
```

(**0,5 ptos**) Indica cuál es el nombre habitual de este archivo en Docker y la línea de comandos que hay que ejecutar para crear una imagen de nombre **myapache** con este archivo.

(**0,5 ptos**) Indica qué hay que escribir en vez de **#** (línea 2 del archivo) para actualizar la lista de paquetes de Ubuntu e instalar el servidor web apache.

Apartado 2. Formulario vulnerable a XSS Stored (2 puntos)

Dada una aplicación web que tiene el siguiente formulario, que sabemos es vulnerable a **XSS stored**, responde a las siguientes preguntas:



(1 pto) Indica que debe escribir en la caja de texto para que cada vez que se cargue la página se muestre un mensaje con el contenido de las cookies.

(1 pto) Indica tres mejoras que podrías realizar para evitar esta vulnerabilidad y dónde se deben configurar/establecer cada una (en la parte servidora o en la parte cliente).

Apartado 3. Test (6 puntos)

1. **¿Cuál de las siguientes no es una vulnerabilidad del top 10 de OWASP en aplicaciones móviles?**

a) Almacenamiento de datos inseguro.
b) Controles de privacidad inadecuados.
c) Insuficiente validación de entrada/salida.
d) Falsificación de peticiones en el servidor.

2. **Para evaluar los lenguajes de programación en cuanto a su seguridad deberíamos valorar más que el propio lenguaje**

a) El sistema operativo en el que se utiliza.
b) El número de vulnerabilidades de software reportadas.
c) El ciclo de desarrollo de este dentro de un proyecto.
d) Ninguna de las anteriores.

3. **¿Cuál de las siguientes pruebas verifica que distintos módulos que funcionan por separado funcionen de manera conjunta?**

a) Pruebas funcionales.
b) Examen de la unidad.
c) Pruebas de aceptación.
d) Ninguna de las anteriores.

4. **¿Cuál de los siguientes no es un elemento habitual en el código fuente?**

a) Comentarios.
b) Comandos de procesamiento: importación de módulos/librerías.
c) Funciones.
d) Ninguna de las anteriores.

5. **Para prevenir que un formulario sea un vector de ataque es importante que**

a) En el navegador se valide higienice correctamente la entrada de datos para que los mismos no tengan que validarse en la parte servidora y así no sobrecargarla.
b) La interacción con la base de datos sea a través de sentencias no parametrizadas.
c) En el servidor se valide e higienice correctamente la entrada de datos, aunque también se hagan en el navegador.
d) Ninguna de las anteriores.

6. **¿Cuál de las siguientes no es una vulnerabilidad del top 10 de OWASP en entornos web?**

a) Componentes Vulnerables y Obsoletos.
b) Diseño inseguro.
c) Fallos de Autenticación e identificación.
d) Ingeniería inversa.

7. **Dada la siguiente línea de código**

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

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

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

8. **Una ventaja del software de fuentes abiertas es**

a) Incentiva la innovación colectiva.
b) Incrementa el coste.
c) Reduce la estabilidad.
d) Todas las anteriores.

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

a) JWT.
b) Oauth.
c) Con certificados.
d) Ninguno de los anteriores.

10. **El ASVS versión 4.0.3 define 3 niveles de Seguridad**

a) Nivel 1 (Opportunistic) - Nivel 2 (Secure) - Nivel 3 (Advanced).
b) Nivel 1 (Opportunistic) - Nivel 2 (Secure) - Nivel 3 (Sensible Data).
c) Nivel 1 (Normal) - Nivel 2 (Secure) - Nivel 3 (Advanced).
d) Ninguna de las anteriores.

11. **En Git hay tres etapas primarias (condiciones) en las cuales un archivo puede estar:**

a) Estado inicial - Estado chequeado - Estado aprobado.
b) Estado modificado - Estado preparado - Estado confirmado.
c) Estado inicial - Estado preparado - Estado aprobado.
d) Ninguna de las anteriores.

12. En iOS

a) Cada aplicación está funcionando con un usuario específico que se crea para esa aplicación.
b) Cada aplicación tiene un directorio de inicio único para sus archivos, que se asigna aleatoriamente cuando se instala la aplicación.
c) Todas las aplicaciones se ejecutan en un entorno compartido por todas.
d) Todas las anteriores.

13. ¿Cuál es el estándar que define un conjunto de orígenes pre-aprobados desde los que un navegador puede cargar recursos cuando un usuario visita un sitio web?

a) CSP.
b) SOAP.
c) HSTS.
d) Ninguno de los anteriores.

14. DevOps

a) Es un estándar que define las herramientas a utilizar por los desarrolladores.
b) Es un equipo o departamento de la organización compuesto por desarrolladores.
c) Es una metodología basada en la creación de software de forma continua y de mayor calidad mediante versiones más frecuentes.
d) Ninguna de las anteriores.

15. ¿Cuál de las siguientes no es una herramienta de gestión automatizada de configuración de sistemas?

a) Selenium.
b) Ansible.
c) Puppet.
d) Chef.

16. ¿Cuál de los siguientes lenguajes necesita un intérprete para ser ejecutado?

a) C.
b) C++.
c) Go o Golang.
d) Ruby.

17. ¿Cuál de las siguientes no es un principio básico de las metodologías AGILE?

a) Trabajo conjunto entre el cliente y desarrolladores.
b) Gran aceptación y respuesta al cambio de los requisitos definidos durante el proyecto.
c) Equipos auto-organizados.
d) Ninguna de las anteriores.

18. MDM

a) Es una solución que solo controla lo que sucede en la nube.
b) Se basan en la administración remota de los terminales corporativos de los empleados.
c) Son perfectos para los entornos BYOD.
d) Todas las anteriores.

19. En Android

a) Todas las aplicaciones se ejecutan en un entorno compartido por todas.
b) Todas las aplicaciones se ejecutan con el mismo usuario (“mobile”).
c) Existen dos niveles de acceso: accesos estándar o los más especiales o peligrosos.
d) Todas las anteriores.

20. El tampering consiste en

a) La manipulación no autorizada de aplicaciones móviles, lo que implica alterar el código binario o su entorno para afectar su comportamiento.
b) El proceso de analizar la aplicación compilada para extraer información sobre su código fuente.
c) Las Apps deben de estar firmadas por el desarrollador y si no lo están, sean rechazadas por la tienda y además el instalador del dispositivo no permitirá instalarla.
d) Ninguna de las anteriores.