

Examen para PPS03.

Intento 1.

Pregunta 1

¿Cuál es el TOP1 de OWASP?:

- a. Pérdida de control de acceso.
- b. Inyección.
- c. XSS.
- d. Denegación Servicio.

Pregunta 2

¿Cuál de los siguientes NO es un elemento clásico de un formulario?:

- a. Checkbox.
- b. Botón.
- c. Reconocimiento facial.
- d. Campo de texto.

Pregunta 3

Los WAFs son entorno de cloud. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 4

Podemos ayudar a la seguridad del software añadiendo contramedidas tanto a nivel de sistemas como de software adicional como CAPTCHAs. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 5

¿De qué lado se suele producir los ataques de robo de sesión?:

- a. De ninguno de los anteriores.
- b. Del lado del servidor.
- c. Del lado del aplicativo.
- d. Del lado del cliente.

Pregunta 6

Cuál de las siguientes se considera una fundación sin ánimo de lucro que ayuda en identificar riesgos y adoptar medidas al respecto:

- a. OWASP.
- b. OVBA.
- c. OSINT.
- d. VBSA.

Pregunta 7

¿Qué cambio suele ser habitual para configurar un WAF?:

- a. Cambiar el código fuente de nuestro aplicativo.
- b. Cambiar los CAPTCHAs.
- c. **Cambiar registros DNS.**
- d. Avisar al administrador de red.

Pregunta 8

Debemos de apoyarnos en la lista de OWASP para entender los riesgos que puede sufrir nuestro software. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 9

¿Qué tipo de ataques se considera de tipo Client Side Injection?:

- a. **Session Hijacking.**
- b. SQL Injection.
- c. SQL Transversal.
- d. Brute Forcing.

Pregunta 10

CSP es una contramedida para evitar ataques como los de inyección de código. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Intento 2.

Pregunta 1

Que es la autorización:

- a. Proceso de gestión de los derechos de una base de datos.
- b. Conjunto de instrucciones que se lleva a cabo durante el login del usuario.
- c. **Proceso de asignación de permisos que sucede después de la autenticación.**
- d. Proceso de logado de un usuario en un sistema.

Pregunta 2

OWASP ofrece un Top de riesgos para móviles y para web. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 3

Un formulario es una vía de entrada de datos al aplicativo web. ¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 4

El proceso de autenticación Basic Auth es ideal cuando:

- a. Cuando no se va a manejar datos sensibles o que tengan muchas restricciones de uso.
- b. Cuando no trabajamos ni con aplicativos REST o SOAP.
- c. Cuando trabajemos en distintas capas de seguridad.
- d. Cuando trabajamos con datos que son de carácter personal.

Pregunta 5

El objetivo de OWASP es:

- a. Evaluar software.
- b. Evaluar software y aplicaciones.
- c. Evaluar aplicaciones.
- d. Trabajar en mejorar la seguridad del software.

Pregunta 6

¿Qué necesita un WAF cuando lo instalamos?:

- a. Un tiempo para aprender sobre el aplicativo, los datos y usuarios.
- b. Cambios en el aplicativo
- c. Software específico.
- d. Un administrador de red y otro de seguridad.

Pregunta 7

¿Qué significa WAF?:

- a. Web Application Firewall.
- b. Wave App Firewall.
- c. Web Avanced Forwarder.
- d. Web Advanced Firewall.

Pregunta 8

¿Qué versión de OAuth es la más utilizada?:

- a. v6.
- b. v3.
- c. v2.
- d. v8.

Pregunta 9

¿Es recomendable almacenar contraseñas y datos personales por parte de las aplicaciones?:

- a. No.
- b. Si, siempre.
- c. **Depende, lo ideal es que la aplicación guarde únicamente los datos realmente necesarios y en caso de ser datos relevantes los securice de alguna manera.**
- d. Sí, según el tipo de dato manejado por la aplicación

Pregunta 10

Los formularios mal configurados son uno de los vectores de entrada de los aplicativos web.

¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Intento 3.

Pregunta 1

¿Qué significa HSTS?:

- a. High Standard Transport Security.
- b. **HTTP Strict-Transport-Security.**
- c. High Standard HTTP Security.
- d. High Security Transport Standard.

Pregunta 2

La seguridad del código fuente es lo único que interviene en hacer un aplicativo seguro.

¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 3

Para securizar un aplicativo deberemos controlar la entrada de datos en los formularios.

¿Verdadero o Falso?

Seleccione una:

Verdadero

Falso

Pregunta 4

Un WAF no es más que un Firewall con más capacidades. ¿Verdadero o falso?

Seleccione una:

Verdadero

Falso

Pregunta 5

Un WAF nos puede ayudar a detectar y bloquear ataques de botnets. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 6

¿De qué manera podemos proteger las contraseñas almacenadas?:

- a. Mediante cifrados y funciones hash.
- b. De ninguna manera.
- c. En la práctica no es viable.
- d. Almacenándolas en texto claro.

Pregunta 7

El TOP10 de OWASP tiene el objetivo de identificar riesgos. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 8

¿Qué tipos de funciones Hash se recomienda usar?:

- a. Diffie-Hellman.
- b. md5.
- c. SHA.
- d. RSA.

Pregunta 9

Los niveles de aplicación definidos en el ASVS tienen en cuenta el dato manejado y el entorno de la aplicación. ¿Verdadero o Falso?
Seleccione una:

Verdadero

Falso

Pregunta 10

El objetivo de las pruebas de aceptación es verificar la sincronización entre módulos. ¿Verdadero o falso?
Seleccione una:

Verdadero

Falso