## ¡Felicitaciones! ¡Aprobaste!

**Calificación recibida** 100 % **Para Aprobar** 75 % o más

Ir al siguiente elemento

**1.** Completa el espacio en blanco: _____ son códigos o comportamientos maliciosos que se utilizan para aprovechar las fallas de codificación en una aplicación web. **1 / 1 punto**

- ○ El spear phishing
- ◉ Los exploits basados en la web
- ○ La ingeniería social
- ○ La interfaz de línea de comandos

**Correcto**
Los exploits basados en la web son códigos maliciosos o comportamientos que se utilizan para aprovechar las fallas de codificación en una aplicación web.

**2.** ¿Cuál de los siguientes lenguajes suele utilizarse para llevar a cabo ataques de secuencia de comandos en sitios cruzados (XSS). Selecciona dos respuestas. **1 / 1 punto**

- ☐ SQL
- ☑ HTML

**Correcto**
Los ataques XSS se entregan explotando los dos lenguajes utilizados por la mayoría de los sitios web: HTML y JavaScript.

- ☐ Python
- ☑ JavaScript

**Correcto**
Los ataques XSS se entregan explotando los dos lenguajes utilizados por la mayoría de los sitios web: HTML y JavaScript.

**3.** ¿Qué código del lado del servidor se puede usar para defenderse contra los ataques de inyección SQL? **1 / 1 punto**

- ○ Saneamiento de entradas
- ○ Kit de phishing
- ◉ Sentencia preparada
- ○ Ataque por inyección

**Correcto**
Para defenderse contra los ataques de inyección SQL pueden usarse sentencias preparadas. Una sentencia preparada es una técnica de codificación que ejecuta sentencias SQL antes de pasarlas a una base de datos.

**4.** Nombra dos ejemplos de situaciones en las que pueden realizarse inyecciones SQL. **1 / 1 punto**

- ☑ Cuando un usuario ingresa sus credenciales

**Correcto**
Pueden realizarse inyecciones SQL cuando se utiliza el formulario de inicio de sesión para acceder a un sitio y cuando un usuario ingresa sus credenciales. La inyección SQL puede tener lugar en áreas del sitio web que están diseñadas para aceptar entradas de usuarios.

- ☐ Cuando existe un script malicioso en la página web que un navegador carga
- ☐ Cuando se inyecta un script malicioso directamente en el servidor
- ☑ Cuando se utiliza el formulario de inicio de sesión para acceder a un sitio

**Correcto**
Pueden realizarse inyecciones SQL cuando se utiliza el formulario de inicio de sesión para acceder a un sitio y cuando un usuario ingresa sus credenciales. La inyección SQL puede tener lugar en áreas del sitio web que están diseñadas para aceptar entradas de usuarios.

**5.** En un ataque de inyección SQL, ¿qué intentan obtener los agentes de amenazas? Selecciona dos respuestas. **1 / 1 punto**

- [x] Derechos administrativos

**Correcto**
Los agentes de amenaza atacan vectores de ataque para obtener información sensible, modificar tablas e incluso obtener derechos administrativos sobre la base de datos.

- [ ] Explotación de lenguajes
- [x] Información sensible

**Correcto**
En un ataque de inyección SQL, los agentes de amenaza intentan obtener información sensible y derechos administrativos.

- [ ] Categorización del entorno