

[Área personal](#)

Mis cursos

[Ciberseguridad Web - \(PER 7660\) - Febrero 2023](#)

[Actividades](#)

[Cuestionario](#)

Comenzado el	domingo, 4 de junio de 2023, 17:38
Estado	Finalizado
Finalizado en	domingo, 4 de junio de 2023, 17:44
Tiempo empleado	6 minutos 4 segundos
Calificación	9,00 de 10,00 (90%)


Pregunta 1

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuál es la longitud mínima recomendada de un ID de sesión?

Seleccione una:

- ☐ A. 28 bits.
- ☒ B. 128 bits.  Evita ataques de adivinación.
- ☐ C. 1024 bits.
- ☐ D. 2048 bits.


Pregunta 2

Incorrecta

Se puntúa 0,00 sobre 1,00

¿Con qué parámetros de los siguientes es más segura una *cookie*?

Seleccione una:

- ☐ A. Secure.
- ☒ B. HTTPOnly. 
- ☐ C. Expires.
- ☐ D. Todas las anteriores.


Pregunta 3

Correcta

Se puntúa 1,00 sobre 1,00

¿Qué tipo de ataque permite suplantar a un usuario?

Seleccione una:

- ☐ A. De repetición capturando un ID de sesión activo.
- ☐ B. Adivinación del ID de un ID de sesión activo.
- ☐ C. Fijación de sesión.
- ☒ D. Todas las anteriores.  Todos lo permiten.


Pregunta 4

Correcta

Se puntúa 1,00 sobre 1,00

Un *token* anti-CSRF permite:

Seleccione una:

- ☒ A. Validar la procedencia de una petición.  Evita peticiones no legítimas desde otro sitio web distinto al de la aplicación.
- ☐ B. Evitar XSS.
- ☐ C. Evitar SQLi.
- ☐ D. Ninguna de las anteriores.


Pregunta 5

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuándo se debe crear el ID de sesión?

Seleccione una:

- ☐ A. Antes de la autenticación.
- ☒ B. Después de la autenticación correcta.  Evita ataques de fijación de sesión.
- ☐ C. En cualquier momento.
- ☐ D. No es necesario.


Pregunta 6

Correcta

Se puntúa 1,00 sobre 1,00

¿Dónde puede ubicarse el ID de sesión?

Seleccione una:

- ☐ A. Cabecera *set-cookie*.
- ☐ B. Parámetro URL.
- ☐ C. Parámetro POST.
- ☒ D. Todas las anteriores.  Además, mediante reescritura de URL.

Pregunta 7

Correcta

Se puntúa 1,00 sobre 1,00

¿Cómo se denomina la base de datos del mecanismo de autorización?

Seleccione una:

- ☒ A. Lista de control de acceso  La lista de control de acceso relaciona usuarios, roles, permisos y

acceso.

recursos.

- ☐ B. Base de datos.
- ☐ C. Roles.
- ☐ D. Recursos.

Pregunta 8

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuál es un ataque a la autorización?

Seleccione una:

- ☐ A. TOCTOU.
- ☐ B. XSS.
- ☐ C. LFI.
- ☒ D. Todos los anteriores.  Además, CSRF y SQLi.


Pregunta 9

Correcta

Se puntúa 1,00 sobre 1,00

¿Cuál es un mecanismo de defensa para una buena autorización?

Seleccione una:

- ☐ A. Política robusta de contraseñas.
- ☐ B. Separación de roles y tareas.
- ☐ C. Administración robusta de permisos.
- ☒ D. Todas las anteriores.  Además, asegurar el principio de mínimos privilegios.


Pregunta 10

Correcta

Se puntúa 1,00 sobre 1,00

¿A qué es debido TOCTOU?

Seleccione una:

- ☐ A. A no diseñar operaciones atómicas.
- ☐ B. A no bloquear el acceso a los recursos debidamente.
- ☐ C. No tener un ID de sesión largo.
- ☒ D. La A y  Las operaciones deben ser lo más atómicas posibles y bloquear-liberar los recursos la B. debidamente durante el acceso.

◀ Test 6. Autenticación en las aplicaciones web

Ir a...

Test 8. Seguridad en el desarrollo de las Aplicaciones Web ▶