Pregunta 1

10 de 10 puntos

Angular y otros frameworks Web implementan un mecanismo de solución para vulnerabilidades del tipo CSRF, que consiste en la generación de un identificador oculto "fresco" que se le envía al usuario y que se usa como un dato adicional a todos los requests posteriores que vienen del usuario hacia el servidor, tal como por ejemplo la que se encuentra detallada en https://medium.com/@d.silvas/how-to-implement-csrf-protection-on-a-jwt-based-app-node-csurf-angular-bb90af2a9efd.

Respuesta seleccionada:
Esta librería o similares tendría poco efecto para mitigar vulnerabilidades como XSS ya que en ese caso el problema aparece cuando el contenido en código javascript que se registra en algún campo de usuario, aún generando un request válido, se permite almacenar como datos de usuario.

Respuestas:

Esta librería o similares puede también utilizarse para mitigar las vulnerabilidades provocadas por inyecciones de código SQL ya que los requests que llegan al servidor estarían protegidos de ser generados a mano.

Esta librería o similares tendría poco efecto para mitigar vulnerabilidades como XSS ya que en ese caso el problema aparece cuando el contenido en código javascript que se registra en algún campo de usuario, aún generando un request válido, se permite almacenar como datos de usuario.

Esta librería o similares podrían utilizarse también para mitigar escenarios de vulnerabilidades de XSS ya que el token de CSRF que se genera desde el servidor prohibiría a los usuarios embeber código javascript en las páginas.

Esta librería o similares se puede utilizar como está para evitar ataques de XSS, ya que la existencia del token permitiría verificar que todos los requests que llega al servidor son válidos, y rechazaría las peticiones que tienen contenido javascript.

Pregunta 2

10 de 10 puntos

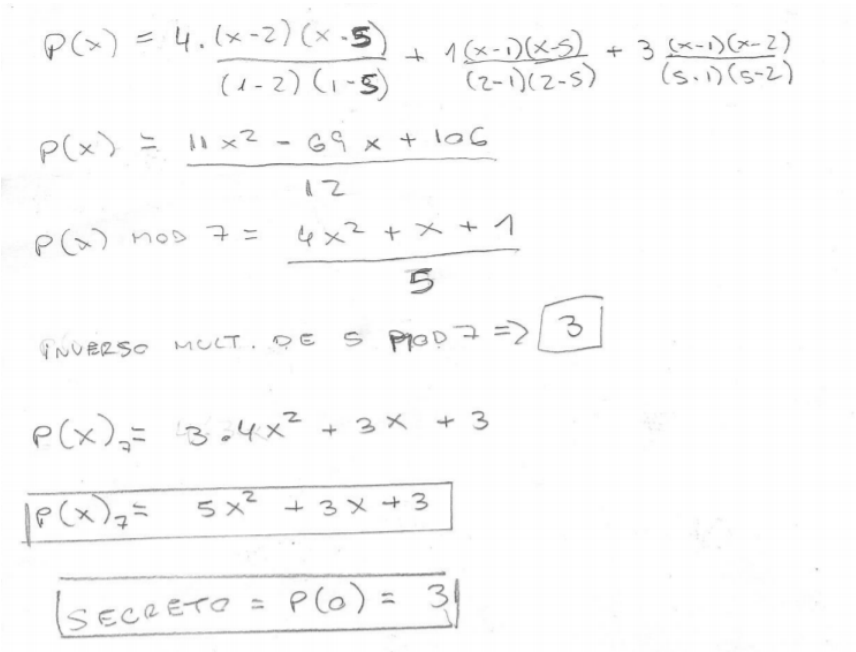
Considerar un esquema de secreto compartido de Shamir (3,4) en $\mathbb{Z}_7$, con el conjunto de 4 sombras (1,4)(2,1)(3,1)(5,3)

a) Recuperar el secreto.

b) Indicar el polinomio utilizado para obtener el conjunto de sombras.

Dado el contexto, es importante detallar en la hoja los pasos para arribar a la solución. Completar el ejercicio en una sola carilla.

Respuesta seleccionada: shamir.pdf
Comentarios para respuesta: [No se ha dado ninguna]



Pregunta 3

10 de 10 puntos

Todos los ataques similares de inyección de código, como SQL Injection, se producen por tener datos de control mezclados con datos de usuario.

Respuesta seleccionada: Verdadero
Respuestas: Verdadero
Falso

Pregunta 4

10 de 10 puntos

Un sysadmin de la empresa les dice que va a correr ssh en el puerto 33 en vez del 22 para evitar posibles ataques y vulnerabilidades.

Esto iría en contra del principio:

Respuesta seleccionada: 1. Diseño abierto

Respuestas:
1. Diseño abierto
2. Economía de Mecanismos
3. Mediación completa
4. Mecanismos exclusivos

Pregunta 5

10 de 10 puntos

Facebook los contrata para diseñar un modelo de seguridad para el control de la información oficial que se publica en la plataforma. Teniendo en cuenta los modelos BIBA, Bell Lapadula y Muralla China, planteen cómo estructurarían la solución para evitar la proliferación de "fake news". Aclarar por qué y cómo usarían uno y no otro.

Respuesta seleccionada:	Dado que la política de seguridad es para asegurar la integridad de la información oficial que se publica en una red social, utilizaría el modelo de BIBA estricto ya que se busca que los sujetos que hagan las publicaciones, lo hagan en base a información que leyeron de mayor integridad que ellos (se escribe hacia abajo y se lee hacia arriba). El modelo de Bell Lapadula garantiza confidencialidad, lo que no aplica a este problema, y muralla china es un modelo que soluciona problemas de conflictos de interés que tampoco aplica para este caso de fake news.
Respuesta correcta:	La respuesta correcta tienen que girar alrededor de la comparación entre los diferentes modelos enfatizando que un modelo BIBA estricto es la solución más adecuada a donde se necesita una verificación de integridad (veracidad, confiabilidad) de la información.
Comentarios para respuesta:	Un poco Muralla China puede aplicar, ya que uno pensaría que, sobre todo corporaciones, pueden publicar noticias que sí beneficien sus propios intereses. Está perfecta la respuesta.

Pregunta 6

10 de 10 puntos

El modelo de Muralla China consiste en tres reglas básicas. La primera es la propiedad de seguridad simple, la segunda la matriz de permisos discrecionales y la tercera las reglas de compartimientos.

Respuesta seleccionada: Falso

Respuestas:
- Verdadero
- Falso

Pregunta 7

10 de 10 puntos

El Project Manager de su equipo le indica que para evitar ataques de XSS sobre la página web principal, se van a realizar chequeos en los browser cliente de cada usuario. De este modo se ahorrarían recursos debido a que no se debería enviar cada request a una API y de esta forma se ahorrarían costos.

Qué le parece la idea? Piense desde el punto de vista de seguridad.

Respuesta seleccionada:	Me parece una mala idea ya que no se puede confiar en nada de lo que provenga o suceda del lado del cliente. Tranquilamente un atacante podría modificar el código para saltearse el chequeo y de esa forma realizar de todas formas el ataque de XSS.
Respuesta correcta:	Si los chequeos se aplican desde el lado del cliente, estos pueden ser bypasseados por lo tanto no es una buena idea y siempre se deben realizar chequeos a nivel de servidor (server side)
Comentarios para respuesta:	[No se ha dado ninguna]

Pregunta 8

10 de 10 puntos

La realización de pentesting permite certificar que un sistema es seguro.

Respuesta seleccionada: Falso

Respuestas:
- Verdadero
- Falso

Pregunta 9

10 de 10 puntos

¿Cuales de los siguientes suelen ser fuentes de problemas para generar vulnerabilidades?

Respuestas seleccionadas:
1. Fallos de implementación
2. Uso indebido del sistema

Respuestas:
1. Fallos de implementación
2. Uso indebido del sistema
3. Utilizar infraestructura Cloud
4. Utilizar software Open Source

Pregunta 10

10 de 10 puntos

Actualmente diversos bancos ofrecen a sus usuarios la selección de un nombre de usuario de un alfabeto de 26 letras que caduca a los 90 días (adicionalmente al password). José Cifrín, el CSO del Banco de Seguranza, dice que el modelo de amenazas que establecieron opera bajo el supuesto que un atacante puede probar 10^9 usuarios por segundo, y se desea que el atacante tenga una probabilidad de éxito de $\frac{1}{1000}$ a lo largo de 365 días.

a) ¿ Cuál es la longitud mínima de un nombre de usuario que cumpla con lo pedido ?

b) Los usuarios encuentran esta tarea de cambio de usuario bastante desagradable. Sin embargo, el CSO descarta esta afirmación por considerarla que no está alineada a los principios de seguridad. ¿ Es esto correcto ?

c) ¿ Qué alternativa a este esquema de autenticación podría implementarse en este caso ?

Respuesta seleccionada:

a)
Fórmula de Anderson: P >= T*G / N

P = 1/1000
T = 90 días
G = (10^9)*60*60*24
N = 26^L (L = longitud nombre de usuario)

$L >= Log_{26}(T*G / P)$
$L >= Log_{26}((90*10^9 * 60*60*24)/(1/1000))$
L >= 13.35

RTA: la longitud mínima del nombre de usuario debe ser de 14 caracteres

b)
El CSO está equivocado ya que la aceptación psicológica del usuario es un principio de diseño seguro que se debe tener en cuenta.

c)
Una alternativa de autenticación podría ser la implementación de Two-Factor-Authentication (2FA). La ventaja de este método es que los usuarios no tendrán que cambiar su nombre de usuario cada cierta cantidad de tiempo (lo eligen solo una vez) pero la desventaja es que se agrega un paso adicional a la hora de loguearse que es la de introducir un token numérico generado por una entidad externa segura.

Respuesta correcta:

La cuenta sale directa. La "Aceptación del Usuario" es también un principio de diseño de seguridad que tiene que tenerse en cuenta. El CSO está equivocado al respecto. En c) se puede ser creativo pero una opción es usar 2FA o similar. Habría que explicar ventajas y desventajas.

Comentarios para respuesta:

[No se ha dado ninguna]

Ejercicio 1

Esta libreria o similares tendria poco efecto para mitigar vulnerabilidades como XSS ya que en ese caso el problema aparece cuando el contenido en codigo javascript que se registro en algun campo de usuario, aun generando un script valido, se permite almacenar como datos de usuario.

Ejercicio 2

a. Tomamos $(1,4), (2,1), (3,1)$.

$$P(x) = 4\frac{(x-2)(x-3)}{(1-2)(1-3)} + \frac{(x-1)(x-3)}{(2-1)(2-3)} + \frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$\Rightarrow P(x) = 2(x^2-5x+6) - (x^2-4x+3) + \frac{1}{2}(x^2-3x+2)$$

$$\Rightarrow P(x) = \frac{3}{2}x^2 - \frac{15}{2}x + 10 \mod 7$$

Rta: $S = P(0) = 10 \mod 7 = 3$

b. $P(x) = 5x^2 - 11x + 10 \mod 7 = 5x^2 + 3x + 3$

Ejercicio 3

VERDADERO

Este ataque ocurre cuando ingresamos los inputs de los usuarios directamente a una instruccion SQL.

Ejercicio 4

a. Diseño abierto: La seguridad no debe depender del secreto del diseño o la implementacion.
b. Economia de Mecanismos: los mecanismos de seguridad deben ser simples.
c. Mediacion completa: Todos los accesos a objetos deber ser verificados.
d. Mecanismos exclusivos: los mecanismos de seguridad no deben compartirse.

Rta: a

Ejercicio 5

- Bell - Lapadula: Este modelo garantiza confidencialidad, lo cual no aplica para este problema.
- Muralla China: Este modelo soluciona problemas de conflictos de interes, lo cual tampoco aplica.
- Biba: Este modelo garantiza integridad. El modelo que mas aplica es el estricto porque queremos que los usuarios hagan publicaciones en base a las publicaciones de mayor integridad que ellos.

Ejercicio 6

FALSO

- No tiene matriz de permisos discrecionales
- No hace uso de compartimientos, maneja COs y COIs

Ejercicio 7

Es mala idea porque los chequeos se hacen desde el lado del cliente entonces estos pueden ser bypasseados (Ej. Postman, CURL...). Por lotanto, los chequeos se deben hacer a nivel servidor.

Ejercicio 8

FALSO

Solo verifica que existen vulnerabilidades pero no verifica que no hayan.

Ejercicio 9

Fuentes de problemas :

1. Requerimientos incompletos, incorrectos o faltantes
2. Fallos en el diseño
3. Fallos en implementacion en HW
4. Fallos en implementacion en SW
5. Errores de uso por errores de operacion
6. Uso indebido del sistema
7. Fallos de los equipos o medio de comunicacion
8. Casos de fuerza mayor, desastres
9. Errores al actualizar, mantener o decomisar

Rta: 1 y 2

Ejercicio 10

$P \geq \frac{IG}{N}$

- $P = 0,001$
- $T = 90 * 3600 * 24$
- $G = 10^9$

a. $N = 26^L$

$\Rightarrow N \geq \frac{IG}{P} = 7.776 \times 10^{18}$

$\Rightarrow 26^L \geq 7.776 \times 10^{18}$

$\Rightarrow \log_{26}(26^L) \geq \log_{26}(7776 \times 10^{18})$

$\Rightarrow L \geq 13.5$

Rta: La longitud minima es de 14 caracteres.

b. FALSO

La afirmacion esta alineada con el principio de diseño de aceptacion psicologica que dice que mientras mas seguro, menos usable.

c. Se puede hacer 2FA para evitar cambiar la contraseña pero esto no lo vuelve mas usable.