

Nicolas Diaz Guzmán

Juan Asenjo Segovia

Francisca Sepúlveda Thomassen

Fritzon Brignolle

Boris Sepúlveda González

Programación Segura

Evaluación sumativa 1

Profesora Pamela Acevedo Bonelli

***Índice***

Vulnerabilidades y Soluciones1

Modelo de amenazas2

Evidencias del uso de la herramienta GIT en GITHUB3

4

5

6

Introducción

***Vulnerabilidades y soluciones***

Problema:

Hace falta el encabezado X-Frame-Options para mejorar la seguridad, ya que sin esto algún usuario malicioso podría usar ClickJacking para ingresar algún elemento y otro usuario al hacer clic podría descargar algún malware.

Texto

Descripción generada automáticamente con confianza media

Solución:

Las políticas de seguridad de contenido según el cuadro de accesorios que nos permite identificar a través de este (deny, sameorigin, allow-from) modificando estas opciones podríamos hacer el sitio web mas seguro.

Problema:

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Solución:

Utilizar una biblioteca o marco comprobado hace que esta vulnerabilidad sea más fácil de evitar, un ejemplo de esto sería el paquete anti-CSRG.

Problema:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Solución:

Problema:

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Solución:



Modelo de amenazas stride

Una de las primeras amenazas que identificamos es la vulneración de datos ya que con este se puede suplantar identidades de personas obteniendo datos a través de la consulta ya que esta está mal programada a través de código php

Manipulación de datos

Dadas las circunstancias en esta página se pueden manipular datos de forma maliciosa ya que al consultar en la página nos muestra información primordial de cada usuario registrado.

Divulgación de información

Es la exposición de datos sensibles sobre esta página, en la cual podemos ver la fuga de datos

***Modelo de amenazas***

Imagen que contiene competencia de atletismo

Descripción generada automáticamente

Las vulnerabilidades previamente señaladas fueron conseguidas a raíz de un reporte generado con la herramienta de Microsoft “Microsoft threat modeling tool”

Modelo de amenazas stride

Una de las primeras amenazas que identificamos es la vulneración de datos ya que con este se puede suplantar identidades de personas obteniendo datos a través de la consulta ya que esta esta mal programada a través de código php

Manipulación de datos

Dadas las circunstancias en esta pagina se pueden manipular datos de forma maliciosa ya que al consultar en la página nos muestra información primordial de cada usuario registrado.

Divulgación de información

Es la exposición de datos sensibles sobre esta página, en la cual podemos ver la fuga de datos

***Evidencia del uso de la herramienta GIT en GITHUB***