Evaluación desarrollo Software seguro II

**Explicación del proyecto y su modelo de datos físico:**

Nuestro proyecto o aplicación web, se trata sobre una red social o servicio que se centrara en el área laboral, un sitio donde todas las personas puedan acceder a buscar trabajo o trabajador(es), con la posibilidad de registrarse para tener completo acceso a los servicios de la aplicación. Con esto podemos permitir que la persona busque entre todos los avisos de trabajo y enviar solicitudes, o bien crear sus propias publicaciones donde se promocione o en el caso de que necesite a alguien para un trabajo puntual.

**Protección contra ataques XSS:**

En Django tenemos escapada de texto usando Jinja como podemos verlo a continuación:

Texto

Descripción generada automáticamente

Gracias a esta sintaxis lo que sea ingresado como texto no se concatenara como script o lenguaje HTML lo que permitiría la protección contra ejecución de código en la aplicación.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**Protección de acceso a base de datos por medio de token:**

Esta sintaxis seguriza nuestro formulario que envía la solicitud a la base de datos, en este caso es para registrar al usuario.

**Protección contra acceso a rutas en las que se necesita inicio de sesión:**

Una de las secciones que es exclusiva para usuarios registrados en la pagina es la de crear publicación, y que esta renderizado para la siguiente vista:

**Texto

Descripción generada automáticamente**

Al comienzo de la función se puede ver la sintaxis “@login\_required”

Al comienzo de la función se puede ver la sintaxis “@login\_required”, lo que quiere decir que los usuarios sin cuenta no puedan acceder a endpoints que son solo para registrados y en cambio los redirija al login de forma automática con la siguiente configuración en settings.py:



Ejemplo:

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

Aquí traté de acceder al apartado de “publicar” el cual está segurizado y la respuesta es una redirección al login.

Mi laboratorio de portswigger:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente  
  
  
Inyección SQL:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Cross-site Scripting:

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

Nombre: Francisco Cornejo