Informe de Software seguro (Evaluación n°2)

En este informe se podrá apreciar la segurización de nuestra aplicación web elaborada con Django, por medio del uso de tokens para el acceso a base de datos y permisos o restricciones para usuarios válido, se verá cómo redirigimos a los usuarios no registrados al apartado de login y que intenten acceder a espacios designados para usarse solo si se está logueado.

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 para buscar trabajo o trabajor(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 de tipo XSS:  
Django cuenta con escapada de texto con el uso de Jinja como podemos verlo en el codigo:

Texto

Descripción generada automáticamente

Gracias a esta sintaxis lo que sea ingresado como texto, no se concatenará como script o lenguaje HTML lo que permitirá protección contra intento de ejecución de código.

Protección de acceso a base de datos por medio de token:

Texto

Descripción generada automáticamente

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 una publicación, y que está renderizado por la siguiente vista:

Texto

Descripción generada automáticamente

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:  
  
  
Inyección SQL:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Cross-site Scripting:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente