Reto

El equipo de seguridad está desarrollando un sistema para gestionar la seguridad de los diferentes sistemas que se encuentran desplegados en la infraestructura Cloud mediante el cruce de información con los CVEs del NIST.

El objetivo de la aplicación permitirnos obtener un listado de vulnerabilidades del NIST (https://nvd.nist.gov/developers/vulnerabilities).

Adicionalmente, esta aplicación debe ofrecer la posibilidad de indicarle qué vulnerabilidades ya se encuentran fixeadas en nuestra infraestructura y que NO queremos que aparezcan en el listado.

En concreto, se debe desarrollar una API REST (con sus convenciones) que tenga los siguientes métodos:

1) Endpoint GET que devuelve el listado **total** de las vulnerabilidades.
2) Endpoint POST que reciba la/s vuln/s fixeada/s.
3) Endpoint GET que devuelva el listado de vulnerabilidades **exceptuando** las fixeadas (ingresadas en el endpoint del punto 2).
4) Endpoint GET que permita obtener información sumarizada de vulnerabilidades por severidad.

Consideraciones

- La base de datos a utilizar queda a elección.
- Lenguaje Python
- Usar Django REST framework.
- La aplicación desarrollada debe poder ejecutarse dockerizada.

Entregables

- Repositorio privado de Github (Agregar como colaborador al usuario **m4lt4**).
- Dockerfile/s para ejecutar la aplicación de manera local.
- README explicando la manera de ejecutar la aplicación.
- Documentación sobre la aplicación y su funcionamiento.

Puntos extra (opcionales)

- Testing.
- Autenticación y autorización de la API.
- Implementación de métodos adicionales en la API.
- Diagrama de la solución utilizando servicios del Cloud (AWS, GCP o Azure).
- Logs/Auditoría de uso de la API.
- Solución deployada en cloud.