Solución a vulnerabilidades de POLUX

Previamente se expresó por medio de las pruebas de carga y seguridad, que el sistema de gestión de trabajos de grado POLUX, presentaba varias vulnerabilidades:

- Varias librerías con diferentes vulnerabilidades entre (bajas, media ,altas y criticas).
- Credenciales quemadas en el código
- Pasos de scanner en drone

Solución para las librerías fue dada por los siguientes pasos:

1-) Verificar por medio del comando ***npm audit*** , las vulnerabilidades encontradas fueron 382.

2-) Se tomo como base para primera instancia como base el cliente de resoluciones para actualizar las librerías a un punto donde no afecten el funcionamiento del programa.

3-) Se comienza a eliminar las librerías que no se usan o están obsoletas o deshabilitadas.

4-) Se actualizan o cambian las librerías que utiliza POLUX.

5-) Se elimina el archivo package-lock.json para poder usar el comando ***npm install*** y se actualice con las nuevas librerías

6-) Se realiza ***npm run-script build*** para poder corroborar que no haya conflictos con el sistema.

Solución credencial quemadas en el código fue dada por:

1-)La eliminación de las credenciales por parte de reportes en spagobi.

2-)En el caso de las credenciales de nuxeo se indica que se tiene planeado un sprint para la corrección de esa parte a través del API gestor documental

Solución pasos de scanner en drone :

1-) Se agrega el paso extraído de otro cliente para su ejecución en el pipeline.