Endpoint Developer Home Assignment, Prompt Security

Your Assignment

Implement an application that will capture PDF file uploads to ChatGPT in chrome (or another web AI site that accepts file uploads), send the files to a file inspection service and log the results.

The file inspection service should inspect and identify PDF files that contain secrets:

1. In case it detected a secret, it is enough to alert the user with a pop-up without blocking it.
2. Your file inspection service should use Prompt Security text inspection API for the identification of the secrets in text.

An example of using the text inspection API using curl:

```
curl --location 'https://eu.prompt.security/api/protect' \
--header 'APP-ID: cc6a6cfc-9570-4e5a-b6ea-92d2adac90e4' \
--header 'Content-Type: application/json' \
--data '{"prompt": "<TEXT TO INSPECT>"}'
```

Implementation Details

- For capturing files in browser you can implement a Chrome Extension
- Feel free to use any language, tool or framework including GenAI sites for this assignment
- An example of an AWS secret is "AKIAIOSFODNN7EXAMPLE"

Submission Guidelines

To submit your completed assignment, please provide us with a Github repo containing:

- The extension code for capturing files
- The file inspection service code
- Include also a README file containing:
    - Instructions for using the service and testing file inspection
    - List of limitations that the extension and service have (if any)
    - List of possible features/requirements that the service needs in order to make it production ready
    - List of performance improvement ideas to support large scale