### Cybersecurity Toolkit Project Report

#### Results

The project transitioned from the initial intent to create a website to developing a set of Node.js scripts. Each tool in the toolkit is designed for ease of web integration, with inputs and outputs clearly defined for seamless implementation.

* Dependency Checkers (checkRequirements.js and checkNode.js): These scripts analyze requirements.txt and package.json for Python and Node.js projects, respectively. They address the OWASP vulnerability regarding the use of components with known vulnerabilities by filtering through GitHub's open repositories and outputting JSON reports.
* Subdomain Enumerators (subDomainByCrt.js and subDomainByBruteForce.js): These tools help in identifying potentially insecure subdomains, a crucial step in mitigating the OWASP risk of insecure subdomain configurations.
* ZAP Scanners (zapScanActive.js and zapScanPassive.js): The active and passive scanning scripts are geared towards identifying a range of security issues, including those highlighted in the OWASP Top 10, such as Injection Flaws and Misconfigurations.
* Password Security (passwordCheckerZap.js): This script aims to test for weak passwords, aligning with the OWASP guidelines on Broken Authentication.

#### What I Did

For each component of the toolkit, I followed a structured approach:

* Developed scripts that interact with established security APIs.
* Ensured that the output is in JSON for easy parsing and integration.
* Created a methodology that allows each script to function as a standalone tool or as part of a larger web interface.

#### How I Was Challenged

Throughout the development process, I encountered and overcame several challenges:

* Handling rate limiting and data normalization when integrating with external APIs like GitHub's Advisory Database.
* Parsing and matching the data accurately from requirements.txt and package.json against known vulnerabilities.
* Ensuring that the tools could be used responsibly without causing undue strain on the target web applications.

#### Moving Forward

As I refine the toolkit, I plan to continue addressing the challenges, enhancing the tool's effectiveness, and staying current with the latest in web security best practices.