POLITECHNIKA POZNAŃSKA

Wydział Informatyki i Telekomunikacji

Application’s security testing

Daniel Kotyński

146905

Daria Głębowska

141221

13.12.2022

1. **Automated security helper**

During *ash* test, the tool found many medium, high and critical vulnerabilities connected to e.g. injection attacks, DoS, cross-site scripting or excessive memory consumption. The detailed report is in the file *aggregated_results.txt*.

2. **Betterscan-ce**

It found only some warnings connected to GoogleYouTubeAPIKey and Base64 High Entropy String.

3. **SpotBugs**

We cannot use this tool because the application which we tested is written in JavaScript, not Java.

4. **Fluid Attack's Scanner**

Unfortunately, we have many issues during using this tool and finally tests weren't finished.

5. **Horusec**

It found many issues, like using alert statements in production code, or using outdated dependencies with suggested fixes. It also found hardcoded google cloud api key.

6. **Mobile Security Framework**

This application doesn't support React Native mobile applications.

7. **Gitleaks**

It found hardcoded private secret to google cloud - the same one found by Horusec before.

8. **SonarQube SCA**

It didn't found any security problems, only few code smells (unused imports and variables)