Software Engineering Tools Lab Assignment No-7

**2020BTECS00043, Chetana Shivkiran Patil**

(Module 5- Source code testing using tools)

Q 1. What is Source code analysis? What is its importance?

Source code analysis, also known as static code analysis, is the process of examining the source code of a software application without executing it, in order to identify potential issues, errors, vulnerabilities, and other quality-related aspects. The analysis is performed using automated tools that scan the codebase and detect patterns or structures that indicate potential problems.

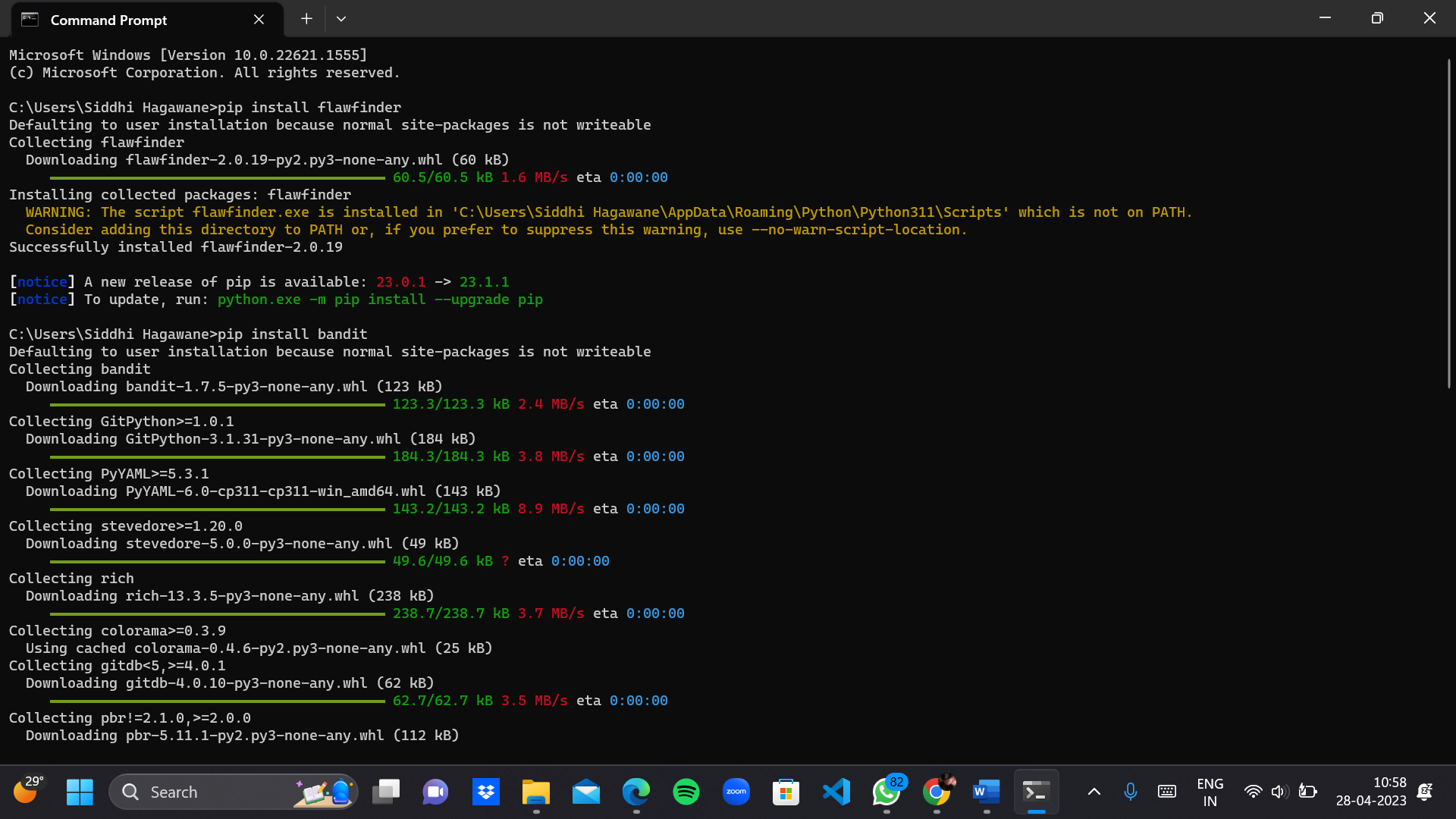
1. Improved code quality: Source code analysis can help identify coding standards violations, code smells, and other issues that can degrade the quality of the codebase.
2. Increased security: Source code analysis can help identify security vulnerabilities in the codebase, such as potential buffer overflows, injection attacks, or other issues that can be exploited by attackers.
3. Enhanced maintainability: Source code analysis can help identify complex or hard-to-maintain code structures, making it easier for developers to update, refactor, or extend the codebase as needed.
4. Faster development: By catching potential issues early, source code analysis can help reduce the time and effort required for debugging and testing, allowing developers to focus on building new features or improving existing ones.

Q 2. Below are the some important open source tools used in testing the source code, provide the information of below tools with respect to

1. Owner/ developer
2. Developed in which language
3. Brief information/introduction
4. Language support (applicable for source code written in language)
5. Advantages
6. Disadvantages

**Source code analysis tools-**

1. VisualCodeGrepper
   1. Owner/developer: Developed by Joris van de Vis for CodeClimber.net.
   2. Developed in which language: Written in Python.
   3. Brief information/introduction: VisualCodeGrepper is an open-source static code analysis tool that searches for patterns of interest in source code using regular expressions. It can detect issues such as potential security vulnerabilities, coding standard violations, and code smells.
   4. Language support: Supports source code written in multiple languages including C, C++, C#, Java, JavaScript, PHP, Python, Ruby, and more.
   5. Advantages: Easy to install and use, customizable search patterns, support for multiple languages, fast scanning, and integration with external tools such as SonarQube and Jenkins.
   6. Disadvantages: Limited functionality compared to more advanced static code analysis tools, may produce false positives, and lack of comprehensive documentation.
2. Rips
   1. Owner/developer: Developed by Johannes Dahse.
   2. Developed in which language: Written in PHP.
   3. Brief information/introduction: RIPS is a free and open-source tool for detecting security vulnerabilities in PHP applications. It uses static code analysis techniques to detect issues such as SQL injection, cross-site scripting (XSS), and file inclusion vulnerabilities.
   4. Language support: Supports PHP source code.
   5. Advantages: Easy to install and use, comprehensive detection of security vulnerabilities, customizable analysis rules, and integration with popular development tools such as Jenkins and GitLab.
   6. Disadvantages: Limited language support, may produce false positives, and lack of support for other programming languages.
3. Brakeman
   1. Owner/developer: Developed by Justin Collins.
   2. Developed in which language: Written in Ruby.
   3. Brief information/introduction: Brakeman is an open-source static code analysis tool for Ruby on Rails applications. It can detect security vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It also generates reports that provide detailed information about the issues found.
   4. Language support: Supports Ruby on Rails source code.
   5. Advantages: Easy to install and use, comprehensive detection of security vulnerabilities, customizable analysis rules, and integration with popular development tools such as Jenkins and GitHub.
   6. Disadvantages: Limited language support, may produce false positives, and lack of support for other programming languages.
4. Flawfinder
   1. Owner/developer: Developed by David A. Wheeler.
   2. Developed in which language: Written in Perl.
   3. Brief information/introduction: Flawfinder is an open-source static code analysis tool that scans C/C++ code for potential security vulnerabilities such as buffer overflows, format string vulnerabilities, and more. It generates reports that provide detailed information about the issues found.
   4. Language support: Supports C and C++ source code.
   5. Advantages: Easy to install and use, comprehensive detection of security vulnerabilities, customizable analysis rules, and integration with popular development tools such as Jenkins and Git.
   6. Disadvantages: Limited language support, may produce false positives, and lack of support for other programming languages.
5. Bandit
   1. Owner/developer: Developed by OpenStack Security Group.
   2. Developed in which language: Written in Python.
   3. Brief information/introduction: Bandit is an open-source static code analysis tool that scans Python code for potential security vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It generates reports that provide detailed information about the issues found.
   4. Language support: Supports Python source code.
   5. Advantages: Easy to install and use, comprehensive detection of security vulnerabilities, customizable analysis rules, and integration with popular development tools such as Jenkins and GitHub.
   6. Disadvantages: Limited language support, false positives, limited functionality, Lack of support for complex applications.



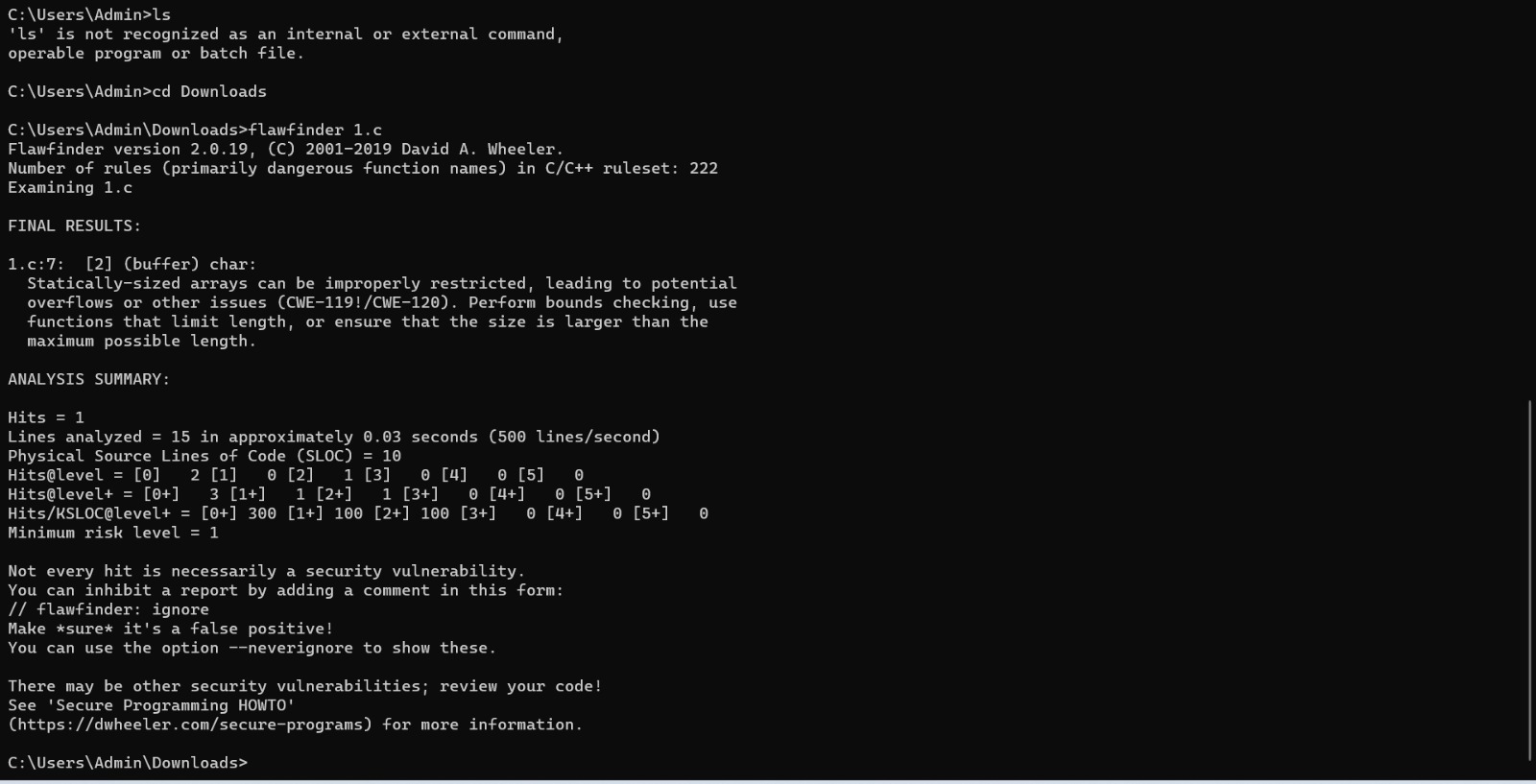
Q 3. Perform source code testing using **Flawfinder** for the code written in ‘c’ and ‘cpp’ language given below

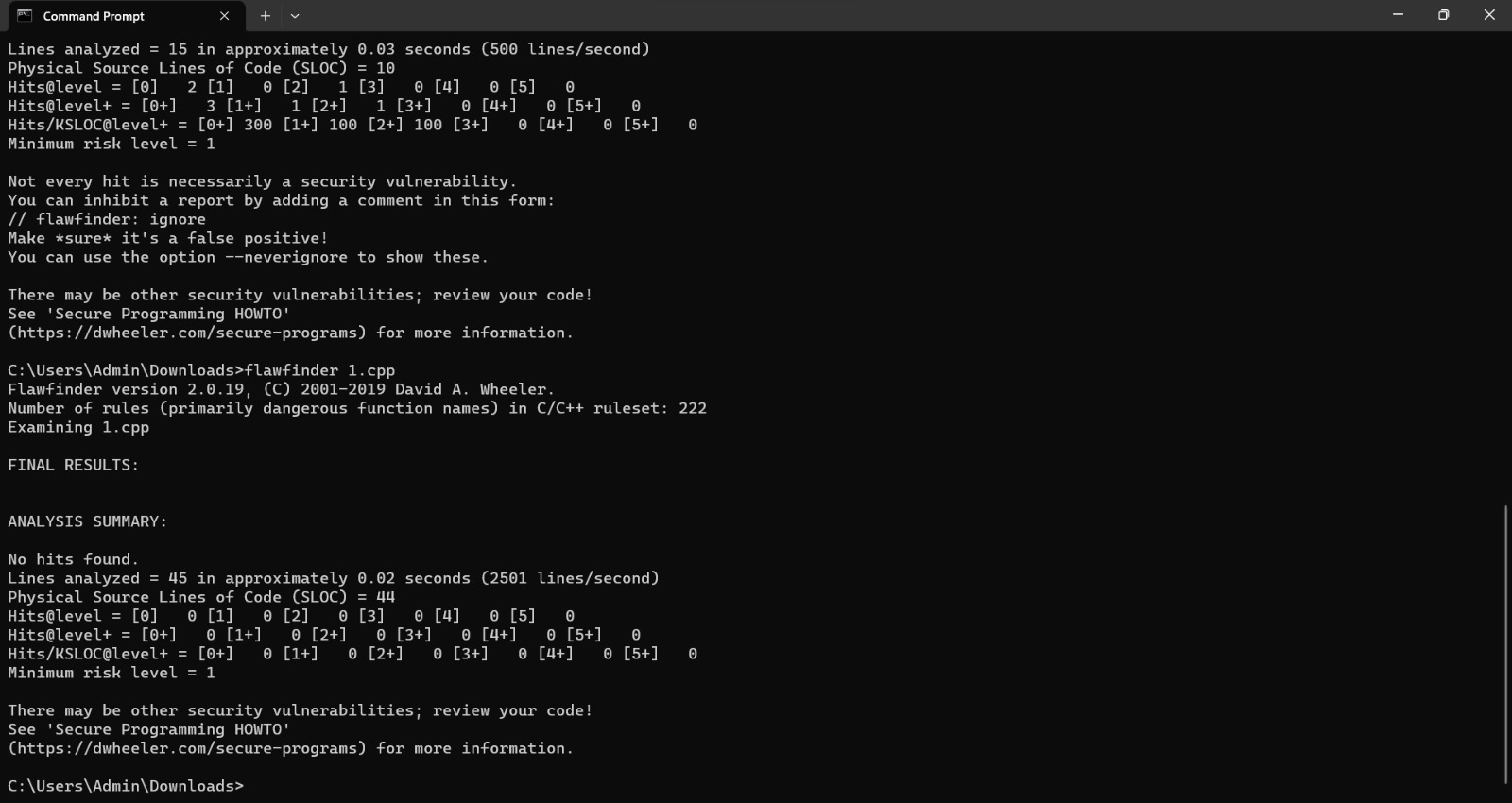
Link- https://github.com/sidp1991/SETAssignment

Note-use files program1.c and program2.cpp present on above link.

After performing analysis create a report which will contain below points

* + 1. Number of hits
    2. Potential risks
    3. Suggested alternatives for these risks
    4. Updating the code as per suggestions
    5. Re-execution of code after updating the changes.





Q 4. Perform source code testing using **Bandit** for your code written in ‘python’ language (use your previous code) for any security flaws

After performing analysis create a report which will contain below points

1. Number of hits
2. Potential risks
3. Suggested alternatives for these risks
4. Updating the code as per suggestions
5. Re-execution of code after updating the changes.

