A Python Tool for Enhancing Coding Practices and Security of Java Programs

Venkata Pathuri [rpathuri@umd.edu] and Indu Narisetty [lohith80@umd.edu]

ABSTRACT

More and more cyberattacks are going after Java programs, which shows how important it is to create secure coding practices and tools that can find vulnerabilities. In this project, we want to make a Python tool that takes a Java program file as input, checks the source code, and finds vulnerable libraries or functions that can be exploited using OWASP Top 10.

Venkata and Indu are on our team. They will work together to make and test the tool. The scope of the project includes understanding the different types of OWASP Top 10 vulnerabilities and their impact on the security of a Java program. We will also explore the best practices for securing Java programs and analyze the effectiveness of the proposed tool in identifying vulnerabilities and suggesting necessary changes to overcome them.

The tool will be written in Python and will utilize the OWASP Top 10 list to determine where the Java application is vulnerable. The application will display a list of the Java file's vulnerabilities and recommend the necessary corrections. The objective of the project is to contribute significantly to the existing body of knowledge by providing Java programmers with a useful tool for detecting and fixing vulnerabilities. With the tool, developers may safeguard their code from known vulnerabilities and make it compatible with several programming languages.

In conclusion, the tool suggested will make it easy to find and fix OWASP's top 10 Java vulnerabilities. The project will give us the chance to learn about and use the best security methods while helping the academic and research communities.