Abstract

This project focuses on developing a Flask-based web application for analysing potentially malicious files uploaded by users. The application allows users to upload files which are then analysed to determine if they pose a security risk. Key features include file type detection, static analysis of Portable Executable (PE) files using the static analysis module, and heuristic-based malware detection.

The application employs Flask for its web framework and integrates SQLite for storing analysis results. Files uploaded by users are checked against a predefined set of allowed extensions. Upon upload, the application uses the filetype library to detect the file type based on its extension. If the file is identified as a PE file (.exe, .dll), additional analysis is performed to extract PE information such as number of sections and entry point.

Malware detection is implemented through simple heuristic rules, evaluating characteristics like the number of sections and entry point address. Results of the analysis are stored in an SQLite database, including file metadata and analysis outcomes.

The web interface provides feedback to users based on the analysis results, directing them to appropriate responses such as displaying warnings for potentially malicious files or confirming the safety of uploaded files. This project aims to enhance cybersecurity awareness by empowering users to verify the safety of files before interacting with them further.

MANU C MADHU