Abstract

This project introduces a robust web-based application designed to enhance cybersecurity practices by providing users with a reliable platform to securely upload and analyse files for potential malware threats. Leveraging Flask, a powerful Python web framework, the application offers a user-friendly interface that facilitates seamless file uploads and employs sophisticated backend processes for file type detection and malware analysis.

Key functionalities include comprehensive file handling capabilities with stringent validation to allow uploads of specified file types such as executables (`*.exe`, `*.dll`) and common document formats (`*.docx`, `*.pdf`). Upon uploading a file, the application utilizes the `filetype` library, which employs file signature analysis to accurately identify the file type, ensuring robust handling of diverse file formats.

For Portable Executable (PE) files, the application conducts in-depth static analysis using the `pefile` library. This analysis extracts critical information such as the number of sections and entry point address, which are then evaluated against heuristic rules to detect potential malware characteristics. Users receive immediate feedback on the safety status of uploaded files, empowering them to take appropriate actions based on the analysis results.

All analysis outcomes are securely stored in an SQLite database, capturing essential metadata including file names, MD5 and SHA256 hashes, PE file information, and dynamic analysis results where applicable. This database serves as a repository for historical analysis data, enabling users to review past assessments and ensuring transparency and accountability in file handling practices.

The web interface dynamically presents analysis results to users, guiding them through the implications of each analysis finding and suggesting actionable steps based on the detected file type and its associated risk profile. This approach not only enhances user experience by providing clear and actionable insights but also promotes cybersecurity awareness and best practices among users.

By integrating advanced file analysis techniques with a responsive and intuitive user interface, this project aims to empower users, ranging from individual consumers to enterprise-level organizations, to make informed decisions regarding file safety and security. Ultimately, it contributes to a safer digital ecosystem by mitigating potential risks associated with malicious files and promoting proactive cybersecurity measures.

MANU C MADHU