Report

# **Project Title:** USB Sanitizer

Objective: The goal of this project is to enhance the security of USB drives by detecting and quarantining potentially harmful files automatically.

Scope: This tool is designed to be used on systems where USB drives are frequently connected, ensuring that any suspicious files are quickly isolated to prevent potential malware execution.

# Methodology:

1. **Initial Scan:** The tool performs an initial scan of the specified USB drive to detect any existing suspicious files.
2. **Real-time Monitoring:** Using the Watchdog library, the tool monitors the USB drive for any new files added.
3. **Detection and Quarantine:** Files matching predefined suspicious extensions or filenames are moved to a quarantine folder, ensuring that the USB drive remains clean.

# Results:

The USB Sanitizer successfully detected and quarantined all predefined suspicious files during both the initial scan and real-time monitoring phases. Logs were maintained for all detected files, providing a clear audit trail of the sanitization process.

# Conclusion:

The USB Sanitizer is an effective tool for maintaining the integrity of USB drives, providing automated detection and quarantine of suspicious files.