Project Abstract: Automated Reconnaissance Orchestrator (Phase 1)

Problem:
Security experts waste hours running various security tools manually to evaluate website vulnerability. Each of the tools has to be run individually, output copied by hand, and results summarized into reports - error-prone and time-consuming work.

Solution:

ARO integrates six well-known security tools into a single automated platform:

1. Input: Website domain (e.g., example.com)

2. Automated Process:

- Identifies all subdomains and associated websites
- Verifies what sites are actually up
- Uncover hidden web pages and documents
- Checks for known security issues

3. Results: Professional PDF report containing all results

Technology: Developed with Python for automation, Docker for easy installation, and adheres to industry-standard development principles such as version control and automated testing.

Main Benefits: Replaces 4-6 hours of manual labor with one command that takes minutes. Eliminates human errors while generating consistent, professional reports. Satisfies all academic project expectations including documentation and proper software development practices.

Impact: Makes professional security testing available to students and small enterprises. Provides foundation for advanced AI-enabled features in later development cycles.