PROJECT CHARTER

This innovative project, outlined in its detailed project charter, was conceived to provide security-conscious individuals and organizations with a clear, consolidated view of their public digital footprint. The core objective was to meticulously plan and execute the development of this secure web/app, ensuring its functionality met the highest standards for data accuracy and secure report delivery.

My responsibilities for this project charter were comprehensive, beginning with defining the project's precise scope and identifying the key functionalities required for the web/app's successful operation. I contributed to outlining the core features, such as data extraction mechanisms, report generation logic, and the secure PDF conversion process. I was also tasked with creating a **tactical project model** that detailed the web/app's phased development and deployment strategy, including technical specifications and resource allocation.

PROJECT TITLE

Domain dive- Beyond surface level viewing

PURPOSE / JUSTIFICATION OF THE PROJECT

Targets to increase the efficiency of the red team of Cycops by automating the gathering and structuring of the open-source intelligence (OSINT) that will be given a user-entered domain name or email address. The tool will cut the reconnaissance time by minimum of 50% and create a form of consistency in such a report as well as securely deliver findings in a password-protected PDF file, as it replaces the manual reconnaissance processes with an automated one. This is also in line with the mission of Cycops to carry out the high quality, efficient passive reconnaissance with the guarantee of the data security and adherence to privacy policies.

PROJECT OBJECTIVES

At the completion of the project (Week 7) the tool will:

- enable the user to enter a domain name or email address through a secure web interface that carries 100 percent uptime during the testing.

- Obtain OSINT information, containing at least five publicly available sources (e.g., WHOIS, DNS records, subdomains, data leaks) through 95 percent accuracy.

- Produce a benchmarked, analytical report within 5-minutes per query.

- Generate a secure password-protected PDF report with AES-256 compliant options attached.

- Allow downloading reports securely, including authentication and the HTTPS protocol, and have zero occurrence of unauthorized access during testing.

SCOPE

In Scope:

Creation of a user input interface at the web-based interface (domain/email).

- Unified with Internet hacker/exploit scanning tools (i.e., WHOIS, Shodan, HaveIBeenPwned).
- A computerized data gathering and formatting in a legible form.
- Password encrypted creation of PDF reports.
- User authentication and HTTPS (secure way of downloading).
- Simple user dashboard with the history of generating reports and downloads.

Beyond the Scope:

- Active real-time threat identification (e.g. Port scanning, vulnerability exploits).
- Access to own or paid OSINT data sources.
- Manual or human in the loop analysis of gathered data.
- Developing applications to use in mobile devices.

DELIVERABLES

- Web Application: A mobile-friendly, tamper-evident web application with authentication of the user (OAuth or an analog), input fields where user can enter domain/email, and view the history and status of reports.

- Integration with OSINT: minimum five OSINT APIs/sources, directly usable via the backend and supporting error handling in case of API failure.

- Report Generation Engine: It is a module to create a structured and branded PDF report based on OSINT data with AES-256 encryption and password protection assignable by users.

- Safe Download: Download is based on HTTPS and can only be accessed by authenticated users.

- User Documentation: A user guide that will include how to use the tool, the system requirements and problem solving.

- Test Report: A quality assurance report testing functionality, security and performance.

STAKEHOLDERS

- Project Sponsor: Grants funds, checks the milestones, and the answerability to the business goals (Cycops CTO).

- Red Team Users: The main end-users; they are the source of requirements, feedbacks and input on usability testing.

- Development Team: Does the designing, coding and deployment of the tool, does the technical requirements.

- QA Team: Offers functional, security and usability testing services; delivers on success criteria of deliverables.

- Security Team: Reports on the applied encryption and authentication mechanism to have compliance with the security standards.

RISKS AND MITIGATION

- Risk: Public APIs of OSINT have low availability or reliability.
  Mitigation: Choose a multi-backup APIs, and use error handling mechanism.

- Risk: Risk of data privacy on OSINT collected data.
  Mitigation: Make sure that GDPR and other laws are met

- Risk: There is a security risk of web interface or download process.
  Mitigation: Scan the penetration testing and OWASP good practices.

- Risk: Lack of timely delivery since integration may be difficult.
  Mitigation: Choose to allocate buffer time in Weeks 2-3, modular development shall be prioritized.