# Project Proposal: Open-Source OSINT Tool for Investigators

[AUSAINT]

March 7, 2025

## 1 Team Information

- **Team Name:** [AUSAINT]
- **Team Members:**
  1. Afnan Bin Abbas 2022048
  2. Muhammad Umar Maqsood 2022447
  3. Shamina Durrani 2022543
  4. Aqib Shakeel 2022104
- **GitHub Repository Link:** `https://github.com/shaminadurrani03/AUSAINT.git`

## 2 Title & Project Proposal

### 2.1 Project Title

**OSINT Investigative Suite: A Secure Open-Source Intelligence Gathering Tool**

### 2.2 Abstract

With the rise in cyber threats such as phishing, credential leaks, and domain impersonation attacks, organizations and individuals need a reliable way to gather intelligence on email addresses and domains. Many OSINT tools exist but are either too complex, require premium access, or are not user-friendly. Our project aims to develop a free, accessible, and secure web-based OSINT tool to gather intelligence from open sources while ensuring data security.

### 2.3 Core Features

- **Social Media Intelligence (SOCMINT):** Profile lookups, leaks detection
- **IP & Domain Intelligence:** WHOIS, geolocation, DNS analysis
- **Email & Phone OSINT:** Leak checks, validity checks
- **Web Scraping for OSINT:** Identifying exposed sensitive files, subdomains
- **Secure Reporting System:** PDF reports, data visualization

## 3 Security Requirements & Planning

### 3.1 Security Objectives

1. **Data Integrity:** Ensure collected intelligence is not modified during retrieval.
2. **User Privacy Protection:** Prevent unauthorized data logging or leaks.

3. **Access Control:** Implement authentication for privileged OSINT queries.
4. **Secure API Integrations:** Utilize only vetted, free, and secure APIs.
5. **Threat Mitigation:** Implement protection against **injection attacks, brute force, and API abuse.**

### 3.2 Planned Security Measures

- **Input Validation:** Prevent SQL injections and XSS attacks.
- **Rate Limiting & API Key Protection:** Prevent API abuse.
- **Authentication & Role-Based Access Control:** Limit access to sensitive features.
- **Logging & Anomaly Detection:** Track suspicious activities.
- **Encrypted Database Storage:** Securely store retrieved intelligence.

### 3.3 Technology Stack

- **Frontend:** HTML, CSS, JavaScript (React.js for UI)
- **Backend:** Flask (Python-based API service)
- **Database:** PostgreSQL (for storing intelligence results securely)
- **OSINT Modules:** Open-source libraries (Sherlock, Twint, Sublist3r, WHOIS, etc.)

## 4 Expected Deliverables & Milestones

| Week | Deliverables |
|---|---|
| Week 1 | Project Proposal, Security Planning, GitHub Repository Setup |
| Week 2 | Threat Modeling & Risk Assessment Report |
| Week 3 | System Architecture & Secure Design Diagrams |
| Weeks 4-6 | Secure Coding & Initial Feature Implementation |
| Week 7 | Security Testing, Vulnerability Analysis |
| Week 8 | Secure Code Review, Final Security Enhancements |
| Week 9 | Final Report, Source Code, Live Demo & Presentation |

## 5 Conclusion

This OSINT web application will provide an easy-to-use, free, and secure platform for cybersecurity professionals, researchers, and users to gather intelligence on email addresses and domains. The project integrates multiple free OSINT tools, follows secure software development principles, and ensures ethical use of collected data.