Project Overview

What This Tool Does

I built a Python-based email security analyzer that integrates five different third-party APIs to provide phishing and domain reputation analysis.

This tool automates a large part of the email analysis workflow by querying VirusTotal, AbuseIPDB, WhoisXML, Google Custom Search, and DNS servers simultaneously, then aggregating findings into a single analysis report.

Core Analysis Functions

The analyzer handles four main security checks that cover different attack vectors:

- Header analysis extracting sender information and validating SPF/DMARC records
- Domain intelligence retrieving WHOIS data and ownership details
- Blocklist verification checking domains and IPs against reputation databases
- Authentication validation confirming SPF and DMARC configuration through DNS

Each function targets specific phishing indicators. Header analysis catches domain spoofing attempts, domain intelligence reveals newly registered domains commonly used in phishing campaigns, blocklist checks identify known malicious infrastructure, and authentication validation confirms legitimate senders have proper email security configured.

Security Implementation

The current implementation stores API keys in code for development convenience, but production deployments would move these to environment variables or dedicated secrets management. This separation prevents credential exposure in version control while maintaining easy local development.

Primary Use Cases

I built this tool to address specific security operations scenarios in my daily work:

- Phishing investigation for rapid assessment of suspicious emails
- Domain assessment evaluating new or suspicious domains via registration history
- Authentication validation verifying SPF and DMARC configuration

Planned Enhancements

Several features would extend the tool's capabilities:

- Secure API key storage
- Email attachment analysis using VirusTotal file scanning

- URL scanning and reputation checking for embedded links
- Rate limiting controls for API quota management
- Web-based interface for non-technical users

The modular architecture makes these enhancements straightforward to implement. Each API integration operates independently, so adding new capabilities doesn't require refactoring existing functionality.

Why This Project Matters

This project demonstrates several key security engineering skills:

- API integration across multiple security intelligence platforms
- Data aggregation from disparate sources into unified analysis
- Security tool development solving real SOC workflow problems