Exploring PhishTank for Phishing Detection
Final Report
Cyber Security

Name: K. Manmohan Rathod
Program Name: Phishing Detection Tool – CS Tool Exploration
Date: 09/01/2025
GitHub Repository: https://github.com/irathod/phishtank-exploration

Exploring PhishTank for Phishing Detection – Final Report

Project Overview

The goal of this project was to explore and implement the **PhishTank open-source phishing detection database** to identify malicious URLs and protect users from phishing attacks. The objective was to analyze suspicious links, flag phishing attempts using heuristics, and provide actionable feedback to enhance user awareness.

Technologies & Tools Used

- PhishTank API: Open-source phishing database for URL verification
- Python: Backend implementation
- Streamlit: Web interface for real-time URL scanning
- Git & GitHub: Version control and repository hosting

System Architecture

1. URL Input: Users enter a suspicious URL through the Streamlit interface.
2. Heuristic Analysis: Detects phishing indicators (e.g., '@' symbol, missing HTTPS, IP domain).
3. PhishTank Verification: Cross-checks URL with the PhishTank database.
4. Result Display: Shows verdict (Legitimate, Suspicious, Phishing) and reasons for flagging.

Security Features

- Real-time phishing detection
- Uses PhishTank’s continuously updated phishing database
- No sensitive data storage
- Clear, user-friendly interface with actionable advice

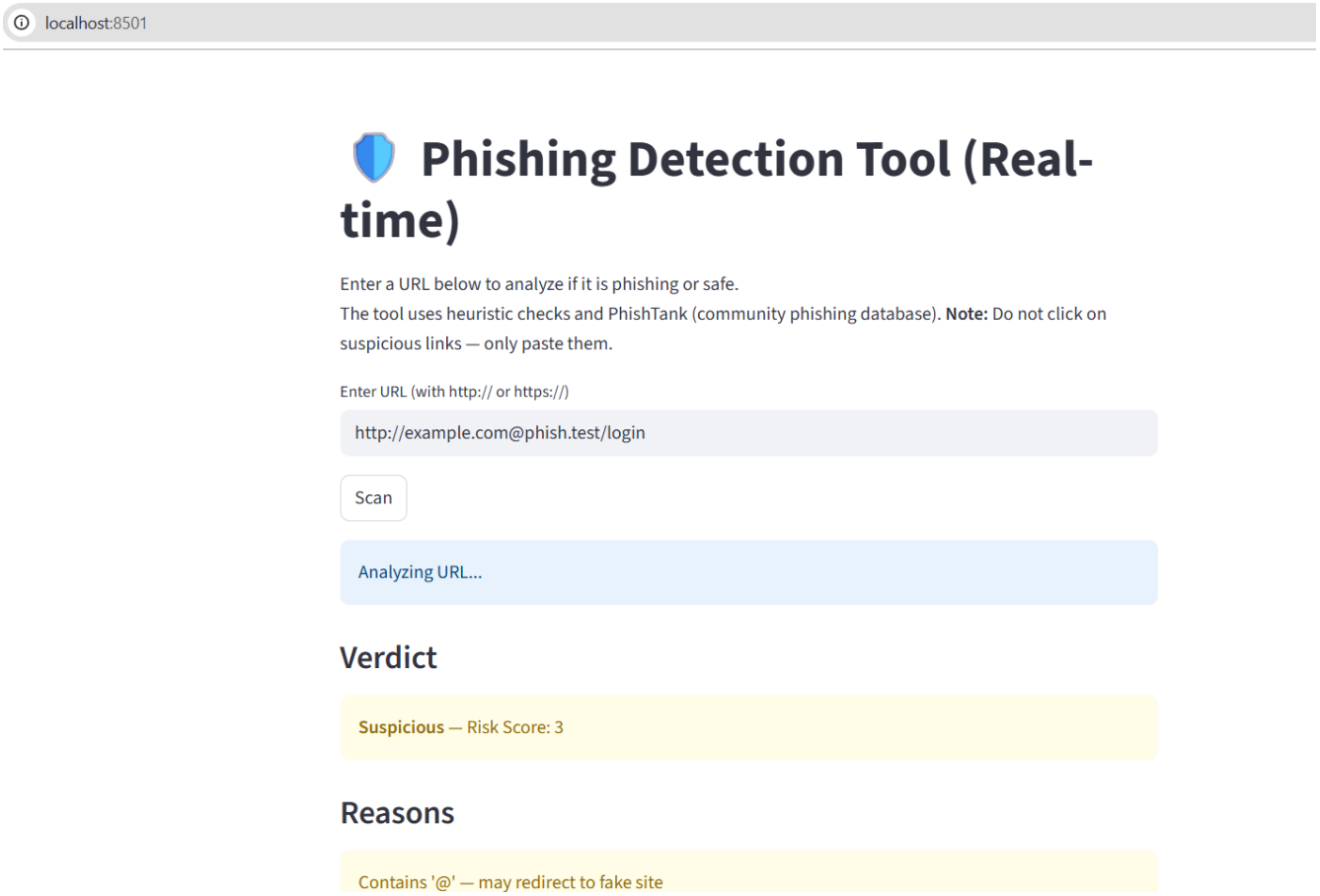
Folder Structure

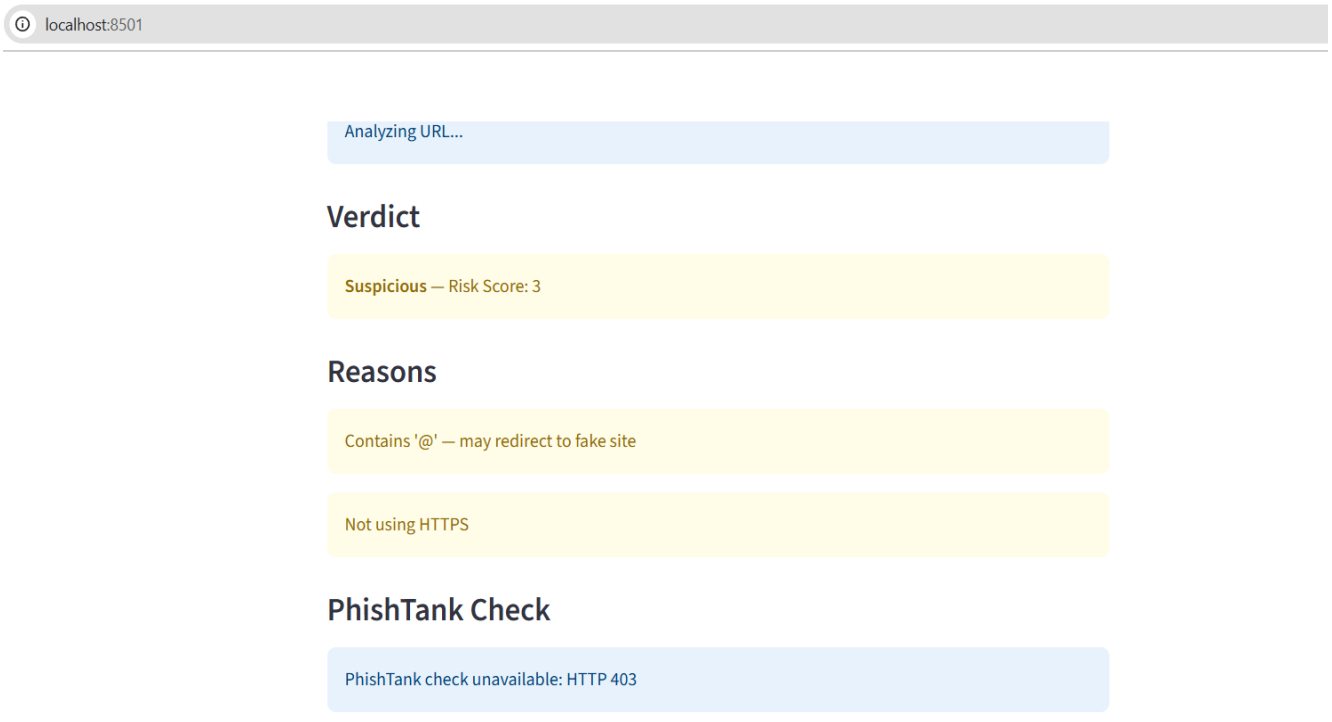
```
phishtank-exploration/
├── app.py                          # Main Streamlit application
├── heuristics.py                   # Heuristic analysis for phishing indicators
├── requirements.txt                # Python dependencies
├── README.md                       # Project documentation
├── screenshots/                    # Folder for screenshots
│   ├── app_result.png              # Phishing detection result
│   └── interface.png               # Tool interface screenshot (if any)
└── Phishing_Detection_Report.pdf # Final project report
```

Screenshots

1. Tool Interface

2. Detection Result





Testing & Results

- Tested using phishing and legitimate URLs.
- Tool successfully identified suspicious URLs based on heuristic scores and PhishTank results.
- Users receive real-time alerts and actionable recommendations.

Deliverables

- GitHub repository containing the code and documentation.
- Screenshots demonstrating tool functionality.
- Final report summarizing project and findings.

Learning Outcomes

- Practical experience integrating a real-world phishing detection API.
- Understanding of heuristic-based URL analysis.
- Hands-on practice with GitHub, Python, and Streamlit for cybersecurity applications.

Conclusion

This project successfully demonstrates how PhishTank can be integrated into a simple phishing detection tool to provide real-time alerts and educate users about phishing threats. The implementation can be extended for organizational use to monitor corporate email and web traffic for malicious links.