

Phishing URL Scanner - Python Project Report



Author: HIMANSI

1. Introduction

Phishing attacks are a growing cybersecurity threat. This project aims to help users identify suspicious URLs using real-time analysis powered by VirusTotal API.

2. Technologies Used

- Python - Core programming language
- Tkinter - GUI interface
- Regex (re) - URL validation
- tldextract - Domain extraction
- requests - API communication
- CSV - Data logging
- os/dotenv - Secure API key handling

3. Backend Logic Flow

- 1. Start GUI (Tkinter)
- 2. User submits URL
- 3. Validate URL using regex
- 4. Extract domain using tldextract
- 5. Check existing CSV log
- 6. Call VirusTotal API if not found
- 7. Analyze API response
- 8. Display result in GUI
- 9. Log the result into scan_log.csv

4. Sample Log Output

Timestamp | URL | Domain |

Status 2025-06-10 12:34:56 | http://abc.com/test | abc.com | Safe

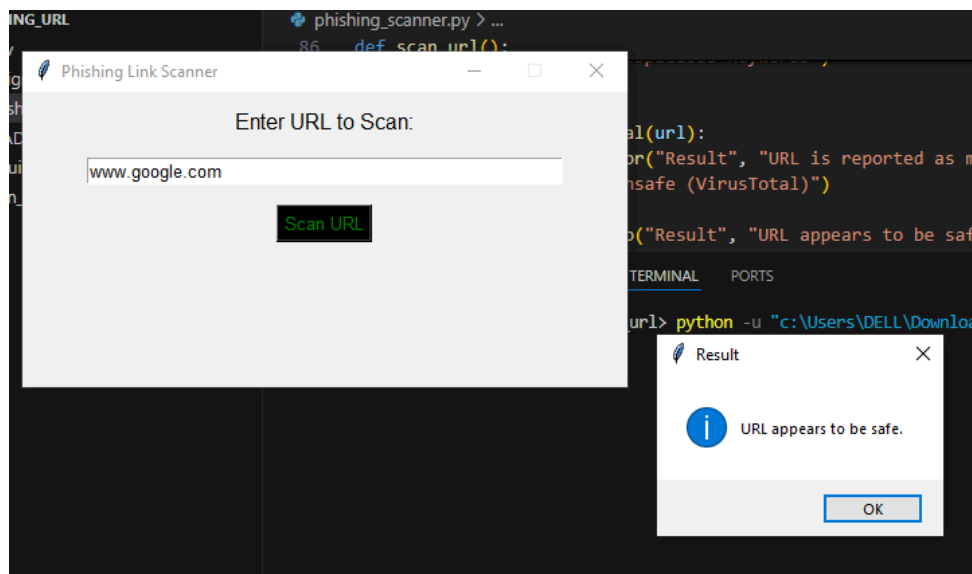
5. Future Improvements

- - Add email alerts for malicious URLs
- - Add support for batch scanning
- - Visual analytics dashboard

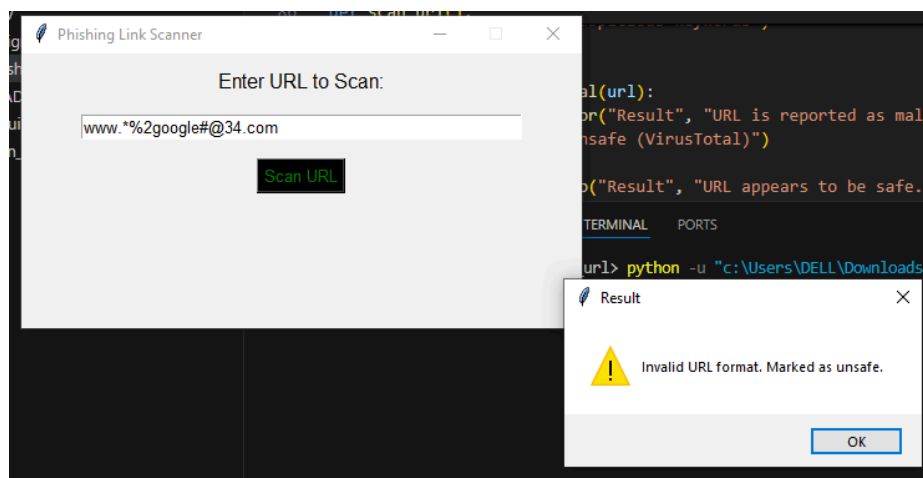
6. Conclusion

- This tool simplifies the process of detecting potentially harmful links and strengthens cybersecurity awareness for everyday users.

screenshot



2.



3.

```
1 2025-06-10 10:36:12,jijijijij,Invalid URL
2 2025-06-10 11:27:30,www.google.com,Safe
3 2025-06-10 11:28:10,www.*%2google#@34.com,Invalid URL
4
```