Email Anlayzer

PRESENTATION OF PROJECT WORK

BY:-

PRIYA KUMARI : 2100460100085
SUHANI YADAV : 2100460100109
Harsh Katiyar : 2100460100053
Anupam : 2100460100023
Harsh Kumar Gupta : 2200460109010

UNDER GUIDANCE OF :-

NAME OF GUIDE : NEETU KUMARI

Outlines

- Introduction
- Literature Survey
- Inferences from Literature Survey
- Comparative Analysis of Existing Systems
- Problem Statement
- Solution Approach
- Methodology
- Real-World Applications
- Software and Hardware Requirements
- Modules and Architectural Description
- Project Progress Status
- References

START

Introduction:

Objective:

To develop a Python Django-based web app to analyze email headers, check for spoofing and dns records, and scan URLs/attachments using the VirusTotal API with google gemini chatbot intergration.

Key Features:

Parse and extract sender details.

Analyze header information for spoofing elements.

Integrate threat analysis using VirusTotal API.

User-friendly interface for results visualization.

START

Literature Survey

Tool A: Detects email spoofing through email headers.

- Technique: SPF, DKIM, and DMARC validation.
- Example: Tools like MXToolbox or Postmark.

Tool B: Scans URLs and attachments for threats.

- Technique: Signature-based malware detection using VirusTotal or other static analysis tools.
- Example: VirusTotal Scanner.

Tool C: Visualizes email headers for easier analysis.

- Technique: Graphical visualization of email paths and server hops.
- Example: Google's Message Header Analyzer.

Inferences Drawn from Literature Survey

Tool A: Detects email spoofing through email headers.

- Technique: SPF, DKIM, and DMARC validation.
- Example: Tools like MXToolbox or Postmark.

Tool B: Scans URLs and attachments for threats.

- Technique: Signature-based malware detection using VirusTotal or other static analysis tools.
- Example: VirusTotal Scanner.

Tool C: Visualizes email headers for easier analysis.

- Technique: Graphical visualization of email paths and server hops.
- Example: Google's Message Header Analyzer.

Comparative Analysis of Existing Systems

Feature	Tool A	Tool B	Tool C	Email Analyzer
DNS / Spoof Check	✅	❌	✅	✅
Threat Analysis	❌	✅	❌	✅
Header Parsing	❌	❌	✅	✅
User-Friendly UI	❌	✅	✅	✅

START

Problem Statement

Shortcomings of Existing Systems:

- Lack of integration between email parsing and threat analysis.

Limited usability for non-technical users.

Proposed Solution:

- Develop a unified tool combining email header parsing, spoof detection, dns check and threat analysis.

START

Solution Approach

Email Header Parsing:

Extract and analyze sender, recipient, and server details.

Spoof Check:

Validate SPF, DKIM, and DMARC records.

DNS Check:

Validate sender's domain through DNS lookups.

Frontend Development:

- Create an interactive interface for result visualization.
- Chatbot integration for any queries and help.

START

Tools:

- Backend: Python, Django
- API: VirusTotal, Google Gemini
- Frontend: HTML, CSS, JavaScript

Methodology

1. Upload email file(.eml format).
2. Parse and analyze data
3. Check SPF/DKIM/DMARC records and other various headers.
4. Scan URLs/attachments with VirusTotal.
5. Display results in the UI.

START

Real-World Applications

Benefits:

- Enhanced email security for organizations.
- Protection against phishing and malware attacks.

Target Users:

- Cybersecurity teams.
- Enterprises handling sensitive information.

Problem Solved:

- Organizations wanting to analyze suspicious emails.

Software and Hardware Requirements

Software:

- Python 3. x
- Django Framework
- VirusTotal API
- Google Gimini API

Hardware:

- RAM: 1–2 GB
- CPU: Modern dual-core processor.
- Storage: 20 GB free space for dependencies, database, and logs.

START

Modules and Architectural Description

Modules:

Email Parser: Extract header data.
DNS / Spoof Check: Validate SPF, DKIM, DMARC And DNS Record
Threat Scanner: Interface with VirusTotal API.
Chatbot : Google Gimini
Frontend: Display results.

Architecture:

Modular Django-based architecture with REST APIs.

Project Progress Status

Completed:

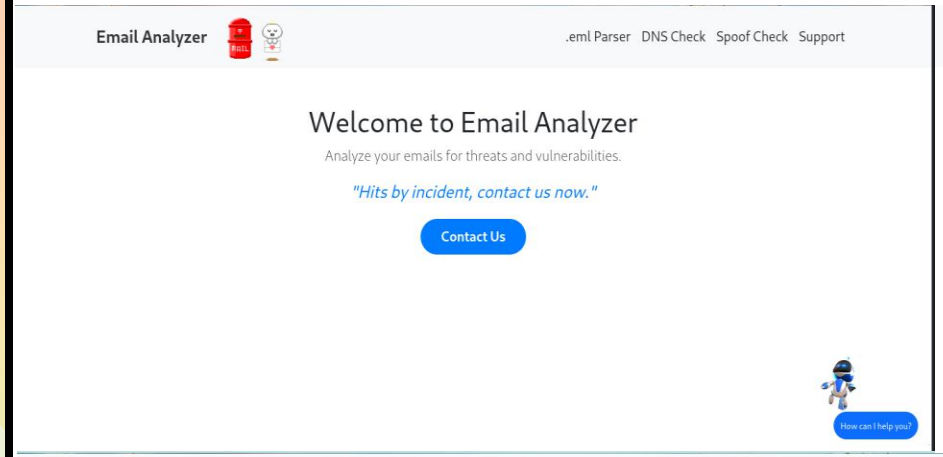
- Header parsing and spoof checking(Basic).
- VirusTotal integration for threat analysis
Chatbot for help and support.

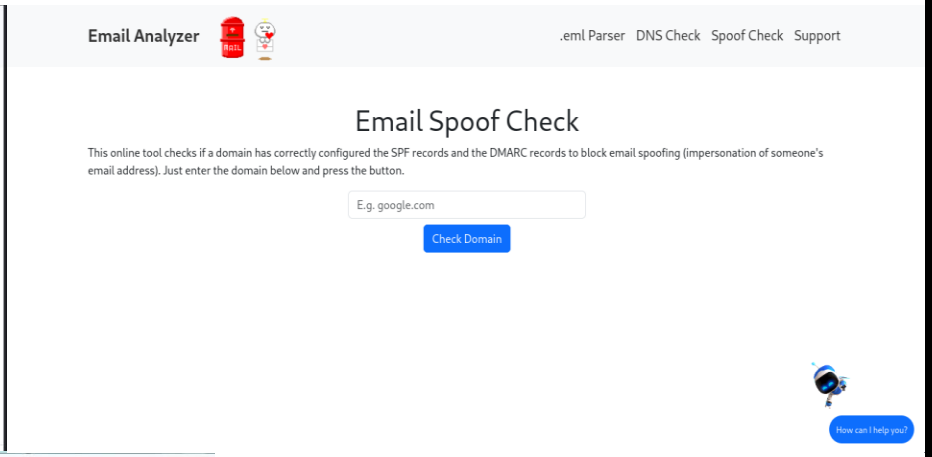
Pending:

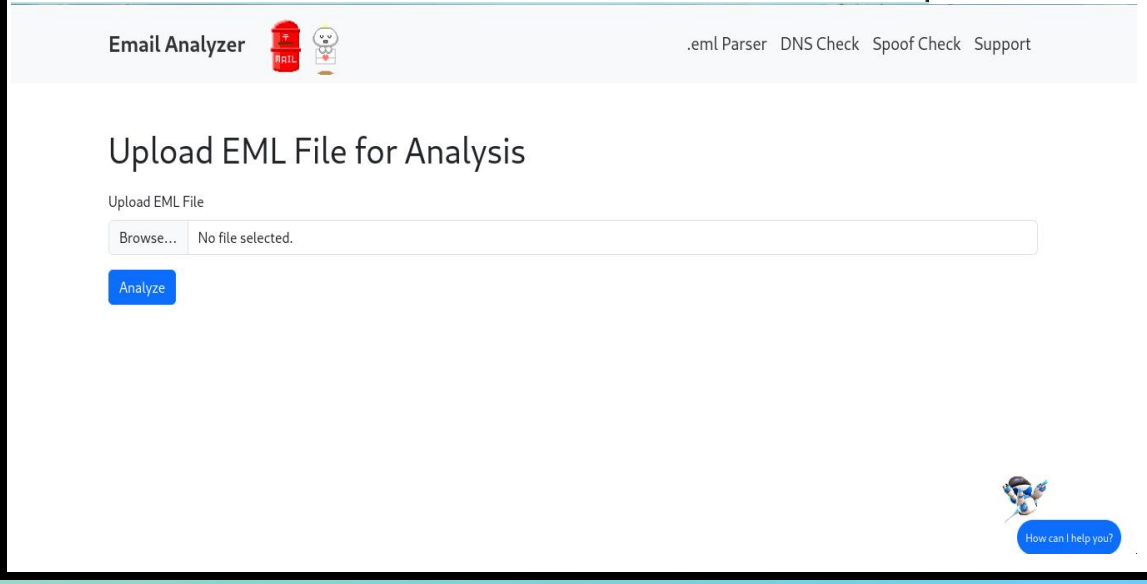
Header parsing and spoof checking(Robust).

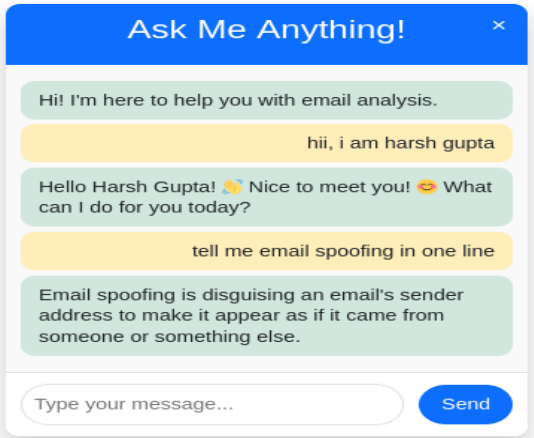
- Finalizing frontend UI.
- Testing and debugging.

Snapshot of project progress status









Thank you