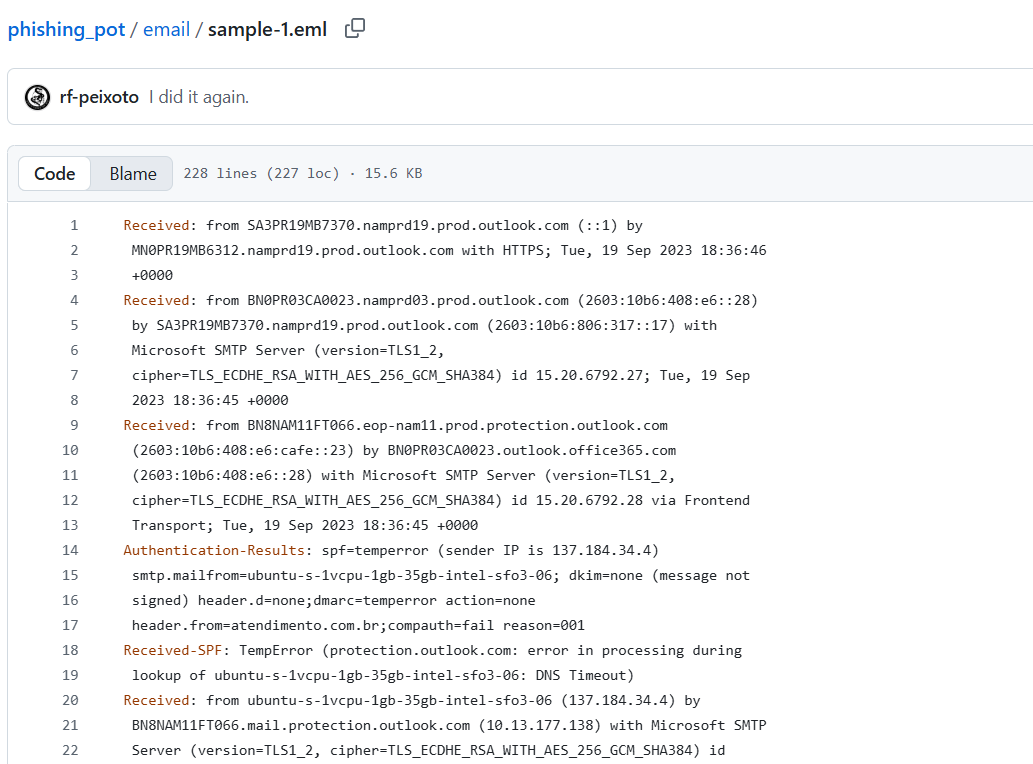
**TASK – 2**

**Cybersecurity Intern**

Madhav P Rajeev

[Madhavrajeev93@gmail.com](mailto:Madhavrajeev93@gmail.com)

**Analyse Phishing email sample**

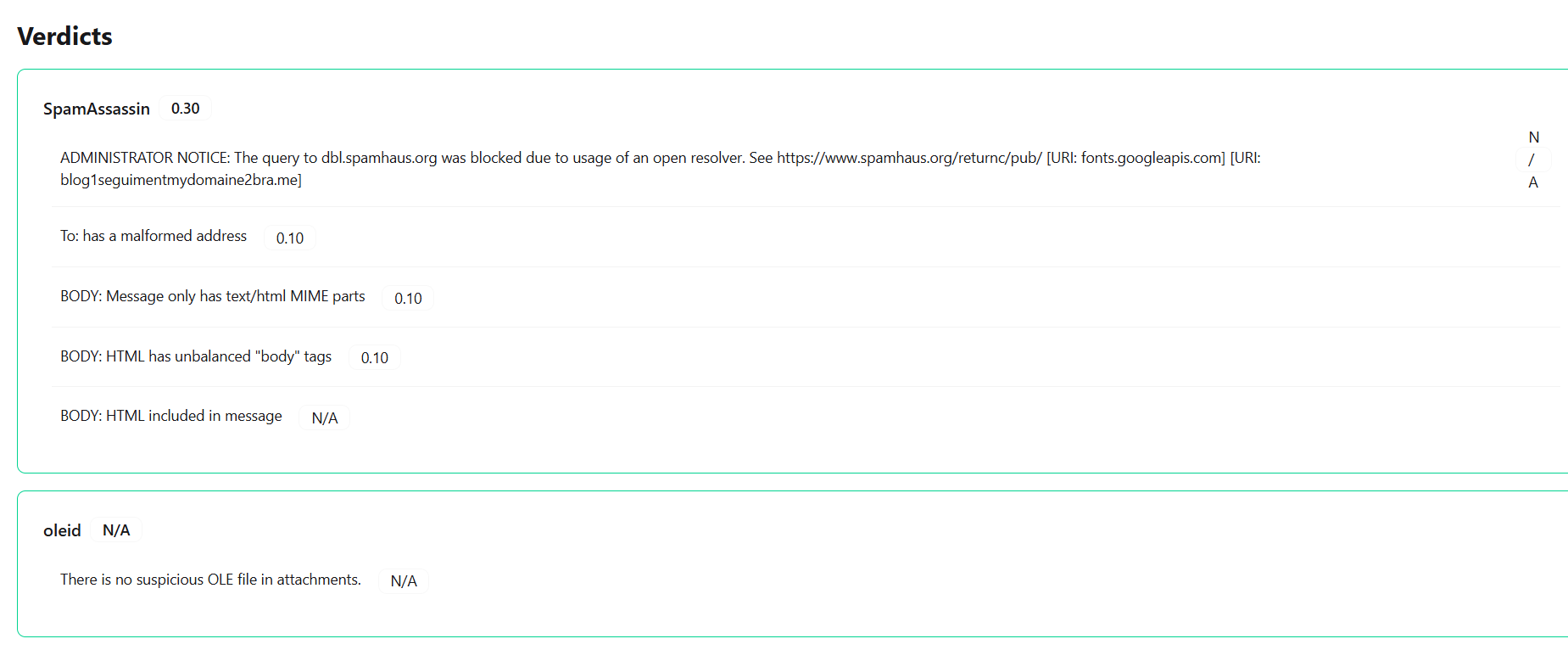
****

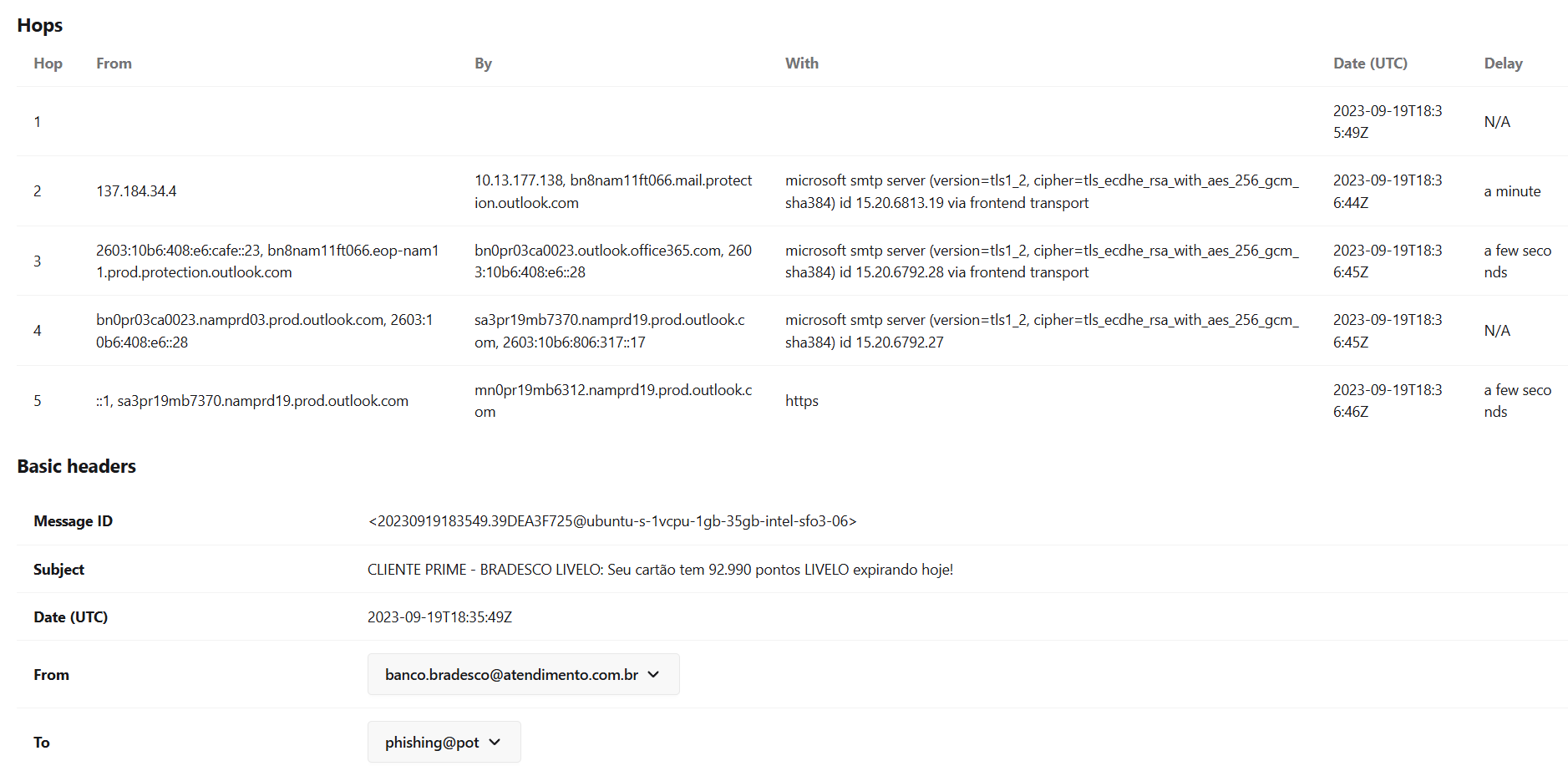
Sample Mail for Analysis

**Tool used for analysis:**

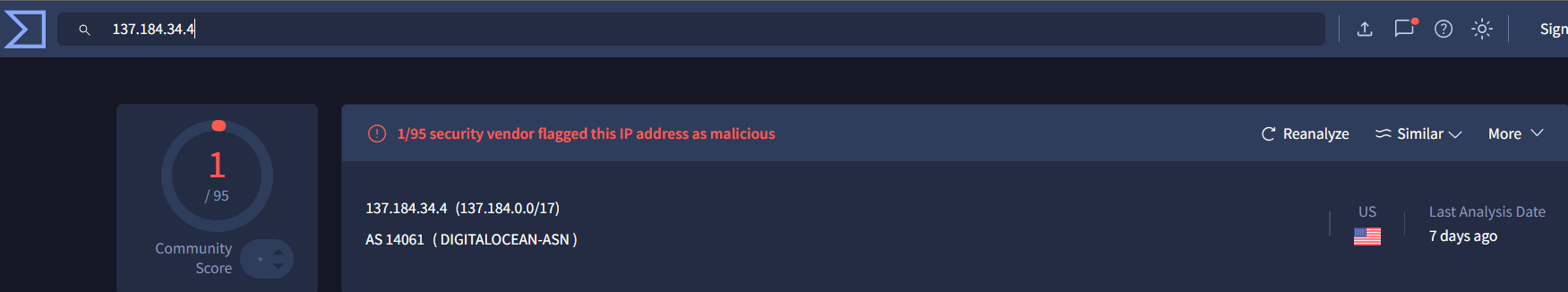
<https://eml-analyzer.herokuapp.com/#/>

**Results:**

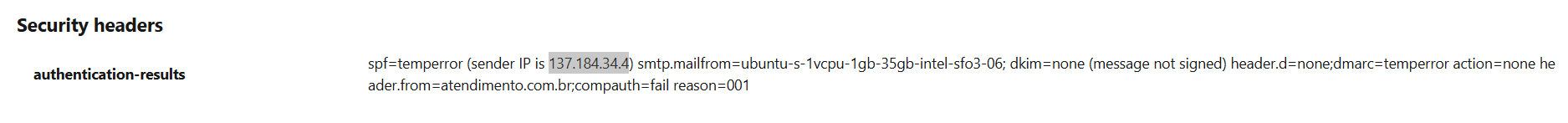




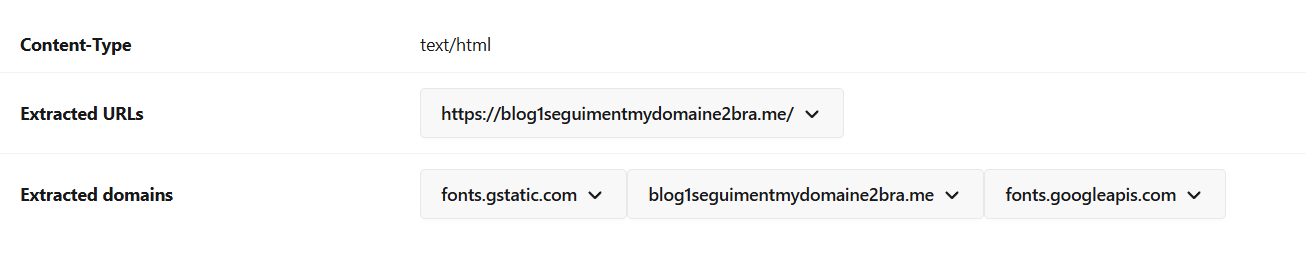
**Senders IP blacklisting :**

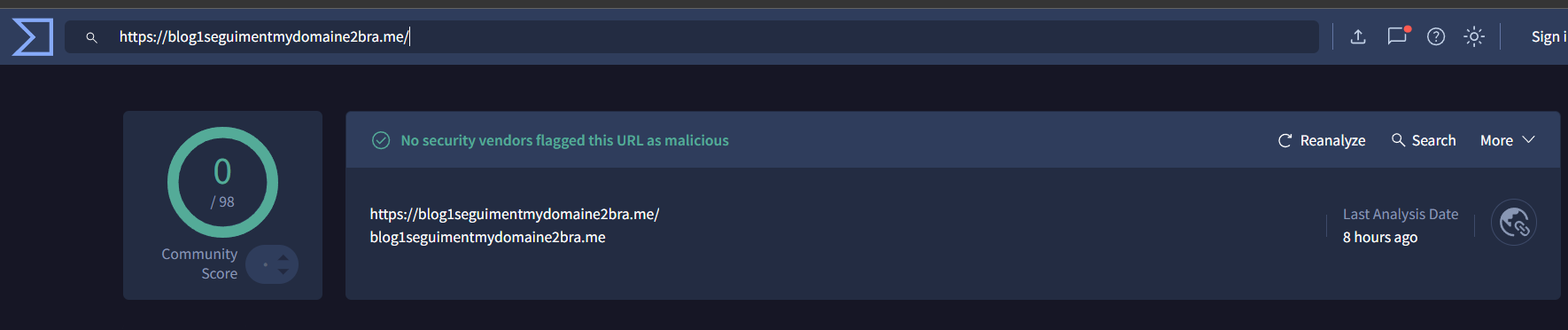


**Authentication Result :**



**Extracted Email:**





Not found suspicious

**Summary:**

In this project, I obtained a sample phishing email from GitHub and conducted a detailed analysis using an EML analyzer. The focus was on examining the email’s metadata, attachments, sender information, and embedded URLs to assess its potential malicious nature.

The analysis revealed that the email did not contain any suspicious OLE (Object Linking and Embedding) files, which are often leveraged by attackers to deliver malware payloads. The sender’s IP address was cross-verified on VirusTotal and found to be blacklisted by only 1 out of 95 security vendors, indicating a relatively low risk score. Additionally, the email contained a single embedded URL, which was also scanned using VirusTotal and determined to be non-malicious by all vendors.

Overall, the findings suggest that while the email was classified as a phishing sample, the specific instance analyzed exhibited minimal immediate indicators of compromise. This highlights the importance of comprehensive multi-layered analysis—evaluating headers, attachments, IP reputation, and URLs—before drawing conclusions about the threat level of an email.