Email OSINT Investigation Report

Target Type: Email Address
Target Value: bandarunithish490@gmail.com

Objective
To analyze publicly available information and breach exposure associated with the target email address using open-source intelligence techniques.

OSINT Methodology
- Breach exposure analysis using Have I Been Pwned
- Public search engine analysis
- Developer platform and paste site enumeration
- Threat and risk assessment based on exposure

Findings
The target email address was identified in one publicly reported data breach. The breach originated from the platform Cutout.Pro in February 2024.

Breach Details
- Breached Service: Cutout.Pro
- Breach Date: February 2024
- Compromised Data: Email addresses, IP addresses, names, passwords (salted MD5 hashes)

Public Exposure Analysis
Search engine and platform-specific OSINT checks were conducted across general search engines, GitHub, and paste-sharing platforms. No publicly indexed profiles, repositories, or credential leaks were identified beyond the reported breach.

Security Implications
Exposure of the email address increases the risk of phishing and social engineering attacks. The presence of hashed passwords increases credential-stuffing risk if password reuse exists.

Conclusion
This investigation demonstrates how OSINT techniques can be used to assess digital exposure and security risks associated with an email address using publicly available information.