Passive Reconnaissance Report

Target: vulnweb.com

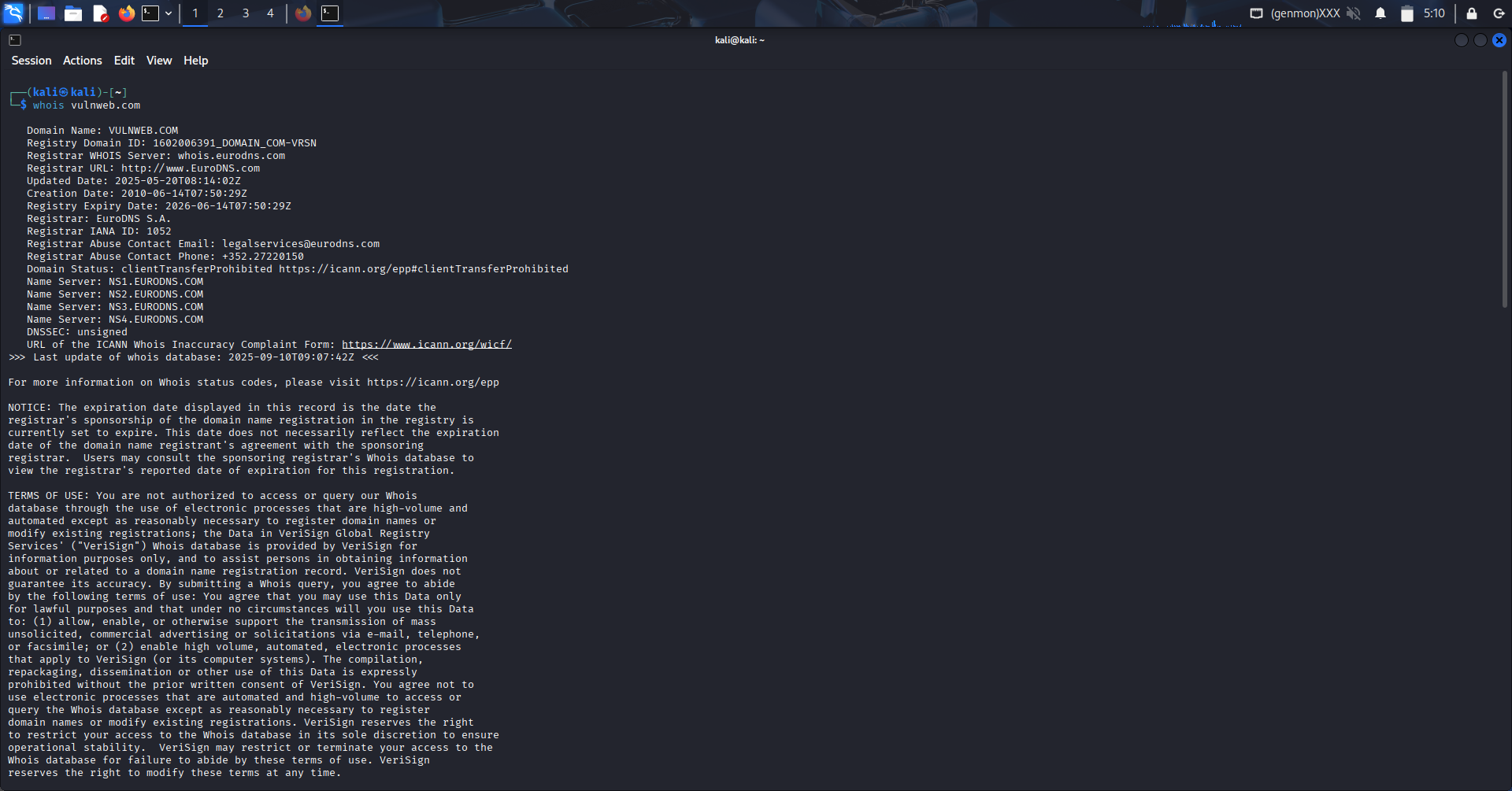
1. Target Domain Name Chosen

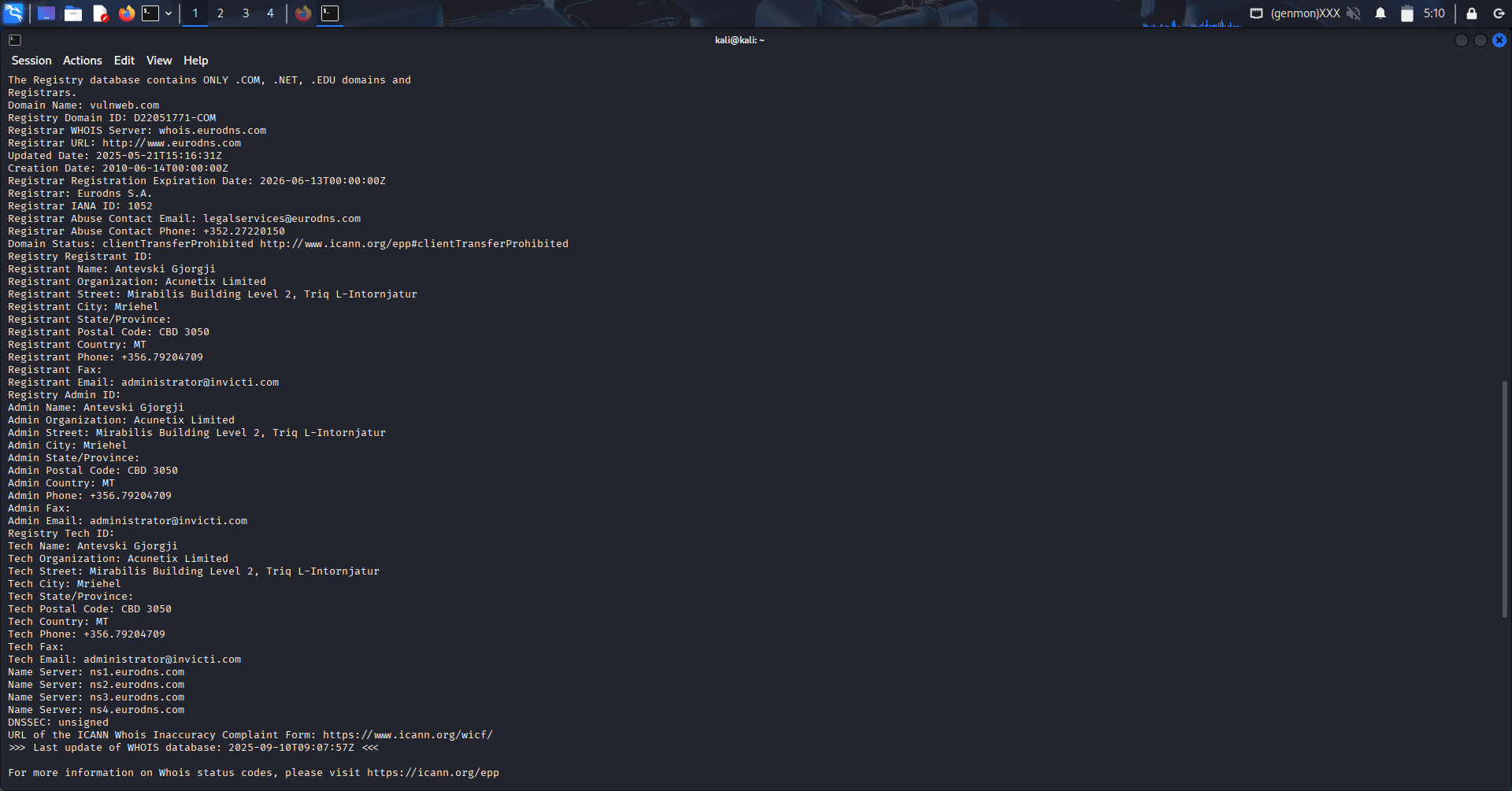
The target domain selected for passive reconnaissance is:

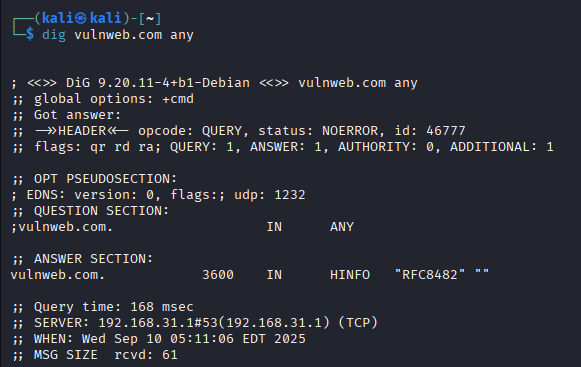
vulnweb.com

# 2. WHOIS & DNS Findings

The following screenshots show WHOIS information and DNS records for the target:

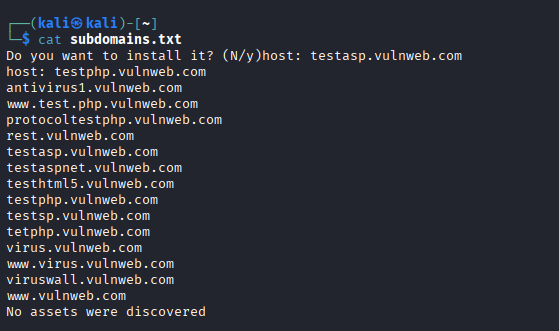






# 3. Subdomains Discovered

The reconnaissance identified the following subdomains:



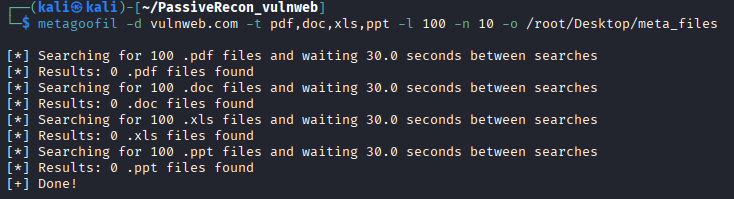
# 4. Email IDs or Employee Data

The following screenshot shows email IDs or employee-related information identified:



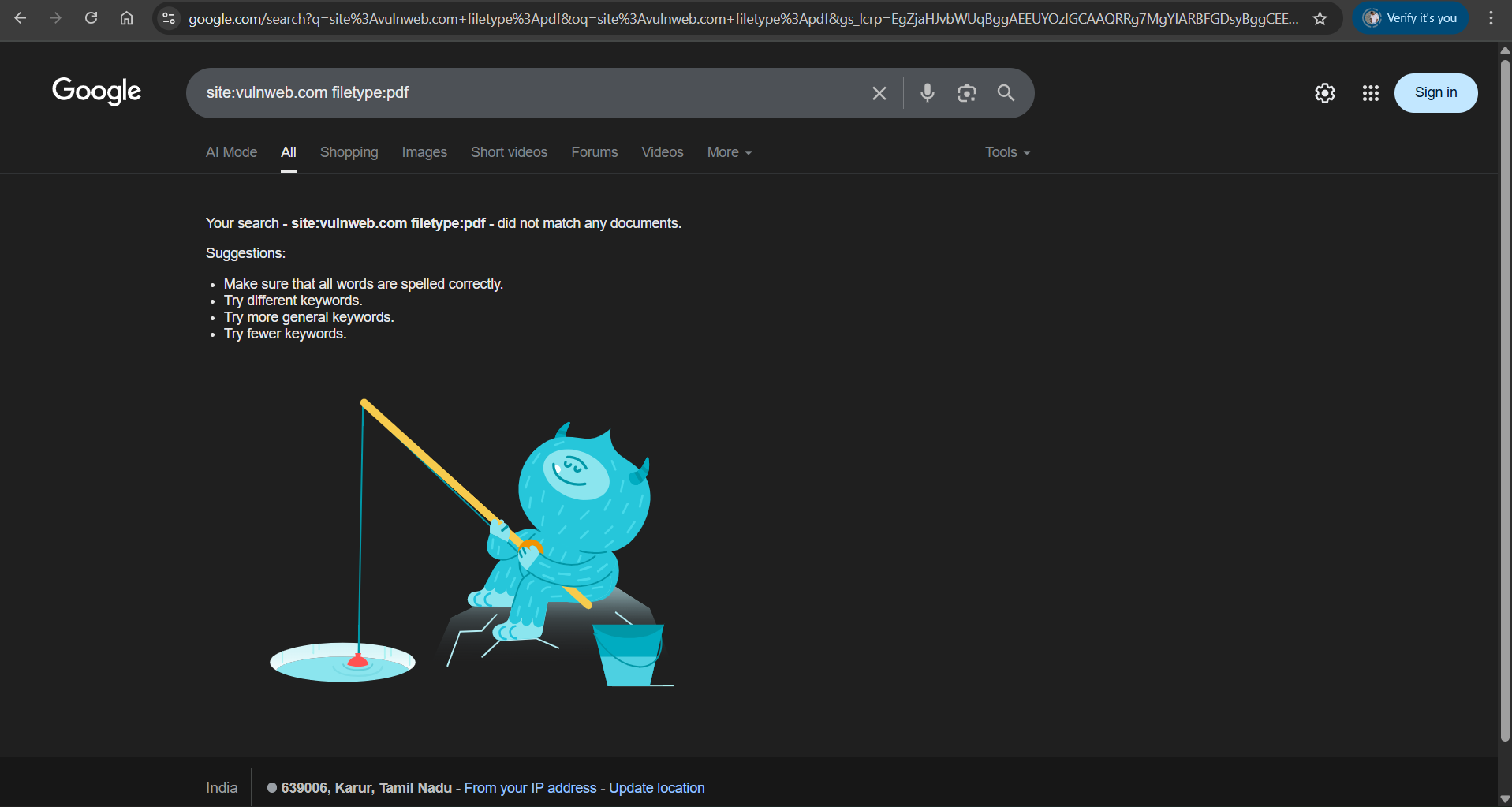
# 5. Metadata Information

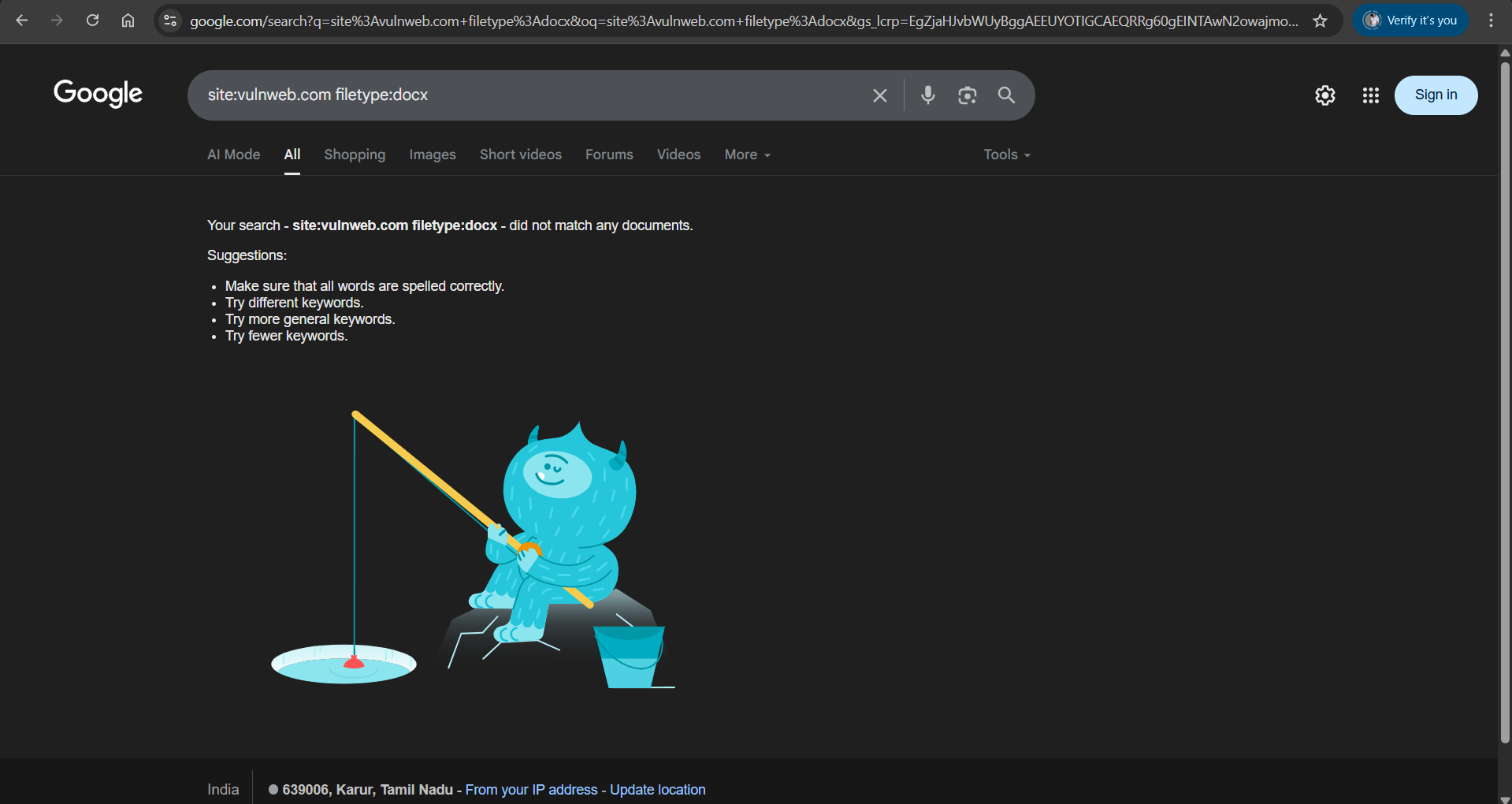
The following screenshot shows extracted metadata from public files:

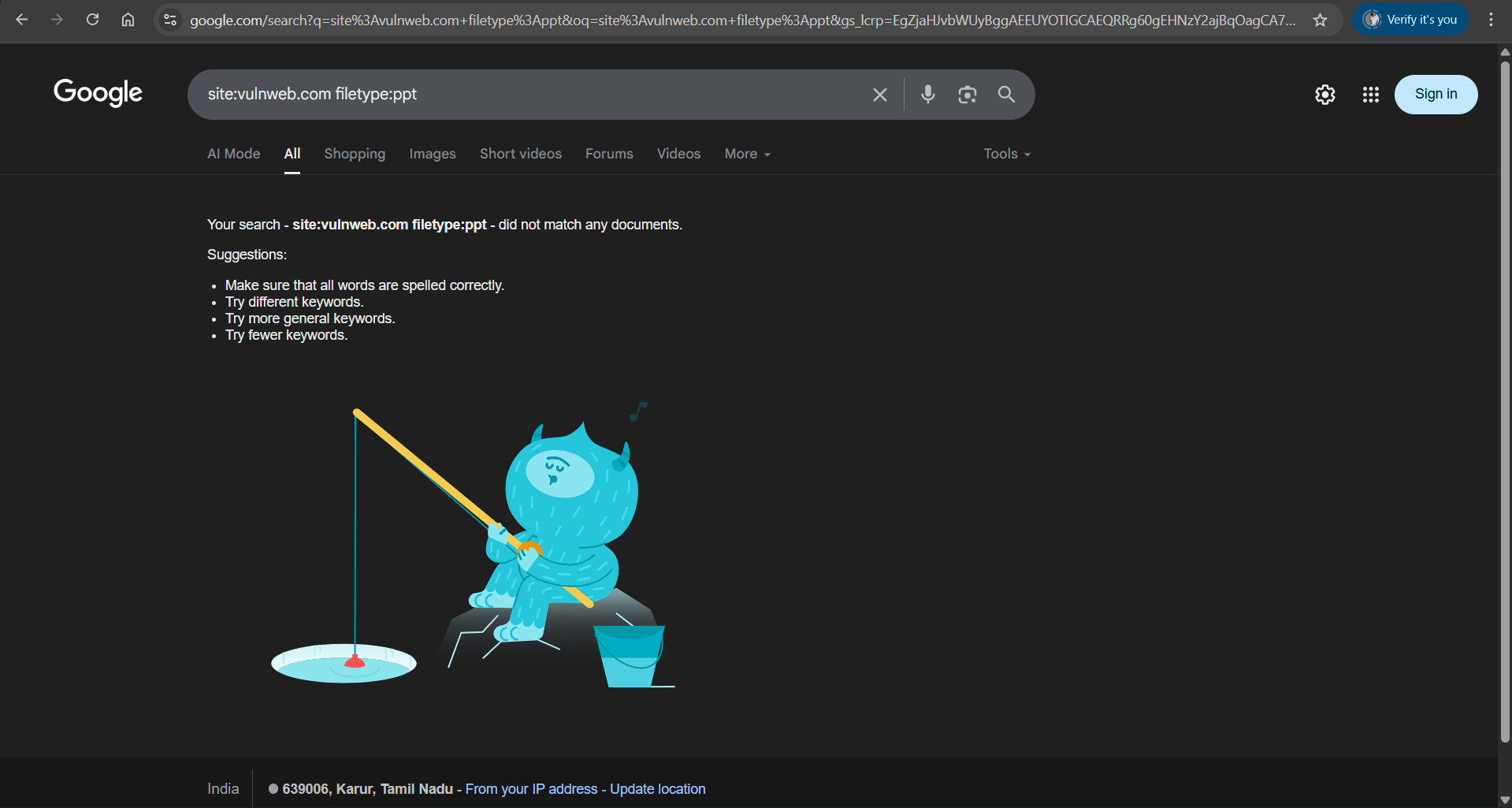


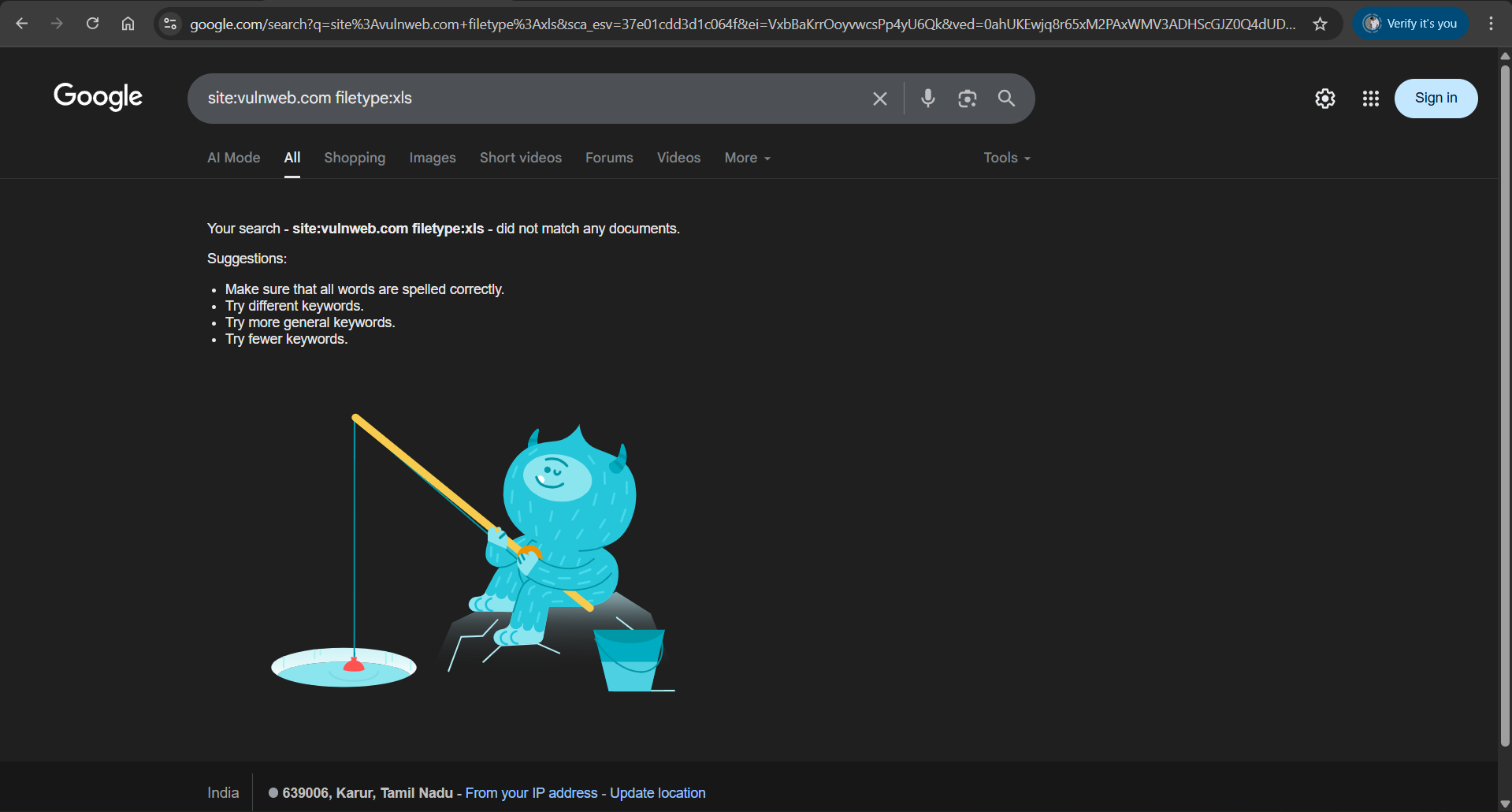
# 6. Google Dorks Attempted (with results)

Google dorking attempts were made to identify sensitive information. Results are shown below:



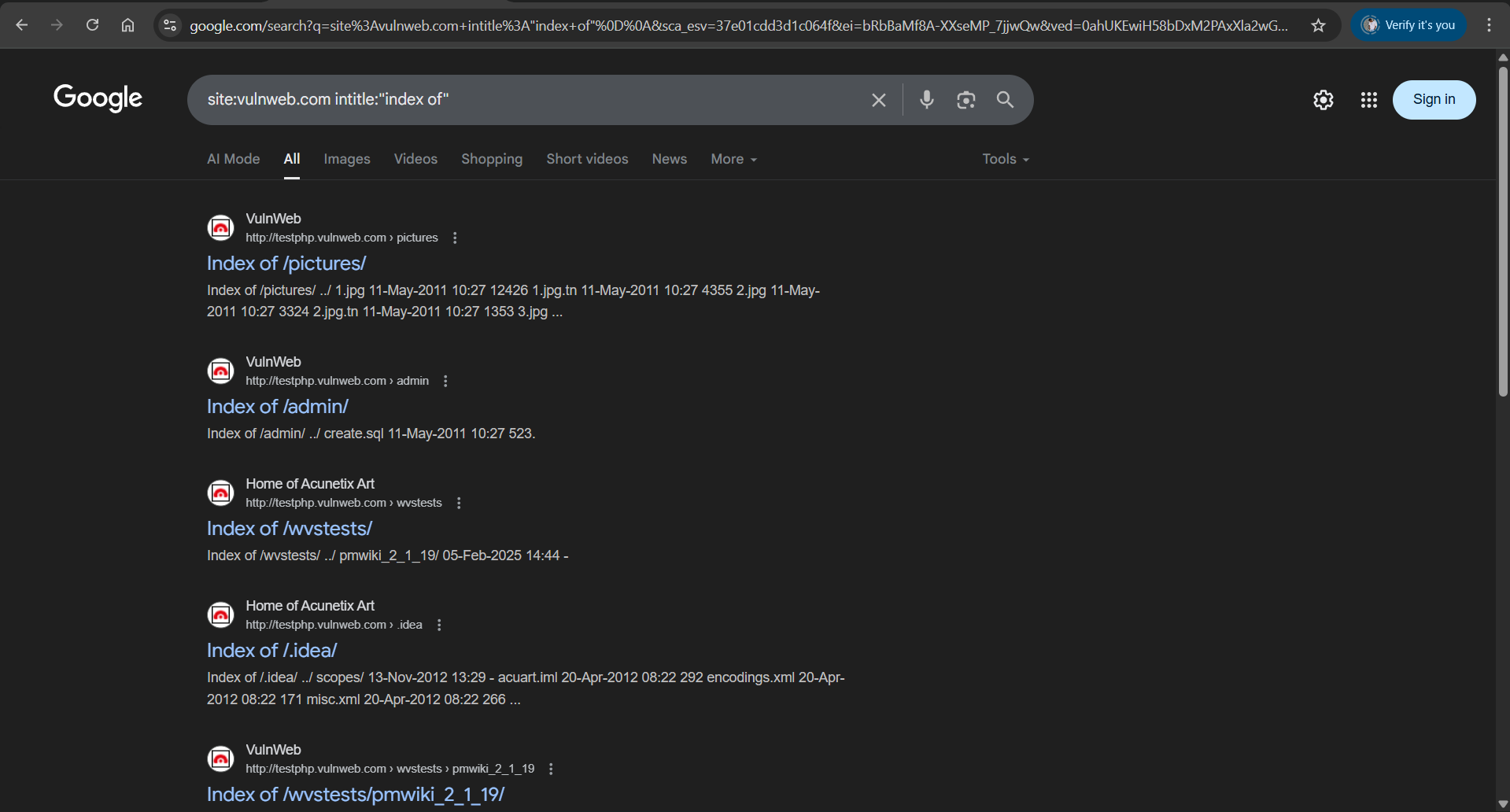


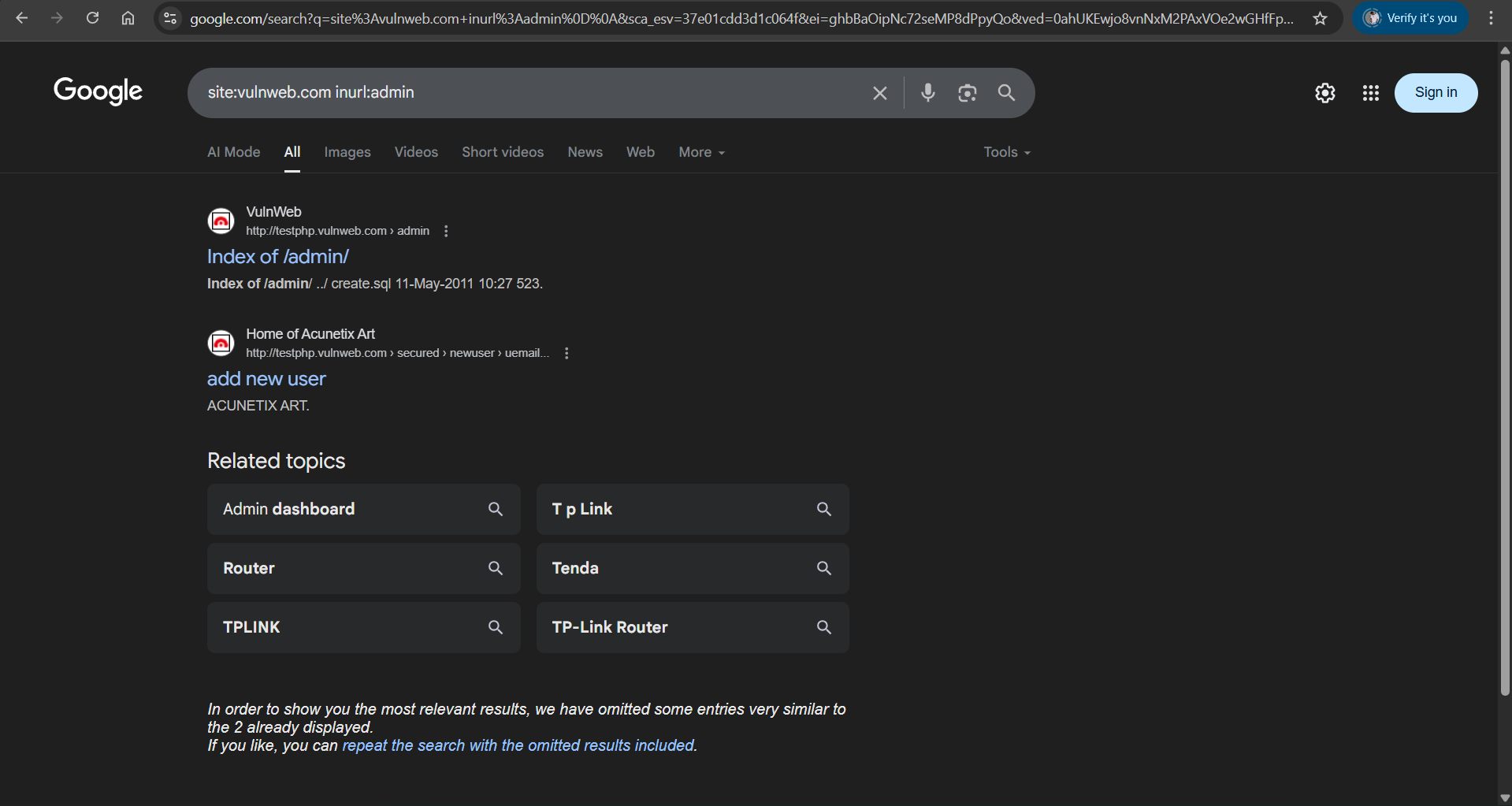


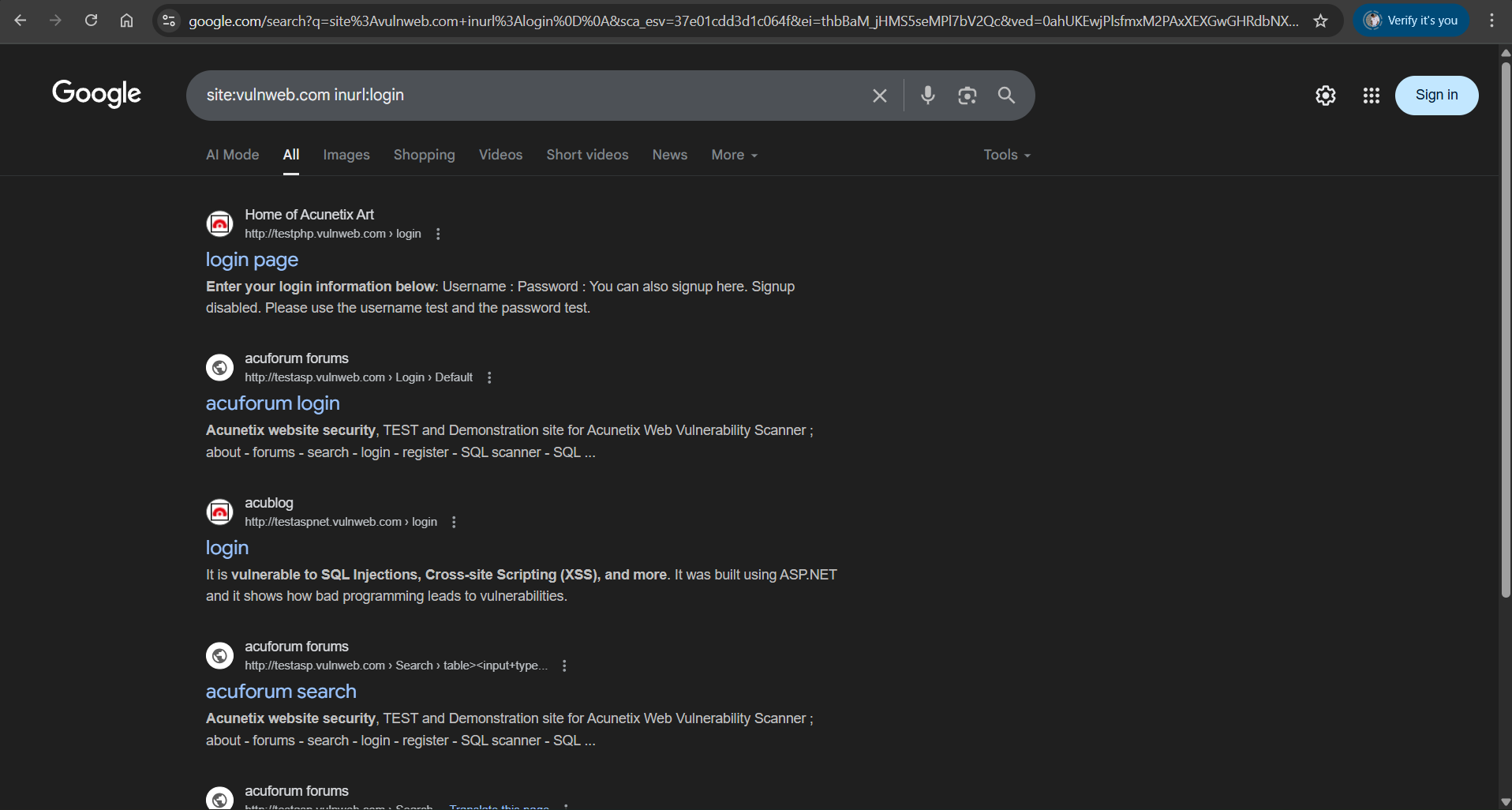


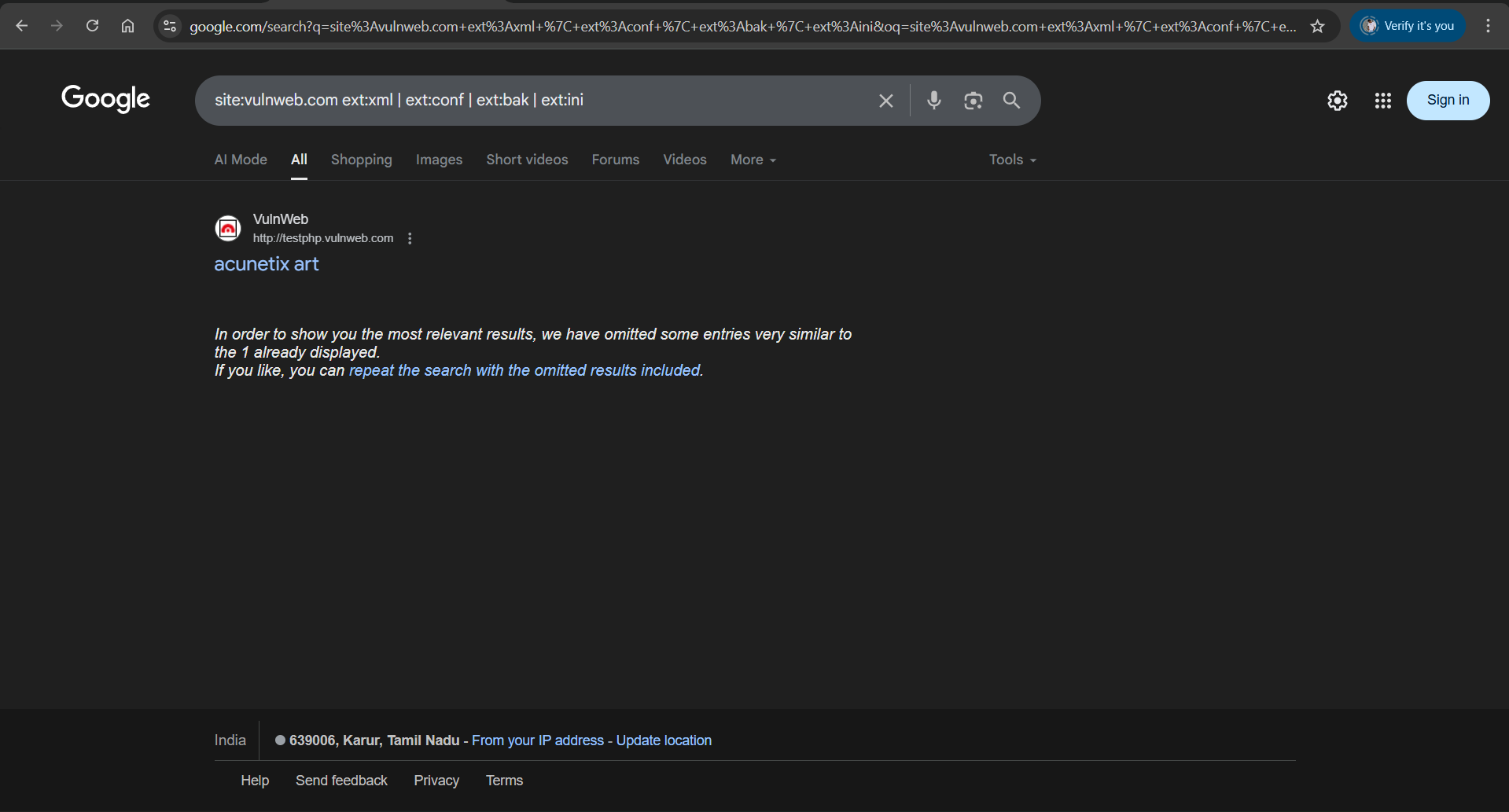
# 7. OSINT Summary from Social Media/Public Platforms

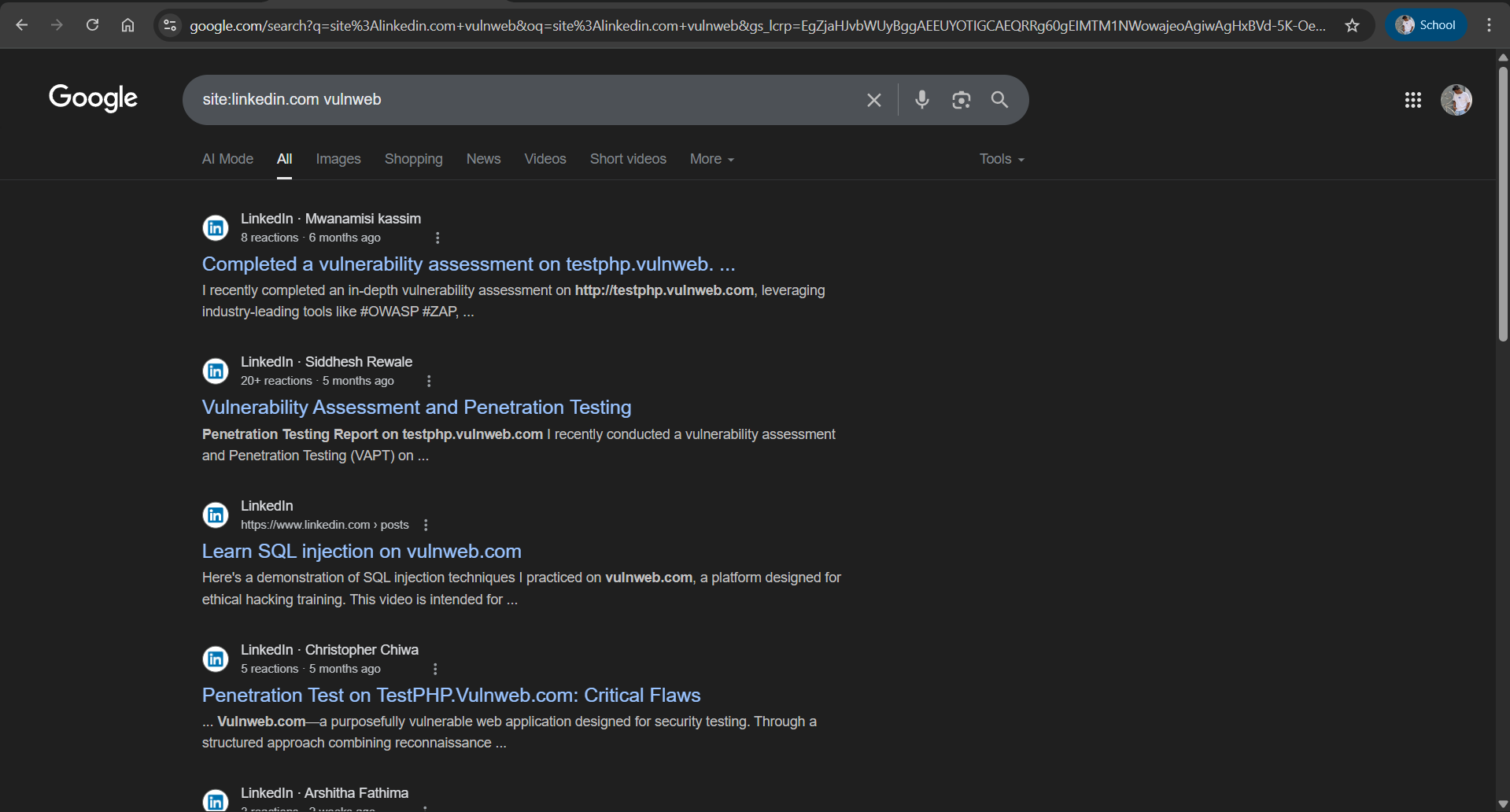
The following screenshots summarize OSINT findings from public platforms and social media:

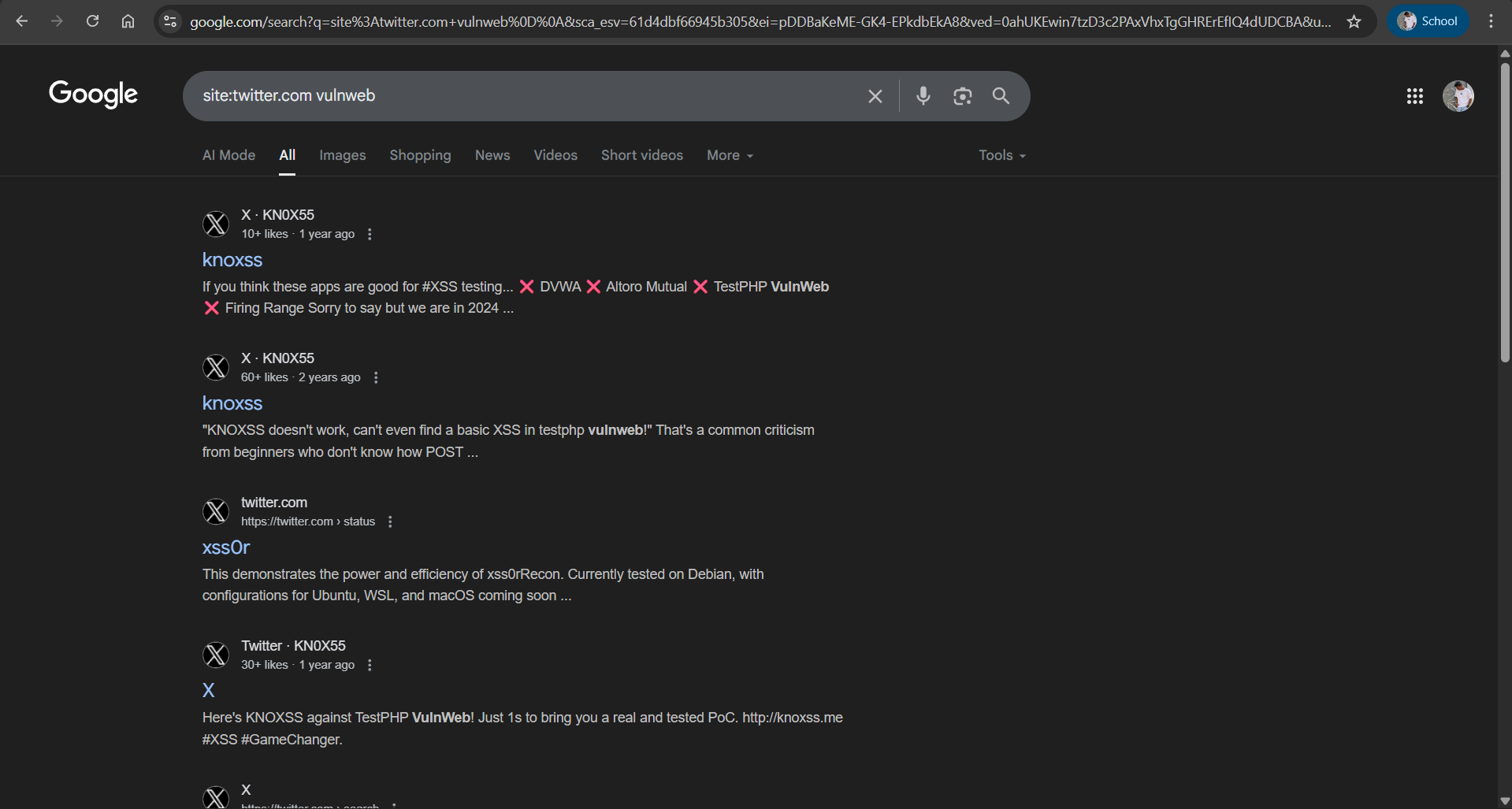


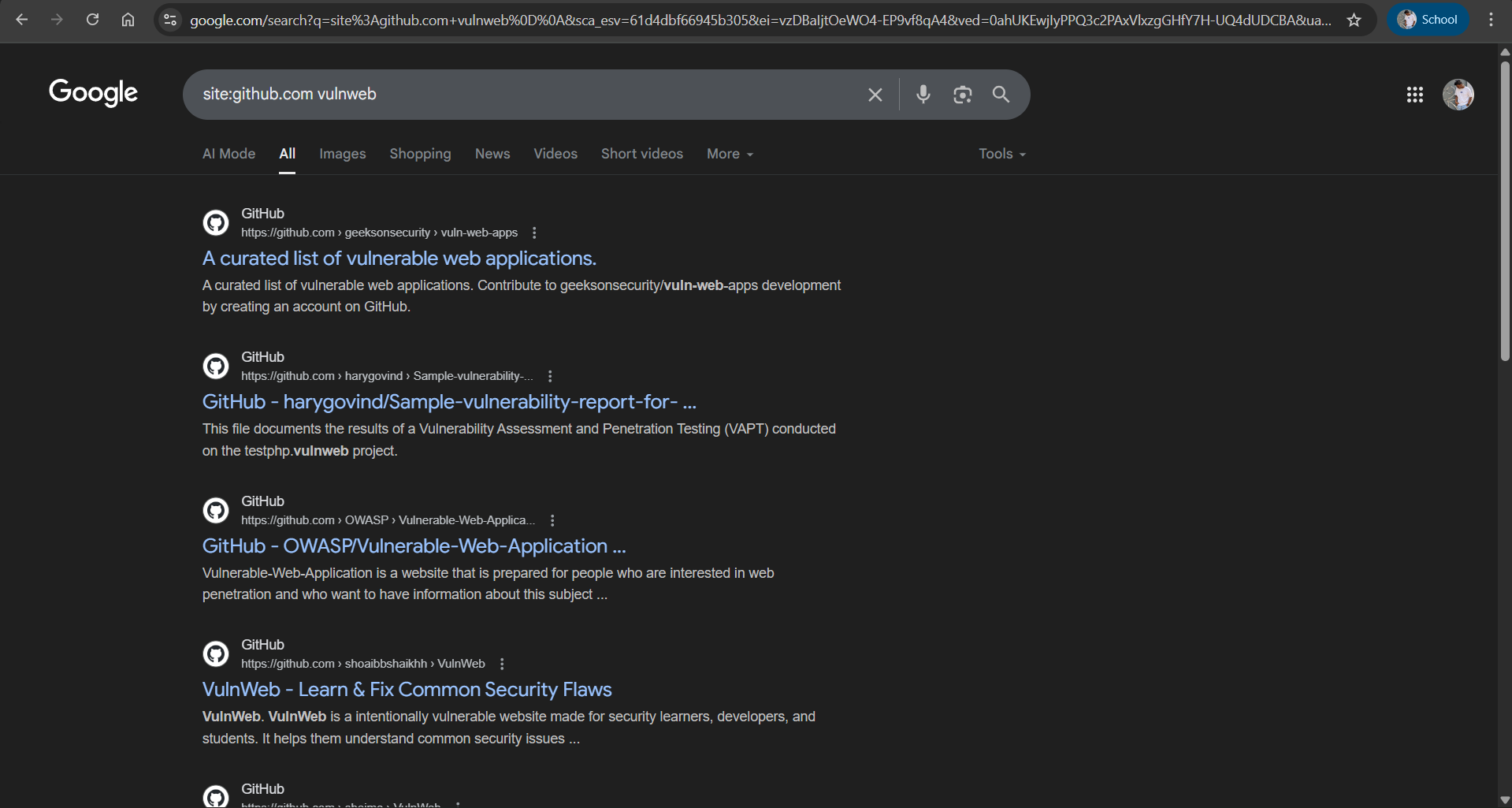






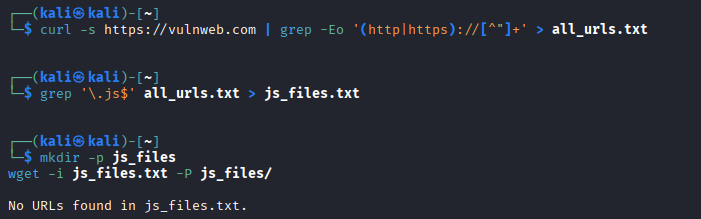






# 8. URLs & Leak Data in JS Files

The following screenshot shows potential sensitive data or leaks found in JavaScript files:



# 9. Conclusion

From the passive reconnaissance performed on vulnweb.com, the following possible attack surfaces were identified:  
- Publicly available WHOIS and DNS records  
- Subdomains that may be leveraged for further reconnaissance  
- Publicly exposed email addresses  
- Metadata extracted from documents  
- Sensitive information discoverable via Google dorking  
- OSINT details from social media and public platforms  
- Potential secrets and URLs exposed in JavaScript files  
  
These findings indicate possible avenues for attackers and should be addressed by the target organization.