**OpenVuln Scanner with OpenVuln SecFramework**

**A comprehensive, open-source tool for OSINT research and analysis**

Rajheshwar Va, Sharat Nb , Vishal Sc and Suganthi Nd

*a b c d Kumaraguru College of Technology, Coimbatore, India*

**Subject Area**: Computer Science

**Type of the Paper**: Cyber Security OSINT Tool Analysis

**Type of Review**: Developer and performance-based review

**Abstract**

The research paper presents OpenVuln Scanner, a cutting-edge OSINT security tool that aims to streamline the process of performing security assessments for organizations. By combining the power of OSINT research and analysis with a carefully crafted vulnerability assessment framework, the tool provides a comprehensive solution for identifying and mitigating potential security threats. The proposed framework takes into consideration various security domains and provides a systematic approach to evaluating an organization's security posture. The OpenVuln Scanner not only performs a thorough scan of publicly available information but also provides insightful analysis and recommendations for mitigating identified vulnerabilities. The tool is designed to be user-friendly and can be easily integrated into an organization's existing security infrastructure. With the aim of enhancing the overall security posture of organizations, the tool provides a valuable contribution to the field of cybersecurity.

Keywords: information technology, assets, information, OSINT search, vulnerability analysis, security framework

**Introduction**

Cyberspace underwent significant changes in the twenty-first century as a result of technical growth and the emergence of several innovative applications. Blogging platforms, social networking, image sharing, and video sharing are a few examples of creative applications that were created at the beginning of the twenty-first century and quickly gained global appeal *(Hussen et al., 2021)* [1] *(Dashtipour et al., 2016)* [2]With the emergence of smartphones and the availability of high-speed internet connections, these platforms became enormously popular, resulting in a record-high user base for these apps. Social media has become closely tied to everyday life. Meanwhile, the advancement of cloud computing has led to the adoption of this service by corporate communities. By this point, the most traditional services, such as newspapers, libraries, bill payment, government, and education, had been digitized and were keeping all of their data on the internet. As new technologies started blooming, the practice of using the Internet as a data store transformed the same as a “gold mine” for obtaining data of all kinds. As a result, Open Source Intelligence (OSINT), a more than half-century-old practice used to extract meaningful intelligence from publicly available data and which was previously used by defense personnel, regained widespread popularity *(Charalambous et al., 2016)* [3] In recent years, OSINT has expanded its reach into a wide range of sectors, making it vital for a wide range of applications. OSINT is in high demand, as is its acceptance, because it is less expensive, has no dangers, and is based on publicly available data. OSINT has the ability to create new and unique data and insights, but it also has technological, political, and ethical challenges that must be addressed (Layton & Watters 2016) [4]. OSINT has been used to identify weaknesses in IT infrastructure over time. (Azevedo et al., 2019) [5] whereas law enforcement organisations are tasked with profiling criminals and radicals, forensic investigation of criminal activities deploying OSINT in the sphere of cyber security (Hassan & Hijazi 2018) [6]

**An overview on open-source intelligence**

During World War II, OSINT was created for espionage objectives. (Glassman & Kang 2012) [7]. OSINT acquired prominence in the modern period as a result of the internet revolution, which led to vast volumes of data being accumulated on the Internet. Posts on social media, blogs, journals, published articles, newspapers, video-audio files, online forums, discussion groups, corporate websites, government records, and maps are all examples (Klaus et al., 2020) [8] (John et al., 2007) [9], of data sources for modern-day OSINT. OSINT is increasingly being used by governments and intelligence agencies to conduct investigations and combat cybercrime (Nouh et al., 2019) [10]. Data gathering, data processing, data exploitation, and data extraction are the four components of OSINT activity. Data collection is done from websites using search engines such as Duckduckgo, Shodan, and others. The data processing stage is largely responsible for removing undesired information and converting raw data into usable data. It is crucial that data is obtained for the proper purposes, and that no more data is gathered than is truly necessary. (Gibson 2016) [11]. The data exploitation phase, also known as the analysis phase, is responsible for confirming the data's legitimacy and veracity. Open-source information and data are turned into open source intelligence throughout the analysis and interpretation process. (Gibson et al., 2016) [12]. At the data extraction step, the intelligence obtained from the OSINT procedure is delivered.(Pastor-Galindo et al., 2020) [13] Open source Intelligence has a number of advantages including being less risky, inexpensive, and easy to obtain (Hassan 2019) [14]

**Literature Review**

Opensource intelligence developed along with technological innovation. Many actors, including business corporations, antisocial individuals, governmental organisations, law enforcement agencies, etc., have been persuaded to incorporate opensource intelligence for their own gain by the enormous amounts of data that have accumulated in the public domain as a result of the development of social media platforms. The accessibility to the internet has made it possible for people to easily locate and post any kind of information. (Edwards et al., 2017) [15]

Lee & Shon (2016) [16] presented a new framework based on open-source intelligence for critical infrastructure cyber security threat inspection. There were four steps in this framework: creating an open source intelligence plan, preparing open source intelligence, collecting data from open source platforms, and providing security intelligence.

According to Hayes & Cappa (2018) [17], OSINT can be used to perform risk analyses for the business in order to guard against future cyberattacks on its vital infrastructure, which was a component of the US electrical grid. The company's network, apps, devices, and crucial IT resources were profiled using a vulnerability assessment and other open-source intelligence analysis processes.

Wiradarma & Sasmita (2019) [18] suggested a similar approach for examining website vulnerabilities. The victim's information is gathered from open sources using OSINT tools like Maltego and others during the information gathering stages of penetration testing. Combining information from OSINT, penetration testing, and the ISO 31000 risk assessment standard resulted in a suggestion for system improvement.

An investigation of the development of research and study material production in the OSINT platform was carried out by Herrera-Cubides et al. in 2020 [19]. Research knowledge distribution databases and archives for educational resources are two of the physical sources of OSINT that are examined in this investigation. This study offers academics a road map to the state of OSINT research and instruction today as well as a priceless metadata description to improve resource accessibility and reusability in the educational environment.

TExtractor is an OSINT tool recommended by Magalhes & Magalhes (2019) [20] that will make gathering information about cyberthreats simpler. TExtractor is a tool that searches for keywords connected to the actions of harmful individuals while extracting text from video and audio from public sources. The study's findings are presented, and they show that a tool like TExtractor can accurately identify references to cyberattacks on audio/video sources with a detection rate of 60% to 70% in real time. TExtractor could also be used to maintain track of a brand or automate the clipping process, which entails locating brand or product references in audio or video channels.

Kanta et al. (2020) [21] investigated the potential for Open Source Intelligence (OSINT) to be leveraged for more efficient password cracking in his study. The literature on secure passwords, password cracking, and OSINT is reviewed in-depth, along with the ethical concerns that these subjects generate. Password complexity research as well as demographic factors that affect password selection is also offered. The effect of OSINT by law enforcement on password cracking is finally investigated.

Kang (2020) [22] provides the assessment variables for cyber threats among cyber-attack databases and analyses the priority of those elements in order to quantify cyber risks. He selected the attack's goal, attack type, target, attack's ease of use, attack durability, frequency of OSINT database, and elements of each component's lowest layer as evaluation variables for cyber threats. Only after each element has been selected is its priority evaluated utilizing the analytical hierarchy procedure.

**Drawbacks of existing systems**

Currently, there are tools in the market available to perform functions such as

− WHOIS Lookup

− Subdomain Enumeration

− DNS Records Lookup

− Geolocation

− OS Detection etc.

But these tools are available individually and require a lot of effort to install as there are a lot of problems associated such as mismatches and non-availability of dependencies, incompatibility of the modules associated with the operating system etc.

Similarly, the forementioned tools are mostly freemium – meaning though free versions of those tools are available, they do not offer you a lot of features that the paid, premium version does. The price of these tools are too high such that an individual who wants to experience the full potential of these OSINT tools may or may not be able to afford to.

Considering organizations, they would have to pay a hefty amount for buying multiple licenses, further increasing the CapEx (Capital Expenditure) of an organization.

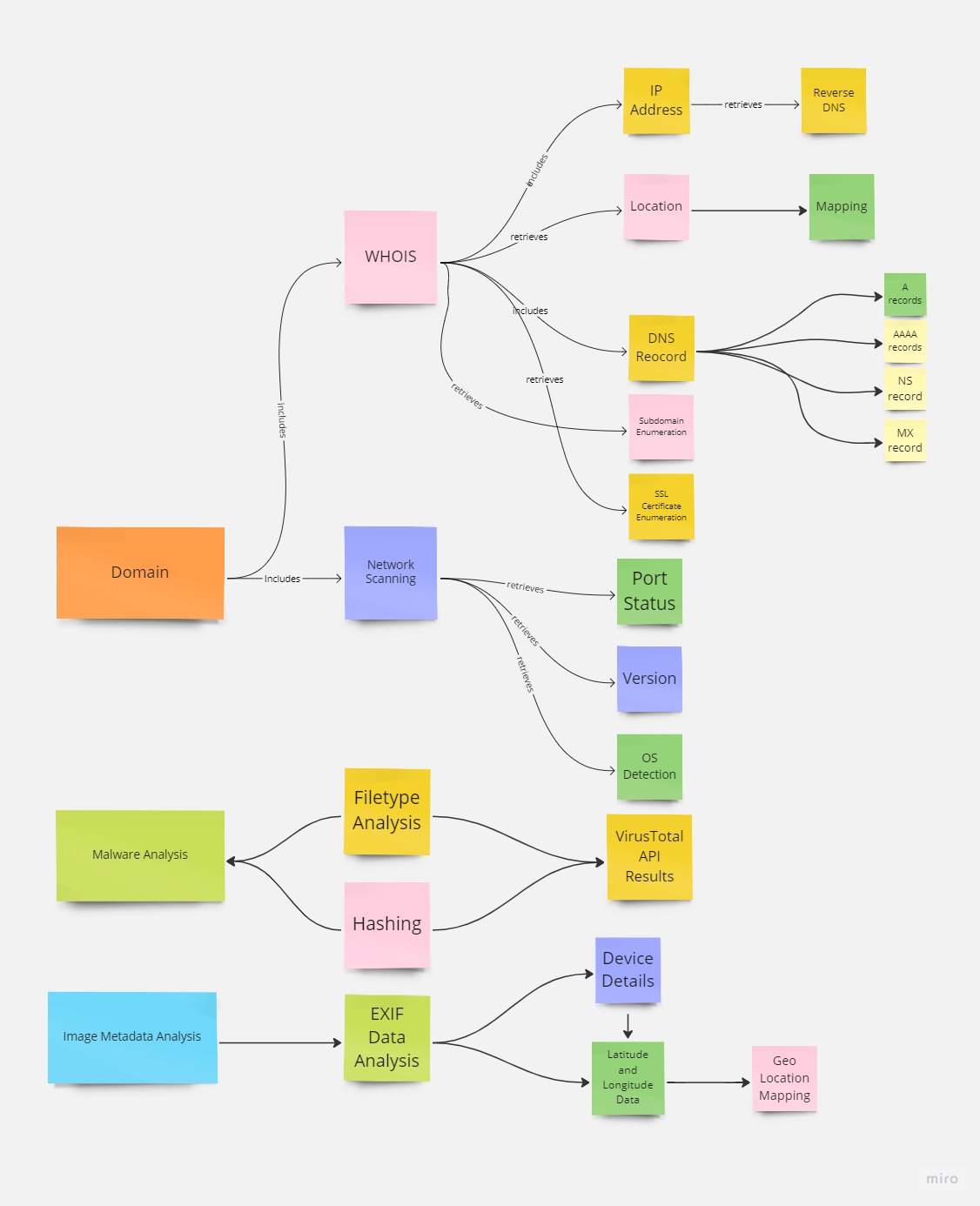
Organizations might not even purchase these tools as it does not assure them ROI (Return on Investment) on buying these tools.

**Proposed Solution**

The OpenVuln Scanner with OpenVuln SecFramework is a comprehensive OSINT tool that provides a streamlined approach to information gathering for cybersecurity purposes. The tool gathers publicly available data about an organization, such as its domain, on the internet and displays the results on a user-friendly dashboard. The dashboard provides cumulative results, enabling the user to quickly gain insights into the organization's cyber threat landscape.

To achieve this, the tool utilizes interconnected modules that work in a strategic manner to gather information. This means that the user can customize the tool's functionality to meet their specific needs, making it a versatile and adaptable solution for a wide range of industries.

Moreover, the OpenVuln Scanner with OpenVuln SecFramework provides an industrial-level standard security framework for Identity and Access Management (IAM) and IT Assets Management (ITAM). This framework ensures that the tool can be used in various industries, including hospitals and educational institutions, to manage and secure sensitive information effectively.



*(Fig 5.1) Workflow of OpenVuln Scanner*

**Modules that comprise the OpenVuln Scanner**

The tool is made up of various modules, each of which is specifically designed to perform different OSINT tasks. The WHOIS details gatherer, for example, allows users to gather registration details about the domain, while the Network Scanner module enables users to scan the domain for open ports and other vulnerabilities. The Operating System (OS) detection module is used to identify the type of operating system running on the domain, which can be useful for identifying potential vulnerabilities. The DNS Enumeration and Subdomain Enumeration modules enable users to gather information about the domain's subdomains and DNS servers, respectively. The IP Address Lookup module provides users with information about the domain's IP address, and the SSL Certificate Enumeration module enables users to scan the domain for SSL/TLS vulnerabilities. Finally, the Adult Content Detection module is used to identify any adult content that may be present on the domain.

All of these modules work together to generate a comprehensive OSINT report that provides users with detailed information about the domain. This report can be used to identify potential vulnerabilities and security weaknesses, making it a valuable tool for the attacking phase of cybersecurity research. By utilizing the information gathered from the OpenVuln Scanner, users can improve their overall cybersecurity posture and stay ahead of emerging threats.

Graphical user interface, application, Teams

Description automatically generated

*(Fig 6.1) A screenshot of the OpenVuln scanner’s dashboard*

**Key features and Capabilities of the OpenVuln Scanner**

**Fetching WHOIS details**

The WHOIS details gathering module is a crucial component of the OpenVuln Scanner. This module is designed to gather detailed information about the domain, including the IP address, network ID, registrant name and organization, country, city, latitude and longitude details, and ASN ID. All of this information can be incredibly valuable for conducting OSINT research, particularly during the reconnaissance phase. Figure (6.2) shows a detailed WHOIS report of a domain.

The information gathered by the WHOIS details gathering module is displayed in a detailed dashboard. This dashboard includes a wide range of information, including network details, domain registration information, and contact information for the domain registrant. By presenting all of this information in one place, the OpenVuln Scanner makes it easy for users to quickly and easily gather the information they need for their OSINT research.

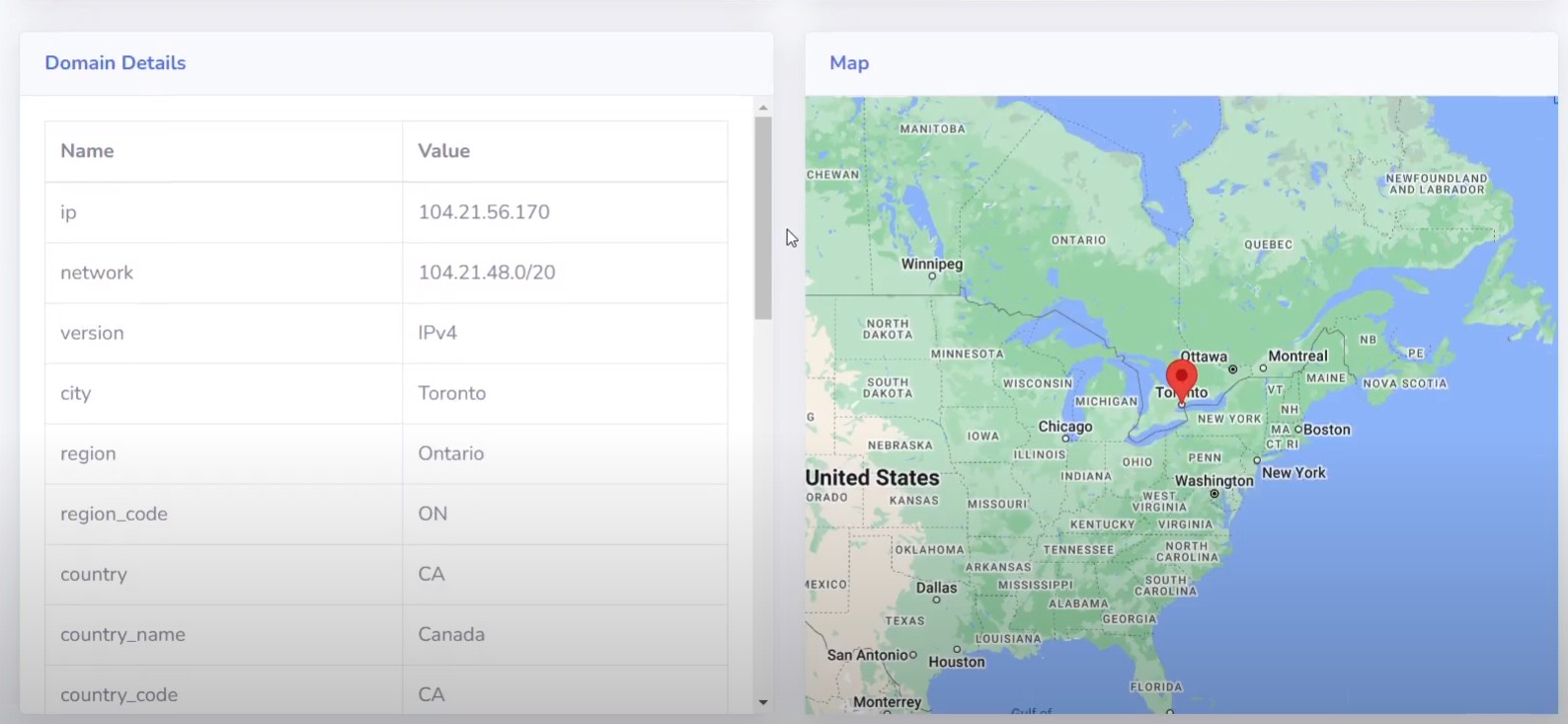
Table

Description automatically generated

*(Fig 6.2) Information fetched from a WHOIS query is displayed here.*

**Geolocation**

One of the standout features of this module is the map integration. The OpenVuln Scanner dashboard includes a map that displays the location details of the server. This map can be used in combination with the 360° viewer for extensive OSINT, allowing users to gather a wide range of information about the domain and its associated infrastructure. Figure (6.3) shows the location of a domain’s server.



*Fig (6.3) The geo-location respective to the hosts’ IP address is being shown*

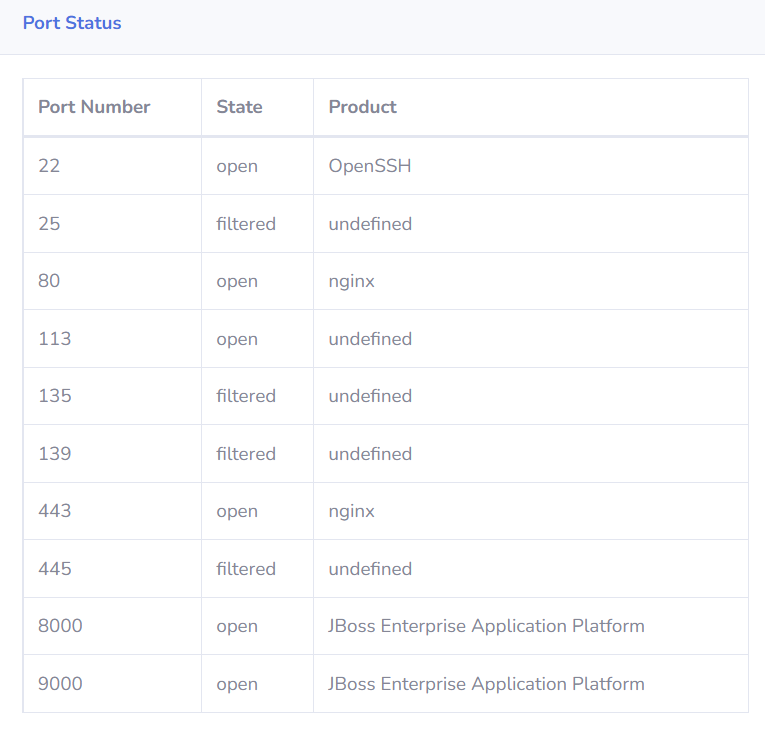
**Network Analysis and Service Detection**

The network analyzer module is a powerful Python-based tool that is designed to scan the status of ports in the server where the website is hosted and the services that are running on those ports. By doing so, this module can provide users with a wide range of valuable information, including details about the services that are running on each port, as well as the version of the service that is running.

This information can be incredibly valuable when conducting OSINT research. By knowing which services are running on which ports, users can gain a better understanding of the infrastructure that supports the website. This information can be used to identify potential vulnerabilities and attack vectors that can be exploited to compromise the security of the site.

The network analyzer feature presents users with a detailed view (as shown in Fig. 6.4), of the information needed about the services running on the server. This information can be used to identify potential vulnerabilities and attack vectors, allowing users to take proactive measures to protect their sites and infrastructure.

Overall, the network analyzer module is a powerful tool that can help users conduct effective OSINT research and enhance their cyber security defenses. By providing detailed information about the services running on the server, this module can help users stay ahead of emerging threats and take proactive steps to protect their sites and infrastructure.



*(Fig 6.4) View of port scan and service detection scan results on a server*

**OS Detection**

The OS detection module is an essential component of our OpenVuln Scanner tool that is used for Open-Source Intelligence (OSINT). The module is designed to provide information on the operating system running on the server by analyzing the banner that is fetched as a response from the server. The module works by analyzing the specific strings of characters present in the banner to identify the operating system running on the server. This information is extremely useful in identifying and exploiting vulnerabilities specific to the operating system running on the server. The details gathered by this module, including the operating system and its version, are displayed in the dashboard as shown in the Fig.(6.5).This information can be used by security professionals to enhance the security of their IT infrastructure and protect against potential threats.



*(Fig 6.5) A screenshot of OS scan results displayed*

**Technology Stack detection**

The Technology Stack detection module is a powerful component of our Open Vuln Scanner tool that is used for Open-Source Intelligence (OSINT). This module uses the Wappalyzer API to gather information about the web framework, plugins, and security systems used in the target website. This information is critical in identifying vulnerabilities and finding potential exploits in the attacking phase. By detecting the technology stack used in the website, we can identify the specific weaknesses in the website's security system and find the most effective way to exploit them. The information gathered by this module is displayed in the dashboard as show in the Fig (6.6). By analyzing this information, security professionals can take the necessary steps to secure their IT infrastructure against potential threats.

Table

Description automatically generated

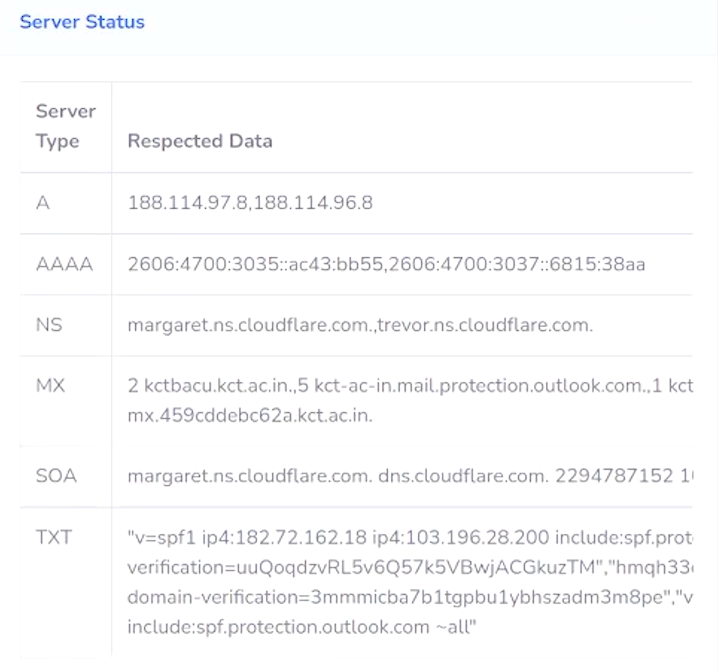
*(Fig 6.6) A view of technology stack detection scan result on the dashboard*

**DNS Records Collection**

The DNS Records module of our OpenVuln Scanner tool allows users to enumerate the DNS records associated with a domain, providing valuable insights into the target organization's infrastructure.

A records contain the IPv4 address associated with the domain, while AAAA records store the IPv6 address. Name Server records contain the name of the authoritative name server within the domain or DNS zone, and mail exchanger records specify the mail server responsible for accepting email messages on behalf of the domain. Start of Authority records store important information about the domain or zone, including the email address of the administrator, when the domain was last updated, and how long the server should wait between refreshes.

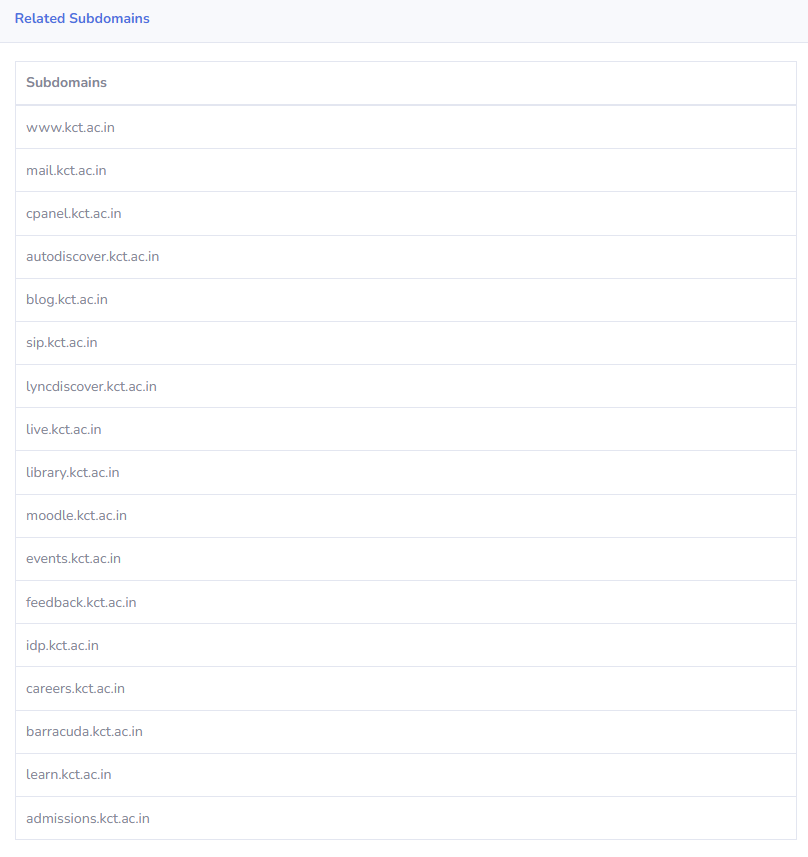
By collecting this information, the tool helps users to gain a better understanding of the target organization's infrastructure, which can be used to identify potential vulnerabilities or attack vectors. The DNS records gathered by the tool gets displayed on the dashboard as shown in the figure (6.7), allowing users to easily analyze and make use of this valuable data.



*(Fig 6.7) A snapshot of the automated DNS query results*

**Subdomain Enumeration**

The subdomain enumeration module allows for the expansion of the scope of an OSINT analysis. By discovering subdomains related to the target domain, security researchers and penetration testers can identify previously unknown applications, services, or web pages that may contain vulnerabilities or misconfigurations. In addition, subdomain enumeration can help identify forgotten or abandoned subdomains that may still be active and potentially vulnerable to attack. By broadening the attack surface in this way, security professionals can gain a more comprehensive understanding of the target organization's security posture and identify potential entry points for exploitation.



*(Fig 6.8) Sub-domains of a domain being displayed*

**SSL Certificate Enumeration**

The SSL certificate enumeration module of OpenVuln Scanner gathers information about the SSL certificates of the domain and its subdomains. This module is helpful in identifying the certificate issuer and the organization, which could be useful in analyzing the security posture of the domain. The module also collects historical data about the certificates, which could provide insights about the domain's security history. Since some WHOIS details might be hidden for privacy reasons, SSL certificate enumeration module is an alternative way to gather information about the domain. The details gathered from this module are displayed in the dashboard as shown in the figure (6.9)

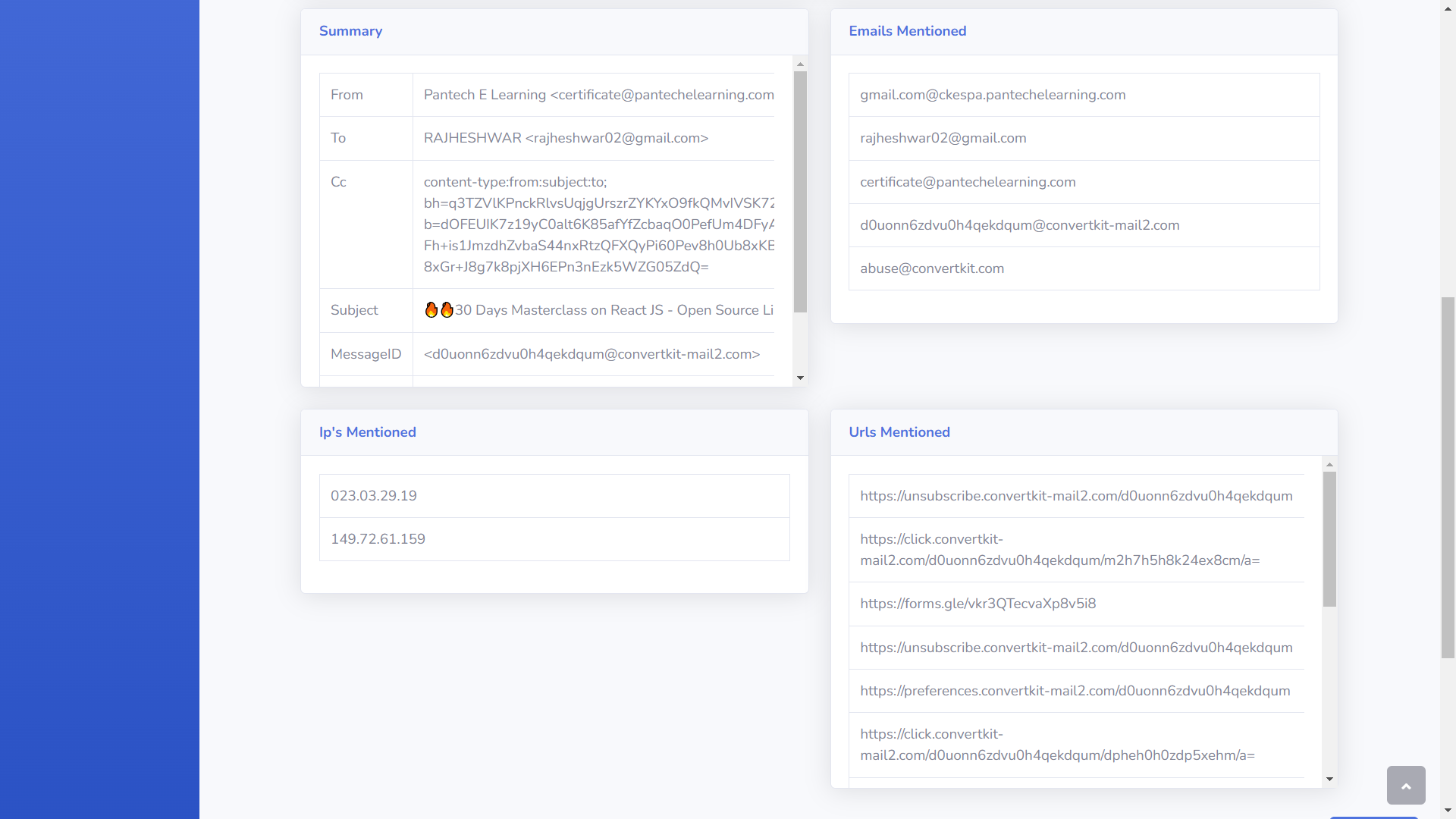
Graphical user interface, table

Description automatically generated

*(Fig 6.9) SSL certificates fetched of a domain being displayed.*

**E-Mail Header Analysis**

The tool also includes an email header analysis module which analyzes the email header of any email and gathers valuable information about the sender, the recipient, and the email's path through various email servers. The analysis can provide details such as the IP address of the sender, the email client used, the date and time the email was sent, and other important metadata. This can be useful in identifying potential phishing or spoofing attempts, as well as tracking down the source of suspicious emails. The email header analysis module in our tool provides a user-friendly interface to view and analyze email headers, and also includes a visual representation of the email's path through various email servers. With this module, our tool provides a comprehensive solution for conducting Open-Source Intelligence (OSINT) on a domain or organization, including both technical and non-technical information.



*(Fig 6.10) Email header information fetched being displayed.*

**Malware Analysis**

Malware analysis is the process of analyzing malicious software, or malware, to determine its functionality and behavior. The goal of malware analysis is to identify how the malware works, what damage it can cause, and how to mitigate or eliminate its impact.

The malware analysis module of our tool is designed to detect and analyze any potential malware present in the scanned domain. The module uses various techniques to detect and analyze potential malware. By detecting and analyzing malware, the tool helps organizations to prevent potential data breaches, protect their customers' data, and maintain their reputation.

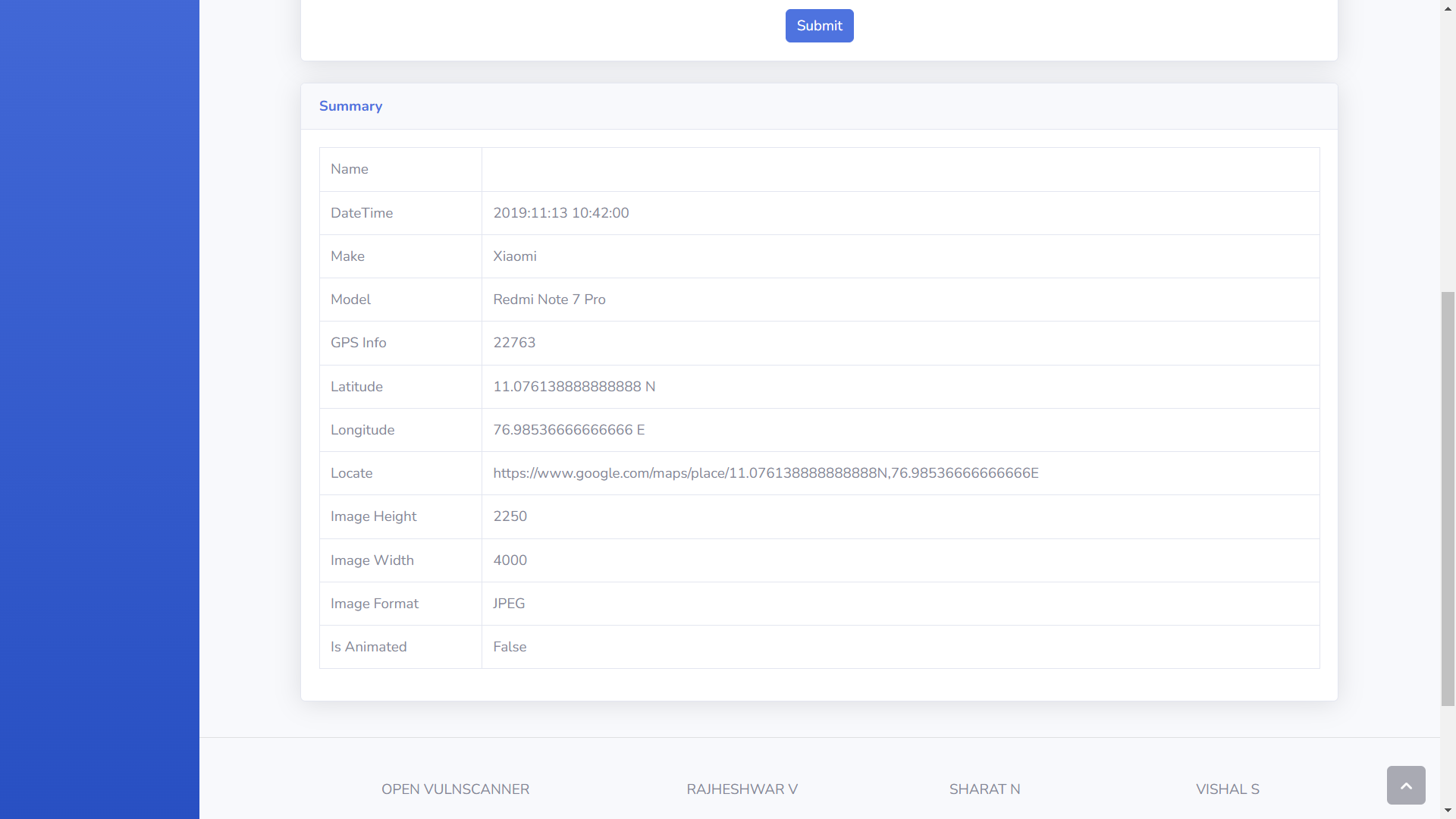
Graphical user interface, application, Teams

Description automatically generated*(Fig 6.11) Metadata of a malware showing information such as filetype, hashing and Virustotal results..*

**Metadata Analysis**

Malware analysis is the process of analyzing malicious software, or malware, to determine its functionality and behavior. The goal of malware analysis is to identify how the malware works, what damage it can cause, and how to mitigate or eliminate its impact.

The malware analysis module of our tool is designed to detect and analyze any potential malware. The module utilizes various techniques such as file-type detection, malware signature-based detection. The malware analysis feature detects the file type and does creates a signature of the entire file. It then scans the file for malicious signatures with respect to the signature database .The feature also uses the VirusTotal API to generate a report based on the end result of the scan. By detecting and analyzing malware, the tool helps organizations to prevent potential data breaches, protect their customers' data, and maintain their reputation.



*(Fig 6.12) Metadata of an image showing information such as date, co-ordinates etc.*

**Security Assessment Framework**

The tool generates a comprehensive report with respect to the in-house proposed security framework that includes information about the organization's security posture and gives a score that indicates the level of security of the organization.

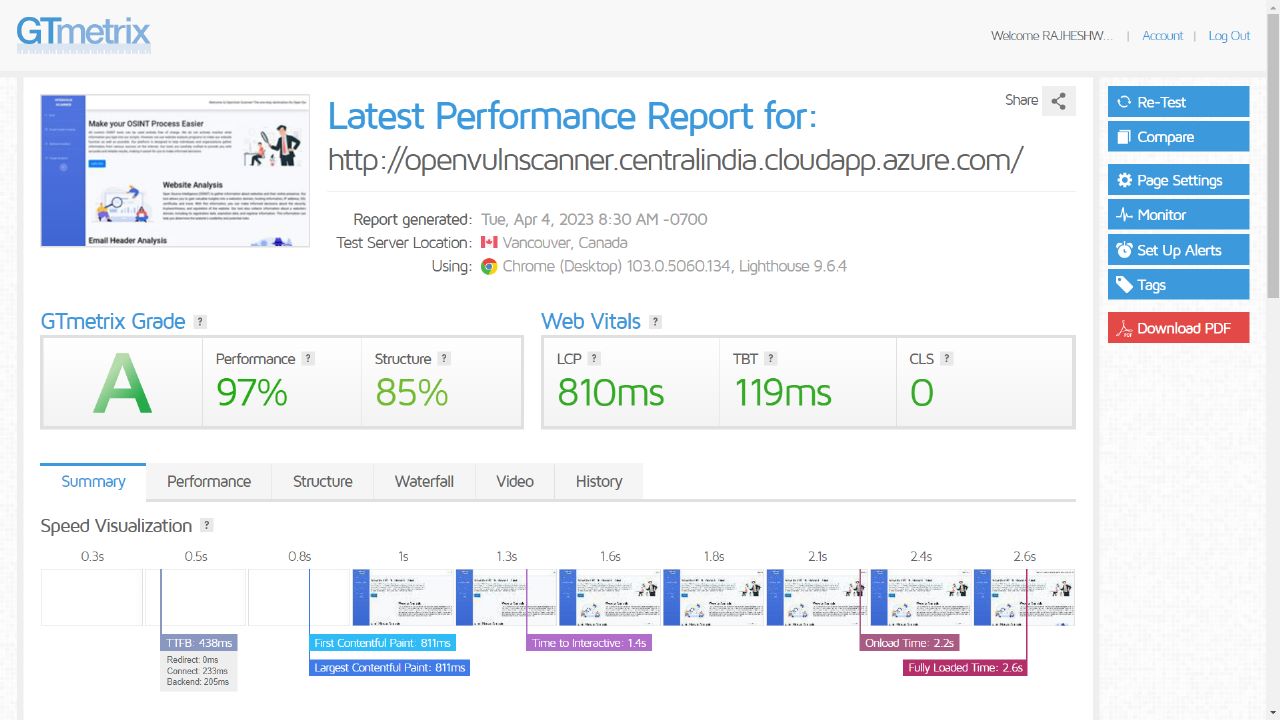
The OSINT analysis includes gathering information about the organization's web presence, domain registration details, SSL certificate information, and email header analysis. It also includes a technology stack detection module that identifies the web framework, plugins, and security systems used by the organization. This information can be useful in identifying vulnerabilities and weaknesses in the organization's security posture.

The vulnerability assessment part of the framework involves running a suite of vulnerability tests to identify potential vulnerabilities in the organization's web assets. The tests include port scanning, network scanning, operating system detection, and service detection. These tests can help identify weaknesses in the organization's infrastructure and web applications that could be exploited by attackers.

The generated report complies with industrial-level standard security frameworks providing a detailed analysis of the organization's security posture and includes recommendations for improving security. The report's score provides an indication of how secure the organization is and can be used as a baseline for future security assessments. Overall, the tool combined with the proposed framework provides a robust and thorough analysis of an organization's security posture that can help identify vulnerabilities and improve the organization's overall security.

**Performance Review**

The cloud platform hosting and lightweight framework used in the tool make it highly performant compared to other tools that require local installation and utilize local computing resources. The tool's deployment on cloud platforms like Azure ensures that it benefits from high-performance cloud IaaS infrastructure, resulting in faster performance and reduced latency. Moreover, the tool's use of lightweight frameworks like Django complements its performance by providing a minimalistic and efficient environment for executing code. The combination of cloud hosting and lightweight frameworks makes the tool highly responsive, reducing the time taken for scans and assessments. Performing a comprehensive assessment and enumeration of a whole domain can be a time-consuming process, and the proposed tool is no exception. However, this is a trade-off for the comprehensive and detailed analysis that the tool provides. In comparison to other tools available in the market, the time taken by the proposed tool is similar, if not better, considering the comprehensive nature of its analysis.



*(Fig 7.1) Performance metrics of the application as measured by GTmetrix*

In our research, we compared the proposed framework with other existing frameworks and found that it is more comprehensive and covers all security aspects of an organization. Unlike other security guidelines such as HIPAA, which focus on only one security aspect such as the storage of health data, our proposed framework covers all aspects of security, making it a wholesome solution. Furthermore, the proposed framework allows organizations to create a security policy that is tailored to their specific needs rather than providing one-size-fits-all guidelines. This level of customization ensures that organizations can develop a security policy that is practical, effective, and feasible for their specific environment. Overall, our performance review indicates that the proposed framework is a robust and comprehensive solution for enhancing the security posture of organizations. Overall, the proposed tool along with the framework provides a good balance between performance and comprehensive analysis, making it a valuable addition to any security team's arsenal.

**Advantages and Limitations**

Advantages

* The time required for the report generation with all the details takes one day on average, whereas we automate the process and generate an easily interpretable report within a few minutes.
* As the code is self-implemented in Python you get to customize the implementation of the functionality to what you'll eventually be using your code for, so it's tailored to your workflow.
* The use of Django complements the project with features like security, scalability, versatility, and support of most OS and is easy to work with.
* The software can be used by cyber security employees to assess the systems of their organization at ease.
* This software can be used by personnel ranging from amateur to experienced.

Limitations

* Since some of the code is proprietary, future developers working on the project have to learn the theory and best practices for the approach, but the code has been well re-factored so that anyone can collaborate without any hassle.
* It does a complete, comprehensive OSINT search which consumes a tad more time more. than other tools.
* Since the tool comes in integrated with many modules, the module dependency chain is high.

**Conclusion and Future Work**

The future work is to implement this project in real time helping people ranging from beginners to professionals to easily perform an advanced OSINT search and vulnerability analysis without any hassle that enable them to modify their security practices, methodologies and strategies already in place and put forth security defense mechanisms in the form of hardware, software and security professionals based on the factors such as risk, ALE (Annual Loss Expectancy) and the cost based on the vulnerabilities found by the tool with respect to the proposed security framework along with this tool. Furthermore, this project can be improved by adding more modules and capabilities related to scanning, analyzing and preventing cyber security threats evolving every day in this modern digital world making it an all-in-one cyber security tool similar to the commercial, proprietary ones available in the market.

**References**

[1] Hussen Maulud, D., Zeebaree, S. R., Jacksi, K., Mohammed Sadeeq, M. A., & Hussein Sharif, K. (2021). State of art for semantic analysis of natural language processing. Qubahan Academic Journal, 1(2), 21-28.

[2] Dashtipour, K., Poria, S., Hussain, A., Cambria, E., Hawalah, A. Y., Gelbukh, A., & Zhou, Q. (2016). Multilingual sentiment analysis: State of the art and independent comparison of techniques. Cognitive Computation, 8(4), 757–77

[3] Charalambous, E., Kavallieros, D., Brewster, B., Leventakis, G., & Koutras, N. (2016). Combatting Cybercrime and Sexual Exploitation of Children: An Open Source Toolkit. In Open source intelligence investigation: From strategy to implementation (pp. 233–249). essay, Springer.

[4] Layton, R., & Watters, P. A. (2016). The Automating of Open Source Intelligence. In Automating open source intelligence algorithms FOR OSINT (pp. 1–17). essay, Syngress.

[5] Azevedo, R., Medeiros, I., & Bessani, A. (2019). PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT. In 2019 18th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 483–490).

[6] Hassan, N. A., & Hijazi, R. (2018). The evolution of open-Source intelligence. In Open source intelligence methods and tools a practical guide to online intelligence (pp. 11–11). essay, APRESS.

[7] Glassman, M., & Kang, M. J. (2012, March). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682.

[8] Klaus, S., Franziska, S., & Reiner, C. (2020). Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). Society for Imaging Science and Technology, 2020(3), 1-99.

[9] John, D. S. M., Goodchild, M. F., & Longley, P. (2007). In Geospatial analysis: A comprehensive guide to principles, techniques and software tools (pp. 39–39). essay, Matador

[10] Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! understanding the socio-technical challenges faced by law enforcement. Proceedings 2019 Workshop on Usable Security, 1-11

[11] Akhgar, B., Bayerl, P. S., Sampson, F., & Helen Gibson. (2016). Acquisition and Preparation of Data for OSINT Investigations. In Open source intelligence investigation: From strategy to implementation (pp. 69–93). essay, Springer.

[12] Gibson, H., Ramwell, S. S., & Day, T. (2016). Analysis, Interpretation and Validation of Open Source Data. In Open source intelligence investigation from strategy to implementation (pp. 95– 110). essay, Springer-Verlag.

[13] Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The not yet exploited goldmine of osint: Opportunities, open challenges and future trends. IEEE Access, 8(1), 10282–10304.

[14] Hassan, N. A. (2019). Gathering Evidence from OSINT Sources. In Digital forensics basics: A practical guide using Windows OS (pp. 311–322). essay, Apress.

[15] Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017, August). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security*, *69*, 18–34.

[16] Lee, S., & Shon, T. (2016). Open source intelligence base cyber threat inspection framework for critical infrastructures. 2016 Future Technologies Conference (FTC), 4(1), 1375-1384.

[17] Hayes, D. R., & Cappa, F. (2018, September). Open-source intelligence for risk assessment. *Business Horizons*, *61*(5), 689–697.

[18] Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019, December 8). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), 17–29.

[19] Herrera-Cubides, J. F., Gaona-García, P. A., & Sánchez-Alonso, S. (2020, October 29). Open-Source Intelligence Educational Resources: A Visual Perspective Analysis. *Applied Sciences*, *10*(21), 7617.

[20] Machado, A. M., & Magalhães, J. P. (2019). TExtractor: An OSINT Tool to Extract and Analyse Audio/Video Content. In Innovation, engineering and entrepreneurship (Vol. 505, pp. 3–9). Cham; Springer International Publishing.

[21] Kanta, A., Coisel, I., & Scanlon, M. (2020, December). A survey exploring open-source Intelligence for smarter password cracking. *Forensic Science International: Digital Investigation*, *35*, 301075.

[22] Kang, S., Moon, M., Shin, K., & Lee, J. (2020, March 31). A Study on Priority Analysis of Evaluation Factors for Cyber Threats using Open Source Intelligence (OSINT). *Journal of Information and Security*, *20*(1), 49–57.

[23] Yogish Pai, U. & Krishna Prasad, K. (2021). Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review. International Journal of Applied Engineering and Management Letters (IJAEML)