iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.68072

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Project Sleuth: A Comprehensive All-in-One Bug Bounty Automation Tool

Aditya Upadhyay[1], Abhishek Raj Verma[2], Shrayash Shukla[3], Mr. Vimal Gupta[1]
Department of Computer Science and Engineering, JSS Academy of Technical Education Noida, India

Abstract: ***Project Sleuth is a comprehensive cybersecurity tool designed to automate and streamline the process of bug hunting and reconnaissance. The tool integrates a range of techniques, including subdomain enumeration, credential brute-forcing, network scanning, CVE testing, and OSINT (Open-Source Intelligence) gathering. Its primary purpose is to assist ethical hackers and cybersecurity analysts in identifying vulnerabilities across diverse targets, accelerating vulnerability assessment and penetration testing processes.***

By combining multiple recon tools into a cohesive workflow, Project Sleuth simplifies complex security testing tasks, enabling users of varying technical skill levels to efficiently identify and address security risks. The tool also offers flexibility and modularity, allowing users to customize the recon modules according to specific needs. Future enhancements to the project may include integration of machine learning to prioritize vulnerabilities based on risk and cloud-specific security features to broaden its applicability. Overall, Project Sleuth aims to provide a powerful and accessible solution for proactive cybersecurity efforts, highlighting the importance of automation in securing modern digital assets.

Keywords: Cybersecurity, Reconnaissance, Automation, Vulnerability Management, OSINT

I. INTRODUCTION

In the digital era, cybersecurity has become a cornerstone of protecting sensitive information, critical infrastructure, and organizational assets. As cyber threats grow in complexity and frequency, security professionals face mounting challenges, including the time-intensive nature of manual testing and the need to stay ahead of rapidly evolving attack vectors. These challenges highlight the pressing need for innovative tools that streamline and enhance the efficiency of cybersecurity efforts.

It is the offering of this software that meets the requirement of Project sleuth. Project sleuth is a complete cybersecurity solution offering automated bug hunting and reconnaissance. It is intended for use by ethical hacker and cybersecurity analysts and does focus on the main point of ethical reconnaissance, such as subdomain enumeration, brute-forcing and CVE testing, service enumeration, and vulnerability scanning, and so on OSINT. By automated critical processes such as those, the user can quickly and successfully find the vulnerability in any number of targets, making it a great tool and asset for vulnerability assessment and penetration testing.

A. Objectives

The primary objective of Project Sleuth is to automate critical security reconnaissance tasks, such as subdomain enumeration, brute-forcing, CVE testing, service enumeration, and vulnerability scanning. By streamlining these processes, the tool aims to enhance the efficiency and accuracy of vulnerability detection, reducing the time and effort required for manual testing. Additionally, Project Sleuth provides robust tools for Open Source Intelligence (OSINT) gathering, enabling cybersecurity professionals to uncover valuable information about potential targets. Ultimately, the tool seeks to empower ethical hackers and analysts with a user-friendly platform that accelerates threat identification and mitigation while improving the overall effectiveness of vulnerability assessment and penetration testing efforts.

B. Motivation

The motivation behind Project Sleuth lies in addressing the challenges faced by cybersecurity professionals in an era of escalating cyber threats. Manual testing methods are not only time-consuming but also prone to human error, leaving critical vulnerabilities undetected. By automating these processes, Project Sleuth reduces the workload on security teams, allowing them to focus on strategic decision-making and advanced threat analysis. This tool is driven by the need to enhance productivity and effectiveness in vulnerability assessment and penetration testing.

C. Significance

The noteworthiness of Project Sleuth does not just lie in the fact that it connects the growing demand for cybersecurity solutions and the limitations of manual testing; it goes beyond that. By automating reconnaissance and vulnerability detection, the tool helps ethical hackers as well as analysts to more quickly identify and remediate security flaws. What makes it even more important as a feature set- from subdomain enumeration through OSINT gathering is that an organization can use this complete tool just to make it even better in protection against cyberattacks coming from the outside or by its own members. Just because Project Sleuth saves time, it does not mean it also does not stand to enhance the accuracy and reliability of assessments in security, thus making cyberspace much safer.

II. LITERATURE REVIEW

1) *Sanghvi and Dahiya* (2013) saw the cyber reconnaissance as the most important approach that leads to cyber attacks. They remarked on the phase as being significant since it is accompanied by early detection and mitigation strategies. It conceptualizes the emerging nature in reconnaissance techniques and why it is critical to have robust monitoring systems. Yet it did not give much detail on practical implementations which leave much room to explore real-life applicability. [1]
2) *Božić et al. (2019)* gave a thorough view regarding penetration testing and vulnerability assessment concerning phases, tools, and methods involved in it. They outlined obstacles to the detection of vulnerabilities and underscored the significance of tool automation. The research was an all-inclusive study but would not deal much with the performance of tools with a comparison, hence left to continuous research as a future agenda. [2]
3) *Shah et al. (2019)* presented an excellent tenure regarding an active reconnaissance phase penetration testing where port scanning was optimized through Nmap. They used advanced optimization techniques and realized the scanning results were improved greatly by speed and accuracy. Nevertheless, the test was highly based on traditional networks while bringing in only little applicability insight with respect to cloud or hybrid environments. [3]
4) *Ramadhan et al. (2020)* engineered Sudomy, a new sub-domain tool for enumeration and analysis, combination of information-gathering techniques to educe speed and the accuracy of finding subdomains. Sudomy was efficient in discovering subdomains, but the dependence on already defined data sources limited it to highly dynamic or obfuscated environments, suggesting for broadened adaptive methodologies. [4]
5) *Saraswathi et al. (2022)* developed a whole information gathering tool by unifying several tools, thus automating the repetitive works of an ethical hacker. It could easily define effectiveness in reducing manual efforts in the process; however, there are maintenance issues as far as accuracy is concerned due to the fact that web architecture generally changes very fast. [5]
6) *Barman et al. (2023)* created a systematic framework for reconnaissance and enumeration as a part of the ethical hacking life cycle. It encompassed structured guidance, which would increase the consistency and thoroughness of an ethical hacker's reconnaissance phase. However, it was found to be unable to cater to cases of excessive specific design or very complex environments found in standardized examples. [6]
7) *Odun-Ayo (2021)* surveyed common tools and techniques for conducting reconnaissance attacks and brought forward the views on strengths and weaknesses. The study was meant to show how reconnaissance tools are becoming more and more sophisticated and urged for countermeasures. The only thing that the study did not bring was the detailed analysis of the tools and that can be useful for foreseeing the upcoming trends. [7]
8) *Railkar (2022)* has given the study about the vulnerability scanning tools for network security and compared their capabilities and limitations. This clearly describes how specific a tool needs against the definite network it is used for and also summarizes the gaps in coverage provided by these tools by understanding new attack vectors. It is a very detailed study, but mostly on the commercial tools, with a few references for open-source tools. [8]
9) *Bairwa et al. (2014)* took proactive approaches on the use of web application vulnerability scanners for security. Their argument proved that these tools are effective in detecting existing vulnerabilities, but they failed in zero-day threats. The research called for vulnerability scanners to be integrated with other security measures to facilitate better overall shielding. [9]
10) *Subhangani and Chaudhary (2022)* evaluated various vulnerability scanning technologies, focusing on their applicability in modern network environments. They observed that although improvements had been made in scanning accuracy and speed, challenges still existed regarding encrypted traffic and evasion. This study thus proposed further research in adaptive scanning techniques to cope with these challenges. [10]

Table 1: Gap Analysis

S.No.	Proposed Work	Gap
1.	Sanghvi and Dahiya (2013): Explored cyber reconnaissance as a precursor to cyberattacks. [1]	- Lacks practical implementation details for early detection and mitigation. - Does not address the effectiveness of tools in real-world scenarios.
2.	Božić et al. (2019): Provided an overview of penetration testing and vulnerability assessment. [2]	- Limited comparative analysis of specific penetration testing tools. - Insufficient focus on the integration of emerging technologies in vulnerability assessments.
3.	Shah et al. (2019): Optimized port scanning during active reconnaissance using Nmap. [3]	- Focuses primarily on traditional networks, with limited insights into cloud or hybrid environments.
4.	Ramadhan et al. (2020): Developed Sudomy for subdomain enumeration and analysis. [4]	- Relies on predefined data sources, reducing effectiveness in dynamic or obfuscated environments. - Lacks adaptability for detecting advanced obfuscation techniques.
5.	Saraswathi et al. (2022): Automated the reconnaissance process for ethical hackers. [5]	- Challenges in maintaining accuracy when dealing with rapidly changing web architectures. - Limited focus on scalability for large-scale reconnaissance operations.
6.	Barman et al. (2023): Proposed a framework for reconnaissance and enumeration in ethical hacking. [6]	- Framework struggles to adapt to highly customized or complex network environments. - Limited validation of the framework in diverse real-world scenarios.
7.	Odun-Ayo (2021): Reviewed common reconnaissance tools and techniques. [7]	- Lacks detailed analysis of emerging tools and techniques. - Does not explore countermeasures against sophisticated reconnaissance attacks.
8.	Railkar (2022): Analyzed vulnerability scanning tools for network security. [8]	- Focuses primarily on commercial tools, with limited attention to open-source alternatives. - Limited discussion of tools' effectiveness against newer attack vectors.
9.	Bairwa et al. (2014): Studied proactive approaches to web application security with scanners. [9]	- Ineffective in detecting zero-day vulnerabilities. - Advocates integration with other security mechanisms but lacks implementation details.
10.	Subhangani and Chaudhary (2022): Evaluated vulnerability scanning technologies. [10]	- Challenges in handling encrypted traffic and evasion techniques. - Limited adaptability to modern, complex network architectures.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

III. PROPOSED WORK

As an enhancement to the current literature on the automation in cybersecurity, Project Sleuth will provide an end-to-end tool that automates various tasks throughout security reconnaissance and vulnerability detection. The tool is focused on overcoming the challenges cited in other papers, such as extensive manual testing, the demand for a dynamic vulnerability scanning process, and the capability of current tools when it comes to handling modern, complex attack vectors.

A. Installation and Setup of Tools

The first phase of Project Sleuth involves the installation and configuration of a suite of cybersecurity tools necessary for performing vulnerability assessments. This includes:

- Port Scanners (e.g., Nmap) for identifying open ports and services.
- Subdomain Enumeration Tools (e.g., subfinder, github-subdomains) for discovering subdomains associated with the target domain.
- Brute-Forcing Tools (e.g., ffuf, dirsearch) for testing directory and credential vulnerabilities.
- Vulnerability Scanners (e.g., dalfox, katana, Nikto) for scanning known vulnerabilities via CVE databases.

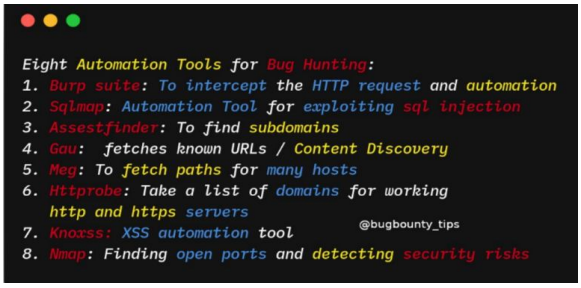


Fig 1. Bug bounty Tools

B. Reconaissance Phase

Once the tools are set up, the next phase involves performing reconnaissance to gather information about the target system. This includes:

- Subdomain and Endpoint Enumeration: Project Sleuth automates the process of discovering subdomains and endpoints using both active and passive techniques. This phase is crucial for identifying potential attack surfaces.
- Service and Port Scanning: The tool automatically scans for open ports and services, providing detailed information about the services running on each port. This includes identifying service versions and potential vulnerabilities that may be exploitable.
- OSINT Gathering: Project Sleuth integrates Open Source Intelligence (OSINT) gathering capabilities, allowing users to collect relevant information from publicly available sources such as domain records, social media, and leaked databases. This intelligence helps build a more comprehensive profile of the target.

1) *Before Recon:* This represents the initial stage, where the tester or researcher primarily gathers basic, publicly available information about the target, such as, the company name, available scope, user creds, overview of the company business, and details from the program page.
2) *After Recon:* This represents the outcome of performing active and passive reconnaissance, where detailed, technical, and actionable data is uncovered, including: Subdomains, ASNs, Database information, endpoint, juicy links, etc.

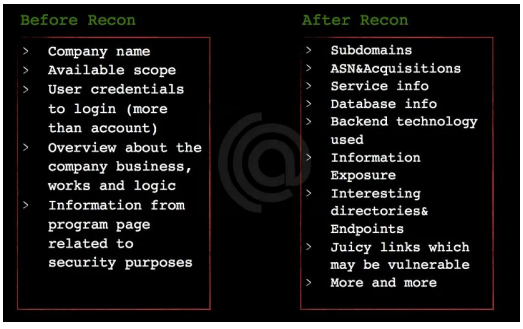


Fig 2. Before Recon & After Recon

C. Vulnerability Assessment

After the reconnaissance phase, Project Sleuth moves on to a detailed vulnerability assessment:

- CVE Testing: The tool scans for known vulnerabilities using up-to-date CVE databases, identifying common vulnerabilities that may exist in the target system.
- Brute-Forcing and Credential Testing: Project Sleuth includes tools for brute-forcing directories and testing weak credentials across different protocols (e.g., SSH, FTP, HTTP). This process helps identify weak points in the target's authentication mechanisms.
- Advanced Vulnerability Detection: In addition to CVE testing, Project Sleuth incorporates advanced techniques for detecting zero-day vulnerabilities, misconfigurations, and other emerging threats that may not be cataloged in standard vulnerability databases.

IV. CONCLUSION

Project Sleuth represents a significant advancement in the field of cybersecurity, aiming to address the growing challenges faced by ethical hackers and cybersecurity professionals in their efforts to identify vulnerabilities across diverse digital environments. In an era where cyber threats are becoming more sophisticated and prevalent, the need for effective, automated reconnaissance tools has never been more critical. Traditional methods of vulnerability assessment, such as manual penetration testing, subdomain enumeration, and brute-forcing, are time-consuming, error-prone, and often insufficient in handling the dynamic nature of modern IT infrastructures. Project Sleuth seeks to streamline and enhance these processes, offering a comprehensive suite of tools designed to automate and optimize the identification of security weaknesses.

The proposed work in Project Sleuth covers several key functionalities that are essential for vulnerability assessment and penetration testing, including subdomain and endpoint enumeration, credential brute-forcing, CVE testing, service enumeration, vulnerability scanning, and OSINT gathering. These features work together to provide a holistic view of a target's security posture, enabling users to uncover potential vulnerabilities more efficiently and accurately. The integration of these functionalities into a single platform is particularly valuable, as it reduces the complexity of using multiple disparate tools and simplifies the overall reconnaissance process. However, despite its capabilities, the project also addresses several gaps identified in existing cybersecurity tools. For instance, many current tools focus primarily on known vulnerabilities (CVEs) and struggle to detect zero-day vulnerabilities or adapt to rapidly changing environments, such as cloud-based infrastructures or microservices. Additionally, existing tools often treat subdomain enumeration and endpoint discovery as separate tasks, which can lead to inefficiencies and missed vulnerabilities. Furthermore, brute-forcing techniques in current tools are often detectable by intrusion detection systems, and manual analysis remains prevalent in vulnerability prioritization, leaving room for human error and inefficiencies.

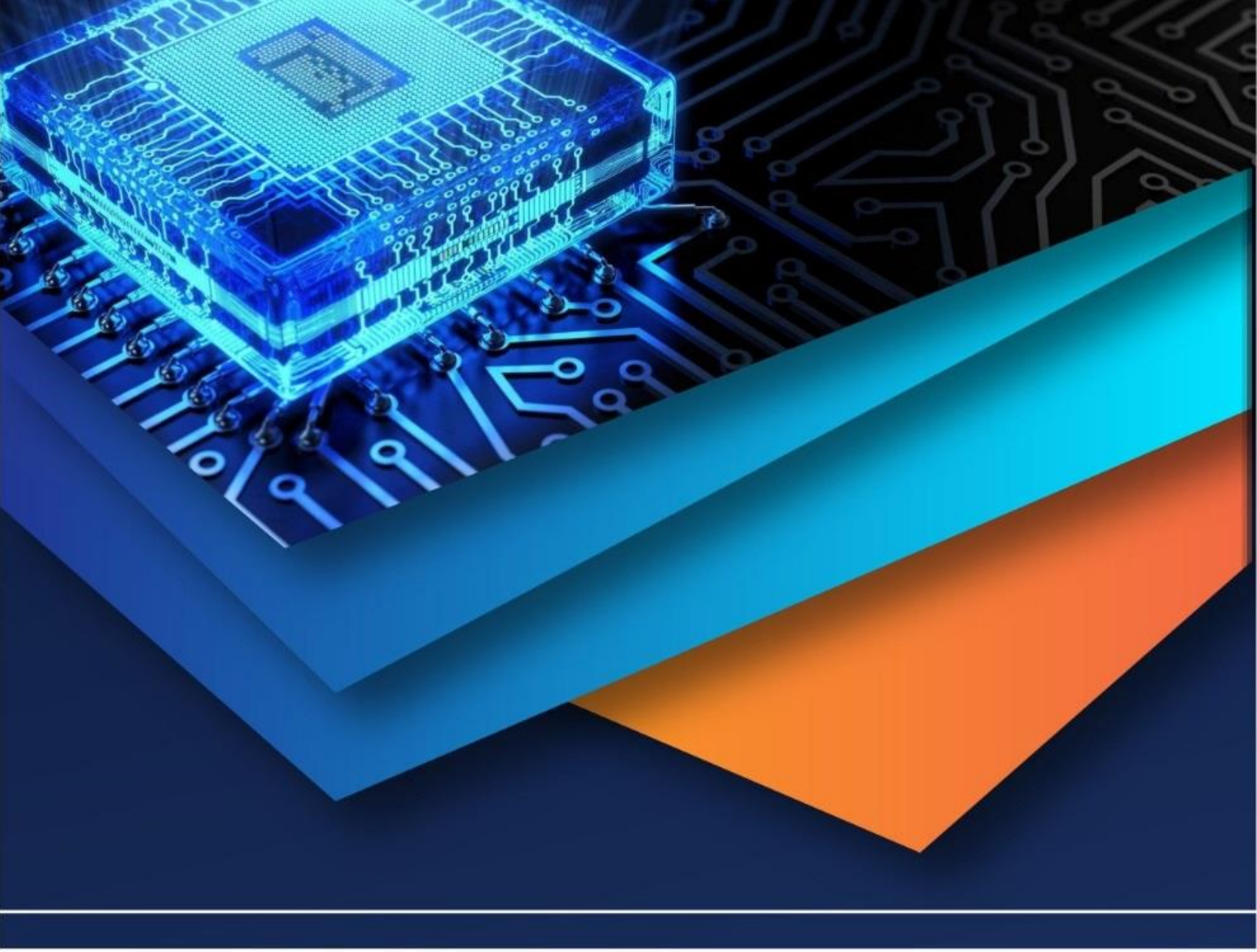
So-called vulnerability detection involves the use of tools and techniques that process information collectively and automatically (as opposed to performance- or human-dependent approaches) to identify and prioritize vulnerabilities as a provision to seaway threats (Project Sleuth). By providing a combined platform where lots of reconnaissance tasks could be automated, it saves time that cybersecurity professionals waste unnecessarily, improves their capabilities, reduces human error, and sufficiently adds efficiency in vulnerability assessment. Automated reporting, with prioritization dependent on exploitability, does provide further sensible value because it presents action points for remediation.

In the future, other capabilities such as real-time vulnerability scan, more sophisticated integration with threat intelligence feeds, and advanced stealth mechanisms for brute-forcing techniques are to be implemented to enhance Project Sleuth's potential longer into the future. Development of such features would address the currently perceived shortcomings of other tools and make Project Sleuth stand out as a very modern tool in the hands of cybersecurity specialists. Lastly, Project Sleuth might change the way vulnerability assessment and penetration testing are considered by ethical hackers and cyber security analysts. It fills existing gaps and provides a more effective automated working way with a promising new chapter in the age-old battle against cyber threats. As threats continue to evolve, tools like Project Sleuth become more and more instrumental in securing environments from digital threats and ensuring that critical systems and data remain safe.

REFERENCES

[1] Sanghvi, H. P., and M. S. Dahiya, "Cyber Reconnaissance: An Alarm before Cyber Attack," International Journal of Computer Applications, pp. 36-38, 2013.
[2] Božić, K., N. Penevski, and S. Adamović, "Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods," Sinteza Conference Proceedings, 2019.
[3] Shah, M., S. Ahmed, K. Saeed, M. Junaid, H. Khan, and Ata-ur-Rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," Proceedings of IEEE Conference, March 25, 2019.

[4] Ramadhan, Rizdqi, Redho Maland, and Dedy Hariyadi, "Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis," IOP Conference Series: Materials Science and Engineering, vol. 771, p. 012019, March 2020
[5] Saraswathi, Vijaya R., Iftequar Sk Ahmed, Sriveda M. Reddy, S. Akshay, Vrushik M. Reddy, and Sanjana M. Reddy, "Automation of Recon Process for Ethical Hackers," 2022 International Conference for Advancement in Technology (ICONAT), IEEE, pp. 1–6, 2022.
[6] Fouz Barman, Nora Alkaabi, Hamda Almenhali, Ikuesan Richard Adeyemi and Mahra Alshedi, "A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle," European Conference on Cyber Warfare and Security, 2023.
[7] Isaac Odun-Ayo, "A Review of Common Tools and Techniques for Reconnaissance Attacks.. Proceedings of the," 28th iSTEAMS Multidisciplinary Research Conference AIUWA The Gambia, 2021.
[8] Dipali Railkar, "A Study on Vulnerability Scanning Tools for Network Security," International Journal of Scientific Research in Computer Science Engineering and Information Technology, 2022.
[9] Sheetal Bairwa, Bhawna Mewara, Jyoti Gajrani, "Vulnerability Scanners-A Proactive Approach To Assess Web Application Security," International Journal on Computational Science & Applications, 2014.
[10] A Subhangani and B Anita Chaudhary, "Examination of Vulnerability Scanning Technologies", 2022



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY