iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50797

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 11 Issue IV Apr 2023- Available at www.ijraset.com

Web Vulnerability Scanning Framework

Prof. Priyanka Shingate[1], Akash Trimbake[2], Mayur Sawant[3], Rushikesh Jagdhane[4], Hrishikesh Jadhav[5]
[1, 2, 3, 4, 5]*Computer Engineering, Zeal College Of Engineering And Research*

Abstract: ***The increasing reliance on web-based systems has brought cybersecurity to the forefront of concerns for organizations and individuals alike. In this paper, we present a framework that leverages open-source tools for information gathering (reconnaissance) and vulnerability assessment in web-based systems. The framework is designed to be hosted as a website, providing a user-friendly interface for cybersecurity practitioners to conduct reconnaissance and identify vulnerabilities in their target systems. Through integration of various open-source tools, our framework enables efficient and effective information gathering and vulnerability scanning, aiding in the identification and mitigation of potential security risks. Our framework contributes to the field of cybersecurity by providing a unified solution for reconnaissance and vulnerability assessment in web-based systems. The integration of open-source tools and the flexibility of our framework make it a valuable resource for cybersecurity practitioners.***

Keywords: Reconnaissance, open-source, vulnerabilities, web application, framework

I. INTRODUCTION

The increasing reliance on web-based systems in various aspects of modern life, such as e-commerce, banking, social networking, and communication, has raised concerns about cybersecurity. Cyberattacks, which can involve theft of information, data breaches, system disruption, and ransomware attacks, pose significant risks to organizations and individuals alike. To address these threats, cybersecurity practitioners need effective tools and techniques for gathering information and assessing vulnerabilities in web-based systems, in order to identify potential weaknesses and vulnerabilities.

In response to these challenges, we propose a framework that aims to assist cybersecurity practitioners in conducting reconnaissance and identifying vulnerabilities in web-based systems. Our framework is built upon open-source tools that are widely used in the industry, providing flexibility, extensibility, and cost-effectiveness, making it accessible to a wide range of users. The framework is designed to be hosted as a website, providing a user-friendly interface that simplifies and optimizes the overall process.

One of the key advantages of our framework is the integration of various open-source tools, leveraging their unique capabilities and functionalities to enable efficient and effective reconnaissance and vulnerability assessment in web-based systems. By integrating these tools into a single framework, we provide cybersecurity practitioners with a consolidated and streamlined approach to conducting reconnaissance and vulnerability assessment.

The user-friendly interface of our framework allows cybersecurity practitioners to easily input their target systems, configure scanning options, and initiate the reconnaissance and vulnerability assessment process. The framework then orchestrates the execution of the integrated tools, automating the scanning and assessment tasks, and providing consolidated results for analysis. The results can include information about potential vulnerabilities, their severity. Furthermore, our framework allows for extensibility, enabling cybersecurity practitioners to add or customize tools based on their specific requirements.

II. MOTIVATION

The Motivation Behind this project is that using open-source tools separately is the lack of integration and coordination among them. Cybersecurity practitioners often need to use multiple tools for different tasks, such as one tool for information gathering and another for vulnerability scanning. The proposed framework offers a user-friendly interface that allows for simultaneous usage of multiple tools, along with the flexibility to seamlessly integrate additional tools as needed.

Here are some Motivations incorporated in this project:

1) *Lack of Integration and Coordination Among Tools:* When using multiple open-source tools separately, there can be a lack of integration and coordination among them. Cybersecurity practitioners may need to switch between different tools, manage multiple interfaces, and manually correlate information from various sources, leading to inefficiencies and redundancies. Our framework provides an integrated solution that allows for simultaneous use of multiple tools, streamlining the workflow and improving coordination among them

2) *Learning Curve Associated with Multiple Tools:* Each open-source tool may have its own interface, commands, and syntax, requiring practitioners to invest time and effort in learning and mastering each tool individually. This can pose a barrier to entry for less experienced practitioners or those with limited resources, as they may need to spend considerable time familiarizing themselves with multiple tools before they can effectively use them for reconnaissance and vulnerability assessment tasks. Our framework provides a unified interface and streamlines commands, reducing the learning curve associated with using multiple tools.
3) *Limited Flexibility in Adapting to Changing Requirements:* Using open-source tools separately may limit the adaptability of the cybersecurity workflow to changing requirements. As new vulnerabilities and attack vectors emerge, practitioners may need to incorporate additional tools or techniques into their workflow. However, with separate tools, integrating new tools or modifying existing workflows can be complex and time-consuming, requiring practitioners to relearn new interfaces and commands. Our framework is designed to be flexible, allowing for easy adaptation to changing requirements by incorporating custom templates and providing flexibility in adding or modifying tools as needed.

In summary, our motivation in this project is to overcome the challenges of using open-source tools separately for reconnaissance and vulnerability assessment by providing a comprehensive and efficient solution in the form of our framework. This solution aims to enhance the cybersecurity practices of organizations and individuals by addressing the limitations of using separate tools, such as lack of integration, learning curve, and limited flexibility, and providing a more streamlined, integrated, and adaptable solution.

III. PROPOSED SYSTEM

Our proposed system comprises two integral modules: the Information Gathering module and the Vulnerability Scanning module. The Information Gathering module empowers users to select specific subdomains to scan and configure various options to collect comprehensive information about the target system. This module serves as a vital reconnaissance tool to gather essential data for further analysis. Similarly, the Vulnerability Scanning module equips users with the capability to conduct thorough vulnerability assessments on the target system. It offers a wide range of options, including custom templates for scanning, allowing users to tailor the scanning process according to their specific requirements. By leveraging open-source tools, this module helps in identifying known vulnerabilities, potential weaknesses, and other security issues.

Upon completion of the scanning process, our system generates a comprehensive report in the form of a PDF document. This report presents a detailed summary of the findings from both the Information Gathering and Vulnerability Scanning modules, providing users with valuable insights into potential vulnerabilities and weaknesses in the target system. Our proposed system offers a unified and efficient solution that combines the functionalities of information gathering and vulnerability scanning into a single framework. It provides flexibility through configurable options, customization through custom templates, and generates detailed reports for comprehensive analysis of the scan results, making it an asset for cybersecurity practitioners and organizations seeking efficient reconnaissance and vulnerability assessment capabilities.

IV. LITERATURE REVIEW

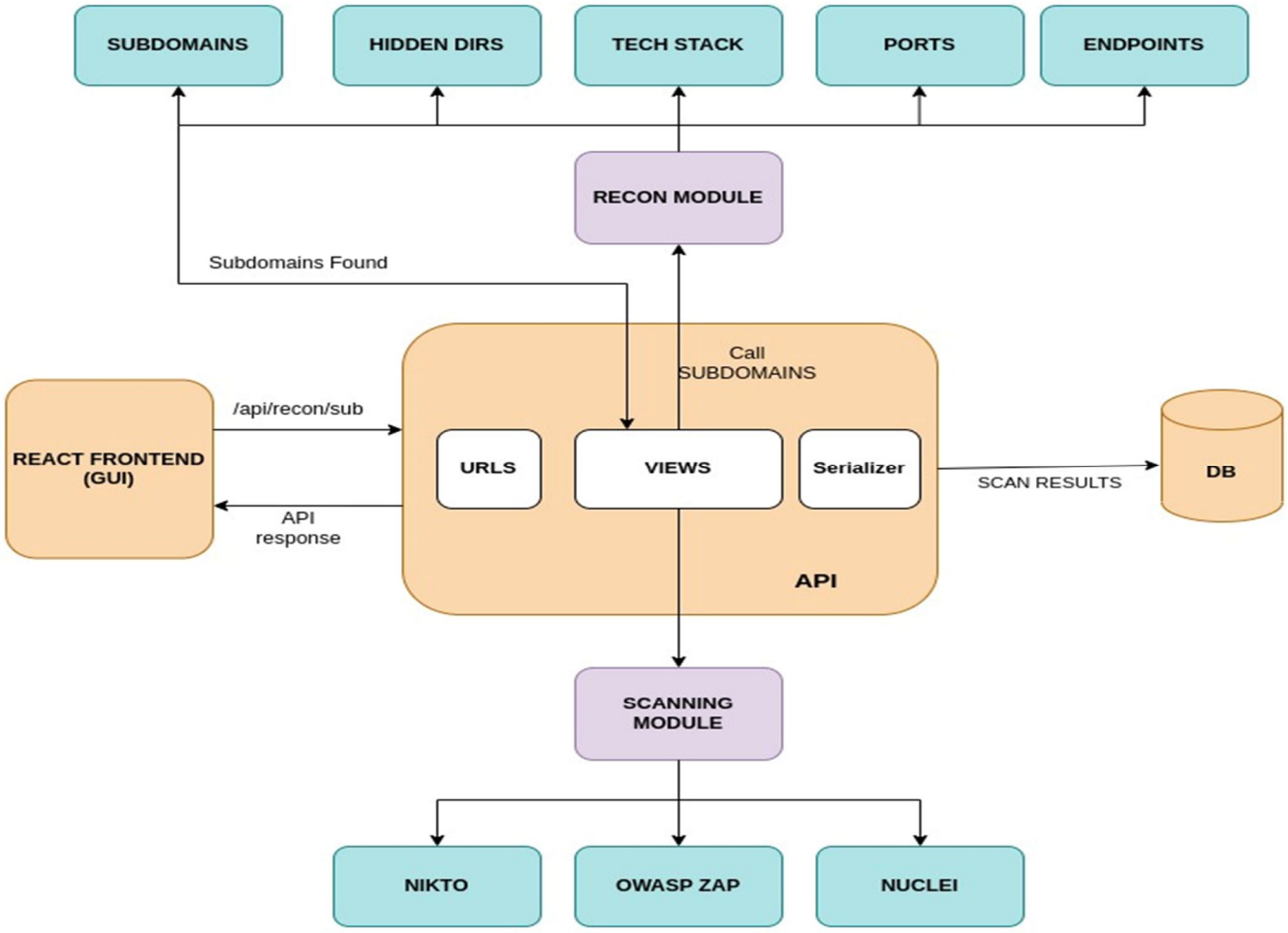
Automation of tasks has become an essential factor in every field of Information Technology. Similarly in Cybersecurity, automation of the general processes would immensely enhance one's efficiency. Companies like Acunetix and Nessus have already developed scanners that work on a local system of the user. Our proposed system involves using already built Open-Source tools to construct a framework and deploy it as a web application. This gives an advantage that the user does not have to rely on the configuration of their host systems which in turn ensures greater performance on low end systems.

In our research, we identified several gaps in the existing approaches to vulnerability assessment, which have been addressed in our project. These gaps include:

1) *Division of Phases:* The traditional process of vulnerability assessment often lacks clear division of phases, which can result in inefficiencies and confusion. In our framework, we have carefully divided the process into two major phases, namely Reconnaissance and Vulnerability Scanning. This clear division allows for better organization and management of the assessment process, leading to improved overall efficiency.
2) *Multiprocessing:* Our framework adopts a multiprocessing approach, where multiple tasks can be executed in parallel, leading to improved efficiency and scalability. This approach makes better use of available resources and allows for future extensibility. By leveraging the power of parallel processing, our framework has the potential to achieve faster and more efficient vulnerability assessment.

3) *Flexibility:* The proposed framework is designed to be highly flexible, allowing for customization through the addition of custom templates. This flexibility enables users or testers to target specific vulnerabilities of interest and customize the framework to suit their specific needs. This level of customization enhances the framework's adaptability to different scenarios and makes it more user-friendly.
4) *Multi-user Deployment:* Our framework is deployed as a web application, which enables it to be accessed by multiple users simultaneously. This multi-user capability allows for collaboration and concurrent usage by multiple testers or users, making it more practical for team-based assessments or larger-scale security testing scenarios.

V. SYSTEM ARCHITECTURE



1) *React Frontend:* The REACT FRONTEND will provide the user with a graphical interface where the user will input the target domain. The user can add a single target or multiple targets. The interface will also display the targets previously scanned with the found information and scan results.
2) *Rest API:* The REST API acts as the interface between the interface and the modules of the framework. It provides the frontend with various endpoints to retrieve information and perform various functionalities.
3) *Recon Module:* The recon module includes a set of tools used in information gathering. The information can include subdomains, hidden directories, open ports, input endpoints.
4) *Scanning Module:* The scanning module of this framework works using three tools that are NIKTO, ZAP and NUCLEI. The first two tools scan the application for predefined vulnerabilities and CVEs and the third module is extremely useful as it allows the user to add custom templates for finding vulnerabilities depending upon the assessment requirements.

5) *Database:* The database will store all the information's related to the scan. The information includes the user information, Domain information, Subdomains, vulnerable parameters.
6) *Report:* Finally the Framework will provide the user with the open to generate a report based on the information gathered. Security experts can make use of these reports to support their VAPT assessments. This will provide the tester with a solid foundation for conducting thorough assessments and finding more security bugs in the application.

VI. FUTURE WORK

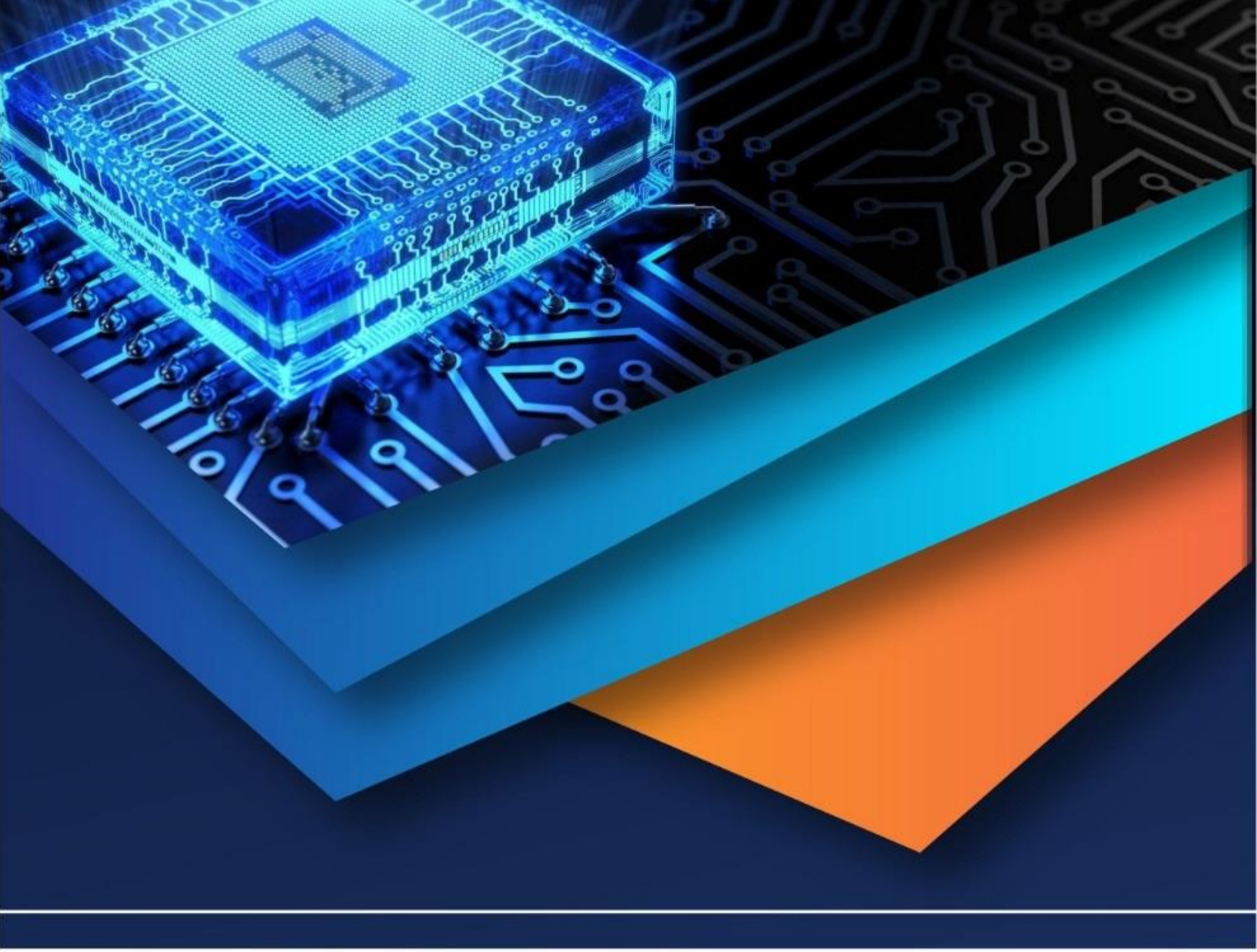
1) Customization and Configuration: Customizations can further enhance the flexibility and configurability of your framework by allowing users to customize and configure various aspects of the scanning process. It would allow the scanner to comply more with the user's methodology.
2) Machine Learning and Artificial Intelligence: Integration of AI and ML into the project would help enhance the tool's capabilities further. This could include developing machine learning models for identifying vulnerabilities or patterns in the data, leveraging natural language processing for report generation and analysis.
3) Integration with DevOps: The framework can be integrated with the DevOps pipelines, integrating the framework with DevOps pipelines to facilitate continuous security testing and reporting throughout the software development lifecycle.
4) Security Testing beyond Web Applications: Scope of the framework can be expanded to include security testing beyond web applications, such as mobile applications, APIs, network devices, and other emerging technologies.
5) Scheduling and automatic Orchestration: The framework can include features like Scan scheduling which would help in increasing the testing surface and identifying new vulnerable features. It would also help organizations to ensure the security of their applications.

VII. CONCLUSION

In conclusion, our survey report highlights the challenges and limitations of using open-source tools separately for information gathering and vulnerability scanning and proposes a framework that provides a unified interface for simultaneous tool usage with flexibility for customization. The proposed framework addresses the identified problems and offers a streamlined approach to efficiently perform reconnaissance and vulnerability scanning tasks. The framework's modular design, user-friendly interface, and extensibility through custom templates make it a promising solution for security practitioners and researchers. The integration of multiple tools into a single framework saves time and effort, while the ability to add more tools and customize options enhances its flexibility and adaptability. Overall, the proposed framework presents a promising approach to address the challenges of using open-source tools separately and offers a foundation for further advancements in cybersecurity.

REFERENCES

[1] IEEE," An Automatic Vulnerability Scanner for Web Applications", 2020.
[2] IEEE," Framework for Web Application Vulnerability Discovery and Mitigation by Customizing Rules through ModSecurity", 2019.
[3] IEEE," Design and Implementation of Core Modules of WEB Application Vulnerability Detection Model", 2019.
[4] IEEE," Vulnerability Assessment and Penetration Testing of Web Application", 2017.
[5] IEEE," Automation of Cyber-Reconnaissance A Java-based Open-Source Tool for Information Gathering", 2017.
[6] Bug Bounty Guide, "https://bugbountyguide.org/2022/11/26/8-best-recon-technique-for-active-subdomain-enumeration/"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY