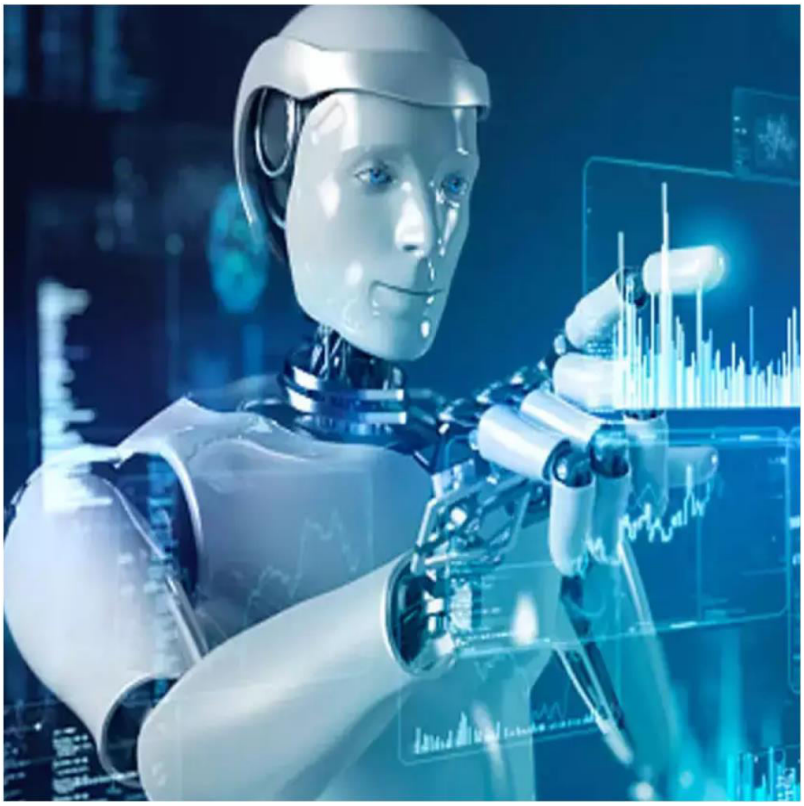
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.524

Volume 14, Issue 1, January 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

Website Vulnerability Scanning System

Meesala Revanth Kumar Naidu[1], Meesala Rohith Kumar Naidu[2], Gavini Rama Sandeep[3], Panchireddy Venu Babu[4], Mopidevi Balaji[5]

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

U.G. Student, Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

ABSTRACT: As we see the rapid development of technology in our society, people need to update themselves to stay safe There are some technologies used by humans that can be very dangerous for various groups such as organization's providing services to humans a they use websites and various assets.

Vulnerability scanning systems can be used to find, fix and repair security holes in web applications and networks. Uses automated scanning techniques to ensure that code, operating systems, and configurations are strategically reviewed for unsafe coding practices — such as SQL injection, cross-site scripting, etc. Geared for organizations of all sizes, our solution provides in-depth findings and actionable insights. To improve security level provides reports. The user-friendly interface and customizable design make the system technical and non-technical, to combat cybersecurity aggressively. Organizations can reduce their exposure to risk and protect valuable data while also remaining compliant with regulatory requirements by implementing such vulnerability scanning solutions.

Having a robust online presence requires an unwavering commitment to security. Our vulnerability scanning system provides a comprehensive analysis to identify potential vulnerabilities in the design of your website. Our platform uses advanced scanning techniques and expert analytics, ensuring that your digital assets remain safe from ongoing threats. We provide comprehensive reporting and actionable insights to empower businesses and individuals alike to prioritize security and protect critical information. Stay ahead of cyber threats Improve the resiliency of your website with our reliable and effective vulnerability scan.

KEYWORDS: Website Scanning, Vulnerability Assessment in Websites

WEBSITE VULNERABILITY SCANNING SYSTEM

Websites are the set of web pages and related content that are linked all together and share a particular domain name for the identification. There are several uses of the websites that are like:

Personal Usage: Sharing the information about their daily life's and related useful information for which they are working on
Education: In these recent days the websites which are known as the W3 Schools, JavaTpoint, GeeksforGeeks and etc.., are sharing the information that are related to the educational assets and information.
Business: In the recent days every organization which providing the resources they are maintaining some websites to provide them for further purposes or uses.

We can see that website are very important aspect of every organization as we observe for every usage of the asset there are also the cons for it. Websites are also having the some of the unused or used functions which can lead them to vulnerable and they need some secure environment for testing their website before they deploy their websites. Some of the security organizations provide some of the tools which can test their website for vulnerabilities. Some of the security organizations provides some IDE (Integrated Development Environment) for securing the organizations websites and their assets in a secure environment.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

I. INTRODUCTION

In this world where the bugs or vulnerabilities are present in everywhere like assets of IOT, mobiles, websites etc, organizations are facing critical data breaches and serious data security challenges in the environments. The need of vulnerability scanners for organizations that will identify the founded bugs or vulnerabilities areas which had a great impact on the organization's assets or reputation. There are several vulnerability scanners like the Nessus, H3ping, Burpsuite, zenmap they are third party tools for the organization. Organization need a vulnerability scanner for their hosting websites for protection of their sensitive data of the organizations, customers, stakeholders, etc. There is a need for the vulnerability scanners that can keep data confidential while providing secure environment to the hosting websites in the organizations.

II. RELATED WORK

As web applications increasingly become integral to everyday life, ensuring their security is paramount. The importance of his cannot be overstated, as web attacks have seen a dramatic increase, primarily due to insufficient input validation mechanisms. Specifically, focused on the threat posed by injection vulnerabilities, including both SQL injection and cross-site scripting (XSS) injections. Despite the widespread awareness of these vulnerabilities and the availability of methods to prevent them, a significant number of developers still lack the necessary security training and awareness. This leaves a vast number of websites vulnerable to attacks, compromising user data and integrity. In response to this challenge, introducing a novel approach: an automated vulnerability scanner designed to specifically target and identify these types of injection attacks. By focusing on SQL injection and XSS vulnerabilities, this system aims to enhance the security of the web landscape, which is continually expanding and evolving. The scanner works by automatically analyzing websites to detect potential exploitable vulnerabilities in their input validation processes. Beyond merely identifying these vulnerabilities, this system also suggests prevention methods. These strategies help the developers to mitigate and identify risks, thereby safe guarding websites against such attacks. Proposed solution contributes significantly to the field of web application security and protect countless cyberattacks.

Vulnerability data assessment is the process of identifying, assessing, indexing, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. Automated testing tools such as Nessus, Acunetix, and Netsparker are commonly used in vulnerability assessment to provide information about identified vulnerabilities and their remediation methods. One of the types of vulnerability data assessment is application scans, which are utilized to test websites and identify common vulnerabilities. Passive scanning is a method used in vulnerability detection that leverages information obtained from transmitted data without direct interaction. It provides information such as the operating system in use, active ports, and installed applications. CVSS (Common Vulnerability Scoring System) is an assessment system that assigns numeric values reflecting the difficulty level of vulnerabilities. These numeric values are then converted into qualitative ratings such as low, medium, high, and critical, aiding in prioritizing remediation efforts. The system consists of metric groups that generate scores, including base score, temporal score, and environmental score. This work aims to utilize vulnerability assessment to assist developers in addressing identified vulnerabilities in developing or existing websites. Through experimentation, the system developed in this thesis demonstrates the capability to perform both on-demand and scheduled vulnerability assessments, providing comprehensive vulnerability reports upon completion of the process. The findings of this research contribute to enhancing the security of web applications by enabling efficient vulnerability management and prioritized remediation strategies. Keywords— passive scanning, vulnerability data assessment, data engineering, security, CVSS, ICT infrastructure.

This research presents a novel framework for automated web application security scanning and information gathering using the Axiom methodology. The framework assists organizations and security researchers in identifying and mitigating vulnerabilities in web applications by automating the discovery of publicly available assets and filtering targets based on initial responses, open ports and other criteria. The use of the Axiom methodology allows for faster scanning times and distributed scanning, making it useful for bug bounties and penetration testing. The framework's performance, limitations and challenges are evaluated. The research demonstrates the potential of the framework in improving the efficiency and scalability of web application security while emphasizing the need for proper configuration and ethical considerations. Keywords: Web Application Security, Automated Security Scanning, Axiom Methodology, Vulnerabilities, Bug Bounties, Penetration Testing, Continuous Monitoring, Automatic Alerting, Configuration, Ethical Considerations.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

Due to the internet's rapid advancement, net safety concerns are becoming more widespread. Hackers will use internet weaknesses to get access to websites, which will result in multiple safety mishaps. An inspection tool that searches websites for security flaws is called a website vulnerability scanner. Web vulnerability scanners have a number of issues on the market, including low scalability, large software, and insufficient scanning accuracy. Conventional scanners usually retrieve the website URL using a crawler, send an attack request to the website with the payload to obtain it, and then output the relevant vulnerability document if the payload can be proven to work. The usage of vulnerability scanners to find vulnerabilities on websites has some utility because it is based solely on these security concerns. Unlike other scanners, this one doesn't have the issues listed above and covered in-depth in the document. Keywords: Vulnerabilities, Scanner, Website.

The commercial value of web applications has significantly increased in recent years. They progressed from simple information-sharing platforms to more sophisticated business applications. Web-based apps, unlike most other technologies, are always accessible from anywhere in the world. This makes them ideal targets for malevolent cyberattacks. Scanners can identify and mitigate an organization's vulnerabilities. However, without a thorough awareness of a system's weaknesses, it would be difficult to undertake effective network defense in order to keep intruders out in the real world. As a result, vulnerability scanning is an important part of a cybersecurity curriculum's success. In this paper, we'll look at the present state of open-source vulnerability scanning technologies. A literature review of vulnerability assessment and reporting, vulnerability scanning, vulnerability scanning technologies, security vulnerabilities, system and application security, and malicious cyber-attacks reveals that a lot of work is being done in this area. This research provides an in-depth examination of vulnerability scanning technologies. In this paper, we covered two important topics: vulnerability scanning and reporting. Then, after identifying gaps in relevant practices and presenting chosen findings, we emphasize future directions and bring this study to a conclusion. The top open-source network vulnerability scanning tools are described in detail. Keywords—Vulnerability assessment, Vulnerability, Security, Threat.

With the increasing concern for security in the network, many approaches are laid out that try to protect the network from unauthorised access. New methods have been adopted in order to find the potential discrepancies that may damage the network. Most commonly used approach is the vulnerability assessment. By vulnerability, we mean, the potential flaws in the system that make it prone to the attack. Assessment of these system vulnerabilities provide a means to identify and develop new strategies so as to protect the system from the risk of being damaged. This paper focuses on the usage of various vulnerability scanners and their related methodology to detect the various vulnerabilities available in the web applications or the remote host across the network and tries to identify new mechanisms that can be deployed to secure the network. KEYWORDS Vulnerability, Static analysis, Attack graph, Scanners, Test–Bed

In today’s world, cyber security has become an important leap in the form for jobs, education. But the reality is the only a few are aware of the major wed vulnerabilities. Some statistical studies show that small scale industries are directly and indirectly connected to the world of internet, but penetration testing, we are going to do this project. In a website if there are any vulnerability, the website can easily hack. So, using penetration testing we are going to build a scanner which will find the vulnerabilities the website. With the help of vulnerability scanning in a website, inspection of the potential points of exploit on a website to identify security holes. A vulnerability scan will deduct and classifies system weakness. It will also deduct bugs in a website and communication equipment. It will predict effeteness of counter measure. Keywords: Cyber security, vulnerability, penetration testing, website scanning

Web applications are becoming truly pervasive in all kinds of business models and organizations. Today, most critical systems such as those related to health care, banking, or even emergency response, are relying on these applications. They must therefore include, in addition to the expected value offered to their users, reliable mechanisms to ensure their security. In this paper, we focus on the specific problem of cross-site scripting attacks against web applications. We present a study of this kind of attacks, and survey current approaches for their prevention. Applicability and limitations of each proposal are also discussed. Keywords: Network Security; Software Protection; Injection Attacks.

In today’s world, Cyber security has become an important leap in the form of jobs, education. But the reality is that only a few are aware of the major web vulnerabilities. Some statistical studies show that small scale industries are directly and indirectly connected to the world of the internet, but they are not aware of the major web vulnerabilities of their web application. Since website hosting has become common nowadays, most of the web applications are prone to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

attacks and malicious attacks of web applications. Assessing and avoiding these vulnerabilities require deep knowledge of these vulnerabilities. There are numerous online scanners available on the Internet that provides only paid limited service. The tools are made in a way that it can only operate in command line interface or in any programming language. So it is a difficult task for a normal person to operate the scanners without previous knowledge. This paper presents a vulnerability scanner that scans the website and detects specific vulnerabilities, along with its location and solution. The vulnerabilities that the scanner considers are: SQL injection, cross site scripting.

WEBSITE VULNERABILITY SCANNING SYSTEM OVERVIEW

a) Dynamic Analysis:

A crucial approach for the vulnerabilities scanning system in the websites is a dynamic analysis, which focuses on examining the scanning the every each of information in the website. It involves in real – time data interaction, data processing and server communication in the server on how the data can be communicated. It updates systems content and performs actions based on user inputs, API calls, and data base interactions.
it had some of the functions that this project is a dynamic approach for some functions that are undergoing process:

- Real – time Interactions: User interacts with your system by submitting the URLs for scanning and how the system responds by performing the real – time scans. A static analysis system would not allow this level of interaction because the content which is present in the static web pages is fixed
- Background Communication: In this project we use an API that is known as the VITE API. It is an API (Application Programming Interface) which the systems communicate with processing of data wand interacts with APIs to perform dynamically. This interaction between the front-end and backend makes the system dynamic as the content is generated and processed based on the user which have requested the data in real time.
- Data Processing and Response: The scanning system processes the data which are vulnerable for each website it can be (functions in code or outdates packages which are being used in the code). It means the output is not fixed but dynamically generated based on the results of each scan which they produced.
- Report Generation: For every scanning the report will be generated based on the which type of scan it is and it specific to that website. whereas static systems do not provide any reporting capabilities in real time and instead they display predefined content.
- Use Of APIs and Proxy Based Scans: Using of the some of the tools like OWASP ZAP and API – Based scanning, the systems are dynamically scans the live websites, processes real – time traffic (in proxy mode) and reacts to the results in real time . These elements involve continuous interactions between the client and server.

b) Dynamic Features:
1. User Input
2. Real – Time Scanning
3. Interactive UI
4. Reporting

III. IMPLEMENTATION

1. System Architecture:

This project most developed in the architecture as microservice with their perspective elements as frontend (React.js) and backend (Vite API). In the architectural part it is divided into several aspects of the development.

- Client – Server Architecture: Systems uses the traditional client – server model where the frontend part reacts with the backend to fetch and process the data. The server is responsible for handling the requests and executing the vulnerability scans and returning the results, as the presentation of the data for the client is in user – friendly format.
- Proxy vs Non – Proxy Flows:
- Proxy – based Method (OWASP ZAP): OWASP ZAP is interacts between the client and the web applications or websites that are being scanned. ZAP acts as a proxy, intercepting the traffic between the client and server, allowing to detect the security vulnerabilities in real time.
- Non – Proxy Method: It uses some of the APIs that are which have been used in the development side and here the VITE API sends requests directly to the web application and analyses the response for common vulnerabilities.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

2. Framework:

In this project two types frameworks have been used as the frontend and backend

- Frontend Framework: As the scanning system has developed in the REACT. Js, it is a powerful JavaScript library for generation and building the user interfaces. React is known for the component – based architecture which allows code reusable, modular of the code and it also helps in the fast rendering using the Virtual DOM.
- Backend Framework: As the scanning system has developed in using of APIs like VITE API, it is a modern JavaScript build tool that provides the faster and learner development workflows. It is also helping bundle the system into efficient modules, serving as the foundation for API requests.
- VITE: It is chosen for its high – speed build times and ability to handle the HMR (HOT Module Replacement) efficiently , ensuring the real – time data updates during development and iterative web applications .

3. Data flow:

As the first comes to the scanning system is the frontend part which the users submits a URL via the user interfaces which is built in the React.js and the second comes the background part which acts like undergoing process that is VITE API , it receives the request , processes it by initiating either a proxy – based scan (via OWASP ZAP) or another method is the non – proxy scan , depending the user choices and then scanning part where the system either proxies requests through zap or makes the API calls directly to scan the website and last part is the Results it analyses the responses and returns a detailed report on the found vulnerabilities and report it in the interactions of frontend where it can be viewed by the user.

4. Software Requirements:

- Web Browser:
  - React Js: it is a java script library that allows the developers to create user interfaces (UIs) for websites, mobile apps and desktop apps. it should be the version 17 or above
- Backend End:
  - VITE API: it is an free, open – source frontend tooling development environment several API s, here we use the Java Script API and it is an fully typed typescript or enables JS type checking in VS code
  - OWASP ZAP: it is an open – source tool that helps in scanning and identifying and fix security vulnerabilities in web applications and websites. And it should be integrated with scanning system. This could either be run locally or through a docker container.

IV. METHOD

Method flow for this project includes a several steps for building the website, processing, intercepting and reporting

1. User Interaction: The user initiates a scan for vulnerabilities by inputting a website or domain URL through the React.JS frontend
2. Request Processing: It is a further step where the frontend sends an HTTP request to the VITE API with users chosen URL whether selecting the proxy or non – proxy method.
3. Proxy – Based Flow: if this method has been selected, the VITE API forwards the request to the OWASP ZAP, which we need to a particular key and it is also acts as a proxy between the client and the target website. ZAP intercepts and analyses all traffic between the client and the website and detecting the security flaws in it.
4. Non – Proxy Flow: if this method is selected the VITE API directly sends requests to the target website without any traffic interception and the responses are analysed suing a predefined set of rules to detect the flaws in it
5. Result Compilation: The results from which had been done in the scanning process (either it can through ZAP or API – based) are compiled into a detailed report by the backend
6. Response: The Vite API returns the scan results to the interface which displays them to user in a proper and readable format
7. Error Handling: The scanning system handles potential error like invalid URLs, timeouts or failed scans by providing feedback to the user.

V. RESULTS AND DISCUSSION

In this project that we have developed website vulnerability scanning system using react.js and VITE API, we implemented the two methods for these methodologies like: proxy – based scanning with OWASP ZAP and non –

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

proxy API – based scanning. This scanning system that we have developed was tested across various websites to evaluate its efficiency, accuracy, and detection capabilities

The proxy – based method using the OWASP ZAP is an very effective in identifying vulnerabilities related to web traffic analysis, such as improper session handling and security misconfiguration which can lead the organizations to a greater impact of losing the trust from the endpoints or organizations.

The Non – proxy API – based offers a faster and more lightweight scanning process. when we can compare it to the proxy – based scanning the non – proxy-based scanning it did not catch vulnerabilities that are tied to the traffic interception, it is also able to detect the more general vulnerabilities in efficiently such as the SQL Injection and XSS through the direct API calls.

When we compared to both of the methodologies which are proxy – based and non – proxy API based are revealed both strengths and limitations in each stage. The proxy – based approach with the OWASP ZAP, while slower due to traffic interception and deep analysis that is proved to be more thorough in detecting the high critical vulnerabilities that are present in the real – time websites which is in the inspection.

Whereas Non – proxy API – based scanning showed its strength in the particular environments where the speed and easier of integrating priorities. This method provides the quick response time and it is easier to deploy without the need for setting up a proxy.

As per our perspective we have choose the react.js frontend because of the it features and provides highly effective in providing the responses and interactive user experience. We have set a asset for the users are able to submit the URLs for scanning and receive the detailed vulnerability reports in a user – friendly format. we also choose the VITE API for seamless communication between the frontend and backend API that is powered by the VITE, it is also ensures that scan results were delivered in a timely manner regardless by the choosing the scanning method.

VI. FUTURE WORK

- Integration of AI and Machine Learning: Implementing the machine learning models to predict and identify the detect the vulnerabilities by learning from the previous scans. This could help from detecting the zero – day vulnerabilities
- Integration of CI/CD: This scanning system can be integrated into CI/CD pipelines so that vulnerability scanning is done automatically triggered during development.
- Enhanced Reporting and Dashboards: Adding the more capabilities of the interactive and detailed visualization tools for the reporting allows users to filter vulnerabilities as per their perspective.
- Scalability: Mainly focusing on scaling the backend of this project for handling the multiple assets scans concurrently, enabling the system to handle the large-scale enterprise use cases. This might involve various aspects like moving to the distributed architecture with containerization (using tools like docker and kubernets).

VII. CONCLUSION

The website vulnerability scanning system that we are deployed successfully has met the projects objectives by offering the two methods for detecting the vulnerabilities those are proxy based with OWASP Zap and non-proxy API – Based scanning. Each method demonstrated its every strength, with the proxy – based method provides a comprehensive vulnerability coverage with the non – proxy approach offers a faster scan with fewer resource requirements.

These two approaches give users the flexibility to choose the method that best suits their needs. This project serves as a valuable and open – source tool for organizations looking to enhance their website security. The combination of the two scanning approaches allows for the flexibility and adaptability, providing the both thorough and quick vulnerability detection. It also demonstrates the potential for future innovation in the field of securing the websites.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 1, January 2025

|DOI: 10.15680/IJIRSET.2025.1401067|

REFERENCES

[1] Martin, D., & Jurjens, J. (2005). Security analysis using automated vulnerability scanning tools. IEEE Security & Privacy, 3(3), 37-44.
[2] Goseva-Popstojanova, K., & Perhinschi, M. G. (2015). On the capability of static code analysis to detect security vulnerabilities. Information and Software Technology, 68, 18-33.
[3] OWASP Foundation. (2025). OWASP ZAP Project: An open-source web application security scanner. Available at https://owasp.org/www-project-zap/.
[4] Scarfone, K., & Mell, P. (2007). Guide to vulnerability scanning. NIST Special Publication 800-115. Available at https://csrc.nist.gov/publications/detail/sp/800-115/final.
[5] Suto, A. (2010). Performance analysis of web application scanners. NCC Group Research Report. Retrieved from https://www.nccgroup.com/.
[6] McGraw, G. (2004). Software security. IEEE Security & Privacy, 2(2), 80-83.
[7] Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. IEEE Transactions on Software Engineering, 37(3), 371-386.
[8] Sheth, A., & Subramanian, V. (2018). Leveraging machine learning for advanced vulnerability detection in web applications. ACM Computing Surveys, 51(5), Article 97.
[9] MITRE Corporation. (2025). CVE Program: Common vulnerabilities and exposures. Retrieved from https://cve.mitre.org/.
[10] Wichers, D. (2013). OWASP Top Ten Project 2013. Available at https://owasp.org/www-project-top-ten/.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details