International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 10, Issue 1, 2024, PP 8-15
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
https://doi.org/10.20431/2349-4859.1001002
www.arcjournals.org

Web Vulnerability Scanning Tools: A Comprehensive Overview, Selection Guidance, and Cyber Security Recommendations

Assem I. Mohaidat[1], Dr Adnan Al-Helali[2]

[1]*Department of Cyber Security, Irbid National University, Irbid*
[2]*Cyber Security Department, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan*

Corresponding Author:** ***Assem I. Mohaidat, *Department of Cyber Security, Irbid National University, Irbid*

Abstract: *The large number of people using the Internet and put all their data on it, which that increase the risk of cyber breaches, and the issue of cybercrime has become a very sensitive topic, so the need has emerged to use vulnerability scanning tools on the web. This paper aims to your definition to web vulnerability scanning tools and provide guidance on how to choose these tools wisely. We will provide an overview of some of these tools, and then we will explain of the most important factors that must consider when choosing the appropriate tool. We will suggest recommendations to individuals and organizations with the aim of increase web application security and prevent the cyber-attacks. The methodology used in this paper is the analytical research methodology, as we will present in this research a comprehensive overview and accurate analysis of this sensitive topic, and we hope that it will be useful to everyone who seeks to achieve safety from cyber-attacks.*

Keywords: *web vulnerability, scanning tools, cyber-attacks, cyber security*

1. INTRODUCTION

During the past decade, especially after the COVID-19 pandemic, the importance of safety on the web has emerged because the current period is the period of the digital age, and life has become fundamentally dependent on the Internet for all categories of people and for all fields such as business, politics, and even in times of recreation. The Internet has controlled most of People's times, as most of their information, whether personal or practical, is available on the Internet, which has opened the door for the theft of this information and its use for personal purposes.

The aims from this research to identify web vulnerability scanning tools and provide guides on how to choose the web vulnerability scanning tools wisely. We will provide a comprehensive overview of some of these tools, then explain the most important factors that must be taken into consideration when choosing the appropriate tool, then suggested recommendations for individuals and institutions with the aim of enhancing the security of web applications and preventing cyber-attacks.

The advancement of web vulnerability scanning tools is considered a crucial complement in the field of cyber security and provides opportunities for sustainable improvement in web security, as identifying the appropriate tools is extremely important. The importance of this study is to provide individuals and institutions in the field of cyber security with the necessary knowledge and guidance in Choosing web vulnerability scanning tools. The methodology used in this research is the analytical research methodology, as we will present in this research a comprehensive overview and accurate analysis of this sensitive topic, and we hope that it will be useful to everyone who seeks to achieve safety from cyber-attacks.

1.1. Objectives of the Paper

- Clarifying understanding about the types of web vulnerability scanning tools and their importance in the field of cyber security.
- Guiding individuals and institutions on how to choose the appropriate tools for their specific needs.
- Explaining the factors affecting the process of selecting tools and providing advice to facilitate this process.

1.2. Research Questions

- What types of web vulnerability scanning tools are available and how do they differ in terms of goals and features?
- What are the factors that influence choosing the appropriate vulnerability scanning tool, and how can it be classified (such as performance, ease of use, cost, etc.)?
- What are the methodological steps that must be followed to choose a vulnerability scanning tool wisely?
- What guidance and advice can be provided to individuals and institutions to ensure that screening tools are chosen wisely?

2. Related Word

2.1. Scanner

This module scans the website to obtain links and can detect forms as well as input fields for certain types of attacks. It represents the initial stage of the process. The process begins by inputting the root URL, performing authentication if required, and then navigating from page to page to identify other URLs and elements such as forms.

However, the system must provide a mechanism to identify already visited links to prevent the process from continuing indefinitely. This mechanism could take the form of a maximum depth marker or a stop condition. In our solution, this is implemented using the Beautiful Soup library and Selenium. While Selenium automatically navigates from page to page, the Beautiful Soup library parses each page to extract the required elements such as links, forms, and other input elements.[1]

2.2. Vulnerability Scanning and Vulnerability Scanne

Vulnerability scanning is a structured and deliberate process which aims to find the potential weaknesses in one organization's environment immersed in Yuji Rose c internet security. This process involves using specialized tools and techniques to identify puncture wounds that cyber threats may utilize. This procedure is a necessary part of a broader vulnerability management plan. Such programs are designed to head off the effect of cyber invasions on an organization and reduce risks from data breaches.

The vulnerability scanning works like a security health check for digital systems. It systematically assesses and analyzes the security infrastructure to detect any vulnerabilities that might expose the organization to potential risks. Through identifying these weaknesses, organizations can take actions and timely to address and rectify them, ultimately enhancing the overall cyber security state and the ability to confront against potential cyber threats. The important goal is to increase the organization's defenses, reducing the likelihood of successful cyber attacks and minimizing the impact of any potential security incidents.

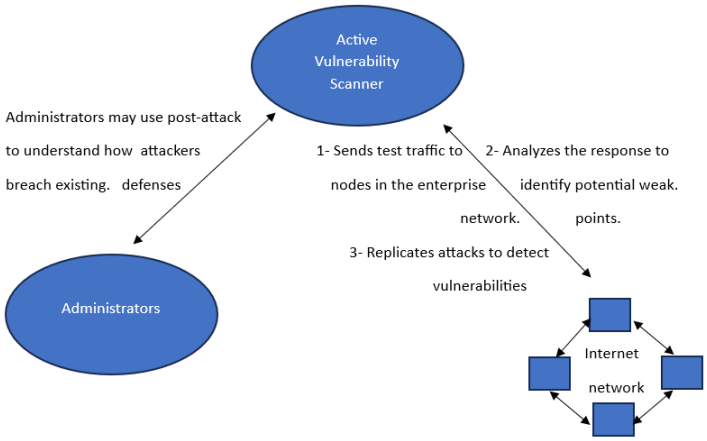
Vulnerability Scanner is a tool designed to automatically search for and report open network security vulnerabilities. The most effective scanners ensure inclusive coverage of your environment, assisting in gaining a inclusive understanding of an organization's overall security posture.

A vulnerability scanner conducts an automatically examination of the network or system to determine potential security weaknesses. By doing that, it allows the organization to obtain a inclusive picture of its security status. These tools simplification the analysis and reporting processes, enabling security teams to take necessary actions for correction and enhancement of security effectively.

3. Network Scanning Methodologies

The methodology focuses on a vital stage in penetration testing operations or cyber auditing, which is Network Reconnaissance. Using Active or Passive scanning tools, detecting assets and services is crucial for assessing vulnerabilities in a network.

An Active Vulnerability Scanner sends test traffic to nodes in the enterprise network and analyzes the responses to identify potential weak points. Security teams use these scanners to replicate attacks, aiming to detect the vulnerabilities that hackers could exploit. Additionally, administrators may employ active scanners post-attack to understand how attackers breached existing defenses.

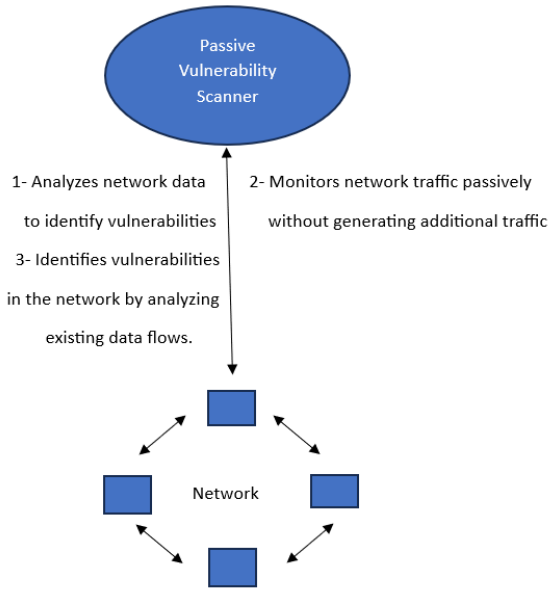


3.1. Active Vulnerability Scanner

Benefits of Active Vulnerability Scanners:

- Continuous Monitoring Achievement: Active vulnerability scanners prove particularly valuable when an organization requires ongoing monitoring to ward off potential threats.
- Vital Device Information Provision: These tools furnish crucial information about devices, encompassing:
  - Device name
  - IP address
- Detailed Configuration Insights: Active vulnerability scanners offer in-depth insights into configuration details, such as:
  - Device make and model
  - Type of installed software applications
  - Software version
  - Operating system type and patch level
  - Firmware type and version

A Passive Vulnerability Scanner is a tool that monitors the flow of network traffic to gather information about the systems and endpoints within the network. the opposite of active scanners, a passive scanner observes and collects data without directly interacting with these systems through actions like sending probe requests or requesting probe responses.



3.2. Passive Vulnerability Scanner

The Benefits of Passive Vulnerability Scanners:

1) Understand data exchanges with various endpoints:

   Gain comprehensive insights into the data being sent to and received from different systems.

2) Monitor currently used operating systems:

Provide real-time monitoring of the operating systems in use.

3) Monitor various software and their versions:

Offer information about different software applications and their respective versions.

4) Monitor available and running services:

Identify available services and those currently operational within the system.

5) Identify network components, including open ports susceptible to threats:

Recognize network components and open ports that may be vulnerable to potential threats.[2]

4. ADVANTAGES OF VULNERABILITY SCANNING

Organizations can derive several benefits from vulnerability assessments without resorting to artificial intelligence:

1- Automation: Vulnerability assessments can be scheduled or initiated as needed, such as in response to specific events like a software project update or server deployment. This ensures the maintenance of an up-to-date overview of the vulnerability landscape.

2- Speed: Scanners have the capability to execute hundreds or even thousands of checks at a pace significantly faster than manual testing would allow.

3- Cost-effectiveness: The combination of speed and automation makes vulnerability scanning a more economical option compared to manual testing, making it feasible to scan a target efficiently.

4- Scalability: With modern cloud-based architectures, services can adjust their resources, allowing scanning of both small and large environments within similar timeframes.

5- Compliance: Many vulnerability scanning solutions include customized checks to assess compliance with widely accepted information security standards or an organization's established baseline control set.

6- Accuracy: Through tailored checks to verify the existence of vulnerabilities, scanners can produce more reliable results compared to relying solely on information stored in software asset management solutions.[3]

5. TYPES OF A VULNERABILITY SCANNER

The Cyber security has become increasingly important to find and fix security vulnerabilities in our digital setups. Web apps are a critical part of how we connect today, and unfortunately, they're often targets for cyber-attacks. To stay ahead of the curve, vulnerability scanners have become key tools. They are essential for checking the security of these apps and helping to prevent attacks.

This article delves into various types of Vulnerability Scanners, each catering to distinct aspects of system security. Understanding the nuances of these scanners is essential for organizations and individuals seeking to fortify their digital assets against cyber threats.

1. Host-Based Scanners: - Host-Based Scanners play a pivotal role in identifying issues within the host or system. By deploying these scanners, vulnerabilities are detected and diagnosed effectively. The installation of a mediator program on the target machine enables continuous monitoring, allowing for the tracking of incidents and real-time alerts for security analysts.

2. Network-Based Scanners: - Network-Based Scanners focus on discovering open ports and identifying unfamiliar services utilizing them. This approach uncovers potential vulnerabilities associated with these services. Network-Based Scanners play a critical role in fortifying the overall network security by discovering and addressing potential threats.

3. Database-Based Scanners: - Database-Based Scanners used advanced tools and techniques to discover security vulnerabilities within database systems. Special emphasis is placed on preventing SQL Injections, a malicious technique where attackers inject SQL statements into a database, compromising sensitive data and allowing unauthorized data manipulation.

4. Wireless Network Scans: - Wireless Network Scans concentrate on potential attack sites within the wireless infrastructure. Confirming the secure configuration of a company's network and detecting unauthorized access points are primary objectives. This type of scanning is essential in safeguarding wireless environments against potential breaches.

5. Application Scans: - Application Scans are dedicated to examining websites for known software flaws and discovering inappropriate network or web application setups. By testing web applications, these scanners contribute to ensuring the integrity and security of online platforms.

Vulnerability Scanners are developed software designed to analyze a network's design, report flaws, and provide actionable recommendations for remediation. a vulnerability Scanners play an important role in cyber security by offering prediction into Common Vulnerabilities and Exposures (CVE). the CVE beside the Common Vulnerability Scoring System (CVSS), helping in assessing the severity of vulnerabilities based on factors such as attack vector, complexity, required privileges, user involvement, and the impact on confidentiality, integrity, and availability. Understanding the diverse functionalities of these scanners is pivotal for making informed decisions in the realm of cyber security. [4]

On the other hand, we could type of vulnerability scanning tools based further divided in terms of the most common tools used for vulnerability assessment encompass a wide range of software designed to identify, evaluate, and address security vulnerabilities within an organization's IT infrastructure. These tools serve as essential components of an organization's cyber security strategy. They include:

1. Port Scanners: this type is used to scan a system or network for open ports, which can be potential entry points for attackers Example: Nmap (Network Mapper)

2. Network Vulnerability Scanners: this type examines network devices and systems for known vulnerabilities and misconfigurations, helping to identify weaknesses that could be exploited Example: Nessus

3. Web Application Scanners: those tools are focused on web applications, these discover vulnerabilities such as SQL injection, cross-site scripting, and other web-related security issues Example: Acunetix [5]

4. Database Scans: Database scanners assess the security of database systems by scrutinizing setup, access controls, and stored data for vulnerabilities, including insecure permissions, injection issues, and unsafe configurations. They offer valuable insights to enhance database security and protect sensitive information. Example: Scuba Database Vulnerability Scanner

5. Source Code Scans: In the early stages of development, it is crucial to proactively assess source code for security vulnerabilities to address issues before they become costly to correction. those tools analyze software applications' source code, detecting security flaws, coding errors, and vulnerabilities. They focus on discover the potential issues like input validation errors, improper coding practices, and the use of vulnerable libraries. Throughout the software development lifecycle, source code scanners play a vital role in helping developers discover and correct vulnerabilities, to ensuring a more secure and strong final product. Example: Snyk scans

6. Cloud Vulnerability Scans: it assesses the security of cloud environments, including IaaS, PaaS, and SaaS installations, providing recommendations to enhance deployment security. They examine cloud configurations, access restrictions, and services to discover misconfigurations, inadequate security practices, and vulnerabilities specific to cloud platforms. Example: Wiz [6]

These tools often offer automated scanning and reporting ability, which allow organizations to address security vulnerabilities dirctly before they are exploited by attackers. When properly selected and implemented, these tools can support an organization's overall cyber security status.

We will now summarize the above with Table1 showing each type and the appropriate working area for each tool.

Table1.

Type of Scanner	Example of the tool used	Focus Area
Port Scanners	Nmap (Network Mapper)	Scanninga system or network for open ports, potential entry points for attackers
Network Vulnerability Scanners	Nessus	Examining network devices and systems for known vulnerabilities and misconfigurations
Web Application Scanners	Acunetix	Focused on web applications: Discovering vulnerabilities like SQL injection, cross-site scripting, and other web-related issues
Database Scans	Scuba Database Vulnerability Scanner	Assessing the security of database systems: Scrutinizing setup, access controls, and stored data for vulnerabilities
Source Code Scans	Snyk scans	Proactively assessing source code for security vulnerabilities: Detecting flaws, coding errors, and potential issues
Cloud Vulnerability Scans	Wiz	Assessing the security of cloud environments (IaaS, PaaS, SaaS): Providing recommendations for enhanced deployment security

6. Classification of Vulnerability Scanners

There is more than one way to classify vulnerability scanning tools, and these methods include:

- Severity Classification:
  - Vulnerability scanners can be categorized based on the severity score provided by the Common Vulnerability Scoring System (CVSS). This score offers insights into the impact and exploitability of vulnerabilities.
- WASC Categories:
  - Another classification criterion involves the Web Application Security Consortium (WASC) categories associated with the vulnerabilities targeted by the scanner.
- Functional Capabilities:
  - Classification can also be based on the functional capabilities of vulnerability scanners, such as their ability to schedule scans, push policies, view scan findings, and manage multiple scanners from the cloud.
- Deployment Across Networks:
  - The deployment of vulnerability scanners across various networks, including public and private clouds, as well as multiple physical locations, is an additional factor considered for classification.
  - In summary, vulnerability scanners can be classified based on:
  - Severity scoring using CVSS.
  - Targeted vulnerability categories according to WASC.
  - Functional capabilities for scheduling scans and managing results.
  - Deployment across diverse network environments.

This multifaceted classification approach enables a comprehensive understanding of vulnerability scanners based on their severity, target focus, capabilities, and deployment scenarios.[7]

7. FACTORS THAT INFLUENCE CHOOSING THE APPROPRIATE VULNERABILITY SCANNING TOOL

In the realm of cyber security, choosing the right vulnerability scanning tool is paramount to safeguarding digital assets and ensuring the resilience of an organization's information technology infrastructure. Several factors play a crucial role in this decision-making process, influencing the effectiveness of the chosen tool in identifying and mitigating potential security risks. Here are essential factors to consider when selecting a vulnerability scanning tool to enhance your organization's cyber security posture.

1- Consider accuracy, ease of use, administration, and system overhead when selecting a product.

2- Prioritize customizability for the environment and specific hosts.

3- Choose a tool with a track record of frequent updates and quick responses to new vulnerabilities.

4- Ensure the tool can update its vulnerability database remotely or locally, on demand, and automatically on a set schedule.

5- Select a tool with scanning preferences, allowing control over intensity and speed to avoid overwhelming hosts or networks.

6- Look for a tool that provides specific recommendations for mitigating identified vulnerabilities, along with references for additional information.

7- The tool should report a reasonable risk level for each identified vulnerability.

8- Choose a product that integrates vulnerability scanning with existing patch management practices.

9- Ensure the product can scan high-risk systems more frequently than others.[8]

8. CONCLUSION

In conclusion, this paper has delved into the critical realm of web vulnerability scanning tools, driven by the escalating risks of cyber breaches in an era where an increasing number of individuals entrust their data to the Internet. The primary objectives of this research were to elucidate the types of web vulnerability scanning tools, underscore their significance in the cyber security landscape, guide individuals and institutions in selecting tools tailored to their specific needs, and elucidate the factors influencing this selection process. Through an analytical research methodology, we have provided a comprehensive overview of these tools, offering insights into their goals, features, and classification.

The research questions addressed in this paper led to a thorough exploration of the types of web vulnerability scanning tools, the influencing factors in their selection (including performance, ease of use, and cost), methodological steps for prudent tool selection, practical case studies illustrating tool application on specific websites, and valuable guidance for individuals and institutions to make informed choices.

As cyber threats continue to evolve, the importance of deploying effective vulnerability scanning tools becomes paramount. It is our hope that this research serves as a valuable resource for those seeking to bolster web application security and fortify their defenses against cyber-attacks. By understanding the methodologies, types, and factors influencing the selection of vulnerability scanners, individuals and organizations can make informed decisions to safeguard their digital assets in an ever-changing cyber security landscape.

REFERENCES

[1] Odion, T. O., Ebo, I. O., Imam, F. M., Ahmed, A. I., Musa, U. N. (2023). "VulScan: AWeb-Based Vulnerability Multi-Scanner for Web Application." IEEEXplore.DOI:10.1109/SEB-SDG57117.2023. 10124601

[2] RiskOptics. (2022). "Vulnerability Scanners: Passive Scanning vs. Active Scanning." Retrieved from https://reciprocity.com/blog/vulnerability-scanners-passive-scanning-vs-active-scanning/

[3] NCSC (2021). Vulnerability Scanning Tools and Services. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services.

[4] Pandey, S., Chaudhary, A. (2022). "Vulnerability Scanning." techrxiv. DOI: 10.36227/techrxiv.20317194

[5] RSI Security. (2023). "7 Types of Vulnerability Scanners." RSI Cybersecurity Blog. Retrieved from https://blog.rsisecurity.com/7-types-of-vulnerability-scanners/

[6] Basan, M. (2023). "12 Types of Vulnerability Scans & When to Run Each." eSecurityPlanet. Retrieved from https://www.esecurityplanet.com/networks/types-of-vulnerability-scans/#port

[7] Grance, T., Stevens, M., & Myers, M. (2003). Guide to Selecting Information Technology Security Products. National Institute of Standards and Technology, NIST Special Publication 800-36.

[8] Tenable. (2023). Tenable Vulnerability Management FedRAMP Moderate User Guide. Retrieved from https://docs.tenable.com/vulnerabilitymanagement/FedRAMP/Content/PDF/VM_FedRAMP_User_Guide.pdf

Citation: *Assem I. Mohaidat & Dr Adnan Al-Helali. "Web Vulnerability Scanning Tools: A Comprehensive Overview, Selection Guidance, and Cyber Security Recommendations" International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), vol 10, no. 1, 2024, pp. 8-15. DOI: https://doi.org/10.20431/2349-4859.1001002.*