A holistic approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb

Azeddien M. Sllame
Computer Network Department
Faculty of Information Technology
University of Tripoli, Libya
a.sllame@uot.edu.ly
Aziz239@yahoo.com

Tayma Esam Tomia
Computer Network Department
Faculty of Information Technology
University of Tripoli
tomiatima@gmail.com
T.Tima@uot.edu.ly

Ruqia Mohammed Rahuma
Computer Network Department
Faculty of Information Technology
University of Tripoli
R.Mahmoud@edu.uot.ly

***Abstract*—This paper describes a cyber security vulnerability assessment methodology powered by AI tactics. The AI-powered tool "ImmuniWeb AI" effectively supported the tools of the suggested approach by automating a number of vulnerability management process tasks, including scanning, evaluation, prioritizing, and remediation. The recommended methodology makes use of the Nikto, Acunitx, Nessus, and ZAP proxy tools, which have been improved by the ImmuniWeb AI online tool, to quickly and effectively scan target systems in order to identify any vulnerabilities. Using such a variety of tools with a wide range of expertise practically produced a comprehensive method that can identify system vulnerabilities and generate well-written reports with appropriate remedy recommendations depending on the vulnerabilities' scores and level of danger. As a result, the outcomes showed how effective the suggested methodology.**

Keywords—vulnerability assessment, risk management, cyber security, vulnerability scoring, vulnerability scanning tools, methodology, AI-powered tool.

I. INTRODUCTION

Hackers are always inventing new ways to get around security measures, exploit configuration mistakes, and get access to IT systems [1]. Vulnerability scanning systems are a practical management solution that may target everything from endpoint devices to web application vulnerability regions. They feature both automated vulnerability assessment and allowed security checks. Vulnerability assessments are systematic analyses of an information system's security vulnerabilities. It ascertains whether the system is known to have vulnerabilities, assigns a severity rating to those vulnerabilities, and, if required, makes mitigation or corrective recommendations. They efficiently decrease the attack surface by utilizing a comprehensive vulnerability database to identify flaws in the system. These tools are essential for safeguarding all digital assets; they might be either an open-source vulnerability scanner or a more potent security scanner. The benefits discover the vulnerabilities before they can be exploited. Proactive protection, peace of mind, and potential security flaws are the main issues they seek to resolve. However, these technologies are highly needed to any organization concerned about the security of their digital landscape. AI-powered assessment tools add more dimensional to vulnerability scanning and detection [1][2][3] [4].

This paper is structured as follows: risk management and assessment is briefly illustrated in section 2. Vulnerability scanning tools are described in section 3. Section 4 outlines vulnerability assessment types. Vulnerability Assessment Methodology steps are outlined in section 5. Vulnerability scoring system is demonstrated in section 6. Section 8 briefs some results. Finally, concluding remarks are outlined in section 9.

II. RISK MANAGAMENT AND ASSESSMENT

Risk management involves identifying, monitoring, and limiting risks to a manageable level, aiming to reduce them to an acceptable level rather than eliminating them entirely. Any object that is valuable to the organization is considered an asset. However, any flaw in the program code, system architecture, implementation, or absence of preventative measures is referred to as vulnerability. Whereas a threat can be defined as any situation that puts an asset at risk of danger, loss, damage, or compromise. Vulnerabilities are internal factors whereas threats are considered as external factors, so as the risk is the probability (or likelihood) of the realization of a threat. Thus, Risk assessments calculate the present risk level by taking into account threats, weaknesses, and implemented mitigations. Typically, when identifying threats we search outside of the organization, but, the process of finding vulnerabilities centers on internal causes. However, the organization's goal is to link vulnerabilities with detected threats, as seen in Fig. 1 [5] [6].

Fig.1. Relationship: Asset, Vulnerability, Threat, and Risk

Based on likelihood and impact, the risk that the combined threat and vulnerability pose is measured. The likelihood of a risk materializing is its chance. Impact is the degree of harm that results from a risk being taken. According to NIST SP 800-30 recommendation the risk management process contains the following steps, as shown in Fig.2. [5]: (1) preparation, (2) conduct assessment; which includes (identifying threat sources and events- vulnerabilities and

Influencing conditions, determining Likelihood of occurrence, determining magnitude of impact, determine risk), (3) communicate the risk assessment results, and (4) maintain the risk results by notifying risk management decisions to find and monitor the appropriate risk responses.

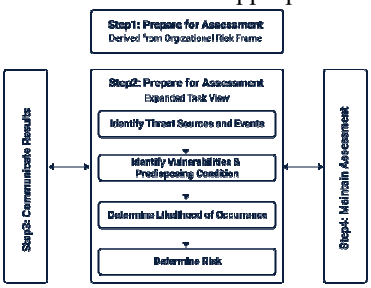

Fig.2. NIST risk management process [5]

III. VULNERABILITY SCANNING TOOLS

Specialized software programs called vulnerability scanning tools are made to find weaknesses in computer systems, networks, or software applications. To find and assess security flaws that might be leveraged by adversaries, developers, IT managers, and cybersecurity experts frequently utilize these technologies. The tools enable firms to assess their risk exposure and put the required security measures in place by searching for known vulnerabilities. A crucial component of contemporary cybersecurity procedures, this proactive approach to security aids businesses in maintaining regulatory compliance and protecting sensitive information. In addition, it designed to offer comprehensive system, application, and network vulnerability detection. Because of its strong capacity to identify vulnerabilities and weaknesses, it is an excellent option for experts looking for a comprehensive security review [7].

Software that does automatic vulnerability scanning is one of the most often used methods for doing vulnerability assessments, however there are other options. The vulnerability scanner searches databases of known vulnerabilities to identify potential vulnerabilities in systems, data, applications, and other components.

The vulnerability scanner extensively inspects the technology, taking into account every component. The target system is examined for known security vulnerabilities, improper configurations, outdated software, and potential opportunities that might be exploited by an attacker. After the scans are finished, the application provides a report detailing all faults discovered and recommends precautions against any hazards [8].

SIEM Integration may make it possible for more feature-rich goods to advance. Through this link, data from a vulnerability scanner may be received by a SIEM (Security Information & Event Management), increasing the possibility of threat analysis. An essential function that makes it possible to create a comprehensive asset catalog and provide consistent security monitoring for every asset is asset detection and monitoring [7] [8].

IV. VULNERABILITY ASSESSMENT TYPES

There are many vulnerability types which can be summarized as follows:

A. Network-Based Vulnerability Assessment

A network-based vulnerability assessment locates weaknesses in firewalls, switches, routers, and other network-related components. The primary goal of a network-based vulnerability assessment is to identify network vulnerabilities that might be exploited by an attacker to carry out an attack, steal data, or gain unauthorized access to the system. To detect vulnerabilities, these applications may use a range of methods, such as port scanning, network mapping, vulnerability scanning, and password cracking.

B. Application-Based Vulnerability Assessment

An application vulnerability assessment may be used to find vulnerabilities in a variety of software products, including desktop, mobile, and web apps. Popular vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) are frequently checked in these sorts of testing. Application vulnerability assessments can be carried out manually or automatically. Every month, OWASP compiles and updates a list of the most critical application vulnerabilities.

C. API-Based Vulnerability Assessment

Assessments of API vulnerabilities are carried out in order to identify and stop any security risks. This process identifies gaps and weaknesses in the API's design, implementation, and operation. The goal is to make sure the API is secure, trustworthy, and protected from dangers. However, during the vulnerability assessment process, a particular attention must be paid to the OWASP API Top 10 vulnerabilities in order to ensure the integrity and security of API interactions.

D. Hosts Vulnerability Assessment

Specific host systems, such as workstations, servers, and laptops, are found to have vulnerabilities through a host-based vulnerability assessment. These analyses usually involve looking through the operating system of the machine to find any vulnerabilities that have been found, such as out-of-date software or security upgrades that have not been installed.

E. Wireless Network Vulnerability assessment

A particularly those in Wi-Fi networks, is the primary objective of the process. A routine part of these assessments is analyzing the wireless network for common vulnerabilities, such insecure passwords, unapproved devices, and insufficient encryption.

F. Social Engineering Vulnerability Assessment

A social engineering vulnerability assessment finds behavioral vulnerabilities in people that might lead to phishing attacks or other forms of social engineering. This type of vulnerability assessment typically involves simulated attack scenarios to examine employees' awareness of security concerns as well as their ability to identify and respond to them.

G. Cloud-Based Vulnerability Evaluation

Cloud-based vulnerability assessments find vulnerabilities in cloud services and infrastructure such as Microsoft Azure and Amazon Web Services (AWS). These assessments check for known vulnerabilities in the cloud architecture while validating the security of apps and Internet services.

H. Evaluation of Physical Vulnerabilities

Physical vulnerability assessments are used to identify hardware vulnerabilities in things like access control systems, security cameras, and locks. These assessments

often include visual inspections of the structure and its security procedures.

V. Vulnerability Assessment Methodology

The following are the main steps taken by a well-defined vulnerability assessment method:

(1) Identify Important and Attractive Assets

The first phases in the vulnerability assessment process include understanding the whole system and identifying which networks and systems are more crucial to the operation of the organization or a company. Evaluate every resource from the perspective of a rival and give them a value based on how desirable they are.

(2) Perform an evaluation of vulnerabilities

Employ automated tools to keep an eye out for vulnerabilities and security flaws throughout the whole network or system. It is necessary to refer to the attractive and important assets as "targets," and more research and testing using real-world scenarios will be required to find and assess any apparent security vulnerabilities. The assessments must to include references to threat intelligence feeds, vulnerability databases, asset management systems, and vendor vulnerability notifications.

Once the network or system's overall effectiveness meets the required security criteria, the vulnerability review is considered completed.

(3) Evaluation of Risk and Vulnerability

The next stage in the vulnerability assessment process is to identify the root cause and source of the security fault that was discovered in phase two. It offers a sensible corrective viewpoint. Each one of such vulnerabilities must be ranked or scored based on a set of criteria, including:

- Which data are at risk?
- Which computer network or system is affected?
- The seriousness of the possible attacks
- Potential danger in the case of an attack;
- Compromised ease of access.

(4) Remediation

The main objective of this stage is to close security flaws by selecting the appropriate remedial actions for discovered vulnerability. Some corrective actions that might be taken include: updating any changes made to operations or configurations; creating and implementing vulnerability fixes; and introducing new security procedures, improved tools, or apply advanced protocols.

(5) Mitigation

Remedial action is utilized since it isn't always feasible to completely fix vulnerabilities. Remedial action is to reduce the risk that vulnerability will be exploited or the harm that may be caused by such exploitation. Virtual patching, which rapidly fixes vulnerabilities without changing the component or source code itself, is one practical technique. This virtual patch effectively saves some time until a more permanent patch or code repair can be implemented by establishing a barrier of protection against prospective attackers.

(6) Reassess the system and make enhancements

This phase involves reevaluating the system's security posture using similar processes as the previous evaluation. These processes could involve code reviews, vulnerability testing, penetration testing, and other relevant techniques. However, the focus at this point is determining if the vulnerabilities that were first identified have been adequately fixed or reduced to a level that is acceptable. An additional objective of the assessment is to identify any new vulnerabilities that have emerged as a consequence of the applied adjustments or settings.

(7) Present Findings

The final stage in the security vulnerability assessment technique is to clearly report the assessment results.

The principal aim of reporting is to provide a precise characterization of the system's effectiveness and, in case the current security measure is not successful, to propose potential remedies. A comprehensive vulnerability assessment report will also include the following details:

Which system is impacted? How easily the system can be hacked or compromised; the potential financial consequences of a successful breach; whether the vulnerability can only be accessed online or requires physical proximity; the vulnerability's age; any legal requirements that the business must adhere to; and the cost of a data breach in the specific industry.

- <u>Threat types discovered by Vulnerability Assessment</u>

Some common threat categories that can be avoided with vulnerability assessment approaches are as follows:

(a) Malicious software infections are a common cyber threats that have the power to totally devastate entire businesses. Phishing emails and phony websites are examples of attack vectors, while malware is frequently distributed through software bugs.

(b) Denial of service (DoS) attacks: Cyberattacks referred to as DoS attacks aim to overwhelm a targeted system or network with traffic or resources to the point where it crashes or ceases to function for authorized users. A vulnerability assessment can identify gaps in the network or system that could allow a hacker to launch a DDoS attack.

(c) Information Leakage: When unauthorized parties get access to private data, such as financial, personal, or intellectual property, there is an information breach.

(d) Dangers from inside: Internal threats are those that arise from within an organization. These risks could come from outside vendors, business associates, or former or current employees who have access to an organization's IT resources. An evaluation of vulnerabilities might uncover gaps in networks, apps, and systems that insiders could exploit to obtain data or put at risk a company's IT security.

(e) Phishing-based cyberattacks: Phishing attacks are a kind of cyberattack in which victims are deceived via social engineering techniques into divulging sensitive information, such as bank account details or login credentials.

(f) Web Application Exploits

"Web application attacks" are cyberattacks that target vulnerabilities in online applications, such as cross-site scripting (XSS) and SQL injection. Businesses can use application vulnerability assessment to identify and prioritize addressing web application vulnerabilities.

VI. Vulnerability scoring systems

Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), however, both are significant parts in understanding and managing cybersecurity risks, maintained by MITRE. A CVE is a dictionary of vulnerabilities in OSs and applications software maintained by MITRA (cve.mitre.org). Each

vulnerability has an identifier that is in the format: CVE-YYYY-####, where YYYY is the year the vulnerability was discovered, and #### is at least four digits that indicate the order in which the vulnerability was discovered. In addition, a brief description of the vulnerability with a reference list of URLs that supply more information on the vulnerability, and the date the vulnerability entry was created. Thus, every time a new vulnerability is found, it's given a CVE number so cybersecurity people can easily identify it. Furthermore, the CVE dictionary provides the principal input for NIST's National Vulnerability Database (NVD) (nvd.nist.gov). Thus, the NVD supplements the CVE descriptions with additional analysis, a criticality metric, calculated using the CVSS, plus fix information [10] [11].

Two common uses of CVSS are calculating the severity of vulnerabilities discovered based on their impact and exploitability on one's systems and as a factor in prioritization of vulnerability remediation activities. The NVD provides CVSS assessments for all published CVE records. However, whenever a vulnerability scan report is produced with a vulnerability detected will normally be assigned an indicator of severity typically using CVSS metrics. CVSS metrics produce a score from 0 to 10 centered on deep-down features of the vulnerability (base), The temporal aspects of vulnerability include the environment in which it arises and changes over time. CVSS contains many important details such as (i) Access Vector (AV) Metric that describes the method an attacker would use to exploit the; (ii) Access Complexity (AC) Metric that outlines the difficulty an attacker would have to exploit the vulnerability; (iii) Authentication (AU) Metric that defines the number of times an attacker would have to authenticate; (iv) Confidentiality (C) Metric that demonstrates the impact to confidentiality of data processed by the system. However, Integrity (I) Metric that describes the impact to integrity of data processed by the system. Availability (A) Metric designates the impact to availability of the system. Then we get CVSS Vector which is single-line format to show the vulnerability ratings for all six metrics for calculating the CVSS score that includes exploitability score and impact score as shown in Fig. 3. A CVSS calculator and analysis with many details can be found in https:// nvd. nist. gov /vuln-metrics/cvss/v3-calculator [5] [10] [11].

There is also a Common Weakness Enumeration (CWE) database, which is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts. However, hackers are commonly exploiting such vulnerabilities to gain access to systems. This is also maintained by MITRA (cwe.mitre.org) [10].

VII. Comparing Penetration Testing with Vulnerability Assessment

While the main goal of vulnerability assessment is to identify weaknesses and vulnerabilities, penetration testing actively takes use of these defects to analyze their real-world consequences. Vulnerability assessments help firms prioritize repairs and identify areas that need attention, while penetration testing helps businesses better understand the potential consequences of successful attacks and improve their incident response capabilities [8] [9].

Key features of vulnerability assessment

• Scanning: Using automated methods, the target system is examined for known vulnerabilities.
• Finding Weaknesses: provides list of vulnerabilities along with security issues that have been ident.
• No Exploitation: The aim of a vulnerability assessment, not actively exploiting them.
• Remediation Recommendations: The evaluation's findings typically lead to the suggestion of remediation and mitigation techniques.

Key features of penetration testing

• Active Exploitation: A key component of penetration testing is actively attempting to exploit vulnerabilities in order to assess their impact [9].
• Actual scenarios: Testers role-play actual attack scenarios to ascertain probable entry points and the likely degree of damage.
• Manual and Automated Testing: Both software and traditional methods are used to identify and exploit vulnerabilities.
• Limited Scope: The primary goal of penetration testing is frequently target systems or componentry.
• Helpful Information: Penetration testing provides important details on the effectiveness of security measures and the potential repercussions of successful attacks.

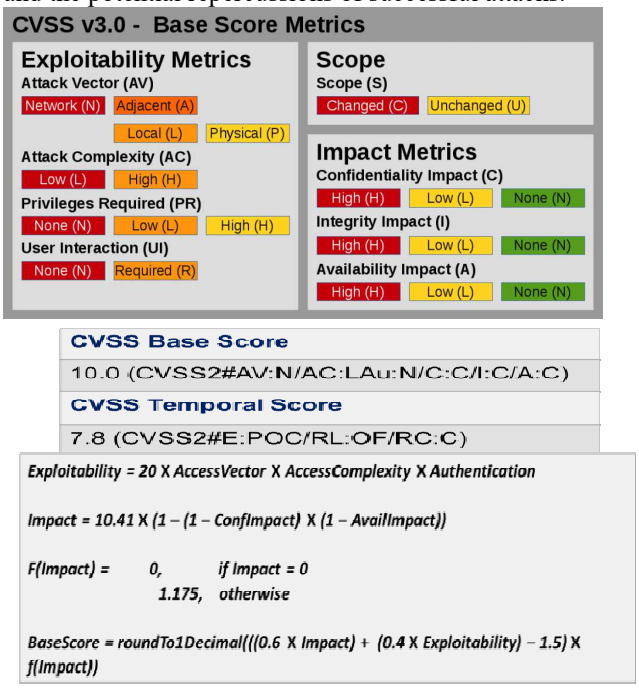

Fig. 3. Vulnerability score calculation summary

VIII. The Case Study

The implementation of the proposed holistic approach for vulnerability assessment which based on open source tools: Nikto, Acunitx, Zaproxy, Nessus is augmented with ImmuniWeb AI tool. However a sketch how web sites and scanned systems look-like can be seen in Fig.4. However, the main tools are:

- **Netcraft**: it is an automated digital risk protection technology combines detection, threat intelligence, and strong disruption & takedown to safeguard your business and clients against phishing, scams, fraud, and cyberattacks [12].

- **NMAP**: is a free and open-source tool for security audits and network discovery. It is also helpful for many systems and network managers for activities like scheduling service upgrades, keeping track of host or service uptime, and inventorying the network. Nmap makes creative use of raw IP packets to identify hosts on a network, the services (name and version of the application) they provide, the operating systems (and OS versions) they run, the kinds of firewalls and packet filters they have in place, and a plethora of other features [13].
- **Nessus**: A comprehensive vulnerability scanner from Tenable Network Security, it is used to assess the modern attack surface [14].
- **Nikto**: Fast web scanner for common vulnerabilities. Open-source, best for beginners [15].
- **ZAP** (**Zaproxy**): Powerful web application tester. Customizable, supports advanced testing [16].
- Acunetix: A web application scanner with a focus on deep scanning and automated exploitation [17].
- **ImmuniWeb AI web tool**: ImmuniWeb streamlines, expedites, and lowers the cost of application security testing, compliance, and protection. Application security testing that is both risk-based and threat-aware. With its patented machine-learning technology and human testing, ImmuniWeb upends the conventional practice of application security testing for web and mobile applications. Every open network port is thoroughly examined using our sophisticated fingerprinting technology during the non-intrusive network security assessment to identify the network service that is currently operating and its version, giving you a risk-based score for each network IP address [18].

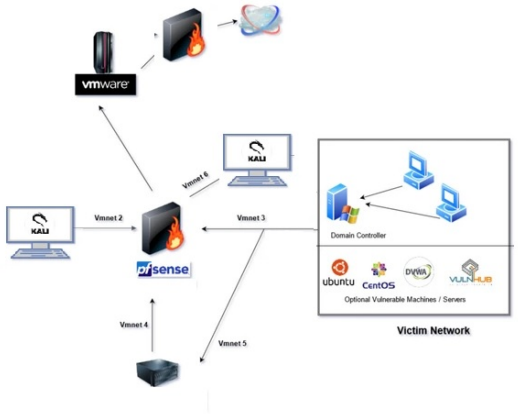

Fig.4. Overlook to the vulnerability scanning process over

- There are many web sites used for training on vulnerability assessment process such as: hack thebox, *Hackthissite, CTFlearn, Google Gruyere, OWASP Mutillidae II*. We applied the methodology and tools on *Hackthissite and OWASP Mutillidae [16]*.

(A) The process includes: scanning using Netcraft, which discovers IP addresses and showed all details about IP address location and DNS information, as illustrated on Fig. 5. Therefore, through the Netcraft scan, we acquired significant information encompassing domain age, IP address details, and potential content management systems.

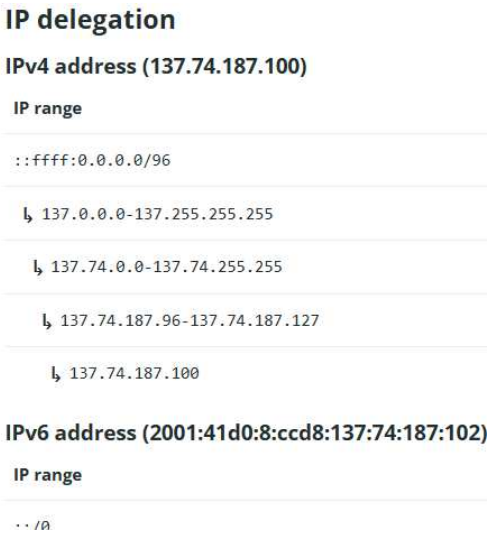

Fig. 5: Snapshot of part of Netcraft results

(B) Starting with Netcraft information, Nmap tool is applied to find all ports, services, OS, service versions, and trace root the IP address of the target to conduct an in-depth network scan of the target URL to gather crucial information such subnet details, and potential security weaknesses exploitable for further assessment investigation. The Nmap scan for Windows operating systems provided valuable insights into the target URL's network topology, as illustrated in the figures (mention figure numbers), as described in Fig. 6.

(C) Having successfully identified the target's IP address and hostname, we are now equipped to leverage specialized web vulnerability scanners to systematically assess its security posture and uncover potential vulnerabilities exploitable for further penetration testing.

(D) To initiate the vulnerability assessment phase, we employed the Tenable Nessus vulnerability scanner to conduct a comprehensive scan of the target system, aimed at identifying potential security weaknesses exploitable by attackers, as seen in Figure 7. Therefore, the report is so lengthy which ran for 5-10 hours, the results showed that there is much vulnerability and their critically score with CWE numbers in the tested site which include: SQL injection, web server allows password auto completion, and HTTP vulnerabilities [19-24]. Considering the primary objective of assessing the potential security weaknesses within the web application, we selected for the 'web application threats scan' option within the Nessus tool, which utilizes dedicated plugins and modules to identify vulnerabilities specific to web technologies and configurations. Thus, the web vulnerability scan yielded a comprehensive set of findings, which we will now analyze in detail. This includes identifying vulnerabilities categorized by severity (critical to informational), understanding their nature and potential impact, and assessing the exploitability of high-risk vulnerabilities. Within Nessus, the web scanning results provide detailed vulnerability information through dedicated columns. These columns include Common Vulnerability Scoring System (CVSS) severity (Sev) for sensitivity assessment, the risk score for prioritization, the vulnerability name for specific identification, the vulnerability family for categorization,

and the count for identifying the number of similar vulnerabilities present.

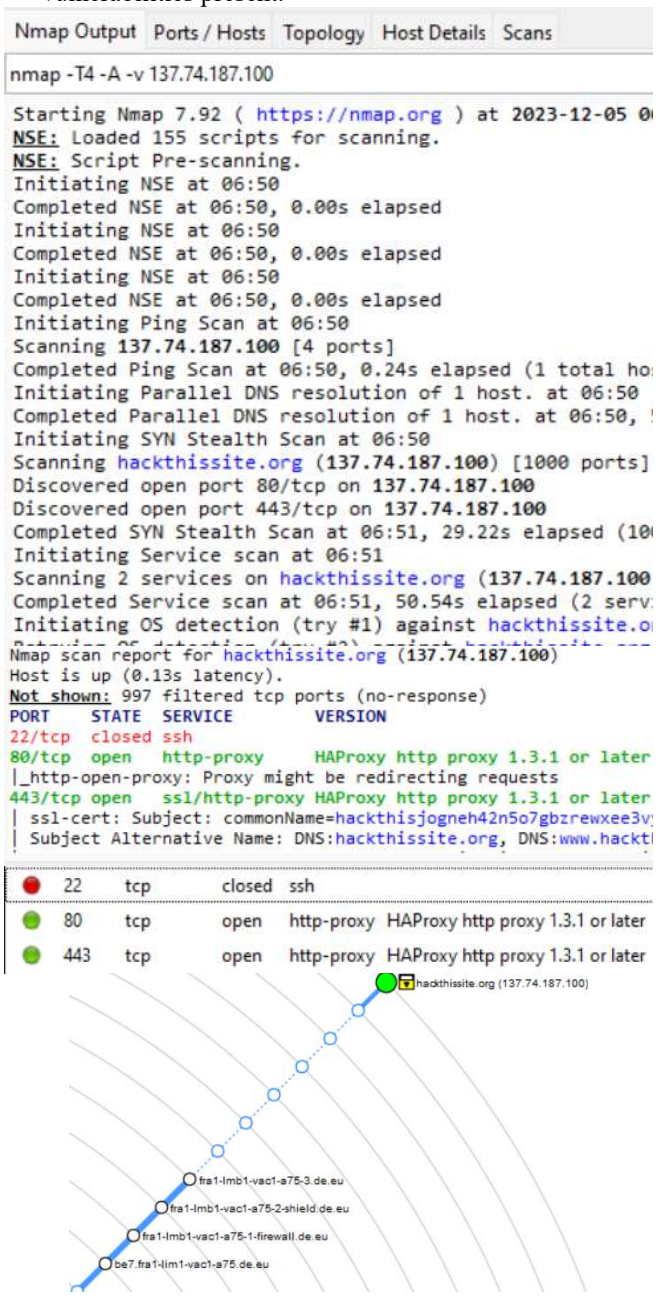

Fig. 6. NMAP results: scanning, ports, and trace root.

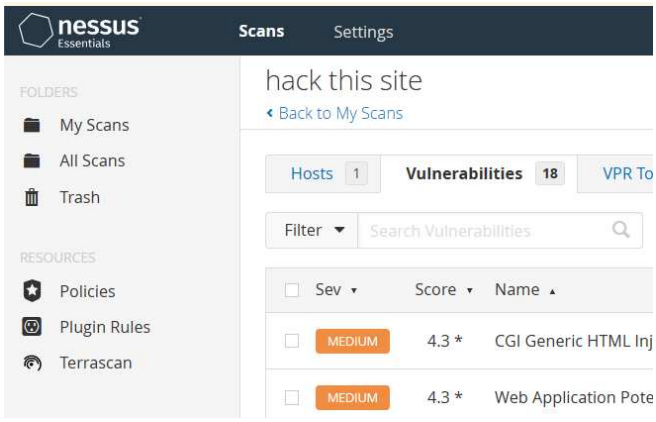

Fig.7. Nessus: (a) hack this site: initial scan

Fig.7. Nessus: (b) scan results: some vulnerabilities

(E) Applying Nikto tool as a command tool applied to do scanning web servers for out-of-date and unpatched software as well as searching for dangerous files that may reside on web servers.

(F) Acunetix Vulnerability Scanner: It is a comprehensive web application security testing tool that works well in complex situations as well as on its own. It provides numerous choices for integration with industry-leading software development tools, as well as integrated vulnerability evaluation and vulnerability management. The results of this tool are really remarkable; as shown in Fig. 8. with full of details written out in report, demonstrating CVE details including score, and risk analysis with severity calculation and recommendations, including all related CWE or CVE.

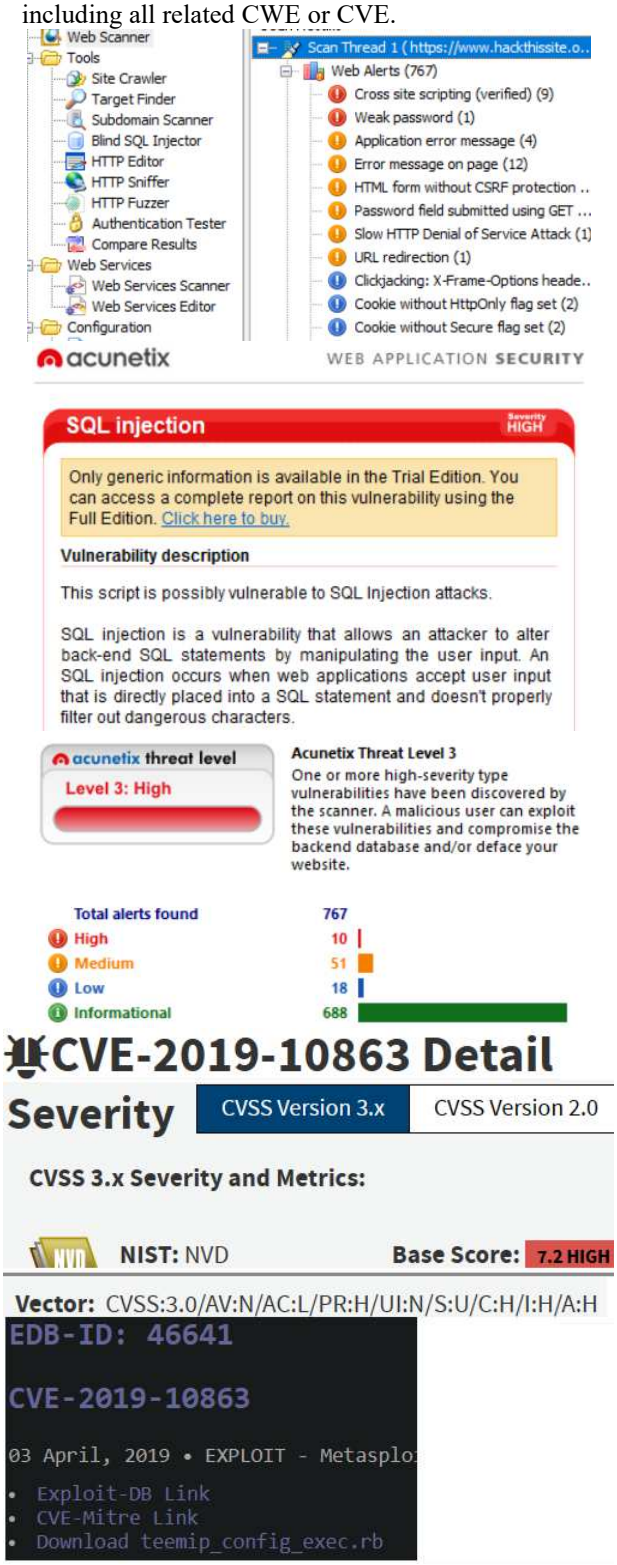

Fig.8. Acunetix Vulnerability Scanner results

(G) ZAP (Zaproxy), or Zed Attack Proxy it is one of the most well-known OWASP projects. ZAP can be utilized for manual webpage testing and proxy interceptions. Application error disclosure, Cookie not HttpOnly flag, SQL injection, Application error disclosure, XSS injection, Private IP disclosure, missing anti-CSRF tokens and security headers, and Session ID in URL rewrite are among the things ZAP uncovers. The result of this tool is described in Fig. 9. While Fig.10, shows Wireshark results during the test with Zaproxy tool.

(H) Immuni web-AI-platform: The result of applying AI based tool produced efficient results, as shown in Fig. 11. That discovers many vulnerability such as server issues, cross-site-scripting, and HTTP header problems, illustrated with their CVE id and score.

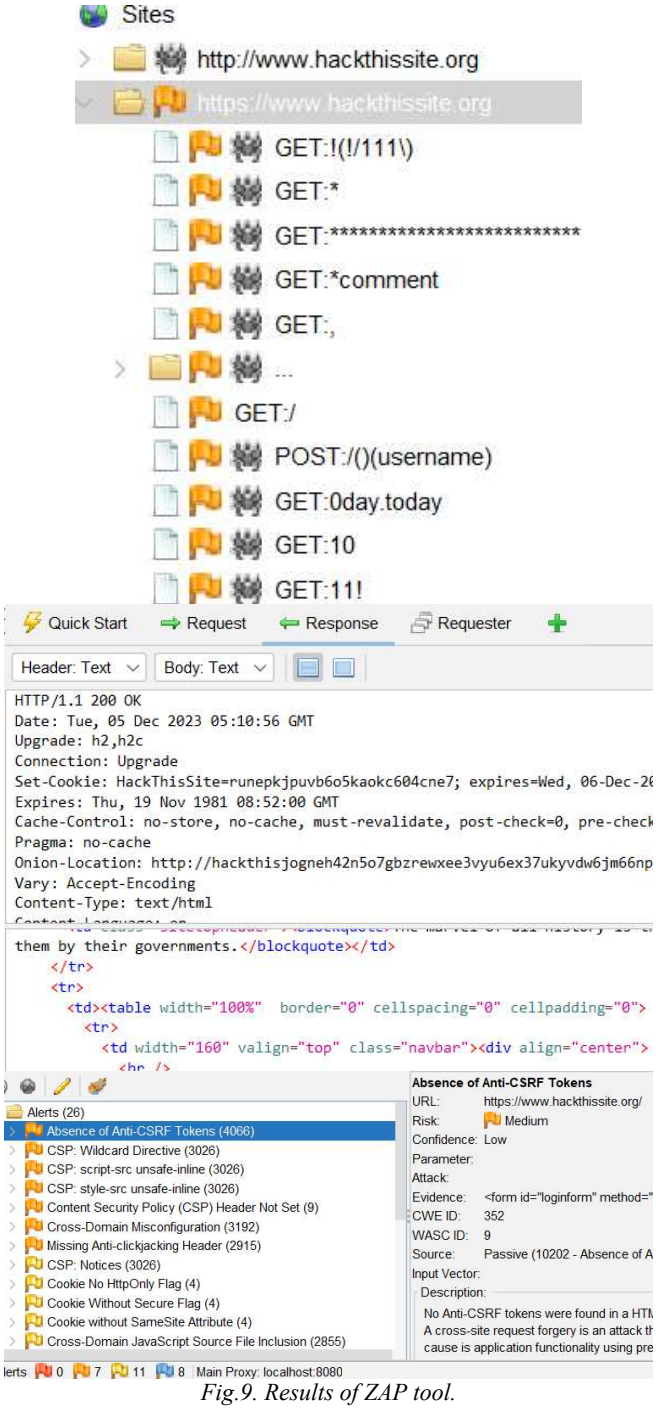

Fig.9. Results of ZAP tool.

Info	Length	Protocol	Destination	Source
[ACK] 443 → 63377	54	TCP	137.74.187.104	192.168.1.6
Dup ACK 904443#1]	54	TCP	192.168.1.6	137.74.187.104
[RST] 63381 → 443	54	TCP	192.168.1.6	137.74.187.104
ACK] 63406 → 443	66	TCP	192.168.1.6	137.74.187.104
[ACK] 443 → 63406	54	TCP	137.74.187.104	192.168.1.6
hackthissite.org)	571	TLSv1.2	137.74.187.104	192.168.1.6
Server Hello	1466	TLSv1.2	192.168.1.6	137.74.187.104
[ACK] 63401 → 443	1466	TCP	192.168.1.6	137.74.187.104
[ACK] 443 → 63401	54	TCP	137.74.187.104	192.168.1.6
[ACK] 63401 → 443	1466	TCP	192.168.1.6	137.74.187.104
[ACK] 63401 → 443	1466	TCP	192.168.1.6	137.74.187.104
Server Hello Done	799	TLSv1.2	192.168.1.6	137.74.187.104
[ACK] 443 → 63401	54	TCP	137.74.187.104	192.168.1.6
Handshake Message	180	TLSv1.2	137.74.187.104	192.168.1.6
[ACK] 63402 → 443	54	TCP	192.168.1.6	137.74.187.104

Fig.10: Wireshark snapshot showing some ZAP tool accessing a web site under test.

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities update to the most recent version **3.7.1**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2020-7656	CWE-79 - Cross-site scripting
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
5.5 Medium	CVE-2012-6708	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 - Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 - Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 - Cross-site scripting

Some HTTP headers related to security and privacy are missing or misconfigured.

MISSING REQUIRED HTTP HEADERS

X-Frame-Options | X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Permissions-Policy

SERVER

Web server does not disclose its version.

Fig.11. Immuniweb-AI-platform report snapshot

IX. Conclusions

This paper described a continuous research running in cyber security which concentrates on risk, threat, vulnerability relationship, by applying open-source tools. The application of AI-driven tool "ImmuniWeb AI" effectively supported the ordinary tools of the suggested approach by automating a number of vulnerability management process tasks, including scanning, evaluation, prioritizing, and remediation. The recommended approach makes use of the Nikto, Acunitx, Nessus, and ZAPS proxy tools, which have been improved by the ImmuniWeb AI online tool, to quickly and effectively scan target systems in order to identify any vulnerabilities. Finally, employing a broad range of instruments with diverse specialist capabilities led to the creation of an all-encompassing approach powered with AI competences that is capable of detecting system vulnerabilities and producing well-written reports with suitable remediation recommendations based on the vulnerabilities' scores and degree of danger. Consequently, the results demonstrated the value of the proposed methodology.

References

[1] Fredrik Heiding, et al.: Research communities in cyber security vulnerability assessments: A comprehensive literature review, Computer Science Review, Volume 48, May 2023, 100551, Elsevier publishing.

[2] Tarakçi, Emin and Anıl Mustafa Gönül. "Risk Analysis and Assessment Framework for Cyber Security in Management Systems",OHS Academy, 6(3), 165-172. https://doi.org/10.38213/ohsacademy.1402624

[3] Dasgupta Sanhita, et al. "AI-Powered Cybersecurity: Identifying Threats in Digital Banking." 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023, pp.2614-2619.

[4] Shetty, Nahush, Vulnerability Assessment for Cybersecurity using Machine learning, SSRN e library, June 2021, http://dx.doi.org/10.2139/ssrn.3884044

[5] NIST: SP 800-30, NIST guide for conducting risk assessment (www . nist . gov , last access 29.4.24)

[6] A. S. Cerqueira Junior, and C. H. Arima. "Cyber Risk Managament and ISO 27005 applied in Organizations: A Systematic Literature Review", Rev. Foco, vol. 16, no. 02, p. e1188, Feb. 2023.

[7] Nair, Aarya et al. "Vulnerability Scanning and Analysis Tool (VSAT)." 2023 9th International Conference on Smart Computing and Communications (ICSCC) (2023): 338-343.

[8] Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. 2023. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions" Electronics 12, no. 6: 1333. https://doi.org/10.3390/electronics12061333

[9] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. Procedia Computer Science, Vol. 57, 710-715.

[10] Mitra: cve. Mitra .org , last access 29.4.24)

[11] Nvd .nist .gov, , last access 29.4.24)

[12] Netcraft last access 29.4.24)

[13] NMAP tool last access 29.4.24)

[14] Nessus last access 29.4.24)

[15] Nikto last access 29.4.24)

[16] OWASP ZAP last access 29.4.24)

[17] Acunetix last access 29.4.24)

[18] ImmuniWeb AI web tool last access 29.4.24)

[19] Bharadwaj R.K., Mantha et al. "Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects." *Proceedings of the Creative Construction e-Conference 2020* (2020).

[20] Wang, Liwei, Robert Abbas, Fahad M. Almansour, Gurjot Singh Gaba, Roobaea Alroobaea, and Mehedi Masud. "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks." Journal of Intelligent Systems 30, no. 1 (2021): 592-603.

[21] M. Mirjalili, A. Nowroozi, M. Alidoosti: A survey on web penetration test, Adv. Comput. Sci.: Int. J. 3 (6) (2014).

[22] Mariam Abojella Msaad, Reema A. Saad, Azeddien M. Sllame: A Simulation based analysis study for DDoS attacks on Computer Networks, in the IEEE 1st Int. Maghreb Meeting of the conference on Sciences and Techniques of Automatic control and computer engineering (IEEE MI-STA'2021), pp. 756-761, May 2021, Tripoli, Libya.

[23] Goutam, Arvind and Vijay Kumar Tiwari. "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application." 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (2019): 601-605.

[24] Azeddien M. Sllame, Ahmed Samoud: A Simulation-Based Analysis Study of Different Data Centers' Networks Employing MPLS technique as a Fault Tolerance Mechanism, In IEEE 3nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA'2023), May 2023, Benghazi, Libya.