A Review of Vulnerability Scanners For Web Applications and Networks

Pushpender Bhardwaj[1], Prof. Arvind Kalia[2]
[1]Dept of Computer Science
[2]Professor, Dept of Computer Science
[1, 2] Himachal Pradesh University, Shimla

Abstract- *All organisations around the world are concentrating on cyber risks due to the cases of cybercrime increasing day by day. Companies with-out adequate cybersecurity strategies face serious financial and reputational risks. Therefore, it be-comes crucial for an organisation to monitor and analyse its systems and networks. They hire cyber security analysts for this job. They have to analyse the system and networks regularly by doing vulnerability assessments into it.*

The automatic version of penetration testing is preferred over manual penetration testing as it saves lots of time and resources.This paper presents a literature review on automated vulnerability scanners forweb applications and networks, which helped us in finding how vulnerability scanners can be useful in detecting vulnerabilities. Additionally, various strategies and some open-source tools used in the vulnerability scanning of web applications and networks have been studied.

Keywords- Penetration Testing, Vulnerability Assessment, IT Security, Web Application Security Scanners, Network Vulnerability scanner

I. INTRODUCTION

Cyber security has become a major concern as digital technology becomes more popular in human lives. Every organisation depends on the usage of computer networks, systems, and Internet technologies. Most of our daily routine activities are depends on digital devices connected through networks or the Internet. When computers and other devices are used for communication, the way that they communicate has posed many challenges to the users. One of its challenges is cyber security. Cyber security is the practice in which different measures are taken against data thefts or for the protection of computer systems from damages such as hardware, software, or information and also from the illegal access of computers, networks, data, and programs. To handle these kinds of issues, organisations must be ensured to follow security standards and regulations such as penetration testing.

Penetration testing, also known as PEN Testing is all about assessing the security of an IT infrastructure by securely attempting to exploit the vulnerabilities. Penetration testing generally aims to break into the systems to find out the vulnerabilities and improve the system's security so that the system can't be accessed by an unauthorised person[23].

Strategies of PEN Testing [24]

a) Black Box PEN Testing: In this type of testing the team does not know the target system. In this testing security breach, possibilities are discovered from scratch. The team mainly focuses on gathering information about the target system rather than the internal details of the system.
b) White Box PEN Testing: In white box penetration testing, the testers are allowed complete access to the test target. Source code information, operating system information, and target network IP addresses are also known by the testers.
c) Grey Box PEN Testing:In grey box penetration testing, the testers are only given a limited portion of the necessary data about the target, and the rest information is to be found out by the tester.

Phases of PEN testing[23]

a) Reconnaissance: Reconnaissance is the initial step in a penetration testing process. During this phase, the tester collects as much information about the system that is being targeted. The goal is to collect as much information fora better understanding of how a target works and its vulnerabilities for developing an effective attack strategy.
b) Scanning: It is the second phase in pen testing after the reconnaissance phase in this phase we determine how the target system will react to various intrusion attempts.
c) Gaining Access: This phase uses various web attacks to determine the vulnerabilities present in the target system. Then tester tries and exploits these vulnerabilities to determine what kind of harm they can cause.
d) Maintaining Access: This stage aims to check whether the vulnerability is used to achieve a long presence in the exploited system. If the system allows to remain the

unauthorised user for a long duration they can steal the most sensitive information of the organisation.

e) Reporting: In this phase, the tester creates a report summarising the results of the penetration test when the exploitation phase is over. In this phase with the help of a report, the tester can suggest fixes for the vulnerability that is found in the system to enhance its security.

II. OBJECTIVE

- The objective is to make a systematic review of the literature on vulnerability scanners for web applications and networks.
- Find out the various vulnerability scanners used in the study and how many of them are open-source scanners.

III. LITERATURE REVIEW

A comparative study of various tools and methods has been provided in Table 1. Kushe[1] evaluated the performance of network vulnerability scanners based on parameters such as i) the ability to search ii) scanning time and the ability to detect vulnerability where more factors can be included such as false positive rate. Nagpure and Kurkure[4] also, evaluated the performance of the vulnerability scanners but with alimited number of scanners. Tundis,et al[6] also evaluated the performance of the scanners but most scanners are commercial scanners. Amankwah, et al.[15] evaluated 8 web vulnerability scanners which are more suitable because it involves both commercials as well as open-source scanners but the test is done only on two web environments. Most of the researchers have followed the OWASP TOP10 vulnerability list to test for vulnerabilities in the systems. Shah et al.[12] and Mohammed[13] have used Nmap for network scanning for vulnerability. Only Mubaiwa andMukosera[22] have proposed an algorithm that accelerates the process of testing for vulnerabilities for identifying SQL injection and XSS but failed to detect all vulnerabilities.

It can be observed from the comparison in Table 1 that most of the researchers have used commercial vulnerability scanners (Nessus, Acunetix, Nexpose, Burp suite, Shodan, Censys, AppScan) and only a few of them used open-source vulnerability scanners (Nmap, Vega, Nikto, Angry Ip scanner) for comparative analysis. Out of those vulnerabilities scanners some of the scanners are outdated(Retina). As this paper focuses on open-source vulnerability scanners because they are freely available and a large community of contributors supports open-source projects.

IV. SCOPE OF STUDY

The main purpose of this study is to determine the work done on vulnerability scanners for web applications and networks. The study considers the importance of vulnerability scanners and researchers experimental viewpoint on the various vulnerability scanners. Also considering the reasons why they have selected those scanners in their research.

The study is limited to 35 research papers out of which 22 are selected for literature review from the years 2017-2022 maximum of 5 papers from each year. The papers are selected from different journals. Only the vulnerability scanners that are used for web applications and network scanning were chosen in the study because these two areas are the most prominent that make an organisational foundation more secure in cyberspace.

Table 1: Work done on vulnerability scanners.

S.NO	TITLE	AUTHOR & YEAR	FEATURES	LIMITATION	TOOLS USED
i.	Comparative study of two network vulnerability scanning tools: NESSUS & RETINA	Kushe, R. [2017] [1]	Performance comparison between NESSUS and RETINA vulnerability scanners on three features i.e - the ability to search, scanning time, and the ability to detect vulnerability.	Compared only two scanners which are commercial scanners. More features can be included for evaluation.	Nessus and Retina

ii.	Ethical hacking & network defence: choose your best network vulnerability scanning tools	Wang, Y. &Yang, J. [2017] [2]	A study has been conductedon OpenVAS(Open Source) which is a suitable alternative to NESSUS. Tested OpenVAS and NMAP in a virtual lab environment.	Limited to specific vulnerability scanners.	Open VAS, Nmap
iii.	Security assessment of web applications throughpenetration system techniques	Lubis, A.&Tarigan, A. [2017] [3]	Tested their university website for vulnerabilities and loopholes using NESSUS	A single commercial scanner was tested.	Nessus
iv.	Vulnerability assessment and penetration testing ofweb application	Kurkure, S. &Nagpure, S. [2017] [4]	A comparison between automated penetration testing and manual penetration testing has been done by performing it on twoweb applicationsi.e. E-commerce and Cloud application.	Only web-based analysiswas performed	Burpsuite, Acunetix, OWASP ZAP
v.	Assessment of website security by penetrationtesting using Wireshark	Purkayastha, S. et al. [2017] [5]	Performed vulnerability analyses by usingwiresharkwhich is a packet sniffer to perform the penetration testing technique of information gathering to indicate whether a website is secure or vulnerable.	Limited to network-based analysis.	Wireshark
vi.	A review of network vulnerabilities scanning tools: types, capabilities, and functioning	Tundis, A. et al. [2018] [6]	A discussion is performed onvarious publicly availablenetwork vulnerability scanning tools. Their features are described and advantages & disadvantages are highlighted.	Network-based analysis with a limited number of vulnerabilities is discussed	Shodan, Censys, Thingful, Punkspider, IVRE, VUlners, Nessus, Skipfish, Acunetix, Vega

vii.	A study on penetration testing process and tools	Zaher, H.M. &Beheshti, B. D [2018] [7]	A discussion is performed on penetration testing and the factors to be considered while performing a penetration test, the process of conducting a penetration test. And commonly used tools and software for conducting a penetration test.	Tools have only been discussed no implementation or analysis was done.	Not addressed.
S.NO	**TITLE**	**AUTHOR & YEAR**	**FEATURES**	**LIMITATION**	**TOOLS USED**
viii.	Automated penetration testing:An overview	Abu-Dabaseh, F. &Alshammari, E. [2018] [8]	A study has been conducted on the importance of penetration testing as well as its automation process.	Comparison between manual and automated penetration is made not between any tools.	Hping, Harvester, Metagoofil, Nmap, Zap, Metasploit, Nessus
ix.	Penetration Testing Using SQL Injection to Recognize the Vulnerable Point on Web Pages	Ibrahim, A.B. &Kant, S.[2018] [9]	An investigation was made to identify and exploit web application-level vulnerabilities in a large number of web applications with the helpof Acunetix scanner for vulnerability assessment and different types of SQL injection.	A single commercial scanner was tested.	Acunetix
x.	Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based onOpenvas	Xia, Y. et al. [2019] [10]	Designed and implemented a vulnerability scanning tool based on OpenVAS according to the characteristics of the system network.	Designed their vulnerability scanning tools, not any comparative analysis is made.	The self-designed tool was evaluated.

xi.	Reinforcement learning for efficient network penetration testing	Ghanem, M.C. & Chen, T.M [2019] [11]	A proposed system named Intelligent Automated Penetration Testing System (IAPTS). Which can act as a module and integrate with most of the industrial penetration testing frameworks to improve significantly the efficiency and accuracy of medium and large networks context.	IAPTS needs high-calibre human expert supervision during early learning phases. Not any scanners are used in the experiment Limited to network infrastructure	AI-based PEN sstesting system.
xii.	Penetration testing active reconnaissance phase- optimized port scanning with Nmap tool	Shah, M. et al.[2019] [12]	Demonstrated traffic accountability and time to complete the specific task during reconnaissance phase active scanning with Nmap tool	Limited to single network scanner Nmap.	Nmap
xiii.	Automatic port scanner	Mohammed, M.O. [2020] [13]	An experiment is performed for the identification of open ports and services through the network and available IP on the network which is possible to attack using NMAP.	A single network scanner NMAP is used.	Nmap
xiv.	Effective filter for common injection attacks in online web applications	Ibarra-Fiallos, S. et al. [2020] [14]	Designed a simple, fast, and highly reliable filter for stopping common injection attacks in web applications through a set of rules based on several regexes and other decisive settings.	Web vulnerabilities are only discussed not any comparative study is made.	Not addressed
S.NO	**TITLE**	**AUTHOR & YEAR**	**FEATURES**	**LIMITATION**	**TOOLS USED**
xv.	An empirical comparison of commercial and open-source web vulnerability scanners	Amankwah, R. et al. [2020] [15]	A comparative study was performed on the vulnerability detection capabilities of eight Web Vulnerability Scanners (Commercial and Open source) using two vulnerable web applications (DVWA and WebGoat).	A comparison between commercial and open-source scanners is made.	ZAP, Skipfish, Acunetix, Arachni, WebInspect, Vega, AppScan, IronWASP

xvi.	Comparative analysis of different security tools to detect network risks	Raut, J.T. et al. [2020] [16]	An outline is made about the various network threats. Various open-source tools are available to protect against various threats. Tools like Acunetix, Intrusion prevention systems (IPS) have been also discussed	Limited to specific vulnerability scanners	Acunetix
xvii.	A comprehensive literature review of penetration testing	Vats, P. et al. [2020] [17]	A literature review has been done on the work done by various researchers in the area of penetration testing. They reviewed the various aspects related to pen testing.	Not addressed	Not addressed
xviii.	A survey on network penetration testing	Jayasuryapal, G. etal.[2021] [18]	A survey has been conducted on network penetration testing in which they have covered important terms and steps to do strong penetration testing on organisations. And they also mentioned mechanisms including information gathering to the post-exploitation.	Not addressed	Not addressed
xix.	Web vulnerability through cross-sitescripting(XSS) detection with OWASP security shepherd	Wibowo, R.M.&Sulaksono [2021] [19]	A review has been conducted for technology on OWASP Security Shepherd. They had chosen the technology as an appropriate and inexpensive alternative for users to ward XSS attacks	More attacks must be included for performing attacks.	OWASP Security Shepherd
xx.	A systematic literature review on the characteristics and effectiveness of web application vulnerability Scanners	Alazmi, S. et al. [2022] [20]	A literature review has been conducted on web vulnerability scanners. They also find out the most frequently used scanners and investigated their feature and characteristics.	Not addressed	Not addressed

S.NO	TITLE	AUTHOR & YEAR	FEATURES	LIMITATION	TOOLS USED
xxi.	A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions	Shahid, J. et al. [2022] [21]	An evaluation has been made on the performance of 11 web application vulnerability scanners by testing on intentionally defined vulnerable applications i.e DVWA and the level of their respective precision and accuracy.	Scanners are tested with only a single application DVWA other web application assessment tools can also be used.	Acunetix, IBM APPSCAN, Nessus, Burpsuite, Wapiti, Arachni, WebInspect, Nikto, Netsparker, W3af, OWASP-ZAP
xxii.	A Hybrid Approach To Detect Security Vulnerabilities In Web Applications	Mubaiwa, T. G&Mukosera, M. [2022] [22]	Proposing an algorithm viablythat identifies SQL injections, XSS injection and can be utilized in any genuine application that runs on a web server, wherever the client and the database interrelate. The simulation was done using a tool developed in Python.	Hybrid method failed to detect all vulnerabilities, the fuzzing component of the algorithm must apply more advanced reasoning to improve the findings.	Not addressed

Various vulnerability scanners are used in the study by various researchers.

Table 2: Vulnerability scanners used by researchers

S. NO	SCANNER	PLATFORM	WRITTEN IN	FEATURES	DEVELOPER	STABLE RELEASE	OWNERSHIP TYPE
i)	Nessus [25]	Cross Platform GUI	Nessus Attack Scripting Language	Remote security scanner and network vulnerability scanner	Tenable, Inc.	8.11.1/ August 20, 2020	Shareware
ii)	Retina	Discontinued					
iii)	Nmap[26]	CLI, GUI	Python, C, Lua, C++	Network Scanning, OS detection, Port scanning	Gordon Lyon	7.93/ September 1, 2022	Open Source
iv)	Open VAS[27]	Cross Platform	C	Vulnerability scanner,	Greenbone Networks	22.4.0 / 18 July	Open Source

		GUI		unauthenticated and authenticated testing		2022	
v)	Burp suite[28]	Cross Platform GUI	Java	Automated scanner, Intercepting proxy	Portswigger	2022.3.8/ May20, 2022	Sharewar e
vi)	Acunetix [29]	Not Known	Not Known	Web vulnerability scanner, Cloud scanning	Invicti Security	v15.1 - 10 Nov 2022	Sharewar e
S. NO	**SCANN ER**	**PLATFOR M**	**WRITTEN IN**	**FEATURES**	**DEVELOPE R**	**STABLE RELEAS E**	**OWNE RSHIP TYPE**
vii)	OWASP ZAP[30]	Cross Platform GUI	Java	Automated scanner, Intercepting proxy	OWASP	2.12.0/ Oct28, 2022	Open Source
viii)	Wiresha rk[31]	Cross Platform GUI	C, Lua, C++	Packet analyzer, network troubleshootin g	Wireshark Foundation	4.0.0 / Oct4, 2022	Open Source
ix)	Vega[32]	Cross Platform GUI	Java	Automated scanner, Intercepting proxy, proxy scanner	Subgraph	1.0	Open Source
x)	Hping[3 3]	CLI	C	Security auditing and testing of firewalls and networks,	Salvatore Sanfilippo	hping3-20051105 / November 5, 2005	Open Source
xi)	Nexpose [34]	Cross Platform	Not Known	Vulnerability scanner	Rapid7	6.6.164 / Oct 12, 2022	Sharewar e
xii)	Skipfish[35]	CLI	C	Information gathering, testing the security of websites and web servers	Google	Dec 4, 2012	Open Source
xiii)	W3af[36]	Cross Platform	Python	Web vulnerability scanner	Andres Riancho	1.6.54 / 10 June 2015	Open Source
xiv)	Nikto[37]	CLI	HTML, Perl, roff	Web application scanner	Chris Sullo	2.1.6 / July 9, 2015	Open Source
xv)	Masscan	CLI	C	TCPport	Robert	1.3.2/	Open

	[38]			scanner	Graham	Jan 31, 2021	Source
xvi)	Angry IP Scanner [39]	Cross Platform GUI	Java	IP address and port scanner	Anton Keks	3.8.2 / Jan22, 2022	Open Source
xvii)	Aircrack-ng[40]	Cross Platform	C	WiFi network security	Thomas d'Otreppede Bouvette	1.7 / May10,2022	Open Source

V. CONCLUSION& FUTURE SCOPE

The rise in cyber security cases leads to a lot of risks to organisations. If the users data or organisational data is compromised by hackers it may lead to a huge loss to the organisation. Therefore, organisations always try to protect their systems and network from any illegal access by doing penetration testing.In penetration testing, regular vulnerability assessment has been a major task. So this task must be automatic and automatic vulnerability scanners are used to detect the vulnerabilities and helps in fixing them. Different automatic scanners are used to accomplish this task. Some of them are commercial and some of them are open-source vulnerability scanners.

The present study involves the review of the literature in the area of vulnerability scanners that helps in detecting vulnerabilities. It can be observed from the comparison that scanners such as Nessus, Acunetix, Burpsuite, OWASP Zap, Nmap were used for vulnerability assessment more than others, Out of which OWASP Zap and Nmap are open-source vulnerability scanners that produce better results like commercial scanners. This study comprehensively discussed the vulnerability scanners that are used for vulnerability assessment and finding the fixes for them, and their performance was evaluated on different parameters. In the future, more open-source vulnerability scanners can be included along with the strategies to handle the latest vulnerabilities present at that time. Further, research needs to be conducted to find which open-source vulnerability scanner can detect and fix all the vulnerabilities that are listed by OWASP Top10 on different parameters.

REFERENCES

[1] Kushe, R. (2017), Comparative study of vulnerability scanning tools: Nessusvs Retina. International scientific journal "security & future", 1(2), (pp. 69-71).

[2] Wang, Y., Yang, J. (2017, March). Ethical hacking and network defense: choose your best network vulnerability scanning tool. In 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) (pp. 110-113).

[3] Lubis, A., Tarigan, A. (2017, January). Security Assessment of Web ApplicationThrough Penetration System Techniques. International Journal of RecentTrends in Engineering & Research (IJRTER), 4(100), (pp. 296-303).

[4] Nagpure, S., Kurkure, S. (2017, August). Vulnerability assessment and penetration testing of Web application. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1-6).

[5] Sandhya, S., Purkayastha, S., Joshua, E., & Deep, A. (2017, January). Assessment of website security by penetration testing using Wireshark. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-4).

[6] Tundis, A., Mazurczyk, W., &Muhlh ¨ auser, M. (2018, August). ¨ A review ofnetwork vulnerabilities scanning tools: types, capabilities and functioning. In Proceedings of the 13th international conference on availability, reliability and security (pp. 1-10).

[7] Al Shebli, H. M. Z., & Beheshti, B. D. (2018, May). A study on penetrationtesting process and tools. In 2018 IEEE Long Island Systems, Applicationsand Technology Conference (LISAT) (pp. 1-7).

[8] Abu-Dabaseh, F., & Alshammari, E. (2018, April). Automated penetrationtesting: An overview. In The 4th International Conference on Natural Language Computing, Copenhagen, Denmark (pp. 121-129).

[9] Ibrahim, A. B., & Kant, S. (2018). Penetration testing using SQL injectionto recognize the vulnerable point on web pages. International Journal of Applied Engineering Research, 13(8), (pp. 5935-5942).

[10] Xia, Y., Liu, C., & Yu, K. (2020, February). Design and Implementationof Vulnerability Scanning Tools for Intelligent Substation Industrial ControlSystem Based on Openvas. In IOP Conference Series: Earth and Environmental Science (Vol. 440, No. 4, p. 042031). IOP Publishing.

[11] Ghanem, M. C., & Chen, T. M. (2019). Reinforcement learning for efficientnetwork penetration testing. Multidisciplinary Digital Publishing Institute,11(1),(pp. 1-23).

[12] Shah, M., Ahmed, S., Saeed, K., Junaid, M., & Khan, H. (2019, January).Penetration testing active reconnaissance phase–optimized port scanningwith nmap tool. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6).

[13] Mohammed, M. O. (2020, September) Automatic Port Scanner. InternationalJournal of Innovative Science and Research Technology, (pp. 711-717).

[14] Ibarra-Fiallos, S., Higuera, J. B., Intriago-Pazmino, M., Higuera, J. R. B., ˜Montalvo, J. A. S., &Cubo, J. (2021). Effective filter for common injectionattacks in online web applications. IEEE Access, 9, (pp. 10378-10391).

[15] Amankwah, R., Chen, J., Kudjo, P. K., & Towey, D. (2020). An empirical comparison of commercial and open-source web vulnerability scanners.Software: Practice and Experience, 50(9), (pp. 1842-1857).

[16] Raut, J. T., Sharma, Y. K.,& Patil, V (2020). Comparative analysis of different security tools to detect network risks. European Journal of Molecular & ClinicalMedicine, 7(8), (pp. 4841-4846).

[17] Vats, P., Mandot, M., & Gosain, A. (2020, June). A comprehensive literaturereview of penetration testing & its applications. In 2020 8th InternationalConference on Reliability, Infocom Technologies and Optimization (Trendsand Future Directions)(ICRITO) (pp. 674-680).

[18] Jayasuryapal, G., Pranay, P. M., & Kaur, H. (2021, April). A Survey on Network Penetration Testing. In 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 373-378).

[19] Wibowo, R. M., &Sulaksono, A. (2021). Web Vulnerability Through CrossSite Scripting (XSS) Detection with OWASP Security Shepherd. IndonesianJournal of Information Systems, 3(2), (pp. 149-159).

[20] Alazmi, S., & De Leon, D. C. (2022, March). A Systematic Literature Review onthe Characteristics and Effectiveness of Web Application Vulnerability Scanners, IEEE Access, (pp. 33200-33219).

[21] Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi,N. (2022, April). A Comparative Study of Web Application Security Parameters:Current Trends and Future Directions. Applied Sciences, 12(8), 4077, (pp. 1-23).

[22] Mubaiwa, T. G., &Mukosera, M. (2022, February). A hybrid approach todetect security vulnerabilities in web applications. International Journal ofComputer Science and Mobile Computing, Vol.11 Issue.2, (pp. 89-98).

[23] "Penetration Testing" [Online]. Available: https://www.imperva.com/learn/application-security/penetration-testing/[Accessed on: 20-Sep-2022]

[24] "Penetration testing- Quick Guide" [Online]. Available: https://www.tutorialspoint.com/penetration_testing/pentration_testing_qick_guide.htm [Accessed on: 20-Sep-2022]

[25] "Nessus (software)" [Online]. Available:https://en.wikipedia.org/wiki/Nessus_(software) [Accessed on: 20-Sep-2022]

[26] "Nmap"[Online]. Available:https://en.wikipedia.org/wiki/Nmap[Accessed on: 20-Sep-2022]

[27] "OpenVAS"[Online]. Available:https://en.wikipedia.org/wiki/OpenVAS [Accessed on: 20-Sep-2022]

[28] "Burp Suite Community Edition" [Online]. Available:https://portswigger.net/burp/communitydownload [Accessed on: 20-Sep-2022]

[29] "Acunetix" [Online]. Available:https://www.acunetix.com/ [Accessed on: 20-Sep-2022]

[30] "OWASP ZAP"[Online]. Available: https://www.zaproxy.org/ [Accessed on: 20-Sep-2022]

[31] "Wireshark" [Online]. Available: https://en.wikipedia.org/wiki/Wireshark [Accessed on: 20-Sep-2022]

[32] "Vega Vulnerability Scanner"[Online]. Available:https://subgraph.com/vega/ [Accessed on: 20-Sep-2022]

[33] "hping"[Online]. Available:https://en.wikipedia.org/wiki/Hping [Accessed on: 20-Sep-2022]

[34] "Nexpose Vulnerability Scanner"[Online]. Available:https://www.rapid7.com/products/nexpose/ [Accessed on: 20-Sep-2022]

[35] **"**Meet skipfish, our automated web security scanner"[Online]. Available:https://security.googleblog.com/2010/03/meet-skipfish-our-automated-web.html [Accessed on: 20-Sep-2022]

[36] "w3af" [Online]. Available:https://en.wikipedia.org/wiki/W3af[Accessed on: 20-Sep-2022]

[37] "Nikto (vulnerability scanner)" [Online]. Available: https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner) [Accessed on: 20-Sep-2022]

[38] "Masscan" [Online]. Available:https://github.com/robertdavidgraham/masscan [Accessed on: 20-Sep-2022]

[39] "Angry IP Scanner"[Online]. Available: https://www.bugcrowd.com/glossary/angry-ip-scanner/ [Accessed on: 20-Sep-2022]

[40] "Aircrack-ng" [Online]. Available: https://en.wikipedia.org/wiki/Aircrack-ng[Accessed on: 20-Sep-2022]