IJNRD.ORG ISSN : 2456-4184
International Research Journal IJNRD Research Through Innovation
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Automated Testing Of a Website Using Web Threat Detector

Y. Mythili Maha Lakshmi, Y. Vamshi Vardhan Raj, Unnam Deepthi Chowdary, Oduri Gehini Naga Sai Ratna, Dr. Gayathri Edamadaka

Department of Computer Science and Engineering, Koneru Lakshmaiah University, Hyderabad, India

***Abstract*—Daily advancements in technology are making vulnerabilities more prevalent. Typically, attackers take advantage of these weaknesses to exploit the systems. Attackers use many methods to exploit systems to gain information or to get access to that specific system. To secure the system, the organizations use VAPT in defense to secure their systems as well as to improve the security of the systems. There are two ways to secure the system using VAPT ones is manual pentesting and the other is automated pentesting. VAPT focuses on protecting the system by fixing the exploits as an attacker can gain access or the information of the system through loopholes or the endpoints. So VAPT usually is a defense mechanism to protect the system or the website from attackers. Many organizations do VAPT regularly to secure their websites and also to fix the endpoints that are vulnerable or exposed to the internet from attackers. To secure the system from hackers our project helps the organizations and the users to scan the target and to check the vulnerabilities which are present on the target along with the remediation and the threat level. We have used a few tools like Nmap, whois, dnswalk to develop the project.**

***Index Terms*—Vulnerability Assessment and Penetration Testing VAPT, Severity, Vulnerability, Exploits, Attacker, Automated testing, security.**

I. Introduction

In this era, the technology is playing a crucial role. And with the increasing technology, lack of security has become a major problem. Though VAPT can resolve this issue there is no guarantee that software or a system is 100 percent secure. Organizations and users try to secure the system as much as possible by fixing the vulnerabilities. In today's world, it is very important to secure the system as one loophole or one endpoint that is exposed to the internet or accessible by the attacker can lead to a huge loss such as an information leak or access gaining. VAPT is one of the methods to secure the system and most of the organizations are conducting external VAPT and internal VAPT regularly. There is no guarantee that a VAPT can find all the vulnerabilities that are available on the target but there is a high chance of finding many of the vulnerabilities which helps in securing our website. Regular VAPT and Red Teaming can help us in finding many vulnerabilities and endpoints. Many organizations are conducting vulnerability assessments regularly which helps them to identify the vulnerabilities at the specific endpoints. In this way, organizations can secure their website and protect their information from attackers and other unprivileged users. In this paper, we are going to describe vulnerability assessment and penetration testing and the importance of doing vulnerability assessment along with the vulnerabilities that we have found through our project. Our project is an automated tool that helps users identify the vulnerabilities that are present on the target along with the severity level of the vulnerability and remediation. The severity of the vulnerability will help the user or the organization prioritize certain vulnerabilities based on the severity level while fixing the vulnerabilities. The remediation of the vulnerability which will be given by our tool will help the users or the organizations to understand the way to fix the vulnerability that has been found on their target system.

II. Pentesting and it's workflow

A. Pentesting

Vulnerability Assessment and Penetration Testing (VAPT). Vulnerability Assessment and Penetration Testing is a step by step process. Vulnerability Assessment is used for security testing to identify security vulnerabilities in an application, networks, clouds, and endpoints. Vulnerability Assessment is a process of scanning the networks, software, and systems to find out their vulnerabilities, and weaknesses in them. This weakness provides a backdoor for the attacker to attack their victims. Access control, boundary conditions, input validation, authentication, configuration weakness, and exception handling vulnerabilities are just a few examples of the vulnerabilities that might exist in a system. Assessing a system's, piece of software's, or network's vulnerability involves looking for flaws and vulnerabilities. These vulnerabilities may provide an attacker access to the victim's backdoor. Penetration testing is the next step or phase for the Vulnerability Assessment and Penetration Testing. Penetration testing tries to exploit the system in an authorized manner. The penetration tester has the authorization to perform penetration testing, and he carefully abuses the system to identify potential vulnerabilities

B. Pentesting Workflow

Scope is the first step in the VAPT workflow. In Scope, we will collect the assets of the target. These encompass several critical elements such as systems, networks, and applications, and define the boundaries within which the assessment. The

Identify applicable funding agency here. If none, delete this.

vulnerability assessment can only be performed on the assets which are found in the recon. This gives a focused analysis of the most critical assets and potential attack surfaces. Information Gathering is the next step of the VAPT workflow. Information Gathering plays a vital phase in VAPT. This phase establishes the base for locating possible weak points and avenues of assault. In addition, the examination and open-source intelligence (OSINT) help to create a thorough grasp of the protocols, configuration, and security threats associated with the target environment. In this process, we will be using tools like Acunetix, Nuclei, Nessus, and Burp Suite [2]. Vulnerability. Detection is the next step in the VAPT workflow. Vulnerability Detection aims to identify security flaws and weaknesses which are within the systems, applications, and networks. This process involves various techniques and various tools to analyze, and systematically scan the security of the target environment. Information Analysis Planning is the next step in the VAPT workflow. In this information analysis, the data collected during the reconnaissance is organized and interpreted to gain the vulnerabilities of the target environment, potential attacks, and weaknesses. Privilege Escalation is the next step in the VAPT workflow. Privilege Escalation is a critical security concern in the networks and computer systems unauthorized elevation of user privileges to gain access. Result Analysis is the next step in the VAPT workflow. This phase involves in interpretation and examination of the findings which were acquired during the assessment. Reporting is the next step in the VAPT workflow. This is an important phase that encapsulates the findings, insights, and recommendations from the assessment process. Cleanup is the final step of the VAPT workflow. This process is crucial assuring the target environment is secure. In this phase security experts will handle any alterations, adjustments, or impairments experienced throughout the examination to reinstate the confidentiality, availability, and integrity of the networks, systems, and applications.

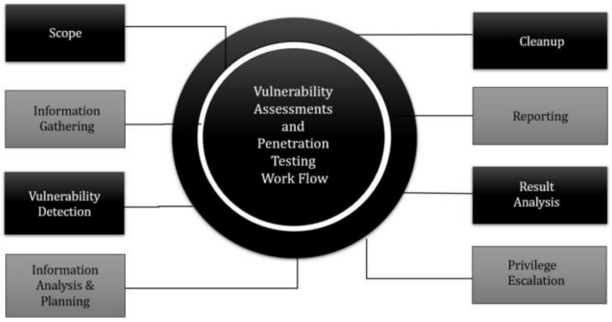
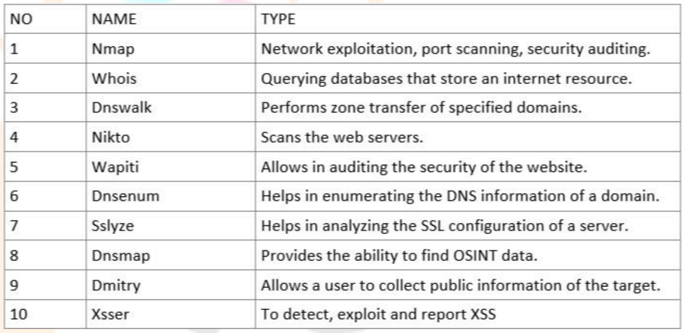


Fig. 1. This is the step by step workflow that will be followed in the VAPT to secure the system.

III. Methods

A. TOOLS USED

Our project helps the users and organizations who want to do a vulnerability assessment on their specific target. Our project is an automated vulnerability assessment tool that will allow users to perform a vulnerability assessment on their target. After performing the vulnerability assessment the user will be able to see the vulnerabilities that have been identified by our tool on that specific target along with the severity level and the remediation of that vulnerability. The severity level helps the user to understand the priority sequence of the vulnerabilities while fixing it and the remediation will help the user to understand the way to fix the vulnerability at a specific endpoint. As the user needs to know both the severity level of the vulnerability and the remediation of the vulnerability before fixing the vulnerability. We have used several tools to develop this project which will help in port scanning and vulnerability identification. These tools have added a significant impact to our project and have helped us in gaining more accurate results. These tools not only helped us to achieve our goal but also helped us to make a simple project where a user can use all the tools together to test their website to find accurate results. Below are the tools that are included in this project.



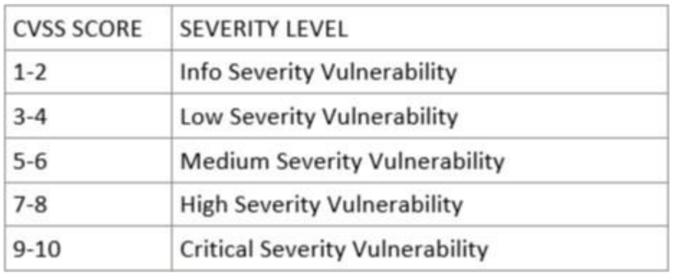
NO	NAME	TYPE
1	Nmap	Network exploitation, port scanning, security auditing.
2	Whois	Querying databases that store an internet resource.
3	Dnswalk	Performs zone transfer of specified domains.
4	Nikto	Scans the web servers.
5	Wapiti	Allows in auditing the security of the website.
6	Dnsenum	Helps in enumerating the DNS information of a domain.
7	Sslyze	Helps in analyzing the SSL configuration of a server.
8	Dnsmap	Provides the ability to find OSINT data.
9	Dmitry	Allows a user to collect public information of the target.
10	Xsser	To detect, exploit and report XSS

Fig. 2. These above are the tools that have been included in our project to develop an automated pentesting tool

B. SEVERITY LEVELS

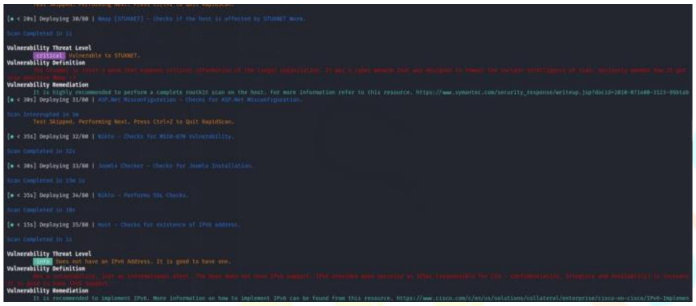
While performing a vulnerability assessment the user needs to identify the priority of the vulnerabilities while fixing them. If the user fails to identify the priority of the vulnerabilities while fixing them then that might cause a huge impact on the organization as the attacker can exploit the vulnerability before the user fixes it so the user needs to know the priority of the vulnerability while fixing them. Our project helps the user to identify the priority of the vulnerability while fixing it with the severity level that is displayed along with the vulnerability. This severity level helps the user to identify the priority vulnerabilities while fixing the vulnerabilities. These CVSS scores help us in identifying the severity of the vulnerability which is not only useful to identify the severity level of the vulnerability but also useful to understand the segregation and impact of the vulnerability. .

The CVSS score helps us to determine the severity level of the vulnerability. Every severity level has many vulnerabilities based on the impact of the vulnerability and it is very important to segregate the vulnerabilities based on the severity level to identify the impact of the vulnerability and also to fix the vulnerability.



CVSS SCORE	SEVERITY LEVEL
1-2	Info Severity Vulnerability
3-4	Low Severity Vulnerability
5-6	Medium Severity Vulnerability
7-8	High Severity Vulnerability
9-10	Critical Severity Vulnerability

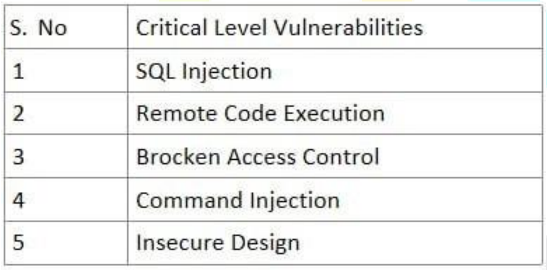
Fig. 3. Segregation of severity levels of the vulnerabilities based upon the CVSS score.



```
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.
[● < 20s] Deploying 30/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 1s

Vulnerability Threat Level
        critical  Vulnerable to STUXNET.
Vulnerability Definition
        This STUXNET is Level-1 worm that exposes critical information of the target organization. It was a cyber weapon that was designed to thwart the nuclear intelligence of Iran. Seriously wonder how it got
 here? Hope this isn't a false positive Nmap ;)
Vulnerability Remediation
        It is highly recommended to perform a complete rootkit scan on the host. For more information refer to this resource. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tab
[● < 30s] Deploying 31/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.

Scan Interrupted in 0s
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 35s] Deploying 32/80 | Nikto - Checks for MS10-070 Vulnerability.

Scan Completed in 32s

[● < 30s] Deploying 33/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 13m 1s

[● < 35s] Deploying 34/80 | Nikto - Performs SSL Checks.

Scan Completed in 10s

[● < 15s] Deploying 35/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 1s

Vulnerability Threat Level
        info  Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
        Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availability) is incorpor
 It is good to have IPv6 Support.
Vulnerability Remediation
        It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implemen
```

Fig. 4. The critical level vulnerability - Vulnerable to STUXNET

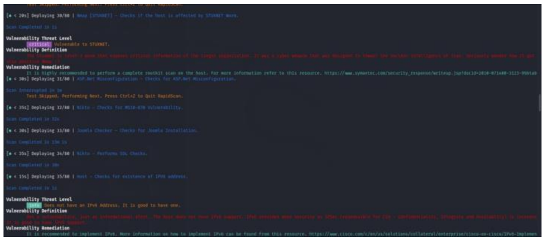
As shown in the figure-4 we have identified a critical level vulnerability by using our tool. The critical vulnerabilities are the vulnerabilities that have a high impact and these are the vulnerabilities that are mostly targeted by the hackers. Organizations need to perform VAPT regularly to secure their websites or systems from exploits performed by hackers.



S. No	Critical Level Vulnerabilities
1	SQL Injection
2	Remote Code Execution
3	Brocken Access Control
4	Command Injection
5	Insecure Design

Fig. 5. Examples of critical level vulnerabilities

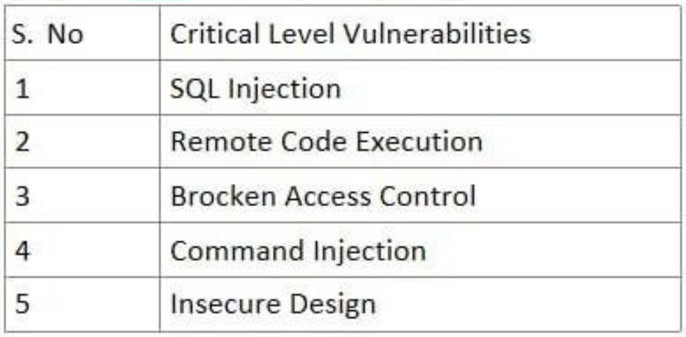
As shown in Figure 5 the vulnerabilities that have a high impact on the system or data are categorized into critical- level vulnerabilities. These vulnerabilities have to be fixed on priority by the users because if these vulnerabilities are exploited by the hacker then it might lead to a huge loss of data or unauthorized access.



```
[● < 20s] Deploying 30/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 1s

Vulnerability Threat Level
        critical  Vulnerable to STUXNET.
Vulnerability Definition
        This STUXNET is Level-1 worm that exposes critical information of the target organization. It was a cyber weapon that was designed to thwart the nuclear intelligence of Iran. Seriously wonder how it got
 here? Hope this isn't a false positive Nmap ;)
Vulnerability Remediation
        It is highly recommended to perform a complete rootkit scan on the host. For more information refer to this resource. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tab
[● < 30s] Deploying 31/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.

Scan Interrupted in 0s
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 35s] Deploying 32/80 | Nikto - Checks for MS10-070 Vulnerability.

Scan Completed in 32s

[● < 30s] Deploying 33/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 13m 1s

[● < 35s] Deploying 34/80 | Nikto - Performs SSL Checks.

Scan Completed in 10s

[● < 15s] Deploying 35/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 1s

Vulnerability Threat Level
        info  Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
        Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availability) is incorpor
 It is good to have IPv6 Support.
Vulnerability Remediation
        It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implemen
```

Fig. 6. The High-level vulnerability - RDP server has been detected over UDP

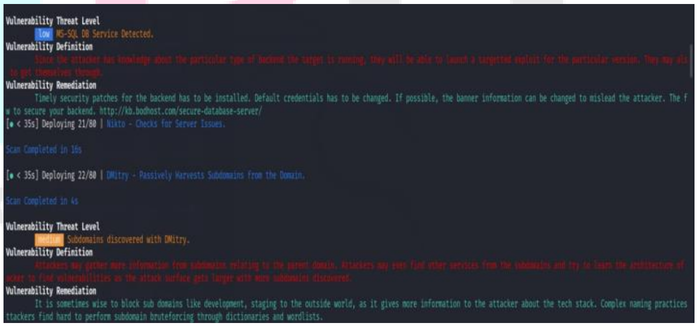
As shown in Figure 6 the vulnerabilities that have a high impact on the system or data are categorized into high-level vulnerabilities. These high-level vulnerabilities are the vulnerabilities that have a high impact and these are the vulnerabilities that are mostly targeted by hackers or unauthorized users.



S. No	Critical Level Vulnerabilities
1	SQL Injection
2	Remote Code Execution
3	Brocken Access Control
4	Command Injection
5	Insecure Design

Fig. 7. Examples of high-level vulnerabilities

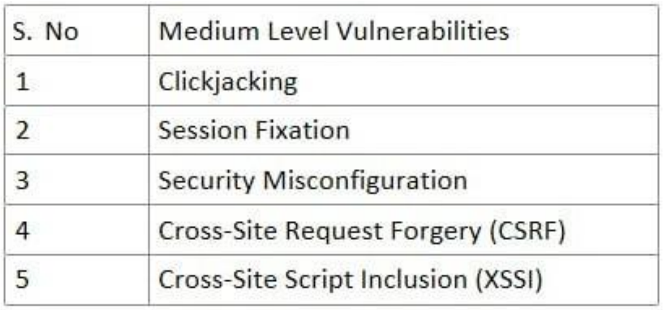
These vulnerabilities have to be fixed on priority just like the critical level vulnerability as these vulnerabilities can also be exploited by the hacker or the third party which might lead to a huge loss of data or unauthorized access.



```
Vulnerability Threat Level
        low  MS-SQL DB Service Detected.
Vulnerability Definition
        Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may als
 to get themselves through.
Vulnerability Remediation
        Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The f
w to secure your backend. http://kb.bodhost.com/secure-database-server/
[● < 35s] Deploying 21/80 | Nikto - Checks for Server Issues.

Scan Completed in 16s

[● < 35s] Deploying 22/80 | DMitry - Passively Harvests Subdomains from the Domain.

Scan Completed in 4s

Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of
acker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices
ttackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

Fig. 8. The medium-level vulnerability - Subdomains discovered through Dmitry

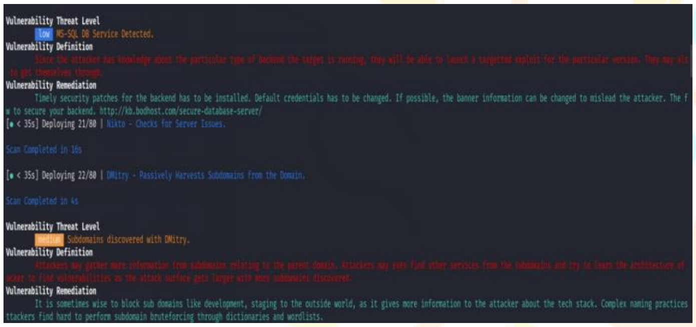
As shown in Figure 8 the vulnerabilities that have a medium-level impact on the system or data are categorized into medium-level vulnerabilities.



S. No	Medium Level Vulnerabilities
1	Clickjacking
2	Session Fixation
3	Security Misconfiguration
4	Cross-Site Request Forgery (CSRF)
5	Cross-Site Script Inclusion (XSSI)

Fig. 9. Examples of medium-level vulnerabilities

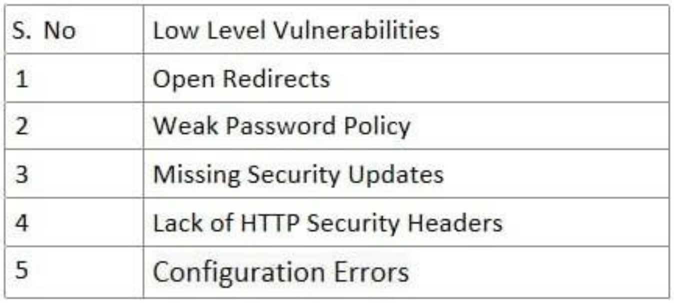
These vulnerabilities don’t have a huge impact like the critical and high-level vulnerabilities but it is important to fix these vulnerabilities to make the system more secure.



```
Vulnerability Threat Level
        low  MS-SQL DB Service Detected.
Vulnerability Definition
        Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may als
 to get themselves through.
Vulnerability Remediation
        Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The f
w to secure your backend. http://kb.bodhost.com/secure-database-server/
[● < 35s] Deploying 21/80 | Nikto - Checks for Server Issues.

Scan Completed in 16s

[● < 35s] Deploying 22/80 | DMitry - Passively Harvests Subdomains from the Domain.

Scan Completed in 4s

Vulnerability Threat Level
        medium  Subdomains discovered with DMitry.
Vulnerability Definition
        Attackers may gather more information from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of
acker to find vulnerabilities as the attack surface gets larger with more subdomains discovered.
Vulnerability Remediation
        It is sometimes wise to block sub domains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices
ttackers find hard to perform subdomain bruteforcing through dictionaries and wordlists.
```

Fig. 10. The low-level vulnerability - MS-SQL DB service detected

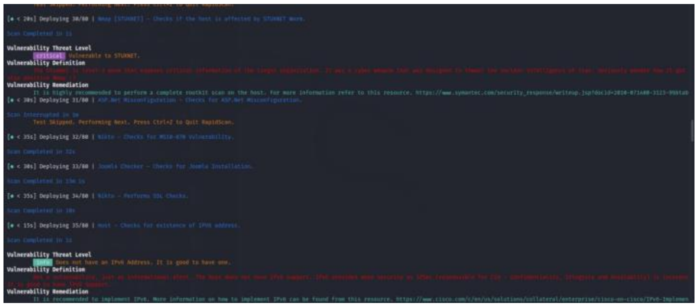
As shown in Figure 10 the vulnerabilities that have a low impact on the system or data are categorized into low-level vulnerabilities. These low-level vulnerabilities are the vulnerabilities that have a low impact and these are the vulnerabilities that are mostly informative. These may contain information about the outdated technologies that are being used by the system.



S. No	Low Level Vulnerabilities
1	Open Redirects
2	Weak Password Policy
3	Missing Security Updates
4	Lack of HTTP Security Headers
5	Configuration Errors

Fig. 11. Examples of low-level vulnerabilities

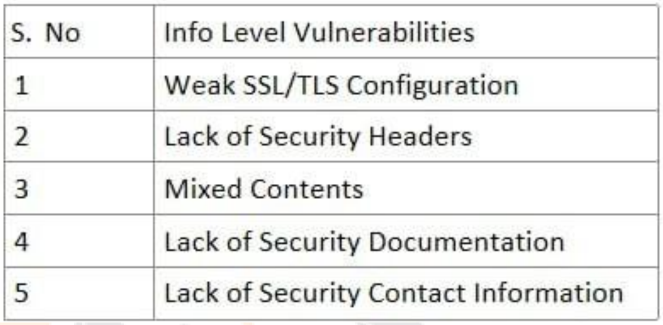
These vulnerabilities don’t have a huge impact like the critical, medium, and high-level vulnerabilities as it has not much impact on the system but it is advised to fix these vulnerabilities to make the system more secure.



```
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.
[● < 20s] Deploying 30/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 1s

Vulnerability Threat Level
        critical  Vulnerable to STUXNET.
Vulnerability Definition
        [illegible]
[illegible]
Vulnerability Remediation
        It is highly recommended to perform a complete rootkit scan on the host. For more information refer to this resource. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tab
[● < 30s] Deploying 31/80 | ASP.Net Misconfiguration - Checks for ASP.Net Misconfiguration.

Scan Interrupted in 3s
        Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 35s] Deploying 32/80 | Nikto - Checks for MS10-070 Vulnerability.

Scan Completed in 22s

[● < 30s] Deploying 33/80 | Joomla Checker - Checks for Joomla Installation.

Scan Completed in 13m 1s

[● < 35s] Deploying 34/80 | Nikto - Performs SSL Checks.

Scan Completed in 10s

[● < 15s] Deploying 35/80 | Host - Checks for existence of IPV6 address.

Scan Completed in 1s

Vulnerability Threat Level
        info  Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
        Not a vulnerability, just an informational alert. The host does not have IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availability) is incorpo
It is good to have IPv6 Support.
Vulnerability Remediation
        It is recommended to implement IPv6. More information on how to implement IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implemen
```

Fig. 12. The Info level vulnerability - Does not have the IPV6 address

As shown in Figure 10 the vulnerabilities that have an informational level or low impact on the system or data are categorized into info-level vulnerabilities. These info-level vulnerabilities are the vulnerabilities that have a low impact or no impact and these are the vulnerabilities that are mostly informative.



S. No	Info Level Vulnerabilities
1	Weak SSL/TLS Configuration
2	Lack of Security Headers
3	Mixed Contents
4	Lack of Security Documentation
5	Lack of Security Contact Information

Fig. 13. Examples of low-level vulnerabilities

These vulnerabilities don’t have a huge impact like other severe-level vulnerabilities as it has not much impact on the system. Most of the info-level vulnerabilities are informational which means they give basic information about the technologies being used and have no impact.

IV. Results and Discussion

We have achieved 90 percent accuracy in the process of finding the vulnerabilities in a specific target. The main goal of our project is to identify the vulnerabilities of a specific target that has been provided by the user with the most accurate results along with the remediation and the severity level. Our project not only finds the vulnerabilities that are found on a specific target but will also check whether there are any critical ports open. So that the user can resolve the issue before the attacker accesses the system and the data. Technology and threats are increasing simultaneously. To protect the system or the website performing a vulnerability assessment is necessary. Performing the vulnerability assessment regularly can secure the website from exploits and our project fulfils the same need. Our project not only scans the target but also provides the vulnerabilities that have been found along with the details of that vulnerability which makes the job easy for the user. The user can find all the vulnerabilities along with the severity level and remediation through our project. We were able to find many vulnerabilities with many severity levels. We found many critical level and high-level vulnerabilities along with other low, medium, and high-level vulnerabilities. The results are very accurate which makes it a highly promising tool with accurate and detailed results that gives all the details about the vulnerabilities that have been found.

V. CONCLUSION

Our ultimate goal was to build a project which would help in vulnerability assessment. We began by performing research on existing automated pentesting tools. Next, we have gathered a few tools to develop this project which has not only increased the accuracy of the project but also increased the efficiency of the project. Once we were done with importing the tools we worked efficiently on the severity level indications where we had to segregate the vulnerabilities based on their severity levels. These vulnerability severity levels will help the users prioritize the vulnerabilities while fixing them. Then we efficiently worked on recommendations. These recommendations will help the user in fixing the vulnerability. We carefully compared the results with other vulnerability scanners to find accurate results. After comparing and validating the results it was evident that our tool gives accurate results along with the severity level and the recommendation. Every organization is performing a vulnerability assessment on their assets reg- ularly to secure their website or the system. Our tool helps them to secure their website with accurate results and the other required details. Our tool gives accurate results of the vulnerabilities that are available on the target along with the details of the vulnerability like severity level and remediation.

REFERENCES

[1] Abbadi, I.M., Alawneh, M., 2012. A framework for establishing trust in the Cloud. Comput. Electr. Eng. 38 (5), 1073–1087.

[2] bbadi, I.M., Martin, A., 2011. Trust in the Cloud. Inf. Secur. Techn. Rep. 16, 108–114.

[3] Adjei, J.K., Blackman, C., Blackman, C., 2015. Explaining the role of trust in cloud computing services. Info 17.

[4] Afroz, S., Navimipour, N.J., 2017. Memory designing using quantum dot cellular automata: systematic literature review, classification, and current trends. J. Circuits Syst. Comput. 26 (12), 1730004 (2017)

[5] Alhanahnah, M., Bertok, P., Tari, Z., 2017. Trusting cloud service providers: trust phases and a taxonomy of trust factors. IEEE Cloud Comput. 4,44–54.

[6] Liu Yan, Jay Xiong, A Framework For Web-Based Advanced Persistent Threat Detection, Volume: 3, Issue: 2, 01 July-Dec 2020.

[7] Mehrbod Sharifi; Eugene Fink; Jaime G. Carbonel, Application of crowdsourcing to the detection of web threats, October 2011.

[8] Yangyang Li; Yaping Su, the Insider Threat Detection Method of University Website Clusters Based on Machine Learning, 29 May 2023.

[9] Haosheng Li; Xuejiao Zhao; Qingqing Ren, Development of WEB-based Automatic Detection Tool for Web Attack Traceability, 25 September 2022.

[10] K. Vijayalakshmi; A. Anny Leema, Extenuating web vulnerability with a detection and protection mechanism for secure web access, 18 March 2017