An Investigation of Vulnerabilities Discovery and Assessment in Educational Institutions

SHABANA SHEIKH[1], DR. UMESH KUMAR SINGH[2], ABHISHEKRAGHUVANSHI[3], VANDANARATHORE[4]

[1] *Institute of Computer Sciences, Vikram University, Ujjain, India*

[2] *Director, Institute of Computer Sciences, Vikram University, Ujjain, India*

[3] *Department of Computer Science & Engineering, Mahakal Institute of Technology, Ujjain, India*

[4] *Government College, Jhiran, India*

Abstract- ***The data systems of universities are depended upon substantially for a variety of crucial reasons, including the management of academic programmes, the conduct of research, the dissemination of knowledge, and teaching and learning. One of the numerous new security threats to networks and information systems is the increase in computer-assisted fraud and attacks by cybercriminals both inside and outside the network. There are currently a wide array of dangers to the information systems and network infrastructure that could potentially compromise the dependability of the computer systems used in our educational institutions.This study presents an investigation of vulnerability discovery and assessment in educational institutions host network. In experimental work, two host networks were screened using Acunetix, Zaproxy, and OpenVAS scanners. These host networks belongs to educational institutions of North India. For security point of view, names of all hosts are not disclosed here. Form experimental results, it is clear that Accunetix tool is discovering maximum vulnerabilities in the host network segments.***

Indexed Terms- Vulnerability, Threats, Security and Privacy, Vulnerability Assessment, Accunetix

I. INTRODUCTION

Universities focus solely a lot on data systems for critical functions such as educating children, acquiring knowledge, administrative structure, scientific studies, and knowledge transfer [1]. Researcher insists that an academic information system would have to provide relevant data about study and scientific collaboration opportunities, along with additional education possibilities, when emphasizing the features and functionality of a university information system [2]. According to researchers, dependence extensively on computers as well as other techniques introduces a fresh set of security concerns. Security threats to networks and information systems are increasing from a variety of sources, including computer-assisted fraud and attacks from cybercriminals within or outside the network. Today, there are numerous risks to information system and network infrastructure that adversely impact the dependability of computer systems on our academic institutions [3].

In recent years we have seen a huge increase in popularity of web-based applications. By using web-applications we can interact with a remote server through a web browser. It replaced traditional desktop applications and becoming an essential instrument for large and small organizations around the world [4]. A web-based application runs on any operating system which can be accessed universally. Web appliance plays an important role in the direction of making an individual‟s life informal. Now a day‟s web-based applications are more beneficial rather than desktop applications because this application doesn‟t require additional software [5]. It can easily run on any device. Various online services are available like shopping, financial services, social network, TV editing, mapping, lexis, serach amenities and betting. -The use of such types of services by people efficiently and cost- effectively. It is highly scalable and cost-effective and fast. In today‟s market web-based systems are more in demand. But these systems used various languages

that invites some inherent vulnerability. Now a day it is very essential to recognize this weakness for developing secure web applications. But providing effectiveness and efficiency hasn‟t enough. It requires better security and reliability too. It is more difficult to make web-applications safe because they are already open to the everyone. Use of network firewall, Intrusion prevention system, Secure Socket Layer (SSL) doesn‟t entirely protect a site. Most websites are in the applications layer rather than the network or system layer which is more vulnerable. By using web application scanners we can reduce some vulnerability from web applications. Web applications scanners scan pages of web application and find threats by pretending attacks on application. In today‟s market so many web application scanning tools are available. To figure out the susceptibilities within a network administrator use some severity tools and services including mappers, port scanners, analyzers, etc. Such type of severity tools to solve web administration and observing also help in examining for security configuration problems [6].

Hacking, malware attacks, pop - up ads, phishing, Denial of service (DoS), and Domain Name Service (DNS) spoofing are some examples of common threats to computer networks. The complexity of computer networks in universities far exceeds that of commercial enterprises. But it must keep providing its customers with the same high quality service (students and members of staff). It can be difficult to secure university infrastructures because to the vast number of users, the variety of client computers, and the open nature of an institution whose teaching staff and departments are autonomous. [7].

II. VULNERABILITY SCANNING AND ASSESSMENT TOOLS

To find known vulnerability signature using automated software. It detects and classifies system weakness in networks, computers, and communication devices and also predicts the effective countermeasure [8]. This scan raises some issues like errors, rebooting the system and also reduces productivity [9]. It is divided into two parts authenticated and unauthenticated scan.

i. Authenticated scan: In this scan , the tester logs in as a network user which reveals the vulnerability that are access by authenticated user or an attacker that has obtained access as a legitimate user.
ii. Unauthenticated scan: In this method, a tester without logging into the network reveals vulnerabilities.

Scanning and vulnerability evaluation is a methodical investigation of computer networks and their components in order to determine the security measures in place and the level of security aggression [10] [11]. Because they monitor known security holes and analyse possible dangers before malicious software or hackers can take advantage of them, screening and vulnerability assessment solutions are crucial [12] [13]. The data collected by these instruments serves as a database of vulnerabilities in computer systems or other mechanisms. It aims to investigate every flaw in the given services on the target host range and classify their severity before presenting the results.There are numerous of these kind of tools, but this study focuses primarily on three of them and which are

- Acunetix Vulnerability Scanner
- Greenbone Security Manager / Open Vulnerability Assessment System (OpenVAS)
- Zaproxy Scanner by OWASP

- OpenVAS

The Open Vulnerability Assessment System (OpenVAS) [14], currently known as Greenbone Security Manager is an open-source vulnerability scanner. OpenVAS scans the network and application for security flaws and generates a result based on the status of the network.

- Acunetix Vulnerability Scanner

Acunetix [15] was the initial web security analyzer on the sector and has been continuously improved since 2005. It is a sophisticated, customized tool created by cybersecurity testing experts. Because of this specialization, it was possible to create a realistic alternative that is more efficient than most other proprietary tools.Acunetix vulnerability scanner is a comprehensive web application security screening solution that can be used independently or as part of a larger environment. It includes built-in known vulnerabilities detection and management, as well as numerous functioning with economy software

development tools. By incorporating Acunetix into your security plan, you can drastically enhance your security posture and completely eradicate many potential risks at a minimal price.

- Zaproxy by OWASP

The safety of software. Articles, methods, Documentations, and free tools are available through OWASP online community. It is a graphical user interface written in java. Features provided by ZAP tool:

- It performs fuzzing, scripting, spidering and proxing on web applications using tester. It runs on windows as well as on recent version of kali Linux.
- To run ZAP tool Java runtime environment requires.
- It is easy to use. Also its scanning is manual as well as automatic.
- It also generates reports in XML and HTML format.
- ZAP tool is freely available and open source software used by beginners and professionals penetration testers.
- It has a special ability of automatic security testing that attracks developer and functional testers.
- But it should be used either by personal appliance or those which are authorized to check.

Acunetix, Zaproxyand OpenVAS web scanners are having same set of parameters for vulnerability detection and management. They perform fuzzing, scripting, spidering and proxing on web applications using tester. They run on windows as well as on recent version of kali Linux.

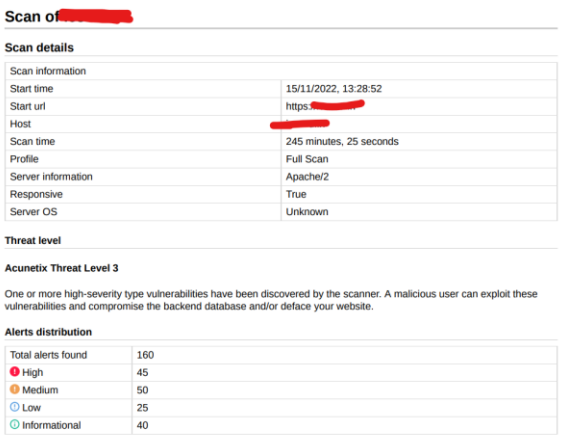
III. VULNERABILITY DISCOVERY

We used a vulnerability assessment strategy to the host that we had just found in order to ensure that this stage of the data collection process would go off without a hitch. This is despite the fact that manual methods cannot compete with automatic scanners in terms of speed. However, it is suggested to apply both human and automated scanning methodologies in order to completely appreciate the vulnerabilities that could have infiltrated the system or network. This can be accomplished by doing the scans in parallel. Let's imagine that the systems we're testing are running on a gigantic network that's made up of hundreds of separate nodes. If you tried to do this manually, you would waste a lot of time and have very little success. At this point in the process, human methods were replaced by automated scanners since it takes longer to acquire a perfect scan using human methods.

Acunetix, Zaproxyand OpenVAS were chosen as algorithmic scanning and security vulnerabilities scanners. The above scanners were deployed to determine what operating systems and services were running on the target hosts, as well as which hosts and utilities were vulnerable

In experimental work, two host networks were screened using Acunetix, Zaproxy, and OpenVAS scanners. These host networks belongs to educational institutions of North India. For security point of view, names of all hosts are not disclosed here.

4.1 Findings and Results of Acunetix



Scan of [redacted]

Scan details

Scan information	
Start time	15/11/2022, 13:28:52
Start url	https:[redacted]
Host	[redacted]
Scan time	245 minutes, 25 seconds
Profile	Full Scan
Server information	Apache/2
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	160
High	45
Medium	50
Low	25
Informational	40

Figure 1: Summary of Vulnerabilities Discovered in Host XYZ-Educational Web Application using Acunetix Scanner

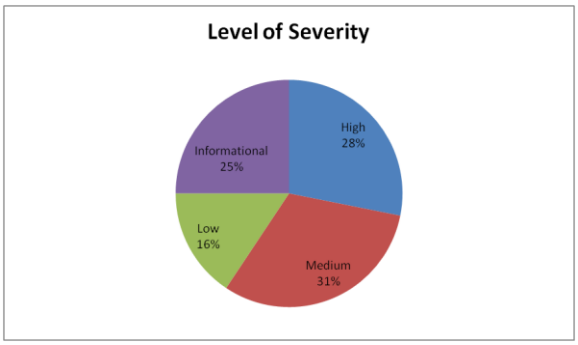


Figure 2: Level of Severity in Host XYZ-Educational Web Application using Acunetix Scanner

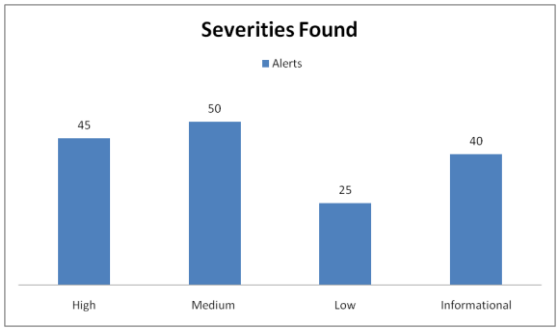


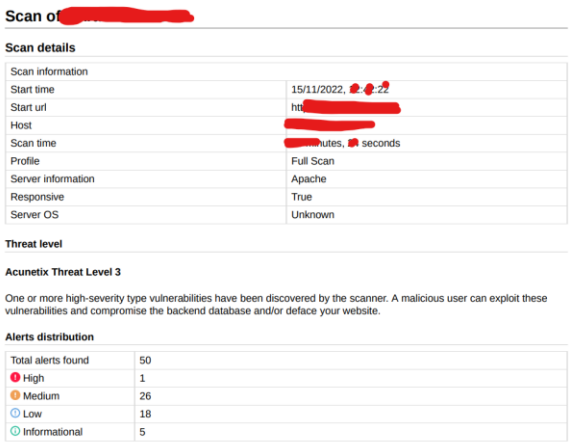
Figure 3: Number of severities found in Host XYZ-Educational Web Application using Acunetix Scanner

These figures 1, figure 2 and figure 3 shows different types of alerts which were found in active scanning. Figure 2 shown level of severity found in scanning of web application. It is clear that the 59 % alerts fall under the category of high/medium level of severity. So, it concludes that the level of severity in educational institutions network is at alarming level.

After the test was accomplished, the outcomes are arranged in the attentive tab. In that mainly total 160 alerts were found with different level risk including High Risk, Medium risk and Low Risk. Vulnerabilities found with different levels. When this tool captures all actions with different links was associated with website. It shows different levels of risk associated with web application. Table 1 presents different vulnerabilities detected in Host XYZ-Educational Web Application using Acunetix Scanner

Table 1: Vulnerabilities discovered in Host XYZ-Educational Web Application using Acunetix Scanner

Vulnerability Discovered	Vulnerability Count	Severity Level
Blind SQL Injection	28	High
Cross site scripting	17	High
Development configuration file	3	Medium
Error message on page	2	Medium
HTML form without CSRF protection	41	Medium
Slow HTTP Denial of Service Attack	1	Medium
Source code disclosure	3	Medium
Clickjacking: X-Frame-Options header missing	1	Low
Documentation file	1	Low
Login page password-guessing attack	3	Low
Possible sensitive directories	2	Low
Session token in URL		Low
Content Security Policy (CSP) not implemented	18	Informational
Content type is not specified	2	Informational
Email address found	25	Informational
Password type input with auto-complete enabled	7	Informational
Possible internal IP address disclosure	6	Informational



Scan of [redacted]

Scan details

Scan information	
Start time	15/11/2022, [redacted]
Start url	ht[redacted]
Host	[redacted]
Scan time	[redacted]utes, [redacted] seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	50
High	1
Medium	26
Low	18
Informational	5

Figure 4: Summary of Vulnerabilities Discovered in Host ABC-Educational Web Application using Acunetix Scanner

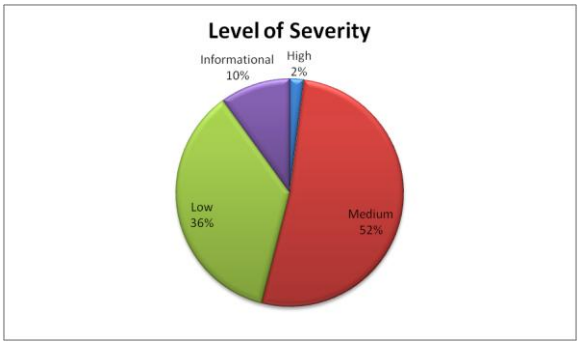


Figure 5: Level of Severity in Host ABC-Educational Web Application using Acunetix Scanner

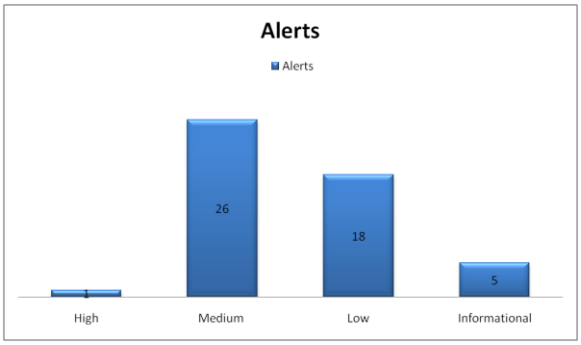


Figure6: No of Severities found in Host ABC-Educational Web Application using Acunetix Scanner

This figure 4, figure 5 and figure 6 shows different types of alerts which were found in active scanning of host ABC by Accunetix scanner. In that mainly total 50 alerts were found with different level risk including 1 alert at High Risk, 26 alerts at Medium risk, 18 alerts at low risk and 5 alerts at informational risk. Vulnerabilities found with different levels. When this tool captures all actions with different links was associated with website. It shows different levels of risk associated with web application. Table 2 presents Vulnerabilities discovered in Host ABC-Educational Web Application using Acunetix Scanner

Table 2: Vulnerabilities discovered in Host ABC-Educational Web Application using Acunetix Scanner

Vulnerability Discovered	Severity Level
Cross site scripting	High
Directory listing	Medium
HTML form without CSRF protection	Medium
User credentials are sent in clear text	Medium
Clickjacking: X-Frame-Options header missing	Low
Cookie(s) without Secure flag set (verified)	Low
Login page password-guessing attack	Low
Unencrypted connection	Low
Content Security Policy (CSP) not implemented	Informational
Password type input with auto-complete enabled	Informational

4.2 Findings and Results of OpenVAS / Greenbone Security Manager

OpenVAS was used to check the host network for any suspicious parts. Both Linux and Windows systems were scanned for security flaws by OpenVAS. Those identical credentials were used to run the OpenVAS scan. Scans resulted in reports that detailed vulnerabilities by plugins and hosts. Each report included the findings of a security scan, including information on the subnet, host, port, and severity for each plugin that had been deployed. OpenVAS's findings detailed the affected hosts, a brief explanation of the vulnerability, an evaluation of the severity of the vulnerability based on whether it affects just one application or the entire system, a suggested solution to the security flaws and how it might work, and additional resources for learning

more about the vulnerabilities that were found. OpenVAS vulnerabilities were rated High, Medium, Low, Log, or False Positive using the Common Vulnerability Scoring System (CVSS).The summary of scan results are shown in figure 7 and figure 8. In host 1 scanning, total 32 alerts were generated and in host 2 scanning, total 5 vulnerability alerts were generated.

Host	High	Medium	Low	Log	False Positive
[redacted]	4	28	0	0	0
Total: 1	4	28	0	0	0

Figure 7: Summary of Vulnerabilities Discovered in Host 1-Educational Web Application using OpenVAS / Greenbone Security Manager

Host	High	Medium	Low	Log	False Positive
[redacted]	0	5	0	0	0
Total: 1	0	5	0	0	0

Figure 8: Summary of Vulnerabilities Discovered in Host 2-Educational Web Application usingOpenVAS / Greenbone Security Manager

4.3 Findings and Results of Zaproxy by OWASP

After scanning completes, ZAP shows the result summary in the form of different categories in the form of XML, HTML, and many more. Basically, alerts are potential susceptibility and have been categorized as high severity, medium and low severity and informational severity, which indicates the degree of associated risks. To shows different categorized of susceptibility in various color flags. Each Flag has different meaning. Red flag says that it has high severity. Orange flag has medium severity, Yellow flag means low level severity and finally blue flag says that there will be no error yet found within website.

It includes attack, evidence, description, other information and reference. It also suggests the solution of the vulnerability. This tool is more helpful for developers to make their web application more secure. The summary of scan results are shown in figure 9 and figure 10. In host 1 scanning, total 16 alerts were generated and in host 2 scanning, total 6 vulnerability alerts were generated.

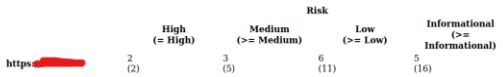


Figure 9: Summary of Vulnerabilities Discovered in Host 1-Educational Web Application using Zaproxy

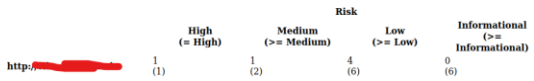


Figure 10: Summary of Vulnerabilities Discovered in Host 2-Educational Web Application using Zaproxy

4.4 Comparing results ofAcunetix, OpenVAS, and Zaproxy Vulnerability Scanners

Result comparison of Acunetix, OpenVAS, and Zaproxy for Host 1 and host 2 is shown in table 3 and table 4 respectively. Form results, it is clear that Accunetix tool is discovering maximum vulnerabilities in the host network segments.

Table 3- Result comparison of Acunetix, OpenVAS, and Zaproxy for Host 1

Tool Name	High	Medium	Low	Informational	Total Alerts
Acunetix	45	50	25	40	160
OpenVAS	4	28	0	0	32
Zaproxy	2	3	6	5	16

Ongoing scanning gives the alerts of associated risk with this website. In this scanning, high risk was detected in which SQL injection. The next medium level of alerts were detected like- Directory listing, HTML form without CSRF protection, User credentials are sent in clear text, Development configuration file, Error message on page, Slow HTTP Denial of Service Attack, Click-Jacking attacks, Source code disclosure, . After that different low level alerts were detected like- x-content type header, Login page password-guessing attack, Possible sensitive directories, Session token in URL

Table 4- Result comparison of Acunetix, OpenVAS, and Zaproxy for Host 2

Tool Name	High	Medium	Low	Informational	Total Alerts
Acunetix	1	26	18	5	50
OpenVAS	0	5	0	0	5
Zaproxy	1	1	4	0	6

CONCLUSION

Universities have computer networks that are much more complicated than those in businesses. But it must keep giving the same high level of service to its customers. Universities can be hard to keep safe because of the large number of users, the different types of client computers, and the openness of an institution where teachers and departments work on their own. Scanning and vulnerability evaluation is a systematic look at computer networks and their parts to find out what security measures are in place and how much security is being attacked. Screening and vulnerability assessment solutions are important because they keep an eye on known security holes and look for possible threats before malicious software or hackers can use them. The information that these instruments gather is used to make a list of weaknesses in computer systems and other mechanisms. Its goal is to look into every problem with the services on the target host range and rate how bad they are before presenting the results. This research will help researchers to plan and conduct penetration testing. This will also help future researchers in designing a vulnerability mitigation plan for the vulnerabilities discovered in this study.

REFERENCES

[1] U. K. Singh, and C. Joshi, "Network Security Risk Level Estimation Tool for Information Security Measure", IEEE PIICON 2016, 7th Power India International Conference, IEEE Computer Society, Bikaner Rajasthan, India, November 25-27, 2016.

[2] U. K. Singh, and C. Joshi, "Quantifying Security Risk by Critical Network Vulnerabilities Assessment", International Journal of Computer Application (IJCA 0975 – 8887), Volume 156(13), December 2016, ISBN 973-93-80883-35-9, pp 26-33, impact factor: 0.782.

[3] YuganshKhera, et al. (2019), "Analysis and Impact of Vulnerability Assessment and Penetration Testing", 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), India, 14th -16th Feb 2019,IEEE.

[4] ShobhaTyagi, Krishan Kumar (2018)," Evaluation of Static Web Vulnerability Analysis Tools", 978-1-5386-6026-3, 5th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2018).

[5] Sandeep Kumar Yadav,Daya Shankar Pandey,Shrikant Lade (2017)," A Comparative Analysis of Detecting Vulnerability in Network Systems", ISSN: 2277 128X,International Journal of Advanced Research in Computer Science and Software Engineering 7(5), May-2017, pp. 336-340

[6] JhilamBiswas,Ashutosh(2014)," An Insight in to Network Traffic Analysis using Packet Sniffer",International Journal of Computer Applications,Volume 94-Number 11.

[7] PratibhaYadav and Mr. Chandresh D. Parekh (2017)," A Report on CSRF Security Challenges & Prevention Techniques", International Conference on Innovations in Information, Embedded and Communication System (ICIIECS), IEEE.

[8] Gurdeep Singh, Jaswinder Singh(2016)," Evaluation of Penetration Testing Tools of KALI LINUX", ISSN 2347 – 8616, International Journal of Innovations & Advancement in Computer Science IJIACS, Volume 5, Issue 9 September 2016.

[9] K. Pranathi , S. Kranthi , Dr. A. Srisaila , P. Madhavilatha (2018), "Attacks on Web Application Caused by Cross Site Scripting", Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1.

[10] Khochare and Dr. B. B. Meshram (2012),"Tools to detect and prevent web attacks", ISSN: 2278-1323, International Journal of Advanced in Computer Engineering & Technology Volume 1, Issue 4.
[11] Fakhreldeen Abbas Saeed, Eltyeb E. AbedElgabar (2014)," Assessment of Open Source Web Application Security Scanners", ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology, Vol. 61 No.2.
[12] Gabriela Roldán-Molinaa,b, Mario Almache-Cuevaa, Carlos Silva-Rabadãob, IrynaYevseyevac, VitorBasto-Fernandesb,d (2017)," A Comparison of Cybersecurity Risk Analysis Tools", Procedia Computer Science 121 , 568–575.
[13] Hessa Mohammed Zaher Al Shebli and Babak D. Beheshti (2018)," A study on penetration testing process and tools",2018,IEEE, Long Island systems, Applications and Technology Conference(LISAT)
[14] https://www.openvas.org/
[15] https://www.acunetix.com/vulnerability-scanner/
[16] https://www.zaproxy.org/