International Journal of Scientific Engineering and Science
Volume 9, Issue 7, pp. 73-78, 2025. ISSN (Online): 2456-7361

White-Hat Hacking: Vulnerability Assessment of University Admission Portal

Amaefule I. A[1], Izuogu, Mary Yadilichukwu[2]
[1, 2]Department of Computer Science, Imo State University, Owerri, Imo State Nigeria.

Abstract— *This study examined university admissions portal vulnerability assessment and white-hat hacking. Finding, evaluating, and documenting security flaws in the university admissions site was the main goal of this project. The system has an authentication method that requires a username, password, and 2-Factor Authentication (2FA) in order for administrators and normal users to properly log in. Penetration testing is a crucial proactive strategy for locating security flaws before malevolent attackers can take advantage of them, as this study showed. For this investigation, the black-box and white-box pen testing methodology was used. It focuses on evaluating university admission portals with SQL Map, BurpSuite Community Edition, and Network Mapper (NMAP). The study's conclusions show that university admission portals are vulnerable to a number of security risks, such as exposed services, unpatched software, improperly configured systems, shoddy authentication procedures, and possible SQL injection flaws. Several risk indicators were identified through the use of automated and human penetration testing methods, highlighting the necessity of ongoing system security monitoring and enhancements. Among other things, the research suggested conducting routine penetration tests.*

Keyboards— *Whie-Hat Hacking, Vulnerability Analysis, Admission Portal, Penetration Testing, Nmap.*

I. Introduction

One of the main concerns with information systems is security. Software security is currently a greater concern than it was in the past due to the expanding internet connectivity of computers, the increasing extensibility of systems, and the unchecked expansion of system size and complexity [1]. In educational institutions, the admissions process is a delicate and important procedure that needs the highest security and integrity. Concerns regarding the security of online admission systems are developing as technology is used more and more in the admissions process. Data breaches and cyberattacks have increased in frequency, and educational institutions are not exempt from these dangers. As a result, making ensuring the admissions system is safe and shielded from unwanted access is crucial.

An essential part of the university's internet presence is the admission site, which enables potential students to apply for admission and obtain vital information [2]. The university admission site is susceptible to cyberthreats and assaults, just like any other web application [3]. A proactive strategy for locating and addressing possible security flaws in the portal is white hat hacking, often referred to as ethical hacking [4].

The practice of safeguarding data and information systems against unwanted access, use, disclosure, interruption, alteration, or destruction is known as information security. The method, guidelines, and precepts used to protect electronic data and other forms of information are collectively referred to as information security. A vital aspect of computer and network security is safeguarding data from unauthorized access, use, disclosure, interruption, modification, or destruction [5]. This involves guarding against unwanted access to systems and networks as well as safeguarding data from physical and digital dangers. In order to avoid data breaches and cyberattacks, information security measures might include both non-technical ones like staff training and policy, as well as technological ones like firewalls and encryption. Preventing data breaches and cyberattacks, as well as guaranteeing the confidentiality, integrity, and availability of information and information systems, are the primary goals of information security [6].

Every firm has robust information security policies that address availability, confidentiality, and integrity. Every data leak, however, serves as a reminder that these standards may not be perfect for ensuring the organization's security on their own. University admission portals are protected by penetration testing, which finds hidden entrances before hackers do by employing methods similar to those of the invaders and then closes those doors with a repair plan. Higher education institutions must have faith in the efficacy of their defenses against intruders. Penetration testing is a useful technique for evaluating how well security measures hold up against an assault. One type of stress testing used to find vulnerabilities and determine security robustness is penetration testing, sometimes known as white hat hacking.

Gaining unauthorized access to a computer system or network is known as hacking. Its goal is to either damage the system or steal important information from it [7]. The use of a computer by an individual (hacker) is known as hacking. The hacker is adept at stealing data from other systems because they have a solid understanding of technology. Finding potential points of entry into any computer system or network in order to breach it is the main goal of hacking. A computer expert who engages in hacking is known as an ethical hacker [8]. Ethical hackers use their expertise to understand how systems are setup, function, and occasionally even test their security [9].

The admissions process at the university is a delicate and important procedure that needs the highest level of security and integrity. The university's admission system is susceptible to data breaches and cyberattacks due to the growing use of technology in the admissions process. Therefore, it is necessary to use penetration tools to evaluate the vulnerabilities of university admission portals.

The purpose of this study is to use a penetration tool to identify the university admission system's vulnerability. Its specific goals are to: find security flaws in the current admission system using a pen testing tool (Network Mapper (Nmap), SQL Map); evaluate how well pen testing tools identify security flaws in the admission system; suggest security fixes and safeguard the admission system against data breaches and cyberattacks.

A. *Penetration testing's significance*

1. Finding Vulnerabilities: Penetration testing assists in locating potential weaknesses in the admissions system, such as misconfigured settings, unpatched software, or weak passwords. Finding these flaws before hackers take advantage of them is crucial to fixing them quickly.
2. Preventing Data Breaches: Universities may enhance the security of sensitive student data, such as academic records and personally identifiable information (PII), by conducting proactive system testing. By doing this, data breaches that can result in financial fraud or identity theft are less likely to occur.
3. Maintaining Reputation: A university's reputation can be seriously harmed by a successful hack on its admissions system. Universities may preserve their reputation and show their dedication to data security by carrying out penetration testing.
4. Upholding Compliance: Institutions of higher learning frequently manage student data in accordance with a number of privacy laws. Penetration testing aids in guaranteeing adherence to laws like the Family Educational Rights and Privacy Act (FERPA) and the General Data Protection Regulation (GDPR).

Adhering to industry best practices is necessary for putting in place a successful penetration testing program. Here are some crucial actions to think about:

a. Careful Planning: Specify the testing's parameters and the essential elements of the admissions process that will be looked at. For the process to be as successful as possible, set goals, deadlines, and test settings. Hire Qualified Experts: Employ ethical hackers with certification and expertise who have the know-how to carry out successful penetration testing. These experts will use their knowledge while abiding by moral principles.
b. Thorough Vulnerability Assessment: To find flaws in the system, including network infrastructure, online apps, and particular software used in the admissions process, identify potential vulnerabilities and conduct thorough testing. Utilize and Report Results: To take use of vulnerabilities they have found, penetration testers should model actual assaults. After an exploit is effective, thorough reports that include the actions done, the possible consequences, and remedial suggestions should be sent.
c. Remediation Planning and Execution: Rank the vulnerabilities in the reports and develop a strategy for taking corrective action. To improve the admissions system's security posture, it is imperative that the vulnerabilities found be fixed as soon as possible.
d. Frequent Testing and Continuous Improvement: Regular penetration testing is crucial since cybersecurity threats are ever-evolving. Regular evaluations provide continued protection and enable the security architecture to be continuously improved.

B. *Benefits of Penetration Testing Beyond Data Protection*

Although the main goal of security penetration testing is data protection, its advantages go beyond protecting private data. Let's examine a few of the main benefits that colleges might obtain from including frequent security penetration testing into their admissions procedures:

1. Regulatory Compliance: Universities can guarantee adherence to pertinent data protection laws, such as the Family Educational Rights and Privacy Act (FERPA) in the US, by carrying out penetration testing. In addition to protecting applicants' privacy, complying with these regulations also protects the institution from any fines and legal ramifications.
2. Reputation management: Higher institutions are trusted with the personal information of applicants, and any data breach might have serious repercussions and damage the school's standing. Frequent security penetration testing keeps the university's reputation intact and shows potential students that it is committed to data protection.
3. Improved Incident Response: Universities may improve their incident response skills by using penetration testing to find weaknesses. Institutions may reduce the impact of security events and guarantee a prompt and efficient reaction in the event of a breach by developing and improving response plans based on an understanding of probable attack vectors.

II. Literature Review

In order to determine which tools may be used to detect likely vulnerabilities on a system, [10] carried out research to do penetration testing and vulnerability assessment on Metasploitable. The goals were to simulate an attack on the Metasploitable computer, discover existing vulnerabilities in the target system, outline the best practices and tools for penetration testing on Metasploitable machines, document the findings, and offer suggestions. The TCP SYN scan was the technique utilized, while the Open-Source Vulnerability Database (OSVDB) and Common flaws and Exposures (CVE) were employed to find the services' flaws. Finally, the target machine's vulnerabilities are examined using the vulnerability scanner OpenVAS on Kali Linux. The machine was found to be insecure, according to the results; there were several open ports that may allow hackers to access the system. The services that were operational are fragile and out-of-date. It was determined that the operating system required an upgrade since it was out of date. A number of ports, including port 512, provide the hacker remote access to the machine.

The absence of updating services results in several vulnerabilities. It is vital to update the services and close the required ports in order to have a secure system. More study on the same subject utilizing more pen testing methods is required.

Conducted research on Penetration Testing Procedures and Instruments [11]. The research evaluated a few scanning technologies based on how many ports they found and how long it took them to find them. Additionally, it examined the many kinds, procedures, and models of penetration testing. The research methodology used in this study was quantitative. Researchgate.net, ieee xplore.org, learning.oreilly.com, Google Scholar, and the ACM Digital Library were among the resources used. According to the survey, Sparta was the most effective and user-friendly scanning tool evaluated. Sparta was suggested because it is a free application that is perfect for small firms (less than 10 employees) and is accessible in Kali Linux (though some lite versions of Kali Linux may need to be downloaded). Larger companies with more intricate systems, however, could need a program that can scan a variety of IP addresses. For these companies, Nmap is more advised. Since each step of penetration testing is carried out using the right tools, a tool's reliability is its most crucial feature. The goal of the experiment was to compare the efficacy of four distinct port scanning techniques on a particular target. Larger companies with more intricate systems, however, could need a program that can scan a variety of IP addresses.

In order to demonstrate free and open-source tools and methodologies to mimic a potential attack that network and system administrators may employ against their network or system, [12] carried out study targeted at finding and elucidating an appropriate approach behind the penetration testing. The primary goals were to look into penetration testing security methods and tools, the appropriate approach for penetration testing, and how administrators of networks and systems can use the penetration test and its approach to comprehend harmful and protective security toward the mentality of an intruder and effectively and efficiently protect the system or network. Given the unstable nature of the penetration test, considerations of law, ethics, budget, and time were made all through the testing process. Free/Open-Source Software (F/OSS) and its methods were the methodology used. The study's findings demonstrated that hosts on the lab network were susceptible to remote code execution, buffer overflow, elevation of privilege, denial of service, spoofing, and information leakage, according to both Nessus and OpenVAS.

According to the study, automated vulnerability assessment tools provided a good baseline for examining the local security of systems, workstations, and infrastructure, despite their noise and potential for false positives and false negatives, which prevented them from always displaying the true security posture of the entire system or network. Additionally, they assisted in locating security settings that are not in compliance and unpatched apps [12]. As a result, any toolkit for network and system administrators or penetration testers should include automated scanners. When set up correctly and efficiently, these scanners may be a useful tool for IT security. Other scanners, such as Nexpose, Retina, or Internet Security Systems, can also be utilized during the Scanning and Vulnerability Assessment phase, however Nessus and OpenVAS were the two chosen for the research. Based only on the quantity of vulnerabilities found, it was challenging to determine whether scanner was more effective or efficient. In order to be effective, the present penetration testing technique must include social engineering methods and tools.

Compared the industry-known OWASP Benchmark for vulnerabilities with the automated online penetration testing techniques of today [13]. The approach used was to compare scanners for online application penetration testing and assess a few chosen web application security scanners. According to the study, point-and-shoot scanners are not as effective as scanners with web proxy and customized crawling. Additionally, the performance of scanners with an active maintenance life cycle was shown to be superior. The study concluded that using several automated scanning technologies to automate scanning was a good idea.

One research was conducted by [14]. In order to make it easier for penetration testers to choose the best tools for their purposes, this study suggests an empirical comparison of pen-testing tools for identifying web app vulnerabilities using accepted standards and methodologies. The quantitative approach was the methodology used. A comparison analysis based on scores was used to assess the tool's capabilities based on the study. Both profit and non-profit pen-testing tools were put through simulation tests. Among the commercial products, Burp Suite Professional had the highest score, while OWASP ZAP came out on top among the non-profit options, according to the data. It is necessary to apply the benchmarking method to further new tools and expand the framework to include more new measures. Only a few tools were measured.

[15] The study's objectives were to illustrate intrusions and assaults on the network architecture and investigate the application of penetration testing in evaluating Central University College's network infrastructure. The study's main goals were to do a penetration test to ascertain how resilient Central University's systems and network infrastructure are to network-based attacks and to potentially aid with network and system security. A quantitative approach was used as the methodology. According to the report, penetration testing might help systems and network administrators strengthen the security of their network architecture provided it is carried out methodically. The study's findings indicated that Nessus had a greater vulnerability detection rate than OpenVAS at both the exterior and internal test locations. The OpenVAS's reduced plug-in count may be the cause of this finding. Finding a trustworthy and standard metric to compare the performance of the scanners was vital since higher detection rates were not a valid way to assess their efficacy because detection might be impacted by false positive and false negative detection. Since the two scanners ranked the vulnerabilities using different criteria, it was a little difficult to tell if they were referring to the same vulnerability or a different one. Considering that Nessus has twice as many plug-ins than OpenVAS, OpenVAS's performance was adequate. As a continuation of the presented work, the research suggested, among other

things, that work be done on automating the whole suggested penetration testing technique to provide a comprehensive security testing solution. The research project examined Central University's network infrastructure's vulnerability assessment and penetration testing. The study did not take social engineering or human considerations into account.

III. Methodology

For this design, the Penetration Testing (Pen-Testing) approach was used. This approach consists of six stages: reconnaissance, scanning, vulnerability analysis, documentation of discovery, risk assessment, and remedy suggestions.

i. Reconnaissance Phase: During this first stage, basic data on the suggested system was acquired in order to comprehend its composition, operation, and susceptibility to outside dangers. To find publicly accessible information, such as domain names, IP addresses, subdomains, and system technologies in use, passive reconnaissance techniques like open-source intelligence (OSINT) were used. This made it possible to get useful intelligence without engaging with the system directly in a way that may be noticed or interfere with operations.

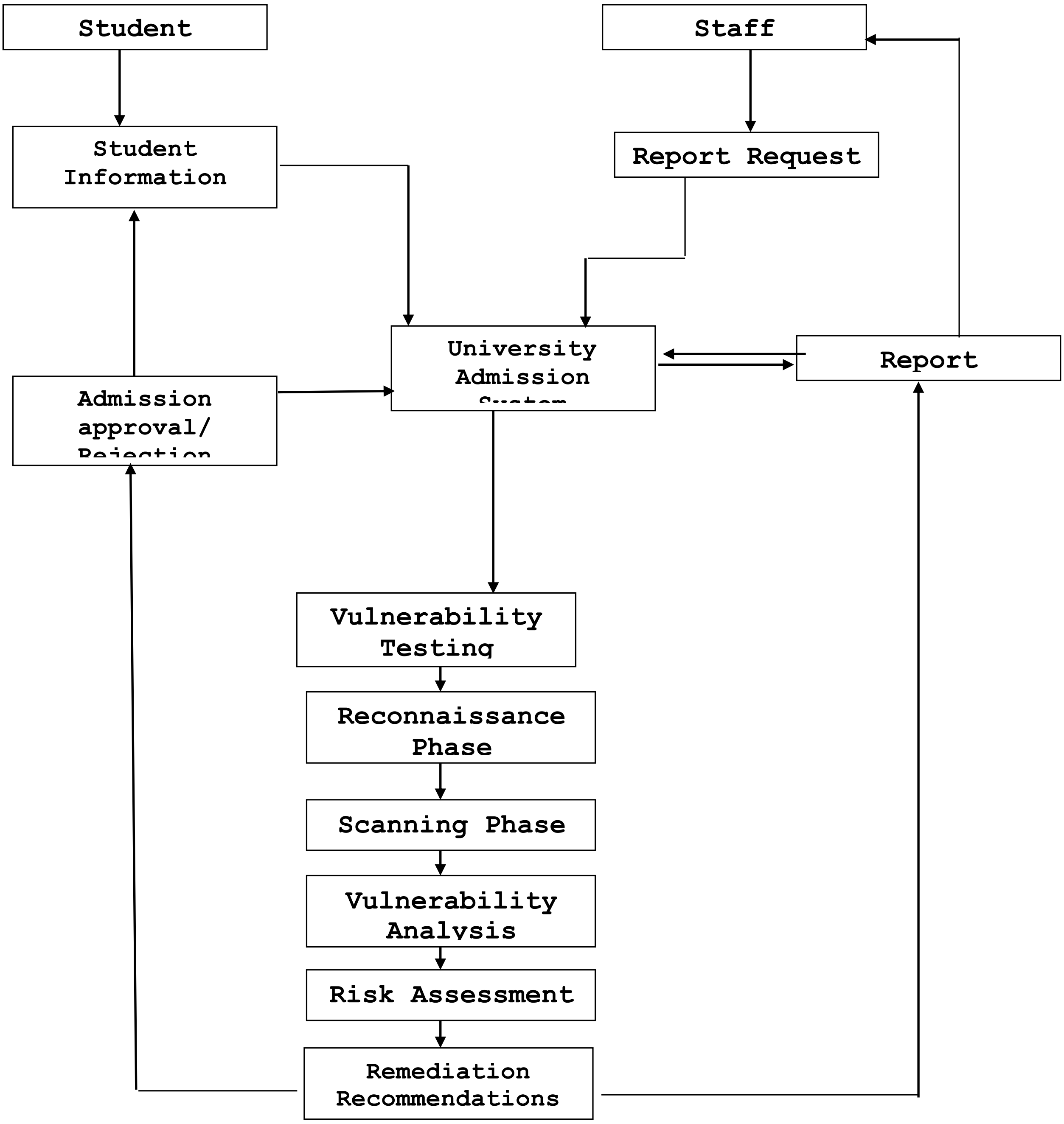

Figure 1: information flow diagram of the penetration Testing

ii. Scanning Phase: The system's network infrastructure was actively scanned during this phase using Nmap (Network Mapper). This was carried out in order to identify running services, find open ports, and list the operating systems and versions that were being used. The system's attack surface map was made possible by the information gathered during this phase. Various scanning methods, including version detection and TCP SYN scans, were employed to uncover potentially dangerous concealed services and configuration errors.

iii. Vulnerability Analysis: During this stage, the system's operational components were examined for known vulnerabilities. To match discovered services and software versions with vulnerabilities that have been made public, tools including vulnerability scanners, CVE databases, and Nmap scripting engine (NSE) scripts were utilized. Additionally, the research involved looking for vulnerable interfaces, out-of-date software, and weak setups that an attacker may exploit.

iv. Documentation of discovery: In this step, every discovery from the reconnaissance, scanning, and vulnerability analysis stages was recorded. This included thorough explanations of every vulnerability that was found, along with information on the impacted components, risk levels, and possible system effect. To bolster the validity and repeatability of the evaluation results, screenshots, logs, and tool outputs were also provided.

v. Risk Assessment: During this stage, a risk assessment procedure was used to rank the vulnerabilities according to their seriousness and possible influence on the system. Exploitation, data sensitivity, accessibility levels, and commercial effect were among the factors taken into account. To assist stakeholders in making well-informed decisions, each vulnerability was graded using a defined risk scoring approach, like the Common Vulnerability Scoring approach (CVSS).

vi. Remedial Recommendations: At this stage, specific remediation plans were put out for every vulnerability that was found. These suggestions included updating out-of-date software, resetting network or application settings, installing intrusion detection systems and firewalls, and applying security updates. To guarantee ongoing system security, both short-term mitigating techniques and long-term preventative actions were recommended when suitable.

VI. Mitigation Strategies

Measures done to lessen the likelihood and severity of possible vulnerabilities in the future are referred to as mitigation techniques. Among the mitigation techniques are:

1. Performing routine penetration tests.
2. Security best practices training for staff members.
3. Regular system updates and patches.
4. Reduce harm by putting security controls and safeguards in place, such intrusion detection systems.

VII. Conclusion

This study used ethical hacking techniques and penetration testing tools including Nmap, SQLMap, and Burp Suite Community Edition to examine the security posture of a university enrollment portal. As higher schools increasingly rely on web-based systems to manage admissions and handle sensitive student data, it is imperative that these systems be sufficiently secured against cyberattacks. According to our research, penetration testing is a crucial preventative measure for spotting security flaws before malevolent intruders may take advantage of them. The study's results showed that university enrollment websites are vulnerable to a number of security risks, such as exposed services, unpatched software, improperly configured systems, shoddy authentication procedures, and possible SQL injection flaws. Several risk indicators were identified through the use of automated and human penetration testing methods, highlighting the necessity of ongoing system security monitoring and enhancements. The study makes it clear that ethical hacking is essential for identifying vulnerabilities and for bolstering information systems through ongoing testing and repair techniques. The three main tenets of information security—confidentiality, integrity, and availability—should be respected by a secure admittance system. Universities may protect application data, maintain confidence, and preserve institutional integrity by establishing remedial steps and integrating frequent vulnerability assessments.

References

[1] McGraw, G. (2006). Software Security: Building Security In, Adison Wesley Professional.

[2] Kim, P. (2014). The Hacker Playbook: Practical Guide to Penetration Testing. ISBN: 1494932636.

[3] OWASP Top 10:2021. (2021). Available online: https://owasp.org/Top10/ (accessed on 14 January 2025).

[4] Penetration Testing Execution Standard (PTES) (2017). Retrieved from https://www.penetrationtesting.com accessed 21st January, 2025.

[5] Abdalla, P.A. & Varol, C. (2020) 'Testing IoT Security: The Case Study of an IP Camera', IEEE. Available at: https://ieeexplore.ieee.org/document/9116392 Doi: 10.1109/ISDFS49300.2020.9116392.

[6] Kong, C.T. and Yiu, S.M. (2021) 'Hacking CCTV by changing time', IEEE. Available at: https://ieeexplore.ieee.org/document/9514241 doi:10.1109/ICECCE52056.2021.9514241.

[7] Trabelsi, Z., McCoey, M. (2017). Ethical Hacking in Information Security Curricula. *International Journal of Information and Communication Technology Education,* 12(1):1-10.

[8] Wang, Y. and Yang, J. (2017). [IEEE 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) - Taipei, Taiwan (2017.3.27-2017.3.29)] 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA) - Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool., (), 110-113. doi:10.1109/WAINA.2017.39.

[9] Prabhat, K.S. and Biswamohan, A. (2020). A Review Paper on Ethical Hacking. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(12):163-168.

[10] Iman, S.A. (2022) C Vulnerability Assessment and Penetration Testing of Web Application. Vaasan Ammattikorkeakoulu, *University of Applied Sciences, Information Technology*, 1-43.

[11] Sushmitha, M. R. (2021). "A Study of Penetration Testing Processes and Tools" (2021). Electronic Theses, Projects, and Dissertations. 1220. https://scholarworks.lib.csusb.edu/etd/1220

[12] Nishant, S. (2012). Security Assessment via Penetration Testing: A Network and System Administrator's Approach. Master's Thesis. University of Isolo. Department of Informatics, 1-98.

[13] Mandar, P.S. (2019) carried out research on comparative analysis of the automated penetration testing tool. School of Computing, National College of Ireland.

[14] Marwan, A., Dhoha, A. and Anca, J. (2022). An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. School of Computer Science, Umm Al-Qura University, Mecca P.O. Box 715, Saudi Arabia School of Computer Science, University College Dublin, Belfield, D04 V1W8 Dublin, Ireland.

[15] Joel, K.A. (2014). Network and Systems Security Assessment using penetration testing in a university environment: The case of Central University College. Kwame Nkrumah University of Science and Technology. School of Graduate Studies, Kumasi Ghana.