Wadi AlShatti University Journal of
Pure and Applied Science

مجلة جامعة وادي الشاطئ
للعلوم البحتة والتطبيقية

Volume 3, No. 1, January-June 2025 Online ISSN: 3006-0877 المجلد 3، الاصدار 1، يناير- يونيو 2025

COMPUTER SCIENCES

Security Assessment of Some Libyan Banks Websites

Rabia Masoud [1,*], Alsanossi Ahmed [2], Maher Alghali [3]

[1] Electrical and Electronic Eng. Dept., Faculty of Engineering, Wadi Alshatti University, Brack, Libya
[2] Computer Science Dept., Faculty of Sciences. Wadi Alshatti University, Brack, Libya
[3] Network Dept, Information Technology Faculty, Sebha University, Sebha, Libya

ARTICLE HISTORY

Received 23 October 2024
Revised 09 November 2024
Accepted 12 November 2024
Online 03 January 2025

KEYWORDS

E-bank;
Libyan Bank Website;
Cybersecurity;
Vulnerability;

ABSTRACT

In contemporary times, cybersecurity has become a major concern due to a significant rise in security threats, specifically hacker attacks on websites in the digital world. Given the website's broad accessibility, the security level of the site should always be upheld. The aim of this study is to evaluate and identify vulnerabilities in the websites of Libyan banks, and provide suggestions to the entities with weak links (vulnerabilities) in their web applications. The Nessus tool was utilized to evaluate the security vulnerabilities of several banking websites in Libya to determine their level of web security. This study discovered several vulnerabilities at high, medium, and low levels on e-bank websites, making them unsecure for customers to trust their private data into their care. This research notifies the electronic banking sector about these security vulnerabilities and the immediate requirement to address them. Some suggestions have been proposed to help address these security weaknesses. These suggestions have provided the best results. A diligent application of these methods in addressing the vulnerabilities would provide a more secure and less vulnerable e-banking websites for users. The recommended precautions could help protect both banks and their customers, as well as decrease cyber threats while using the website.

التقييم الأمني للمو اقع الالكترونية لبعض المصارف الليبية

ربيع احمودة مسعود [1،*]، السنوسي محمد احمد [2]، ماهر عبدالله الغالي [3]

الملخص

في العصر الحديث، أصبح الأمن السيبراني مصدر قلق رائد بسبب الارتفاع الكبير في التهديدات الأمنية، و قرصنة المواقع الإلكترونية في العالم الرقمي. نظراً لسهولة الوصول إلى الموقع الإلكتروني، فيجب الحفاظ دائماً على مستوى عالي من الحماية. تهدف هذه الدراسة إلى تقييم وتحديد نقاط الضعف والثغرات الامنية في مواقع البنوك الليبية، وتقديم توصيات للتقليل من الثغرات الامنية في تطبيقات الويب الخاصة بها. تم استخدام أداة Nessus لإجراء تقييم شامل للثغرات الأمنية المحتملة لبعض من المواقع الإلكترونية المصرفية في ليبيا. أظهرت نتائج الدراسة وجود العديد من الثغرات الامنية على المستويات العالية والمتوسطة والمنخفضة تحتويها مواقع البنوك الإلكترونية، مما يجعلها عرضة للاختراق وسرقة بيانات العملاء لديها. ينبه هذا البحث قطاع الخدمات المصرفية الإلكترونية بهذه الثغرات الأمنية والمتطلبات الفورية لمعالجتها. حيث يقدم بعض التوصيات من اجل معالجة نقاط الضعف والثغرات الامنية التي تحتويها هذه المواقع. إن التطبيق المستمر لهذه الأساليب في معالجة نقاط الضعف من شأنه أن يوفر مواقع ويب مصرفية إلكترونية أكثر أمانًا وأقل ضعفًا للمستخدمين. ويمكن أن تساعد هذه التوصيات في حماية البنوك وعملائها، فضلاً عن تقليل التهديدات الامنية أثناء استخدام الموقع الإلكتروني

الكلمات المفتاحية:

البنك الالكتروني
موقع ويب
الأمن السيبراني
الثغرات الامنية

Introduction

The advances in information and communication technology (ICT) has enabled numerous electronic services to become possible. This revolution is not just transforming people's daily lives, but also altering the dynamics of relationships between businesses and customers. These transformations are quickly evolving into a new type of banks known as electronic banks (e-banking). In fact, many organizations have embraced this new technology to improve the quality and efficiency of customer service, while also reduce costs in comparison to the traditional approach [1]. Electronic banking is a cost-effective method to carry out banking transactions, share information, and purchase or sell goods or services from any location at any time. Additionally, it serves as a method to retain current clients and draw in new ones to the bank [2].

E-banking enables customers, whether they are individuals or businesses, to access accounts, conduct transactions, or obtain information on financial products and services through a

Corresponding author: r.masoud@wau.edu.ly
https://doi.org/

public or private network, including the internet [3]. E-banking offers essential services like checking account balances, paying bills, transferring funds, requesting credit card advances, and ordering checks for quicker service. Hence, it is clear that e-banking significantly enhances the efficiency and convenience of banking operations and services for customers. Customers can make transactions from one corner of the country to the other without having to physically touch anything[4].

Though e-banking offers various advantages, the increasing of distance between banks and customers could result in security worries and a loss of trust. In recent years, there has been a consistent increase in the amount of attacks targeting weaknesses in electronic banking systems [2]. Researchers focused on the security and privacy of electronic banking services, as they have a significant impact on business performance and customer satisfaction. Banks that provide online access to their banking systems need to create strong security protocols to ensure secure and authenticated communication over unsecured channels [5]. The solutions mentioned in literature, which are discussed in this paper, are either ineffective or insufficient. In order to propose security solutions, one must first comprehend and categorize the current challenges, risks, and methods of attack associated with e-banking. Moreover, it is necessary to evaluate current strategies in order to identify benefits and weaknesses [6].

The process of vulnerability assessment involves defining, identifying, and classifying security gaps (vulnerabilities) on computers, networks, or communication infrastructure.[7]. Furthermore, vulnerability analysis can assess how effective preventive actions are before and after implementation. The findings from a vulnerability assessment can be utilized to assess the security level of the website. This level of maturity can be utilized to assess how well security controls have been implemented on the website, allowing for actions to address threats resulting from security weaknesses [8].

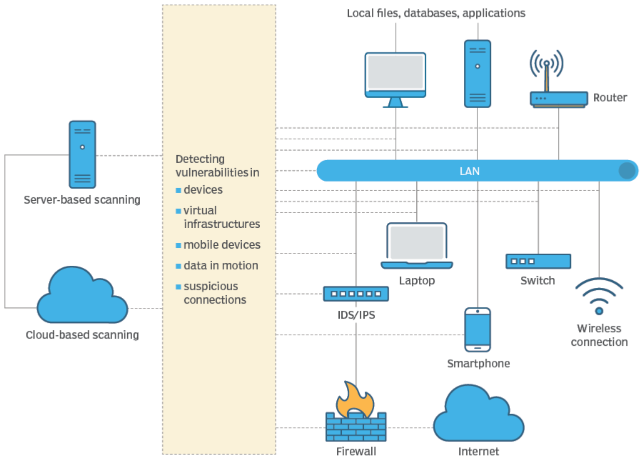


Fig1: How a vulnerability scan works

Conducting a vulnerability assessment is a method to enhance an organization's cybersecurity. Through vulnerability assessment, organizations can identify system vulnerabilities and address them appropriately to mitigate any potential risks. [9]. In this research, we employed vulnerability assessment techniques to pinpoint vulnerabilities in the websites of Libyan banks. We used the Nessus tool to identify vulnerabilities within the websites. The study results will offer crucial insights to banks regarding weaknesses on their website, enabling them to take necessary steps to address them.

Literature Review

Currently, as technology advances, agencies and organizations are in competition to develop websites for their agencies [10]. Recently, human work has become easier with the existence of a website. Siteefy website reports that there are 1,079,154,539 websites globally as of August 2024, with 192,375,760 of them being active. There is a constant daily increase of around 252,000 websites worldwide, equivalent to about 3 new websites per second [11]. Web developers face a challenge in maintaining security due to the rising usage of the web. This is because it fails to eliminate the potential for hacking that could disrupt.

Websites lacking proper security measures when connected to the internet may face attacks aimed at stealing, altering, or disrupting the services and information on the website [12]. Users can share and manipulate information using different platforms through web-based applications [13]. Ignoring a vulnerability in a computer network system can lead to severe consequences in the event of a threat or harmful attack on the system. Given the risks and drawbacks of improperly using services on local networks and internet applications, it is crucial for businesses and organizations to adopt initial measures to reduce them. Analyzing a website's vulnerability is essential. Various technologies and practices are now being implemented under the cybersecurity concept to ensure the security of computer systems and user data, specifically because of the different activities conducted by individuals through internet-based electronic networks. One of the biggest threats to cybersecurity is the cyber-attacks conducted by criminals in order to gain financial benefits by stealing data from individuals or organizations [14].

Electronic banking channels are less secure than traditional face-to-face banking operations. In the case of online banking, all data being stored on the internet increases the risk of a hacker potentially gaining unauthorized access to account information. Hence, information is vulnerable to being lost, changed, or denied. Attacks on e-banking can come from both inside and outside sources [15]. Bank employees, who are knowledgeable about the system and its vulnerabilities, can carry out intrusions. There has been a significant rise in the quantity of documented vulnerabilities in web applications. Most vulnerabilities stem from inadequate validation of input [16]. Information security must be prioritized in all sectors. It is a matter that affects both individuals and all types of organizations [17]. This is especially crucial in the finance industry, due to the significant financial sums at stake and the confidential information of both clients and organizations. Organizations conduct penetration testing to evaluate security in infrastructures, networks, web applications, and other assets by emulating an attacker's actions to uncover weaknesses. [18] research focus on analyzing security audit results of multiple financial web applications from a single institution using automated tools to evaluate their security levels. [19] research aims to examine different methods and forms of attacks commonly carried out on websites on the internet. It has been found that certain vulnerabilities and security breaches are present on a website. This study utilized both htaccess method and website script to enhance security. However, despite the enhancements made, the website cannot be guaranteed 100% secure, as data security encompasses not only fixing issues on the web and server side, but also considering network security.

Researchers in a study by [20] focused on carrying out tests to identify security vulnerabilities in the University of Muhammadiyah Purwokerto's scientific journal website through the utilization of OpenVAS and Acunetix WVS tools. The outcome of this research reveals that. OpenVAS identified 9 data gaps, whereas Acunetix WVS detected 166 data gaps. Furthermore, [21], conducted additional research with the goal of identifying, explaining, evaluating, and addressing vulnerabilities at ABC University using the Common Vulnerability Scoring System. Low, moderate, high, and critical vulnerabilities were identified in the vulnerability scan results.

In addition, a study carried out by [22] tested the security of the OJS website with VA, utilizing the OWASP. The tests conducted have found 70 high vulnerabilities, 1929 medium vulnerabilities, and 4050 low vulnerabilities in OJS. A total of 6049 was the vulnerability value tested in OJS. [23] demonstrated that Nessus can identify vulnerabilities more quickly compared to Netclarity. Moreover, according to [24], Nessus operates quicker than Retina when the Web App feature is disabled, but it slows down significantly compared to Retina when the Web App module is enabled. When it comes to scan depth, Nessus has a slight edge because it comes with a highly useful web mirroring tool in HTTP. Both studies found that Nessus speeds up the scanning process. According to [12] Vulnerability analysis is a procedure that outlines, identifies, categorizes security vulnerabilities in computers, networks, or communication infrastructure. Researchers are interested in assessing the maturity of campus websites by utilizing Nessus.

Web developers are facing difficulties in ensuring security due to the growing utilization of the internet. This is due to the fact that it does not dismiss the chance of hacking that could disrupt [22]. An IT system vulnerability is a possible flaw in the system that, if taken advantage of, can lead to the system being targeted for attack. These attacks can have harmful impacts, like theft and data leaks, spreading false information, altering systems, and causing system paralysis. In order to predict this, web developers must carry out vulnerability assessments. The importance of vulnerability assessment is often overlooked, viewed merely as a procedural task that is seldom implemented [25, 26]. Vulnerability assessment involves determining, recognizing, categorizing, and ranking vulnerabilities within web systems. Specific tools or software can detect weaknesses in the network. Methods for vulnerability assessment can assist in identifying vulnerabilities present on the internet. The evaluation outcome is utilized by developers and network administrators to make proactive choices and assess survivability during a security breach [27].

Research Methods

The research methodology employed is the constructive research method, aimed at evaluating the security vulnerabilities of bank websites through testing and gathering responses from web security vulnerability assessments. Four bank websites in Libya, including two private and two public banks, underwent vulnerability testing in September 2024. The discovery of weaknesses in websites is known as vulnerability analysis. Nessus tool is utilized for conducting vulnerability analysis to automatically detect vulnerabilities in websites. The reason for utilizing this tool is to identify every potential vulnerability in Libyan bank websites.

Nessus, developed by Tenable.sc, is available for use through a subscription or the free version. [28]. Nessus performs quick, thorough scans to detect vulnerabilities before attackers can exploit them. The solution follows a risk-oriented method to recognize and evaluate vulnerabilities [29, 30]. Consequently, it assigns threat levels to each discovered vulnerability depending on the severity of the threat to your system's security. Nessus, a widely-used vulnerability scanner, aids organizations by auditing their network to identify weaknesses as a security scanner [31].

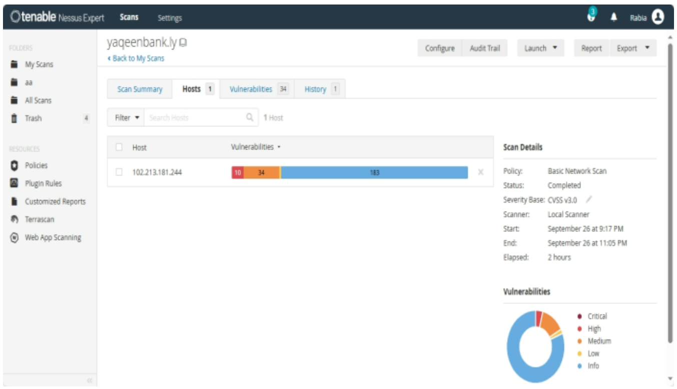
Tenable calculates a fluctuating Vulnerability Priority Rating (VPR) for the majority of vulnerabilities. The Vulnerability Priority Rating (VPR) is an ever-changing complement to the vulnerability's CVSS score, as Tenable continually adjusts the VPR to accurately represent the current threat environment. VPR values range from 0.1 and 10.0, with a greater value indicating a greater potential for exploitation table 1 [28].

Table1: Vulnerability Priority Rating.

VPR Category	**VPR Range**
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1to 3.9

Result and Analysis

Nessus will audit or assess the targeted website, by scanning the website and then determining the weaknesses of the Libyan bank websites. Among the 4 websites there are security holes, we found that the most vulnerabilities are Alejma'a Alarabi Bank, the vulnerability at the high level were 10 (according to the severity base, uses VPR Category the range is in the range of 7.0 to 8.9), at the medium level 34 (according to the severity base, uses VPR Category the range is in the range of 4.0 to 6.9), and low level were1(according to the severity base, uses VPR Category the range is in the range of 0.1 to 3.9) Figure 1.



yaqeenbank.ly
‹ Back to My Scans

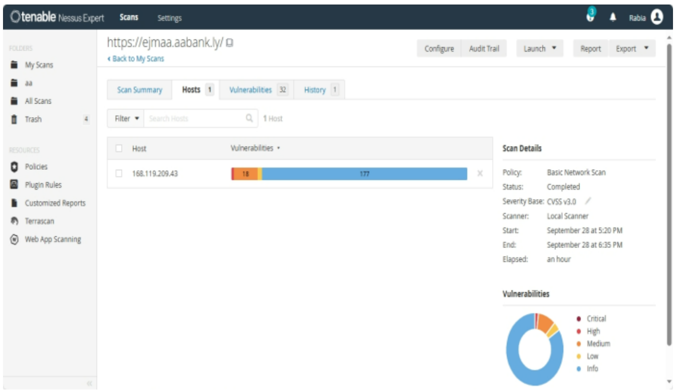
Host	Vulnerabilities
102.213.181.244	10 34 183

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 26 at 9:17 PM
End: September 26 at 11:05 PM
Elapsed: 2 hours

Fig. 2: The results of the scan capture with Nessus on Alejma'a Alarabi Bank

The vulnerability of Yaqeen Bank website was at the high level were 2 (according to the severity base, uses VPR Category the range is in the range of 7.0 to 8.9), at the medium level 18 (according to the severity base, uses VPR Category the range is in the range of 4.0 to 6.9), and low level 3 (according to the severity base, uses VPR Category the range is in the range of 0.1 to 3.9) Figure 2.



https://ejmaa.aabank.ly/

Host	Vulnerabilities
168.119.209.43	18 177

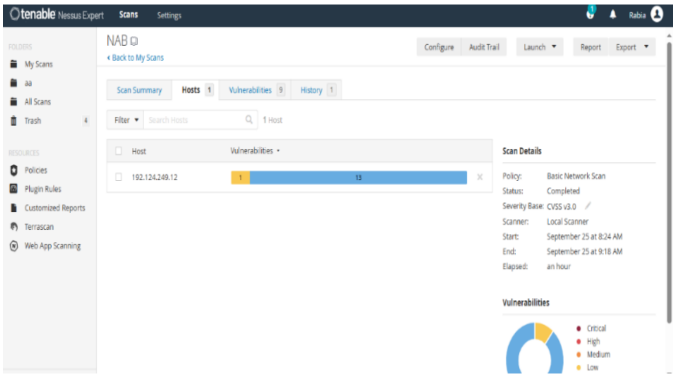
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 28 at 5:20 PM
End: September 28 at 6:35 PM
Elapsed: an hour

Vulnerabilities

Fig. 3: The results of the scan capture with Nessus on Yaqeen Bank website

The Nessus Scanner result of North African Bank website has only one low level vulnerability (according to the severity base, uses VPR Category the range is in the range of 0.1 to 3.9) Figure 3.



NAB

Host	Vulnerabilities
192.124.249.12	1 13

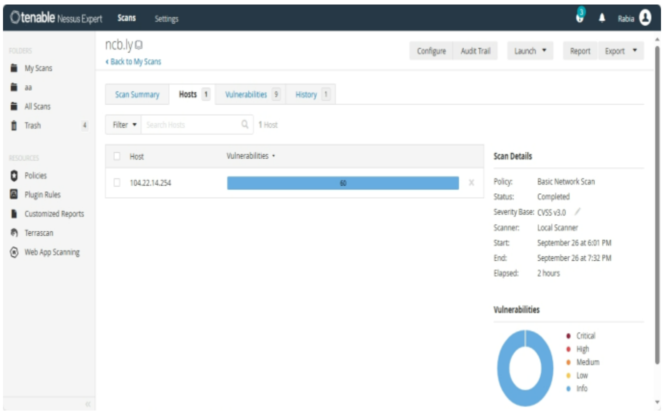
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 25 at 8:24 AM
End: September 25 at 9:18 AM
Elapsed: an hour

Vulnerabilities

Fig. 4: The results of the scan capture with Nessus on North African Bank website.

Finally, the resulted that the National Commercial Bank website don’t have vulnerabilities at any level Figure 4.



ncb.ly

Host	Vulnerabilities
104.22.14.254	60

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: September 26 at 6:01 PM
End: September 26 at 7:32 PM
Elapsed: 2 hours

Vulnerabilities

Fig. 5: The results of the scan capture with Nessus on the National Commercial Bank website

The findings presented in Table2 indicate that Alejma’a Alarabi Bank exhibited the most vulnerabilities of high severity level. The results clearly indicate that Libyan private bank websites face significantly higher risks when compared to public bank websites, as shown by Nessus.

Table 2: Scanning Results Using Nessus.

	Name of the Website	**Type of bank**	**Total number of severity risks**			
			Critical	**high**	**medium**	**low**
1	Alejma’a Alarabi Bank	Private	-	10	34	1
2	Yaqeen Bank	Private	-	2	18	3
3	North African Bank	Public	-	-	-	1
4	National Commercial Bank	Public	-	-	-	-

Conclusion

Testing the website's vulnerability will reveal various weaknesses present on the site. These vulnerabilities could potentially endanger the security of the assets belonging to the organization in control of the website. Using tools from open source allows for automated vulnerability tests to be conducted on different operating systems. From the results of testing the Libyan banks website by scanning it using a software called Nessus, we found several vulnerabilities from each website with different vulnerability levels. Alejma’a Alarabi Bank website were having the most vulnerabilities; it was in high severity level. And the vulnerability at the medium level is on Yaqeen Bank website, the two banks are a privet banks. Meanwhile, the resulted showed that the public banks were have less vulnerabilities.

The results mainly relate to accessible ports, as well as configurations and features. The vulnerabilities must be addressed promptly by the website administrator. Firewalls on the network should be set up to restrict access to open ports, along with implementing intrusion detection systems and network segmentation. Web developers need to deactivate unnecessary features, set them up properly, and install required patch updates. Finally, we conclude the article on a positive note, expressing optimism that it will catch the attention of relevant authorities. We encourage them to regularly assess the vulnerability of encryption techniques and make necessary corrections as needed. This could assist banks in enhancing security which would in turn boost the trust of customers (end-users) and improve acceptability, a goal desired by banks. Additionally, we hope that the recommendations provided by a cryptographer will be implemented by banks soon, aiding them in avoiding numerous attacks.

Author Contributions: “All authors have made a substantial, direct, and intellectual contribution to the work and approved it for publication.”

Funding: “This research received no external funding.”

Data Availability Statement: “The data are available at request.”

Acknowledgments: "The authors would like to express their appreciation to all persons and organizations who contributed to the publication of this research paper. We would also like to thank our colleagues at Waddi Alshatti University for their comments and support throughout the research process. Therefore, we would like to thank them for their valuable opinions and suggestions".

Conflicts of Interest: “The author declares no conflict of interest.”

References

[1] R. Ihmouda, N. H. M. Alwi, and I. Abdullah, "*A systematic review on e-government security spects*," vol. 3, no. 6, pp. 60-7, 2014.

[2] B. Chaimaa, E. Najib, and H. J. W. P. C. Rachid, "*E-banking overview: concepts, challenges and solutions*," vol. 117, pp. 1059-1078, 2021.

[3] G. Mogos, N. S. M. J. I. J. o. E. E. Jamail, and C. Science, "*Study on security risks of e-banking system*," vol. 21, no. 2, pp. 1065-1072, 2021.

[4] H. Alzoubi, M. Alshurideh, B. A. Kurdi, K. Alhyasat, T. J. I. J. o. D. Ghazal, and N. Science, "*The effect of e-payment and online shopping on sales growth: Evidence from banking industry*," vol. 6, no. 4, pp. 1369-1380, 2022.

[5] T. Alkhdour, B. M. AlWadi, and M. Alrawad, "*Assessment of Cybersecurity Risks and threats on Banking and Financial Services*," 2024 2024.

[6] Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, A. K. J. I. J. o. s. r. Jaiswal, and management, "*A systematic literature review on the cyber security*," vol. 9, no. 12, pp. 669-710, 2021.

[7] R. P. K. Kollepalli et al., "*An Experimental Study on Detecting and Mitigating Vulnerabilities in Web Applications*," vol. 14, no. 2, 2024.

[8] W. Saffady, Managing information risks: *threats, vulnerabilities, and responses. Rowman & ittlefield Publishers*, 2020.

[9] R. Ihmouda, N. H. Binti, and M. Alwi, "*Penetration testing for libyan government website*," 2013.

[10] W. Wardana, A. Almaarif, and A. J. J. I. I. idjajarto, "*Vulnerability assessment and penetration testing on the xyz website using NIST 800-115 standard,*" vol. 7, no. 1, pp. 520-529, 2022.

[11] Siteefy. (2024). Available: *https://siteefy.com/how-many-websites-are-there/*

[12] I. Mantra, M. S. Hartawan, H. Saragih, and A. J. P. C. S. Abd Rahman, "*Web vulnerability assessment and maturity model analysis on Indonesia higher education*," vol. 161, pp. 1165-1172, 2019.

[13] I. N. W. S. A. MM, N. W. S. ARIYANI, I. I. W. A. Wijaya, M. Erg, I. J. J. o. I. E. MT, and pplications, "*ATCS System Security Audit Using Nessus*," vol. 7, no. 3, 2017.

[14] D. K. Saini and J. H. Yousif, "*Vulnerability and Attack Detection Techniques: Intrusion Detection System,*" in Cybersecurity: CRC Press, 2021, pp. 17-26.

[15] S. Zarei, "Risk management of internet banking," in Recent Researches in Artificial Intelligence. *10th WSEAS International conference on Artificial Intelligence, Knowledge Engineering and Data Bases (AIKED 11)*, Cambridge, UK, 2011.

[16] T. Scholte, D. Balzarotti, E. J. C. Kirda, and Security, "*Have things changed now? An empirical study on input validation vulnerabilities in web applications*," vol. 31, no. 3, pp. 344-356, 2012.

[17] F. Nel, L. J. I. Drevin, and C. Security, "*Key elements of an information security culture in organisations,*" vol. 27, no. 2, pp. 146-164, 2019.

[18] T. Vieira, C. J. W. a. s. Serrão, and v. a. f. w. a. s. a. a. c. study, "Web applications security and vulnerability analysis *financial web applications security audit–a case study*," no. 2, pp. 86-94, 2016.

[19] E. B. Setiawan and A. Setiyadi, "Web vulnerability analysis and implementation," *in IOP conference series: materials science and engineering*, 2018, vol. 407, no. 1, p. 012081: IOP Publishing.

[20] F. Wibowo, H. Harjono, and A. P. J. J. I. Wicaksono, "*Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto* Menggunakan OpenVAS dan Acunetix WVS," vol. 6, no. 2, pp. 212-217, 2019.

[21] A. Budiman, S. Ahdan, and M. J. J. K. Aziz, "Analisis Celah Keamanan Aplikasi Web E-Learning *Universitas Abc Dengan Vulnerability Assesment*," vol. 9, no. 2, 2021.

[22] I. Riadi, A. Yudhana, and W. Yunanri, "Analisis Keamanan Website Open Journal System *Menggunakan Metode Vulnerability Assessment*," vol. 7, no. 4, pp. 853-860, 2020.

[23] S. Chimmanee, T. Veeraprasit, K. SriphREw, and A. Hemanidhi, "A performance comparison of vulnerability detection between NetClarity Auditor and Open Source Nessus," *in Proceeding of the 3rd European Conference of Communications* (ECCOM'12), 2012, pp. 280-285.

[24] R. J. S. Kushe and Future, "Comparative study of *vulnerability scanning tools: Nessus vs Retina*," vol. 1, no. 2, pp. 69-71, 2017.

[25] A. Goutam and V. Tiwari, "Vulnerability assessment and penetration testing to enhance the security of web application," *in 2019 4th International Conference on Information Systems and Computer Networks (ISCON), 2019*, pp. 601-605: IEEE.

[26] E. A. Altulaihan, A. Alismail, and M. J. E. Frikha, "A survey on web application penetration testing," vol. 12, no. 5, p. 1229, 2023.

[27] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. J. E. Akin, "*A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions*," vol. 12, no. 6, p. 1333, 2023.

[28] Tenabel. (2024, 24-8). Nessus 10.8 User Guide. Available:*https://docs.tenable.com/nessus/Content/PDF/Nessus_10_8.pdf*

[29] A. Y. Eshetu, E. A. Mohammed, and A. O. J. J. o. B. D. Salau, "Cybersecurity vulnerabilities and solutions in Ethiopian university websites," vol. 11, no. 1, p. 118, 2024.

[30] A.-D. Tudosi, A. Graur, D. G. Balan, and A. D. J. S. Potorac, "*Research on Security Weakness Using Penetration Testing in a Distributed Firewall,*" vol. 23, no. 5, p. 2683, 2023.

[31] S. Pandey and A. J. A. P. Chaudhary, "Vulnerability scanning," 2023.