Journal of Big Data

RESEARCH Open Access

Cybersecurity vulnerabilities and solutions in Ethiopian university websites

Ali Yimam Eshetu[1], Endris Abdu Mohammed[1] and Ayodeji Olalekan Salau[2,3*]

*Correspondence:
ayodejisalau98@gmail.com

[1] School of Electrical and Computer Engineering, Institute of Technology, Woldia University, Woldia, Ethiopia
[2] Department of Electrical/Electronics and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria
[3] Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India

Abstract

This study investigates the causes and countermeasures of cybercrime vulnerabilities, specifically focusing on selected 16 Ethiopian university websites. This study uses a cybersecurity awareness survey, and automated vulnerability assessment and penetration testing (VAPT) technique tools, namely, Nmap, Nessus, and Vega, to identify potential security threats and vulnerabilities. The assessment was performed according to the ISO/IEC 27001 series of standards, ensuring a comprehensive and globally recognized approach to information security. The results of this study provide valuable insights into the current state of cybersecurity in Ethiopian universities and reveals a range of issues, from outdated software and poor password management to a lack of encryption and inadequate access control. Vega vulnerability assessment reports 11,286 total findings, and Nessus identified a total of 1749 vulnerabilities across all the websites of the institutions examined. Based on these findings, the study proposes counteractive measures tailored to the specific needs of each identified defect. These recommendations aim to strengthen the security posture of the university websites, thereby protecting sensitive data and maintaining the trust of students, staff, and other stakeholders. The study emphasizes the need for proactive cybersecurity measures in the realm of higher education and presents a strategic plan for universities to improve their digital security.

Highlights

- The study investigates the causes of cybersecurity vulnerabilities in university websites, with a focus on Ethiopian Universities.
- The evaluation was based on ISO/IEC 27001 series standards and utilized three different automatic VAPT evaluation tools: Nmap, NESSUS, and VEGA.
- The research identified a range of issues contributing to cybersecurity vulnerabilities, including outdated software, poor password management, a lack of encryption, and inadequate access control.
- The study underscores the importance of proactive cybersecurity practices in the higher education sector and provides a roadmap for universities to enhance their digital security.

Keywords: Cybersecurity in higher education, Information security standards, Nessus, Nmap, VAPT, Vega

Introduction

Ensuring a robust security of university websites has become integral in this digital age, given the expanding reliance on online platforms for educational services, information dissemination, data storage, and administrative functions. When we refer to a "university website," we mean the entire internet presence of the university. This comprises the public information front-facing system, the faculty and student online learning and administration system, and the internal administration system used for university operations.

The 2023 Verizon Data Breach Investigations Report (DBIR) analyzed 16,312 security incidents and 5199 breaches. 83% of breaches involved external actors with the majority being financially motivated, 74% of breaches involved the human element, which includes social engineering attacks, errors, or misuse, and 50% of all social engineering attacks are pretexting incidents [1]. The permeation of cyber threats and vulnerabilities poses a formidable challenge to the integrity and confidentiality of university data systems. Understanding the factors that contribute to cyber security fault vulnerability within the realm of university websites is critical for proactively addressing potential risks and fortifying these digital infrastructures [2].

Having this in mind, because of the nature of the hostile environment, websites are vulnerable to security faults. Specifically, most of the organizations in Ethiopia that develop and use websites for their activities emphasize the availability and timely accessibility of their websites. This leads their websites to have unguaranteed confidentiality and integrity. Even they did not know to what extent they were risky and exposed to security fault vulnerability. Due to this reason, their customers do not feel free to use their websites. Therefore, it is necessary to study the causes and impacts of these vulnerabilities by assessing the risk and conducting audits using world-standard methodologies. This will enable us to take appropriate countermeasures before the activities and resources of these institutions are devastated. Specifically, higher education institutions (university) websites need to be kept in secure and safeguarded environments since their insecurity of simple data leakage by any means has a great impact on every aspect of the nation including economic, political, and social disorder [3].

Websites can be affected by several vulnerabilities which can be logical or technical [4]. Some examples of technical vulnerabilities are SQL injection, local inclusion, cross-site scripting, and remote file inclusion [5, 6]. These technical vulnerabilities can affect website security. There are different reasons for the occurrence of vulnerability on websites. Some vulnerabilities happen because of poor programming or outdated systems. Web security is a mechanism to protect both websites and users (visitors) from cyber threats and unauthorized access to their information [7]. Malware can slow down the speed of a website, expose confidential information like credit card numbers, and even remove websites from search engines permanently. The practice of protecting websites and general network infrastructures from any unauthorized actions is known as cybersecurity.

The International Telecommunication Union states that cyber security is the collective application of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practices, assurance, and expertise that can be used to guard the cyber system, organization, and related assets [8]. Furthermore, it is important because the government, military, corporate, financial, and health organizations collect, process, and store unprecedented amounts of data on computers and other devices.

A significant portion of that data can be sensitive information, whether that is intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences [9]. For effective cyber security, an organization needs to coordinate its efforts throughout its entire cyber system. Security countermeasures ensure the confidentiality, availability, and integrity of cyber systems by preventing asset losses from cyber security attacks [10]. Effects of cyber security failure lead to the loss of intellectual property, direct financial loss from cybercrime, loss of sensitive business information, sabotage of operations, extra costs for systems' recovery, and stakeholders' loss of on-system confidence.

The cybersecurity process in higher education institutions is part of a holistic organizational and economic system and is ideally suited for functional modeling and graphical descriptions of processes [11]. In cybersecurity, identifying potential threats and vulnerabilities is paramount. This study addresses this important challenge by leveraging automated vulnerability assessment and penetration testing (VAPT) tools, specifically Nmap, Nessus, and Vega, to detect and analyze potential cyber risks [12–14]. In the complex world of information security, adhering to established standards is crucial. This study conducts an assessment in strict accordance with the ISO/IEC 27001 series of standards, ensuring a comprehensive and globally recognized approach to safeguarding information.

This investigation seeks to explore the underlying causes that render university websites susceptible to cyber security faults, identifying critical weaknesses and potential entry points for cyber-attacks. By delving into the multifaceted landscape of cyber security, this inquiry aims to illuminate the specific areas of vulnerability within university websites, discerning the intricacies that make them prone to exploitation by malicious actors.

Furthermore, this study endeavors to delineate comprehensive counteractive measures, aiming to devise robust strategies that fortify the cyber security posture of university websites. By identifying best practices, procedural enhancements, and technological approaches, this investigation strives to bolster the resilience of these vital digital platforms, mitigating the potential impact of cyber security faults and enhancing overall data protection.

Related work

In recent years, the field of cyber security has become increasingly important due to the rise in cyber threats and attacks. Universities, being repositories of valuable data and research, have become prime targets for cybercriminals. University websites, in particular, are vulnerable to cyber security faults that can compromise the integrity, confidentiality, and availability of sensitive information [15, 16]. This literature review aims to investigate the causes behind cyber security fault vulnerability in university websites and identify counteractive actions to mitigate these vulnerabilities.

Dioubate et al. [17] explored the role of cybersecurity in the performance of Malaysian higher education institutions. It uses semi-structured qualitative interviews with 10 cybersecurity risk management officers from 10 public universities. The data were analyzed using thematic analysis to identify the strengths and deficiencies of the current cybersecurity frameworks. It has contributed to protecting the data of students and

staff, which in turn allowed the universities to improve their reputation. The efficient use of resources, identification, and detection of risk exposures, and improved cybersecurity communication between the technical team and top management are essential for a good decision-making process. This study significantly contributes to the understanding of the performance and applicability of cybersecurity in universities.

In their study, Harrell et al. [18] conducted a large-scale vulnerability assessment of 272 higher education institutions. It identifies vulnerabilities that fail to provide comprehensive remediation strategies. Selected flaws are recreated and remediated in a virtual environment to develop enhanced, automated reporting mechanisms. The remediation reports generated from the tools often cause significant information overload while failing to provide actionable solutions. The study develops enhanced reports that address 27.80% of vulnerabilities found in scanned higher education institutions, enabling efficient vulnerability remediation. This study addresses the lack of appropriate knowledge in higher education institutions to improve their cybersecurity posture. It provides succinct reports to enable efficient vulnerability remediation.

Dioubate and Daud [19] applied cybersecurity risk management in Malaysian public universities. The qualitative research method is applied to collect data by interviewing experts in cybersecurity risk management. The results show the factors that lead to risks and benefits obtained when the stakes are managed. This research shows a greater understanding and knowledge of risk management. The future direction of this study is to propose a cybersecurity risk management framework based on the reviews of the existing frameworks used in Malaysian public universities.

The cybersecurity landscape has evolved over the last few decades and its latest trends and projections for the next decade [20]. It also takes an extensive literature review and desk research of methods that could respond to the cybersecurity vulnerabilities of the next decade. The paper illuminates the importance of strengthening Higher Education Institution (HEI) cybersecurity capacities and explores why HEIs face severe challenges in tackling the ever-escalating cyberattacks. The paper proposes a system-wide approach to safeguard HEI cybersecurity and highlights the necessity to reassess prioritized areas.

Similar to our study, Alhumud et al. focus on evaluating the cybersecurity performance of Saudi universities [21]. The study employs a mixed-method design, utilizing questionnaires and interviews to collect data. The participants include representatives from 10 Saudi universities. There is room for improvement in the cybersecurity practices of Saudi universities. Concerns were expressed about the lack of well-defined policies and procedures, insufficient training and awareness programs, and non-compliance with cybersecurity regulations and standards. The majority of participants affirmed the importance of cybersecurity in strategic objectives and Total Quality Management.

Ulven and Wangen [22] investigated cybersecurity risk by reviewing existing literature on known assets, threat events, threat actors, and vulnerabilities in higher education. The study applies the Comprehensive Literature Review (CLR) Model and includes published studies from the last twelve years. The primary finding was that empirical research on cybersecurity risks in higher education is scarce, and there are large gaps in the literature. The paper concludes nine strategic cyber risks with descriptions of frequencies from the compiled dataset and consequence descriptions. The results will serve as input

for security practitioners in higher education, and the research contains multiple paths for future work.

The role of cybersecurity in higher education institutions is presented by Singar and Akhilesh [23]. It highlights the importance of the internet and online services in the modern learning and teaching environment and the risks that come with increased utilization of the Internet and connected devices. The paper identifies cyber threats as risks that impact the information and data security of higher educational institutions. It emphasizes the need for implementing security measures in the higher education sector to prevent hackers from stealing and misusing the information assets collected by the institutes.

Meharu [24] investigated the increase in cyber-attacks in Ethiopia and the lack of a standardized legal cybersecurity framework, strategy, and governance at the national level. The paper also highlights the lack of awareness and expertise in cybersecurity as contributing factors to the increasing level of cyber-attacks in the country. The findings reveal that only 11.6% of government institutions in Ethiopia have legal frameworks to prevent cyber-attacks, while 87.4% have no recognized legal frameworks. The paper also mentions that some local researchers are developing cybersecurity frameworks and strategies for specific sectors, but these frameworks have not been rigorously tested. The paper suggests that future researchers should focus on developing a virtual training system or intelligent security tutoring system to address the shortage of cybersecurity professionals and the lack of cybersecurity know-how in the country.

The investigation of cybersecurity in higher education institutions is a mandatory task. The purpose of our research is to provide a comprehensive overview of the cybersecurity landscape in Ethiopian universities. While it's true that similar studies have been conducted in other countries, this is the first of its kind in Ethiopia. Therefore, the findings are indeed novel in this context. The other contribution of our study, it serves as a benchmark for future research in this area. By presenting a descriptive analysis, we have laid the groundwork for more delicate studies to be conducted in the future. We believe that our work contributes significantly to the knowledge base by filling a gap in the literature.

Methodology

The findings of the VAPT assessment are not self-explanatory for all communities within the cyberspace. Instead, they require detailed descriptions to effectively disseminate the research output to all readers and implementers. Due to this reason, an exploratory type of research approach is used. So, in addition to showing all findings of the data collection techniques, we have narrated the impacts, tendencies, and possible ways of countermeasures for cyber vulnerability.

In our study, we gathered data from primary sources using a survey and a Vulnerability Assessment and Penetration Test (VAPT). We also reviewed related literature, policy manuals, and standards as secondary sources to corroborate our findings with established norms.

In our study, we used purposive sampling to select research areas from Ethiopia's 44 public and 2 Science and Technology Universities [25]. We analyzed the websites of

16 universities, including 3 comprehensive, 3 applied science, all 8 research universities, and the 2 Science and Technology Universities, and to assess their cyber security. The selection process of universities for research could be biased due to factors such as accessibility of data, geographical location, reputation, and the researcher's familiarity with the institution. This could limit the diversity and representativeness of the sample. Details of these universities are in Table 1.

The respondents are selected based on their roles and positions that have a direct relation to information technology, cyber security, safety and security, risk assessment, and management. The participants for the study consisted of the network, safety, security, and risk assessment professionals from respective Universities.

In this research, our primary objective is to examine the conditions that render targeted websites susceptible to cybercrime. To accomplish this, we surveyed to gauge the level of awareness among experts regarding website security and performance. We also identified potential vulnerabilities in the target website that could be exploited by intruders using automated Vulnerability Assessment and Penetration Testing (VAPT). Based on our findings, we suggested appropriate countermeasures to address these vulnerabilities and defects, aligning the targeted websites with the standards prevalent in the cyberspace world. The methodologies we employed to carry out these tasks are outlined and detailed in Figure 1.

Web security standards

Websites are attractive targets for cyberattacks due to their global availability, simplicity, anonymity, and potential for financial gain [26]. To protect it from these threats, everyone involved in website development and operation must adhere to global cybersecurity standards. These standards provide checklists, procedures, and guidelines aimed at ensuring the security, consistency, availability, and reliability

Table 1 List of studied university websites

No	Host University	Short Form	Differentiations
1	Woldia University	WLDU	Comprehensive Universities
2	Mekdela Amba University	MKAU	
3	DebreTaboor University	DTU	
4	Wollo University	WU	Applied Universities
5	Semera University	SU	
6	Debrebirhan University	DBU	
7	Bahirdar University	BDU	Research Universities
8	University of Gonder	UOG	
9	Jimma University	JU	
10	Addis Ababa University	AAU	
11	Hawassa University	HU	
12	Arbaminch University	AMU	
13	Haramaya University	HAU	
14	Mekele University	MU	
15	Addis Ababa Science and Technology University	AASTU	Science and Technology Uni
16	Adama Science and Technology University	ASTU	

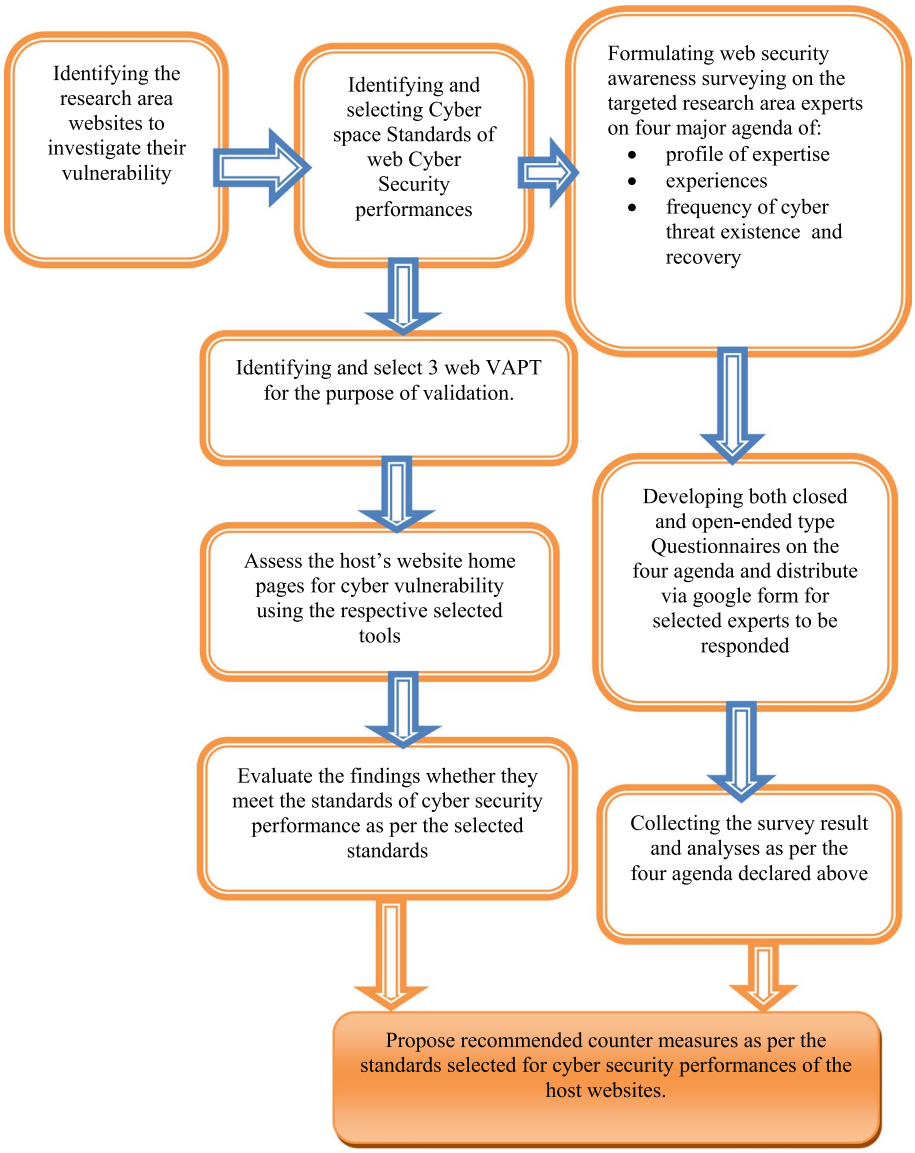


Fig. 1 Research methodology design flow

of cyberinfrastructure [26]. There are numerous cybersecurity standards, including the NIST 800 series, ISO_IEC_2700 series, ISF SOGP, and SOX. All standards except ISO_IEC_27001 are developed by specific companies or nations based on their requirements.

For example, the Information Technology Laboratory (ITL) developed the NIST standards to strengthen the economy and public interest [27]. However, ISO_IEC_27001 is a globally standardized security measure for information systems developed by a committee of international stakeholders [28]. It provides guidelines for monitoring, operating, verifying, maintaining, and improving the information security management system "ISMS". This standard is designed to understand the training, awareness, and ability of ISMS personnel to conduct investigations to investigate

cyber issues on websites, identify vulnerabilities, develop corrective actions, and ultimately report findings.

Vulnerability assessment and penetration testing (VAPT) tools

Vulnerability to the cyber security risks of the data transmission cyberspace via websites is the defects of the overall website security processes, design, implementation, and operational monitoring and control of the services including the vandalism of the standards of website security policies. Using vulnerability assessment and penetration testing (VAPT), the given organization's website can be easily detected. VAPT is used for inspecting the softness of the cyberinfrastructure through which the probability of existences for intruders/hackers to gain unauthorized access. In this study, two stages of vulnerability examination were performed using the VAPT methodology.

- Network Infrastructure Based (NIB-VAPT): This stage includes identifying open ports, exposed operating systems, running application software, outdated software versions, missing patches, or misconfigurations that can be exploited by unauthorized users. Tools such as Network Mapper and Nessus were used for vulnerability assessment and penetration testing.
- Database-based (DB-VAPT): This stage focuses on assessing vulnerabilities in the website's database system, such as SQL and shell injection, cross-site scripting, and session cookies. During this phase, Vega tools were used for assessment and penetration testing.

Network Mapper (Nmap) is an open-source tool for auditing cybersecurity, managing service upgrades, and monitoring host availability [29]. IP packets are used to identify the hosts available on the network, the services they offer, their operating systems, and the type of packet filters/firewalls in use. Nmap stands out as a robust tool utilized for arranging investigations and security appraisals. Being open source and broadly grasped inside the cybersecurity space it serves as a choice for conducting organized filters. One of the restrictions of Nmap is , that it may not always accurately identify the working framework or administrations running on a gadget. This could lead to untrue positives or negatives. So, to expel this issue we ought to have to check over and over.

Nessus is an industry-standard world's most widely deployed vulnerability assessment tool provided by Tenable [30]. It helps cyberspace security experts reduce their organization's website attacks and it is also a widely used tool for researchers in the area of cyberspace security to assess and examine the susceptibility of the target website to unauthorized attacks of non-legitimate intruders/hackers.

Nessus displays the generated vulnerability assessment results as per the descending order of their severity from critical to informal. In general, the results are categorized into critical, high, medium, low, and informative levels of severity with their respective CVSS V3 base scores.

A Common Vulnerability Scoring System (CVSS) is an open framework communicating the characteristics and severity of application service vulnerabilities. It consists of three metric groups Base, Temporal, and Environmental. The Base group matrices, used here in the Nessus assessment, represent the inherent qualities of vulnerability by

producing a score ranging from 0.0 to 10.0. Those numerical scores translated into a qualitative representation of low, medium, high, and critically severe vulnerability. The severity magnitude can be calculated according to the CVSS V3 calculator [31]. Nessus holds a status, among vulnerability-checking tools bragging a cluster of plugins. It exceeds expectations in identifying vulnerabilities that may be misused by actors to invade an arrange. Also, it is easy to utilize and gives comprehensive reports, which encourage comprehension and activity on the outcomes. Its effectiveness generally depends on the quality of its powerlessness database. It might miss new vulnerabilities that are not however in its database. Moreover, it may report false positives.

Vega is an open-source Vulnerability Assessment and Penetration Testing (VAPT) service developed by Subgraph. It identifies website vulnerabilities such as SQL injection, cross-site scripting (XSS), remote file includes, shell injection, and disclosed sensitive information [32]. Vega is an open-source, free web application security scanner and testing tool. Vega can assist you with identifying and validating vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and unintentionally revealing sensitive information. Because of their strength, dependability, and widespread use in the cybersecurity field, those tools were selected over others. They are the best at identifying cybersecurity flaws in Ethiopian university websites because they provide a thorough approach to penetration testing and vulnerability assessment. It might also miss vulnerabilities that require a specific sequence of actions to exploit. It needs a repetitive scanning mechanism.

Automated vulnerability scanning and penetration testing are also provided by programs such as Intruder, Acunetix Web Vulnerability Scanner, and Invicti Security Scanner. These tools are frequently commercial, though, and they might not be as affordable for a research setting as Nmap, Nessus, and Vega.

Research findings and analysis

In this section, findings from the survey and each of the VAPT methods were presented in both statistical presentation and detailed analysis. The collected quantitative data were displayed in tabular form, with an analysis conducted for each method. Finally, a summary of the findings' consolidated analysis was presented for each web vulnerability method.

In this study, a qualitative approach was used to identify potential threats and vulnerabilities in targeted areas and to gauge the awareness of front-line professionals about these risks [33]. A questionnaire, developed using Google Forms, was distributed to ICT professionals to gather data on the frequency of these incidents and the countermeasures taken. The findings were then compiled, compared, and cross-referenced with literature reviews and automated VAPT results.

The survey, comprising 30 questions, was divided into four sections: ICT expertise profile and responsibilities (5 questions), vulnerability and cyber threat experiences (13 questions), the impact of cyber threats (2 questions), and countermeasures taken against cyber threats (10 questions). The majority of the questions (90%) were closed-ended to facilitate responses.

As outlined in the third section of the research methodology, the questionnaire approach is employed to gather data on potential existing or future cybersecurity vulnerabilities, as well as the countermeasures that university professionals have implemented or may implement. Consequently, Figures 2-12 depict the responses to these questions.

Discussion

Figure 2, reveals that the majority of survey respondents, approximately 68.1%, are IT administrators and engineers. Their primary duties include system, network, and data administration, as well as the design and implementation of their institutions' cyber infrastructures. The remaining 31.3% of respondents are management personnel, risk governance, C-level executives, and system analysts. This indicates that the survey was conducted among those directly responsible for and highly involved in the institutions' cybercrime responsiveness.

As depicted in Figure 3, when asked if users alter their cyber infrastructure security systems, 90.6% of respondents answered "yes," while 9.4% were unsure, responding with "maybe." This suggests that all the institutions' cyber infrastructure security systems are potentially altered or disabled by users.

The survey also assessed the potential vulnerabilities and likelihood of cyber breaches. Respondents were asked to rate the possible causes of vulnerability to cyber breaches, as shown in Figure 4. The three most serious causes identified were the use of outdated patches, unsecured network perimeters, and the absence of antivirus software or the presence of unused installed software, with high to very high ratings of 78.125%, 59.375.%, and 56.25% respectively.

These vulnerabilities are confirmed by the survey results, with 81.3% of respondents experiencing cyber security breaches in their institutions' cyber infrastructures. 6.3% were unsure if they had experienced breaches, while 12.5% reported no encounters with cybercrime. This is illustrated in Figure 5.

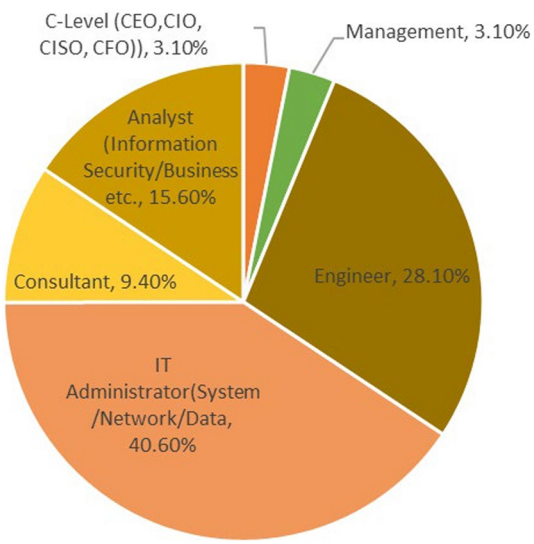


Fig. 2 Respondent's job position

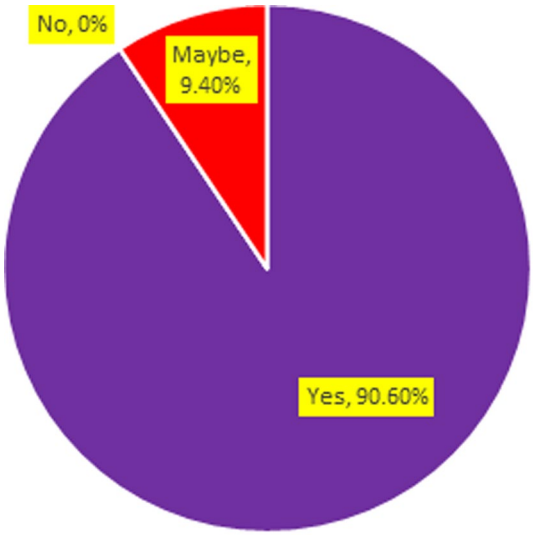
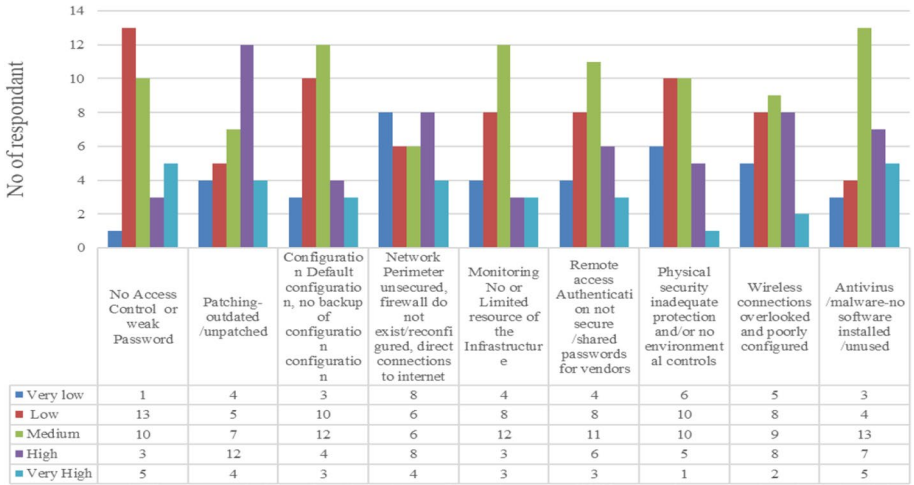


Fig. 3 Security systems are altered by users or not



	No Access Control or weak Password	Patching-outdated /unpatched	Configuration Default configuration, no backup of configuration configuration	Network Perimeter unsecured, firewall do not exist/reconfigured, direct connections to internet	Monitoring No or Limited resource of the Infrastructure	Remote access Authentication not secure /shared passwords for vendors	Physical security inadequate protection and/or no environmental controls	Wireless connections overlooked and poorly configured	Antivirus /malware-no software installed /unused
Very low	1	4	3	8	4	4	6	5	3
Low	13	5	10	6	8	8	10	8	4
Medium	10	7	12	6	12	11	10	9	13
High	3	12	4	8	3	6	5	8	7
Very High	5	4	3	4	3	3	1	2	5

Fig. 4 Possible causes of being vulnerable to cyber breaches

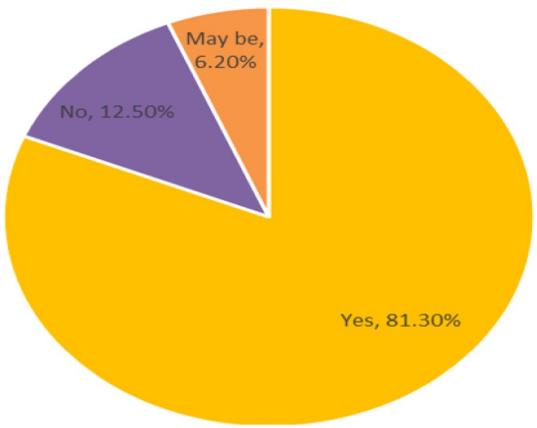


Fig. 5 Cybersecurity breach incidents

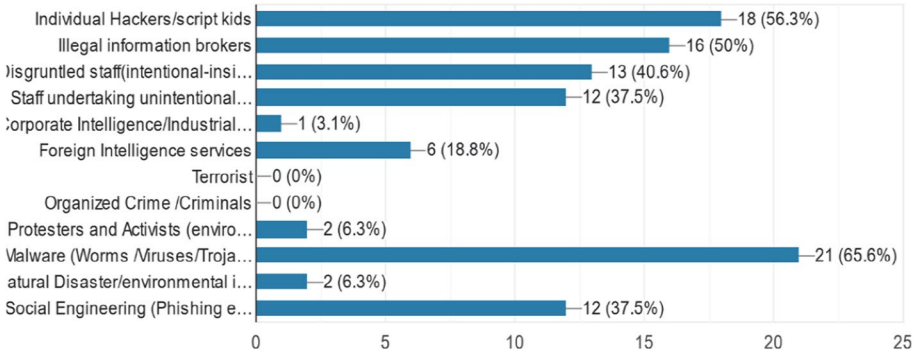
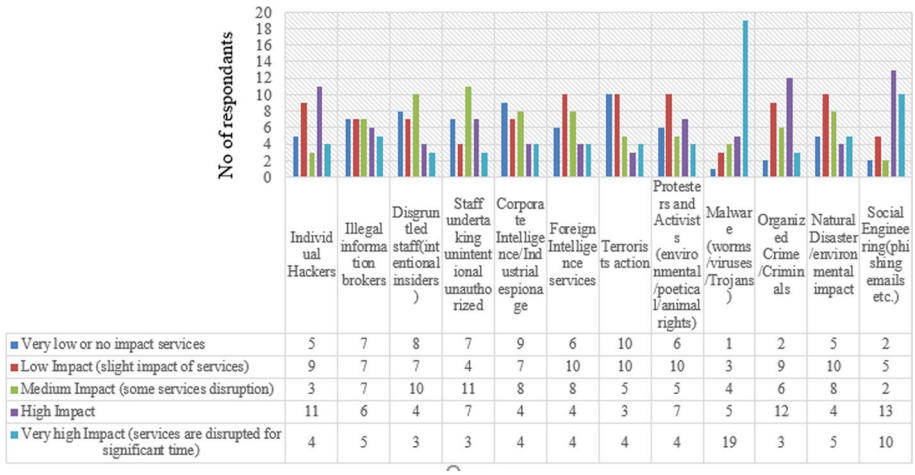


Fig. 6 Treats mostly found in cyberinfrastructure



	Individual Hackers	Illegal information brokers	Disgruntled staff(intentional insiders)	Staff underta king unintent ional unautho rized	Corpora te Intellige nce/Ind ustrial espiona ge	Foreign Intellige nce services	Terroris ts action	Proteste rs and Activist s (enviro nmental /poetica l/animal rights)	Malwar e (worms /viruses /Trojans)	Organiz ed Crime /Crimin als	Natural Disaster /environ mental impact	Social Enginee ring(phi shing emails etc.)
Very low or no impact services	5	7	8	7	9	6	10	6	1	2	5	2
Low Impact (slight impact of services)	9	7	7	4	7	10	10	10	3	9	10	5
Medium Impact (some services disruption)	3	7	10	11	8	8	5	5	4	6	8	2
High Impact	11	6	4	7	4	4	3	7	5	12	4	13
Very high Impact (services are disrupted for significant time)	4	5	3	3	4	4	4	4	19	3	5	10

Fig. 7 Impact rate of Cyber-threats

When asked to select the top three threats to their cyber infrastructures, 65.6% of respondents identified malware (including worms, viruses, Trojans, and spyware) as the primary threat. Individual hackers and illegal information brokers were the next two threats, selected by 56.3% and 50% of respondents respectively. This is shown in Figure 6. Malware, which collects critical information and allows intruders unauthorized access to cyber infrastructures, was ranked as the third top cause of vulnerability, which could explain its prominence as a cyber threat.

Figure 7 shows that the four most impactful cyber threats are malware, social engineering, threats, and organized criminals, with impact ratings of 75%, 71.875%, 62.5%, and 46.875% respectively.

The survey also examined the services most affected by these ungoverned cyber threats and the extent of their impact. Respondents indicated that the most affected cyber security service is unauthorized control of infrastructures and loss of availability, with 53.125% and 40.625% of respondents confirming this, as shown in Figure 8.

The survey results reveal that approximately 34.4% of respondents actively monitor and control their cyber infrastructure to protect against cybercrime. However, the remaining 65.6% either do not manage their cyber infrastructure or are uncertain about their governance methods. This data is represented in Figure 9.

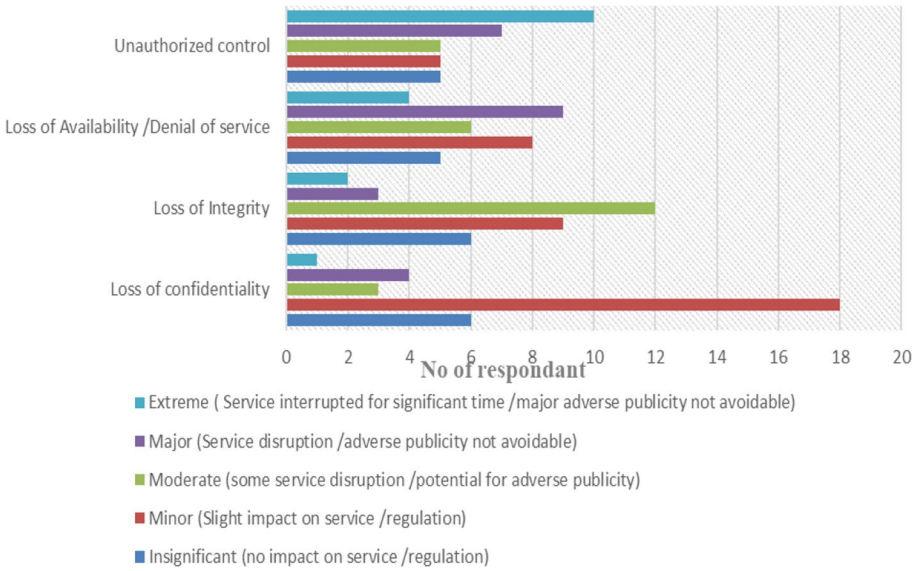


Fig. 8 Cyber threat impacts on cyber security services

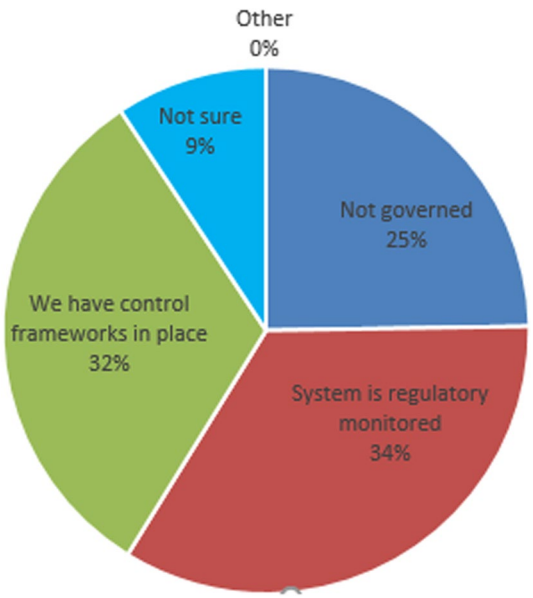


Fig. 9 Respondents on security and governance of their cyberspace

Figure 10 illustrates that all proposed mitigation measures, which respondents could select as being implemented in their cyber infrastructures, received a response rate ranging from 59.375% to 75%. Specifically, 75%. of respondents indicated that measures such as infrastructure monitoring and securing remote access authentication (no shared password for vendors) are either not implemented or they are unsure if they are implemented in their institutions' cyberinfrastructure.

This data supports the previous findings regarding the governance of the institutions' cyberinfrastructure. The responses to the question "What is the maturity level of your cyber security governance?" further illustrate this point. As shown in Figure 11, 37.5% of

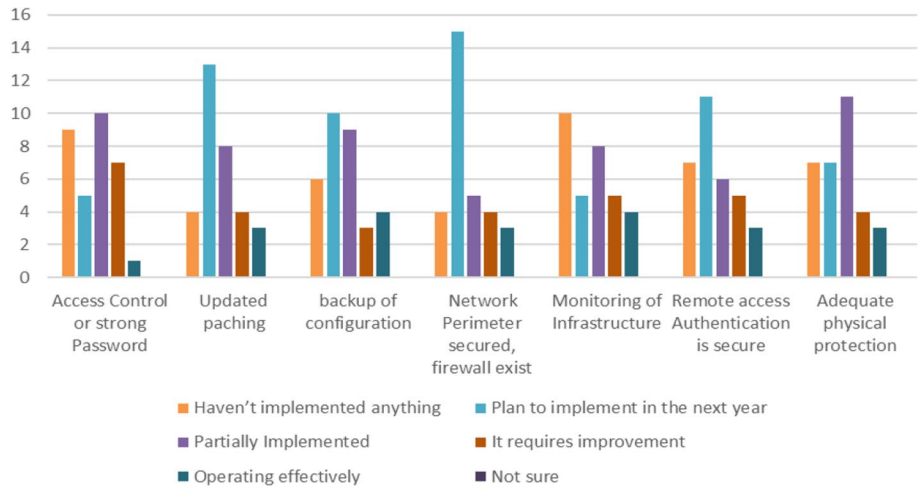


Fig. 10 Respondents Mitigation Measures up on Cyber-threats

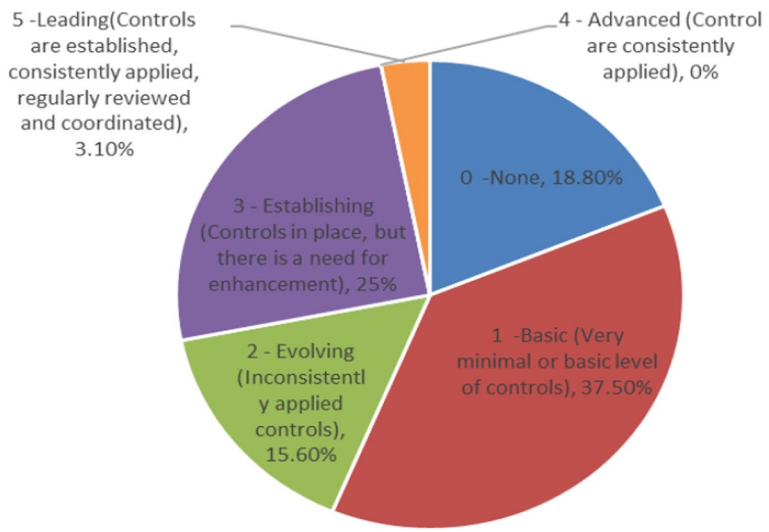


Fig. 11 Maturity of cyber security governance for their cyber-infrastructure

respondents rated their cyber security governance as basic, indicating a minimal level of maturity. Meanwhile, 15.6% reported inconsistently applied governance, and only 25% rated their governance as establishing and leading or at an established maturity level.

These results suggest that the institutions are in the early stages of implementing necessary cybercrime mitigation measures and that significant effort is required in this area.

Figure 12, shows that out of 15 proposed cyber threat countermeasures, 13 have either a low impact, have not been implemented, or it is uncertain whether they have been implemented in the respondents' cyberspaces. This indicates that 86.67% of these mitigation methods, including network segregation, system hardening, vulnerability audits, data encryption, physical access control, environmental standards, system change control, 3rd party remote access, and patch management, have not had a significant impact on the institutions surveyed. These methods received effectiveness

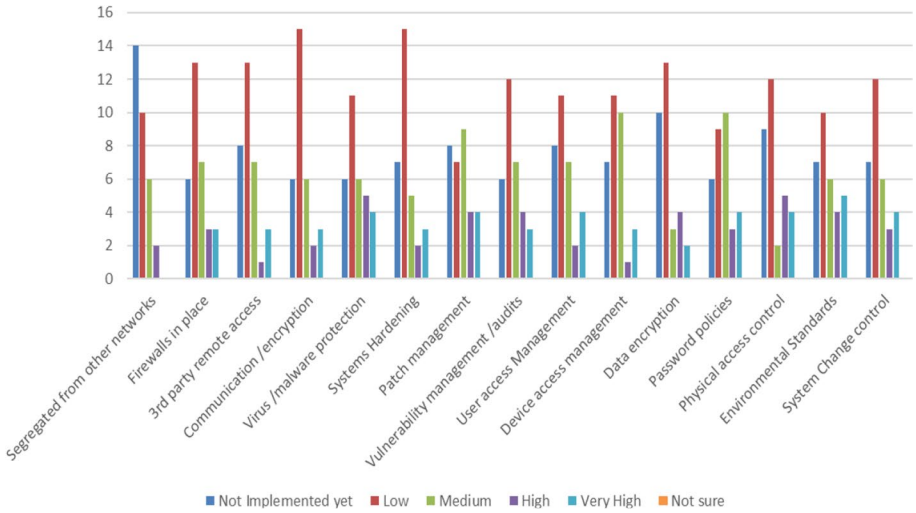


Fig. 12 Effects of Mitigation Methods of Cyber Threat

ratings ranging from 59.375% to 75%. from respondents. This shows the need for proactive measures to secure cyber infrastructures in institutions.

VAPT investigation findings

In addition to the survey, a Vulnerability Assessment and Penetration Testing (VAPT) was conducted on 16 public university websites, including the three categories (applied, research, and Science-Technology Universities) [34].

Automated tools were used to assess each site, with findings extracted, reorganized, and analyzed according to cybersecurity standards (ISO-IEC-27000 series). In the end, comparisons of institutions based on the results of the assessment are performed as a summary of the result analysis and interpretations of the respective sections.

The Nmap tool examines the network infrastructure of the respective websites. It delivers how many application service ports are closed, open, and filtered from the total tested well-kwon TCP ports of 1000.

As per reference [35], the accuracy percentage of Nmap's OS detection scanning indicates the degree of alignment between the target cyber infrastructure's response and the fingerprints in the Nmap database. A higher accuracy percentage implies greater confidence in Nmap's operating system guesses for the targeted cyber infrastructures. An accuracy below 80% usually means Nmap is less certain of the guessed OS, which could be due to firewall filtering, real-time patching, or customization of the target operating system. Once intruders/hackers have investigated the types of services, topologies, operating systems, and open ports, they can devise strategies to attack the target through those ports, topology gateways, properties, services, and operating systems.

As demonstrated by the Nmap scanning result, for this study, all 16 tested institutions' URLs provided the aforementioned information with 87-100% accuracy, except for HAU. Coupled with outdated patching implementation (as mentioned in the survey above), these institutions are susceptible to cybercrime from aggressive intruders/

hackers. Linux 4. x and Linux 3. x were identified or predicted by Nmap as the most likely operating systems of the targeted cyber networks.

As indicated in Table 2, almost all websites, except JU, have more than 96.1% filtered TCP ports. This is beneficial as all packet communications through those ports are regulated by firewall policies. This means that when cyber criminals' remote scanners send SYN packets or an ICMP ping packet, they are met with an algorithm like iptables that prevents the attacked cyber infrastructure from responding. Instead, it blocks further attempts.

Result of vulnerability assessment & penetration testing tool

As shown in Table 2, 11 out of the 16 websites tested by this tool during the testing period had at least one closed port. Notably, JU had 99.7% of TCP ports in a closed state. This implies that when an intruder sends either a SYN or ICMP ping packet remotely, the targeted host responds with an RST packet, forcing the intruder to reset their request. Unless under certain circumstances where these closed ports are opened and the intruder repeatedly attempts to gain access, the system remains secure. Here, no firewall acts to filter incoming remote intruder scanning packets; instead, it protects itself from the intruder-sent packet since it is closed. A determined intruder could seize an opportunity by waiting for the brief interval when the closed port becomes open. Therefore, responsible professionals must ensure these ports are governed by their firewall policies, effectively making them filtered TCP ports.

Intruders persistently scan ports remotely to determine if the target has services that are susceptible to buffer overflow. These vulnerable services are ports in an open state. Open ports are those where server programs are running, assigned to be a port for the server. If an intruder receives a SYN+ACK packet when attempting to scan the target by sending an SYN or ICMP ping packet remotely, they can confirm the presence of open ports in the target cyberspace, making it vulnerable to system attacks.

Nessus uses the Common Vulnerability Scoring System (CVSS) from the National Vulnerability Database (NVD) which has Common Vulnerabilities and Exposure (CVE) standards. CVSS consists of severity factors of attack vector, complexity, intruder interaction, and the impact of the existing vulnerability over system confidentiality, integrity, and availability and also it considers the required privileges for the existing vulnerabilities [36]. By taking this in mind Nessus calculates the CVSS base score factor of each vulnerability using the formula of calculator syntax described in "Discussion" section. .

We have compiled the comprehensive findings of Nessus in Table 3 in a tabular format, complete with detailed descriptions of impacts and mitigating solutions for the respective vulnerabilities of all 16 examined institutions.

As shown in Table 2, it illustrates that Nessus identified a total of 1,749 vulnerabilities across all the websites of the institutions examined. A significant majority of these vulnerabilities 1,413 (or 80.8%) are classified as Info-type vulnerabilities.

The remaining 336 vulnerabilities (or 19.2%) are direct vulnerabilities that expose the respective institutions' cyber infrastructures' immediate flaws. Many of these vulnerabilities stem from the use of unsupported system versions, indicating that institutions are using software with expired licenses. This results in all hosts lacking the latest security patches from their respective vendors. The use of outdated patches is one of the top vulnerabilities identified by survey respondents in the awareness assessment survey.

Table 2 Result of vulnerability assessment & penetration testing tool

No	Host University	Short form	Vulnerability Assessment & Penetration Testing Tool													
			Nmap			Nessus						Vega				
			CP	OP	FP	C	H	M	L	I	T	H	M	L	I	T
1	Woldia University	WLDU	9	15	976	1	1	45	0	173	220	352	4	31	337	724
2	Mekdela Amba University	MKAU	6	2	992	1	0	2	0	49	52	6	1	3	519	529
3	DebreTaboor University	DTU	60	12	928	0	6	29	0	242	277	0	0	0	2	2
4	Wollo University	WU	9	15	976	0	0	44	2	190	236	59	8	549	929	1545
5	Semera University	SU	0	19	981	0	0	2	2	108	112	1	1	0	3	5
6	Debrebirhan University	DBU	13	12	975N	0	0	25	2	96	123	1	1	471	389	862
7	Bahirdar University	BDU	10	15	975	0	1	5	0	25	31	0	1	5	0	6
8	University of Gonder	UOG	35	4	961	0	1	3	0	56	60	0	2	869	241	1112
9	Jima University	JU	997	3	0	0	2	3	0	49	54	0	7	97	59	163
10	Addis Ababa University	AAU	1	1	998	1	0	0	0	14	15	81	10	147	286	524
11	Hawassa University	HU	0	2	998	48	28	39	4	38	157	5	175	675	1758	2613
12	Arbaminch University	AMU	1	2	997	0	0	4	0	38	42	0	16	0	859	875
13	Haramaya University	HAU	0	1	999	0	0	1	0	31	32	2	1	497	688	1188
14	Mekele University	MU	0	1	999	0	1	26	0	250	277	0	1	1	0	2
15	Addis Ababa Science & Technology University	AASTU	1	2	997	0	0	0	0	15	15	494	4	267	24	789
16	Adama Science and Technology University	ASTU	0	2	998	0	0	7	0	39	46	3	7	0	337	347
Total			1142	108	14,750	51	40	235	10	1413	1749	1004	239	3612	6431	11,286
Mean			71.38	6.75	921.88	3.19	2.50	14.69	0.63	88.31	109.31	62.75	14.94	225.75	401.94	705.38
Standard Deviation			239.50	6.34	238.73	11.58	6.75	16.37	1.17	78.08	91.59	140.32	41.54	281.62	459.06	673.55

NB: CP = Closed Port, OP = Open Port, FP = Filtered Port, C = Critical, H = High, M = Medium, L = low, I = Informational and T = Total

Table 3 Impact on the security of cyber infrastructure description and its mitigation

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
PHP Unsupported Version Detected (V7.1.33)	The lack of new patch security updates is a critical vulnerability for cybercrime	Upgrade to vendor-supported patch update version of PHP. i.e. 8.0.x/8.1.x for a Server: X-Powered-By:
PHP < 7.3.24 Multiple Vulnerabilities	The web server is affected by multiple Vulnerabilities	Upgrade to PHP version 7.3.24 or later. Since it is before 7.3.24 which is not supported by Vendor
PHP < 7.3.28 Email Header Injection	Due to a failure to properly handle CR-LF sequences in a header field, the web server is affected by email header injection Vulnerability and an authenticated remote attacker can exploit this vulnerability by inserting line feed characters into email headers to gain full control of content	Upgrade to PHP version 7.3.28 or later. Since it is before 7.3.28 which is not supported by Vendor
SSL Certificate Cannot Be Trusted	Since the certificate chain contains a certificate that is not valid, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against it	Purchase or generate a proper SSL certificate for this service
SSL Certificate Expired	The remote server's SSL certificate has already expired	Purchase or generate a new SSL certificate to replace the existing one which was expired
SSL Certificate With Wrong Hostname	The X.509 SSL certificate for this service is for a different host which may be for lin5.ethiotelecom.et	Purchase or generate a proper SSL certificate for this service
SSL Self-Signed Certificate	The X.509 SSL certificate chain for this service ends in an unrecognized self-signed certificate. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host	Purchase or generate a proper SSL certificate for this service
TLS Version 1.0 Protocol Detection	The remote service encrypts traffic using an older version of TLS 1.0 which has several cryptographic design flaws	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0
TLS Version 1.1 Protocol Deprecated	The remote service encrypts traffic using an older version of TLS 1.1 which lacks support for current and recommended cipher suites	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1
Unix Operating System Unsupported Version Detection	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities	Upgrade to a version of the Unix operating system that is currently supported. Debian 8.0 support ended on 2018–06-17 and should be upgraded to Debian Linux 11. x ("Bullseye")

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
SSH Server CBC Mode Ciphers Enabled	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the cipher text	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode
SSH Weak Key Exchange Algorithms Enabled	The remote SSH server is configured to allow key exchange algorithms which are considered weak. The weak key exchange algorithms enabled are: diffie-hellman-group-exchange-sha1 and diffie-hellman-group1-sha1	Contact the vendor or consult product documentation to disable the weak algorithms
Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	The version of Apache running on the remote host is 2.4.x before 2.4.27. It is, therefore, affected by the following vulnerabilities: A denial of service and read-after-free error	Upgrade to Apache version 2.4.27 or later Installed version: 2.4.26 Fixed version: 2.4.27
PHP 7.1.x < 7.1.11 Multiple Vulnerabilities	The version of PHP running on the remote web server is 7.1.x before 7.1.11. It is, therefore, affected by multiple vulnerabilities	Upgrade to PHP version 7.1.11 or later Installed version: 7.1.7 Fixed version: 7.1.11
PHP 7.1.x < 7.1.15 Stack Buffer Overflow	The version of PHP running on the remote web server is 7.1.x before 7.1.15. It is, therefore, affected by a stack buffer overflow vulnerability	Upgrade to PHP version 7.1.15 or later. Installed version: 7.1.7 Fixed version: 7.1.15
PHP 7.1.x < 7.1.26 Multiple Vulnerabilities	The version of PHP running on the remote web server is 7.1.x before 7.1.26. It is, therefore, affected by multiple vulnerabilities including integer underflow, denial of service (DoS), heap-based buffer overflow, heap-based buffer overflow, heap-based buffer over-read, information disclosure, Multiple heap-based buffer over-read, and an out-of-bounds read error	Upgrade to PHP version 7.1.26 or later Installed version: 7.1.7 Fixed version: 7.1.26
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	The version running on the remote host is 2.4.x before 2.4.33. It is, therefore, affected by multiple vulnerabilities including out-of-bounds write, arbitrary file upload, session management, out-of-bounds access, write after free, out-of-bounds read, and weak digest	Upgrade to Apache version 2.4.33 or later Installed version: 2.4.26 Fixed version: 2.4.33
PHP 7.1.x < 7.1.28 Multiple Vulnerabilities	The version of PHP running on the remote web server is 7.1.x before 7.1.28. It is, therefore, affected by multiple vulnerabilities like heap-based buffer over-read and heap-based buffer overflow conditions	Upgrade to PHP version 7.1.28 or later Installed version: 7.1.7 Fixed version: 7.1.28

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
PHP 7.1.x < 7.1.27 Multiple Vulnerabilities	The version of PHP running on the remote web server is 7.1.x before 7.1.27. It is, therefore, affected by multiple vulnerabilities like Uninitialized reads in the EXIF component of PHP, an invalid read in the EXIF component of PHP, and an access control bypass vulnerability	Upgrade to PHP version 7.1.27 or later Installed version: 7.1.7 Fixed version: 7.1.27
PHP 7.1.x < 7.1.29 Heap-Based Buffer Overflow Vulnerability	The version of PHP running on the remote web server is 7.1.x before 7.1.29. It is, therefore, affected by vulnerabilities of a heap-based buffer over-read by which an unauthenticated, remote attacker exploits to cause a denial of service	Upgrade to PHP version 7.1.29 or later Installed version: 7.1.7 Fixed version:7.1.29
PHP 7.1.x < 7.1.30 Multiple Vulnerabilities	The version of PHP running on the remote web server is 7.1.x before 7.1.30. It is, therefore, affected by vulnerabilities like uninitialized and out-of-bounds read vulnerability and a heap-based buffer overflow condition by which an attacker can exploit to cause a denial-of-service condition or the execution of arbitrary code	Upgrade to PHP version 7.1.30 or later Installed version: 7.1.7 Fixed version: 7.1.30
Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	The version of Apache http installed on the remote host is before 2.4.41. so, it is, affected by multiple vulnerabilities including limited XSS by an attacker could cause the link on the error page to be malformed and instead point to a page of their choice	Upgrade to Apache version 2.4.41 or later Installed version: 2.4.26 Fixed version: 2.4.41
Apache < 2.4.49 Multiple Vulnerabilities	The version of Apache http installed on the remote host is before 2.4.49. It is, therefore, affected by multiple vulnerabilities like ap_escape_quotes () may write beyond the end of a buffer when given malicious input and Malformed requests may cause the server to dereference a NULL pointer	Upgrade to Apache version 2.4.49 or later Installed version: 2.4.26 Fixed version: 2.4.49
Apache 2.4.x > = 2.4.7 / < 2.4.52 Forward Proxy Dos / SSRF	The version of Apache http installed on the remote host is equal to or greater than 2.4.7 and before 2.4.52. It is, therefore, affected by a flaw related to acting as a forward proxy So the web server is affected by a denial of service or server-side request forgery vulnerability	Upgrade to Apache version 2.4.52 or later Installed version: 2.4.26 Fixed version: 2.4.52
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	The version of Apache http installed on the remote host is before 2.4.53. It is, therefore, affected by multiple vulnerabilities of buffer overflow and read/write beyond bounds that allow an attacker to overwrite heap memory	Upgrade to Apache version 2.4.53 or later Installed version: 2.4.26 Fixed version: 2.4.53

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
OpenSSL 1.0.2 < 1.0.2ze Vulnerability	The version of OpenSSL installed on the remote host is before 1.0.2ze. It is, therefore, affected by a vulnerability	Upgrade to OpenSSL version 1.0.2ze or later Reported version: 1.0.2l Fixed version: 1.0.2ze
Apache 2.4.x < 2.4.52 Mod_Lua Buffer Overflow	The version of Apache HTTP installed on the remote host is before 2.4.52. It is, therefore, affected by a flaw related to mod_lua when handling multipart content. So, the web server is affected by a buffer overflow vulnerability	Upgrade to Apache version 2.4.52 or later Installed version: 2.4.26 Fixed version: 2.4.52
OpenSSL 1.0.2 < 1.0.2zf Vulnerability	The version of OpenSSL installed on the remote host is before1.0.2zf. It is, therefore, affected by a vulnerability	Upgrade to OpenSSL version 1.0.2zf or later. Reported Version: 1.0.2lFixed version: 1.0.2zf
Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	The version of Apache HTTP installed on the remote host is before 2.4.55. It is, therefore, affected by multiple vulnerabilities like carefully crafted If: and Inconsistent Interpretation of HTTP	Upgrade to Apache version 2.4.55 or later Installed version: 2.4.26 Fixed version: 2.4.55
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	The version of Apache HTTP installed on the remote host is before 2.4.56. It is, therefore, affected by multiple vulnerabilities such as HTTP request splitting	Upgrade to Apache version 2.4.56 or later. Installed version: 2.4.26 Fixed version: 2.4.56
Apache 2.4.x < 2.4.28 HTTP Vulnerability (Optionsbleed)	The version of Apache running on the remote host is 2.4.x before 2.4.28. It is, therefore, affected by an HTTP vulnerability	Upgrade to Apache version 2.4.28 or later. Installed version: 2.4.26 Fixed version: 2.4.28
PHP 7.1.x< 7.1.17 Multiple Vulnerabilities	According to its banner, the version of PHP running on the remote web server is 7.1.x before 7.1.17. It is, therefore, affected by multiple vulnerabilities	Upgrade to PHP version 7.1.17 or later Installed version: 7.1.7 Fixed version: 7.1.17
PHP 7.1.x< 7.1.20 Exif_Thumbnail_Extract() Dos	The version of PHP running on the remote web server is 7.1.x before 7.1.20. It is, therefore, affected by a denial-of-service vulnerability	Upgrade to PHP version 7.1.20 or later Installed version: 7.1.7 Fixed version: 7.1.20
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	The version of Apache running on the remote host is 2.4.x before 2.4.34. It is, therefore, affected by the following vulnerabilities specially crafting HTTP/2 requests, and by specially crafted HTTP requests,	Upgrade to Apache version 2.4.34 or later. Installed version: 2.4.26 Fixed version: 2.4.34
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	The version of Apache running on the remote host is 2.4.x before 2.4.38. It is, therefore, affected by multiple vulnerabilities of A denial of service (DoS) which remote attackers can exploit via sending request bodies in a slow loris way to plain resources and occupy a server thread	Upgrade to Apache version 2.4.38 or later Installed version: 2.4.26 Fixed version: 2.4.38

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
PHP 7.1.x < 7.1.31 Multiple Vulnerabilities	According to its banner, the version of PHP running on the remote web server is 7.3.x before 7.1.31. It is, therefore, affected by buffer overflow vulnerabilities	Upgrade to PHP version 7.1.31 or later Installed version: 7.1.7 Fixed version: 7.1.31
OpenSSL 1.0.2 < 1.0.2za Vulnerability	The version of OpenSSL installed on the remote host is before 1.0.2za. It is, therefore, affected by a vulnerability like ASN.1 strings	Upgrade to OpenSSL version 1.0.2za or later. Reported Version: 1.0.2l Fixed version: 1.0.2za
Apache > = 2.4.17 < 2.4.49 mod_HTTP2	The version of Apache HTTP installed on the remote host is greater than 2.4.17 and before 2.4.49. It is, therefore, affected by a vulnerability like a crafted method sent through HTTP/2	Upgrade to Apache version 2.4.49 or later. Installed version: 2.4.26 Fixed version: 2.4.49
OpenSSL 1.0.2 < 1.0.2zd Vulnerability	The version of OpenSSL installed on the remote host is before1.0.2zd. It is, therefore, affected by a vulnerability like the BN_mod_sqrt() function, which computes a modular square root and contains a bug that can cause it to loop forever for non-prime moduli. Thus, be subject to a denial-of-service attack	Upgrade to OpenSSL version 1.0.2zd or later Reported version: 1.0.2l Fixed version: 1.0.2zd
OpenSSL 1.0.2 < 1.0.2zg Multiple Vulnerabilities	The version of OpenSSL installed on the remote host is before 1.0.2zg. It is, therefore, affected by multiple vulnerabilities of type confusion that may allow an attacker to pass arbitrary pointers to read memory contents or enact a denial of service	Upgrade to OpenSSL version 1.0.2zg or later. Reported Version: 1.0.2l Fixed version: 1.0.2zg
Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	The version of Apache HTTP installed on the remote host is before 2.4.58. It is, therefore, affected by multiple vulnerabilities like mod_macro buffer over-read, Out-of-bounds Read, Apache HTTP Server: DoS in HTTP/2, and Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST	Upgrade to Apache version 2.4.58 or later Installed version: 2.4.26 Fixed version: 2.4.58
OpenSSL 1.0.x < 1.0.2m Rsa/Dsa Unspecified Carry Issue	The version of OpenSSL running on the remote host is 1.0.x before 1.0.2 m. It is, therefore, affected by an unspecified carry vulnerability	Upgrade to OpenSSL version 1.0.2m or later. Reported Version: 1.0.2l Fixed version: 1.0.2m
OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	The version of OpenSSL running on the remote host is 1.0.x before1.0.2n. It is, therefore, affected by multiple vulnerabilities that allow potential recovery of private key information or failure to properly encrypt data	Upgrade to OpenSSL version 1.0.2n or later Reported version: 1.0.2l Fixed version: 1.0.2n
OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities	The version of OpenSSL running on the remote host is 1.0.x before 1.0.2o. It is, therefore, affected by a remote DoS vulnerability	Upgrade to OpenSSL version 1.0.2o or later Reported version: 1.0.2l Fixed version: 1.0.2o

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities	The version of OpenSSL running on the remote host is 1.0.x before 1.0.2p. It is, therefore, affected by a denial-of-service vulnerability and a cache timing side channel vulnerability	Upgrade to OpenSSL version 1.0.2p or later Reported version: 1.0.2l Fixed version: 1.0.2p
PHP 7.1.x < 7.1.22 Transfer-Encoding Parameter XSS Vulnerability	The version of PHP running on the remote web server is 7.1.x before 7.1.22. It is, therefore, affected by a cross-site scripting vulnerability. An attacker could leverage this vulnerability to inject malicious code that executes within the security context of the affected site	Upgrade to PHP version 7.1.22 or later Installed version: 7.1.7 Fixed version: 7.1.22
Apache 2.4.x < 2.4.35 DoS	The version of Apache running on the remote host is 2.4.x before 2.4.35. It is, therefore, affected by the vulnerability of sending continuous SETTINGS frames of maximum size an ongoing HTTP/2 connection could be kept busy and would never time out. This can be abused for a DoS on the server	Upgrade to Apache version 2.4.35 or later Installed version: 2.4.26 Fixed version: 2.4.35
OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	The version of OpenSSL running on the remote host is 1.0.x before 1.0.2q. It is, therefore, affected by a denial-of-service vulnerability and a cache timing side channel vulnerability	Upgrade to OpenSSL version 1.0.2q or later Reported version: 1.0.2l Fixed version: 1.0.2q
OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability	The version of OpenSSL running on the remote host is 1.0.x before 1.0.2r. It is, therefore, affected by an information disclosure vulnerability due to the decipherable way of application responds to a 0-byte record. An unauthenticated, remote attacker could exploit this to potentially disclose sensitive information	Upgrade to OpenSSL version 1.0.2r or later Banner: Reported version: 1.0.2l Fixed version: 1.0.2r
OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	The version of the tested product installed on the remote host is before the tested version. It is, therefore, affected by multiple vulnerabilities of situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted	Upgrade to OpenSSL version 1.0.2t or later Reported version: 1.0.2l Fixed version: 1.0.2t
OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	The version of OpenSSL installed on the remote host is before1.0.2u. It is, therefore, affected by a vulnerability of procedure overflow	Upgrade to OpenSSL version 1.0.2u or later Reported version: 1.0.2l Fixed version: 1.0.2u-dev

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	The version of Apache HTTP installed on the remote host is before 2.4.42. It is, therefore, affected by multiple vulnerabilities of uninitialized memory when proxying to a malicious FTP server. and redirect instead to an unexpected URL within the request URL	Upgrade to Apache version 2.4.42 or later Installed version: 2.4.26 Fixed version: 2.4.42
OpenSSL 1.0.2 < 1.0.2 × Null Pointer Dereference	The version of the tested product installed on the remote host is before the tested version. It is, therefore, affected by null pointer dereference vulnerability	Upgrade to OpenSSL version 1.0.2 × or later Reported version: 1.0.2l Fixed version: 1.0.2x
PHP < 7.3.28 Email Header Injection	According to its self-reported version number, the version of PHP running on the remote web server is before 7.3.28. It is, therefore affected by an email header injection vulnerability by which unauthenticated, remote attackers exploit this to gain full control of email header content	Upgrade to PHP version 7.3.28 or later Installed version: 7.1.7 Fixed version: 7.3.28
OpenSSL 1.0.2 < 1.0.2zc-Dev Vulnerability	The version of OpenSSL installed on the remote host is before1.0.2zc-dev. It is, therefore, affected by a vulnerability like carry propagation bug	Upgrade to OpenSSL version 1.0.2zc-dev or later. Reported Version: 1.0.2l Fixed version: 1.0.2zc-dev
OpenSSL 1.0.2 < 1.0.2zh Multiple Vulnerabilities	The version of OpenSSL installed on the remote host is before 1.0.2zh. It is, therefore, affected by multiple vulnerabilities that lead to a denial-of-service (DoS) attack on affected systems	Upgrade to OpenSSL version 1.0.2zh or later. Reported Version: 1.0.2l Fixed version: 1.0.2zh
OpenSSL 1.0.2 < 1.0.2zi Vulnerability	The version of OpenSSL installed on the remote host is before 1.0.2zi. It is, therefore, affected by a vulnerability like Issue summary	Upgrade to OpenSSL version 1.0.2zi or later. Reported Version: 1.0.2l Fixed version: 1.0.2zi
OpenSSL 1.0.2 < 1.0.2zj Vulnerability	The version of OpenSSL installed on the remote host is before1.0.2zj. It is, therefore, affected by a vulnerability of Issue summary angina	Upgrade to OpenSSL version 1.0.2zj or later. Reported Version: 1.0.2l Fixed version: 1.0.2zj
HTTP Trace / Track Methods Allowed	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. So here the vulnerability enabled Debugging functions on the remote web server	Disable these HTTP methods
JQuery 1.2 < 3.5.0 Multiple XSS	The version of JQuery hosted on the remote web server is greater than or equal to 1.2 and before 3.5.0. It is, therefore, affected by multiple cross-site scripting vulnerabilities	Upgrade to JQuery version 3.5.0 or later Installed version: 1.12.4 Fixed version: 3.5.0

Table 3 (continued)

Vulnerability	Impact On the Security of Cyber Infrastructure Description	Mitigation Solution
OpenSSL 1.0.2 < 1.0.2w Information Disclosure	The version of OpenSSL installed on the remote host is 1.0.2 before 1.0.2w. It is, therefore, affected by a vulnerability. The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections that have used a Diffie-Hellman (DH) based cipher suite. So, the remote service is affected by an information disclosure vulnerability	Upgrade to OpenSSL version 1.0.2w or later. Reported Version: 1.0.2l Fixed version: 1.0.2w
OpenSSL 1.0.2 < 1.0.2y Multiple Vulnerabilities	The version of the tested product installed on the remote host is the before-tested version. It is, therefore, affected by multiple vulnerabilities	Upgrade to OpenSSL version 1.0.2y or later. Reported Version: 1.0.2l Fixed version: 1.0.2y
Web.Config File Information Disclosure	An information disclosure vulnerability exists in the remote web server due to the disclosure of the web. config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information	Ensure proper restrictions are in place, or remove the web. config file if the file is not required
SSL Medium Strength Cipher Suites Supported	The remote host supports the use of SSL ciphers that offer medium-strength encryption	Reconfigure the affected application, if possible, to avoid the use of medium-strength ciphers
Smtp Service Cleartext Login Permitted	The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used	Configure the service to support less secure authentication mechanisms only over an encrypted channel

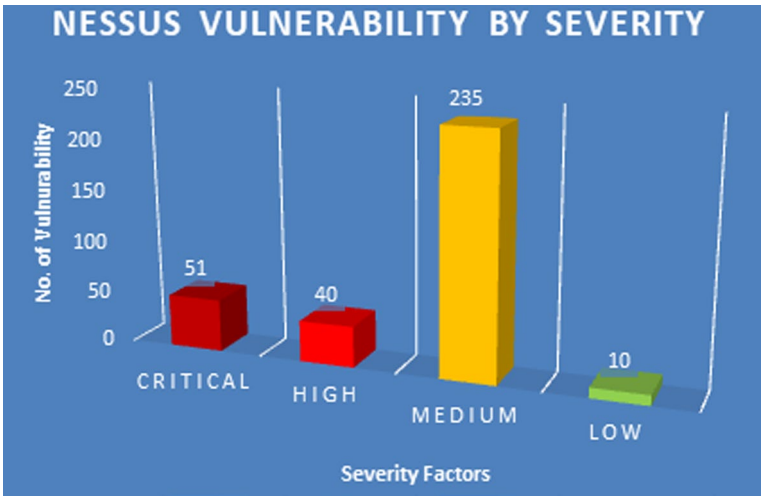


Fig. 13 Nessus vulnerability by severity

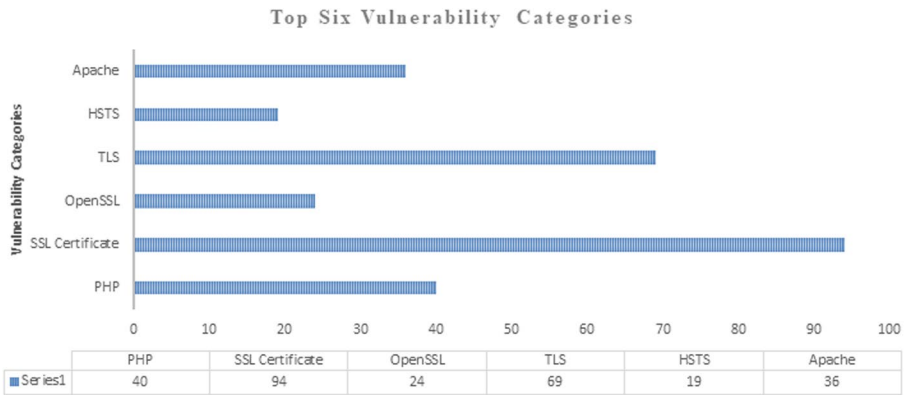


Fig. 14 Top Six Vulnerability Categories

In terms of severity, most of the identified vulnerabilities fall under the medium severity category, which could lead to significant cybersecurity breaches over time. The top five institutions with the most vulnerability are Woldia, Wollo, DebreTaboor, and Mekele University. The most critical vulnerabilities are found on Hawassa, with one each in Addis Ababa, Woldia, and Mekdela Amba. In terms of high-severity vulnerabilities, Hawassa leads as shown in Fig. 13.

According to the tendencies of the most redundantly occurred vulnerabilities type, the top six categories are illustrated as shown in Fig. 14. SSL certificate category consists of vulnerabilities like self-signed, untrusted, expired certificates, and certificates with the wrong hostnames. Those vulnerabilities lead the cyber systems to carry out man-in-the-middle attacks. Those vulnerabilities happened in almost all institutions examined here except ASTU. TLS category is also the second redundantly vulnerable in almost all institutions except AASTU. Vulnerabilities under this category are Version usage of Version 1.0 and 1.1 which are currently expired versions or do not have new updated patches supported by vendors. Those vulnerabilities cause the institutions to have flawed cryptographic designs for their cyber infrastructures.

The PHP category vulnerability has existed in all institutions except AASTU. Most of those vulnerabilities are due to unsupported web application scripting language (PHP) and improper handling of CR-LF sequences. This causes the institutions to be affected by multiple vulnerabilities including integer underflow, denial of service (DoS), heap-based buffer overflow, heap-based buffer over-read, information disclosure, and email header injection

The Apache-related vulnerabilities happened on Hawassa which is due to the Version being unsupported and having no updated patch security supported by the vendor. This causes the institution to be affected by multiple vulnerabilities including denial of service, read-after-free error, cross-site scripting, out-of-bounds write, arbitrary file upload, out-of-bounds access, write-after-free, out-of-bounds read, and weak digest

The remote web server is not enforcing HSTS, as defined by RFC 6797 [37] is the sixth top vulnerability that happened on almost all institutions except AASTU. This HSTS is a response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, and SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. As a result, the remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

Vega provides vulnerabilities by categorizing them under high, Medium, Low, and Informal as per their impact and complexity over the target host's cyberspace confidentiality, integrity, and availability.

As presented in Table 2, Vega vulnerability assessment held up on the selected 16 public University websites reports 11,286 total findings. From those results, 6, 431 (57% of the total) findings are informational those illustrate the overall secrets of the respective web applications. The informational findings detected by Vega assessment include Blank body, unspecified character set, Error HTTP, Meta Tags, unfixed X-frame header, unfixed cookie HTTP only and secure flag, uploaded form files, possible AJAX code, etc. This information gives important directions for cybercrime intruders/hackers. This implies with this type of information delivery of the web applications; all institutions are fully vulnerable to being attacked by cyber criminals (unethical hackers). The rest 4,855 (43% of the total) findings are the current vulnerabilities of the cyber infrastructures for those institutions following their risk severity level of which 20.68% are High, 4.9% are Medium, and 74.4% are Low.

As shown in Figure 15 and Table 2, the top four vulnerable institutions with highly severe labeled vulnerability cyber issues are WLDU, WU, AAU, and AASTU which cover 35.06%, 5.88%, 8.07%, and 49.2% respectively.

The highly severe cyber defects detected by Vega assessment in this study include cross-site scripting, shell injection, SQL injection, Bash "Shell Shock" injection, session Cookie without HTTP Only Flag and secure flag, clear text Password over HTTP, insecure cross-origin Resource Access control, page Finger print differential, Possible Social Security number, etc.

The top three frequently detected vulnerabilities in a high number of web applications are cross-site scripting, Injection (SQL, Shell, and shellshock), Session Cookie without HTTP Only and Security flag (/), and Clear Text Password over HTTP which is depicted in Figure 16.

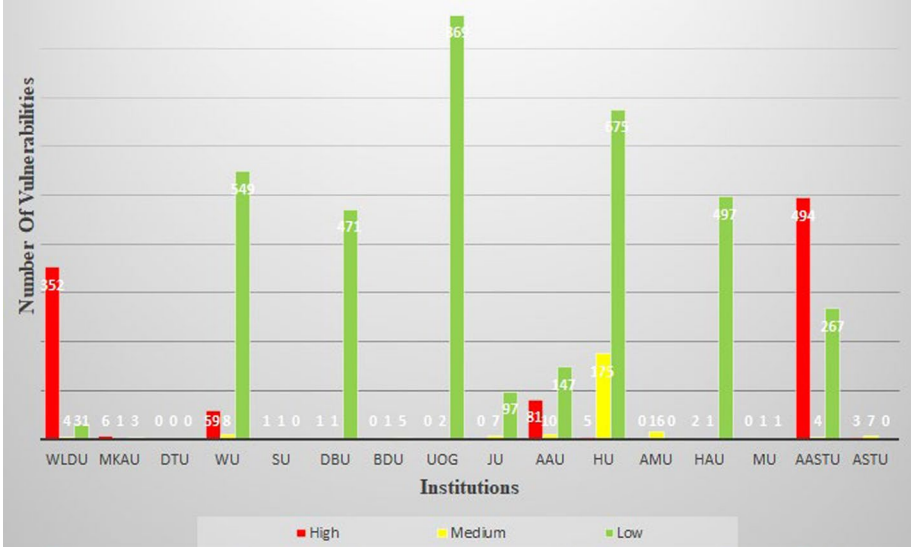


Fig. 15 Number of Vulnerabilities as per Institutions

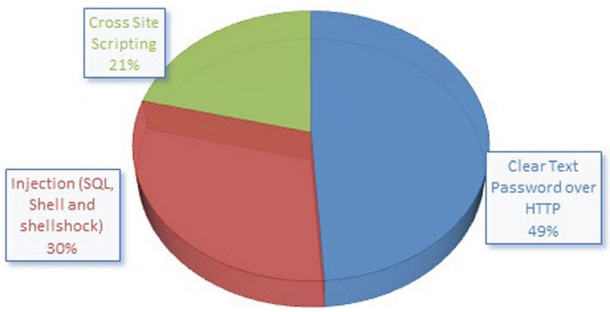


Fig. 16 Top three vulnerabilities detected

As in the pie graph of Figure 16 of highly severe detected vulnerabilities, Clear Text password over HTTP covers 49% of vulnerabilities which are ranked first. Of those vulnerabilities, all 100% are detected from www.aastu.ed.et and the second-ranked Injection vulnerability has 30% coverage of all high-risk vulnerabilities from which 76.08% are shell Shock injections detected from Woldia. 38.21% of the third-ranked vulnerability which is cross-site scripting are detected from Addis Ababa.

Vega's vulnerability assessment reveals that the web applications S. No. 11, 12, and 10 are the most susceptible, accounting for 73.22%, 6.69%, and 4.2% of all identified medium-risk vulnerabilities. These vulnerabilities include the local file system and its path, potential HTTP PUT files, possible source code exposure, HTTP Trace server type (Apache/2.4.26 (Win32), and PHP errors. The local file system path vulnerability is the most common across all investigated web applications. This vulnerability is sensitive as it can disclose server environment details to an attacker, thereby increasing the success rate of blind attacks. The second most common vulnerability is the PHP error page signature, which can leak sensitive information such as software patch levels, configuration settings, and database or file system structure.

In terms of low-level severe risk vulnerabilities, Vega's assessment identifies UOG, HU, WU, HAU, and DBU as the top five vulnerable web applications, covering 24.06%, 18.06%, 15.2%, 13.76%, and 13.04% respectively. The most common vulnerabilities in this category include email addresses, internal addresses, Autocomplete password fields, and Directory listing. The most frequent vulnerability is the discovery of internal addresses. These are references to internal hosts or networks found in publicly accessible content. Such addresses can disclose information about the internal network structure to an attacker, thereby increasing the likelihood of successful blind attacks involving other vulnerabilities. It can also expose the internal network structure, including Internal IP addresses, to external attackers.

In general, university websites are the most important gateways of cybercrimes due to their ubiquitous behavior and accessibility by all members and outsiders throughout the world. Highly ranked cyber-secured and highly accessible infrastructure has a great impact on the University's reputability in Worldwide computation ranks. As described in the findings of the above assessments using survey and VAPT techniques University websites are vulnerable to cybercrimes in numerous ways including missed patch management, missed firewall support port and other service management, cross-site scripting, SQL injections, and the like. In this study, we have conducted vulnerability assessment and penetration testing simply to reconnaissance the vulnerabilities and report the findings as a research output.

The results found in the above investigations assured that all of the investigated Universities are vulnerable at least with one type of vulnerability. This result also indicates the need for further vulnerability assessments should be performed and mitigation policies should be designed by the responsible administrators of the respective institutions to safeguard their cyberspaces from unethical hackers. Cyber security vulnerability investigation is a proactive defensive mechanism as it plays a significant role by simulating intruders to reconnaissance vulnerable defects from cyberspace. The output of vulnerability assessment is used for protecting cyber infrastructures before unethical hackers act on them.

Proposed counter measure mitigation solutions

For the respective key findings identified by the study as listed above, the countermeasures designed and proposed for those who want to tackle the issues are illustrated as follows. Those countermeasure mitigation solutions are developed based on: ISO-IEC-27001 standard guidelines.

Awareness development of cyber professionals

According to the National Institute of Standards and Technologies (NIST) [38], training of cyberspace professionals is the vehicle for disseminating cyber security information for establishing and maintaining a robust and relevant countermeasure upon the vulnerabilities confronted. NIST also considers cyber security awareness training as an escapable program rather it being one part of the overall cyber security program. This training is conducted for all levels of personnel to provide awareness about the information itself, services needed to protect, and overall responsibilities of protecting the organization's cyberspaces they are belonging from cyber criminals.

The steps that you have used to develop awareness for cyber professionals begin by evaluating the present cybersecurity expertise of your IT personnel. Next, create a thorough training curriculum covering the fundamental ideas, dangers, and best practices of cybersecurity. Update this program often to handle new threats and technological advancements. Making sure the training curriculum is current and interesting enough to promote learning is the biggest obstacle. It might be difficult to locate resources or trainers with the necessary qualifications. Also, Make use of internet tools and platforms that provide cybersecurity education. Involve the students in interactive lessons, practical applications, and hands-on activities.

In multiple respects, our study is consistent with the ISO/IEC 27001 series of standards. Firstly, the guidelines provided in ISO/IEC 27001 serve as the foundation for our risk assessment methodology. The ISO/IEC 27001 risk assessment process's essential elements—assets, threats, vulnerabilities, impacts, likelihoods, and risk levels have all been identified.

Second, by following the guidelines in ISO/IEC 27001's Annex A, the vulnerabilities found in our analysis can be mitigated. For example, inadequate access control was one of the vulnerabilities we found. The controls from ISO/IEC 27001 for user access management (A.9.2) and access control policy (A.9) can be used to address this.

Furthermore, our results are consistent with other relevant cybersecurity standards. For example, by following the encryption specifications outlined in the NIST cybersecurity framework, the vulnerability associated with insecure communications can be reduced.

Patch management

Vendor-unsupported outdated versions of cyber security services are patches without use. This can be the reason for individual hackers to have ways for making unauthorized access, modify and disrupt the whole cyberspace, and use critical information for unethical activities like accessing registrar information to change students' grades and finance information to theft money and the like. Since instances of this type of vulnerability are large in number, it is difficult to put it here.

Make a list of all the systems and software that are currently in use to start. Collect information on vulnerabilities and patches that are available regularly. Examine these patches in light of appropriateness and grant them deployment permission. Before patching, test the updates in a safe environment. It can be very difficult to keep track of all the systems, software, and patches that are related to them. Hence, to expedite the process, make use of automated patch management technologies.

Avoiding open ports from cyber spaces

According to the findings of Nmap scanning as in chapter four, all institutions are vulnerable to being attacked by cybercriminal intruders easily through the available open ports. Therefore, the mitigation solution for such types of vulnerabilities is performing a similar type of scanning by the administrators of the respective cyber spaces by sending SYN packets. After receiving the SYN+ACK packet for the request from the target resend the RST signal for the target. Immediately the open port makes itself a closed port. Another way of protecting the open ports is to make them be governed by firewall

policies of the respective cyberspace which means making them to be filtered state. It can be difficult to strike a balance between minimizing open ports and preserving essential functionality. So, Establish stringent guidelines requiring a reason to be given for maintaining a port open. Make sure these defenses are still sound by reviewing them regularly.

HSTS enforcement

HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. Make sure your website can be accessed via HTTPS first. Next, set up your server so that every response includes the HSTS header. The lack of HSTS allows downgrade attacks, and SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. The remote web server is not enforcing HSTS, as defined by RFC 6797. As a result, the remote HTTPS server does not send the HTTP "Strict-Transport-Security" header. The mitigation solution for such type of vulnerability is configuring the remote web server to use HSTS. Your site may stop working due to misconfiguration. Before deploying the configuration, give it a thorough test in a safe environment.

XSS, injections, and clear text password over HTTP and others

Descriptions and respective mitigation solutions for those vulnerabilities are described in Table 4.

Conclusion

The study aimed to explore the vulnerabilities of cyberspace on cybercrime in 16 selected public universities, focusing on their web pages. The awareness of cyberspace professionals regarding these vulnerabilities was evaluated through a questionnaire-based survey conducted in sixteen of the sampled universities. The study employed VAPT assessment tools to scrutinize the vulnerabilities of the websites.

The findings indicated that all the university websites were critically vulnerable to cybercrime breaches in one way or another. The VAPT assessment revealed that the key issue was the outdated patch implementations on their servers, a fact confirmed by the survey respondents. Other significant findings included the widespread presence of XSS, Injections, and Clear text Passwords over HTTP, along with numerous open ports. These threats pose a high risk of causing the respective University websites to crash due to an aggressive cybercrime intruder exploiting these identified vulnerabilities or any other means unless the responsible stakeholders take action.

Finally, the importance of stakeholder engagement in cybersecurity efforts cannot be overstated. By involving university administrators, IT staff, policymakers, and the academic community, a collaborative approach to establishing more robust cybersecurity infrastructures can be advocated.

Recommendations

Based on the findings identified by this study, those examined University websites are at risk ON cybercrime vulnerabilities unless the responsible respective officials strongly act upon them. If so, before starting their actions, we recommend there to plan and start

Table 4 The descriptions and mitigation of those vulnerabilities over the remote host cyber infrastructures

Vulnerability	Description	Mitigation Solutions
Cross-Site scripting	Is a class of vulnerabilities affecting web applications that can result in security controls implemented in browsers being circumvented. Its vulnerabilities occur when a lack of input validation permits users to inject script code into the target website such that it runs in the browser of another user who is visiting the same website. This would circumvent the browser's same-origin policy because the browser has no way to distinguish authentic script code from inauthentic, apart from its origin	• The developer must identify how the untrustworthy data is being output to the client without adequate filtering
SQL injection	These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintended actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application	• The best defense against SQL injection vulnerabilities is to use parameterized statements • The use of stored procedures can simplify complex queries and allow for tighter access control settings • Object-relational mapping eliminates the need for SQL
Shell Injection	These command injection vulnerabilities often occur when inadequately sanitized externally supplied data is as part of a system command executed through a command interpreter, or shell. These vulnerabilities can grant remote access to attackers if exploited successfully	• Execution of system commands through a command interpreter, such as with system(), should be avoided • If necessary, the developer should take extra care with validating the input before it is passed to the interpreter
Shellshock Injection	This vulnerability may manifest itself remotely in web applications if user-supplied input is passed to the Bash shell environment, which can occur if header or parameter values are converted to local environment variables. If successfully exploited, this vulnerability may lead to command execution on the underlying host	• The bash shell should be upgraded on the affected host. This can often be done through the package management system, such as apt or yum • Execution of system commands through a command interpreter, such as with system(), should be avoided • If necessary, the developer should take extra care with validating the input before it is passed to the interpreter
Session Cookie Without httpOnly and Security flag (/)	When this flag is not present, it is possible to access the cookie via client-side script code. The HTTP Only and security flags are security measures that can help mitigate the risk of XSS attacks that target the session cookies of the victim. If the HttpOnly/security flag is set and the browser supports this feature, the attacker-supplied script code will not be able to access the cookie	When creating the cookie in the code, set the HttpOnly and security flags to true
Clear Text Password over HTTP	Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in the unauthorized disclosure of passwords to passive network attackers	Passwords should never be sent over cleartext. The form should be submitted to an HTTPS target

by reconnaissance their cyberspace infrastructure defects with the methods we use here or by designing any appropriate method for their own. Even recommend our findings as a startup for optimizing the respective cyber security as per the standards of ISO-IEC-27001 series.

Furthermore, since things are dynamically changing in the cases of cyberspace security, those examined Universities even any related organization's cyber infrastructures shall be overcoming their skill and alert cyber professionals by delivering short-term and long-term training on the overall cyberspace issues.

Lastly, we recommend those Universities or any related institutions, before starting the deployment of websites for implementations, should have strongly examined the basic agendas of cyber security vulnerabilities based on the checkpoints of the respective standards. After deployment, the responsible administrators should follow everything in the cyberspaces specifically, the vendor-supported patch management with serious and committed taskforces.

Acknowledgements
Not applicable.

Author contributions
Ali Yimam Eshetu: Conceptualization, Methodology, Software, Performed the experiment, Visualization, Writing- Original draft preparation. Endris Abdu Mohammed: Investigation, Methodology, Visualization. Ayodeji Olalekan Salau: Data curation, Formal analysis, Methodology and Writing- Reviewing and Editing, Validation.

Funding
Authors declare no funding for this research.

Availability of data and materials
The datasets generated during and/or analyzed during the current study are not publicly available but are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate
Approval has been obtained from the Woldia University Research, Publication and Ethics Review Board.

Competing interests
The authors declare that they have no competing interests.

Received: 13 January 2024 Accepted: 6 August 2024
Published online: 23 August 2024

References

1. Deriba FG, Salau AO, Mohammed SH, Kassa TM, Demilie WB. Development of a compressive framework using machine learning approaches for SQL injection attacks. Przeglad Elektrotechniczny. 2022;7(1):181–7. https://doi.org/10.15199/48.2022.07.30.
2. Mitsarakis K. Contemporary cyber threats to critical infrastructures: management and countermeasures 2023, https://repository.ihu.edu.gr/xmlui/handle/11544/30295. Accessed Jan 11 Jan 2024.
3. Chinese Academy of Cyberspace Studies, Improving capacity of cyber security safeguarding, in china internet development report 2017, Chinese academy of cyberspace studi, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 101–130. https://doi.org/10.1007/978-3-662-57521-5_6.
4. Hemberg E et al., Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting. arXiv, Feb. 10, 2021. http://arxiv.org/abs/2010.00533. Accessed 11 Jan 2024.
5. Rajangam B, Alagarsamy M, Radhakrishnan CR, Assegie TA, Salau AO, Quansah A, Chowdhury NM, Chowdhury IJ. Security-based low-density parity check encoder for 5G communication. Bull Electr Eng Inform. 2024;13(4):2707–15. https://doi.org/10.11591/eei.v13i4.7019.
6. Balasubramanian K, Web application vulnerabilities and their countermeasures, in cryptographic solutions for secure online banking and commerce, IGI Global, 2016, pp. 209–239. https://www.igi-global.com/chapter/web-application-vulnerabilities-and-their-countermeasures/153499. Accessed 21 Nov 2023.
7. Sardar R, Anees T. Web of things: security challenges and mechanisms. IEEE Access. 2021;9:31695–711.

8. R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, IEEE, 2015, pp. 119–134. Accessed: Nov. 21, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7158473/
9. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks | journal of cyber security and mobility. https://journals.riverpublishers.com/index.php/JCSANDM/article/view/6087. Accessed Nov 21 Nov 2023.
10. Applied sciences | free full-text | an integrated cyber security risk management approach for a cyber-physical system. https://www.mdpi.com/2076-3417/8/6/898. Accessed: Nov. 21, 2023.
11. Kryshtanovych M, Kozlovskiy Y, Chubinska N, Huzii I, Lukashevska U, Ensuring cybersecurity for higher educational institutions, in *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, IEEE, 2021, pp. 183–186. https://ieeexplore.ieee.org/abstract/document/9772173/. Accessed 19 Apr 2024.
12. Gandikota PSSK, Valluri D, Mundru SB, Yanala GK, Sushaini S. Web application security through comprehensive vulnerability assessment. Proc Comput Sci. 2023;230:168–82.
13. Chancusi A, Diestra P, Nicolalde D. Vulnerability analysis of the exposed public IPs in a higher education institution. in Proceedings of the 2020 10th International Conference on Communication and Network Security, 2020, pp. 83–90. https://doi.org/10.1145/3442520.3442523.Accessed 19 Apr 2024.
14. Salau AO, Assegie TA, Akindadelo AT, Eneh JN. Evaluation of Bernoulli Naive Bayes model for detection of distributed denial of service attacks. Bull Electr Eng Inform. 2023;12(2):1203–8. https://doi.org/10.11591/eei.v12i2.4020.
15. Gill SH, et al. Security and privacy aspects of cloud computing: a smart campus case study. Intell Autom Soft Comput. 2022;31(1):117–28.
16. Abomhara M, Køien GM. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mobil. 2015;4(1):65–88.
17. Dioubate BM, Norhayate WDW, Anwar ZF, Fauzilah S, Faiz HM, Hai LO. The role of cybersecurity on the performance of malaysian higher education institutions. Jurnal Pengurusan. 2023;67:1–12.
18. Harrell CR, Patton M, Chen H, Samtani S, Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions, in *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, 2018, pp. 148–153. https://ieeexplore.ieee.org/abstract/document/8587380/. Accessed 19 Apr 2024.
19. Dioubate BM, Daud WN. A Review of cybersecurity risk management framework in Malaysia Higher Education Institutions. Int J Acad Res Bus Soc Sci. 2022;12(5):1031–93.
20. Cheng EC, Wang T. Institutional strategies for cybersecurity in higher education institutions. Information. 2022;13(4):192.
21. Alhumud TAA, Omar A, Altohami WMA. An assessment of cybersecurity performance in the Saudi universities: a total quality management approach. Cogent Educ. 2023;10(2):2265227. https://doi.org/10.1080/2331186X.2023.2265227.
22. Ulven JB, Wangen G. A systematic review of cybersecurity risks in higher education. Future Internet. 2021;13(2):39.
23. Singar AV, Akhilesh KB, Role of Cyber-security in Higher Education. in *Smart Technologies*, K. B. Akhilesh and D. P. F. Möller, Eds., Singapore: Springer Singapore, 2020, pp. 249–264. https://doi.org/10.1007/978-981-13-7139-4_19.
24. Meharu M, Web security vulnerability analysis in selected Ethiopian governmental offices (using white box and black box testing)," PhD Thesis, St. Mary's University, 2022. http://repository.smuc.edu.et/handle/123456789/7079. Accessed 20 Apr 2024.
25. Differentiating the higher education system of Ethiopia,... - Google Scholar. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Differentiating+the+Higher+Education+System+of+Ethiopia%2C+A+National+Study+&btnG. Accessed 18 Dec 2023.
26. Taherdoost H. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics. 2022;11(14):2181.
27. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments. Boca Raton: CRC Press; 2021.
28. Aquino Cruz M, Huallpa Laguna JN, Huillcen Baca HA, Carpio Vargas EE, and Palomino Valdivia FDA. Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division," in *Advances in Emerging Trends and Technologies*, vol. 1302, M. Botto-Tobar, O. S. Gómez, R. Rosero Miranda, and A. Díaz Cadena, Eds., in Advances in Intelligent Systems and Computing, vol. 1302. , Cham: Springer International Publishing, 2021, pp. 264–272. https://doi.org/10.1007/978-3-030-63665-4_21.
29. Alhamed M, Rahman MH. A systematic literature review on penetration testing in networks: future research directions. Appl Sci. 2023;13(12):6986.
30. Pate K. A survey on vulnerability assessment & penetration testing for secure communication. in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2019, pp. 320–325. Accessed: Dec. 19, 2023. https://ieeexplore.ieee.org/abstract/document/8862767/
31. Mell P *et al.* Measuring the common vulnerability scoring system base score Equation. National Institute of Standards and Technology, Gaithersburg, MD, 2022, Accessed: Dec. 19, 2023. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=935413
32. Altulaihan EA, Alismail A, Frikha M. A survey on web application penetration testing. Electronics. 2023;12(5):1229.
33. Ahmad S, Wasim S, Irfan S, Gogoi S, Srivastava A,Farheen Z. Qualitative v/s. quantitative research-A summarized review. *population*, vol. 1, no. 2, 2019, Accessed: Dec. 22, 2023. https://www.academia.edu/download/104933106/Sharique_Ahmed_--_FINAL.pdf
34. Salau AO, Marriwala N, Athaee M. Data Security in Wireless Sensor Networks: Attacks and Countermeasures, Lecture Notes in Networks and Systems, Vol. 140. Springer, Singapore, pp. 173–186, 2021. https://doi.org/10.1007/978-981-15-7130-5_13
35. Everson D, Cyber attack surface mapping for offensive security testing, 2023, Accessed: Dec. 22, 2023. [Online]. Available: https://tigerprints.clemson.edu/all_dissertations/3259/
36. Cirnu CE, Rotună CI, Vevera AV, Boncea R. Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. Stud Inf Control. 2018;27(3):359–68.

37. Srivastava A and Shah P. Identification of the issues in IoT Devices with HSTS Not Enforced and Their Exploitation," in *2021 International Conference on Security and Information Technologies with AI, Internet Computing and Big-data Applications*, vol. 314, G. A. Tsihrintzis, S.-J. Wang, and I.-C. Lin, Eds., in Smart Innovation, Systems and Technologies, vol. 314. , Cham: Springer International Publishing, 2023, pp. 325–334. https://doi.org/10.1007/978-3-031-05491-4_33.
38. Safitri EHN and Kabetta H, Cyber-risk management planning using NIST CSF V1. 1, ISO/IEC 27005: 2018, and NIST SP 800–53 Revision 5 (A Study Case to ABC Organization), in 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), IEEE, 2023, pp. 332–338. https://ieeexplore.ieee.org/abstract/document/10277652/. Accessed 24 Dec 2023

Publisher's Note