Journal of Applied Sciences, Information and Computing

Volume 4, Issue 1, July 2023

ISSN: 1813-3509 https://doi.org/10.59568/JASIC-2023-4-1-06

IDENTIFICATION AND MITIGATION OF THE VULNERABILITY OF WEB APPLICATIONS IN INSTITUTIONS OF HIGHER EDUCATION

[1]Sabo Muhammed, [2]Muwanga Zake, [3]V.S. Manjula, [4] Auwal Saleh

[1]Department of Information Technology and System, Kampala International University, Uganda.
sabo.muhammed@kiu.ac.ug
[2]Department of Information Technology and System, School of Mathematics and Computing, Kampala International University, Uganda. Zake.muwanga@kiu.ac.ug
[3]Corresponding Author, Professor in the Department of Computer Science, School of Mathematics and Computing, Kampala International University, Uganda.Manjusunil.vs@gmail.com,
Orcid ID: (0000-0003-0308-3289)
[4]Department of Computer Science, Binyaminu Usman Polytechnic Hadejia. Jigawa State, Nigeria. auwalus6@gmail.com

Abstract

The security of information technology, specifically web applications, has become an area of concern today. Computer cybercrime is now a significant problem that affects more than just businesses and organizations. Higher education institutions also began to experience computer threats that revealed their information assets. Universities, polytechnics, colleges of education, research centers, and other postsecondary institutions are probably the most vulnerable because they house sensitive data on their faculty, staff, and students, as well as academic records of scientific and technological advancements and research. The first step in an information system security strategy is risk analysis management It helps in assessing the risk of information assets to know their security level or status, and assist in define a security control measures and implementation of technical plan to avoid threats that exploit some vulnerability that could cause severe damage to an asset or infrastructure of institutions higher education (IHEs). This article presents some recommendations to perform a risk analysis management in IHEs to accessed threats and vulnerability that helps to lower the risk of their information assets. This article presents existing educational threat and vulnerability on their web applications. Ensuring security is a goal of every organization regardless of its size or purpose and also proposed a risk management model. With the information technology, an organization may be considered secure when it ensures the confidentiality, integrity, and availability of information and IT assets. Confidentiality may be broken due to theft of sensitive information such as trade secrets, clients' personal information.

Keywords: web application, vulnerabilities, threats, risk analysis; higher education institutions

1. Introduction

According to Georgescu (2020), a web application is a program that runs on a remote server and is accessed via the internet using a browser interface. Web applications have evolved from being static to dynamic information stores into highly functional programs that process data and execute command-and-control actions with tangible consequences. Web applications, however, are vulnerable to a variety of attacks. Institutions of Higher Education in particular, adopt resources in web applications for varied functions including but not limited to learning, management and administrative. Learning processes, for example, are hosted in webs for classes, independent work of students to find information on varied study topics. In order to manage, integrate, access, evaluate, and analyse digital resources, web applications technology should be used to increase awareness, knowledge, and skills (Huang, Hood & Yoo, 2013). According to Faizi (2018), by taking advantage of the chance to control their education using these online tools, students can effectively establish interactive learning environments. It also says that students can learn outside of the classroom and school setting thanks to the creativity and initiative of this new digital technology. These online resources have expanded and produced rich learning environments on a worldwide scale. The communication or collaboration between those who instruct and those who are being taught (Aşıksoy, 2 018). Web application 2.0 technologies have the ability to improve communication, problem-solving, and self-regulation skills, as evidenced by the review literature (e.g., Ianos & Brezeanu, 2020). Related research has also shown that web application tools improve kids' auditory qualities, learning, and skills while also making a significant contribution to student-teacher parent interactions (e.g. Özpınar, 2020). It is said that web application-based learning environments give every student the chance to succeed. Because web-based learning incorporates online course content, it is sometimes referred to as online learning or e-learning. Kıyıcı and Özer (2 017). Discussion forums via email, videoconferencing, and live lectures (video streaming) are all possible through the web. An example web-based is the Learning Management System (LMS) that online instructors can use to create, host, deliver and sell online courses. An example web-based is the Learning Management System (LMS) lecturers can able to use learning management system to create, host, deliver and sell online courses. An LMS is one of best web application usually used by academic institutions to support teaching and learning. Examples of institutions of higher education that use LMS include Sule Lamido University, Federal University Dutse in Jigawa State, Nigeria and Kampala International University in Uganda.

1.1 Background of the Study

This research focuses in the assessment of vulnerability for web application of Institutions of higher education. Modern Institutions that adopted new technology in their mode of operation which are conducted through the web application for pastor and efficient performance among staff and student, the web application has provide platform where customer apply for admission while students are registered on the registration platform and process their tuition fees payment, also enhance collaborate with their lecturers for learning and sharing academic resources and taking online exam through the web application but all activities cannot be achieved successful without taking measures to ensure the safety of web application by identifying the weakness of the in term of vulnerability assessment. As online learning has become a key delivery channel for education and training, it is important to secure your learning management system by identifying and remediating vulnerabilities. This assessment must be carried out by higher education institutions. However, vulnerability assessment is an ongoing process where new vulnerabilities are discovered due to outdated software versions or after configuration changes.

https://doi.org/10.59568/JASIC-2023-4-1-06

The objective to identify security weakness of web applications with regards to threats and vulnerability, propose a risk analysis model for mitigation and management. With the following specific objectives.

1. To identify threats and vulnerability against web applications in Institution of Higher Education,
2. To make risk analysis of the vulnerabilities.
3. Design a model for vulnerability risk management of web applications.

2. Review of Literature

2.1 Education Information Systems

Higher education institutions are typically settings or places where people exchange knowledge, conduct research, and receive instruction. But there is a ton of official, private, and restricted data and information held by IHEs and the organizations that are affiliated with them that needs to be safeguarded. Against Theft or Disclosure of Critical or Confidential Information Could Cause Financial, Property, and Reputational Damage. Customer information, intellectual property, financial and legal documents, and correspondence are just a few of the many procedures, resources, and data that can be safely stored in IHE. There are many important areas that need to be protected, such as:

• The unit under education and research development, which includes data on test results, exam results, intellectual development, research and development, student information, research projects, etc.

• Human Resources (data on staff and students, personal data, reports, etc

Legal (internal records, agreements, private worker or employee information, even following their voluntary retirement or contract termination at the conclusion of their service term, etc.)

• Under the heading of economic and financial records (procurement records, financial data, payroll records, inventory records, etc.)

• Records of information technology infrastructures, including their setup, IT management data, passwords and login information, databases, and copyright information on IT innovations, among other things.

The improved use of information and its evolving nature have made reforms within IHEs more accountable and require them to follow strict guidelines in order to guarantee the confidentiality, availability, and integrity of their information systems. IHE is compelled by numerous factors to create a security plan in order to safeguard the IT resources that underpin their operations, including.

• There are new opportunities for teaching, learning, and research thanks to new technologies such as digital libraries, wireless computing, virtual learning environments, and portal software;

• Higher quality services, particularly in terms of IT systems and knowledge, are required from university administration, employees, and users.

• There is a growing need to create complex models and make initial IT investments in infrastructure to guarantee that IS are resilient and adaptable to meet changing requirements as IT and information systems continue to become intricately woven into many IHE activities and processes.

•It is becoming more challenging for management to guarantee that investments in security controls are in line with institutional objectives due to the growing complexity of IS, their information technologies, and their interrelationships.

2.2 Web Applications for Institutions of Higher Education

Web applications used by higher education institutions typically include a variety of software and tools designed to support teaching, learning, research, and administrative functions. Here are some common examples:

1. Higher education institutions frequently use learning management systems (LMS) to administer and deliver online courses, course materials, assignments, assessments, and student communication. Examples of LMS platforms are Canvas, Blackboard, and Moodle. Higher education institutions frequently use the Canvas Learning Management System (LMS) web application to manage online courses, assignments, discussions, and assessments. With features like grading, attendance tracking, multimedia content integration, and collaboration tools, it offers an intuitive interface

https://doi.org/10.59568/JASIC-2023-4-1-06

that is easy for both teachers and students to use (Instructure, 2021).

2. Blackboard Learn is another popular web application used by higher education institutions for creating and managing online courses. It offers tools for content creation, assessment, communication, and student engagement, along with integration options for third-party applications. Blackboard Learn also provides analytics and reporting features for tracking student progress (Blackboard, 2021).

3 .Plagiarism detection tools: Turnitin is a popular web application used in higher education institutions to check for originality and prevent plagiarism in student papers and assignments. Turnitin is a web application used in higher education institutions for checking plagiarism in student assignments and providing feedback on writing. It helps educators ensure academic integrity and provides tools for originality checking, grading, and peer review. Turnitin also offers features for collaborative writing and feedback, as well as integration with learning management systems (Turnitin, 2021).

4. Survey and research tools: Qualtrics, SurveyMonkey, and Google Forms are web applications commonly used by higher education institutions for conducting surveys, collecting data, and conducting research among students, faculty, and staff. Qualtrics is a web application used for conducting surveys and collecting data in higher education institutions. It offers a wide range of survey question types, customization options, and reporting features for analysing survey results. Qualtrics also provides tools for data visualization, statistical analysis, and advanced survey logic (Qualtrics, 2021).

5. Productivity and collaboration tools: Email, collaboration, document creation, and communication between teachers, staff, and students are all done with Google Workspace for Education (formerly G Suite for Education), Microsoft Office 365, and other productivity tools. Higher education institutions frequently use the Google Workspace for Education suite of online tools, which includes Google Docs, Sheets, Slides, and Drive, for file storage, document creation, and collaboration. It provides real-time editing, commenting, and sharing features, along with integration options for other Google tools such as Google Classroom and Google Meet (Google, 2021).

6. Tools for virtual meetings and video conferences: Zoom, Microsoft Teams, and Google Meet are popular online programs used by academics, staff members, and students for webinars, virtual meetings, and online collaboration. In higher education institutions, Zoom is a popular web application for online meetings and video conferencing. It has features like screen sharing, chat, re cording options, and audio and video conferencing. Zoom is commonly used for virtual classrooms, online lectures, and collaborative group discussions, and also provides integration options with learning management systems (Zoom, 2021).

7. Online library resources: Many higher education institutions provide access to web applications for online library resources, such as such as databases, journals, ebooks, and other research tools, to support scholarly research and academic writing. Online learning resources: Web applications such as Khan Academy, Coursera, and edX provide online learning resources, courses, and tutorials for students, faculty, and staff to enhance their knowledge and skills.

8. Khan Academy is a free web application that offers educational resources and interactive learning modules for various subjects. It provides video lessons, practice exercises, and assessments for students at different grade levels, and also offers personalized learning paths and progress tracking features. Khan Academy is widely used by higher education institutions as a supplemental learning tool (Khan Academy, 2021).

3.3 Need to manage vulnerabilities of web application

Maintaining the security of an organization's information systems requires the use of vulnerability management. It entails locating, evaluating, ranking, and addressing vulnerabilities in the network, hardware, and software infrastructure of the company. Effective vulnerability management can help prevent security breaches, data loss, and other security incidents that can be costly for organizations. Several reports and studies have emphasized the need for vulnerability

https://doi.org/10.59568/JASIC-2023-4-1-06

management in organizations. For instance, a Ponemon Institute study discovered that companies able to put vulnerability management programs in place were able to cut the risk of a data breach by half. (2017) Ponemon Institute.

A cyber-attack transpires when an intruder compromises security measures surrounding a material or digital asset. According to their origin and state, we classify cyberattacks as follows:
Both Passive and Active Assaults An "active" attack seeks to modify or interfere with the functionality of system resources. On the other hand, a "passive" attack aims to obtain data from a system without causing any harm to the system's resources (IETF 2007). Passive attacks, on the other hand, seek to gather information for an offline attack. For instance, hackers frequently use packet analysis and inspection to make it easier to examine security protocols offline and improve exploits.

3.4 Inside and Outside Attacks

In contrast, unauthorized or illegitimate users initiate "outside" attacks outside the security perimeter. Outsider attackers include hackers, organized criminal groups and States. The attack On the other hand, "outside" attacks are carried out by illegitimate or unapproved users beyond the security perimeter. Hackers, states, and organized crime are examples of external attackers. The assault We can also classify attacks based on where they originate. An "Inside Attack" is defined by the Internet Security Glossary as one that is started by an entity types are not mutually exclusive as outsiders often rely on insider. Because more people are using online and mobile applications, cyberattacks are happening on a daily basis. Over 70% of applications globally have vulnerabilities that hackers could exploit or, in the worst case scenario, have already exploited, according to statistics. In this context, there are two main categories of data loss. Either an organization or an individual considers data to be confidential. No matter the category, losing data means losing money or ruining one's reputation (Prashant, 2017). Cybercrime is a category of criminal activity that takes place on computers, the Internet, and cyberspace. Cybercrime is now a widespread issue as our society transforms into an information society where communication occurs online. Cybercrime has the capacity to profoundly affect society, the economy, and our daily lives (Josephine, 2021). A cyber pandemic was also brought about in 2020, the year of the pandemic. Threats and attacks have multiplied dramatically and have gotten more sophisticated. Given that there is an attack every 39 seconds and 2,244 times a day on average, security becomes a top priority for businesses of all sizes (Josh, 2021). Businesses are expected to spend over $1 trillion on cybersecurity between 2017 and 2021, according to Cybersecurity Ventures, and more malware will be released than ever before. Since 2013, security breaches have resulted in the theft of 3,809,448 records every day. 158,727 per hour, 2,645 per minute, and 44 every second of the day are reported by Cybersecurity Ventures (University, 2021).

3.5 The OWASP

The OASP is a widely recognized resource for web application security threats and countermeasures, and it provides a comprehensive list of vulnerabilities that web developers and administrators should be aware of. There are several potential loopholes or vulnerabilities that educational institution web applications may have. Here are a few examples: It may be simpler for attackers to access the application if users select weak or simple passwords or use the same password for several accounts.

The web application might make use of plugins or out-of-date software with known vulnerabilities. Attackers may use these flaws to obtain unauthorized access to the system or do other damage. Users might be granted more access rights than is necessary, which raises the possibility of misuse or illegal access to data.
Inadequate security testing: Regular security testing, such as vulnerability scanning and penetration testing, may not be performed on the web application, which could result in vulnerabilities going unidentified and un fixed. Social engineering techniques, like phishing

https://doi.org/10.59568/JASIC-2023-4-1-06

emails or phone calls, can be used by attackers to fool users into disclosing private information or into doing other things that could jeopardize the application's security.

It is crucial that educational institutions locate these weaknesses and vulnerabilities and fix them with suitable security measures, like frequent security testing, user education, access controls, and password policies. Risk analysis of web application

Risk analysis is a crucial component of web application security since it aids in the identification and ranking of the risks connected to an organization's web applications. The following steps are commonly included in the risk analysis process:
Finding the web application's assets, such as its data, hardware, software, and network infrastructure, is the first step. Finding potential web application threats, such as malware, hacking, social engineering, or other attacks, is the next stage.

Assess vulnerabilities: The next stage after identifying the threats is to evaluate the web application's vulnerabilities that these threats might exploit. It is possible to estimate the chance of a successful attack by looking at the threats and vulnerabilities that have been found. Finding out what would happen in the event of a successful attack—such as data loss, financial loss, or reputational harm to the company—is the next stage.

Prioritize risks: The organization can prioritize the risks and create a plan to mitigate them based on the likelihood and impact of the risks. Put risk management techniques into practice: Lastly, to lessen the possibility and effect of hazards that have been identified, the company can put risk management techniques into practice, such as security controls, policies and procedures, and employee training.
Web application risk analysis can be carried out using a variety of frameworks and tools, such as the OWASP Risk Assessment Methodology, ISO/IEC 27001, and the NIST Cybersecurity Framework.

3. METHODOLOGY STRIDE MODEL:

A framework for recognizing and classifying possible risks to web applications is the STRIDE model. Six categories of threats are taken into account by the STRIDE model: denial of service, spoofing, tampering, repudiation, information disclosure, and elevation of privilege. According to Shostack (2014), "A useful framework for recognizing and classifying possible risks to web applications is the STRIDE model.
Zero Trust Model: The Zero Trust model is a framework that assumes every request to access a resource could be malicious, thereby lowering the risk of web application vulnerabilities. Forrester Research (2021) has pointed out.
NIST Cybersecurity Framework: One well-known framework for controlling cybersecurity risk is the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). A set of best practices and guidelines for recognizing, evaluating, and controlling cybersecurity risk—including risk related to web applications—are included in the framework. NIST Cybersecurity Framework is the source.
ISO/IEC 27001: This standard offers a structure for creating, putting into practice, preserving, and continuously enhancing an information security management system (ISMS). Guidelines for performing risk assessments of web applications and other information assets are included in the standard. According to ISO/IEC 27001**,**
OWASP Risk Assessment Methodology: An organized method for carrying out risk analyses of web applications is offered by the Open Web Application Security Project (OWASP) Risk Assessment Methodology. The methodology offers a scoring system for risk prioritization along with instructions on identifying assets, threats, vulnerabilities, and impacts. (Source: Methodology for OWASP Risk Assessment) In addition to these sources, there are many other resources available for conducting risk analysis of web applications, including industry-specific guidelines, regulatory frameworks, and best practices developed by security professionals and organizations. Organizations must periodically assess and update their risk analysis procedures to make sure they continue to be effective in the face of changing vulnerabilities and threats.

https://doi.org/10.59568/JASIC-2023-4-1-06

Propose Model The term "design model" typically refers to a structured framework, methodology, or approach that guides the design process, providing a systematic way to conceptualize, plan, and execute design projects. It serves as a roadmap for designers, helping them organize their ideas, make informed decisions, and achieve desired design outcomes. When a design model is accompanied by a citation, it means that the proposed approach is based on existing research, literature, or empirical evidence. The citation provides the design model with legitimacy and credibility by demonstrating that it is based on accepted knowledge or industry best practices. Citations strengthen a design model's academic or professional rigor, validate the validity and dependability of the suggested approach, and enable others to confirm and cite the original source for additional information. Fitzpatrick and Kånåhols (2019) provided the source. Designing with Humans in Mind for Sustainable Packaging: A Case Study. International Journal of Sustainable Packaging, 1(1), 1-12.r information or research. The propose model is a contribution by researcher after careful review of the three Model and frame work, to come with a model that will identify and mitigate vulnerability of web application for institutions of higher education. The vulnerability risk and management model, this will put organisation one foot step ahead of attacker or hacker in exploitation of organisational information resources and IT Infrastructure especially in the area under study institutions of higher education.

The Risk management process involves:

- The following steps are involved in the risk management process:
- Choosing controls to lessen the risks noted in the risk assessment view.
- Formalization of the hazards noted in the context of the risk assessment.

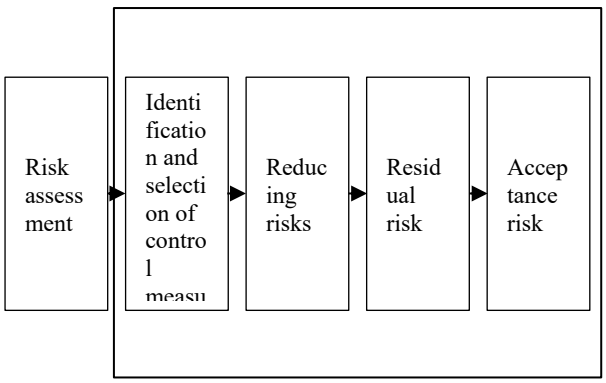

Fig. 3.1 Risk management Proces

The propose develop model for risk management process in IHE as a guide to reduce or control the risk.

Research Design

The study's research design is thoroughly described by the researcher. The process of choosing a method for a given research problem, maximizing its advantages while minimizing its disadvantages is known as research design. Plans and procedures for research that range from general hypotheses to specific techniques for gathering and analyzing data are known as research designs (Creswell 2013).

Table 1: Vulnerability Risk Management Analysis Assets

ASSETS
Human Resources
Activities
Information
Facilities
Equipment

Population of Study

This study is not an exception to the rule that every research process has a population that the study is conducted upon. The term "population" describes every person residing in a certain area. Bello (2009) defined population as a group that the researcher is interested in studying in order to make inferences. Population is defined as a well-defined collection of individuals or objects known to have similar characteristics. The research population of this study comprised of primary (IT professional) Administrators, Managers, Directors, (MIS Department) and secondary (the three higher institutions) population. The primary population of the study consisted of all IT professional staff in Institutions of Higher Education under study. The researcher used all the professional IT staff of Institutions of Higher Education in Jigawa State, Nigeria. The researcher based his population upon those indicates the Vulnerability assessment of Institutions of Higher Education. These are, Sule Lamido University Kafin Hausa

https://doi.org/10.59568/JASIC-2023-4-1-06

had 45, College of Education Gumel 30 and Binyaminu Usman Polytechnic Hadejia which had 25 IT Professional staff, all these 100 staff would serve as primary population of the study while the three Institutions of Higher Education would serve as secondary population of the study.

Table 2: Shows the population of the study:

S/N	Name of the Institutions	Identification and Mitigation of Vulnerability web application in IHE	Professional ITStaff
1	SLU KHS, JIG	Available and opr	45
2	GOEC, JIG	Available and opr	30
3	BUPOLY, JIG	Available and opr	25
	Total		**100**

Sampling Method A sampling method is a device employed in the selection of representative members, objects or elements from a given population. The target population of this study comprises all the professional IT staff of three Institutions of Higher Education in Jigawa State, Nigeria. That is composed of 100 IT professional staff. These are considered capable of providing the required information. Purposive sampling will be used by the researcher to examine the entire population of interest, for instance, a group whose members are all interested in the same thing. The sample size for the study will be determined by using a comprehensive enumeration of a well-defined subgroup within the larger population. According to Laurakas, P. (2008), a purposive sample is one in which a representative sample of the entire population is chosen for the study.

4. RESULT AND DISCUSSION

Questions and Answers from the Survey

To ensure that respondents were qualified professionals for the survey, two questions were included in the instrument: Question 1, "What is your current role within the organization?" and Question 2, "How many years have you been in IT security?" The CEO, Director/Manager, and Pen Tester/IT Security were the typical roles held by the respondents. Every respondent had worked in IT security for at least five years..

Table 3: Respondents Response Rate

Administered Questions	Frequency	Percentage %
Questionnaire	100	100%
Retrieved	93	93%
Not retrieved	7	7%
Total	**100**	**100%**

Table 4: Current Role in Institutions ICT Department

Current role in Institution ICT Department

		Percentage of Frequency	Percent (%)	Valid Percent	Total Percent
Valid	Pen tester / Web master	5	5.4	5.4	5.4
	IT Auditor / Analyst	21	22.6	22.6	28.0
	IT Manager / Director	12	12.9	12.9	40.9
	CIO / CTO / CEO	23	24.7	24.7	65.6
	ICT Staff	32	34.4	34.4	100.0
	Total	93	100.0	100.0	

Table 4: Shows the categories of respondents in IHE that answer the questionnaire.

https://doi.org/10.59568/JASIC-2023-4-1-06

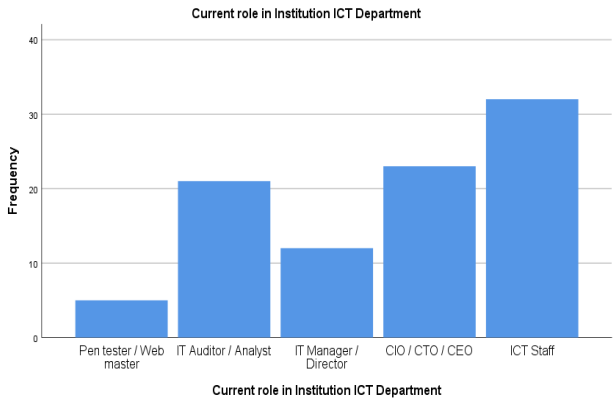

Figure 1: Threats Identified in Institutions Web Application

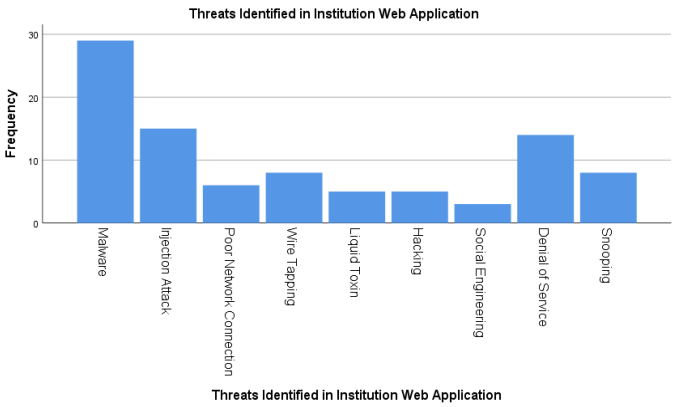

Figure 2: Vulnerability Identified in Institutions Web Application

Threats Identified in Institution Web Application

		Frequency	Percentage of Frequency	Percent (%)	Valid Percent	Total Percent
Valid	Malware	29	31.2	31.2	31.2	
	Injection Attack	15	16.1	16.1	47.3	
	Poor Network Connection	6	6.5	6.5	53.8	
	Wire Tapping	8	8.6	8.6	62.4	
	Liquid Toxin	5	5.4	5.4	67.7	
	Hacking	5	5.4	5.4	73.1	
	Social Engineering	3	3.2	3.2	76.3	
	Denial of Service	14	15.1	15.1	91.4	
	Snooping	8	8.6	8.6	100.0	
	Total	93	100.0	100.0		

Table 5: Shows some of the threats identified in Institution of higher education from the survey result.

Vulnerability Identified in Institutions Web Application

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Lack of software patching	17	18.3	18.3	18.3
	Erro in software code	20	21.5	21.5	39.8
	Poor configuration	5	5.4	5.4	45.2
	Broken access control	26	28.0	28.0	73.1
	Weak password	8	8.6	8.6	81.7
	Expire certificate	17	18.3	18.3	100.0
	Total	93	100.0	100.0	

Table 6: Shows the result of some of the vulnerability found in institution of higher education.

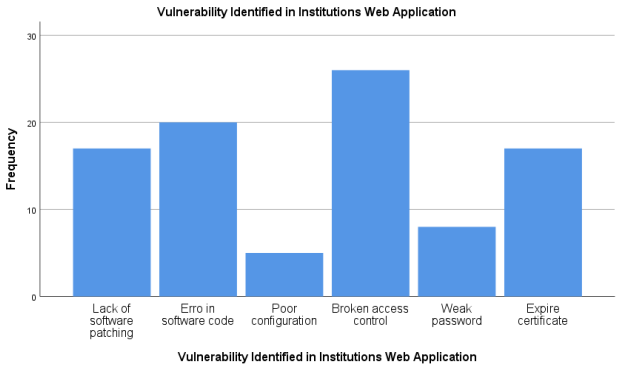

Figure 3: Institutions Preferred Vulnerability Software

https://doi.org/10.59568/JASIC-2023-4-1-06

Institutions Preferred Vulnerability Software					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Rapid7	10	10.8	10.8	10.8
	Qualys guard vulnerability	22	23.7	23.7	34.4
	IBM security apps scan	2	2.2	2.2	36.6
	Tenable nessus vulnerability	43	46.2	46.2	82.8
	Burp suite pro	3	3.2	3.2	86.0
	Cenzic	4	4.3	4.3	90.3
	Saint vulnerability scan	5	5.4	5.4	95.7
	Back track	4	4.3	4.3	100.0
	Total	93	100.0	100.0	

Table 7: Shows the result of Institutions Preferred Vulnerability Software

The above result shows that IHE about 46.2% are using Tenable Nessus vulnerability scanner because of its performance and functionality, while others use Qualys guard vulnerability about 23.7% IHE. For assessing vulnerability in their web Applications.

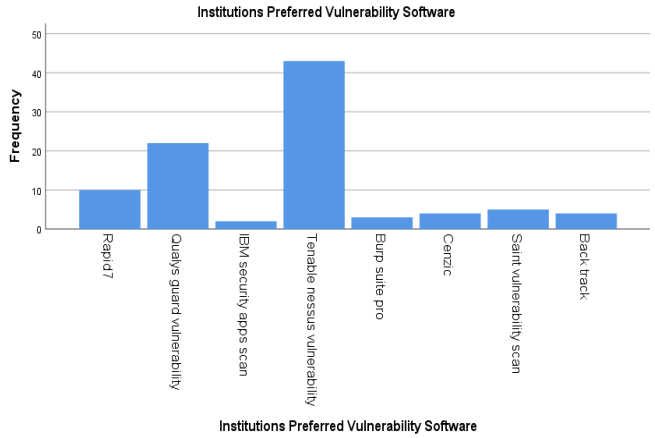

Figure 4: IHE Critical Assets and impact level

Assets in Institutions of Higher Education		
Facilities	File servers	Personal records of employees and student
Administrative offices	Websites	Electronic files
Labs	Repositories	Tangible records
Website	Created software programs	Emails account
Network infrastructure	Desktop units	Research
Web host	Individual computers	Agreements for collaboration
Servers for databases	Specialized machinery	Agreements
Mail server	Cards of report	Statements of finances

Table 8: Show the crucially important component in IHE.

Table 9: IHE Threats Scenario:

https://doi.org/10.59568/JASIC-2023-4-1-06

Earthquake Flood Power Interruption Blackmail Extortion Stole Fraud Riot Sabotage	Threat	Unauthorized Access Social Engineering Malicious code Spoof Denial of service Cracking passwords Data Modification	Threat	Community Ex employee Hacker Material (failure) Natural Subversive group Internal staff discontent Inexperienced staff Discontent Inexperienced staff internal staff Provider	Threat Agent

Table 9: Show the internal and external threat scenario associated to IHE.

Table 10: OWASP Scoring guide:

Probability and Effect Sizes	
0 to <3	**LOW**
3 to <6	**MEDIUM**
6 to 9	**HIGH**

Table 10: Show the scoring guide adopted on this paper to access the impact level best on quantitative and qualitative data analysis.

Table 11: IHE Risk Matrix

		Threat Level		
Impact	Expe	Medium Risk 6	High Risk 8	Critical Risk (Unacceptable) 9
	Migh	Low Risk (Acceptable) 3	Medium Risk 5	High Risk 7
	Unlik	Low Risk (Acceptable) 1	Low Risk (Acceptable) 2	Medium Risk 4
		Low	**Medium**	**High**

Table 11: Risk matrix showing the threat impact level to IHE.

https://doi.org/10.59568/JASIC-2023-4-1-06

Table 12: IHE Overall impact level

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall impact = 7.25 (High)					**Overall business impact = 2.25 (Low)**			

Table 12: Show the validation of result to the overall impact level to IHE.

Table 13 and 14 Describe the mitigation techniques and control measures in how to be implemented to reduce data breach in IHE.

Threats	Management Process on Functions and safeguards				
	Identity	**Protect**	**Detect**	**Respond**	**Recover**
Out of memory	- Inventory of IT system	-Autoscaling instances. -Increase instances sizes	-Infrastructure monitoring alert on memory usage to trigger incident	-Develop ops pipeline redeploys with new instance size.-Restart machine	-Charge configuration setting to account for this threat
SQL Injection	-Identify web page which required user input.	-Sanitized input fields -Use cases which used SQL attacks. WAF/RASF	-SAS/DAST Scanners -IDS Alert	-Block bad user accounts -Turn off API	-Post mortem -Backup
Insider Threat	-List of users with Admin privileges	-Require two-person approval	-Log privileged activities	-Contact Security -Remove user access	-Legal Investigation

STRIDE LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Pretending to be someone or something	Robust authentication methods and the street of authentication

https://doi.org/10.59568/JASIC-2023-4-1-06

T	Tampering	Access and Integrity Controls	Changing code or data	Digital watermark/isolation, access controls, and crypto hash
R	Repudiation	Non-refusal	Denying having carried out a particular action	Infrastructure logging, complete packet capture
I	Information Disclosure	Confidentiality	Revealing data or information to uninvited parties or roles	Isolation or Encryption
D	Denial of service	Accessibility	Refuse or lower the level of service quality	Throttling of bandwidth, redundancy, QoS, and failure
E	Elevation of privilege	Permission / Minimal Privilege	Acquire skills without proper authorization	MAC, RBAC, DACL, Sudo, UAC, and protected privileged accounts
LM	Lateral movement	Segmentation / Least *privilege*	Increase power after a concession, frequently requiring an increase in privilege	Firewalls with hose bases, segmentation, and boundary enforcement, and credential hardening.

Table 13 : Intuitions of Higher Education Control

5. CONCLUSION

The study suggests procedures that, if put into practice, would increase productivity in higher education institutions by lowering data breaches and enhancing information availability, confidentiality, and integrity as well as web application security controls. The suggested model will make it possible to identify risks, vulnerabilities, and threats more effectively. The model specifically suggests a risk analysis model for management and mitigation.

5. REFERENCES

[1]Alexander, J. (2021). Risk, Threat, or Vulnerability? How to Tell the Difference. Retrieved from Kenna Security: https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

[2]Arslan, Kevser, and Fatma Coştu. "Web 2.0 Applications in the Teaching Process: A Swot Analysis." Shanlax International Journal of Education, vol. 9, no. 4, 2021, pp. 460–79. DOI: https://doi.org/10.34293/education.v9i4.4238

[3]Bhatia G, e. a. (2021). Vulnerability Assessment and Penetration Testing. International Journal of Engineering Research & Technology (IJERT), 167-172.

[4]Blackboard. (2021). Blackboard Learn. Retrieved from https://www.blackboard.com/teaching-learning/learning-management/blackboard-learn

[5]Botler, V. (2021). How to setup OWASP ZAP to scan your web application for security vulnerabilities. Retrieved from Triad: National Institute of Standards and Technology (NIST), Gaithersburg, Maryland.

[6]Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, & mixed approaches. London, UK: Sage. Instructure. (2021). Canvas Learning Management System

https://doi.org/10.59568/JASIC-2023-4-1-06

(LMS). Retrieved from https://www.instructure.com/canvas/

ISO/IEC 27001: ISO/IEC 27001 is an international standard for information security management systems (ISMS)

[7]ISO/IEC (2008) ISO/IEC 27005: Information Technology — Security Techniques — Information Security Risk Management, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), Geneva, Switzerland.

[8]ISO (2009) ISO 31000: "Risk Management - Principles and Guidelines, International Organization for Standardization (ISO), Geneva, Switzerland",ITU (2008a) ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat, Geneva.

[9]NIST. (2020). Computer Security Incident Handling Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://doi.org/10.59568/JASIC-2023-4-1-06