Migration Letters

Volume: 20, No: S8(2023), pp. 1252-1262

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

Analysis of Risks and Vulnerabilities in a University-Level LMS System

Janeth Mora Secaira[1], Raúl Díaz Ocampo[2], Eduardo Samaniego Mena[3]

Abstract
The growing development of LMS (Learning Management System) in higher education institutions raises several among which is the increase in security problems that affect confidentiality, integrity and availability in information systems. Therefore, it has become necessary to identify vulnerabilities in these systems to ensure information security. It is essential to use vulnerability scanners to examine the security of web applications.
In this article, we present the results obtained through the analysis method, Open Web Security Project (OWASP), which focuses on identifying risks while providing information on probability and technical impact; will need a reliable value judgment at a quantitative and qualitative level, regarding the vulnerabilities of the Academic Management System (SGA) platform of the State Technical University of Quevedo (UTEQ) of Ecuador, and conclude with security recommendations on the protection of relevant information from the actors involved in this process, in the university context.

Keywords: *Analysis of risks, vulnerabilities, university-level LMS system.*

1. INTRODUCTION

Higher Education Institutions (HEIs) are complex organizations and, as such, need to manage the information they generate. Computer science and telecommunications are the tools that support the management of organizations' information systems. LMS is defined as a teaching system that makes use of internet technologies to provide multiple solutions that improve knowledge and performance [1] and [2]. In addition, the following definition is proposed: "It is an idea of learning through digital connections and peer-to-peer collaboration, facilitated by Web applications. Users - students now have the ability to search, create and collaborate, with the aim of completing a series of needs to obtain or learn new information" [3] [4]. By virtue of this, LMS (also called e-learning) have characteristics such as: interactivity, flexibility, scalability, standardization, usability and functionality[5] .

A learning platform, or LMS, is software usually installed on a web server (it can be installed on an intranet), which is used to create, approve, administer, store, distribute and manage virtual training activities (it can be used as a complement to face-to-face classes or for distance learning) [6],[7] and today they play a major role in the educational context. In addition, with the latest events that have occurred worldwide and in the face of

[1] Universidad Técnica Estatal de Quevedo, Ecuador, E-mail: jmora@uteq.edu.ec, ORCID: https://orcid.org/0000-0001-9405-2028
[2] Universidad Técnica Estatal de Quevedo, Ecuador, E-mail: rdiaz@uteq.edu.ec, ORCID: https://orcid.org/0000-0002-8264-8614
[3] Universidad Técnica Estatal de Quevedo, Ecuador, E-mail: esamaniego@uteq.edu.ec, ORCID: https://orcid.org/0000-0002-6196-2014

the social distancing measures implemented by the COVID19 pandemic, they have become popular in their use and accessibility by students and teachers [8].

However, these platforms can be subject to vulnerabilities due to many information security issues such as: social engineering, computer viruses, phishing, malvertising, pharming, and SQL injection; that if they are not attended to in a timely and adequate manner, they could be the cause, in the worst case, of the destruction of information [9].

Information systems (IS) security is the protection against unauthorized access to information or modification of information. Protection should cover storage, processing, and transmission [10]. Information security consists of 3 elements [11] and [12]:

- Confidentiality: Information accessible only to those authorized to receive it
- Integrity: No unauthorized modification of information is permitted
- Availability: Information can be accessed in all circumstances permitted by the information security policy

Threats or risks are realized through one or more vulnerabilities in information systems. Among the main threats are: breach of confidentiality, breach of integrity, denial of service, illegitimate use, malware, repudiation, masking, traffic analysis, brute force attack [13] and [14]. The information that is handled in E-learning is generally confidential and therefore requires protection from attacks and threats that may affect the right to intimacy, privacy and protection of student data, these services use applications that are supported in multimedia systems of video, voice and data over the internet protocol (IP)[9].

E-learning education can be seen as an innovative approach to bring well-designed, student-centered and interactive instruction, which can be delivered to anyone, place and time, using the ICT (Information and Communication Technology) attributes of an E-learning platform It is an online work environment where resources are shared to work remotely or in a blended way, which must have minimum tools for its operation [15], divided into the following categories:

- Content tools: (Allow the instructor to publish and distribute course materials.)
- Communication and collaboration tools: (Forums, chat rooms and internal course messaging).
- Monitoring and evaluation tools (Design exams, publish assignments, generate reports of each student's activity, provide feedback to the student on their performance).
- Admin tools: (Create groups, accept students, and give privileges.)
- Complementary tools: (Course content search systems, add applications).

Due to the massive growth of LMSs derived from the pandemic situation, it is necessary to analyze the different vulnerabilities and attacks that these systems are exposed to[8]. A vulnerability is a weakness in an IT asset that can be exploited by a threat and cause damage to the availability, integrity, and confidentiality of that asset[16].

In addition, vulnerability scanners can be used to examine the security of web applications, and there are many studies in the literature that compare the detection capabilities of these tools. Open Web Application Security Project OWASP Zed Attack Proxy (OWASP ZAP) is a free dynamic vulnerability scanning tool, in this active scanning search policies are applied that can be configured by the user or you can simply use the default policies that do a complete scan of the web applications for vulnerabilities.

It is important to take into account the recommendations of the (OWASP). It is possible to identify the most common vulnerabilities in websites and propose some alternative solutions to mitigate these vulnerabilities, design and develop secure web applications [17].

The Open Web Application Security Project (OWASP), an organization that provides information for risk management in computer application security, published the top 10 of the most common vulnerabilities in 2021, they are as follows [18]:

Table 1. Top 10 threat categories according to OWASP 2021

#	Vulnerability Categories
1	A01: Remote Access Control
2	A02: Cryptographic Failures
3	A03: Injection
4	A04: Unsafe Design
5	A05: Security Misconfiguration
6	A06: Vulnerable and Obsolete Components
7	A07: Identification and Authentication Failures
8	A08: Data and Software Integrity Failures
9	A09: Security Monitoring and Logging Failures
10	A10: Server-Side Request Forgery

Source: Owasp, 2021

In the case of our experience, the academic management platform (SGA), was designed to help communication between teachers and students, it has different tools, such as uploading learning resources, files, calendars, forums and creating online learning communities. The tool is accessed through the virtual classroom, the platform has been improved and adjusted to teaching needs, having introduced changes in the format and content from the administration unit of the educational platform of the UTEQ. In recent years and mainly during the pandemic, the use of the WMS platform has increased exponentially.

Table 2 shows the categorization of risk levels according to OWASP 2021, to detail the impact and its respective description.

Table 2. Risk levels according to OWASP 2021

Risk Level	Description
Loud	Vulnerability that, if exploited, would compromise information security, causing a negative impact on EMS. It needs to be fixed immediately
Stocking	Vulnerability that, if exploited, would have a slight impact on the operations of the EMS
Casualty	A vulnerability that, if exploited, would not cause major inconveniences
Informative	Warnings and/or recommendations that alert you to possible configurations that can be improved. They have very little impact on the operation of the applications

Source: Authors' Elaboration

Academic web applications are hosted on server 1, where users can access them via the internet or intranet. The operating system of the servers is CentOS 7. These web applications are developed with Python and have a database implemented in Postgresql, to store the information. (source: SGA Academic Management System)

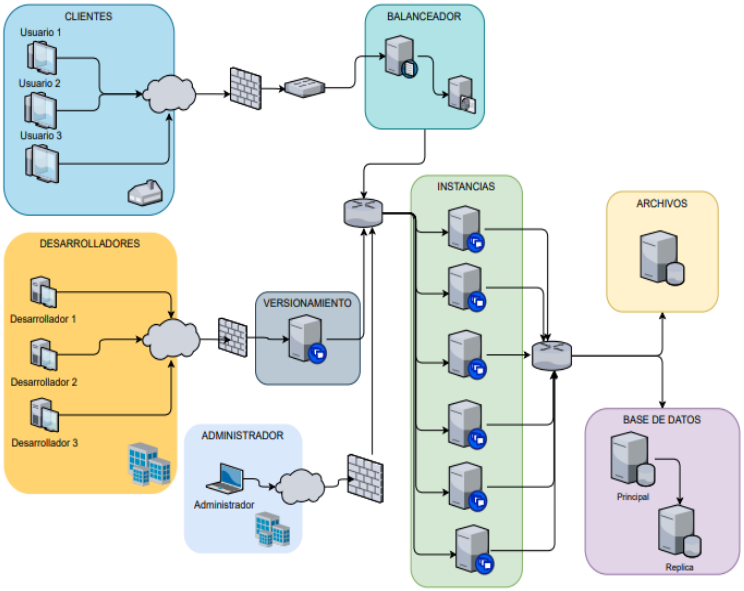


Figure 1: Diagram of the structure of the EMS - UTEQ

Source: (GHS, 2022)

2. MATERIALS AND METHODS

The research methodology is based on mixed qualitative and quantitative analysis. The application of the OWASP 2021 web security testing guide makes it possible to identify and fix vulnerabilities within configurations in web applications, considering computer security factors. The current situation of the SGA platform of UTEQ (Ecuador) is taken as a case study.

The application of the OWASP guide will be used to analyze possible attacks and establish in terms of security at what levels the Web application is, where vulnerabilities can be identified and prevented, both in the type of: injection, information collection, server security and browsing rules in the web platform, to minimize and mitigate security threats [19].

3. RESULTS AND DISCUSSION

The OWASP ZAP tool is used, according to the structure shown in Table 3, in the first column of this Table the dimensions are indicated: injection, information collection, server security and scan rules, then the detected vulnerabilities are presented, classifying them in the following columns according to the 3 principles of information security (availability, integrity and confidentiality).

Table 3. Dimensions and vulnerabilities according to the principles of information security

Dimension	Vulnerability	Availability	Integrity	Confidentiality
Injection	Cross-site scripting		*	
	String Formatting Error		*	
	SQL Injection Failure		*	

	Cache control policies		*	*
	Vulnerable JS Library		*	
Collection of Information	Cookie without the same site attribute		*	*
	Cookie without a secure flag			
	Directory Browsing	*	*	
Server Security	Timestamp Disclosure	*	*	*
	Private IP Disclosure	*	*	*
	Route route	*		
Scan Rule	Content Security Policy	*	*	*
	Cross-Domain JavaScript Source File Inclusion: Cross-Domain Misconfiguration	*	*	*
	Disclosure of information (suspicious comments)	*	*	*
	Information Disclosure - Debug Error Messages	*	*	*
	Weak authentication method	*	*	
	Secure Pages Include Mixed Content	*	*	*

Source: Authors' Elaboration

The results obtained from the OWASP ZAP analysis, taking into account the indicators of the level of risk, probability of occurrence and percentage of risk by vulnerability, classified by periods (months), can be seen in Table 4.

Table 4. Vulnerabilities by dimensions (by periods).

Dimension	Vulnerability	Averages					
		Period1	Period2	Period3	Average	%	Level
Injection	Cross-site scripting	23,25	21,25	29,25	24,58	8,42%	INFORMATIVE
	String Formatting Error	7,00	8,00	15,75	10,25	3,51%	LOW
	SQL Injection Failure	10,25	7,00	9,25	8,83	3,03%	LOW
	Cache control policies	35,50	32,00	38,50	35,33	12,10%	INFORMATIVE
	Vulnerable Javascript library	11,50	12,50	14,75	12,92	4,43%	MIDDLE
Collection of Information	Directory Browsing	18,00	17,25	26,10	20,45	7,01%	INFORMATIVE
	Cookie without a secure flag	14,00	13,00	14,75	13,92	4,77%	LOW
	Cookie without the same site attribute	16,70	13,45	14,70	14,95	5,12%	LOW
Server Security	Timestamp Disclosure	17,75	17,00	19,00	17,92	6,14%	INFORMATIVE
	Private IP Disclosure	9,75	9,25	11,00	10,00	3,43%	LOW

	Route route	17,00	20,25	24,75	20,67	7,08%	INFORMATIVE
Scan Rule	Content Security Policy	16,47	14,17	16,00	15,54	5,33%	MIDDLE
	Inclusion of cross-domain JavaScript source files: Cross-domain misconfiguration.	19,70	16,45	19,95	18,70	6,41%	LOW
	Disclosure of Information - Suspicious Comments	21,30	21,20	23,25	21,92	7,51%	INFORMATIVE
	Information Disclosure - Debug Error Messages	11,85	11,15	18,00	13,67	4,68%	LOW
	Weak authentication method	12,75	15,50	15,00	14,42	4,94%	LOW
	Secure Pages Include Mixed Content	19,00	14,25	20,25	17,83	6,11%	MIDDLE
Total		281,77	263,67	330,25	291,89	100%	

Source: Authors' Elaboration

During the three scanned periods, the following results were obtained: In the Injection dimension, the most significant vulnerability at the level of informational risk as an alert of possible configuration is that of cache control policies, in addition to there being a medium risk level in the Javascript Library that would have a slight impact on the operability of the WMS and String format error that has a low risk level that does not it would cause inconvenience.

In addition, in the dimension of information collection, the most relevant vulnerability at the level of information risk is the browsing of the directory, also in the Cookie without the same attribute of the site, causes a low level of risk that, despite not causing inconveniences, should be reviewed.

In the server security dimension, the main vulnerability at the level of information risk is path path, on the other hand, there is a low level of risk in the disclosure of private IPs that would have an impact that would not cause inconveniences.

Finally, in the scan rule dimension, the vulnerability with information risk level is the disclosure of information - suspicious comments, there is a medium risk level in safe pages that include mixed content that would have a slight impact on the operability of the EMS, and the inclusion of JavaScript source files between domains has a low risk level.

Table 5 shows the results obtained from the vulnerabilities by dimensions (time range):

In the time range from 07:30 to 10:30, the most significant vulnerability in terms of information risk is the cross-site script, in addition to there being a medium level of risk in secure pages, they include mixed content that would have a slight impact on the operability of the WMS and the inclusion of JavaScript source files between domains has a low level of risk due to misconfiguration between domains that would not cause inconveniences.

In the time range from 10:30 a.m. to 1:30 p.m., the most significant vulnerability at the level of information risk is the cache control policies, in addition to there being a medium risk level in the Javascript Library that would have a slight impact on the operability of the WMS and the Cookie without the same attribute of the site domains has a low risk level;

In the time range of 1:30 p.m. to 3:30 p.m., the most significant vulnerability in terms of information risk is cache control policies, in addition to there being a medium level of risk in secure pages, they include mixed content that would have a slight impact on the

operability of the SGS and the inclusion of JavaScript source files between domains has a low risk level;

In the time range from 3:30 p.m. to 5:30 p.m., the most relevant vulnerability at the level of information risk is the cache control policies, in addition to there being a medium risk level in the content security policy that would have a slight impact on the operability of the WMS and weak authentication method has a low risk level;

Table 5. Vulnerabilities by dimensions (by time range)

DIMENSION	VULNERABILITY	07H30 TO 10H30	10:30 A.M. TO 1:30 P.M.	1:30 p.m. to 3:30 p.m.	3:30 PM TO 5:30 PM	LEVEL
INJECTION	Cross-site scripting	26,33	29,00	23,33	19,67	INFORMATIVE
	String Formatting Error	8,67	9,67	13,33	9,33	LOW
	SQL Injection Failure	6,00	16,00	5,67	7,67	LOW
	Cache control policies	26,00	46,67	30,33	38,33	INFORMATIVE
	Vulnerable Javascript library	13,33	14,00	11,00	13,33	MIDDLE
COLLECTION OF INFORMATION	Directory Browsing	15,00	29,67	12,33	24,80	INFORMATIVE
	Cookie without a secure flag	13,67	7,00	25,67	9,33	LOW
	Cookie without the same site attribute	16,13	16,33	15,33	12,00	LOW
SERVER SECURITY	Timestamp Disclosure	21,67	10,33	29,00	10,67	INFORMATIVE
	Private IP Disclosure	7,00	15,67	8,00	9,33	LOW
	Route route	19,33	23,33	20,33	19,67	INFORMATIVE
SCAN RULE (INTEGRITY – CONFIDENTIALITY – AVAILABILITY)	Content Security Policy	23,67	7,33	12,11	19,07	MIDDLE
	Inclusion of cross-domain JavaScript source files: Cross-domain misconfiguration.	24,20	10,27	27,80	12,53	LOW
	Disclosure of Information Suspicious Comments	23,00	22,20	21,67	20,80	INFORMATIVE
	Information Disclosure - Debug Error Messages	17,33	9,67	15,33	12,33	LOW
	Weak authentication method	15,00	15,33	11,67	15,67	LOW
	Secure Pages Include	27,33	8,33	24,00	11,67	MIDDLE

	Mixed Content

Source: Authors' Elaboration

Table 6 describes the results obtained from the vulnerabilities found with their respective level of risk, through the scanning of the applications of the LMS platform, which were: informative 141 with a risk of 48.29%, low 105 with a risk of 35.96% and medium 46 with 15.75%, which represent 100%. It should be noted that no vulnerabilities with a High risk level were found.

Table 6. Detail of the vulnerabilities found with their respective level of risk

Dimension	Vulnerability	Risk Level					
		Informative	Low	Middle	High	Total	Percentage of risk
Injection	Cross-site scripting	25	0	0	0	25	8,42%
	String Formatting Error	0	10	0	0	10	3,51%
	SQL Injection Failure	0	9	0	0	9	3,03%
	Cache control policies	35	0	0	0	35	12,10%
	Vulnerable Javascript library	0	0	13	0	13	4,43%
Collection of Information	Directory Browsing	20	0	0	0	20	7,01%
	Cookie without a secure flag	0	14	0	0	14	4,77%
	Cookie without the same site attribute	0	15	0	0	15	5,12%
Server Security	Timestamp Disclosure	18	0	0	0	18	6,14%
	Private IP Disclosure	0	10	0	0	10	3,43%
	Route route	21	0	0	0	21	7,08%
Scan Rule	Content Security Policy	0	0	16	0	16	5,32%
	Inclusion of cross-domain JavaScript source files: Cross-domain misconfiguration.	0	19	0	0	19	6,41%
	Disclosure of Information - Suspicious Comments	22	0	0	0	22	7,51%
	Information Disclosure - Debug Error Messages	0	14	0	0	14	4,68%
	Weak authentication method	0	14	0	0	14	4,94%
	Secure Pages Include Mixed Content	0	0	18	0	18	6,11%
Percentage by risk of vulnerability		48,29%	35,96%	15,75%	0,00%		
Total		141	105	46	0	292	100,00%

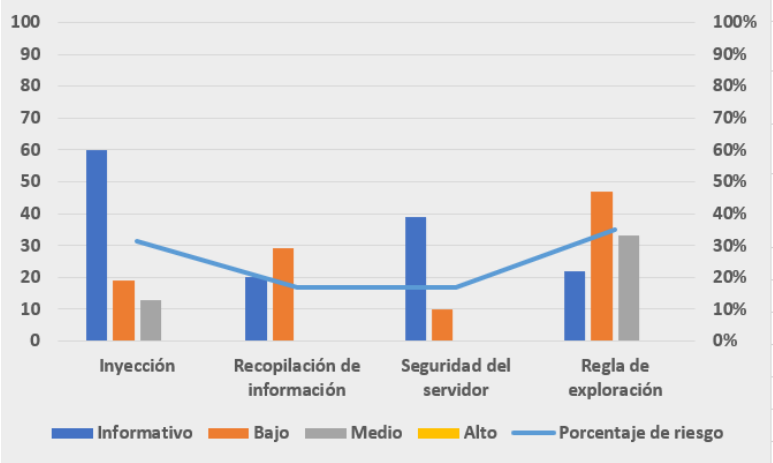
Source: Authors' Elaboration.

In addition, from the point of view of the level of risk we have that the vulnerabilities that require more attention are: Cache control policies at the information level, Javascript library, at a low risk level, the inclusion of JavaScript source files across domains:

misconfiguration between domains and medium risk level, Content Security Policy, Secure Pages include mixed content.

Graph 1 shows the results obtained through the scanning of the applications of the LMS platform, which were by vulnerability dimensions: injection 92 with a risk of 31.51%, information collection 49 with a risk of 16.78%, server security 49 with 16.78% and scan rule 102 with 34.93%. representing 100%.

Figure 1. Percentages of risk levels by dimension



Source: Authors' Elaboration.

4. CONCLUSIONS

The OWASP methodology is a benchmark for the improvement of security in web applications, thus allowing the implementation of procedures that guarantee the security of information and the prevention of cyberattacks that may be generated, which provides follow-up and background documentation to then execute a feedback of the failures presented during security incidents. In addition, it allows us to create mitigation plans and periodic authorship, which generates greater use of auditing tools and greater security of the applications that are implemented within organizations.

The existence of vulnerabilities in the web applications of the UTEQ SGA platform was determined, with a medium and low level of informational risk. The dimensions of vulnerabilities that require more attention are: configuring cache control policy rules to ensure the security of resources between devices, preventing SQL injection failure to protect databases, and constantly updating Javascript libraries. The content security policies of the EMS should also be updated, authentication systems should be improved to ensure correct configuration between domains and not allow the disclosure of information and thus strengthen the security of mixed content pages.

The vulnerabilities detected are part of the configuration of web applications, however, the application of the OWASP methodology provides the necessary tools to find possible alternative solutions and minimize the vulnerabilities of the web components, after the installation of the LMS platform and thus safeguard the security of the information.

5. RECOMMENDATIONS

It is necessary to carry out periodic analyses of the vulnerabilities of the EMS platform, based on the OWASP methodology, bearing in mind the top ten suggested by the methodology, which will allow to have a record of data on the evolution of vulnerabilities and provide better security of assets in the teaching-learning process.

It is recommended that the EMS content security policies be updated, authentication systems improved through the use of strong passwords and regular password changes, followed by a review of website cookies along with the inclusion of login forms for both employees and external users.

Perform technical corrections to infrastructure and application vulnerabilities, using remediation procedures and server maintenance, in addition to validating if XSS filters are enabled.

It is recommended that EMS administrators implement an Information Management system, which includes controls and procedures that help manage security incidents to protect the confidentiality, integrity and availability of information, perform maintenance on servers and validate whether XSS filters are enabled.

6. FUTURE JOBS

Future work includes the following:

To improve the scope proposed in this work, through the application of tests with other detection tools, which includes the use of the unified classification of vulnerabilities to provide information to students about the vulnerabilities to be avoided in the development of applications or in their detection methods.

Define and implement a knowledge base of values and fields, in order to be able to perform the analyses more quickly, which is completed as the tool performs the analysis, so that the information collected in previous analyses can be used in the following ones.

References

1. Rosenberg, M.J., E-learning: strategies for transmitting knowledge in the digital age. 2002: McGraw-Hill Inter-American
2. Espinosa, H.R., L.F.R. Betancur, and D.J.R.d.l.e.s. Aranzazu, Computer literacy and the use of learning management systems (LMS) in university teaching. 2014. 43(171): p. 139-159.
3. Schlenker, B.J.E.-M., What is e-Learning 2.0. The eLearning Guilds' Learning Solutions. 2008: p. 1-9.
4. Bermudez Herrera, L.A., Elaboration of a study of technological innovation applied in training processes with learning management systems (LMS) in university education in Ecuador. 2018, Quito: Universidad de las Américas, 2018.
5. Otero Escobar, A.D., Virtual Learning Platforms in Higher Education (2022).
6. Castro, S.M., et al., 19 E-LEARNING PLATFORMS.
7. Ramírez-Correa, P.E., et al., Moderating effect of learning styles on a learning management system's success. 2017. 34(1): p. 272-286.
8. Broncano, M.P.E. and D.F.Á.J.E.S.J. Pesantez, Cybersecurity in learning management systems (LMS). 2021. 5(1): p. 46-54.
9. Olmedo, M.R.M. and V.E.J.J.R.U.C. Chaves, Information security in e-learning platforms in times of COVID-19 pandemic. 2020. 4(1).
10. Kubacka, A., D. Biały, and R.J.I.J.o.R.i.E.-l. Gołąb, Perception of Information Security in the Process of Distance Learning During the COVID-19 Pandemic on the Example of University Teachers' Experiences. 2021. 7(2): p. 1-18.
11. Castro, M.I.R., et al., Introduction to Computer Security and Vulnerability Analysis. Vol. 46. 2018: 3Science.
12. Escobar, H.A.Q.M., D.A.D. Pérez, and M.N.P.J.R.M.d.A.d.I. Rul, Computer security in educational platforms used at the higher level: a pending task. 2016. 2(3): p. 1-18.

13. Díaz Contreras, J.S. and D.L. Villota Oliveros, E-Learning Platforms, Their Risks and Threats. 2019, Universidad Santiago de Cali.
14. Heredia Noriega, H.H., Information security risks that arise when using computer tools for the development of virtual classes by teachers and students in Colombia.
15. Rovai, A.P.J.J.o.A.L.N., A preliminary look at the structural differences of higher education classroom communities in traditional and ALN courses. 2002. 6(1): p. 41-56.
16. Zambrano, S.M.Q. and D.G.M.J.D.d.l.C. Valencia, Computer Security: Considerations. 2017. 3(3): p. 676-688.
17. Lala, S.K., A. Kumar, and T. Subbulakshmi. Secure web development using OWASP guidelines. in 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). 2021. IEEE.
18. Wibowo, R.M. and A.J.I.J.o.I.S. Sulaksono, Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd. 2021. 3(2): p. 149-159.
19. Oquendo, H.G. and L.O.J.P.e.I. Giraldo, Analysis of Risks and Vulnerabilities in Education 4.0 of the Teaching-Learning Process. 2022. 16(1).