

Article

Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders

Souheil Abdel-Latif Akacha ¹  and Ali Ismail Awad ^{1,2,*} 

¹ College of Information Technology, United Arab Emirates University, Al Ain P.O. Box 15551, United Arab Emirates; akachasouheil@gmail.com

² Faculty of Engineering, Al-Azhar University, Qena P.O. Box 83513, Egypt

* Correspondence: ali.awad@uaeu.ac.ae; Tel.: +971-37135531

Abstract: The onset of the COVID-19 pandemic prompted educational institutions to swiftly integrate e-learning software systems, including learning management systems (LMSs), as essential tools for online education. This study aims to probe the inherent security vulnerabilities of three widely utilized e-learning platforms, namely, Moodle, Chamilo, and Ilias, spanning the pre-pandemic, pandemic, and post-pandemic periods. The rapid adoption of these platforms during the pandemic revolutionized online education but also unveiled security risks. This paper delves into these security vulnerabilities, offering insights before, during, and after the pandemic. Through an analysis of existing patches and security measures, areas for improvement are identified. Furthermore, the paper considers emerging cybersecurity technologies and trends, providing comprehensive recommendations to enhance system resilience against evolving cyber threats. The results obtained here can provide educational institutions with a guide for action to enable effective mitigation of e-learning software security vulnerabilities and ensure the continued security and sustainability of online education systems.

Keywords: e-learning software systems; cybersecurity vulnerabilities; COVID-19 pandemic; cyberattacks; mitigation strategies; sustainability of e-learning systems; resilience of e-learning systems



Citation: Akacha, S.A.-L.; Awad, A.I. Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability* **2023**, *15*, 14132. <https://doi.org/10.3390/su151914132>

Academic Editors: Gláucia Daú, Annibal Scavarda, Osvaldo Luiz Goncalves Quelhas, Patrick Jaska and Atef H. Harb

Received: 6 August 2023

Revised: 9 September 2023

Accepted: 19 September 2023

Published: 24 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The COVID-19 pandemic has had a profound impact on education globally, with widespread school closures affecting over 1.5 billion students in more than 180 countries as shown in Figure 1 [1,2]. To adapt to this situation, educational institutions have shifted to remote work and online learning, known as work from home (WFH) [3]. While this transition presents challenges, it also offers an opportunity to transform and improve higher education on a global scale.

Online education has emerged as a potential solution, providing students with Internet access and the easy availability of learning materials [1]. This has led to the development of e-learning software systems and mobile learning applications to meet immediate learning needs during the crisis [4]. However, a shift to remote instruction has negative effects on students, including disrupted learning and limited growth opportunities. Disadvantaged students may face difficulties due to a lack of technological devices, and parental supervision is often required for younger students using digital tools. Teachers and students also require additional training to effectively use e-learning technologies [5,6].

Despite these challenges, e-learning offers promising opportunities for education, leveraging communication tools such as computers, computer networks, multimedia, and mobile devices. It facilitates interaction between professors and students, maximizing outcomes with minimal effort [7]. The evaluation process in e-learning relies on software systems utilizing wireless networks, such as wireless local area networks (WLANs), to

assess performance. Transparent and credible evaluation methods are essential, promoting interactions between students and instructors while improving academic performance [8].

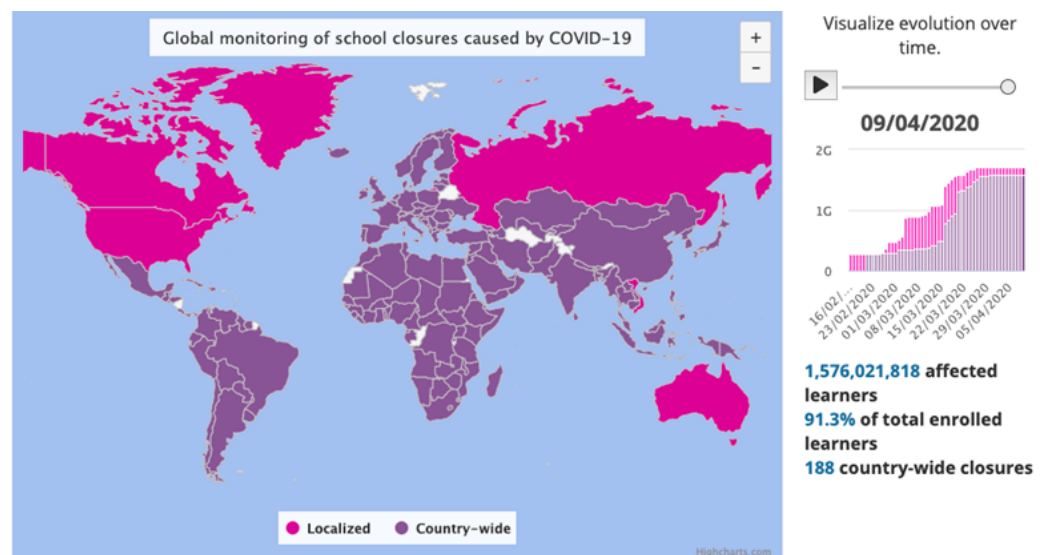


Figure 1. COVID-19 impact on education. The figure was extracted from [2].

Before the pandemic, the e-learning industry was already growing, with an investment of USD 18.6 billion in 2019 and a predicted global budget of USD 350 billion by 2025. E-learning software systems, or learning management systems (LMSs), such as Moodle, Chamilo, and Ilias, have gained significant traction as shown in Figure 2 [9,10]. These web-based LMSs supplement traditional instruction by providing resources and activities for students and teachers in online classes.

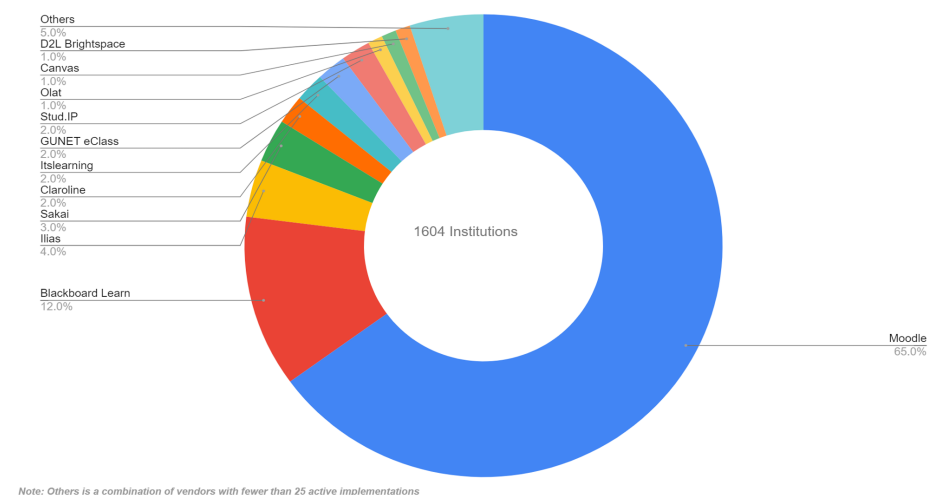


Figure 2. Distributions of e-learning software systems usage. The statistics were extracted from [10].

An increased use of e-learning software systems also brings security threats that need to be addressed. As more students use these platforms, the valuable data transmitted and stored within them become a target for malicious actors. Data breaches, phishing attacks, malware, ransomware incidents, insider threats, and inadequate system security pose significant risks [11]. In Section 2, further details regarding these e-learning systems, security threats, and the reasons for choosing specific platforms will be explored. This comprehensive analysis aims to provide an understanding of the security landscape and the rationale behind system choices in the context of e-learning [11].

1.1. Problem Statement and Contributions

The COVID-19 pandemic has led to increased adoption of e-learning software systems, such as the Moodle, Chamilo, and Ilias LMSs for remote education. However, this rapid transition to digital platforms raises concerns about security vulnerabilities and necessary countermeasures to ensure the trustworthiness of these systems. The goal of this paper is to analyze the security vulnerabilities present in Moodle, Chamilo, and Ilias before, during, and after the pandemic, and compare the countermeasures implemented by these platforms.

This research examines the timeline of the pandemic and its impact on the availability of security patches, assessing which vulnerabilities have been addressed and which still persist in these platforms. Furthermore, it evaluates the effectiveness of security measures in these e-learning software systems and determines which platform offers superior security and countermeasures.

By conducting a comprehensive analysis of the security aspects of the Moodle, Chamilo, and Ilias LMSs, this study contributes to enhancing the trustworthiness and reliability of e-learning software systems in the face of evolving cybersecurity challenges. The findings of this research will enable educational institutions to understand and effectively mitigate security vulnerabilities in e-learning software systems, ensuring the sustainability of these LMSs during and after the COVID-19 pandemic [11]. This work addresses the following research questions:

- RQ-1. What are the prevalent security vulnerabilities in the Moodle, Chamilo, and Ilias e-learning software systems that schools, institutions, and other educational organizations have used before, during, and after the COVID-19 pandemic?
- RQ-2. How may COVID-19 have impacted the prevalence of these security vulnerabilities?
- RQ-3. What patches are available for current vulnerabilities, and what future improvements can be envisaged?

This study will add to the corpus of research about cybersecurity, focusing on evaluating the security aspect of the predominantly utilized e-learning software systems (Moodle, Chamilo, and Ilias) by gathering security vulnerabilities from the Common Vulnerabilities and Exposures (CVE) database and conducting an extensive validation and analysis. The main contributions of this study are as follows:

1. We discover the prevalent security vulnerabilities on Moodle, Chamilo, and Ilias e-learning software systems that schools, institutions, and other educational organizations have been using before, during, and after the COVID-19 pandemic. The data are collected by extracting relevant CVE entries specifically related to these platforms before, during and after the pandemic. The goal is to identify potential weaknesses and loopholes in these software systems that could be exploited by malicious actors to compromise data, disrupt operations, or gain unauthorized access to sensitive information.
2. We validate the existence of security vulnerabilities in the aforementioned e-learning software systems before, during, and after the pandemic. A controlled testing environment is prepared by replicating the configurations and setups commonly found in educational institutions. The assessment involves using a third-party tool, OWASP ZAP, for web application security testing and for vulnerability assessments on the deployed e-learning systems. This process aims to verify the presence and impact of the identified and analyzed vulnerabilities in the CVE database.
3. We analyze the security vulnerabilities in the considered e-learning systems before, during, and after the pandemic. The vulnerabilities are meticulously examined in the context of the different time periods. By comparing the vulnerabilities before, during, and after the pandemic, the study seeks to identify any patterns, trends, or shifts in the security posture of the LMSs and how different stakeholders, such as vendors and developers, responded to security challenges during different phases of the pandemic.
4. We provide valuable practical recommendations for stakeholders, including LMS developers and vendors, with regard to prioritizing and strengthening security aspects

within e-learning systems. By proposing these future improvements, this paper aims to enhance the overall trustworthiness and resilience of these e-learning systems.

5. We enhance the sustainability of online education systems by strengthening security measures, ensuring the continuity of LMSs, and mitigating risks for educational institutions.

1.2. Paper Structure

The rest of this paper is structured into eight sections. Section 2 offers background information on the Moodle, Chamilo, and Ilias LMSs, including their features, functionalities, and significance in education. Section 3 critically reviews existing work related to this study and highlights the current research gap that the study addresses. Section 4 is dedicated to the data collection process from the CVE database to identify the security vulnerabilities of the aforementioned e-learning systems before, during, and after the COVID-19 pandemic. A statistical data analysis to gain insights into the vulnerabilities and their trends before, during, and after the pandemic is presented in Section 5. Section 6 describes a practical experiment to validate and verify the collected and analyzed CVE data. Discussions of the research findings and the recommendations arising from these findings are presented in Section 7. Finally, research conclusions are given in Section 8.

2. Background

This section focuses on three prominent e-learning software systems, namely, Moodle, Chamilo, and Ilias, and their significance in the education landscape. These platforms have been widely adopted, particularly during the COVID-19 pandemic when remote learning became prevalent, as indicated by the statistical data in Figure 2 [10]. Before delving into their definitions, we outline the rationale behind their selection, highlighting the reasons that render them pivotal for our study. This is primarily due to their open-source and free nature, as well as their security vulnerabilities arising for the following reasons:

1. **Third-party integrations:** Open-source platforms allow third-party integrations, which can increase the risk of security vulnerabilities if these integrations are not properly vetted or maintained.
2. **Custom code:** Users can create custom code for these platforms, such as plugins or themes, which can introduce security vulnerabilities if not developed and maintained correctly.
3. **Code vulnerabilities:** Open-source platforms often have a large amount of code that can become outdated and difficult to manage, leading to coding errors and vulnerabilities that can be exploited by attackers.
4. **Lack of automatic updates:** Some open-source platforms may not have automatic updates, leaving the system vulnerable to known security threats if updates are not applied promptly.
5. **Human error:** Open-source platforms rely on human administrators to configure and maintain the system. Mistakes or failure to follow security best practices can make the system vulnerable to attacks.

Moodle (Figure 3) is a popular LMS introduced in 2002. It allows users to build and manage courses, track learner progress, and facilitate online education. Moodle is widely used by institutions in various industries. It offers several benefits, being open source, easy to use, flexible, compatible with different devices, allowing optional integration with other systems, and supporting collaborative learning [12].

Chamilo (Figure 4) is another LMS and talent management system. It enables businesses to create and offer courses to their employees while keeping track of their educational and professional accomplishments. Chamilo is managed by the nonprofit Chamilo Association and has a large global user community. It offers features such as session management, easy creation of learning pathways, course import and design tools, reporting and statistics, and skills management [13].

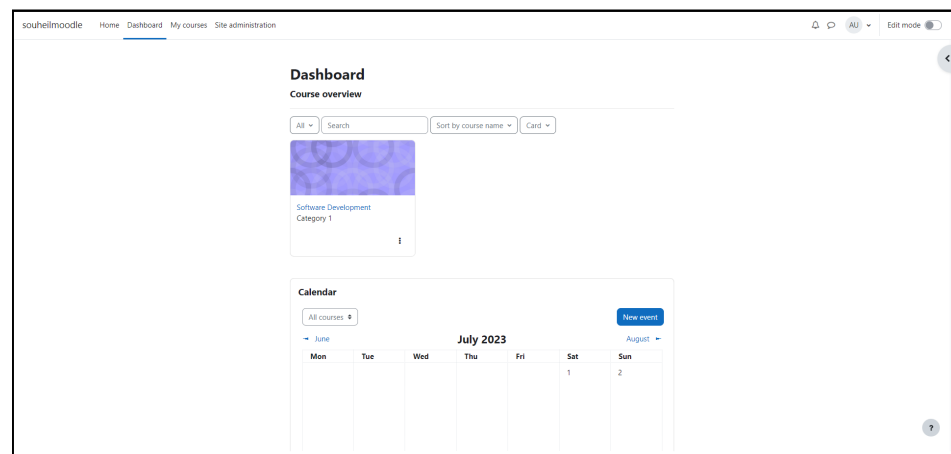


Figure 3. Moodle v4.2 dashboard user interface.

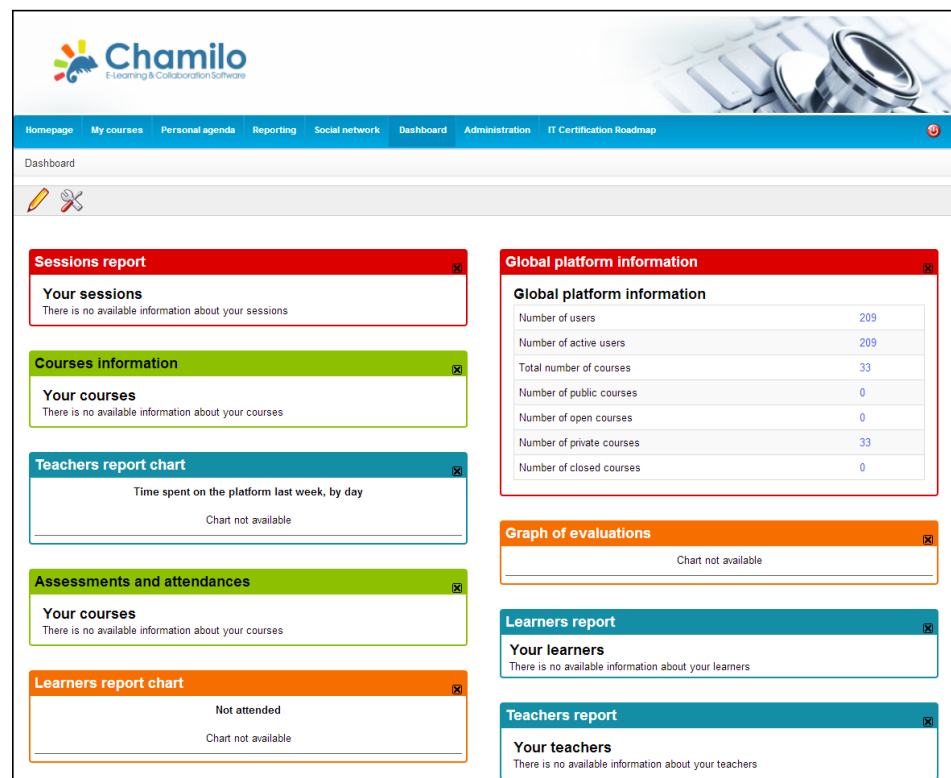


Figure 4. Chamilo v1.11.20 dashboard user interface.

Ilias (Figure 5) is a flexible environment for online learning beyond the traditional concept of courses. It can be compared to a library of learning resources that can be made available to non-registered users. Ilias includes three primary working areas: personal desktop, repository, and administration. The personal desktop provides customizable elements, such as system messages, news, calendar, and bookmarks. The repository allows users to create and save various learning resources. The administration section provides access to administrative settings for all features and objects in the system. Ilias is an open-source LMS that can be easily installed, configured, and tailored to meet specific needs [14].

The usage of these three platforms significantly increased during the COVID-19 pandemic, owing to their crucial role in providing accessible and flexible education as more people turned to online learning. However, the security concerns and vulnerabilities encountered by these platforms during this time are a source of worry. Educational institutions

have experienced a surge in cyberattacks, with cybercriminals targeting personal information, attempting to gain control over devices, and exploiting remote access technologies and online learning platforms for unauthorized entry.

The shift to online learning has exposed the education sector to various challenges, including the use of open-source technologies with vulnerabilities, inadequately trained teachers for online courses, and students lacking necessary devices and Internet connections. The education sector has also lacked clear cybersecurity policies to protect its assets, employees, and students. During the pandemic, the education industry accounted for the highest number of malware encounters among businesses, indicating its heightened vulnerability to cyber threats. To understand the risks posed by online learning platforms, it is essential to consider the principles of information security, confidentiality, integrity, and availability. Learning platforms exhibit technical and human vulnerabilities, leading to the discovery of numerous security flaws. These flaws can be categorized into authentication, availability, confidentiality, and integrity attacks.

Authentication threats involve insecure communication protocols and the improper management of active sessions. Availability threats include denial-of-service (DoS) attacks and logical attacks. Confidentiality threats arise from insecure cryptographic storage, insecure direct object references, information leakage, and improper error handling. Integrity threats include buffer overflow, cross-site request forgery attacks, cross-site scripting, injection flaws, and malicious file execution. Overall, the vulnerabilities and threats faced by learning systems during the COVID-19 pandemic have posed significant risks to the security and integrity of personal data, potentially leading to financial losses and other malicious activities.

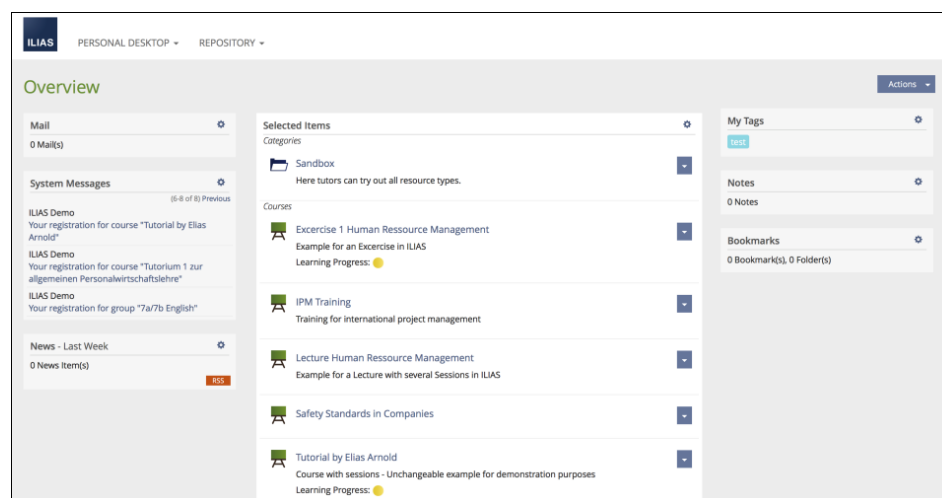


Figure 5. Ilias v7 dashboard user interface.

3. Related Works

The education sector is facing a growing challenge due to increasing digitization, with cyber threats posing a significant risk to the system. Even before the COVID-19 pandemic, cyber incidents targeting higher education institutions had resulted in large-scale breaches of personal data. For example, in 2018, the University of Yale experienced a hack that exposed the personal information of 119,000 individuals [15].

During the pandemic, educational institutions faced increased hazards and lockdown measures, leading to the widespread adoption of WFH and e-learning systems. One study highlighted the positive impact of e-learning systems in significantly improving student performance (20%), autonomy (18%), and self-directed learning (12%) [16]. These systems streamlined the assessment process and benefited both administrators and students.

Institutions worldwide have embraced in-house and outsourced software solutions to adapt to the demands of e-learning. For example, Athabasca University in Canada developed an electronic exam system [17], and prominent institutions like MIT, Stanford,

and Berkeley have utilized online software systems for course delivery and exams. Aschaffenburg University and the University of King Abdul Aziz [18] have also achieved positive outcomes with blended-learning exams. Neelain University in Sudan [19] and several universities in Nigeria [20–22] have successfully implemented e-exams.

However, despite the benefits, there are still challenges in maintaining exam integrity and ensuring security and confidentiality in non-controlled environments. Administrations are facing difficulties in enhancing system authentication and security. Recent research has shown that phishing and smishing were involved in 86% of cyberattacks during COVID-19, with a rise of 51% in such attacks during the pandemic. Of these, 17% were addressed at a worldwide level, 14% in the UK, 14% in the USA, 25% in China, and 30% in other nations, including Japan, Singapore, Italy, and Spain. Telecommunication and video conferencing systems, along with e-learning software systems, were the most targeted platforms in the education sector. Attacks such as man-in-the-middle (MitM) and distributed denial-of-service (DDoS) attacks pose threats to e-learning systems, leading to data breaches and privacy violations [23].

The abrupt rise in the usage of online learning platforms during the pandemic has raised safety concerns, given the previous cyberattacks on academic institutions. Increased online activities for students involve potential risks, such as data theft and exposure to hazardous individuals. Accessing online learning platforms over an unsecured home or public networks, the lack of computer skills among young children, and the use of potentially insecure online apps by teachers are factors that impact e-learning safety [23,24].

Higher education institutions, particularly those engaged in COVID-19 research, have become targets for malicious parties. Cyberattacks aimed at stealing COVID-19 data or impairing services have been reported, with both individuals and foreign countries suspected to be behind these attacks. The attacks raise concerns, especially with regard to the development of potential coronavirus vaccines. Ransomware and password theft attacks have been attempted [25].

The COVID-19 pandemic has caused disruptions to normal operations, including the cancellation of exams at Northumbria University in the UK [26]. Ransomware attacks have resulted in severe financial losses, with attackers blocking access to data and demanding ransoms. In 2020, the University of California paid USD 1.14 million in response to a ransomware attack [27]. Data breaches and cyberattacks have led to potential legal actions against universities due to compromised personal data. Despite the recognition of the importance of cybersecurity, many educational institutions lack proper cybersecurity policies and specialized departments.

Amidst the global upheaval during the pandemic, with nations being compelled to enforce lockdowns, the realm of education faced the unprecedented challenge of ensuring continuous learning for students. Swiftly adapting to the new reality, educational institutions migrated to online platforms, but this shift to the digital domain brought forth an alarming surge in cybersecurity threats [28]. Experts had foreseen this risk, understanding that the hasty transition to online modes might render educational institutions vulnerable to cyberattacks.

Higher education institutions have experienced a high frequency of cyberattacks, with 80% reporting attacks and 54% reporting weekly attacks. These breaches have resulted in material losses, and 82% of the victims required updated security measures. While there is increasing recognition among top managers of the importance of cybersecurity, there is still room for improvement in implementing cybersecurity policies and measures [3].

Recent insights from a comprehensive Barracuda Networks report [29] have shed light on the gravity of the situation. In the initial three months of the lockdown, cyberattacks targeted over 1000 educational institutions, with a staggering 3.5 million cyber incidents analyzed across various sectors. The historical lack of emphasis on cybersecurity in educational settings rendered them attractive targets for malicious actors [30]. Compounding the issue, these institutions harbor valuable and sensitive information, such as the personal

data of students, teachers, staff, and parents' payment details, making them susceptible to data breaches [31].

The types of cyberattacks that plagued educational institutions in 2020 paint a grim picture of the challenges they faced. Among the most rampant were phishing attacks, affecting approximately 60% of the institutions, followed by unauthorized access to accounts, experienced by around 33%. Additionally, a significant 27% of incidents involved ransomware and other malware attacks, underscoring the severity of the cybersecurity landscape. Perhaps most concerning was the fact that almost half of the affected institutions (49%) remained unaware of these infections for a prolonged period, amplifying the potential damage [32,33].

Numerous distressing incidents of cyberattacks on educational institutions have garnered attention, magnifying the gravity of the situation. In one such breach in February 2021, a server containing critical data, including student and staff ID numbers, admissions details, and academic records, was compromised, impacting approximately 200,000 individuals. Reputed institutions like Simon Fraser University in British Columbia also fell victim to data breaches, leading to the exposure of sensitive information [34]. In another instance, Quebec's education sector faced the brunt of malicious hackers, resulting in unauthorized access to the personal data of 360,000 teachers and former teachers [35].

It is essential to recognize that these attacks transcend geographical boundaries, as evidenced by the Blackbaud hack during the summer of 2020. This extensive data breach affected multiple universities, including prestigious institutions such as the University of London and the Rhode Island School of Design. Following the breach, one of the involved universities reportedly paid a ransom to regain access to certain donors' information [36].

In the wake of these alarming events, educational institutions worldwide have come to realize the urgent need to strengthen their cybersecurity defenses. A notable report from July 2020 revealed that 54% of UK universities had reported data breaches to regulators, underscoring the importance of bolstering security measures. Furthermore, the report highlighted that 46% of university staff members had not received any security training in the preceding 12 months, stressing the critical need for improved cybersecurity preparedness [28].

The consequences of cyber threats in higher education require that greater attention be paid to the cybersecurity sector. First, there is the risk of significant financial losses due to ransomware attacks and data breaches. The education sector has experienced a higher surge in ransomware attacks compared with other sectors, with universities paying substantial ransoms. Data breaches also incur high costs and can damage universities' reputations, impacting funding opportunities. Second, there is disruption of the learning processes. DDoS attacks and viruses distributed through online learning platforms have impeded access to materials and caused system outages. Third, there is increased vulnerability to intellectual property theft. State-sponsored hacking campaigns have targeted universities, leading to the theft of research data, academic information, and intellectual property [3].

The research conducted in this paper aims to fill the gaps in understanding the security vulnerabilities of these e-learning platforms and provide useful insights to educational institutions, administrators, and policymakers. The goal is to create safer, more secure, and sustainable learning environments for students, educators, and educational institutions.

4. Data Collection

To obtain a comprehensive understanding of the security vulnerabilities present in the Moodle, Chamilo, and Ilias LMSs before, during, and after the COVID-19 pandemic, we gathered information from the Common Vulnerabilities and Exposures (CVE) database. The data collected from this database include information such as vulnerability identifiers, descriptions, severity levels, and affected versions of the LMSs.

4.1. Moodle

Tables 1–3 list the security vulnerabilities found in Moodle, covering the periods, respectively, before (2018–2019), during (2020–2021), and after (2022) the COVID-19 pandemic. These tables highlight the various vulnerabilities, including potential exploits and weaknesses in the system, that could compromise the security and integrity of Moodle.

Table 1. Moodle CVE security vulnerabilities before COVID-19 pandemic (2018–2019) [37].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2018	Code Execution	1	CVE-2018-14630	17 September 2018	9 October 2019	6.5 (Low)	Remote code execution via XML import of legacy quiz questions.
		2	CVE-2018-1133	25 May 2018	24 August 2020	6.5 (Low)	Remote code execution on the server through a calculated question.
	XSS	1	CVE-2018-14631	17 September 2018	9 October 2019	4.3 (Medium)	Reflected XSS due to insufficient filtering in Boost theme search.
		2	CVE-2018-1136	25 May 2018	3 October 2019	4 (Low)	Authenticated users can add malicious HTML blocks to Dashboard.
		3	CVE-2018-1045	22 January 2018	5 February 2018	3.5 (Medium)	XSS vulnerability via a calendar event name.
	Bypass Something	1	CVE-2018-1043	22 January 2018	3 October 2019	4 (Low)	Bypass of blocked hosts list using multiple A record hostnames.
	Gain Information	1	CVE-2018-10890	10 July 2018	9 October 2019	5 (Low)	Hidden categories disclosure in core_course_get_categories.
		2	CVE-2018-1135	25 May 2018	25 June 2018	4 (Low)	Students can download Moodle files via URL manipulation.
		3	CVE-2018-1044	22 January 2018	5 February 2018	4 (Low)	Unauthorized viewing of quiz results through quiz web services.
	CSRF	1	CVE-2018-16854	26 November 2018	9 October 2019	6.8 (Medium)	Login CSRF vulnerability in Moodle versions 3.5 to 3.5.2.
2019	XSS	1	CVE-2019-3847	27 March 2019	7 November 2022	3.5 (Medium)	Administrators can access other users' Dashboards and execute JavaScript.
		2	CVE-2019-3810	25 March 2019	7 November 2022	4.3 (Medium)	Users' full names are not properly escaped in /userpix/page.
		3	CVE-2019-3808	25 March 2019	19 October 2020	4 (Low)	Misclassification of 'manage groups' capability as not having XSS risk.
		1	CVE-2012-1169	14 November 2019	18 November 2019	5 (Low)	Personal information disclosure with user names in breadcrumbs.
		2	CVE-2012-1161	14 November 2019	15 November 2019	4 (Low)	Course information leak via hidden courses in tag search.
		3	CVE-2012-1159	14 November 2019	15 November 2019	4 (Low)	Overview report allows users to see hidden courses.
		4	CVE-2012-1158	14 November 2019	18 November 2019	4 (Low)	Gradebook information leak with hidden grade items in export.
		5	CVE-2012-1155	14 November 2019	22 November 2019	5 (Low)	Database activity export issue exposes entries from other groups.
	CSRF	1	CVE-2019-10186	31 July 2019	2 February 2023	6.8 (Medium)	CSRF token missing in the XML loading/unloading admin tool.

Table 2. Moodle CVE security vulnerabilities during COVID-19 pandemic (2020–2021) [37].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2020	DOS	1	CVE-2020-25630	8 December 2020	8 December 2020	5 (Low)	Denial-of-service risk due to unzipping zip files without checking user quota. Affects versions 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13. Fixed in 3.9.2, 3.8.5, 3.7.8, and 3.5.14.
	Code Execution	1	CVE-2020-10738	21 May 2020	22 May 2020	6.5 (Low)	Remote code execution risk when a SCORM package is added to a course and interacted with via web services. Affects versions 3.8 before 3.8.3, 3.7 before 3.7.6, 3.6 before 3.6.10, 3.5 before 3.5.12.
	SQL Injection	1	CVE-2020-25700	19 November 2020	3 December 2020	4 (Low)	Database module web services allowed students to add entries within unauthorized groups. Affects versions 3.9 to 3.9.2, 3.8 to 3.8.5, 3.7 to 3.7.8, 3.5 to 3.5.14. Fixed in 3.9.3, 3.8.6, 3.7.9, and 3.10.
	XSS	1	CVE-2020-25702	19 November 2020	3 December 2020	4.3 (Medium)	JavaScript inclusion when renaming content bank items. Affects versions 3.9 to 3.9.2. Fixed in 3.9.3 and 3.10.
		2	CVE-2020-25631	8 December 2020	8 December 2020	4.3 (Medium)	JavaScript inclusion in a book's chapter title on the "Add new chapter" page. Affects versions 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7. Fixed in 3.9.2, 3.8.5, and 3.7.8.
		3	CVE-2020-25628	8 December 2020	8 December 2020	4.3 (Medium)	Reflected XSS risk in the tag manager filter. Affects versions 3.9 to 3.9.1, 3.8 to 3.8.4, 3.7 to 3.7.7, 3.5 to 3.5.13. Fixed in 3.9.2, 3.8.5, 3.7.8, and 3.5.14.
		4	CVE-2020-25627	9 December 2020	10 December 2020	4.3 (Medium)	Stored XSS risk in the moodlenetprofile user profile field. Affects versions 3.9 to 3.9.1. Fixed in 3.9.2.
		5	CVE-2019-18210	11 February 2020	21 December 2021	3.5 (Medium)	Persistent XSS in /course/modedit.php allows authenticated users (teacher and above) to inject JavaScript into the session of another user.
		6	CVE-2019-14884	18 March 2020	19 March 2020	4.3 (Medium)	Reflected XSS risk from fatal error messages. Affects versions 3.7 before 3.7.3, 3.6 before 3.6.7, 3.5 before 3.5.9.
		7	CVE-2019-14881	18 March 2020	1 April 2020	4.3 (Medium)	Blind XSS reflected in some locations where user email is displayed. Affects Moodle 3.7 before 3.7.3.

Table 2. Cont.

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2021	Gain Information	1	CVE-2020-25703	19 November 2020	19 October 2021	5 (Low)	Participants table download included user emails even when hidden. Affects versions 3.9 to 3.9.2, 3.8 to 3.8.5, 3.7 to 3.7.8. Fixed in 3.9.3, 3.8.6, 3.7.9, and 3.10.
	DOS	1	CVE-2021-20185	28 January 2021	21 October 2022	5 (Low)	Messaging did not impose a character limit when sending messages, resulting in client-side denial of service. Affects versions before 3.10.1, 3.9.4, 3.8.7, 3.5.16.
	Code Execution	1	CVE-2021-21809	23 June 2021	24 August 2022	9 (Low)	Command execution vulnerability in the default legacy spellchecker plugin. Requires administrator privileges to exploit. Affects Moodle 3.10.
		2	CVE-2021-3943	22 November 2021	23 November 2021	7.5 (Low)	Remote code execution risk when restoring backup files. Affects versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10.
		1	CVE-2021-43558	22 November 2021	14 June 2022	4.3 (Medium)	Reflected XSS risk in the filetype site administrator tool. Affects versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10.
	XSS	2	CVE-2021-32244	16 June 2021	21 June 2021	3.5 (Medium)	Cross-site scripting (XSS) in Moodle 3.10.3 allows remote attackers to execute arbitrary web script or HTML via the “Description” field.
		3	CVE-2021-20280	15 March 2021	30 November 2021	3.5 (Medium)	Text-based feedback answers required additional sanitizing to prevent stored XSS and blind SSRF risks. Affects Moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.
		4	CVE-2021-20279	15 March 2021	23 March 2021	3.5 (Medium)	ID number user profile field required additional sanitizing to prevent stored XSS risk. Affects Moodle before 3.10.2, 3.9.5, 3.8.8, 3.5.17.
		5	CVE-2021-20186	28 January 2021	1 February 2021	2.1 (High)	Stored XSS risk due to insufficient sanitizing of TeX content when the TeX notation filter is enabled. Affects versions before 3.10.1, 3.9.4, 3.8.7, 3.5.16.
		6	CVE-2021-20183	28 January 2021	1 February 2021	4.3 (Medium)	Reflected XSS risk in some search inputs due to insufficient escaping of search queries. Affects Moodle before 3.10.1.
		1	CVE-2021-43559	22 November 2021	14 June 2022	6.8 (Medium)	CSRF risk in the “delete related badge” functionality. Affects versions 3.11 to 3.11.3, 3.10 to 3.10.7, 3.9 to 3.9.10.

Table 3. Moodle CVE security vulnerabilities after COVID-19 pandemic (2022) [37].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2022	DOS	1	CVE-2020-14322	16 August 2022	7 December 2022	0	Denial of Service (DoS) risk in Moodle versions before 3.9.1, 3.8.4, 3.7.7, and 3.5.13, due to uncontrolled loading of files in yui_combo.
	Code Execution	1	CVE-2022-45151	23 November 2022	31 January 2023	0	Stored-XSS vulnerability in “social” user profile fields of Moodle allows arbitrary code execution in the context of the vulnerable website.
		2	CVE-2022-45150	23 November 2022	31 January 2023	0	Reflected Cross-Site Scripting (XSS) vulnerability in Moodle’s policy tool allows arbitrary code execution in the context of the vulnerable website.
		3	CVE-2022-40314	30 September 2022	4 October 2022	0	Remote code execution risk when restoring backup files from Moodle 1.9.
		4	CVE-2022-35653	25 July 2022	28 July 2022	0	Reflected XSS issue in the LTI module of Moodle allows arbitrary code execution in the user’s browser.
		5	CVE-2022-35651	25 July 2022	29 July 2022	0	Stored XSS and blind SSRF vulnerability in Moodle’s SCORM track details allows arbitrary code execution and potential data theft.
		6	CVE-2022-35649	25 July 2022	1 August 2022	0	Vulnerability in Moodle’s handling of PostScript code allows remote code execution.
	SQL Injection	1	CVE-2022-40315	30 September 2022	4 October 2022	0	Limited SQL injection risk in the “browse list of users” site administration page.
		2	CVE-2022-30599	18 May 2022	13 June 2022	7.5 (Low)	SQL injection risk in the Badges code relating to configuring criteria.
		3	CVE-2022-0983	25 March 2022	30 March 2022	6.5 (Low)	SQL injection risk in Badges code relating to configuring criteria, accessible to teachers and managers.
		4	CVE-2022-0332	25 January 2022	1 February 2022	7.5 (Low)	SQL injection risk in the h5p activity web service, allowing retrieval of user attempt data.
		5	CVE-2021-32474	11 March 2022	18 March 2022	6.5 (Low)	SQL injection risk on sites with MNet enabled and configured.
	XSS	1	CVE-2022-45151	23 November 2022	31 January 2023	0	Stored-XSS vulnerability in “social” user profile fields of Moodle allows arbitrary code execution in the context of the vulnerable website.
		2	CVE-2022-45150	23 November 2022	31 January 2023	0	Reflected cross-site scripting (XSS) vulnerability in Moodle’s policy tool allows arbitrary code execution in the context of the vulnerable website.
		3	CVE-2022-40313	30 September 2022	4 October 2022	0	Recursive rendering of Mustache template helpers containing user input could result in an XSS risk or a page failing to load.
		4	CVE-2022-35653	25 July 2022	28 July 2022	0	Reflected XSS issue in the LTI module of Moodle allows arbitrary code execution in the user’s browser.
		5	CVE-2022-35651	25 July 2022	29 July 2022	0	Stored XSS and blind SSRF vulnerability in Moodle’s SCORM track details allows arbitrary code execution and potential data theft.
		6	CVE-2022-30596	18 May 2022	13 June 2022	3.5 (Medium)	Vulnerability in Moodle’s ID numbers display when bulk allocating markers to assignments allows stored XSS risk.

Table 3. Cont.

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2022	XSS	7	CVE-2021-36568	13 September 2022	30 September 2022	0	Arbitrary “Topic” addition in Moodle allows Cross-Site Scripting Stored (XSS).
		8	CVE-2021-32478	11 March 2022	7 November 2022	4.3 (Medium)	Redirect URI in Moodle’s LTI authorization endpoint allows reflected XSS and open redirect risks.
		9	CVE-2021-32475	11 March 2022	18 March 2022	3.5 (Medium)	ID numbers displayed in the quiz grading report allows stored XSS risk.
		10	CVE-2020-14320	16 August 2022	17 August 2022	0	Reflected XSS risk in the filter of the admin task log.
		11	CVE-2020-1691	5 August 2022	7 August 2022	0	Vulnerability in Moodle’s message handling allows stored cross-site scripting.
	Directory Traversal	1	CVE-2022-35650	25 July 2022	1 August 2022	0	Input validation error when importing lesson questions in Moodle allows arbitrary file read.
	Bypass Something	1	CVE-2022-30600	18 May 2022	13 June 2022	7.5 (Low)	Account lockout threshold bypass in Moodle’s login attempts counting logic.
		2	CVE-2021-40693	29 September 2022	3 October 2022	0	Authentication bypass risk in Moodle’s external database authentication due to a type juggling vulnerability.
		3	CVE-2020-1755	16 August 2022	17 August 2022	0	X-Forwarded-For headers vulnerability in Moodle allows IP address spoofing.
	CSRF	1	CVE-2022-45149	23 November 2022	31 January 2023	0	CSRF vulnerability in Moodle’s course redirect URL allows arbitrary actions on behalf of the victim.
		2	CVE-2022-2986	6 October 2022	10 November 2022	0	CSRF risk in Moodle when enabling and disabling installed HSP libraries.
		3	CVE-2022-0335	25 January 2022	1 February 2022	6.8 (Medium)	CSRF vulnerability in Moodle’s “delete badge alignment” functionality.

4.2. Chamilo

Tables 4–6 list the security vulnerabilities found in Chamilo, covering the periods, respectively, before (2018–2019), during (2020–2021), and after (2022) the COVID-19 pandemic. These tables highlight the various vulnerabilities, including potential exploits and weaknesses in the system, that could compromise the security and integrity of Chamilo.

Table 4. Chamilo CVE security vulnerabilities before COVID-19 (2018–2019) [38].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2018	Code Execution	1	CVE-2018-1999019	23 July 2018	17 September 2019	7.5 (Low)	Unserialization vulnerability in Chamilo LMS version 11.x allows remote code execution through the “hash” GET parameter in the /webservices/api/v2.php API endpoint. Fixed in After commit 0de8470.
	SQL Injection	1	CVE-2018-20329	21 December 2018	7 January 2019	5.5 (Low)	SQL injection in Chamilo LMS version 1.11.8 allows unauthorized users to extract and/or modify database information via the sessions catalogue.
	XSS	1	CVE-2018-20328	21 December 2018	7 January 2019	3.5 (Medium)	XSS in Chamilo LMS version 1.11.8’s social groups tool allows authenticated users to affect others under specific conditions.
		2	CVE-2018-20327	21 December 2018	7 January 2019	3.5 (Medium)	XSS in Chamilo LMS version 1.11.8’s gradebook dependencies tool allows authenticated users to affect others under specific conditions.
2019	Code Execution	1	CVE-2019-13082	30 June 2019	3 July 2019	7.5 (Low)	Remote code execution in Chamilo LMS 1.11.8 and 2.x through an unauthenticated file upload feature in lp_upload.php, allowing uploading of ZIP archives with .php files.
	XSS	1	CVE-2019-1000015	4 February 2019	20 February 2019	4.3 (Medium)	Cross-site scripting (XSS) in Chamilo LMS version 1.11.8 and earlier allows sending an XSS payload in a ticket subject field to steal cookies.

Table 5. Chamilo CVE security vulnerabilities during COVID-19 pandemic (2020–2021) [38].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2020	XSS	1	CVE-2013-0739	30 January 2020	31 January 2020	4.3 (Medium)	XSS vulnerability in Chamilo 1.9.4 due to improper validation of user input in chat.php.
		2	CVE-2013-0738	30 January 2020	31 January 2020	4.3 (Medium)	Multiple XSS and HTML Injection Vulnerabilities in Chamilo 1.9.4: blog.php and announcements.php.
		3	CVE-2012-4029	8 February 2020	12 February 2020	4.3 (Medium)	XSS vulnerability in Chamilo LMS before 1.8.8.6, allowing remote injection via category name parameter in add sent category action.

Table 5. Cont.

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2021	Code Execution	1	CVE-2021-37391	10 August 2021	19 August 2021	3.5 (Medium)	Stored XSS vulnerability in Chamilo LMS 1.11.14, allowing unauthorized users to send invitations with malicious code via social network's send invitation feature.
		2	CVE-2021-35413	3 December 2021	12 July 2022	6 (Medium)	RCE vulnerability in Chamilo LMS v1.11.x, enabling authenticated attackers to execute arbitrary code via crafted .htaccess file.
		3	CVE-2021-31933	30 April 2021	17 May 2021	6.5 (Low)	Remote code execution vulnerability in Chamilo through 1.11.14, allowing PHP code execution through improper input sanitization in file uploads.
	SQL Injection	1	CVE-2021-35414	3 December 2021	6 December 2021	7.5 (Low)	SQL injection in Chamilo LMS v1.11.x via the doc parameter in main/plagiarism/compilatio/upload.php.
		2	CVE-2021-34187	28 June 2021	1 July 2021	7.5 (Low)	SQL Injection in Chamilo through 1.11.14 via searchField, filters, or filters2 parameter.
	XSS	1	CVE-2021-43687	1 December 2021	15 December 2021	4.3 (Medium)	XSS vulnerability in chamilo-lms v1.11.14 if an attacker passes a message hex2bin in the cookie.
		2	CVE-2021-37391	10 August 2021	19 August 2021	3.5 (Medium)	Stored XSS vulnerability in Chamilo LMS 1.11.14, allowing unauthorized users to send invitations with malicious code via social network's send invitation feature.
		3	CVE-2021-37390	10 August 2021	17 August 2021	4.3 (Medium)	Reflected XSS vulnerability in Chamilo LMS 1.11.14, exploitable through social network search feature.
		4	CVE-2021-37389	10 August 2021	17 August 2021	4.3 (Medium)	Stored XSS in Chamilo 1.11.14 via main/install/index.php and main/install/ajax.php using the port parameter.
		5	CVE-2021-35415	3 December 2021	6 December 2021	3.5 (Medium)	Stored XSS vulnerability in Chamilo LMS, allowing execution of arbitrary web scripts or HTML via crafted payload in course "Title" and "Content" fields.
		6	CVE-2021-26746	19 February 2021	25 February 2021	4.3 (Medium)	XSS vulnerability in Chamilo 1.11.14 through a main/calendar/agenda_list.php?type= URL.
		7	CVE-2020-23126	3 November 2021	4 November 2021	4.3 (Medium)	XSS vulnerability in Chamilo LMS version 1.11.10, affecting user and social network friends via personal profile edition form.
	Directory Traversal	1	CVE-2021-31933	30 April 2021	17 May 2021	6.5 (Low)	Remote code execution vulnerability in Chamilo through 1.11.14, allowing PHP code execution through improper input sanitizations in file uploads.
	Gain Information	1	CVE-2021-32925	13 May 2021	16 May 2022	5.5 (Low)	Chamilo 1.11.x reads XML data without disabling the ability to load external entities in admin/user_import.php.

Table 6. Chamilo CVE security vulnerabilities after COVID-19 pandemic (2022) [38].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2022	Code Execution	1	CVE-2022-40407	29 September 2022	4 October 2022	0	Zip slip vulnerability in Chamilo v1.11 allows attackers to execute arbitrary code via a crafted Zip file.
		2	CVE-2022-27426	15 April 2022	25 April 2022	6.5 (Low)	Server-side request forgery (SSRF) in Chamilo LMS v1.11.13 allows attackers to enumerate the internal network and execute arbitrary system commands via a crafted Phar file.
		3	CVE-2021-40662	21 March 2022	29 March 2022	6.8 (Medium)	Cross-site request forgery (CSRF) in Chamilo LMS 1.11.14 allows attackers to execute arbitrary commands on victim hosts via a crafted URL.
		4	CVE-2021-38745	21 March 2022	29 March 2022	4.6 (High)	Zero click code injection vulnerability in Chamilo LMS v1.11.14 allows attackers to execute arbitrary code via a crafted plugin. Triggered through user interaction with the attacker's profile page.
	SQL Injection	1	CVE-2022-27423	15 April 2022	25 April 2022	7.5 (Low)	SQL injection vulnerability in Chamilo LMS v1.11.13 via the blog_id parameter at /blog/blog.php.
	XSS	1	CVE-2022-27425	15 April 2022	25 April 2022	4.3 (Medium)	Cross-site scripting (XSS) vulnerability in Chamilo LMS v1.11.13 via the component /blog/blog.php.
		2	CVE-2022-27422	15 April 2022	25 April 2022	4.3 (Medium)	Reflected cross-site scripting (XSS) vulnerability in Chamilo LMS v1.11.13 allows attackers to execute arbitrary web scripts or HTML via user interaction with a crafted URL.
	CSRF	1	CVE-2021-40662	21 March 2022	29 March 2022	6.8 (Medium)	Cross-site request forgery (CSRF) in Chamilo LMS 1.11.14 allows attackers to execute arbitrary commands on victim hosts via a crafted URL.
	File Inclusion	1	CVE-2022-42029	17 October 2022	19 October 2022	0	Authenticated local file inclusion vulnerability in Chamilo 1.11.16 allows users with access to 'big file uploads' to copy/move files from anywhere in the file system into the web directory.

4.3. Ilias

Tables 7–9 list the security vulnerabilities found in Ilias, covering the periods respectively before (2018–2019), during (2020–2021), and after (2022) the COVID-19 pandemic.

These tables highlight the various vulnerabilities, including potential exploits and weaknesses in the system, that could compromise the security and integrity of Ilias.

Table 7. Ilias CVE security vulnerabilities before COVID-19 (2018–2019) [39].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2018	XSS	1	CVE-2018-11120	17 May 2018	15 June 2018	4.3 (Med.)	XSS in ILIAS 5.1.x, 5.2.x, and 5.3.x before 5.3.5.
		2	CVE-2018-11118	17 May 2018	15 June 2018	4.3 (Med.)	XSS in ILIAS RSS subsystem.
		3	CVE-2018-11117	17 May 2018	15 June 2018	4.3 (Med.)	XSS in ILIAS Services/ Feeds.
		4	CVE-2018-10665	2 May 2018	7 June 2018	4.3 (Med.)	XSS in ILIAS 5.3.4 via PHP_SELF.
		5	CVE-2018-10428	23 May 2018	8 March 2019	4.3 (Med.)	XSS in ILIAS before 5.3.4.
		6	CVE-2018-10307	18 May 2018	18 June 2018	4.3 (Med.)	XSS in ILIAS 5.2.x through 5.3.x.
		7	CVE-2018-10306	18 May 2018	19 June 2018	4.3 (Med.)	XSS in ILIAS Services/ Form.
		8	CVE-2018-5688	14 January 2018	5 February 2018	4.3 (Med.)	XSS in ILIAS Setup component.
2019	Code Exec. XSS	1	CVE-2019-1010237	22 July 2019	9 October 2019	4.3 (Med.)	Code Exec. XSS in Ilias 5.3 before 5.3.12; 5.2 before 5.2.21.
	XSS	1	CVE-2019-1010237	22 July 2019	9 October 2019	4.3 (Med.)	XSS in Ilias 5.3 before 5.3.12; 5.2 before 5.2.21.

Table 8. Ilias CVE security vulnerabilities during COVID-19 (2020–2021) [39].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2020	Code Execution	1	CVE-2020-25268	10 November 2020	21 July 2021	6.5 (Low)	Remote code execution via external news feed in ILIAS 6.4.
	XSS	1	CVE-2020-25267	10 November 2020	18 November 2020	3.5 (Medium)	XSS issue in question-pool file-upload preview in ILIAS 6.4.
2021	Code Execution	1	CVE-2020-23996	13 May 2021	21 May 2021	6.5 (Low)	Local File inclusion vulnerability in ILIAS before 5.3.19, 5.4.10, and 6.0 allows remote authenticated attackers to execute arbitrary code via import of personal data.
	File Inclusion	1	CVE-2020-23996	13 May 2021	21 May 2021	6.5 (Low)	Local file inclusion vulnerability in ILIAS before 5.3.19, 5.4.10, and 6.0 allows remote authenticated attackers to execute arbitrary code via import of personal data.

Table 9. Ilias CVE security vulnerabilities after COVID-19 (2022) [39].

Year	Type	#	CVE ID	Publish Date	Update Date	Score & Complexity	Description
2022	XSS	1	CVE-2022-45916	7 December 2022	6 January 2023	0	ILIAS before 7.16 allows XSS.

5. Statistical Data Analysis

In this section, data on security vulnerabilities of Moodle, Chamilo, and Ilias e-learning software systems collected from the CVE database are subjected to a rigorous statistical analysis with the aim of extracting meaningful insights and patterns to enable a deeper understanding of vulnerabilities, their impact, and their potential trends. This statistical data analysis plays a crucial role in achieving the research objectives and answering the research questions posed in this paper, thereby contributing to the overall knowledge and understanding of e-learning software system security.

5.1. Moodle

Table 10 and Figure 6 present data on the number of Moodle vulnerabilities and their types from 2018 to 2022, as well as the overall count for the five-year period. Each column of the table provides specific information about the data. The year column indicates the year when vulnerabilities were reported. The # of vulnerabilities column displays the total number of vulnerabilities reported each year. The data show a consistent increase in the number of reported vulnerabilities each year, reaching a peak of 46 in 2022. This upward trend signifies a growing concern for addressing security vulnerabilities. The subsequent columns represent the types of vulnerabilities reported, including DoS, code execution, SQL injection, cross-site scripting (XSS), directory traversal, bypass, gain information, and cross-site request forgery (CSRF). Each column presents the number of vulnerabilities of a particular type reported per year and the cumulative count for the five-year period.

DoS vulnerabilities occur when an attacker overwhelms a system or network, causing it to become unresponsive. Table 10 reveals three DoS vulnerabilities reported over the five-year period, with one vulnerability reported each year from 2020 to 2022. Code execution vulnerabilities involve executing arbitrary code on a system, enabling unauthorized access or control. The data indicate 11 code execution vulnerabilities reported over five years, with 6 reported in 2022.

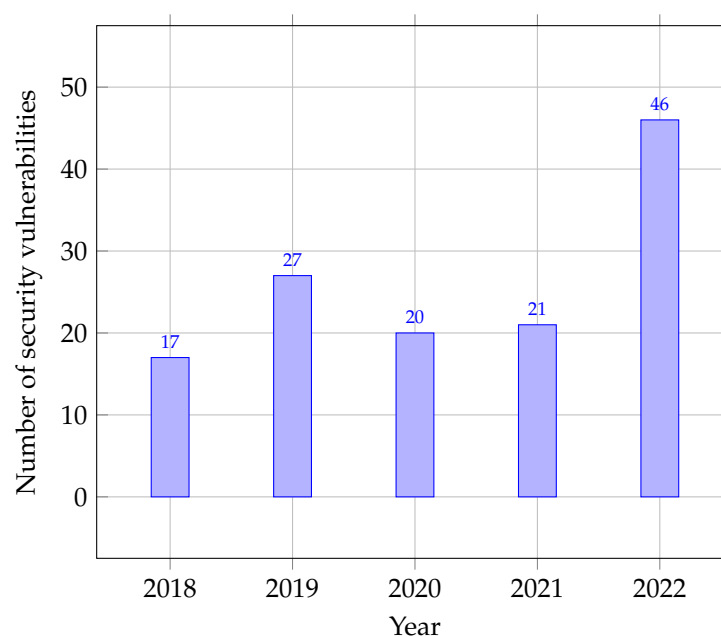


Figure 6. Moodle CVE vulnerability distribution per year (2018–2022).

Table 10. Moodle CVE vulnerability statistics (2018–2022).

Year	# of Vuln.	Vulnerability Types													
		DoS	Code Exec.	Overflow	Mem. Corr.	SQL Inj.	XSS	Dir. Trav.	HTTP Resp.	Split.	Bypass	Gain Info.	Gain Priv.	CSRF	File Incl.
2018	17	-	2	-	-	-	3	-	-	-	1	3	-	1	-
2019	27	-	-	-	-	-	3	-	-	-	-	5	-	1	-
2020	20	1	1	-	-	1	7	-	-	-	-	1	-	-	-
2021	21	1	2	-	-	-	6	-	-	-	-	-	-	1	-
2022	46	1	6	-	-	5	11	1	-	-	3	-	-	3	-
Total	131	3	11	-	-	6	30	1	-	-	4	9	-	6	-

SQL injection vulnerabilities occur when attackers manipulate database queries to gain unauthorized access or retrieve sensitive information. The table shows six SQL injection vulnerabilities reported from 2020 to 2022, with one reported in 2020 and five in 2022. XSS vulnerabilities involve injecting malicious code into web pages to steal information or control web browsers. The data show 30 XSS vulnerabilities reported over five years, with varying counts each year: 3 in 2018 and 2019, 7 in 2020, 6 in 2021, and 11 in 2022.

Directory traversal vulnerabilities allow unauthorized access to sensitive files or execution of arbitrary code. The table indicates one directory traversal vulnerability reported in 2022. Bypass vulnerabilities occur when attackers circumvent security controls to gain unauthorized access or execute arbitrary code. The data show four bypass vulnerabilities reported over five years, with one in 2018 and three in 2022.

Gain information vulnerabilities involve attackers gathering sensitive information about a system or network for planning further attacks. The table shows nine gain information vulnerabilities reported over five years, with three in 2018, five in 2019, and one in 2020. CSRF vulnerabilities occur when attackers manipulate users into unknowingly executing actions on websites. The data reveal six CSRF vulnerabilities reported over the five-year period, with one in 2018, one in 2019, one in 2021, and three in 2022.

Analysis of the data based on the periods before, during, and after the COVID-19 pandemic provides the following insights into the impact of the pandemic on reported vulnerabilities:

- Before the COVID-19 pandemic (2018 and 2019), a total of 44 vulnerabilities were reported, with XSS, code execution, and gain information being the most common types. This suggests that these vulnerabilities were prevalent even before the pandemic.

- During the COVID-19 pandemic (2020 and 2021), a total of 41 vulnerabilities were reported. The most common types during this period were XSS, code execution, and DoS. The lower number of reported vulnerabilities compared with previous years could be influenced by the pandemic, with organizations prioritizing pandemic response and addressing remote work and increased online activities.
- After the COVID-19 pandemic (2021 and 2022), a total of 67 vulnerabilities were reported. The most common types during this period were XSS, code execution, and CSRF. This indicates a shift in the types of vulnerabilities reported after the pandemic, while some prevalent vulnerability types were still maintained.

The data demonstrate an increasing number of vulnerabilities reported each year, highlighting the need to address security concerns in Moodle.

5.2. Chamilo

Table 11 and Figure 7 present data on the number of Chamilo LMS vulnerabilities and their types from 2018 to 2022, along with associated exploits. The table lists various types of vulnerabilities, including DoS, code execution, overflow, memory corruption, SQL injection, XSS, directory traversal, http response splitting, bypass, gain information, gain privileges, CSRF, and file inclusion.

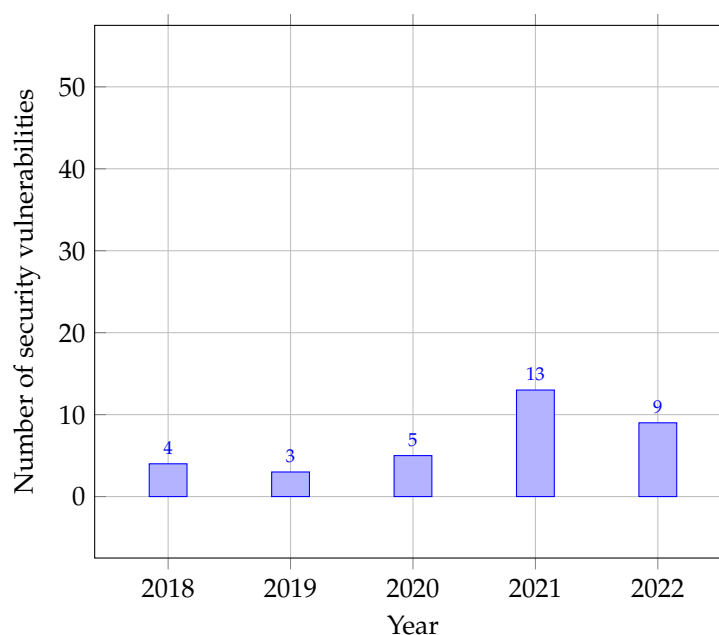


Figure 7. Chamilo CVE vulnerability distribution per year (2018–2022).

Table 11. Chamilo CVE vulnerability statistics (2018–2022).

Year	# of Vuln.	Vulnerability Types												
		DoS	Code Exec.	Overflow	Mem. Corr.	SQL Inj.	XSS	Dir. Trav.	HTTP Resp. Split.	Bypass	Gain Info.	Gain Priv.	CSRF	File Incl.
2018	4	-	1	-	-	1	2	-	-	-	-	-	-	-
2019	3	-	1	-	-	-	1	-	-	-	-	-	-	-
2020	5	-	-	-	-	-	3	-	-	-	-	-	-	-
2021	13	-	3	-	-	2	7	1	-	-	1	-	-	-
2022	9	-	4	-	-	1	2	-	-	-	-	-	1	1
Total	34	-	9	-	-	4	15	1	-	-	1	-	1	1

In 2018, there were only four vulnerabilities detected. Among these, one pertained to code execution, another was related to SQL injection, and the remaining two were associated with XSS issues. Remarkably, there were no instances of DoS, overflow, memory corruption, directory traversal, http response splitting, bypass, gain information, gain

privileges, CSRF, or file inclusion vulnerabilities found in that year. It seemed to be a relatively secure year compared with the subsequent ones.

Moving on to 2019, the number of vulnerabilities decreased slightly to three. These included one vulnerability linked to code execution, one related to XSS, and one that lacked specification. Similar to 2018, there were no occurrences of several other vulnerabilities such as DoS, overflow, memory corruption, SQL injection, directory traversal, http response splitting, bypass, gain information, gain privileges, CSRF, or file inclusion in 2019. This period appeared to maintain a decent level of security.

In 2020, the number of vulnerabilities rose to five, marking a slight increase compared with the previous year. Among these, three vulnerabilities were again associated with XSS, while two were unspecified in nature. Similar to the previous years, there were no instances of DoS, code execution, overflow, memory corruption, SQL injection, directory traversal, http response splitting, bypass, gain information, gain privileges, CSRF, or file inclusion vulnerabilities found in 2020. While the increase in total vulnerabilities might raise some concern, the absence of certain critical vulnerabilities remained consistent.

However, the year 2021 witnessed a significant surge in vulnerabilities, which reached a total of 13. The most prevalent vulnerability type was code execution, accounting for three cases, followed by two instances of SQL injection, seven occurrences of XSS, one report of directory traversal, and another vulnerability reported to gain information. Again, it was noteworthy that DoS, overflow, memory corruption, http response splitting, bypass, gain privileges, CSRF, and file inclusion vulnerabilities were not found during this year.

In 2022, the number of vulnerabilities decreased to nine. Among these, four were associated with code execution, one with SQL injection, two with XSS, one with CSRF, and one with file inclusion. As in previous years, DoS, overflow, memory corruption, directory traversal, http response splitting, bypass, gain information, and gain privileges vulnerabilities were absent.

Overall, during the five-year period from 2018 to 2022, a total of 34 vulnerabilities were discovered. The most prevalent vulnerability type was XSS, which was found in 15 instances, followed by code execution with 9 instances, and SQL injection with 4 instances. The relatively low prevalence of other vulnerabilities indicates that system developers and security experts had been successful in addressing and mitigating some of the most common security risks.

Analysis of Table 11 based on the periods before, during, and after the COVID-19 pandemic reveals the following:

- Before the COVID-19 pandemic (2018 and 2019), vulnerability discovery was relatively low, with a total of seven vulnerabilities found. The types of vulnerabilities discovered during this period were primarily related to code execution, SQL injection, and XSS. The pandemic may have had minimal impact on vulnerability discovery during this period.
- During the COVID-19 pandemic (2020 and 2021), vulnerability discovery increased significantly. A total of 18 vulnerabilities were discovered, with a focus on XSS vulnerabilities, which accounted for 7 instances in 2021 alone. This suggests that the pandemic may have introduced new attack vectors and increased vulnerability discovery owing to remote work and heightened online activity.
- After the pandemic (2022), vulnerability discovery decreased compared with the previous year. A total of nine vulnerabilities were found, primarily related to XSS and code execution. This decrease may indicate a return to pre-pandemic levels of vulnerability discovery, as the initial surge during the pandemic subsided.

The data reveal that security vulnerability discovery in Chamilo LMS was influenced by the COVID-19 pandemic, with an increase in vulnerabilities during the pandemic period, particularly in relation to XSS vulnerabilities.

5.3. Ilias

Table 12 and Figure 8 present data on the number and types of Ilias LMS vulnerabilities discovered from 2018 to 2022. Analysis of this table provides insights into prevalent vulnerability types and their trends over time.

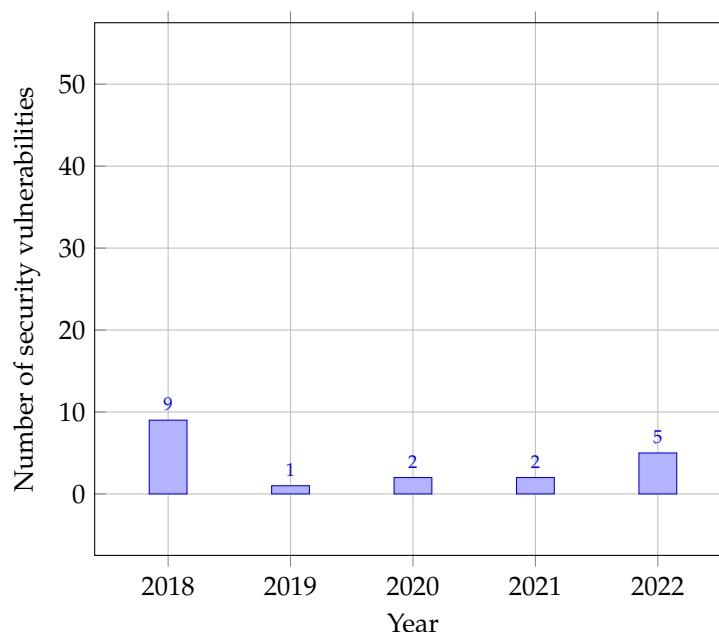


Figure 8. Ilias CVE vulnerability distribution per year (2018–2022).

Table 12. Ilias CVE vulnerability statistics (2018–2022).

Year	# of Vuln.	Vulnerability Types												
		DoS	Code Exec.	Overflow	Mem. Corr.	SQL Inj.	XSS	Dir. Trav.	HTTP Resp. Split.	Bypass	Gain Info.	Gain Priv.	CSRF	File Incl.
2018	9	-	-	-	-	-	8	-	-	-	-	-	-	-
2019	1	-	1	-	-	-	1	-	-	-	-	-	-	-
2020	2	-	1	-	-	-	1	-	-	-	-	-	-	-
2021	2	-	1	-	-	-	-	-	-	-	-	-	-	1
2022	5	-	-	-	-	-	1	-	-	-	-	-	-	-
Total	19	-	3	-	-	-	11	-	-	-	-	-	-	1

In 2018, a total of nine vulnerabilities were brought to light, and what is striking is that all of them were related to cross-site scripting (XSS). This emphasizes that XSS posed a significant threat during that year, capturing the attention of vulnerability researchers, who actively sought out and identified vulnerabilities in this specific area. The high number of XSS vulnerabilities discovered in 2018 underscores the pressing need for developers to implement robust security measures against this type of attack.

Moving on to 2019, only one vulnerability was unearthed, which had implications for both code execution and XSS. The relatively low number of vulnerability discoveries during this period indicates that it might have been a year of heightened security or less-intensive research activities. However, it is noteworthy that the types of vulnerabilities found were more focused on execution-based issues, hinting at potential vulnerabilities that could allow attackers to execute malicious code on vulnerable systems.

In 2020, vulnerability discovery remained relatively low, with only two vulnerabilities identified. One of these was related to XSS, similar to the trends observed in previous years. However, the second vulnerability was categorized as code execution, reflecting a more diversified set of vulnerability types compared with the preceding year. This suggests that while overall vulnerability identification remained limited, researchers were uncovering different types of security weaknesses, with both XSS and code execution issues being prominent.

In 2021, the number of vulnerability discoveries remained at a low level, with just two cases identified. One vulnerability was related to code execution, continuing the trend seen in previous years. However, the second vulnerability was attributed to file inclusion, indicating that researchers were paying attention to this particular type of vulnerability. It is apparent that during this period, vulnerability discovery still focused on code execution-related threats and emerging issues, such as file inclusion.

Lastly, in 2022, five vulnerabilities were discovered, with one again related to XSS, showcasing its persistent prominence as a security concern. However, the details of the remaining four vulnerabilities were unspecified, leaving room for speculation about the exact nature of these potential threats. The continuous discovery of XSS vulnerabilities underscores the need for ongoing efforts to secure web applications against this prevalent attack vector.

Overall, the analysis of vulnerability discoveries over the five-year period highlights two recurring themes: XSS and code execution vulnerabilities were the prevailing issues identified by researchers. These findings stress the critical importance of addressing and mitigating these specific security risks effectively. While other types of vulnerabilities seemed to surface less frequently during this period, it is crucial to acknowledge that the threat landscape is continually evolving, and developers and security experts must remain vigilant in their efforts to safeguard digital systems from emerging and existing threats. Regular security assessments, proactive measures, and staying up to date with the latest security best practices are essential components of maintaining a robust cybersecurity posture.

In terms of trends over time, vulnerability discovery was relatively low in 2019, 2020, and 2021, with only one or two vulnerabilities discovered per year. However, there was a significant increase in the number of vulnerabilities discovered in 2018 (nine vulnerabilities) and 2022 (five vulnerabilities). This suggests that vulnerability discovery may follow a cyclical pattern and can fluctuate considerably over time.

Analysis of Table 12 before, during, and after the COVID-19 pandemic reveals the following:

- Before COVID-19 (2018 and 2019), vulnerability discovery was relatively low, with nine vulnerabilities found in the first of these years and only one in the second. The types of vulnerabilities discovered during this period were primarily related to XSS and code execution. The pandemic did not appear to have a significant impact on vulnerability discovery during this period.
- During the pandemic (2020 and 2021), vulnerability discovery remained relatively low, with only two vulnerabilities discovered each year. Similarly, the types of vulnerabilities found during this period were primarily related to XSS and code execution. This suggests that vulnerability discovery was not significantly affected by the pandemic during this period.
- After COVID-19 (2022), the number of vulnerabilities discovered increased compared with the previous year. There were five vulnerabilities discovered in 2022, with one related to XSS. This indicates that vulnerability discovery has returned to pre-pandemic levels, and the types of vulnerabilities found align with those discovered before the pandemic.

This analysis revealed that security vulnerabilities in Ilias LMS were not significantly affected by the COVID-19 pandemic. XSS and code execution vulnerabilities remained prevalent throughout the five-year period, with fluctuations in the number of vulnerabilities discovered each year.

5.4. Comparative Analysis of Security Vulnerabilities in 2018–2022

In this subsection, a comprehensive comparative analysis of Moodle, Chamilo, and ILIAS is performed, with a focus on their vulnerability trends from 2018 to 2022. This five-year period includes the critical phases of pre-COVID, during COVID, and post-COVID, which allows us to explore how these LMS platforms were affected by the evolving cybersecurity landscape amid the global pandemic. By examining the number of vulnerabilities reported

for each system across these years, we aim to gain valuable insights into the security performance of these platforms and understand their resilience in the face of emerging threats. The findings from this analysis should contribute to a better understanding of the overall security posture of these LMS solutions and provide essential implications for stakeholders, including vendors and developers, to ensure a safe and reliable e-learning environment.

Figure 9 displays the number of vulnerabilities identified in Moodle, Chamilo, and Ilias from 2018 to 2022. The total number of vulnerabilities identified for each platform is provided.

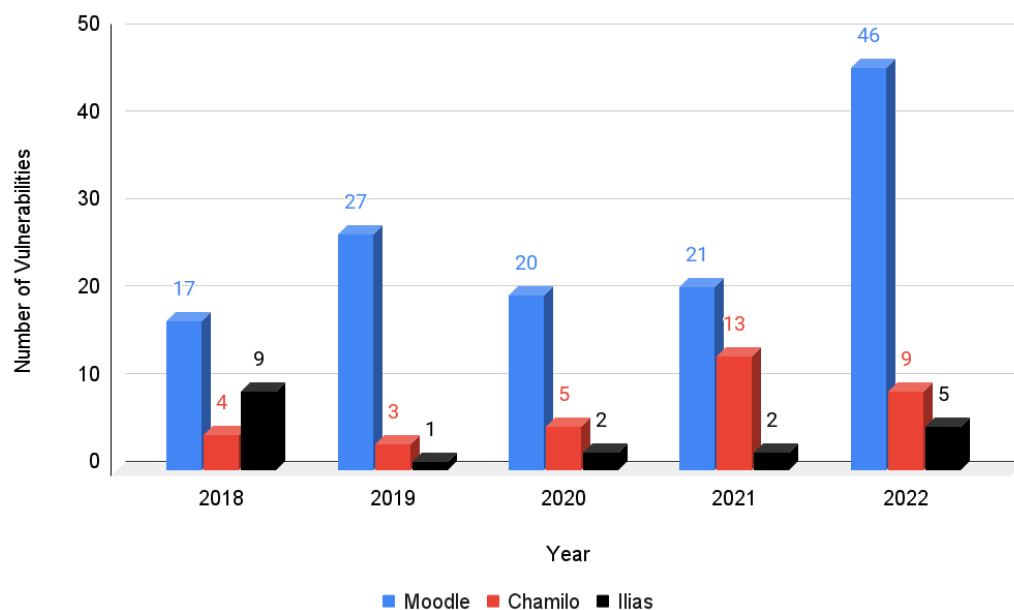


Figure 9. Comparison of vulnerability trends in Moodle, Chamilo, and Ilias in 2018–2022.

Moodle, an open-source LMS widely used worldwide, has a significantly higher total number of vulnerabilities compared with Chamilo and Ilias. In fact, it has over three times as many vulnerabilities as Chamilo and nearly seven times as many as Ilias. Over the years, the number of vulnerabilities identified in Moodle has been steadily increasing. There was a significant surge in vulnerabilities from 2021 to 2022, nearly doubling the count. By contrast, Chamilo and Ilias have had relatively low vulnerability numbers without clear trends. Examining the vulnerabilities found in Moodle, Chamilo, and Ilias before, during, and after the COVID-19 pandemic reveals several noteworthy observations.

Before the COVID-19 pandemic, specifically in 2018 and 2019, the vulnerabilities identified in Moodle raised substantial concerns about the platform's security posture. With 17 and 27 vulnerabilities reported in the respective years, the numbers were noticeably higher than those of Chamilo and Ilias. This discrepancy in vulnerability counts underscores the existence of a distinct vulnerability landscape within the e-learning ecosystem, highlighting Moodle as an area requiring particular attention in terms of security.

Throughout the pandemic (2020 and 2021), the number of vulnerabilities in Moodle continued to remain at elevated levels and even surged further in 2021, with a total of 21 vulnerabilities identified. Chamilo, on the other hand, experienced only a slight increase in vulnerabilities during 2020, and the number decreased to just three in 2019. Ilias experienced a comparatively low number of vulnerabilities during the pandemic, with only two identified in 2020. An important aspect to consider here is the rapid shift to online learning imposed by the pandemic, which significantly increased the demand for LMSs such as Moodle, Chamilo, and Ilias. This increased usage likely subjected these platforms to increased scrutiny, leading to the detection of more vulnerabilities.

Post-COVID-19 (2022), a significant surge in the number of vulnerabilities was observed across all three platforms. Notably, Moodle stood out with the highest number of

vulnerabilities identified, totaling 46. Conversely, Chamilo and Ilias had significantly fewer vulnerabilities during this period, with, respectively, nine and five identified.

Drawing definitive conclusions about vulnerability trends before, during, and after COVID-19 is challenging. However, the data suggest that Moodle consistently faces security threats, whereas Chamilo and Ilias exhibit lower and fluctuating vulnerability numbers. It is important to note that the vulnerability count does not solely indicate a platform's security level since factors such as popularity, scrutiny, and code complexity also contribute. Nonetheless, LMS providers should promptly address vulnerabilities through patches or updates, and organizations using LMSs must stay informed and take necessary measures to safeguard their data and systems.

The data indicate that Moodle had security concerns even before the COVID-19 pandemic, underscoring the need for continuous security monitoring and proactive vulnerability management in educational technology platforms.

On the basis of Figures 9 and 10, we will present a comprehensive analysis that correlates the security vulnerabilities of Moodle, Chamilo, and Ilias with their respective usage patterns during distinct time frames: the pre-COVID-19 years of 2018–2019, the COVID-19 era of 2020–2021, and the post-COVID year of 2022. By examining the fluctuations in security vulnerabilities and their impact on user adoption, we aim to uncover insights into the intricate relationship between the security landscape of these platforms and the preferences of users during various phases of global events. This analysis will shed light on how security concerns intersect with user engagement and platform sustainability within the dynamic realm of e-learning.

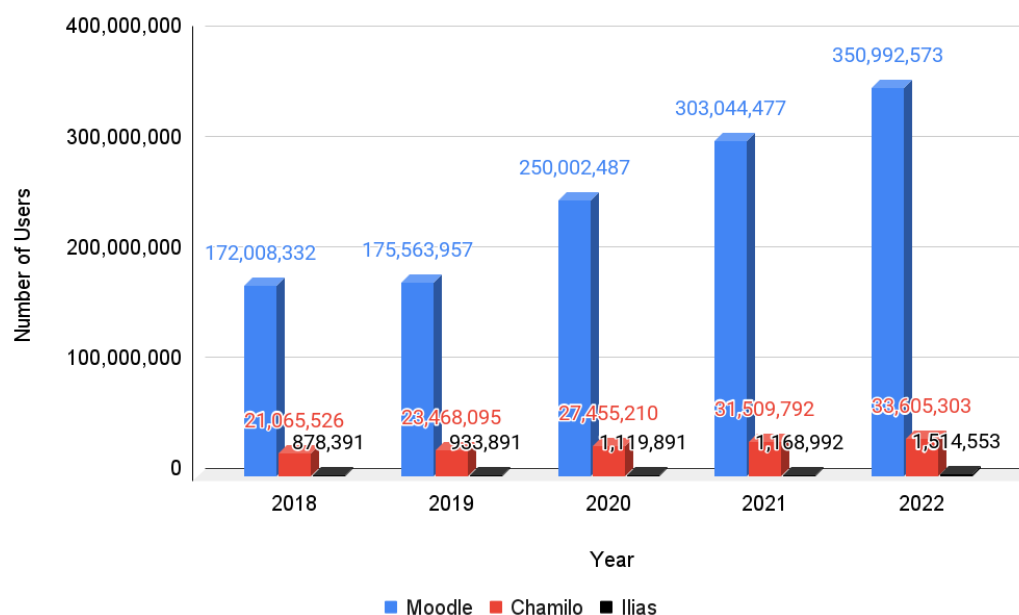


Figure 10. Comparison of usage trends for the Moodle [40], Chamilo [41], and ILIAS [42] LMSs from 2018 to 2022 (before, during, and after the COVID-19 pandemic).

Moodle: Before the COVID-19 outbreak (2018–2019), Moodle reported 17 and 27 vulnerabilities in 2018 and 2019, respectively. Despite these vulnerabilities, Moodle's user base exhibited consistent growth, with 172,008,332 users in 2018 and 175,563,957 in 2019 [40]. As the pandemic hit (2020–2021), Moodle's vulnerabilities decreased slightly to 20 in 2020 and then increased to 21 in 2021. Interestingly, this period saw a substantial increase in user adoption, as the user base surged from 250,002,487 in 2020 to 303,044,477 in 2021 [40]. In the year following the pandemic (2022), Moodle's vulnerabilities experienced a significant spike to 46. Nonetheless, the platform continued to attract users, who reached an impressive 350,992,573 [40]. This suggests that Moodle's vulnerability trends did not strongly deter its user acquisition efforts, indicating the platform's importance in the e-learning landscape.

Chamilo: Preceding the pandemic (2018–2019), Chamilo reported low vulnerabilities, with four in 2018 and three in 2019. This period of low vulnerabilities correlated with growth in the user base, from 21,065,526 in 2018 to 23,468,095 in 2019 [41]. As the pandemic unfolded (2020–2021), Chamilo faced an increase in vulnerabilities, recording five in 2020 and 13 in 2021. Remarkably, Chamilo’s user base continued to expand, reaching 27,455,210 in 2020 and 31,509,792 in 2021 [41]. Post-pandemic (2022), Chamilo managed to reduce its vulnerabilities to nine, while maintaining a relatively stable user base of 33,605,303 [41]. This suggests that Chamilo’s vulnerability challenges did not impede the growth in its user base, indicating the continued relevance of this platform in the e-learning domain.

Ilias: Before the pandemic (2018–2019), Ilias demonstrated favorable security performance, with nine vulnerabilities in 2018 and only one in 2019. Despite catering to a smaller user community, Ilias consistently expanded its user base from 878,391 users in 2018 to 933,891 in 2019 [42]. Amid the pandemic (2020–2021), Ilias maintained its security stability, with two vulnerabilities reported in both years. Concurrently, the platform saw modest user growth, attracting 1,119,891 users in 2020 and 1,168,992 in 2021 [42]. In the post-COVID year 2022, Ilias experienced a slight increase in the number of vulnerabilities to five, while achieving notable user growth, with 1,514,553 users [42]. This underscores the ability of Ilias to balance security integrity with user acquisition, appealing to those seeking a reliable e-learning platform.

In all three cases, the correlation between security vulnerabilities and user usage suggests a complex interplay between security concerns and the perceived value of these platforms for online learning, where user needs and platform features seem to have influenced user adoption despite varying levels of security vulnerabilities.

6. Vulnerability Validation

This section presents a comprehensive data validation process designed to assess the accuracy and reliability of collected security vulnerabilities in the popular e-learning software systems Moodle, Chamilo, and Ilias. By exploiting a combination of automated scanning tools and manual verification techniques, the proposed methodology aims to provide a robust and in-depth assessment of potential vulnerabilities, ensuring the credibility and relevance of the findings of this study.

In the validation process for the collected security vulnerabilities, shown schematically as a flowchart in Figure 11, a multi-faceted strategy is adopted to ensure accuracy and reliability. A virtual machines lab is set up to deploy the e-learning software systems for controlled testing and analysis. OWASP ZAP, a widely used web application security testing tool, is used to perform vulnerability assessments on the deployed systems [43].

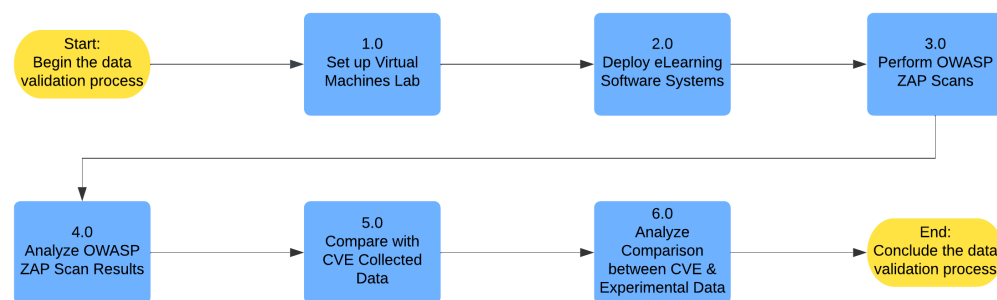


Figure 11. Flowchart of the validation process for the collected security vulnerabilities.

The OWASP ZAP scans validate the identified vulnerabilities by detecting security weaknesses in the LMSs. The results generated by the scans are carefully analyzed to verify the presence of identified vulnerabilities and assess their severity levels. Any inconsistencies or discrepancies between the identified vulnerabilities and the scan results may require further investigation using manual testing, targeted attacks, or additional security assessment tools.

The validation process also considers any patches or updates released by the developers of the LMSs after the COVID-19 pandemic. By checking the status of an identified vulnerability in the latest version of an LMS and comparing it with data from the CVE database, the presence of patches or mitigation measures can be verified.

The use of OWASP ZAP scans in the validation process aims to provide a robust assessment of the security vulnerabilities in the selected LMSs. This methodology enhances the credibility of the collected data and ensures the accuracy and relevance of the study findings.

Table 13 presents a detailed comparison between the analyzed CVE data and the data validated through the experimental process using OWASP ZAP. This table provides insights into the alignment and consistency between the identified vulnerabilities and the results obtained from the OWASP ZAP scans. The results of this comparison enhance the reliability and accuracy of the collected data, ensuring a comprehensive analysis of the security vulnerabilities present in the Moodle, Chamilo, and Ilias LMSs before, during, and after the COVID-19 pandemic.

Table 13. Comparison of collected CVE vulnerabilities and experimental data.

Vulnerability Description	Moodle		Chamilo		Ilias	
	Collected CVE Data	Experiment Data	Collected CVE Data	Experiment Data	Collected CVE Data	Experiment Data
Denial of Service (DoS)	1	-	-	-	-	-
Code Execution	6	-	4	-	-	-
Buffer Overflow	-	-	-	-	-	-
Memory Corruption	-	-	-	-	-	-
SQL Injection	5	-	1	-	-	-
Cross-Site Scripting (XSS)	11	-	2	-	1	-
Directory Traversal	1	-	-	-	-	-
HTTP Response Splitting	-	-	-	-	-	-
Bypass Something	3	-	-	-	-	-
Information Disclosure	-	-	-	-	-	-
Privilege Escalation	-	-	-	-	-	-
Cross-Site Request Forgery (CSRF)	3	-	1	-	-	-
File Inclusion	-	-	1	-	-	-
Absence of Anti-CSRF Tokens (Medium)	-	9	-	27	-	10
Content Security Policy (CSP) Header Not Set (Medium)	-	10	-	111	-	12
Directory Browsing (Medium)	-	2	-	-	-	-
Big Redirect Detected (Potential Sensitive Information Leak) (Low)	-	2	-	-	-	-
Cookie No HttpOnly Flag (Low)	-	1	-	1	-	3
Cookie without SameSite Attribute (Low)	-	1	-	3	-	15
Server Leaks Version Information via "Server" HTTP Response Header Field (Low)	-	18	-	249	-	36
Timestamp Disclosure - Unix (Low)	-	9	-	-	-	-
X-Content-Type-Options Header Missing (Low)	-	15	-	176	-	31
Information Disclosure—Suspicious Comments (Informational)	-	27	-	155	-	33
Modern Web Application (Informational)	-	6	-	41	-	8
User Agent Fuzzer (Informational)	-	192	-	1151	-	-
User Controllable HTML Element Attribute (Potential XSS) (Informational)	-	15	-	1	-	56
Gain Information	-	-	-	-	-	-
Gain Privileges	-	-	-	-	-	-
PII Disclosure (High)	-	-	-	6	-	-
Application Error Disclosure (Medium)	-	-	-	1	-	-
Hidden File Found (Medium)	-	-	-	1	-	-
Missing Anti-clickjacking Header (Medium)	-	-	-	46	-	10
Vulnerable JS Library (Medium)	-	-	-	18	-	6
Information Disclosure—Debug Error Messages (Low)	-	-	-	1	-	-
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (Low)	-	-	-	28	-	12
Cookie Poisoning (Informational)	-	-	-	-	-	12
Information Disclosure—Sensitive Information in URL (Informational)	-	-	-	-	-	5
Loosely Scoped Cookie (Informational)	-	-	-	-	-	12

By adopting this comprehensive strategy, the validation process seeks to ensure the security and integrity of e-learning systems. With the widespread use of online education platforms like Moodle, Chamilo, and Ilias, educational institutions and learners entrust these systems with sensitive data and valuable resources. The validation process is designed to assess the accuracy and reliability of collected security vulnerabilities in these e-learning software systems. The aim of validating the identified vulnerabilities is to ensure that

potential security weaknesses are accurately identified, assessed for severity, and addressed appropriately. The ultimate goal is to enhance the overall security posture of e-learning systems, protecting both user data and institutional assets from potential cyber threats.

Data mismatch between the collected CVE data and experimental data could arise from several factors, contributing to the complexity and nuances of vulnerability assessment in e-learning software systems. Understanding these potential sources of data mismatch is crucial since it can lead to more informed decision making in the realm of cybersecurity. The following are some of the possible sources:

1. **Data source differences:** The CVE database relies on external reports and submissions from various sources, including security researchers, vendors, and organizations. These reports might not cover all vulnerabilities, especially those that are not publicly disclosed or are specific to certain configurations. By contrast, the experimental data are generated through controlled testing using the OWASP ZAP tool, which may uncover unique vulnerabilities that have not yet been reported to the CVE database.
2. **Timing and version differences:** The process of reporting vulnerabilities to the CVE database can be time consuming. After a vulnerability has been discovered, it may take some time for it to be analyzed, verified, assigned a CVE identifier, and added to the database. During this time gap, experimental data collected through OWASP ZAP scans might already reflect the presence of the vulnerability. Moreover, the experimental data collected through OWASP ZAP scans are based on the specific versions of the e-learning software systems (Moodle v4.2, Chamilo v1.11.20, and Ilias v7) deployed in the virtual machines lab. These versions may differ from those in the CVE database, which can lead to a data mismatch.
3. **Configuration and contextual differences:** Certain vulnerabilities may only manifest under specific conditions or server configurations. The experimental data might or might not capture these context-specific vulnerabilities during controlled testing, but such details may or may not be adequately represented or documented in the CVE database, leading to discrepancies that make it challenging to test all possible configurations comprehensively.
4. **Post-pandemic changes:** The study takes into account patches and updates released by the developers of Moodle, Chamilo, and Ilias after the COVID-19 pandemic. Such updates might address vulnerabilities that were previously recorded in the CVE database but are not yet reflected in the experimental data. Consequently, there may be inconsistencies between the two datasets regarding the status of specific vulnerabilities.

It is crucial to emphasize that the validation process remains an ongoing endeavor, consistently refined with the integration of fresh insights. Through a meticulous validation of the amassed data, this study ensures the precision of identified vulnerabilities, thereby faithfully reflecting the evolving security panorama of the LMSs. Such a rigorous validation approach also facilitates the formulation of robust mitigation strategies, instrumental in fortifying the security posture.

7. Discussion and Recommendations

Here, we present the outcomes of our inquiry into security vulnerabilities in the prominent e-learning software systems Moodle, Chamilo, and Ilias. Our analysis revealed a noticeable surge in vulnerabilities, particularly within the Moodle framework, and concurrently identified prevalent vulnerability patterns spanning all three platforms. However, it is crucial to recognize the limitations imposed by our reliance on reported vulnerabilities, underscoring the need for a more comprehensive exploration of the serious and far-reaching consequences of these vulnerabilities. This paper effectively addressed the research questions posed and, on the basis of the results obtained, recommends prioritizing security, communication with developers, and increasing the security awareness of end-users.

7.1. Findings and Limitations

The statistical data analysis revealed the security vulnerabilities of Moodle, Chamilo, and Ilias. The findings provide important insights into the types and trends of vulnerabilities over a five-year period and the potential impact of the COVID-19 pandemic on vulnerability discovery.

The increasing trend of reported vulnerabilities in Moodle over the five-year study period calls for immediate action to address security gaps in the platform. With the rise in cyber threats and attacks on educational platforms, Moodle's developers and administrators must proactively implement robust security measures. Additionally, the consistent prevalence of XSS, code execution, and gain information vulnerabilities highlights the need for a more comprehensive approach to fortify the system's defenses against these common exploit vectors. By doing so, Moodle can safeguard the sensitive data of its users and maintain the trust of its vast user base.

Chamilo, on the other hand, presents a unique vulnerability discovery pattern, showing fluctuations in the number of identified vulnerabilities from year to year. This dynamic nature of vulnerability detection in Chamilo necessitates continuous monitoring and rapid response to any new threats that may arise. Given that XSS remains the most frequently encountered vulnerability in Chamilo, mitigating this particular risk should be a top priority. By focusing on proactive security measures and incorporating regular security audits, Chamilo can better address vulnerabilities and enhance its resilience against potential attacks.

Ilias, by contrast, displays a distinct cyclical pattern in vulnerability discovery, with notable spikes in identified vulnerabilities in 2018 and 2022. Understanding this cyclical nature of vulnerabilities is essential for the developers and maintainers of Ilias. By analyzing the factors contributing to these fluctuations, they can better allocate resources to tackle vulnerabilities during periods of higher risk. Regular security assessments and code reviews can help identify potential weak points in the system, allowing for timely remediation.

Overall, the statistical analysis effectively addressed the research questions by providing insights into vulnerabilities, their impact, and potential trends in Moodle, Chamilo, and Ilias. In addition to these findings, it is worth noting two critical aspects that require special attention. First, the familiarity levels of the user base with these three e-learning platforms—Moodle, Chamilo, and Ilias—are significant factors that can potentially contribute to higher vulnerability if the user base is substantial. A user base well versed in the platform's operations and intricacies is more likely to identify and exploit vulnerabilities. Thus, enhancing security awareness among end users becomes essential to prevent security breaches and unauthorized access. Second, attention should be paid to security vulnerabilities concerning the data uploads, data types, sizes, and form parameters allowed by each of these e-learning platforms. The ability to upload data, varying data types, and form parameters can provide entry points for malicious activities. It is paramount to thoroughly assess the allowed data interactions and implement stringent security measures to prevent data breaches, unauthorized access, and potential malware distribution.

7.2. Recommendations for Users

Educational institutions, administrators of e-learning platforms, and operators of the platforms should accord paramount importance to the security dimensions of Moodle, Chamilo, and Ilias. The subsequent set of recommendations is intended to fortify the security fabric of e-learning software systems:

1. Conduct regular security audits to identify and mitigate vulnerabilities through code reviews, penetration testing, and vulnerability assessments.
2. Stay updated and promptly apply security patches to address known vulnerabilities.
3. Provide security training and awareness programs for system administrators, operators, and end users to reduce the risk of successful attacks.

4. Foster collaboration and information sharing among stakeholders, educational institutions, platform developers, and security researchers to address vulnerabilities and emerging threats.
5. Evaluate the security aspects of third-party integrations and regularly review and update them to maintain system security.
6. Develop and implement incident response plans to minimize the impact of security breaches or vulnerability exploits.
7. Educate end users about security risks and promote best practices, such as strong passwords, two-factor authentication, and safe browsing habits.

7.3. Recommendations for Vendors

Vendors and developers in the realm of e-learning software systems, encompassing platforms such as Moodle, Chamilo, and Ilias, should proactively enhance the security measures embedded within their products. The following set of insights and recommendations can guide this essential enhancement procedure:

1. Implement secure coding practices and follow established software development frameworks, integrating security at every stage.
2. Establish vulnerability disclosure and reporting mechanisms, promptly addressing reported vulnerabilities and keeping users informed.
3. Provide timely security updates and patches, emphasizing their importance and providing guidance on the update process.
4. Develop comprehensive and accessible security documentation to help users implement and maintain secure configurations.
5. Conduct regular security testing, including penetration testing, vulnerability scanning, and code audits.
6. Invest in ongoing security training for developers and personnel involved in the software's development and maintenance.
7. Foster an engaged user community, encouraging feedback, bug reporting, and feature requests to improve security and functionality.

8. Conclusions

This paper explores the security vulnerabilities of the Moodle, Chamilo, and Ilias e-learning software systems before, during, and after the COVID-19 pandemic. Through a comprehensive analysis of existing literature, data collection from the CVE database, and statistical data analysis, valuable insights are gained into the nature of these vulnerabilities, their impact, and their potential trends.

The findings of this study reveal that these e-learning software systems have faced security threats and vulnerabilities before, during, and after the COVID-19 pandemic. It is evident that addressing these vulnerabilities is crucial for ensuring the integrity, confidentiality, and availability of educational resources and data. On the basis of the results of this research, several recommendations are formulated. It is recommended that stakeholders, including educational institutions and e-learning platform vendors, prioritize the security aspects of Moodle, Chamilo, and Ilias. Regular security updates and patches should be implemented to mitigate risks. Additionally, strong emphasis should be placed on user education and awareness to prevent and mitigate potential security incidents.

This study contributes to furthering understanding of the security vulnerabilities in e-learning software systems and provides insights that can guide future research and practical applications. By addressing the security vulnerabilities in the Moodle, Chamilo, and Ilias learning management systems, educational institutions can enhance the overall security posture of their online environments, contributing to the security, and hence the sustainability, of online education systems.

Author Contributions: The work presented here was performed in a collaboration involving all the authors. Conceptualization, S.A.-L.A. and A.I.A.; Data Curation, S.A.-L.A.; Methodology, A.I.A.; Investigation, S.A.-L.A.; Formal Analysis, S.A.-L.A.; Writing—Original Draft Preparation, S.A.-L.A. and A.I.A.; Writing—Review and Editing, S.A.-L.A. and A.I.A.; Visualization, S.A.-L.A.; Research Supervision, A.I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that there is no conflict of interest.

References

1. UNESCO. *Education during COVID-19 and Beyond*; Technical Report; United Nations Educational, Scientific and Cultural Organization: Paris, France, 2020.
2. Unesco Institute of Statistics. UIS COVID-19 Response: Data to Inform Policies that Mitigate Setbacks in Education Gains. 2020. Available online: <https://uis.unesco.org/en/news/uis-covid-19-response-data-inform-policies-mitigate-setbacks-education-gains> (accessed on 5 August 2023).
3. Arogbodo, M. Impacts of the COVID-19 pandemic on online security behavior within the UK educational industry. *PsyArXiv* **2022**. [CrossRef]
4. Murphy, M.P.A. COVID-19 and emergency eLearning: Consequences of the securitization of higher education for post-pandemic pedagogy. *Contemp. Secur. Policy* **2021**, *41*, 492–505. [CrossRef]
5. Lockee, B.B. Online education in the post-COVID era. *Nat. Electron.* **2021**, *4*, 5–6. [CrossRef]
6. TS Briefing. *Impact and Implications of the COVID-19-Crisis on Educational Systems and Households*; Technical Report; Trade Union Advisory Committee (TUAC) to the OECD: Paris, France, 2020.
7. Ahmed, F.R.A.; Ahmed, T.E.; Saeed, R.A.; Alhumyani, H.; Abdel-Khalek, S.; Abu-Zinadah, H. Analysis and challenges of robust e-exams performance under COVID-19. *Results Phys.* **2021**, *23*, 103987. [CrossRef] [PubMed]
8. Almaiah, M.A.; Al-Khasawneh, A.; Althunibat, A. Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Educ. Inf. Technol.* **2020**, *25*, 5261–5280. [CrossRef] [PubMed]
9. Irish Tech News. How COVID-19 Affected e-Learning and Its Security. 2020. Available online: <https://irishtechnews.ie/how-covid-19-affected-e-learning-and-its-security/> (accessed on 5 August 2023).
10. Alexei, A.; Alexei, A. Cyber security threat analysis in higher education institutions as a result of distance learning. *Int. J. Sci. Technol. Res.* **2021**, *10*, 129.
11. Jackson, M. The Impact of Cyberattacks and Cyberthreats on Higher Education Institutions. Master's Thesis, College of St. Scholastica, Duluth, MN, USA, 2021.
12. Hubken Group. What Is Moodle? The Ultimate Guide to Moodle LMS. Available online: <https://www.hubkengroup.com/resources/what-is-moodle-lms-guide> (accessed on 5 August 2023).
13. Joinup European Commission. About Chamilo LMS. Available online: <https://joinup.ec.europa.eu/collection/education-culture-and-sport/solution/chamilo-lms/about> (accessed on 5 August 2023).
14. NEST. ILIAS—Reliable and Quality Learning Management System. Available online: <https://en.online-learning.bg/ilias-lms> (accessed on 5 August 2023).
15. Fuchs, H. Yale faces lawsuit for data breach. *Yale Daily News*, 2018. Available online: <https://yaledailynews.com/blog/2018/08/31/yale-faces-lawsuit-for-data-breach/> (accessed on 5 August 2023).
16. Paudel, P. Online education: Benefits, challenges and strategies during and after COVID-19 in higher education. *Int. J. Stud. Educ. (IJonSE)* **2021**, *3*, 70–85. [CrossRef]
17. Annand, D.; Huber, C.; Michalczyk, K. The use of Lotus Notes as a comprehensive learning, evaluation and production system. In Proceedings of the Computers and Advanced Technology (CATE) Conference, Cancun, Mexico, 20–22 May 2002.
18. Bardesi, H.; Razek, M.A. Learning outcome e-exam system. In Proceedings of the Sixth International Conference on Computational Intelligence, Communication Systems and Networks, Tetovo, Macedonia, 27–29 May 2014; pp. 77–82.
19. Awad, F.R.; Ahmed, T.E.; Siddik, M.S.M. The readiness of countries for E-learning with special focusing on the Sudanese experience. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 181–184.
20. Adebayo, O.S.; Abdulhamid, S.M. A survey on e-exams system for Nigerian universities with emphasis on result integrity. *J. Sci. Technol. Math. Educ.* **2011**, *7*, 173–180.
21. Egwunyenga, E.J. Problems of examination malfeasance in Nigerian Universities: Emergent issues and management options. *J. Soc. Sci.* **2019**, *21*, 161–666. [CrossRef]
22. Idemudia, S.; Rohani, M.F.; Othman, S.H. An improvement of student examination assessment through online (e-Exam) by considering psychological distress factors. *Int. J. Comput. Sci. Inform. Technol. Secur. (IJCSITS)* **2016**, *6*, 39–45.

23. Saleous, H.; Ismail, M.; AlDaajeh, S.H.; Madathil, N.; Alrabaee, S.; Choo, K.K.R.; Al-Qirim, N. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digit. Commun. Netw.* **2022**, *9*, 211–222. [CrossRef] [PubMed]
24. Tick, A.; Cranfield, D.J.; Venter, I.M.; Renaud, K.V.; Blignaut, R.J. Comparing three countries' higher education students' cyber related perceptions and behaviours during COVID-19. *Electronics* **2021**, *10*, 2865. [CrossRef]
25. Fouad, N.S. Securing higher education against cyberthreats. *J. Cyber Policy* **2021**, *6*, 137–154. [CrossRef]
26. BBC News. Northumbria University Hit by Cyber Attack. 2020. Available online: <https://www.bbc.co.uk/news/uk-england-tyne-53989404> (accessed on 5 August 2023).
27. BBC News. How Hackers Extorted \$1.14 m from University of California, San Francisco. 2020. Available online: <https://www.bbc.co.uk/news/technology-53214783> (accessed on 5 August 2023).
28. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef] [PubMed]
29. Wickline, T. The Capabilities of Antivirus Software to Detect and Prevent Emerging Cyberthreats. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
30. Steingartner, W.; Galinec, D.; Kozina, A. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry* **2021**, *13*, 597. [CrossRef]
31. Ngwacho, A.G. COVID-19 pandemic impact on Kenyan education sector: Learner challenges and mitigations. *J. Res. Innov. Implic. Educ.* **2020**, *4*, 128–139.
32. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing attacks: Recent comprehensive study and a new anatomy. *Front. Comput. Sci.* **2021**, *3*, 6. [CrossRef]
33. Ramesh, G.; Menen, A. Automated dynamic approach for detecting ransomware using finite-state machine. *Decis. Support Syst.* **2020**, *138*, 113400. [CrossRef]
34. Chatterjee, D. *Cybersecurity Readiness: A Holistic and High-Performance Approach*; SAGE Publications: Thousand Oaks, CA, USA, 2021.
35. Major Data Breach: Personal Information of 360,000 Teachers and Former Teachers in Quebec Exposed. Available online: <https://montreal.ctvnews.ca/major-data-breach-personal-information-of-360-000-teachersand-former-teachers-in-quebec-exposed-1.4822449> (accessed on 5 August 2023).
36. Feng, X.; Feng, Y.; Dawam, E.S. Artificial intelligence cyber security strategy. In Proceedings of the 2020 IEEE International Conference on Dependable, Autonomic and Secure Computing/International Conference on Pervasive Intelligence and Computing/International Conference on Cloud and Big Data Computing/International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 17–22 August 2020.
37. CVE Details. Moodle Vulnerability Statistics. Available online: https://www.cvedetails.com/vulnerability-list/vendor_id-2105/product_id-3590/Moodle-Moodle.html (accessed on 5 August 2023).
38. CVE Details. Chamilo Vulnerability Statistics. Available online: https://www.cvedetails.com/vulnerability-list/vendor_id-12983/Chamilo.html (accessed on 5 August 2023).
39. CVE Details. Ilias Vulnerability Statistics. Available online: https://www.cvedetails.com/vulnerability-list/vendor_id-12023/Ilias.html (accessed on 5 August 2023).
40. Moodle. Statistics. 2023. Available online: <https://stats.moodle.org/> (accessed on 5 August 2023).
41. Chamilo. Chamilo Stats. 2023. Available online: <https://stats.chamilo.org/> (accessed on 5 August 2023).
42. ILIAS. Known Installations. 2023. Available online: https://docu.ilias.de/ilias.php?baseClass=ilrepositorygui&cmdNode=xd:ly:a0&cmdClass=ildclrecordlistgui&cmd=show&ref_id=3444&tableview_id=9 (accessed on 5 August 2023).
43. ZAP Alert Details. Available online: <https://www.zaproxy.org/> (accessed on 5 August 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.