Review of Online Examination Security for the Moodle Learning Management System

Said Ally
The Open University of Tanzania, Tanzania

ABSTRACT

Moodle software has become the heart of teaching and learning services in education. The software is viewed as a trusted modern platform for transforming learning and teaching modes from conventional face-to-face to fully online classes. However, its use for online examination is very limited despite having a state-of-the-art Quiz Module with features which can auto-generate random question papers and marking schemes. This paper presents a security profile of the Moodle platform as an integral component for administration of online examinations by reviewing its pedagogical assessment features, software configurations, and settings of the Quiz module. The results provide crucial insights that show the Moodle Quiz module is a rich workspace that meets all practical requirements for an efficient, secured, cost-effective, and virtually enabled standard online examination platform. The findings suggest that Moodle can be an effective assessment system if the software is properly and securely hosted and configured on a well established and reliable computing infrastructure.

Keywords: *Moodle Quiz; Software; Security; Online Examination; Assessment*

INTRODUCTION

Security in online examinations is a critical need among educators. Increasing learning demands, the rise of Internet usage, high cost of running face to face examinations, and the need to provide students with immediate feedback, have all together brought about a paradigm shift. This shift from traditional pen and paper to the adoption and use of online examinations makes the examination accessible at any time, on any smart device, and from anywhere.

A typical online examination platform must possess a question bank (Konde *et al*., 2019), and should be designed on secured and trusted software which can automate the generation of question papers and marking schemes based on the set timetable. Other key features include advanced scoring and grading system; time management; candidate verification and authentication; navigation style for moving back and forth on pages; functionalities for remote invigilation of candidates; and security features including use of a safe browser, multi support of various question types, random ordering of pages; shuffling of questions and choices for each candidate; date and time restrictions; and generation of various statistical reports. An online examination system replaces the costs associated with the printing of examination papers, packing, and transportation. Other apparent benefits of online examinations over the traditional pen and paper system include a high flexibility level, as candidates can be assessed from anywhere (Kabir *et al*., 2019), reliability in grading, and efficiency of time, effort and operation (Shraim, 2019).

Even though an online examination is administered using a dedicated software (Kaburlasos *et al*., 2004), the learning management systems (LMS) such as Moodle can also provide efficient administration for online examinations (Sorensen, 2013) when properly configured. Moodle is an acronym for *modular object oriented dynamic leaning environment*. Thus, Moodle provides an

efficient instructor-led and self-paced LMS to support collaborative and multilingual online classes which can take different forms. Moodle supports classes of any size, with students of different ages, from all sectors, and at a variety of educational institutions at all levels. This is possible because Moodle is essentially a virtual learning environment (VLE) capable of transferring knowledge from learner to learner and instructor to learner with an easy to use software interface, drag-and-drop features, and well-documented resources. The teaching and learning services are efficiently administered because Moodle is an all-in-one LMS platform consisting of a powerful set of learner-centric features and flexible tool-set to ensure continuity, iterative, and interactive processes. Some of the supported Moodle activities and tools includes *forums*, *glossaries*, *wikis*, *assignments*, *quizzes*, *choices (polls)*, *SCORM players*, *databases*, *blogs*, *messaging*, *participation, and chats*.

Moodle is an open source community-based software as it is freely downloadable from the Moodle site for adopters to adapt, extend, and modify its source codes. The open source characteristic has made the software robust, secure, modular, and scalable to any size to suit adopters' specific needs. Furthermore, the software supports globally accepted open standards for interoperability (Ueda, *et al*., 2018) to comply with modern standard operating systems, mobile-compatible interfaces, and function with multiple cross-browsers.

There is currently a rapid increase of Moodle adoption at a global level (Yildiz *et al*., 2018) with over 60% usage by higher learning institutions (HLIs) worldwide. The data at January 2022, shows that the software has already reached a user base of 302 million Moodlers, with official registered sites of 180,000, and about 39 million developed courses as shown in Table 1 below:

Table 1: *Moodle Statistics*

SN	Statistical Item	Status
1	Sites	180,000
2	Courses	39,000,000
3	Users	302,000,000
4	Enrolments	1,712,000,000
5	Forum Posts	672,000,000
6	Resources	330,000,000
7	Quiz Questions	6,022,000,000
8	Countries	241
9	Certified Partners	90
10	Percentage Usage by HLIs	Over 60%

Source: Moodle Site, Jan 2022

Despite this large number of Moodle adopters worldwide, and availability of the state-of-the-art functionality of the Moodle Quiz Module (MQM), its usage as an examination platform is very limited. Within the next few years, MQM is likely to become an important online assessment platform as the future aspirations of most HLIs rely on digital education and lifelong learning. The free Moodle license, with its open-source advantages, and rapid expansion of user base, as well as the pace of software enhancement have always been primary reasons which make Moodle trusted as an integral LMS within open and distance learning (ODL) environments. Furthermore, the rise of emerging technologies, the existing institutional and national educational strategies (OUT, 2018; URT, 2015), and the effects of the COVID-19 pandemic which has largely disrupted the educational continuity, make online teaching, learning and assessment no longer an option among HLIs.

This paper presents a perspective on how to securely configure the Moodle platform to support the smooth administration of online examinations. The fact that Moodle is an open-source software (OSI, 2004), freely distributed under the terms of the GNU public license (GPL), (Dhika, *et al*., 2020), adopters might find it a viable and cost-effective platform suitable to run online examinations, in an efficient and secured manner, provided a proper implementation of computing and pedagogical requirements is achieved.

MATERIALS AND METHODS

Research Design

To undertake this study, software review and experimental techniques have been used together in a coherent and logical way to constitute the blueprint for the data collection as proposed by De Vaus (2006). As indicated in Figure 1, the software review was accomplished in the front-end and back-end side of the Moodle software. While the front-end software review focused on pedagogical aspects, quiz default settings and anti-cheat protection features, the back-end software review was mainly completed in the underlying supporting software, system configuration and source codes, and security settings at the level of firewall, SSL, and password salting.
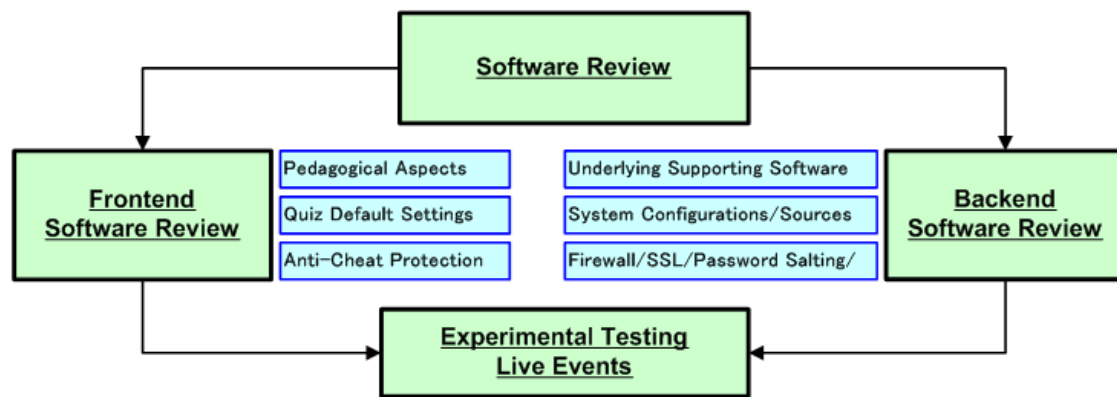

Figure 1: Framework for research design

On the other hand, data were collected from experimental testing of the Moodle software through running live events for online examination sessions.

Software Review

To review the software, the functionalities of the Moodle Quiz Module were critically studied with focus on the security configurations, default settings, and source code screening. Such a technique is fully compliant with the security assessment of any web based open-source software and is aimed at identifying the software design weaknesses and common adopter misconfigurations. Thus, a review of the security threats and Moodle bugs was conducted as follows:

- at the software level using a stable version 3.9 to assess usability of MQM features, integrated Moodle plugins, patches, and upgrades.
- through advanced technique of vulnerability search from the National Vulnerability Database source (NVD, 2021) by matching all Moodle related keywords so as to generate the Common Vulnerabilities and Exposures (CVEs).

- by comparing OWASP Top 10 web vulnerabilities (Khan *et al*., 2019; OWASP, 2021) in relation to Moodle bugs.

Experimental Testing

In addition to software review, a live session testing was conducted using Moodle Quiz with Live Events. To test the performance of a Moodle Quiz module, three online examination sessions were set on 19th, 20th, and 26th February 2021 for non-degree and undergraduate students. Each session was tested using a total of 41 questions constructed with 10 Multiple Choice Questions (MCQs), 28 True/False Questions (TFQs), and 3 Short Answer Questions (SAQs). Depending on the agreed assessment plan, sessions were either conducted as partial real time (PRT) or full real time (FRT) online examinations as indicated in Table 2 below

Table 2: Assessment Plan for MQM Testing with Live Events

Session No	Mode	Question Type	Average Time (Min)	Average Class Performance Score (%)
I	PRT	MCQ, TFQ, SAQ	37.8	44.2
II	PRT	MCQ, TFQ, SAQ	35.5	60.1
III	FRT	MCQ, TFQ, SAQ	33.0	67.9

RESULTS AND FINDINGS

From the Moodle software review and experimental testing conducted, 15 key features categorized as pedagogical, anti-cheat protection, backend security, and experience from live MQM live events were found. The results shown in Table 3 represent the key aspects for facilitating the administration of online examinations using the Moodle platform.

Table 3: Results of Software Review Process and Experimental Testing

Observed Feature	Pedagogical Features	Security Features for Anti-Cheat Protection in Moodle	Moodle Backend Security	Live MQM Events
Moodle Quiz Module	√			
Supported Question Types	√			
Subjects with Special Requirements	√			
Statistical Reports and Item Analysis	√			
Security in Question Paper		√		
Moodle Logs		√		
Add-on Security Plugins		√		
Software License, Sustainability, and Compliance to International Standards			√	
Active Directory and Password Policy			√	
Enforcing Firewall and Secure Socket Layer			√	

MD5 Security Algorithm and Password Salting			√	
Spam Management in Moodle			√	
User Knowledge Challenges				√
Infrastructure Challenges				√
Student's Participation Level				√

Pedagogical Features

Four pedagogical features relevant for running online examinations were found in Moodle. The features include Moodle *Quiz Module (MQM), various question types, supported subjects with special requirements,* and *the statistical reports and item analysis for student performance analysis*.

Moodle Quiz Module

Moodle software consists of the Quiz module which is a very powerful tool that meets many assessment needs. The software can accommodate simple, multiple-choice knowledge tests to more complex, self-assessment tasks including both tutor-marked (TME) and computer-marked (CME) questions depending on the choice of the examiner. Furthermore, the MQM tool allows questions to be created and stored separately in a question bank for future reuse purpose.

Supported Question Types

Moodle allows any type of question paper design or exam blueprint to be directly created and generated from the software. The format of the question paper can be varied with various question types, question weights, and different scaling systems. For instance, Moodle supports numerical question type referred to as "calculated" which comes with security attributes. The questions are constructed with numbers selected randomly from a defined set. For example, the question below can be defined as numerical instead of essay type.

> "*Calculate the average memory access time (Tm) between CPU and RAM given the CPU hit ratio (h) is 95% and the values of cache hit (Tc) and cache miss (Tp) are 100 ns and 800 ns respectively*".

The added security advantage of such kinds of numerical questions is the ability of Moodle in to shuffle the numerical values of **Tm**, **Tc**, **Tp**, and **h** based on the defined set of numbers. The question types supported in the Moodle platform are shown in Table 4 below.

Table 4: Moodle Supported Question Types

Question Type	Question Description
☷ Multiple choice	Allows the selection of a single or multiple response from a pre-defined list
•• True/False	A simple MCQ question with only two choices: True or False
▭ Short answer	Response of one or few words compared to model answers which may contain wild cards.
₁₂ Numerical	Numerical response with units graded by comparing model answers with tolerances.

	Calculated	Like numerical questions but with the numbers used selected randomly from a set.
	Essay	Long term question with online text.
	Matching	The answer to each of a number of sub questions must be selected from a list of possibilities.
	Random short-answer matching	Like a matching question, but created randomly from the short answers in a particular category.
	Embedded answers (Cloze)	Flexible questions created by entering text containing special codes that create embedded MCQs, SAQs, and numerical questions.
	Calculated multichoice	Are like MCQs but with choice elements which include results from numeric values that are selected randomly from a set.
	Calculated simple	Simple version of calculated question which are like numerical questions but with the numbers used selected randomly from a set.
	CodeRunner	Runs student submitted code in a sandbox.
	Drag and drop into text	Missing words in the question text are filled in using drag and drop.
	Drag and drop markers	Markers are dragged and dropped onto a background image. This question type is not accessible to users who are visually impaired.
	Drag and drop onto image	Images or text labels are dragged and dropped into drop zones on a background image. This question type is not accessible to users who are visually impaired.
	Select missing words	Missing words in the question text are filled in using drop-down menus.

Subjects with Special Requirements

Moodle supports subjects with special requirements by integrating standard or compatible third-party modules and plugins. For instance, Moodle uses TeX notation or DragMath equation editor for Mathematics, Hotpot and Poodll plugins for language, and chemistry plugins for displaying molecular structures. As shown in Table 4, Moodle comes with inbuilt Code Runner which work as a software compiler to run programming codes. In addition to subject-specific plugins, Moodle can further support students with disabilities by incorporating several assistive technologies such as screen-readers, screen-magnifiers, alternative mouse, and disabling AJAX and JavaScript to increase software usability levels.

Statistical Reports and Item Analysis

Further screening carried out with Moodle Quiz shows that Moodle is rich in terms of automated tools to easily perform statistical and psychometric analysis. When many students answer a question either correctly or incorrectly, it suggests that the question is either too easy or too difficult. Conducting an item analysis therefore becomes vital for student feedback and for improving teaching and learning techniques, especially when the created questions are too difficult, have flaws, or when students are guessing. Moodle can generate a full assessment report with details of examinations conducted, structure analysis, and printed questions in a

variety of file formats such as comma separated values (.csv), Microsoft Excel (.xlsx), HTML table, Javascript Object Notation (.json), OpenDocument (.ods), and Portable Document Format (.pdf). The basic components of the report include *quiz name, course name, time quiz opens, time quiz closes, exam duration (hours), number of complete attempts, graded attempts, average grade of all attempts (%), median grade (%), standard deviation (%), score distribution skewness, score distribution kurtosis, coefficient of internal consistency (%), error ratio (%), and standard error (%).* The coefficient of internal consistency is also called a Cronbach Alpha. This is a measure of whether all the items in the quiz are testing basically the same thing. The higher the value of the Cronbach Alpha, the better the reliability of questions. Furthermore, for each exam question, Moodle generates a report showing the q*uestion name, number of attempts, facility index, standard deviation, random guess score, intended weight, effective weight, discrimination index, and discriminative efficiency.* Moodle performs automatic analysis of the Facility Index (FI) and the Discrimination Index (DI) with values ranging from 0% to 100%. The FI ("P-value") refers to item difficulty and shows the percentage of students that answered a question correctly. The higher the "P-value" that is, closer to 100%, the easier the question, implying that many students selected the correct answer regardless of the overall pass rate. On the other hand, the DI-value indicates correlation between the score for the question and the overall score attained in the examination, that is, the higher the DI-value for a question, the more 'discriminating' the question is, implying that most students who performed well on the examination have also answered the question correctly, and vice versa. Moodle is useful in finding "broken" questions especially when an examiner has inserted a wrong answer to the question. The marker is alerted when the value in the DI-column is very small to prompt for further investigation of the attempted question to check whether the question was marked correctly.

Live Events for Moodle Quiz Module

As noted in the live testing sessions, three major key areas to realize implementation of online assessment were identified. They include *user knowledge, infrastructure capacity*, and *student participation rate*.

User Knowledge

The most striking challenge encountered during the live event was user's inadequate knowledge in using features of the Moodle Quiz Module (MQM). Most of the MQM features including advanced question types and system settings were not utilized. On average, most question papers used TFQ, MCQ, and SAQ question types. Tutors were not able to apply the advanced MQM security features, perhaps not to mislead students when accessing the question paper. For instance, Safe Exam Browser (SEB) on the client machine and password restrictions were not enforced due to lack of user awareness and guiding procedures on how an examiner can share a password instantly for the students to get access to the question paper. Most examiners were not aware that client machines require SEB installation before the first attempt.

Infrastructure

Moodle supports classes of different sizes ranging from a few students to millions depending on the capacity of the computing infrastructure for the processor/CPU speed, memory/RAM capacity, and bandwidth size. As noted in the heavy sessions of the live MQM event where the candidates login concurrently, the majority of students were not able to access the Moodle site due to a mismatch between server resources and computing workloads. As shown in Table 5, many unfinished attempts were experienced in a one-hour online test for the course OCP 100 with over 600 students. A test with 41 questions was set to display each question on its own webpage. This means that a total of 600x41=24,600 concurrent server requests were constrained within a period

of 60 minutes just for a single course. On average, each cell in the examination timetable at the Open University of Tanzania consists of at least 30 courses as a typical computing requirement for online assessment. The fact that 1 GB of RAM in Moodle can efficiently handle 50 concurrent users, a testing Moodle server equipped with 128 GB of RAM was able to handle 6,400 concurrent server requests (128 GB x 50) with time buffer up to five seconds. Server requests include processing a webpage written in PHP, querying the database, or simply transferring a file, all being processes which consume memory and database connections during expected peaks such as when everyone logs in, when everyone starts their test, and the time when everyone clicks "submit all and finish". When all students click the start button at nearly the same time, the chance that the server will crash is maximized. Thus, being server intensive, a proper planning and balance between computing workloads and computing resources is vital for efficient administration of the Moodle quiz feature.

Student's Participation Level

The study highlighted the strengths of partial real time (PRT) because despite the infrastructure challenges, the participation level was satisfactory. The first two MQM sessions were better in flexibility because the quiz setting allowed students to take their test in a span of 8 hours from 14:00 to 22:00 hours. As shown in Table 5, there was a significant improvement from MQM session 1 to MQM session 2 with the percentage of completion success level increasing from 68.5% to 90.4% of candidates with "finished" status compared to the total number of attempts. Surprisingly, the third full real time online MQM session recorded the highest percentage success level of 99.0% even though it was hard to implement due to intensive resource consumption constraints within a very short time. However, this was possible because session 3 was conducted after normal business hours.

Table 5: *MQM Performance Indicators and Participation Level*

Performance Indicator	Online Exam Session		
	Session I (PRT)	Session II (PRT)	Session III (FRT)
Date	19th Feb 2021	20th Feb 2021	26th Feb 2021
Finished	332	529	704
In Progress	52	18	7
Never Submitted	79	31	0
Overdue	22	7	0
Total Attempts	**485**	**585**	**711**
% Success	**68.5%**	**90.4%**	**99.0%**

Figure 1 provides an illustration of student participation levels against performance indicators of the MQM experiment conducted between the 19th and 26th February, 2021 for all three online examination sessions.
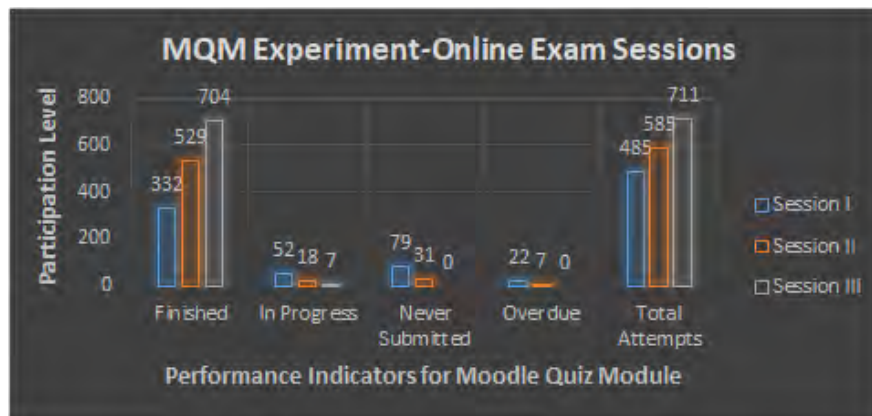
Figure 1: MQM Performance Indicators and Participation Level

Security and Anti-Cheat Protection Features in Moodle

Security in Question Paper

Our experiment in the live test session confirmed that the Moodle Quiz module possesses key security features necessary for setting up a standard online examination that discourages students from cheating. Some of these security features include a *time limit, ability to retrieve questions from question banks on a random basis, choosing navigation mode (free or sequential), restrictions on the number of attempts, randomization and shuffling of questions, and the use of extra passwords.* When questions are shuffled, Moodle automatically changes the order of the questions in a random order every time the session is activated. This makes it harder for students to share answers and to discuss a particular question. For multiple choice questions, shuffling can be extended to the level of distractors for different attempts. When two or more students are working on an exam with randomized answers drawn from a question bank, they will be unable to split the question paper or copy from one another. To prevent students from sharing answers, Moodle uses the question bank facility to group questions with respect to difficulty level such as "*easy*", "*moderate*" and "*difficult*" so that the questions for each student are drawn on a random basis to have a unique, but balanced question paper. Furthermore, the access to the question paper can be restricted based on *sequential* or *free* navigation mode with limits on the number of displayable questions for each webpage. When one question is loaded per page, students will be prevented from taking screenshots and sharing the questions.

Another security feature on the question paper design is the ability of Moodle to control student review options during the attempt, immediately after the attempt, and after the close of the quiz. Areas of the review include *the attempt, whether correct, marks, specific and general feedback, right answer, and the overall feedback.* For all review options, Moodle can hide review summary until when the session is fully closed.

Moodle Logs

As any other software, Moodle has logs with timestamps of student activities and Moodle data. Moodle logs are useful to provide efficient security in the marking stage because any attempts at examination irregularities and malpractices are automatically recorded. Such student malpractices can easily be detected when a student attempts to switch between tabs, browsers, and windows. Moodle logs save all records for future use instantly when the candidate leaves the Moodle screen.

Add-on Security Plugins

Further screening on the Moodle platform shows that the platform is highly flexible and interoperable to allow integration of pluggable authentication architecture. The most common Moodle plugins related to security of online examination include *Safe Exam browser (SEB), iSpringSuite Quiz Maker, Plagiarism Check (Turnitin),* and *Video Assistant Invigilator (VAI).* When SEB is enabled, Moodle is automatically locked from using any other web browsers and becomes fully operating in a state where additional tabs are disabled, navigation is restricted, and the cut/copy/paste and right-clicks remain inactive. The Video Assistant Invigilator (VAI) is an artificial intelligence (AI), and human based proctoring tool useful for detection of facial, voice, mobile phone, distraction, multiple people, and live proctoring wherein invigilators monitor multiple candidates in a single view. The Turnitin plagiarism plugin is useful for checking similarities in text to validate submitted text.

Moodle Backend Security

Software License, Sustainability, and Compliance to International Standards

As noted during the software screening process, Moodle is publicly accessible with open source codes freely provided under the general public license (GNU-GPL). Moodle license is stable, well assured, and static because modification is practically impossible. This is because a change of Moodle license needs to be completed and approved by all Moodle developers in the world and should not apply retrospectively. This attribute is significant for administration of online examinations as it is a viable, cost effective and a sustainable community supported software.

From the software development angle, Moodle is committed to safeguarding data security because Moodle project (Moodle, 2022) operates under scrutiny and is supported by a team of dedicated full-time developers and a network of certified Moodle Partners from an active international community. Thus, the software is highly trusted as it is compliant to international standards. Some of these standards include open source initiative (OSI), certified Learning Tool Interoperability (IMS LTI), a global technical standard of integrating learning applications, and a Sharable Content Object Reference Model (SCORM) specification. This compliant level as a web-based e-learning platform with interoperability capabilities among various LMS has also been suggested by Ueda, *et al*., (2018). Being able to support open standards with high levels of interoperability, flexibility and scalability, Moodle can be integrated with plugins, add-ons, external applications, and any other VLE/LMS-specific modules suitable for typical teaching and learning purposes.

Active Directory and Password Policy

Moodle security is further strengthened with configuration of advanced security facilities such as active directory and password policy. Moodle uses a database of active directory services to securely connect users to the network resources using critical information about the computing environment, user matrix and profiles supported by a widely-used LDAP standard authentication protocol responsible for the enrolment function.

The use of a password policy underlines how secure Moodle is. The policy ensures password complexity is maintained throughout the entire lifetime of Moodle usage by forcing users to change passwords on a regular basis, and to limit password reuse by taking control of the rotation scheme. Some features of a strong password in Moodle include the minimum length of password, number of digits, number of lower-case and upper-case characters, and the number of special non-alphanumeric characters. A default Moodle password setting must have a length of eight (8) characters at minimum and at least one (1) character to represent a digit, lowercase

letter, uppercase letter, and a special non-alphanumeric character. If a user enters a password that does not meet the set password requirements, Moodle generates an error message.

Enforcing Firewall and Secure Socket Layer

Further security analysis of the Moodle site showed that both firewall configurations and a secure socket layer (SSL) can be enforced to increase the security of online examinations. Firewalls set security rules to control and monitor the incoming and outgoing network traffic. The rules allow and block connections to the server based on the specified IP addresses. In contrast to the old Moodle versions which did not support SSL implementation all over the site (Kumar & Dutta, 2011), SSL configurations have become very powerful security features in Moodle sites to ensure that passwords and the privacy of users are protected, and all webpages use *https* during data transmission to remain in a secured state. The links between web server and browser are encrypted to avoid session hijacking and to ensure all traffic from Moodle instance and users are protected.

MD5 Security Algorithm and Password Salting

Another security utility of the Moodle platform is its ability to store user passwords in an encrypted form using a one-way hashing function called MD5 algorithm which normally converts the plain password text into an encrypted message digest in the form of cipher text or fingerprint. One advantage of the MD5 security algorithm is that its hashed output cannot be converted back to its original format (Bhandari, *et al*., 2017), and the password hashing can be made more secure by applying techniques of password salting. The importance of password salt cannot be undermined. It reduces the risk of password theft as it makes it harder to decrypt or reverse the password by adding a longer random string of characters before the hash is calculated (Tian, *et al*., 2018). Likewise, Moodle provides additional security settings for password salt configured at the user level in addition to site level. The ability to generate password salt at user level is a vital security feature to protect Moodle from internal threats which cannot be handled by a site-wide configuration variable for the salt.

Spam Management in Moodle

Like any other web application, Moodle is susceptible to attack due to threats associated with spams. However, spams can only penetrate if Moodle is not properly configured. As found in the software screening process, Moodle generates a security threats analysis report with a spam profile. Based on this report, efficient rootkit detector (Rootkit, 2021) as well as critical software configurations can be used to reduce spams and prevent a Moodle site from hacking, and all possible XSS attacks. Some of the most common security settings related to spam management include disabling the PHP "*register_globals,*" enabling the "*Force users to login for profiles*", "*Profiles for enrolled users only*", and ReCAPTCHA to stop automated spambots.

DISCUSSION

The findings of this study confirm that the Moodle platform contains all basic pedagogical and security features to run online examinations. The results of the source code screening conform to open source attributes as argued by Linawati *et al*., (2017) and Stanković *et al*., (2017). The software possesses facilities necessary for teaching, learning, and assessment in accordance with the demands of curriculum (Sari & Setiawan, 2018) to handle summative and formative assessment (Popovic *et al*., 2018) in a variety of fields including mathematics (Handayanto *et al*., 2018), chemistry and biology (Schettini *et al*., 2020), physiology education (Popovic *et al*., 2018), and language (Permana *et al*., 2020). In contrast to other online examination platforms that are limited to MCQs and TFQs (Raj *et al*., 2012), Moodle has emerged as the pedagogically

advanced assessment platform which supports almost 16 question types common to instructors (Post & Hargis, 2012) and which fits any specific curriculum requirements.

Moodle as any other web-based OSS platform with publicly accessible open-source codes is susceptible to security vulnerabilities and high potential risks due to system weaknesses originated from undiscovered software bugs and misconfigurations. Security of open-source codes continues to be a concern for adopters (Schneider, 2000; Khan, *et al*., 2019), thus Moodle can be seen as an insecure platform due to vulnerable web pages (Pérez, *et al*., 2017).

The fact that Moodle is downloaded as fully functional software with all basic security requirements, the findings of this study stresses that the security loopholes in Moodle are due to poorly customized default settings. When Moodle operates with preconfigured public settings, the average number of vulnerabilities is seven (7) per year with the most common being cross-site scripting (XSS), security bypass, SQL/PHP injection, cross-site request forgery (CSRF), authorization vulnerabilities, and arbitrary file upload (Ally, 2016). While responding to these vulnerabilities, it is significant for adopters to balance between pedagogical and security needs. For instance, web forms of rich content used by teachers to enhance their courses, use the same technologies as malicious users for XSS attacks. This implies that administrators and teachers can post XSS-capable content despite being trusted users. Although Moodle can be integrated with various security plugins including SSL encryption (Alanezi, 2018), Moodle can still be compromised with Quiz specific vulnerabilities such as:

- The CSRF attack which may allow unauthorized deletion of Quiz attempts in some instances.
- Inclusion of JavaScript when re-naming content bank items.
- Addition of entries by students in groups that do not belong in some database module of web services. This may allow students to take an exam which was not developed for them.
- Vulnerability to information exposure of service tokens for users enrolled in the same course.

For secure adoption of Moodle as an online examination platform, a proper security implementation to sidestep the exploitation of the Moodle sites is vital. Moodle consists of over fifty secured authentication methods to manage user roles and permissions to address all security concerns. Moodle pages can be configured with dual firewall, packet filter, and secure https to protect network traffic. Adopters may use free https certificates (SSL, 2021) to prevent session fixation, session hijacking and username prediction by adding a PHP script that change the content of four variables of CFG from http to https as follows: *themewww, wwwroot*, *loginhttps,* and *httpstheme*. Moodle also provides system and user logs and can generate reports on activity and participation at both course and site level.

As noted in this study, it is evident that Moodle can provide the best virtual environment for administration of online examinations in HLIs which conform to findings by John *et al*., (2017), Ueda & Nakamura, (2017); Merello & Zorio-Grima (2017); Dimić, *et al*., (2018); Ahmad *et al*., (2019); Waspada *et al*., (2019); and Dascalu *et al*., (2020). Moodle provides a secure exam environment (SEE) or thin client where students use their laptops to take their exams without access to local files or the Internet. Moodle promises a high security level same as any online examination project which normally takes security seriously. Nevertheless, maximum Moodle security depends on the adopter's competency and experience towards software customization, security configurations and enforcement. This is because there exists a clear software security knowledge gap among institutional Moodle programmers (Weir, *et al*., 2020) due to poor software

security coverage in most of the computer science related curriculum (Ally, 2014) and the technology adoption malpractices due to software misconfigurations (Ally et al., 2018).

Furthermore, working on Moodle security alone is not enough. Moodle is designed as a template-based Content Management System (CMS) written in PHP with associated SQL as the database (Anand & Eswaran, 2018). Moodle uses a three-layered structure with high trust level of the underlying software including MySQL for a database, Apache as server-side software, and PHP programming language as used in other online examination platforms (Yağci and Ünal, 2014; Garg, et al., 2020). Thus, with this layered structure, security of Moodle has largely depended on the security of the underlying supporting software. This suggests that it is imperative for adopters to stay current with the chosen operating system, PHP source codes, webserver (Apache), and the latest stable version of the chosen databases (MySQL, Oracle, PostgreSQL) by referring to vendor websites and various CERT sources (CERT, 2011).

In line with findings by Ullah, *et al*., (2012), although Moodle allows integration with enhanced biometric security solutions such as fingerprint devices, face recognition, audio/voice recognition, and signature biometrics to verify candidates, its implementation for online examinations may add extra cost to adopters. Thus, Moodle support to open standards and its free integration with various external applications and third-party modules (Sáenz, *et al*., 2020) must be executed with extra care in order to get rid of new software bugs. As previously reported, having publicly accessible source codes with preconfigured settings, Moodle adopters should always install the latest Moodle releases and updates from time to time to address security vulnerabilities (Constantin, 2017; Powell, et al., 2019) and to satisfy the primary software characteristics such as high availability, scalability, usability, interoperability, reliability, and security (Ghosh, *et al*., 2019).

To attain maximum benefits of implementing Moodle as the platform for online examinations, the existing challenges must be addressed. Some of these challenges include: lack of proper planning to have a balance between Moodle server resources and computing workloads in handling synchronous activities; many concurrent users; newness of the functionalities of the Moodle Quiz feature among tutors and students; and unreliable Internet service. Other notable challenges include lack of pedagogical knowledge for setting various online questions, specifically the stem and distractors of MCQ questions, and failure to put all possible answers for the SAQs.

CONCLUSION AND RECOMMENDATIONS

For adopters to attain maximum benefits from using Moodle to run online examinations, proper planning for both technical and pedagogical requirements is vital.

With a digitally enabled future for education, the evidence from this study points toward the idea of choosing Moodle as a perfect software to run online examinations. The architectural design of Moodle Quiz provides a sufficient environment to facilitate the smooth and secured conduct of online assessment procedures which are cost effective, time-efficient, security controlled, and OSS in nature. It is important to note that the threats to online examinations can have a detrimental impact on the credibility of the adopting organization. If Moodle is properly adopted, securely configured with well-balanced computing workloads and server resources, the software can provide a sufficient authentication system to counteract collusion and malicious attacks. For the adopter to attain maximum benefits, the following recommendations are vital for implementation in the adoption and usage processes:

1. Adopter must perform regular updates with the latest stable versions and security patches using auto-update systems, rootkit detector, and spam cleaner to ensure security of the Moodle platform and all its underlying software including operating system (OS), database management system (DBMS) (MySQL, PostgreSQL or Oracle), PHP, and

webserver (Apache). Basically, Moodle is designed to be very secure, but this is highly dependent on the security of its underlying software. When security of the underlying software is assured with no software flaws, it is difficult for hackers to break into the Moodle system.

2. It is vital for a Moodle site to be officially registered with Moodle.org and be part of the Moodle tracker and CERT mailing lists to receive notifications about security alerts on issues, patches and updates, and stay updated with emerging security issues including zero-day exploits and their corresponding fixes for Moodle, PHP, MySQL, Apache, and OS website. The Moodle site provides an opportunity to check for the supported versions.

3. Adopter should put in place an efficient and proper plan for computing infrastructure by estimating the required amount of server resources (processing power (CPU), memory size (RAM), large storage capacity (HDD), adequate Internet bandwidth, and reliable power supply) against client workloads for all real-time and concurrent activities while taking care of the length of the question paper, number of exam sets, concurrent users, and the question display mode on a webpage.

4. For potential quick performance, the adopter should load and activate only features and services needed for online examinations. That is, adopters should improve the system by disabling all non-Moodle quiz features, narrowing parameter settings and completely stripping Moodle down to the bare bones by deleting and removing dormant users, old courses and obsolete content, as well as uninstalling all unnecessary functionalities, modules, administrative capabilities, database tables, and disabling unused services and question types.

5. Adopter should separate Moodle for online examination from Moodle for learning by giving different domain names, that is, by installing Moodle as an isolated site (domain name and a public IP address) so as not confuse users and to avoid overloading of the Moodle server with non-examination requests.

6. Adopter should establish centralized institutional security configurations and standard settings for Moodle Quiz.

7. Adopters should give accounts to only trusted users and enforce usage of strong passwords for all privileged users including administrators and teachers so as to protect against "brute force" cracking of accounts, as well as avoid creating public sandboxes with free accounts on production servers.

8. Adopter should configure default settings, review source codes, and set proper file permissions as per the security requirements to maximize software security.

REFERENCES

Ahmad, J., Khan, B. N. A., Raghavan, S., & Sulaiman, T. F. T. (2019). Online examination for takaful basic examination–a license to practice certificate: a Malaysian case.

Alanezi, M. A. (2018). Adaption of Moodle as E-Learning in Saudi Arabian University: Empirical Examination and its Outcomes Using TAM. *International Journal of Computer*, vol. 29, no. 1, pp. 132-148.

Ally, S. (2014). Security Vulnerabilities of the Web Based Open Source Information Systems: Adoption Process and Source Codes Screening. *HURIA: Journal of The Open University of Tanzania*, vol. 17, no.1-13.

Ally, M. S. (2016) Secure Software Deployment: Investigating the Security Vulnerabilities of MOODLE LMS in Public Higher Learning Institutions in Tanzania. *International Journal of Advanced Information Science and Technology (IJAIST), ISSN: 2319:2682,* vol. 47, no. 47.

Ally, S., Jiwaji, N. T., & Tarimo, C. (2018). A Review of Adopter's Common Misconfigurations of Virtual Machines: The Case of Tanzania. *Huria: Journal of the Open University of Tanzania*, vol. 25, no. 2, pp. 158-180.

Anand, A., & Eswaran, S. (2018). Case Study Moodle Approach to Learning and Content Management System (LCMS). *International Journal of Computer Sciences and Engineering*, vol. 6, no. 7, pp. 1147-1152.

Bhandari, A., Bhuiyan, M., & Prasad, P. W. C. (2017). Enhancement of MD5 Algorithm for Secured Web Development. *JSW*, vol. 12, no. 4, pp. 240-252.

CERT, (2011). US-CERT Technical Cyber Security Alert. Website: http://www.us-cert.gov/cas/signup.html. Date Accessed: 15 January 2021

Constantin, L. (2017). Flaws in Moodle CMS put thousands of e-learning websites at risk. Website: https://www.csoonline.com/article/3183533/flaws-in-moodle-cms-put-thousands-of-e-learning-websites-atrisk.html. Date Accessed: 25 January 2021

Dascalu, M. D., Dascalu, M., Ruseti, S., Carabas, M., Trausan-Matu, S., & McNamara, D. S. (2020, June). Cohesion Network Analysis: Predicting Course Grades and Generating Sociograms for a Romanian Moodle Course. In *International Conference on Intelligent Tutoring Systems* (pp. 174-183). Springer, Cham.

De Vaus, D. A. (2006). Research Design in Social Research. London: SAGE, 2001; Trochim, William M.K. Research Methods Knowledge Base.

Dimić, G., Predić, B., Rančić, D., Petrović, V., Maček, N., & Spalević, P. (2018). Association analysis of moodle e-tests in blended learning educational environment. *Computer Applications in Engineering Education*, vol. 26, no. 3, pp. 417-430.

Dhika, H., Destiawati, F., Sonny, M., & Jaya, M. (2020, March). Comparison of Learning Management System Moodle, Edmodo and Jejak Bali. In *International Conference on Progressive Education (ICOPE 2019)* (pp. 90-94). Atlantis Press.

Garg, A., Jaiswal, A., Gupta, A., & Tripathi, D. (2020). Development of Online Examination Platform for Better Evaluation and Monitoring. *Development*, vol. 7, no. 05.

Ghosh, A., Nafalski, A., Nedic, Z., & Wibawa, A. P. (2019). Learning management systems with emphasis on the Moodle at UniSA. *Bulletin of Social Informatics Theory and Application*, vol. 3, no. 1, pp. 13-21.

Handayanto, A., Supandi, S., & Ariyanto, L. (2018, May). Teaching using moodle in mathematics education. In Journal *of Physics: Conference Series* vol. 1013, no. 1, p. 012128. IOP Publishing.

John, M. J., Ramakrishnan, S. H., Sirajudeen, M. M., & Suthagar, S. (2017). Advanced Online Examination using Raspberry Pi. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET),* vol. 4, Special Issue 19.

Kaburlasos, V. G., Marinagi, C. C., & Tsoukalas, V. T. (2004). PARES: A software tool for computer-based testing and evaluation used in the Greek higher education system. In IEEE International Conference on Advanced Learning Technologies, 2004. Proceedings. (pp. 771-773). IEEE.

Kabir, S., Hossain, M. P., Mallik, K., Rahman, M., Islam, M. J., & Khatun, A. (2019). An Extensive Online Examination System with Automatic Assessment Technique. *GUB Journal of Science and Engineering*, vol. 6, no. 1, pp. 54-59.

Khan, F. I., Javed, Y., & Alenezi, M. (2019). Security assessment of four open source software systems. *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 2, pp. 860-881.

Konde, S., Divekar, M., Sonar, P., & Kakade, P. Survey on Online Examination System using Django Framework. In *National Conference on Computational Intelligence and Deep Learning (NCCIDL-19)*, vol. 5, no. 2, pp. 42-44.

Kumar S., & Dutta, K., (2011). "Investigation on Security in LMS Moodle", International Journal of Information Technology and Knowledge Management January-June 2011, vol. 4, no. 1, pp. 233-238

Linawati, L., Wirastuti, N. D., & Sukadarmika, G. (2017). Survey on LMS Moodle for adaptive online learning design. *Journal of Electrical, Electronics and Informatics*, vol. 1, no. 1, pp. 11-16.

Merello, P., & Zorio-Grima, A. (2017). Impact of students' performance in the continuous assessment methodology through Moodle on the final exam. *Educade: Revista de Educación en Contabilidad, Finanzas y Administración de Empresas,* vol. 8, pp. 57-68.

Moodle, (2022). Moodle Open-source learning platform. Website: http://moodle.org. Date Accessed: 06 January 2022

NVD, (2021). Moodle Vulnerabilities. National Vulnerability Database. Website: https://nvd.nist.gov/, National Vulnerability Database Date Accessed: 06 December 2020

OSI (2004) The Open Source Definition v1.9 online: http://www.opensource.org/docs/definition.php Accessed April 27, 2005.

OUT, (2018) Rolling Strategic Plans (RSP 2018/19-2022/23), The Open University of Tanzania.

OWASP, (2021). OWASP Foundation, The Open Source Foundation for Application Security. Website: https://owasp.org/, Date Accessed: 06 January 2021

Pérez, S. O., Díez, C. H., & García, J. M. (2017). Applying Security to Moodle Grades. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 117-123). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Permana, P., Permatawati, I., & Hendra, D. (2020). Optimizing the Quiz Moodle Module for the B1 Level German Language Exam Simulation Application. In *4th International Conference on Language, Literature, Culture, and Education (ICOLLITE 2020)* (pp. 536-543). Atlantis Press.

Post, G. V., & Hargis, J. (2012). Design features for online examination software. *Decision Sciences Journal of Innovative Education*, vol. 10, no. 1, pp. 79-107.

Popovic, N., Popovic, T., Rovcanin Dragovic, I., & Cmiljanic, O. (2018). A Moodle-based blended learning solution for physiology education in Montenegro: a case study. *Advances in Physiology Education*, vol. 42, no. 1, pp. 111-117.

Powell, L. M., Wimmer, H., & Rebman, C. (2019). Learner security & privacy risks: how usage of online social media outside a learning management system affects learners 'digital identity. *Issues in Information Systems*, vol. 20, no. 4.

Raj, P. G., Kumar, P., Sengupta, S., Vats, K., & Gupta, P. R. (2012). An Architectural Insight into the National Online Examination System. *International Journal of e-Education, e-Business, e-Management and e-Learning*, vol. 2, no. 2, p. 126.

Rootkit, (2020). Rootkit Tool for Linux/MacOSX. Website: http://www.chkrootkit.org/. Date Accessed: 18 December 2020

Rootkit, (2021). Rootkit Tool for Windows, *Windows Sysinternals*. Website: http://technet.microsoft.com/en-us/sysinternals. Date Accessed: 25 February 2021

Sáenz, J., Gurtubay, I. G., Izaola, Z., & López, G. A. (2020). pygiftgenerator: a python module designed to prepare Moodle-based quizzes. *European Journal of Physics*, vol. 42, no. 1, 015702.

Sari, A. P. & Setiawan, A. (2018). The Development of Internet-Based Economic Learning Media using Moodle Approach. *International Journal of Active Learning*, vol. 3, no. 2, pp. 100-109.

Schettini, C., Amendola, D., Borsini, I., & Galassi, R. (2020). A blended learning approach for general chemistry modules using a Moodle platform for first year academic students. *Journal of E-Learning and Knowledge Society*, vol. 16, no. 2, pp. 61-72.

Schneider, F. B., (2000), "Open Source in Security: Visiting the Bizarre." Proceedings of the 2000 IEEE Symposium on Security and Privacy (the Oakland Conference), Berkeley, CA. Los Alamitos, CA: IEEE Computer Society. pp. 126-127.

Shraim, K. (2019). Online examination practices in higher education institutions: learners' perspectives. *Turkish Online Journal of Distance Education*, vol. 20, no. 4, pp. 185-196.

Sorensen, E. (2013). Implementation and student perceptions of e-assessment in a Chemical Engineering module. *European Journal of Engineering Education,* vol. 38, no. 2, pp. 172–185.

SSL, (2021). Free SSL/TLS Certificates. Website: https://letsencrypt.org/. Date Accessed: 05 March 2021

Stanković, J., Milovanović, S., & Radović, O. (2017). Applying the Moodle Platform in Online Student Self-Assessment. *Economic Themes*, vol. 55, no. 2, pp. 281-304.

Tian, Y., Zhang, K., Wang, P., Zhang, Y., & Yang, J. (2018). Add" Salt" MD5 Algorithm's FPGA Implementation. *Procedia computer science*, vol. 131, pp. 255-260.

Ueda, H., & Nakamura, M. (2017). Data analysis for evaluation on course design and improvement of "cyberethics" moodle online courses. *Procedia Computer Science*, vol. 112, pp. 2345-2353.

Ueda, H., Furukawa, M., Yamaji, K., & Nakamura, M. (2018). SCORMAdaptiveQuiz: implementation of adaptive e-learning for moodle. *Procedia computer science*, vol. 126, pp. 2261-2270.

Ullah, A., Xiao, H., & Lilley, M. (2012, June). Profile based student authentication in online examination. In *International Conference on Information Society (i-Society 2012)* (pp. 109-113). IEEE.

UNISA, (2021). University of South Africa. Website: https://lo.unisa.edu.au/mod/book/tool/print/index.php?id=1297436. Date Accessed: 17 February, 2021

URT, (2015), National Education Policy, Ministry of Education and Vocation Training, United Republic of Tanzania

Waspada, I., Bahtiar, N., & Wibowo, A. (2019, May). Clustering student behavior based on quiz activities on moodle LMS to discover the relation with a final exam score. In *Journal of Physics: Conference Series*, vol. 1217, no. 1, p. 012118). IOP Publishing.

Weir, C., Rashid, A., & Noble, J. (2020). Challenging software developers: dialectic as a foundation for security assurance techniques. *Journal of Cybersecurity*, vol. 6, no. 1.

Yağci, M., & Ünal, M. (2014). Designing and implementing an adaptive online examination system. *Procedia-Social and Behavioral Sciences*, vol. 116, pp. 3079-3083.

Yildiz, E. P., Tezer, M., & Uzunboylu, H. (2018). Student opinion scale related to Moodle LMS in an online learning environment: Validity and reliability study. *International Journal of Interactive Mobile Technologies*, vol. 12, no. 4.