Safety Measures Investigation in Moodle LMS

Shakir Khan
Researcher at E-Learning and Distance Learning Deanship, King Saud University, Riyadh Saudi Arabia

Mohammed AlAjmi, PhD.
Vice Dean-Quality and Development, Head of Quality and E-Leaning units, Prince Sultan College for EMS King Saud University, Riyadh, Saudi Arabia

Arun Sharma, PhD.
Department of Computer Science, Krishna Institute of Engineering and Technology, Ghaziabad-201206, India

ABSTRACT

E-learning gives the chance to scholar to act together electronically with each other as well as with their educators. This communication can be via SMS, e-mail or on conversation board or in chat rooms. Although identifying that the globe at large will persevere to utilize verbal communication and terminology in changed behaviour, so the word of virtual learning environments (VLE) is applied to consign to the web interactions of a multiplicity of kinds that have effect between students and instructors. There are several software systems existing that offer VLE systems. These software's take care in both the forms, commercial and open source software (OSS). Moodle is the one of these systems that has been progressively gaining worldwide attractiveness in e-learning system.

LMS Moodle has much exposure like validation, ease of use, privacy and reliability attacks. So, it is required to develop a method that defends these security faults of LMS Moodle. We present mainly common security defects and propose best security settings of Moodle (Modular Object-Oriented Dynamic Learning Environment) LMS and the server itself. Particularly, we will target on authentication assault from the above pointed out faults. We additionally organize design and session assault. Design assault on Moodle can be largely considered as password forecast and user name forecast. Session assault on Moodle is session takeover. Moodle is an open source software e-learning podium that gives educators tools to build a course web site. Through the last few years, LMS Moodle forced itself as the best solution, and is appropriate one of the most frequent used systems.

The open source teaching or learning management, LMS Moodle has been implemented by many individuals and organizations around the globe because it suggests a tightly included set of tools said to be considered from a social productive perspective. Moodle has been urbanized under the common public license and many of its workings were developed without a detailed design documents counting its security services. Object oriented model of Moodle via an analysis of its safety services as well as solutions to its precautions vulnerabilities.

Keywords: Moodle, Virtual Learning Environment, Open Source Software, Web Assault, Safety, LMS, OSS, Session

1. INTRODUCTION

Together with the rapid rising fame of the Internet in present years, there is a growing persists for methodologies and technologies for e-learning. E-learning is an interactive learning in which the education content is easy to get to online and recommends routine feedback to the student's education behaviour [1]. Consequently, there has been an increasing requirement for VLE methodologies and technologies. VLE (virtual learning environment) is classified as interactive learning in which the education content is accessible on-line and proposes automatic response to the student's wisdom behaviour. While expressing that the world at vast will continue to use terminology in changed and repeatedly unclear behaviour, the phrase of VLE is utilized here to consign to on-line exchanges of different kinds including on-line education that get place between students and teachers [2, 3]. Presently, there are before more than 200 resource of mercantile e-learning and more than 50 of them are Open Source Software (OSS) assistance as free of charge VLE systems. The enhanced well-known OSS are Moodle, Claroline, SAKAI, Ilias, eduplone, WebCT and Bscw, and they have broad developer communities who present well-built points of view allowing for OSS as a clear-cut and potentially feasible competitor to commercial products. Modular Object-Oriented Dynamic Learning Environment (Moodle) is an OSS development that has appeared to assemble the rising importance in OSS. Moodle is an online Learning Content Management System (LCMS) kind of web based, i.e. a Course Management System (CMS) and VLE considered approximately pedagogical ideology, specifically a social constructivist opinion using the joint potential of the Internet. It allows teachers to present and distribute assignments, documents, quizzes graded, etc. with learners in an easy-to-learn way, and to create quality on-line courses. Moodle is a free OSS, it means users can download Moodle free of charge, use, adapt and even to allocate it under the provisions of GNU [4, 5]. An important source for higher education, mainly universities utilize VLE, which has been smart students' growth with high excellence learning around the globe.

Moodle [6], the LMS called is open source software, and can be configured to sprint on most operating systems (Windows XP, Macintosh OS and Linux). Moodle was urbanized from a social constructivist point of view by Martin Dougiamas at Curtin University in Western Australia. Moodle has some description like including the potential to embed resources, announcement and actions cantered on a theme of study, which is not presented somewhere else. The instructor may also identify a multiplicity of modes for process (from weekly designs, topic-based to social designs). The approval and functioning [7] of Moodle has been exceptionally successful. The uptake of the software has been so winning that the first customer conferences (called *MoodleMoots*) organized in July 2004. *MoodleMoots* have been understood in the Germany, United Kingdom, Ireland and the USA. Moodle is also beginning to challenge the control of the pay-as-you-go representation of many of the industrial LMSs existing.

2. MOTIVATION FOR MOODLE CHOICE

Moodle has verified its significance due to a wider recognition in the society and number of association. The software offers support for huge number of choices in changed languages [8, 9]. Moodle permits users the capability to place news items, coursework, electronic journals and resources, and to accumulate assignments etc. The community has fully fledged around the project. Both developers and users contribute in Moodle's active conversation forums, contribution tips, posting system snippets, assisting new users, sharing sources and assessment and new ideas which add strong points to the Moodle [10, 11, and 12].The most significant causes for preferring Moodle are listed below:

2.1 It is an OSS and users can download it freely, utilize it, amend it and even dispense it under the provisions of the GNU certify [2, 4, and 13].

2.2 It is a CMS & VLE that allows instructors to give and share papers, ranked assignments, conversation forums, etc. with their learners in an easy-to-learn approach, and in high quality on-line courses [4, 14].

2.3 Moodle can be utilized on approximately all servers that can apply PHP. Users can download and employ it on any computer and can straightforwardly upgrade it from one edition to the next [11, 15].

2.4 The solution to Moodle that is developed together with *pedagogy* and *technology* keeping in mind. One of the main benefits of Moodle over other LMSs is its well-built grounding in social constructionist pedagogy and good instructive tools [16].

2.5 The Moodle LMS is used worldwide by self-sufficient instructors, educators, schools, institutes, universities and companies. The reliability of Moodle is very high. Presently, there are 3324 web sites from175 countries that have recorded with it, and it has 75 foreign languages [11, 4].

2.6 Moodle runs with no amendment on any system that sustains PHP as scripting language and operating system such as UNIX, Linux and Windows. It utilizes MySQL, PostgreSQL and Oracle databases, and others are also supported [13].

2.7 It has a lot of features helpful to potential students like easy installation, modification of options and settings, good support or help, and good instructive tools. Moreover, it has outstanding documentation, and strong help for security and administration [16].

3. RESTRICTIONS OF MOODLE

Moodle is easy to use, elasticity, low cost and assists to bring VLE technology inside the reach of those with narrow technical or financial resources [9]. On the other way, Moodle has some restrictions as follows:

A. Moodle is only for IT skilled. It is complex for normal consumers to use and more than 66% of them are instructors, researchers and managers [11]. It is not easy for beginner technicians to set up and use Moodle [9] being there are lots of technical words listed in installation instructions.

B. Moodle will job but not by itself. If there is not a course manager that can job with both instructors and technicians in generating on-line materials then Moodle will stay on an empty shell like a better aircraft but with no pilot. Lack of simple-to-obtain assistance [11]. Discussions carry a big deal of information but almost all discussions are in the English language.

C. It does not maintain the SSL functioning all over the site.

D. It stores the user data into cache which can be afterwards used by the enemy to begin the attack for next session.

Brute force attack is feasible on Moodle as the assailant may try altered keys for many numbers of times.

4. SAFETY AND LIABILITY IN MOODLE

TABLE1

Attack Techniques and Security

A. Authentication attacks

1) Broken verification and session administration

2) Insecure communication

B. Accessibility attacks

1) Rejection of service

In this paper we present explanation of the most important security flaws as talked about in literature. They are categorized into four groups: authentication, accessibility, privacy and reliability attacks. Learning management systems [17, 18] are client and server based web applications that handle user needs coming from customers such as web browsers. To hold the user needs, they frequently need to access security-critical resources i.e. databases and files at the hosted server end.

1) Privacy attacks

i Lacking confidence cryptographic storage space

ii Lacking confidence straight object reference

iii Information outflow and rude error handling

2) Reliability attacks

i Buffer excess

ii Cross Site Request Copy

iii Cross Site Scripting

iv Failure to limit URL access

v Injection flaws

vi Malicious file effecting

Table 1 shows an outline of secret attack techniques and vulnerabilities self-determining of the correct LMS functioning as presented in [17]. Model used to cluster attack methods and safety vulnerabilities is broadly accepted AICA (Availability, Integrity, Confidentiality and Authentication) threat modelling approach.

A. Authentication Attacks

Authentication and session administration consist of all features of handling user authentication and controlling active sessions. Authentication is a risky aspect of this process even rigid authentication methods can be broken by inconsistent official document management functions, together with password change, forgot my password; remember my password, account update, and other associated functions. Openness which comes out during conveys of open information (session tokens) lacking appropriate encryption. Attacker can misuse this imperfection to impersonate user and access insecure exchanges.

B. Accessibility Attacks

The main purpose of accessibility attacks is to build e-learning services and data engaged to authorize end users. Most accepted multiplicity of availability attack is denial of service (DoS) assault. A denial-of-service assault (DoS assault) [19] is challenge to build a computer resource unavailable to its future users. Though the means to perform motivation for and objectives of a DoS attack may fluctuate, it usually consists of the determined efforts of a person or people to stop an Internet site or services from implementation powerfully or at all, temporarily or for an indefinite time. Perpetrators of DoS assaults are not restricted to services hosted on prestigious web servers like banks, credit cards payment gateways; it is also utilized in position to CPU resource managing. There are usually two kinds of DoS assault, first are logic assaults and second are flooding assaults. Logic assaults develop existing LMS flaws to crash remote server or considerably decrease its performance. Flooding assaults overloads LMS with a high number of requirements to disable legal users from contacting e-learning resources.

C. Privacy Attacks

Privacy attacks are obedient kind of attacks which permits banned access to secret resources and data. The most important purpose of assailant is not data modification but data access and circulation. The most frequently privacy flaws are: unconfident cryptographic storage, unconfident direct object reference and Information leak and rude error handling.

Insecure cryptographic storage flaws [17,18] which is based on a fact that sensitive information does not have appropriate encryption. Insecure direct object reference usually occurs when LMS uses object references directly in web interfaces without authorization checks being implemented. Pointed out object references can be database records, files and primary keys and are controlled either by URL or form parameters. Information leak and inappropriate error handling refers to accidental discovery of sensitive data and unneeded information through error messages. LMS can disclose responsive information about its logic, configuration and other internal details (e.g. source code and SQL syntaxes etc.). LMS systems not often use cryptographic functions properly to protect data and qualifications or use weak encryption algorithms. In both circumstances, important data is comparatively easy to access by attacker who can conduct identity theft and similar crimes.

D. Reliability Attacks

This cluster contains attacks which try to produce new data or modify and even delete active e-learning data. Reliability assaults are: Buffer overflow assaults, Cross Site Request Forgery (XSRF/CSRF), Cross Site Scripting (XSS), Injection flaws, Malicious file execution and Failure to restrict URL access.

Malicious file execution assault [17, 20] which is based on a fact that LMS fails to control or prohibit effecting of uploaded files. Malicious code is generally uploaded via upload attribute (e.g. assignments or image uploads). This kind of weakness can be originated in several web applications, particularly in those applications which are PHP based. Injection flaw may occur when data given by user (e.g. in form fields) is sent to content checking schedules as part of a demand or query. In such assaults, interpreter fail to identify or respond to character string that may be understood wrongly, which then marks in execution of nasty code by LMS. Ultimately, assault could be intelligent to create, update, read or delete all data existing to LMS. Cross Site Scripting (XSS) [17, 21] refers to hacking method which permits an assaulter to provide weak dynamic web page with hateful script and perform script in victim's browser in order to collect data from a user. Cross Site Request Forgery (XSRF/ CSRF) is client side assaults which utilizes confidence that a LMS has for the user. When a customer is logged into LMS, assaulter can fraud his browser into creation a demand to one of LMS assignment URLs which will reason an alteration on the server. Buffer overflow assaults [17, 22] takes place when a LMS section (e.g. libraries, drivers, server components) attempts to store data into an existing buffer with no authentication its size by introducing big values than accepted. Failure to control URL right to use, some LMS resources is restricted to a small division of privileged users (e.g. administrators). This fault permits an assaulter to recover URLs by estimating the address and carry out illegal operations on unprotected LMS data.

5. SAFETY ASSAULT TO MOODLE

With increasing demands of internet services results in the emergence of multiple service providers which provides access point to internet users. As there are remarkable increments in internet users in recent times, safety issues have turn out to be the major anxiety. We have determined subsequent safety attacks on Moodle like session attack; design attack and consumer log out, session not stopped. Session attack which is efficient against Moodle is session hijacking. As per the anxiety of design attacks, Moodle is weak to password calculation and user name forecast. Another, security weakness is that when the consumer logout still the session is not stopped. When the customer clicks on the back button then he gets to the page which was logged out previously.

A. Design Attacks

Moodle (modular object oriented dynamic learning environment) is unprotected to password calculation and username calculation.

1) Password calculation

Brute force attack [29] can be carried out via the design flaw of Moodle server. To do this assault, the user sends the some needs to the Moodle server with the blank cookie pitch so that the login failure count is restructured to zero when the cookie pitch is blank in the demand.

2) User Name calculation

This may be completed by brute force technique. Brute force assaults may be carried out as like in password calculation. Conversely, instead of transporting several requests with changed password, several usernames are sent with a random password. The reply from Moodle will get longer with an applicable username than with an unacceptable one and this was used to distinguish between them in the assaults realized.

B. Session Takeover

The Session Takeover attacks [24] consist of the deployment of the web session managed mechanism, which is generally managed for a session token. Because http communication utilizes some different TCP connections, the web servers needs a technique to be known with each user's connections. The majority helpful technique depends on a symbol that the Web Server posts to the client browser after a winning client validation. A session symbol is in common composed of a sequence of inconsistent width and it could be used in several ways, as in the URL, in the header of the http request as a cookie, in other components of the header of the http

requisition, or yet in the body of the http request. The Session Hijacking assault assists the session token by theft or speculation a valid session indication to get unauthorized contact to the Web Server. A hacker can also be aligned between client and server by blubbing program to watch the discussion. This is identified as a man in the central point attack.

Session hijacking is a part of the bugging somebody's room assault. Where an assailants give concentration the communication between client and server. They are demanding to find indoors the pay load, in this case the HTTP requirements. The data that can be used to imitate the customer and attractive organized of his or her session. Moodle holds its session throughout two values to identify an active session:

C. Moodle Session and Moodle Session Test.

MoodleSession and MoodleSessionTest main beliefs are stored in the cookie hat are terrified on each HTTP command inside the header of the communication. Attaining a full HTTP demand data with the cookie integrated is simple because Moodle only utilizes SSL passageways on the login service and a little managerial services. Because of that, most HTTP order is completed on plaintext that can be seized and effortlessly decoded. After attaining the cookie, the assailant can use this data on its own HTTP demand, taking full control of the objective user session.

6. PLANNED SOLUTION TO MOODLE SAFETY ASSAULTS

In this paper we proposed solution for the security attacks that are identified in previous section. For example when a user logout from a session then he/she is redirected to account if someone click the back button. By doing this, consumer goes to the earlier active page, and can have accessibility for the account, which is a huge flaw in Moodle. To eliminate this flaw session can be applied, when the session is applied and the consumer login to the system, his session turn out to be active and will stay active for the time till he does not push the logout button. When the logout button is pushed, user's session terminates and the user turns out to be inactive.

A. Login through CAPTACHA

When a user desires to login to Moodle server, the brute force assault takes place. To eliminate this flaws, CAPTCHA can be used which creates some random values that permits the user to penetrate these random values all through his or her login. Verification phase turns out to be stronger against the brute force assault by using this method. The login page is collective with the official CAPTACHA achievement well-known as recaptcha. CAPTACHA functioning designs are based on random code generator algorithm. Design php code with graphics store to create CAPTACHA image for above produced code. With clicking the login button, it compares and matches the security code filled by user and images as well.

B. SSL (Secure Sockets Layer) to Keep Away from Session Hijacking

SSL (Secure Sockets Layer) is the key to keep away from session hijacking difficulty. SSL is the standard security technology for setting up an encrypted connection between a web server and a browser. Moodle previously had an option for using SSL over assured important actions. However such technique cannot keep away from session takeover and user name calculation. In order to keep away from such attacks, the complete site must generate SSL associations with its clients.SSL (Secure Sockets Layer) link guarantees that all information accepted between the web server and browsers stay private and important.SSL (Secure Sockets Layer) can be completed by adding up a PHP scripts that alters the content of the entity that grasps the background configuration named CFG. In *CFG Themewww, Login https, Wwwroot, Https theme* these are the subsequent four variables that are SSL related. SSL is a business standard and is applied by millions of web portals or websites in the security of their online transactions with their clients. To be competent to create an SSL connection, a web server requires an SSL Certificate. When we choose to make active SSL on our web server, we will be confident to complete several questions about the uniqueness of that website and the company. The web server then creates two cryptographic inputs a Private Input and a Public Input.

7. CONCLUSION AND FUTURE WORK

In this paper, Moodle (Modular Object-Oriented Dynamic Learning Environment), an open source software e-learning podium is considered and safety associated issues of Moodle are discuss. Moodle give instructors tools to build a course web site. There are a lot of safety issues like as authentication, accessibility, privacy and integrity assaults is examined under this work and particularly an authentication assault from the above issues is performed throughout the paper. Additionally, in authentication the session assault and design assault trouble are corrected by with SSL (secure socket layer) and login with Captcha functioning respectively.

Whenever a user requests to login to Moodle server, the brute force assault takes place. Captcha implementation is applied to avoid design attack difficulty, and Captcha method which creates some random values that permits the user to fill these random values during his or her login. Authentication phase turns out to be stronger in opposition to the brute force assault by using this method.

SSL is preferred to keep away from session hijacking trouble. SSL is the benchmark security technology for launching an encrypted connection between a web server and a browser and SSL can be completed by adding a PHP scripts that alters the content of the entity that keeps the setting configuration. Login https is applied for secure information transmission. For implementation of these kinds of methods, SSL certification is necessary.

To generate more secure and consistent learning environment, it is necessary to eliminate all the safety flaws of the Moodle. In this paper, we spotlight on the authentication attack. This work can be extended by attending to other safety issues of the Moodle.

8. REFERENCES

[1] S. Graham, "Building Web Services with Java: Making Sense of XML, SOAP, WSDL and UDDI", 1st ed., Pearson Education, pp. 450, 2001.

[2] G. Tortora, "A Multilevel Learning Management System, in: Proceedings of the 14th International Conference on Software and Knowledge Engineering", ACM: Ischia, Italy, pp-403-411, 2002.

[3] Martin, and T. Peter, "Interpretive Analysis of an Internet-based Course Constructed using a New Courseware Tool called Moodle", Quality Conversations in: Proceedings of the 2002 Annual International Conference of the Higher Education, Perth, Australia, pp. 560-473, 2002.

[4] http://www.Moodle.org.

[5] G. Sabine, and L. Beate, "An Evaluation of Open Source e-learning Platforms Stressing Adaptation Issues", in: Proceedings of Fifth IEEE International Conference onLearning Technologies, IEEE, Ischia, Italy, 2005.

[6] A. Bucher, "Moodle Administration: An Administration Guide to Configuring, Security, Customizing and Extending Moodle", Packt, 1-357, September 2008.

[7] K. Brandl, "Are you ready to Moodle, in Language Learning/Technology", Washington, 9, No. 2, pp. 16-23, 2005.

[8] J. Cole, and H. Foster, "Using Moodle: Teaching with the Popular Open Source Course Management System", 2nd ed. O'Reilly, 2007.

[9] Williams and M. Dougiamas, "Moodle for Teachers, Trainers and Administrators of Remote-learner.net", Retrieved from http://Moodle.org.

[10] M. Zenha-Rela and R. Carvalho, "Work in Progress: Self Evaluation through Monitored Peer Review using the Moodle Platform", in Frontiers in Education Conference, 36th Annual., San Diego, CA: IEEE, pp. 230-241, 2006.

[11] A. Chavan and S. Pavri, "Open Source Learning Management in Moodle", in: Linux Journal, 1, No. 2, pp. 78-97, 2004.

[12] J. Itmazi, "Flexible Learning Management System to Support Learning in the Traditional and Open Universities", PhD Thesis, Granada University, Spain, 2005.