Mathematical Problems of Computer Science 39, 129--134, 2013.

Vulnerable Security Problems in Learning Management System (LMS) Moodle

Vahe A. Arakelyan
Institute for Informatics and Automation Problems of NAS of RA
e-mail: a_vahe@sci.am

Abstract

In this paper the security mechanisms of LMS Moodle are investigated. Some vulnerable parts have been discovered and some solutions and methods are proposed to make the system more secure and safe.

Keywords: Moodle, Security, Attack.

1. Introdaction

Moodle is a content management system (LMS) specially designed for creating high-quality online courses. "Moodle" is an abbreviation, which is obtained from the expression "Modular Object-oriented Dynamic Learning Environment''. Moodle has been translated into many languages and is used in 197 countries. The leader of the above mentioned system is Martin Dougiamas from Australia. It is an open source system and a lot of programmers can take part in the developing of it. Moodle is written in PHP language, using SQL-database. Having a number of functions and modules Moodle LMS competes with famous commercial learning systems such as Blackboard, Desire2Learn, SharePoint LMS and so on. The advantage of the distributed open-source software is that it allows to modify the system specific study program characteristics, and, if necessary, add new modules. The rapid progress in information technology allows the use of computers as a teaching effective means. Automation of the learning process is realized by means of computer training programs and the use of electronic textbooks, which are used not only for magnetic storage media (laser disc) to the application, but also for local and global computer networks. By means of the use of global computer network it creates a specialized information-educational field which allows to realize and carry out training, using modern technologies. To implement it in informational educational sphere as well as in local and global computer networks, the effective use of e-learning materials, high-operative development are essential and necessary. The goal of the creation of Electronic Training Materials is to improve the quality of efficiency of the learning process and mastering of specialists. In the field of higher education e-learning, materials can be used as an additional educational resource, which allows to organize the teacher's control on student's independent

work correctly. Thus, higher education will involve a step by step contribution of virtual learning environment technologies, particularly in distance learning. So very soon higher education will be conducted with the use of virtual learning environment. The Yerevan State Pedagogical University and the magistracy of the National Academy of Sciences of RA plan to introduce this system, due to which training will be available to students who live in different regions of Armenia and even beyond the republic, for those who wish to get highly qualified and modern education. At the same time in virtual learning environment (VLE) electronic educational materials for students are the basic source of information [8].

2. Vulnerabilites in Moodle

Such important disadvantages which can make the system weak in case of attacks are presented in this paper. They are classified into four groups: authentication, availability, confidentiality and integrity. Distance learning systems or VLEs are client/server Web programs, which develop requests coming from the user internet browser [5]. Polls processing system often uses strict security rules that require data, such as, e.g., databases and files.

2.1. Authentication Attacks

Authentication and session management include all aspects, which are necessary to identify the user and manage the active session. Identification in this process is considered to be a very dangerous process, even in case of complicated mechanisms it can be broken because of the insufficient management functions of identification data, such as an opportunity of password change or the password may be forgotten and can be restored, a password remembering feature, or transferring plain date during authentication. The attackers can use these data and hack the system.

2.2. DoS Attacks

The main purpose of attacks is to make the education system unavailable for users. The most popular one is Denial of Service attack. Under DoS attack can be any of the web services, including banking systems. There are two types of DoS attacks, logical and flooding. Logical attacks use the VLE's existing errors and carry out such requests to respond them, that makes the system an endless cycle of actions. During the flooding attack a large number of requests are made simultaneously and the system is not able to manage and respond to all of them. In both cases the system productivity is reduced, or it stops to serve the endusers.

2.3. Confidentiality Attacks

Confidentiality attacks are submissive kind of attacks which allow prohibited access to confidential resources and data. The main purpose of an attacker is not the data alteration but data access and distribution. The most frequent confidentiality flaws are insecure cryptographic storage, insecure direct objects reference, improper error handling and information leakage.

2.4. Integrity Attacks

The target of this type of attacks is to create, modify or even destroy the existing e-learning system data. There are different types of Integrity attacks: Buffer overflow, Cross Site Request Forgery (XSRF/CSRF)), Cross Site Scripting (XSS), Injection flaws, upload and run malicious files, Failure to restrict URL access. Harmful files can be uploaded as homework or just music,

which are not controlled by the learning system. In the field of student data (e.g. form field) the attacker can write such a code, which is a command for incorrect actions. With the help of XSRF the attacker can create a dynamic WEB site, which concludes the harmful script and it can steal the web browser from the user. XSRF attack method can be applied by the learning system users. Cross Site Request Forgery (XSRF/CSRF) is a client side Attack which exploits faith that an LMS has for the user. When the user is logged into LMS, the attacker can deceive his browser by making a request to one of LMS tasks, which will cause a change on the server. Buffer overflow attack [5] occurs when a LMS module (e.g. libraries, drivers, server components) tries to store data into an available buffer without validating its size by inserting larger values than expected. In case of Failure to restrict URL access, some LMS resources are limited to a small subset of advantaged users (e.g. administrators).

3. Effective Attacks Against Moodle Security

Studies have found that these types of attacks can hack Moodle security.

- Username prediction
- Password prediction
- Session hijacking

3.1. Password Prediction

A Brute-force attack can be applied because of a structural defect of the Moodle VLE identification methods. The attacker sends requests with blank cookie fields, so the login failure count becomes zero when the cookie field is blank in the request. As a result of this, the attacker may try an infinite number of passwords.

3.2. Username Prediction

The User name prediction is also possible to implement via a brute force method. Multiple requests are sent to the system with different usernames and the same password. In case of the existing username the system responds later than the other non-existent usernames.

3.3. Session Attack

Two session attacks are effective against Moodle: Session Hijacking and Session Fixation. Session hijacking is a part of the eavesdropping attacks, where an attacker listens to the communication between the client and the server trying to find the payload inside: in this case the HTTP request, information that can be used to impersonate the user and take control of his or her session. Moodle manages its sessions trough two values to identify an active session: MoodleSession and MoodleSessionTest. These values are stored in the cookie that is sent to each HTTP request inside the header of the message. In order to impersonate a target user, an attacker must obtain such values. Session Fixation attack also targets the session data of a user. However, this attack is classified as an active attack [3] or an interception attack. Instead of eavesdroping the communication between a target user and the server, the attacker intercepts the HTTP request of the target user.

4. Solutions to Moodle Vulnerabilities

As it was shown in the previous section, Moodle is vulnerable to the following attacks: session fixation, session hijacking, prediction of usernames and prediction of passwords by brute force. Such vulnerabilities can be avoided by modifying certain portions of the code and adding new functions. These modifications will be described later [2].

4.1. To Use SSL Over the Entire Site

Moodle already has an option to use SSL over certain critical actions. However, such method cannot prevent session fixation, session hijacking and username prediction. In order to avoid such attacks the entire site must create SSL connections with its clients. This can be done by adding a PHP scripts that change the content of the object that holds the environment configuration named CFG. Inside CFG there are the following four variables that are SSL related.

- Themewww. This variable holds the location of resources for building the graphical interface as a full URL string. The script has to change the HTTP protocol for HTTPS (SSL request).
- Wwwroot. Moodle uses this variable to know the URL assigned to it for a quick navigation. The script has to change the HTTP protocol for HTTPS.
- Loginhttps. The value of this flag is retrieved from the database and when it is on the login page, it is encrypted trough SSL. The script turns it on, even if the main configurations say otherwise.
- Httpstheme. When the loginthttps is turned on, the original source code changes the URL protocol from HTTP to HTTPS. This script also changes this value to HTTPS, overriding the original loginhttps value.
- The script also has to change the value of the global flag HTTPSPAGEREQUIRED to true. This flag is a part of the Moodle default configuration. Such fixes were implemented in a script called buap_security that is invoked when the main configuration script config.php is called on every user request. The security server configuration page was also changed to reflect the new option of ciphering the entire site by modifying the source code of the security.php located inside the admin package.

4.2. ID Session Regeneration

The SSL protocol cannot protect the site from session fixation when the user requests a connection for the first time if that petition is done by HTTP protocol without SSL. This was fixed by generating a new ID Session when the user is authenticated by login/password matching. PHP allows to change the ID by placing the instruction session_regenerate_id after switching privileges, at the line 2684, from the source code moodlelib.php stored inside the lib package.

4.3. Login with CAPTCHA

The authentication service, implemented as a login page, can be a subject of automatic brute force attack. The login page can be protected by using CAPTCHA [1]. The login page was added with the official CAPTCHA implementation known as reCaptcha. This makes the authentication service stronger against the brute force attacks automated with software tools. Moodleib.php has to be modified in order to check the new data associated with the reCaptcha library.

4.4. Correct Permissions Loading

As the author suggested in [6], usernames stored inside Moodle can be predicted because the permissions are loaded before username and password checking, which make responses to take longer when a request with a valid username is sent. This was fixed by just changing the order of the actions taken by the authenticate_user_login method coded in the moodlelib.php file.

4.5. Username Obfuscation

As a part of its authentication implementation, Moodle stores the username inside the cookie of the HTTP protocol. This field is obfuscated with the RC4 algorithm using a private key defined in the source code. This is highly insecure because even with SSL an attacker can capture the user cookie of older sessions and can decrypt it with the information of the source code. In order to avoid such decryption, a new configuration file was implemented allowing the administrator of Moodle to change the obfuscation private key and even to choose the algorithm used; instead of using the Moodle implementation of RC4 the new configuration file implements the mcrypt library [4] of PHP. It is possible to change also the algorithm used for storing passwords. Currently, Moodle uses MD5 for storing passwords inside its database, but there are works in [7] that show how an MD5 hash can be broken. The new configuration file also offers a possibility for selecting a new hash algorithm available in the hash library [4] of PHP. However, when changing this parameter, the administrator of Moodle must be aware that every password hash previously stored with the old algorithm, even the password of the administrator, will become invalid.

References

[1] A. L. Von, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security", *Conference on the Theory and Applications of Cryptographic Techniques*, EUROCRYPT, pp. 294-311, 2003.

[2] J. Carlos, G. Hernández and C. M. A. León, "Moodle security vulnerabilities", *5th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*, ISBN: 978-1-4244-2499-3, 2008.

[3] M. Eric, "Network security a beginner's guide", *2 Ed., McGraw-Hill/Osborne*, pp.19-24, 2003.

[4] S. Chris, M. Southwell, "Pro PHP security", *Apress*, pp. 66-68, 80-85, 2005.

[5] Stapic' Z., T. Orehovački, M. Đanic', "Determination of optimal security settings for LMS Moodle", *Proceedings of 31st MIPRO International Convention on Information Systems Security*, Opatija, vol. 5, pp. 84-89, 2008.

[6] D. Stuttard and M. Pinto, *The Web Application Hacker's Handbook: Discovering and Expl oiting Security Flaws*, Wiley Publishing Inc., 2007.

[7] X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPENMD", in Cryptology ePrint Archive, http://eprint.iacr.org, (Accessed 25 January 2012), Report 2004/199, 2004.

[8] 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.

Submitted 14.11.2012, accepted 06.02.2013.

Անվտանգության խոցելի խնդիրները ուսուցման կառավարման MOODLE համակարգում

Վ. Առաքելյան

Ամփոփում

Հոդվածում հետազոտված են ուսուցումը կառավարող MOODLE համակարգի անվտանգությունը ապահովող մեխանիզմները: Հայտնաբերվել են որոշ խոցելի հատվածներ, առաջարկվել են լուծումներ և մեթոդներ, որոնց կիրառման դեպքում համակարգը կդառնա ավելի պաշտպանված և անվտանգ:

Уязвимые проблемы безопасности в системе управления обучением Moodle

В. Аракелян

Аннотация

В этой статье исследованы механизмы безопасности системы управления обучением Moodle. Обнаружены некоторые уязвимые части и предложены некоторые решения и методы, с использованием которых можно сделать систему более надежной и безопасной.