ABSTRACT
Information security is becoming a mission-critical concern for organizations. With the increasing number of threats; continuous follow-up for publicly used applications is very critical to ensure a reasonable security level. Learning Management System (LMS) is becoming more popular and publicly used on the internet which makes the security of LMS very crucial. As assessment of applications is essential part of organization risk assessment, the LMS is one of the main applications to be secured. In this work we examined the security features of an open source LMS and propose security enhancements to mitigate the threats we found. The implementation of the security enhancements were also presented.

Keywords

1. INTRODUCTION
Learning Management Systems are used to perform student registration; track learner progress, record test scores, and indicate course completions and finally it allow instructors to assess the performance of their learners [1,2].

As an application widely used by a bulk of users securing this application is becoming more critical. In educational organizations like universities the security of LMS is important to protect the privacy and the integrity of data. Personal data of students including their grades should be kept secure. The educational materials must be kept integrated and the test questions must be kept confidential.

This paper will examine the security aspects of an open source LMS namely ATutor and give solutions to the weaknesses. The next section gives brief introduction about LMS, the security requirements, and the security aspects of LMS. Security assessment of ATutor will be presented in section 3. Section 4 will show the enhancements made.

2. Technical Background
In this section a brief background about LMS followed by some aspects of security will be presented. At the end of the section we elaborate the security requirements of LMS.

2.1 Learning Management System (LMS)
Learning Management System is a software that deploys, manages, tracks and reports on interaction between learner & content and between learner & instructor [2]. Most of these systems are web based. Many commercial and open source systems are available. We choose ATutor as case study since its is a widedly used open source LMS [3].

2.2 Security Requirements
The main aspects of information security are system security and communication security. System security refers to the protection of information within a computer against
unauthorized use and abuse. Communication security refers to the protection of information during its transmission on a network. In general, the main security requirements are: Confidentiality, Integrity, Availability, and Accountability[4]. The rest of this section gives a brief explanation of these requirements and how it is related to LMS.

Confidentiality: Information must be only disclosed or revealed for authorized users. Therefore, sensitive information need to be protected when it is stored or transmitted over the network. The personal information of the students must be kept secure, only the authorized instructor may see the needed information. On the other hand, the exams and tests must be disclosed only to the authorized students when they are ready to take test.

Integrity: Information must not be modified by unauthorized users. This means that information must be protected from malicious or accidental alteration, including insertion of false data, contamination or destruction of data. The course material should be kept integrated and protected from modification by unauthorized users. The exam grades of the students must be kept intact.

Availability: Information must be available to authorized users in a timely fashion. Authorized users must get access to the information when they need it. The students, as well as the instructors, should have the system available all the time.

Accountability: Audit information must be kept and protected to trace actions related to security of the system. In LMS the information related to accessing the system will be important for auditing and forensic analysis. While the information about the progress of the student is part of the features of LMS and not part of the security requirements.

2.3 Message-digest Algorithm (MD5)
Encryption is used to protect the data from unauthorized users. Many encryption algorithms are available in the literature [5]. The MD5 message-digest algorithm is a one way hash algorithm developed by Ronald Rivest at MIT in 1992. MD5 (1992) is an improved version of MD4, but is slightly slower than MD4 (1990). The algorithm takes an input message of arbitrary length and produces a 128-bit hash value of the message. The input message is processed in 512-bit blocks which can be divided into 16 32-bit sub-blocks. The message digest is a set of four 32-bit blocks, which concatenate to form a single 128-bit hash code [5]. Since the MD5 is on way encryption it is used in some operating systems to encrypt the users passwords. We will use the MD5 to encrypt the passwords in the system.

2.4 Security in Learning Management System
The LMS usually accessed over the Internet or the campus Intranet. Consequently it will face many risks like spoofing, sniffing, denial of service…etc. The main security issues in LMS are mainly Users Security and Content Security. This section will elaborate on these two issues.
Users Security: Identification and authentication is the first line of defense. Using the suitable means of identification and authentication prevents unauthorized users from accessing a computer system. Usually LMS have three categories of users students, instructors and administrator. Each of these categories is assigned special privileges. LMS as many other systems use the user name for identification and the password for authentication. Some organizations may use other means to proof identity like finger prints. However, the level of authentication required depends on the organizations policy.

Contents Security: The content of LMS are mainly courses, grades, exams, and progress data. The content is protected form illegal access by using basic identification and authentication. The course content can be copyrighted and should not be exposed to the public except thoes allowed by the organization policy. The exams are confidential and must not be exposed except for authorized people. The grades are considered private information and they are confidential. Moreover, the grades must be kept from any illegal change.

The next section explains how ATutor protects users information and content by defining different types of users with certain privileges to each type.

2.5 Access Control
ATutor has four types of user’s accounts Administrator, Instructor, Student, and Unconfirmed user. Based on the type of user the access is determined. The user types are described bellow:

Administrator: ATutor has three kinds of administrator accounts Super Administrator, Active Administrator, and Inactive Administrator. The Super Administrator account has no restrictions and has access to all of the administrator options. This is the only administrator type that can create and delete other administrator accounts. There must always be at least one Super Administrator account. The Active Administrator account has limited access. This administrator only has privileged access to sections that they were assigned to when their account was created by the Super Administrator. The Inactive Administrator account has not been assigned any access privileges. As a result, this administrator cannot sign-in.

Instructor: It is a regular account which can enroll in courses as well as create courses.

Student: It is a regular account which can enroll in courses, but not create courses.

Unconfirmed user: Unconfirmed accounts are created only when the system is configured to request e-mail confirmation upon registration.

3. Assessing security of ATutor
We selected ATutor as an example of widely used LMS, yet it has some security weaknesses[2]. ATutor is an open source web-based learning management system designed with accessibility and adaptability in mind. ATutor complies with international accessibility standards and allows access to all potential learners, instructors, and
administrator, including those with disabilities. Our assessment of the ATutor version 1.5.1 was based on the issues mentioned in section 2.4 and resulted in three main security threats: SQL injection, Password format & storage, and Logging users activity.

### 3.1 SQL Injection
Structured Query Language (SQL) is a textual language used to interact with relational databases. SQL Injection occurs when an attacker is able to insert a series of SQL statements into a ‘query’ by manipulating data input into a web-based application[6,7].

An SQL Injection attack is an attack that comes from user input that has not been validated. The objective is to fool the database engine to run malicious code that will reveal sensitive information. At the time of our assessment the passwords in ATutor were stored in the database and by using injection the passwords can be revealed. In the new version of ATutor 1.5.2 the SQL injection prevented by using one of the common counter measures for this attack which is input validation.

![Figure 1: The passwords in ATutor stored as plain text.](image)

### 3.2 Password Format
Poor password selection is frequently a major concern for any system's security[4,8]. Based on the organizations policy users should be forced when choosing a password to use special combination that help protecting their accounts. A perfect password should have a mixture of alphanumeric and special characters. In ATutor there was no restriction on password format that means any non-empty password is acceptable.

### 3.3 Password Encryption
The password in ATutor are stored in database as plain text. This makes the users passwords vulnerable to theft. The “at_members” table in the database contains the users information including the passwords as in Figure 1.
3.4 Logging and monitoring
The Administrator Activity Log lists all actions made to the ATutor database tables by the administrator. As in Figure 2, viewing a log entry will give detailed information about the selected activity. The log can be reset by using the Reset Log feature. Logs are very helpful tools for auditing and play a role in computer forensics [9,10]. However, the ATutor lacks logs of the users access time and failed logins.

![Figure 2: The administrator activity log.](image)

4. Security Enhancements
In this section we present the enhancements made to ATutor to make it more secure. The SQL injection was resolved in the latest version 1.5.2., the other issues are listed in this section with proposed solutions.

4.1 Password Format
To restrict users from selecting simple passwords, we added some rules on the password to prevent the simple password.

The rules which we added are: the password length should be more than or equal 6 characters, and should be mixed from capital and small letters, numbers, and special characters. These rules will add some extra protection to the users accounts.
4.2 Password encryption

To secure the stored passwords in the data base we used the MD5 encryption which maps all the passwords into 32 characters hash (Figure 4). The data base table was changed to hold the 32 char instead of the original 20 plain text char. As a consequence the password reminder will not send the old password, but it will reset the password to a new one chosen randomly by the system and send to the users e-mail.
4.3 Adding Access log
We added access log to *ATutor* which contains the IP address, user name, login status, and time & date. The IP address tells from which location a person was accessing the *ATutor* system. The login status can be either log in, log out or invalid log in. The user name is the name used to enter the system. The time and date tells the time event happened. These information will help the administrator to monitor the system login activity. A sample log of login attempts is shown in Figure 5.

<table>
<thead>
<tr>
<th>IP</th>
<th>Log status</th>
<th>User name</th>
<th>Time &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>Salim</td>
<td>20:21:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>Salim</td>
<td>20:25:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asim</td>
<td>20:25:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>asim</td>
<td>20:26:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>Salim</td>
<td>20:26:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>Salim</td>
<td>20:26:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asimdh</td>
<td>20:26:, 02nd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>me</td>
<td>10:39:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>me</td>
<td>10:40:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Invalid log</td>
<td>asim</td>
<td>10:40:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asim</td>
<td>10:40:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>asim</td>
<td>10:40:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Invalid log</td>
<td>asimdh</td>
<td>10:40:, 03rd Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asim</td>
<td>11:40:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>asim</td>
<td>11:41:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asim</td>
<td>11:41:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>asim</td>
<td>11:46:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>asim</td>
<td>11:47:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>asim</td>
<td>11:48:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log in</td>
<td>me</td>
<td>12:25:, 04th Dec</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>Log out</td>
<td>me</td>
<td>12:25:, 04th Dec</td>
</tr>
</tbody>
</table>

Figure 5: Login access logs.

Each time the *ATutor* is accessed, it logs the access information into a log file as an entry. By default, the log file is *access_log.log*, and is located in the directory of *ATutor*.

5. Conclusion
In this paper we examined the security features of popular open source LMS. The security assessment of LMS mainly concentrate on the content and the user information protection. We presented the security threats we found associated with the *ATutor* LMS and implemented some security enhancements for these threats. The encryption of passwords was in our view the main concern. The other enhancements are considered an added value. We believe there is still room for enhancements to make the *ATutor* more secure. The log files can be digitally signed to ensure its integrity. Also the new passwords set by the system at the users request should be sent over a secure channel to avoid sniffing. While making the system more secure is a plus we should keep an eye on the system performance and usability. The added security should not compromise the performance of the system and its usability.
6. REFERENCES