"Dimitrie Cantemir" Christian University
Knowledge Horizons - Economics
Volume 6, No. 1, pp. 132–135
P-ISSN: 2069-0932, E-ISSN: 2066-1061

www.orizonturi.ucdc.ro

THREATS ANALYSIS FOR E-LEARNING PLATFORMS

Costinela-Luminiţa DEFTA[4], Aurel ŞERB[2], Nicoleta Magdalena IACOB[3], Constantin BARON[4]

[1]*Faculty of Tourism and Commercial Management, "Dimitrie Cantemir" Christian University, [1]E-mail: lumi.defta@yahoo.com*
[2,3]*Faculty of Finance, Banking and Accounting Bucharest, "Dimitrie Cantemir" Christian University, [2]E-mail: aurelserb@yahoo.com,*
[3]E-mail: nicoleta.iacob_2007@yahoo.com
[4]Faculty of Marketing, Bucharest, "Dimitrie Cantemir" Christian University, [4]E-mail: constantin_baron@yahoo.com

Abstract *In the recent years many advances have been made in the mechanism of providing on-line instruction, thus the need for security is growing. To achieve a good level of security, there are many important elements that must be taken into account: authentication, access control, data integrity. In this paper we will try to investigate the information security threats within e-learning environments. This paper highlights some key security issues that must be taken into consideration in developing and using an e-learning platform. It focuses on vulnerabilities in relation to the application system and we will not cover the vulnerabilities in terms of host and network in e-learning.*

Key words:
E-learning, threats, security, management

JEL Codes:

1. Introduction

E-learning can be defined as a technology based learning in which learning materials are delivered electronically to remote learners via computer networks. It may cover a wide set of applications, systems and processes, such as e-learning systems, web-based learning, virtual classrooms and digital collaboration.
E-learning system represents a technology that makes use of network technologies such as the Internet, intranet, extranet and more to deliver contents to individuals. It has features to design, deliver and administer online learning.
In corporate environments, it can be used as an efficient way of sharing information between co-workers. In academic environments, it can be used in primary, secondary, tertiary and special training centers to enhance the traditional learning system or to create a complete online learning system. The platform offers various resources for managing groups of students, educational programs and also provides flexible ways to measure students' knowledge.
An e-learning management system is a software package that enables the management and the delivery of online content to learners. It is a complete software package with various features that enables the management and delivery of online content to remote learners. It may also be seen as an interface between its users (learners, lecturers, and administrator) and contents such as course material. There are some popular e-learning management systems such as Moodle, Claroline and ATutor.
All these systems are released under the General Public License (GPL), which means that the initial package can be freely downloaded, installed, and distributed without charge.
Meeting the security requirements in an e-learning system is an extremely complex problem, because it is necessary to protect the content, services and the personal data not only for the external users but also for the internal users, including system administrators.
In the following section, we will discuss the common security threats and countermeasures related to each type of e-learning users. Then, we will analyze the security threats specifically for applications in e-learning environment. The results of the threats analysis can be used as a guide for e-learning providers in terms of implementing e-learning security strategy and also for users with the purpose of increasing their awareness with regard to the potential threats within e-learning environments.

2. Security threats from the user's point of view

The main aim of this section is to identify the growing information security challenges of the e-learning management system from each user's perspective. Some scenarios will be formulated and discussed to illustrate the information security risks related to each user's activities.

2.1 Lecturer

A lecturer is responsible for coaching as well as tracking the performances of his respective learners. He can manage his profile (create account, change

password or contact details), create course materials and upload them, create online assessments, setup grading scales, evaluate the assignments submitted by learners and then upload the results for learners, assign learners to a course and use chat/forum to communicate with his learner and subordinates.
The security threats that may rise from the above specified activities are:
- an unauthorized person can change the profile of the lecturer
- fake course material, assignments, grading scales or assessment results can be created and uploaded by unauthorized users
- course material can be viewed, altered or deleted by an unauthorized person
- the exam set up by the lecturer can be viewed before the due date
- the exam can be deleted when a student knows that he is not ready
- assessment results may be viewed, changed or deleted by an unauthorized person
- an unauthorized person may act as an unauthorized lecturer and register learners to a course.

2.2 Learner

A learner can manage his profile (create account, change password or contact details), access course materials, take online assessment exams or quizzes (which are set by the lecturer), complete posted assignment(s) offline and submit it online for feedback, access their assessment results and use char/forum to communicate with his lecturers and fellow classmates.
Without proper information security an e-learning platform could be exposed to the following most common information security risks, which arise from the learners' activities:
- an unauthorized person may alter/delete the profile of the learner
- someone can access a course material pretending to be the learner
- when a learner finds out he/she cannot pass the test, he can create a Denial of Service attack (DOS) to sabotage the exam
- someone can submit a fake assignment pretending to be the learner
- the student can deny submitting the assignment when he thinks that he will not pass
- submitted assignments can be viewed, copied, changed or deleted
- the grade report may also be viewed by unauthorized persons
- cheating during exams, which include getting unauthorized help from someone or from calculators, cell phones and so on
- the learner can pass his/her personal Identification and Authentication information to his/her friend so that the friend can write the exam on his/her behalf.

It is difficult for a system to determine whether the person logged in is the authentic learner (i.e. the owner of the secret key) or someone else on his/her behalf that has entered the authentication information, so long as the secret key supplied is valid. In that, if this issue is not addressed, the overall integrity of the system can be compromised.
Some of the possible solutions to mitigate the problem are:
- setup effective identification and authentication services such as the biometrics based security mechanisms, which are relatively harder to tamper with
- implement effective security policies and procedures
- implement effective user awareness program
- enforce a supervised environment which would create an extra security layer.

2.3 Administrator

An administrator is the person who oversees and moderates the activities carried out on the e-learning platform. He also defines and assigns privileges to the rest of the users. He can manage his profile (create account, change password and contact details), set up roles and privileges and assign them to learners and lecturers, and assign lecturers to courses.
The following risks may arise from the administrator activity:
- an unauthorized person may alter/delete the profile of the administrator
- fake roles and privileges could be set by an unauthorized user
- the roles and privileges could be altered by an unauthorized user
- an unauthorized person may act as an authorized administrator and assign lecturers to a course.

3. Security platform threats and possible solutions

There are many threats that could affect an e-learning platform, but we'll list just some of them: cross site scripting, cross site request forgery, direct sql code injection in the web page, sql injection in the site address, different searches using search engines to retrieve personalized web-site information (like password, username), password cracking using decryption systems, guessing the web site session id (session prediction).
Because the presentation of all these threats may cover probably an entire book, in the following paragraphs we will detail the most common threats for e-learning platforms: cross site scripting, cross-site request forgery and sql injection.

3.1 Cross Site Scripting (XSS)

The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user. Such a manipulation can embed a script in a page which can be executed every time the page is loaded, or whenever an associated event is performed. Using this attack, an attacker can access sensitive information or launch a denial of service attack.

To mitigate it, the following measures can be taken:

- check that the web site pages return user inputs only after validating them from any malicious code
- convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums
- use testing tools extensively during the design phase to eliminate such XSS holes in the e-learning application before it goes into use.

3.2 Cross-Site Request Forgery (CSRF)

CSRF is an attack that tricks the victim into loading a page that contains malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. Some prevention ideas for this type of attack are:

- check HTTP referrer (URL)
  - for privacy, referrer may not be present
  - redirects on the site might allow for correct referrer even if only redirecting to its own site.

Example:
http://domain.com/redir.php?url=/delete.php?id=75.

- store state
  - when user browses to the form, record state, check it when it is submitted.

Example: server-side state or cookies (attacker cannot set cookie for another user on victim's site without another security bug).

  - hide HTML form filed state.

3.3 SQL Injection

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

SQL injection occurs when:

- data enters a program from an untrusted source;
- the data used to dynamically construct a SQL query.

The main consequences are:

- confidentiality - since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities
- authentication - if poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password
- authorization - if authorization information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability
- integrity - just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

SQL Injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind.

For example, if the e-learning application contains a sql request like:

select id, firstname, lastname from authors,

and someone enters in the application fields: firstname – delete * from authors'known, lastname – name, the sql query becomes:

select id, firstname, lastname from authors where forename = 'delete * from authors'known' and surname ='name'.

The database will execute in fact:

delete * from authors,

which will purge the authors table.

To avoid this, all the special characters should be escaped. In PHP language, in which Moodle is written, we can for example to use the mysql_real_escape_string function, in Java we can use prepared statements and so on.

The most common methods to prevent this kind of SQL injection vulnerability are:

- check the user's input for dangerous characters like single-quotes
- using prepared statements, which tell the database exactly what to expect before any user-provided data is passed to it
- ensure that error messages give nothing away about the internal architecture of the application or the database.

4. Conclusions

In this paper we described some e-learning security threats from the user's (lecturer, learner, administrator) and platform perspectives. We detailed the most common threats for e-learning platforms: cross site

scripting, cross-site request forgery and sql injection. A secure learning platform should incorporate all the aspects of security and make most of the processes more transparent to the teacher and the student.

Most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements. However, it is clear that there will be a growing need for high levels of confidentiality and privacy in e-learning applications, and that security technology must be put in place to meet these needs.

The implied need for security and connected requirements by the use of e-learning systems has only been marginally examined up to now. The trend of moving from traditional education to blended/on-line one make the requirement for a security management framework specific tailored to the e-learning environment to be in the pipeline more than ever. It will act as a guide in helping the e-learning institutions in managing the information security within the e-learning environment.

References

[1] Gallagher T. Finding and Preventing Cross-Site Request Forgery, Black Hat USA, 2006.

[2] Cezar V, Tatar L, Codreanu A. Integrating Information Security in an E-learning Environment, The 7th International Scientific Conference eLearning and Software For Education, Bucharest, 2011.

[3] Defta L. Information security in E-learning Platforms, Proceedings of the 3rd World Conference on Educational Sciences, Instanbul, Turkey, 2011.

[4] Defta L. Security Issues in E-learning Platforms, World Journal on Educational Technology, Vol 3, issue 3, 153-167, 2011.

[5] Edgar R. Security in e-learning. Springer. Vienna University of Technology, Austria, 2005.

[6] Iacob N. Distributed Queries in the E-learning Environment, World Conference on Educational Technology Researches, Volume 28, pages 241–245, 2011.

[7] Assefa S. An Information Security Reference Framework For E-learning Management Systems, University of Johannesburg, 2009.

[8] Edgar R. Security in E-learning, ELearn Magazine, 2005.

[9] Şerb, A. – *Software educațional* - Editura Pro Universitaria. 2011.