Mediterranean Smart Cities Conference (MSCC 2024)
2-4 May, 2024, Martil, Morocco

Security of Open-Source Learning Management Systems (LMS)

KAMAL EL AFOUI
Department of Computer Science
Laboratory of Artificial Intelligence, Data Science & Emerging Systems (LIASSE)
National School of Applied Sciences (ENSA)-Fez, Morocco
kamal.elafoui@usmba.ac.ma

MOHAMMED BERRADA
Department of Computer Science
Laboratory of Artificial Intelligence, Data Science & Emerging Systems (LIASSE)
National School of Applied Sciences (ENSA)-Fez, Morocco
mohammed-berrada@usmba.ac.ma

SAID HRAOUI
Department of Computer Science
Laboratory of Artificial Intelligence, Data Science & Emerging Systems (LIASSE)
National School of Applied Sciences (ENSA)-Fez, Morocco
said.hraoui@usmba.ac.ma

Abstract**—** *This paper delves into the evolution and significance of Learning Management Systems (LMS) in education, with a focus on security and privacy vulnerabilities within open-source LMS platforms. Beginning with a historical overview and the emergence of LMSs, it addresses the lack of consensus regarding their definition and scope. The paper emphasizes the criticality of selecting the right LMS and compares prominent open-source options, including Moodle, Sakai, Blackboard, and Canvas. The analysis explores security concerns, categorizing threats into four main groups: authentication, availability, confidentiality, and integrity attacks. It identifies and discusses twelve critical security flaws from an LMS perspective, stressing the importance of proactive vulnerability recognition. Furthermore, the paper evaluates the usability, content authoring standards, multi-lingual support, and collaboration features of the four LMS platforms. Moodle stands out for its modular structure and extensive language integration options, while Sakai earns praise for its efficient collaboration systems. In conclusion, the paper underscores the crucial decision of selecting an appropriate LMS to enhance the learning experience and achieve educational goals. While Moodle and Sakai are recommended for their robust features, Blackboard and Canvas remain viable options, requiring careful consideration of their relevance to specific educational challenges.*

Keywords— *Learning Management Systems (LMS); Open source; Security; Vulnerability; Recommendations.*

I. INTRODUCTION

The integration of computer technologies in educational practice dates back several decades to the onset of the 'information revolution.' In the 1980s, there were debates about the significance of computers in education [1]. However, in the 1990s, personal computers, educational software, and the World Wide Web experienced explosive growth, making computer-assisted pedagogy a prominent feature in education.

This development led to the rapid emergence of Learning Management Systems (LMSs) - comprehensive learning platforms that support various aspects of education, from administrative tasks to course delivery and assessment. Some researchers [2] attribute the emergence of LMSs to basic "training management systems," which later evolved into comprehensive "e-learning platforms," while others [3] highlight the role of integrated learning systems as predecessors to modern LMS.

However, there is no universal consensus on the exact scope of the term "Learning Management System," which is often used interchangeably with "course management system." In this context, attempting to establish a singular, all-encompassing definition of an LMS or differentiating it from a CMS is considered unproductive. As a result, both terms are frequently used interchangeably. This publication aims to provide an "ostensive" definition of an LMS, covering a wide range of commercial and open-source LMSs and related technologies used in higher education institutions. However, the focus is primarily on LMSs used in academic settings rather than those used for corporate training purposes.

Currently, there are numerous LMS solutions available for higher education from commercial providers. Alternatively, institutions can choose open-source alternatives like Moodle or Sakai without incurring licensing costs. Proprietary in-house e-learning platforms developed by some institutions, particularly for-profit schools, are not addressed in this publication.

After introducing the problem, we will focus on security and privacy vulnerabilities. These vulnerabilities and threats will be discussed from the LMS point of view, and additionally these threats will be grouped into four main groups according to their LMS related type.

In the rapidly evolving landscape of education technology, the selection of a Learning Management System (LMS) is pivotal for institutions seeking to enhance their learning processes. This

document presents an analysis of four prominent open-source LMS platforms: Moodle, Sakai, Blackboard, and Canvas. Our assessment focuses on key criteria essential for effective learning support, including usability, standards-oriented content authoring, multi-lingual support, collaboration features, and support for diverse learning methods. By evaluating these aspects, we aim to provide valuable insights into the strengths and suitability of each LMS for various educational environments.

I. LITERATURE REVIEW

A. Leaning Management System (LMS):

While the goal of a CMS is to store and distribute content, the goal of a Learning Management System (LMS) is to "simplify the administration of learning/training programs within an organization" [5].

LMS allow a learner to launch eLearning and help manage the interactions between learners and eLearning materials, along with other related resources. They also assist learners in planning and monitoring their progress in their learning journey.

LMS are "software that automate[s] the administration of training events" [6]. The automation of administrative functions via LMS can lead to considerable time, personnel, and resource savings. An LMS has significant administrative functions, which help an organization to "target, deliver, track, analyze, and report on…. learning" [5]. These robust administrative functions enable organizations to track completion of mandated training, currency of professional certifications, and mandatory human resource related programs[7].

LMS integrate tools to manage the tracking of learners and the content along with appropriate work flow processes. This combination of tools and processes allows an LMS to support the delivery and management of learning and tracking the results. As [8] explains, learning management systems "enable companies to plan and track the learning needs and accomplishments of employees, customers, and partners".

Every LMS should have the ability to display a catalog, register learners, track learner progress, and provide reports. LMSs must be capable of handling various delivery modes, such as online, instructor-led, self-paced, collaborative, facilitated, nonfacilitated, and others [9].

LMSs are either installed on an organization's intranet or hosted off-site by service providers. When using service providers, LMSs are accessed through either an extranet, which is a private network that uses Internet protocols and public telecommunication systems to share a business's information externally, or the internet, which consists of interconnected networks using TCP/IP protocols [10].

The internet is external to a corporate intranet. [11] emphasizes that a learning management system uses Internet technologies to manage the interaction between users and learning resources, whether the LMS is operated internally or externally to a corporation.

Figure 1 illustrates the relationship of the components that make up a learning management system. An LMS has the capability to manage learners and their records, as well as the learning process. Within an LMS, users interact with their learner data and learning management information. The learning content is not part of this configuration.

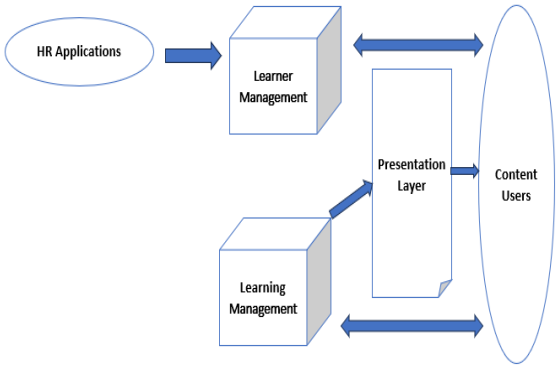

Fig 1: *LMS Components*

Some LMS focus on content management, but it is not their primary focus. According to [11], LMS vary from vendor to vendor in terms of their features, but they all have core capabilities. These include an online course catalog, an online registration system, competency assessment, eLearning launch and tracking, learning assessment, learning material management, customizable reporting, collaborative and synchronous learning tools, and integration with other enterprise applications. The goal of LMS is to manage the processes related to training and education delivery and administration. LMS are structured around the course rather than course content. Collaborative tools within LMS allow learners to work together using internet, intranet, and extranet technology coupled with CMS.

The next section will delve into the combination of content and learning management via the Learning Content Management System (LCMS).

B. Types of LMS

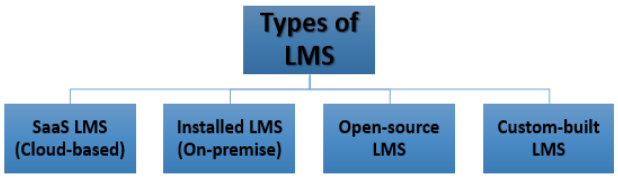

Fig 2: *Types of LMS*

When exploring Learning Management Systems (LMS) it's important to consider 4 types:

- **SaaS LMS (Cloud-based):** This option offers quick setup and easy access, making it suitable for organizations looking for convenience and scalability. However, customization options may be limited, and it's crucial to choose a provider that offers tailored solutions to meet specific needs, such as Disprz LMS.
- **Installed LMS (On-premise):** On-premise LMS solutions provide greater control over data and system management, which can be beneficial for organizations with strict data security requirements. However, they often come with high upfront costs and ongoing maintenance responsibilities, requiring dedicated IT resources.
- **Open-source LMS:** Open-source LMS platforms offer flexibility and customization options, as they are community-driven and allow for collaboration to improve the system. While they provide extensive customization possibilities, setting up and maintaining them may require technical expertise, and comprehensive vendor support may be lacking
- **Custom-built LMS:** Tailored to specific organizational needs, custom-built LMS solutions offer unparalleled customization and control. However, they come with significant development costs, ongoing maintenance challenges, and potential compatibility issues as technology evolves. Additionally, reliance on a small team for maintenance can pose risks in case of turnover or resignations.

C. Features of an LMS

[4] Identify the most common features of an LMS by categorizing them as pedagogical tools for:

- Content creation;
- Communication tools;
- Assessment tools;
- Administration tools.

a) **Content creation** and display tools allow instructors to generate course content using a text/HTML editor or upload various types of files such as documents, spreadsheets, presentations, images, animations, audio, or video into the LMS. Hyperlinks can be used to direct users to external websites or documents. Assignments or drop boxes provide a space for students to submit materials assigned by their instructors for grading and feedback. Instructors can organize content into folders and subfolders and use the content release feature to control the visibility of folders and individual content items to students.

b) **Communication tools** in an LMS enable instructors to facilitate interaction between students and instructors as well as among students. Asynchronous tools include course announcements, student web pages, email communication with instructors and classmates, threaded discussion boards, wikis, blogs, and file sharing. Synchronous tools found in a typical LMS include text chat, whiteboard, and a shared web browser. Students can be grouped into virtual teams or groups, which may have access to text chat, threaded discussion, and file sharing features visible only to group members and the instructor.

c) **Assessment tools** provide instructors with various methods to test, survey, and track student progress and activity. Common tools include a test/assessment manager for creating and deploying exams, a question generator for creating different question types (multiple choice, true/false, essay, short answer, matching, etc.), and question pools or test banks to store questions for multiple exams. Questions in exams (and choices in multiple-choice questions) can be randomized and displayed either one at a time or all at once. Instructors can set time limits for exams and specify the type and amount of feedback students receive for correct and incorrect answers. Exams can be graded, ungraded, or used as anonymous surveys with aggregated results. An electronic grade book for managing student assignments and displaying grades is a highly valued feature of nearly every LMS. Additionally, instructors can track student activity within an LMS, including logins, time spent, and specific areas visited.

d) **Administration tools** for instructors include control panels that allow them to manage settings for content creation, communication, and assessment tools. They can also customize the appearance of the course, control the availability of tools, content, and resources for users, manage files, and move or copy content. Administrative tools for LMS system administrators enable them to manage user accounts and courses, enroll instructors and students, enable or disable accounts and courses, and track activity within the system.

D. LMS Advantages

Before learning management systems became widely available, the delivery of online instruction required faculty or instructional designers to master Hypertext Markup Language (HTML) or web page authoring programs [12].

Turning in assignments generally involved e-mailing the professors, while assessment was done manually, with the results often entered into spreadsheets. Delivery of content online was limited, as publicly available websites were not protected from copyright violation by fair use guidelines [13]. The major advantage of the LMS is that it brought content delivery, communication, assessment, and administration of online instruction into a single secure platform that could be accessed by anyone on the Internet [4].

E. LMS Limitations

The LMS is not without limitations and disadvantages. According to [14], users often found the systems to be slow, confusing, and more focused on administrative needs rather than student needs. Another complaint was that the LMS interface was dull and rigid compared to more engaging online social environments like MySpace, Facebook, and YouTube [14]. [25] suggested that the LMS interface should be simplified and made more intuitive. [26] discovered that current systems primarily served as a repository of materials and did not support sound pedagogical practice. [27] also expressed concern about the lack of instructional design guidance and tools for the development of rich multimedia-based instruction. While some teaching tools exist within an LMS [4], they do not include tools to guide instructors in the design of online instruction and sound pedagogical practice [14].

F. Open Source LMS

As commercial LMS companies grow larger and as their products become more complex and expensive, many schools, colleges, and universities are questioning whether their needs can be better met by open-source products, rather than by a commercial system. Open source has financial and programmatic appeal [15]. For those who subscribe to a social constructivist point of view where reality is constructed from the collective experiences of groups [16], open source also has a philosophical appeal. In an open-source environment, the source code of the product is made available to the user without charge. Software licensing fees, which can be substantial, are eliminated. Open-source software frees the user from a contractual agreement with a specific vendor. A program or system based on open-source software may be customized and branded according to a user or institution's needs and desires rather than to a vendor's current priorities. In the case of learning management systems, there exists a vibrant and active community of developers for Moodle and Sakai, the two most popular systems, and for several others (see Other Open-Source Systems below).

II. LMS SECURITY VULNERABILITIES

Learning management systems (LMS) are client/server web applications that, among rest, manage user requests coming from clients such as web browsers [17]. To handle the user requests, they often require accessing security-critical resources (e.g. databases and files) at the server end. In this section we present description of the most critical security flaws [18][19] that are classified into four categories: authentication, availability, confidentiality and integrity attacks. Table 1 displays a summary of classified attack methods and vulnerabilities independent of the specific Learning Management Systems (LMS) implementation The AICA (Availability, Integrity, Confidentiality, and Authentication) threat modeling approach is widely accepted as a model for categorizing attack methods and security vulnerabilities.

Authentication attacks	
1.	Broken authentication and session management
2.	Insecure communication
Availability attacks	
1.	Denial of service
Confidentiality attacks	
1.	Insecure cryptographic storage
2.	Insecure direct object reference
3.	Information leakage and improper error handling
Integrity attacks	
1.	Buffer overflow
2.	Cross Site Request Forgery
3.	Cross Site Scripting
4.	Injection flaws
5.	Failure to restrict URL access
6.	Malicious file execution

Table 1: Attack methods and security vulnerabilities

A. Authentication attacks

Authentication attack occurs when an attacker steals password and thus identity of legitimate end-user with an aim of free access to paid e-learning services. When a LMS authentication has been broken, an attacker has an opportunity to perform availability, confidentiality or integrity type of attack. Today's most critical authentication vulnerabilities are:

1. **Broken authentication and session management:** vulnerability which occurs because account credential management functions (e.g. remember my password, forgot my password, change my password, etc.) and session tokens are not often properly protected. An attacker can compromise passwords or authentication token to assume other user identity. Furthermore, attacker can intercept and steal authenticated session of a legitimate user.
2. **Insecure communications:** vulnerability which appears during transmits of sensitive information (e.g. session tokens) without proper encryption. Attacker can misuse this flaw to impersonate user and access unprotected conversations.

B. Availability attacks

The main goal of availability attacks is to make elearning services and data unavailable to authorized endusers. Most popular form of availability attack is denial of service (DoS) attack which aims to misuse finite bandwidth and connectivity resources of LMS system. DoS attacks are usually malicious but they can also be result of users' incautious behaviour. There are two general types of DoS attack: logic and flooding attacks. Logic attacks (e.g. ping) exploit existing LMS flaws to crash remote server or significantly decrease its performance [20]. Flooding attacks overloads LMS with a high number of requests to disable legitimate users from accessing e-learning resources. DoS attacks present threat to LMS systems because one request can be replicated to many participants.

C. Confidentiality attacks

Confidentiality attacks are passive kind of attacks which allows unauthorized access to confidential resources and data. The main intention of attacker is not data modification but data access and dissemination. The most frequently confidentiality flaws are:

1. **Insecure cryptographic storage:** flaw which is based on a fact that sensitive information does not have appropriate encryption. LMS systems rarely use cryptographic functions properly to protect data and credentials or use weak encryption algorithms. In both situations, valuable data is relatively easy to access by attacker who can conduct identity theft and similar crimes.

2. **Insecure direct object reference:** this vulnerability usually occurs when LMS uses object references directly in web interfaces without authorization checks being implemented. Mentioned object references can be files, database records and primary keys and are contained either by URL or form parameters. An attacker can misuse direct object references in order to access other objects without authorization.
3. **Information leakage and improper error handling:** refers to unintentional disclosure of sensitive data and unneeded information through error messages. LMS can leak sensitive information about its logic, configuration and other internal details (e.g. SQL syntax, source code, etc.). On the other hand, error messages that LMS generate may display too much information which can be useful to attackers in privacy violation or conducting even more serious attacks.

D. Integrity attacks

This group includes attacks which attempt to create new data or modify and even delete existing e-learning data. Most popular of them are:

1. **Buffer overflow attack:** occurs when a LMS component (e.g. libraries, drivers, server components) tries to store data into an available buffer without validating its size. By inserting larger values than expected (e.g. 800 characters in a limited length field), attackers can cause their malicious code to be executed. There are two ways how attacker can take control over application [21]: by injecting attack code or by using code which is already in LMS address space.
2. **Cross Site Request Forgery (XSRF/CSRF):** client side attack which exploits trust that a LMS has for the user [22]. When a user is logged into LMS, attacker can trick his browser into making a request to one of LMS task URLs which will cause a change on the server. While request comes with the user's cookies, server will perform it as it is original. Attacker could use this vulnerability to do anything what authenticated user can do.
3. **Cross Site Scripting (XSS):** refers to hacking technique which allows an attacker to supply vulnerable dynamic web page with malicious script and execute script in victim's browser in order to gather data from a user. There are three general types of XSS: persistent, non-persistent and DOMbased. In our case, the most important meaning have persistent (stored) attacks [23], in which malicious data are persistently stored on the target back end system (e.g. in database) and displayed to the user in a unfiltered form. This is extremely dangerous in LMS because users could see inputs of all other participants.
4. **Injection flaws:** may occur when data provided by user (e.g. in form fields) is sent to content checking routines as part of a command or query [24]. In such attacks, interpreter fail to detect or respond to character sequences that may be interpreted incorrectly, which then results in execution of malicious code by LMS. Finally, attacker could be able to create, update, read or delete all data available to LMS.
5. **Malicious file execution:** attack which is based on a fact that LMS fails to control or prohibit execution of uploaded files. Malicious code is usually uploaded via the upload feature (e.g. homework or image). This kind of vulnerability can be found in many web applications, especially in those which are PHP based.
6. **Failure to restrict URL access:** some LMS resources are restricted to a small subset of privileged users (e.g. administrators). This weakness allows an attacker to retrieve URLs by guessing the address and perform unauthorized operations on unprotected LMS data.

III. RECOMMENDATIONS FOR SECURING LMS

Here is a summary table outlining the aspects of each Learning Management System (LMS) recommendation well, as suggestions, for ensuring the security of an LMS[25] [26] [27]:

LMS	Standards-Oriented Content	Multi-Lingual Support	Collaboration Features	Support for Learning Methods	Securing LMS Recommendations
Moodle	SCORM, IMS	Yes	Forums, wikis, multimedia, video conferencing, chat	Self-based, blended, collaborative learning	Regular updates, strong authentication, data encryption
Sakai	Not specified	Yes	Collaboration features	Blended, self-learning, collaborative learning	Secure hosting, user permissions, monitoring
Blackboard	Not specified	Yes	Integrated content authoring, forums, chat	Distance learning, collaborative learning	Regular audits, user education
Canvas	Not	Not	Not	Not	Not

Table 2 : Recommendations for Securing LMS

- **Regular Updates** Keep your LMS software up to date with the latest security patches and updates to minimize vulnerabilities.
- **Strong Authentication** Enable multi-factor authentication (MFA) for an extra layer of user authentication security.
- **Data Encryption** Encrypt data at rest and in transit to prevent unauthorized access.
- **Secure Hosting** Choose LMS hosting providers known for their security measures and have the necessary protocols in place.
- **User Permissions** Set up role-based access control (RBAC) to limit access to specific features and data based on your users' roles.

- **Monitoring and Logging** Use monitoring and logging systems that can help detect and respond to suspicious activities, and maintain detailed logs of system activities for auditing purposes.
- **Regular Audits** Periodically perform security audits and penetration testing to find and fix any security weaknesses.
- **User Awareness** Educate your users with security best practices: create strong passwords, be wary of phishing attacks, and more.

IV. CONCLUSION

With the rapid proliferation of distance learning, schools confront the difficult problem of choosing and managing an appropriate technological environment that fits their budget, technical resources, curriculum, pedagogy, and profile of the student body. In this context, the paper is intended to fill the gap in the current literature on the interaction between LMSs, supporting technologies, and relevant teaching methodologies. This paper is intended for administrators, faculty, subject specialists, and all those looking to launch a new or to expand an existing distance learning program.

In particular, it covers commercial and open-source LMSs as well as technologies used for synchronous and asynchronous course delivery, and it offers a comprehensive discussion of factors influencing the transition from one LMS to another. The reader will also find coverage of virtual labs, electronic portfolios, and technological solutions related to the problems of plagiarism, student tracking, assessment, and security of e-learning environment.

Most critical security flaws are classified in group of *authentication*, *availability*, *confidentiality* or *integrity attacks*. Short description on each of twelve security flaws is given from the LMS perspective, while recognition of different and possible vulnerabilities is first step in dealing with them.

Choosing the right Learning Management System is a highly critical decision for ensuring that the learning experience is genuinely enhanced and the educational aims are met. As a result of our assessment, we conclude that Moodle is by far one of the best platforms, based on its modular structure, abundant language integration options, and promising consulting operations. Sakai, in a race with Moodle, comes with equally efficient collaboration systems, enabling co-creation among students. In addition, its multi-lingual features support our preference for this platform. We regard Sakai as being highly beneficial for blended and collaborative learning scenarios. Blackboard and Canvas are not inferior to the aforementioned solutions, but we suggest a more deliberate identification of their relevance in relation to the educational challenges to be addressed.

ACKNOWLEDGMENT

This paper and the research behind it would not have been possible without the exceptional support of my supervisors, Mohammed Berrada and Said Hraoui. Their enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept my work on track. Kamal EL AFOUI, my colleague at National School of Applied Sciences, have also helped over our researches and answered with unfailing patience numerous questions about the topic.

REFERENCES

[1] Cuban, L. (1986). Teachers and Machines: The classroom use of technology since 1920. New York: Teachers College Press.

[2] Mallon, D., Bersin, J., Howard C., & O'Leonard, K. (2009). Learning Management Systems 2009. Executive Summary. Bersin and Associates Research Report.

[3] Bailey, G. D. (Ed.). (1993). Computer Based Integrated Learning Systems. Englewood Cliffs, NJ: Educational Technology Publication

[4] Dabbagh, N., & Bannan-Ritland, B. (2005).*Online learning: Concepts, strategies, and applications*. Upper Saddle River, NJ: Pearson Prentice Hall.

[5] English, P. (2001, April). What the future holds for e-learning. Retrieved February 2, 2004, from http://www.futuremedia.co.uk/elearning_guide_thefutureofelearning.php

[6] Hall, B. (2002b). Six steps to developing a successful elearning initiative: excerpts from the e-learning guidebook. In Allison Rossett (ED.) The ASTD E-Learning Handbook. New York: McGraw-Hill.

[7] Hall, B. (2002a). Learning management systems 2002. Retrieved March 1, 2004, from http://www.brandonhall.com

[8] Robbins, S. R. (2002). The evolution of the learning content management system. Retrieved February 25, 2004, from http://www.learningcircuits.org/2002/apr2002/robbins.html

[9] Singh, H. (2001). Learning content management systems. Retrieved November 20, 2003, from http://www.internettime.com/Learning/lcms/

[10] GetNewWise. (2004). Glossary. Retrieved February 25, 2004, from http://www.getnetwise.org/glossary.php

[11] Rosenberg, M. J. (2001). e-Learning. New York: McGraw-Hill.

[12] Hill, J. R., Wiley, D., Nelson, L. M., & Han, S. (2004). Exploring research on internet-based learning: From infrastructure to interactions. In Jonassen, D. H. (Ed.), *Handbook of research on educational communications and technology* (2nd ed.). New York: Simon and Schuster/Macmillan.

[13] Piña, A. A., & Eggers, M. R. (2006). *Teaching, administering and supporting blackboard, webct and desire2learn*. Paper presented at the annual Technology in Education (TechEd) Conference, Pasadena, CA

[14] Ioannou, A., & Hannafin, R. (2008). Deficiencies of course management systems: Do students care? Quarterly Review of Distance Education, 9(4).

[15] Stewart, B. (2007). Why Athabasca chose moodle. *Distance Education Report, 11*(3). Changing Course

Management Systems: Lessons Learned Changing Course Management Systems: Lessons LearnedChanging.

[16] Driscoll, M. P. (2007). Psychological theories of instructional design. In Reiser, R. A., & Dempsey, J. V. (Eds.), *Trends and issues in instructional design and technology* (2nd ed.). Upper Saddle River, NJ: Pearson Merrill/Prentice-Hall.

[17] W. Xu, S. Bhatkar, R. Sekar, "Practical dynamic taint analysis for countering input validation attacks on web applications", Technical Report SECLAB-05-04, Department of Computer Science, Stony Brook University, 2005.

[18] *OWASP Top Ten Project* [Online Report], Open Web Application Security Project - the open application security community, 2004, Retrieved January 25 2008, URL: http://www.owasp.org/index.php/Top_10_2004

[19] *OWASP Top Ten Project* [Online Report], Open Web Application Security Project - the open application security community, 2007, Retrieved January 25 2008, URL: http://www.owasp.org/index.php/Top_10_2007

[20] D. Moore, C. Shannon, D. Brown, G. M. Voelker, S. Savage, "Inferring Internet Denial-of-Service Activity", *ACM Transactions on Computer Systems (TOCS)*, Vol. 24, No. 2, p. 115 – 139, 2006.

[21] C. Cowan, P. Wagle, C. Pu, S. Beattie, J. Walpole, "Buffer overflows: attacks and defenses for the vulnerability of the decade", *Foundations of Intrusion Tolerant Systems*, p. 227 - 237, 2003.

[22] N. Jovanovic, E. Kirda, C. Kruegel, "Preventing Cross Site Request Forgery Attacks", *IEEE Securecomm and Workshops*, p. 1 – 10, 2006.

[23] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis", *Proceedings of the Network and Distributed System Security Symposium*, 2007.

[24] G. Ollmann, "Writing secure code", *Network Security*, Vol. 2007, No. 5, p. 16 – 20, 2007.

[25] Siemens, G. (2004). Learning management systems: The wrong place to start learning. Retrieved May 4, 2009, from http://www.elearnspace.org/ Articles/lms.htm

[26] Lane, L. M. (2008). Toolbox or trap? Course management systems and pedagogy.*EDUCAUSE Quarterly*, *31*(2).

[27] Piña, A. A., Green, S., & Eggers, M. R. (2008). Learning management systems: Lessons from the front lines. Paper presented at the annual Technology in Education (TechEd) Conference, Ontario, CA.