Information Security in Learning Management Systems

Inuwa Danjuma Usaini

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the Degree of

Master of Science
in
Information and Communication Technologies in Education

Eastern Mediterranean University
July, 2014
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research.

Prof. Dr. Elvan Yılmaz
Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Master of Science in Information and Communication Technologies in Education.

Assoc. Prof. Dr. Ersun İşçioğlu
Chair, Department of Information Communication and Technologies in Education

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Information Communication and Technologies in Education.

Assoc. Prof. Dr. Ali Hakan Ulusoy
Co-Supervisor

Asst. Prof. Dr. Emre Özen
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Ersun İşçioğlu _____

2. Assoc. Prof. Dr. Ahmet Rizaner _____

3. Asst. Prof. Dr. Emre Özen _____

ABSTRACT

Since 1960s the internet has grown to become a worldwide and borderless domain where many people share information from different parts of the world. In learning environment, different Learning Management Systems (LMSs) can be used to perform academic tasks as a way of e-learning.

This thesis focuses three most common Open Source Learning Management Systems (OSLMSs), Atutor, Ilias and Moodle to analyze their security vulnerabilities based on information security triad which covers Confidentiality, Integrity and Availability (CIA).

The study includes the discussion about LMSs, how secure they are, and how to test them. The study follows two ways as physical observation and logical test (scanner as a tool) to analyze LMSs. Some common drawbacks are noticed for all selected LMSs on physical observations. However logical tests performed by Nikto scanner that is analyzed based on S-OSVDB impacts show that Atutor has less vulnerabilities than the others.

The techniques used to tests three LMSs in this thesis do not only help the learning environment to select the most secure LMS, but also help LMSs developers and users to point out the vulnerabilities of the LMSs.

Keywords: Security issues in OSLMS, Nikto, OSVDB, S-OSVDB.

ÖZ

1960 yılından bu yana internetin büyüyüp gelişmesi ve sınırsız bir bilgi alanı halini almasıyla, dünyanın değişik bölgelerindeki insanlar bilgiyi paylaşır hale gelmişlerdir. Eğitim alanında ise internet Öğrenme Yönetim Sistemleri (ÖYS'leri) yardımı ile eğitim faaliyetlerinin uzaktan eğitim (e-eğitim) şeklinde sürdürülmesine olanak sağlamıştır.

Bu tez çalışmasında en yaygın olarak kullanılan açık kaynak kodlu ÖYS'lerden Atutor, Ilias ve Moodle ele alınmış ve bilgi güvenliği gizlilik, bütünlük ve ulaşılabilirlik açısından incelenmiştir.

Çalışmanın kapsamında en uygun ÖYS'ni seçebilmek için ÖYS'nin tanımı, ne kadar güvenli olduğu ve güvenlik testlerinin nasıl yapılacağı incelenmiştir. ÖYS'nin güvenlik incelemeleri fiziksel gözlem ve tarayıcı program yardımı ile gerçekleştirilmiştir. Fiziksel gözlemler sırasında ortak bazı problemler tespit edilmiş olmakla birlikte, Nikto tarayıcı programı ile yapılan testler sonucunda S-OSVDB etkenlerine dayanarak incelenmiş olan ÖYS'lerden Atutor en güvenli ÖYS olarak tespit edilmiştir.

Bu çalışmada ÖYS'leri test etmekte uygulanan yöntemler sadece eğitim kurumlarının en uygun ÖYS'yi seçmelerine değil ayni zamanda ÖYS geliştiricilerine ve kullanıcılarına yaşanan güvenlik zaaflarının duyurulması açısından da yardımcı olacaktır.

Anahtar Kelimeler: Açık kaynak kodlu ÖYS'lerde güvenlik konuları, Nikto, OSVDB, S-OSVDB.

DEDICATION

I would like to dedicate this study to my father, who died September, 2003 (may his soul rest in peace), my mom Hajiya Fatima and my lovely brother Assoc. Prof. Dr. Danbala Danju as a sign of their importance in this study and in my life.

ACKNOWLEDGEMENT

It is the best time to thank to my supervisors Assoc. Prof. Dr. Ali Hakan Ulusoy and Asst. Prof. Dr. Emre Özen for their continuous support and assistance during this study. They are not only supervisors for me but also guidance counselors. I really appreciate their concerns and all they have done for me.

I am obliged a lot to my family especially my mom, my lovely brothers especially Assoc. Prof. Dr. Danbala Danju and his family (Ipek Danju, Ahmed Danju), and Dr. Salisu who allowed me to travel all the way from Nigeria to Turkish Republic of Northern Cyprus and provided me with all supports not only in my studies also in my life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CIA	Confidentiality, Integrity and Availability
ILIAS	Integriertes Lern-, Informations- und Arbeitskooperations-System
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization (ISO) and by the International Electrotechnical Commission
LAN	Local Area Network
LCMS	Learning Contents Management System
LMS	Learning Management System
MOODLE	Modular Object-Oriented Dynamic Learning Environment
OSLMS	Open Source Learning Management System
OSVDB	Open Source Vulnerability Data Base
RDBMS	Relational Database Management System
S-OSVDB	Seven - Open Source Vulnerability Data Base
SQL	Structured Query Language
VLE	Virtual Learning Environment
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines
XAMPP	X (“cross”-platform), Apache HTTP Server, MySQL, PHP and Perl
XSS	Cross Site Scripting

Chapter 1

INTRODUCTION

This chapter presents a brief introduction of the learning environment, information security, Learning Management Systems (LMSs) and aspect of information security in education. The chapter also includes the purpose of the thesis, the questions to be answered, boundaries of the study, the importance of the thesis and outline of the thesis.

1.1 A Brief Introduction of Learning Environment

The learning environment can be described in a variety of ways. Learning environment can be defined as the physical surroundings inside which learning takes place, such as way in to library facilities, seminar places or simulation equipment. Conceptually speaking, the learning environment refers to the whole range of components and activities within which learning happens. In addition to this, it is technically speaking, a learning environment relies on computer-supported systems such as a learning management system, a combination of various learning technologies (including at least one communication module), virtual environments, and web 2.0 [1].

This means that teachers put materials into the information store and students retrieve it. It is suggested that the learning environment may affect students' approach to learning that eventually will influence their learning consequence. Thus, to improve the learning outcomes, the learning environment should be concerned

about the context and skills within the context of student learning. In addition to this, learning environment is seen as the quality of teaching and learning context in which it occurs [2]. Learning environment is abstracted as the psychological, pedagogical, and social context in which learning occurs that shape the attitude and learning behavior of the student [3]. Learning environment uses internet technology through different internet service providers which enable communication between institutions and outsiders, students, academic and non-academic staff.

1.2 Learning Management Systems (LMSs)

LMS sometimes called Virtual Learning Environment (VLE), contents management systems or learning platform, is an e-learning teaching and learning system based on the web that simulations conventional in-person schooling through providing equal computer-generated right to use in courses, discussion content, examinations, schoolwork, scores, evaluations, and extra external resources for instance learning website links [4].

LMS allows learning environment to improve electronic learning resources designed for students, to bargain these developments electronically to learners, to check as well as assess the learners electronically, and to produce electronically learners databases in which learner consequences as well as development can remain monitored.

Colleges and universities use LMSs to deliver online courses and augment on-campus courses. Corporate training departments use LMSs to deliver online training, as well as automate record-keeping and employee registration. LMS is the foremost software of the e-learning solutions that automates the administration of training

events. LMS ranges from systems for handling training and learning records to software for distributing online courses over the internet with features for online collaboration [4]. Thoroughly, LMS manages the log-in of registered users; handles course catalogs, tracks students' activities and results, and presents reports to management. A LMS may not include additional functions such as authoring of content, management of classroom training, instructors and resources, and learners collaboration tools [5].

Presently, there are hundreds of vendors of LMS providers lively in the marketplace. Discovering them, notifying their differences and similarities as well as selecting them is actually a big challenge [6].

Itmazi et al. in [7] mentions the reasons why LMSs are used as followings:

- Track student registration (access and progress).
- Manage courses and programs.
- Enable financial tracking and control of learning.
- Provide course scheduling and administration.
- Provide an administer course registration.
- Manage learning administration and reporting.

1.2.1 Classification of Learning Management Systems

There are two types of LMSs: free and commercial. This is classically the major concern that organizations face while selecting LMSs.

1.2.1.1 Open Source LMS

Open source or free LMS is an LMS which is dispersed free of charge. It is good for learning environment to have a good internal technician staff that can take the responsibility of operation and supervision of the application package.

Many of free LMSs application software providers do not deliver supports for their software. Certain delivers support as well as services based on charges, while others have free support but through community forums. Most of the unpaid LMSs are open source code, which provides you a liberty to modify or alter the software by yourself in whichever method you require.

Open Source LMSs (OSLMSs) have an attractive advantage. Their source code is available. For the reason that the source code is open, it can remain changed on the way to be extremely customizable designed for each organization. On the other hand, most OSLMS products have a tendency to remain more difficult than profitable products - classically they remain utilized by means of more sophisticated manipulators. Additional, without a dependable "support" system in place, creation smooth minor variations can remain hard in place of a junior programmer - support generally takes the procedure of connected forums. There are many OSLMSs. Moodle, Atutor, Sakai and Ilias are examples of OSLMS vendors.

1.2.1.2 Commercial LMS

Commercial LMS is dispersed on paid basis. Most of the time, the amount in lieu of the package consist of technical support that makes the application package easy to install and use especially for non-technicians. Sellers actually do not deliver source code for profitable packages, however sometimes they deliver customization facilities.

As it is mentioned, it financially costs money. Amongst these marketable LMSs producers, there are typically two foremost forms. One is the complete package, which is the complete software package so that the user can install it directly on the server. The other is service-based cloud option. For this type of LMS, the complete

application is not given to the user instead the software is on cloud (on the server) so that whenever the organization pays the subscription, they can access LMS through network. There are many commercial LMSs. Some examples of commercial LMS vendors consist of JoomaLMS, Blackboard, Mcgraw, Litmos LMS and Absorb LMS.

For the study of this thesis, Atutor, Ilias and Moodle (Modular Object-Oriented Dynamic Learning Environment) are discussed to find their vulnerabilities. Reasons for choosing these LMSs are presented in chapter two that discusses literature reviews.

1.3 The Definition of Information Security

Many researchers define information security in different ways. Whitman and Mattord in [8] define information security as the environment to be guarded or make it away from danger. In addition to this, these authors acknowledge information security as the most important from the numerous layers of security required compared to others such as physical, personnel, operational, communications and network securities.

In addition, Andress in [9] describes information security by means of defensive evidence and information systems from unsanctioned right to use, interruption, alteration as well as demolition. These researchers did not mention the significant characteristics of information security. However, Whitman and Mattord in [8] pointed out four characteristics of information security as confidentiality, integrity, utility as well as possession by means of the dangerous matters of the information security. On the other hand, Andress recommends what he called Parkerian Hexad,

that incorporate three characteristics of information security which covers confidentiality, integrity as well as availability that is known as CIA triangle [9].

Based on the above identification, information security can be defined as protecting information, data and computer systems from attackers in order to ensure confidentiality, availability and integrity. The International Association of Privacy Professionals in [10] defines privacy by means of saving individual facts secret at any time and everywhere whenever required.

Solms and Niekerk in [4] mentioned three characteristics of information security as confidentiality, integrity as well as availability of information. In addition to this, information can be in many different forms. It can be written on any material such as paper. It can also be kept in electronic store such as server, computer. And it can also be shared through hardware such as by post of hard copy or software for instance electronic post (e-mail), in addition, it can be showed by films as well. Whitman and Mattord in [8] define information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information".

Whereas learning environment has a duty to keep private information confidential. These issues are all concerned based on right to use information by the authorized users. Besides there are some general policies based on general standards such as international standards which gives directions based on how to protect information in order to ensure CIA are not violated.

Discussion about ISO series related to information security is presented in chapter two. In this study, the CIA triangle definition of information security based on the Andress, Solms and Niekerk definition is going to be applied to LMSs, particularly Atutor, Ilias and Moodle [4, 9].

CIA which stands for confidentiality of information, integrity of information and availability of information [11] can be explained as follows:

Confidentiality: Whenever information is send from source to destination, the information should be unknown to anyone else except the recipient [14]. This is called confidentiality. The user's web circulation as well as data must be kept confidential in transfer - specifically, secure from illegal right to use.

Integrity: Integrity remains damaged if an illegal manipulator implements, adapt, hangs, copies, reiterations, or interruptions data, messages, or assets. This means that integrity is when information is send from one person to another, the information remains intact and unchanged.

Availability: Availability is scarce whenever the server or service remains spoofed, breached, or suspended as well as cannot function as normal [15].

1.4 The Aspects of Information Security in Education

Since 1960s the internet has grown to become a world – girding, borderless domain where many people share information from different parts of the world. According to 2008 survey published by EDUCAUSE, information technology security is the top strategic problem for information technology departments at learning environment [12].

Information systems in learning environment can be considered more difficult than the old-style information systems reprocessed within commercial organizations. More details will be discussed though the thesis about information security in general focused on standard ISO 2700x series which is based on information security standard. Learning environment uses learning management systems for their academic activities. Based on information security triad which covers CIA, the study in this thesis will be answering to the questions of how secure are LMSs, how can learning environment choose better LMS for their academic activities?

1.5 Purpose of the Study

The aim of the thesis is to discuss generally the security risks about the LMSs and tests Atutor, Ilias and Moodle as a sample of OSLMSs in terms of information security triad which cover integrity, availability and confidentiality. The outputs of the thesis will guide the learning environment as a point of reference used for dealing with safeties of LMSs.

1.6 The Research Question

The research questions discussed in this study are:

1. How secure is an OSLMS?
2. How security vulnerabilities of an OSLMS are tested?
3. What are vulnerabilities and risks for an OSLMS?
4. What are the proposed solutions to vulnerabilities and risks for an OSLMS?

1.7 Delimitations of the Study

The delimitations of this study are as follows:

- This study will not go through the details about farewell, server, network, systems structures as well as their insinuations on security.

- This study will not examine management of learning environment's weaknesses on security.
- The study will focus on the standard versions of LMSs and will not include any analysis related to their plug-ins.

1.8 Significance of the Study

Information security is a serious matter in place of learning environment [6]. Many problems arise in the learning environment such as online examination, impersonation, cheating during online exams, and breach of learning environment data. This study will enlighten the learning environment and information security policy makers about the weaknesses of LMSs. The greatness of those risks will support the developers of the LMSs, policy makers as well as information management of the learning environment to decide how to deal with those risks.

1.9 Thesis Outline

The rest of the thesis is organized as follows. In chapter two, the literature review which forms the theoretical basis about the information security standard, information security policy as international benchmark, information security requirements for learning environment, risk management in learning environment and LMSs is presented. In chapter three, the methodology used in the study is presented. The results of the tests, the findings and proposed solutions are discussed in chapter four. Finally the conclusions as well as future research are presented in chapter five.

Chapter 2

LITERATURE REVIEW

In chapter two, three concepts of information security are introduced. Initially, the information security in general as international benchmark is discussed. Then the discussion about information security in learning environment is presented. In this concept security risks in learning environment such as colleges and universities are discussed. Then the discussions about information security in LMSs are presented. In this section, particularly Atutor, Ilias and Moodle as OSLMSs are discussed. Finally the discussions about the history of selected OSLMSs and the reasons for choosing them as the research field are presented.

2.1 Information Security in General

Without general standards that direct, observe, control, manage and provide the general criteria for information security, the information security general practitioners will wrongly setup the information security based on bias, inexperience, inappropriate confidence as well as individual reasons [13].

Communication within learning environment either between employees and students or between organizations needs to be secure and confidence. Security incident is the breaching security objectives of maintaining availability, confidentiality, integrity or altogether.

Information security policies ensure confidentiality, integrity and availability of an learning environment's asset. Information data and IT services should be protected. Learning environment's security objectives will be met when information is available and useful whenever needed. In addition, the systems which provide the information can recover the data in case of failure.

Applying and maintaining security policies such ISO/IEC can help the learning environment to be protected from any security risks.

ISO series is an information security standard issued through the International Organization for Standardization (ISO), which is entitled information technology – security techniques – code of practice for information security management.

Table 2.1 below summarizes the ISO 27001, 27002, 27003, 27004 and 27005 standard series [16].

Table 2.1: ISO standards about information security.

ISO/IEC STARNDARD	ISO DESCRIPTION	ISO OBJECTIVE
ISO/27001	It is for an Information Security Management System (ISMS).	Provides the necessary requirements used for creating, applying, maintaining as well as constantly developing an ISMS.
ISO/ 27002	The standard is intended to address the specific requirements identified via a formal risk assessment.	Documents guiding principle as well as overall codes intended in lieu of starting, applying, maintaining, and improving information security management in the interior of an organization. In addition, it provides a general guide intended for the improvement of managerial security standards as well as operational security management performs.
ISO/ 27003	It is responsible for	Focus on the Plan-Do–Check–Act

	providing help as well as general guidance while applying ISMS.	(PDCA) technique, with admiration towards the founding, applying rereading as well as refining the ISMS.
ISO/27004	It is responsible for direction on the expansion as well as practice of events and dimension used to estimate the efficiency of applied ISMS, as indicated in standard ISO 27001.	It is envisioned to assist an organization to produce the success of its ISMS proposal, implementation as well as management targeting surrounded by the PDCA series.
ISO 27005	It is all about information security risk management.	Mentions guiding principles used for information security risk management in an administrative organization, precisely supportive to the necessary desires of an ISMS mentioned in standard ISO 27001.

2.2 Security Problems in the Learning Environment

Information security in learning environment is the corporate outline of general principles, guidelines, administrative arrangement as well as operational settings used to safeguard confidentiality, integrity and availability in learning environment. With the advanced reasonable environment around the globe, learning environments are not paying more attention to provide the greatest learning experience. As the consequence of information systems technological improvement, the number of records stored in educational environment database increased rapidly [17].

According to White Hat website security statistics report in 2011 [18] *"Most websites were exposed to at least one serious vulnerability every day of 2010, or nearly so (9–12 months of the year). Only 16% of websites were vulnerable less than 30 days of the year overall." a*nd *"71% of Education...".*

For these reasons there is need of implementation of information security in learning environment in order to protect the freedom of both staff and students in academic environment. Colleges and universities collect information from both students and staff and keep it for the academic as well as financial purposes. Both staff and students are very reliant on information and information technology schemes, particularly e-mail as well as the internet, to make their day to day activities for staffs to perform their works and for students to study successfully. Though, learning environment faces number of threats which includes stealing of hardware, international attacks on data by staffs, student or outside hackers. A human disaster which is caused by human error is also another example of threat in learning environment, and finally natural disaster such as flood, explosion as well as fire.

The outcomes of these threats can be stated as the followings:

- Interruption to learning environment service,
- Loss of community as well as scholars confidence in learning environment,
- Punishment in addition to/or illegal reports as a consequence of illegal right to use, revelation of mismanagement of the systems.

2.3 Security Problems in Learning Management Systems

E-learning is actually delivered through an LMS such as OSLMS that is a software platform which delivers internet-based courses and presents assistance for safety [19]. In most of the cases, instructors use an LMS to deliver web-based course notes and other material, in addition to connect with learners and also to track learner's course activities and evaluate learner's performance. In addition, learners use LMS for learning, downloading course materials, sending and receiving messages and checking announcements. Nowadays, lots of money is spent on LMS specifically for

teaching and learning in government or private or both organizations. According to Mallon and Clarey study in 2012, 1.8 to 1.9 billion dollars would remain paid out worldwide on LMS marketplace in 2013 [20].

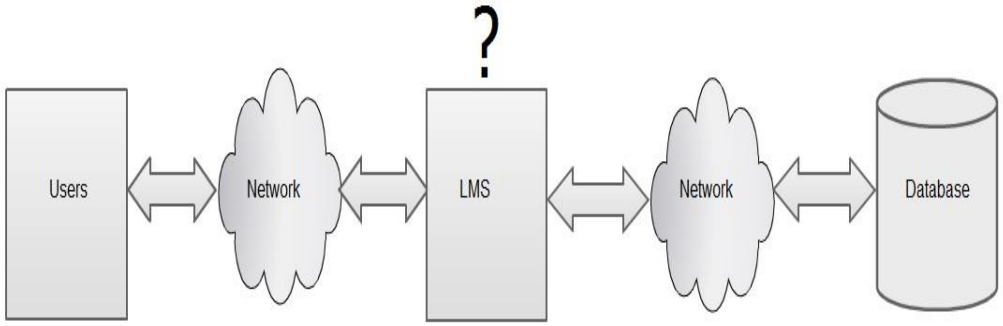

Figure 2.1: How secure is an LMS?

As can be seen from Figure 2.1, an LMS user needs to login into LMS through network access. On the other hand, LMSs' database that can be accepted as the learning environment is also located on the network. Since LMS is the intermediate between learning environment and the users, the security of LMS has to be guaranteed.

There are many studies conducted in LMS security especially on OSLMS. Kumar and Dutta in [21] investigated the security on Moodle based on authentication, availability, confidentiality and integrity attacks. They found that the highest vulnerabilities are in integrity which consists of six vulnerabilities. Confidentiality has three vulnerabilities while there are two vulnerabilities in authentication and only one vulnerability in availability found [21]. The study is conducted through observation.

Floyd et al. in 2012 used three virtual machines and a production server to test the vulnerabilities on Moodle version 2.1. The results showed that there are five weaknesses on Moodle version 2.1. Those are session hijacking, cookie best practices, XSS injection, session management flaw and quiz engine flaw [22]. This study is not on information security characteristics which are compromised CIA.

In [23] Netsparker web application vulnerability scanner was used and tested four different LMSs which includes Atutor, Moodle, Efront and Commsy. The findings revealed that Commsy has more vulnerabilities compared to others. The vulnerabilities of Commsy include XSS, SQLi and info over http. Atutor has two vulnerabilities which include XSS and info over http. Both Efront and Moodle have one vulnerability which is info over http. There are two weaknesses of this study. The study did not discussed about the physical observations of these LMSs such as CAPTCHA that can cause the brute-force attack on the server, and the study is not conducted based on CIA. An additional study was conducted in [24], where four LMSs, Atutor, Ilias, Moodle and Sakai were compared based on software quality characteristics using DeLone and McLean Information System Success Model that is presented in Figure 2.2.

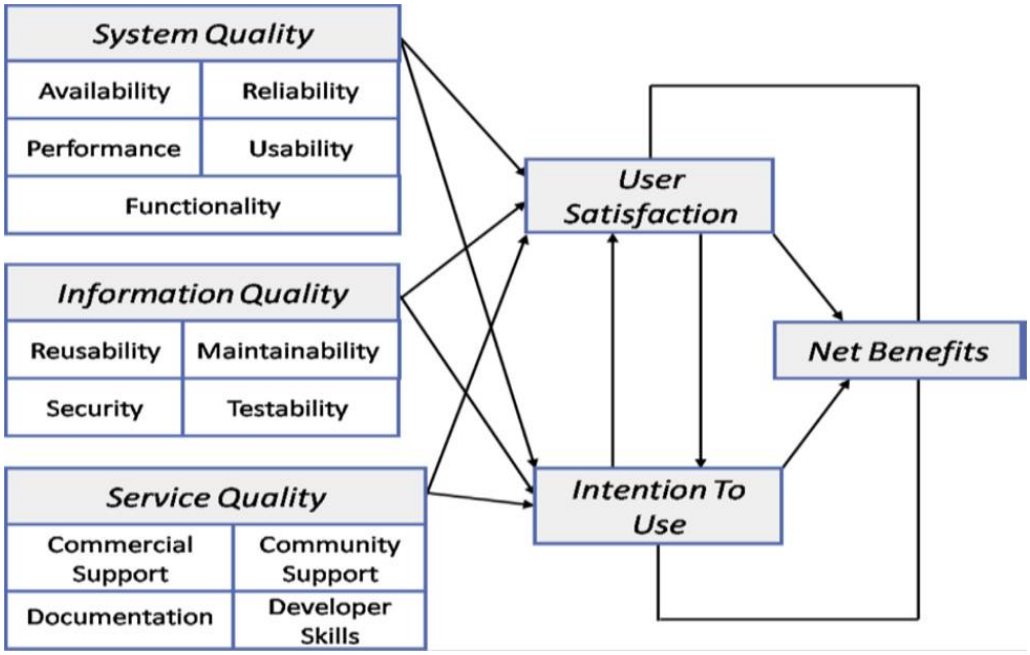

Figure 2.2: DeLone and McLean Information System Success Model [24].

Table 2.2 Summary of findings based on DeLone and McLean Information System Success Model [24]

LMS Tools	Systems Quality Average	Information Quality Average	Service Quality Average
Atutor	3.8	2.2	2.0
Ilias	3	3.0	1.4
Moodle	4.8	2.8	2.6
Sakai	3.6	2.4	1.8

The study classified LMSs based on scale ranking zero to five, where five is the highest ranking based on excellent and zero is very poor. To summarize the results, total scores of each LMS were calculated and the average results were presented as in the Table 2.2.

The above mentioned studies did not follow the analysis based on information security triad which covers confidentiality integrity and availability. In addition, if learning environment wants to use LMS there is no standard way to test the vulnerability of it in order to choose the best one. In this thesis, the methodology

used to test three selected LMSs in chapter three can be used to test any LMSs so that the learning environment can use it to choose the suitable LMS for their academic duties. Through the discussion it is shown how the tests of Atutor, Ilias and Moodle can be performed to find out the vulnerabilities through applying the CIA.

2.4 LMSs in the Learning Environment

The idea of free software as well as code sharing started since 1990's but the open source initiative was established in 1998 [25].

In this study, Atutor, Ilias and Moodle are selected to test their vulnerabilities because they are the most commonly used OSLMSs in learning environment to perform academic duties. The reason of common use of these LMSs comes from the fact that they are cross-platforms which can be used without alteration on whichever system or server that supports PHP, Windows as well as UNIX. They can also be used with PostgreSQL, Oracle and MySQL RDBMSs.

2.4.1 Atutor

Atutor is a free OSLMS, which is used to develop online courses as well as create e-learning content. It was originally developed by Greg Gay at the University of Toronto in Canada and released in 2002. It is now maintained by the Inclusive Design Research Centre at the Ontario College of Art & Design University [26, 27].

Atutor is the first Learning Contents Managements System (LCMS) to fulfill the accessibility specifications of completely World Wide Web Consortium (W3C), Web Content Accessibility Guidelines (WCAG) 1.0 at the AA+ level, allowing the access to all the comprised content of the system at completely levels of user privilege [27]. In addition, developers state that it is the only fully accessible LCMS software on the

marketplace. Moreover, there are four main reasons that impress the users of Atutor: themes, privileges, tool modules, and groups. The theme design lets the users to simply customize the face layout of the software based on their needs. Users can combine multiple versions into single system so that other users can choose any one they want from the preference setting. The privilege system lets the teachers to allocate tool controlling privilege to specific memberships of the course. The latest versions 2.1.1 released on March 14, 2013. It is also cited in many technical appraisals as well as scholarly articles worldwide.

Atutor is being used as the standard LMS by foremost colleges, universities and learning institutes around the world. Granite University uses Atutor for teaching and learning in the university [28]. Similarly Weston University College uses Atutor for assistive technology and other accessibility features [29].

2.4.2 Ilias

Ilias abbreviation is from German that represents IntegriertesLern-, Informations- und Arbeitsko operations-System. That is Integrated Learning, Information and Work Cooperation System in English [24]. Ilias is an LMS which is used in various concepts such as desktop and repository. It also supports LCMS.

The first inventive of Ilias [27] was established by the end of 1997 within the VIRTUS project at University of Cologne. By November 2, 1998 first version of Ilias was distributed and available for learning purposes at the Cologne Faculty of Business Administration, Economics and Social Sciences. Because of increasing interest of additional colleges and universities worldwide, the project squad decided to distribute Ilias as an open source software based on the General Public Licensed

(GPL) in 2000. By the year 2002 and 2004, a new version of Ilias was established and it was called “Ilias 3”. In the year 2004 Ilias turned out to be an OSLMS [31].

Ilias was used not only in learning environment but also in defense and security organizations. It is a protected OSLMS that has been qualified by NATO and is accepted to be used in NATO’s high security intranet. In addition to this, Ilias strongly respects standards and remains the first OSLMS that has been certified as SCORM 1.2 and SCORM 2004 compliant [31].

2.4.3 Moodle

Modular Object Oriented Dynamic Learning Environment (Moodle) is a free OSLMS, which is developed by Martin Dougiamas. It is open source and a community develops it from this point on. It is designed to help educators to create interactive online courses. Moodle is one of the most user friendly LMS. It has become very popular with over fifty thousand registered site, thirty million users, and more than three million courses. It is used in more than two hundred countries and it is translated in seventy five different languages [32].

In terms of functionality, it includes authentication, enrollment, quiz, content packaging, and course import/export. Moodle runs in cross-platform operating systems which support PHP and RDBMS that are offered by most internet service providers.

The first version of Moodle was released on 20th August, 2002. Since first released version, it has been continually updated by a widespread list of experts who have contributed to the development of its many stages. The latest version which this study conducted is version 2.6.1, released on 5th March, 2014.

According to Moodle statistics report on 18th April, 2014. There are about 85,388 registered sites with Moodle. Roughly 240 different countries use Moodle. In terms of courses, there are 8,239,374 courses registered to Moodle on different server platforms. There are about 76,784,625 active users in the Moodle worldwide. In addition, 1,167,903 active teachers currently use the Moodle worldwide as LMS. The number of users who are enrolled to the courses on Moodle is about 122,808,089. 138,859,710 forums post presently the Moodle worldwide. In terms of teaching and learning materials, there are 72,554,091 different materials on the Moodle. Finally, there are 234,071,516 quiz questions in the Moodle worldwide [33].

Moodle is available in a diversity of download packages through different stages of constancy from the official Moodle web site http://download.moodle.org. The following are the most important reasons for choosing Moodle in the research:

Moodle is selected because it is worldwide used almost in all of the colleges and universities [34]. Eastern Mediterranean University uses Moodle in some faculties for educational purposes for a while [35]. In Brazil, Escola Técnica da Universidade Federal do Rio Grande do Sul uses Moodle since 2004 [36]. Athabasca University that is located at Canada is the only Canada's leading distance-education and online university, as well as Canada's Open University, portion approximately 30,000 scholars in each year. The university uses Moodle as well, to deliver courses and other learning activities [37]. Furthermore, in South Africa, Rhodes University in Graham's town uses Moodle as its official LMS. It presently has over 10,000 active students, together with more than 550 instructors in their Moodle's database [38]. Similarly in the United Kingdom, the Open University which is the only university devoted to distance education since October 2010 contains more than 700,000 users

as well as 7,000 online courses on its Moodle database [39]. Sukhothai Thammathirat Open University changes their LMS from Atutor to Moodle from the year 2012 for the purposes to upsurge the variety of the university's curriculum [30]. Based on these above examples, Moodle can be considered as one of the most common LMS used by the universities.

Based on the aforementioned reasons, Atutor, Ilias and Moodle deserve to represent OSLMS to be the area of research in this study.

Chapter 3

METHODOLOGY

In chapter three, firstly the discussion about the research method that is carried in this thesis is mentioned. Physical observation on selected three OSLMSs Atutor, Ilias and Moodle are discussed. Logical test is the final section in this chapter, which states how the data is collected based on penetration tests. This section covers the data collection methodologies, the tools that are used to collect the data and their functions. Then finally explains qualitative data analysis through contents analysis.

3.1 Research Method

The research methodology used in this thesis is qualitative research. Qualitative research is all-purpose words that bring up the collections of approaches and methods of gathering and evaluating the data that are clearly different from quantitative or mixed-method research because of the lack of quantification and statistical study [40]. There is no standard or straightforward way to choose the methodology. Research is named as qualitative whenever the aim of that study is to explain things through explanation of quality instead of presenting things through how much quantity [41]. Nikto scanner which is used to analyze Atutor, Ilias and Moodle in this research creates outputs that are presented as qualitative results. That is why the selected methodology is referred as qualitative research.

3.2 Physical Observations on OSLMSs

Amongst countless selections in LMSs, Atutor, Ilias and Moodle are the most widespread LMSs chosen. These LMSs are used not only in learning environments such as colleges and universities but also in some companies, and home educators for teaching and learning purposes [42, 43].

Here is the discussion of vulnerabilities as the physical observations on three selected OSLMSs Atutor, Ilias and Moodle.

Teachers can use LMSs to conduct online exams. However by observing the physical appearances on the standard versions of these three LMSs there is no setting for video chat. The lack of video chat on these LMSs can enable the impersonation during online exams. However this weakness can be overcome by adding video chat plug-ins.

As another weakness during the login process the lack of CAPTCHA has been observed. CAPTCHA is PHP design code using collection of graphics to generate CAPTCHA image [21]. Figure 3.1, which is the login page of Bamboo shows the importance of CAPTCHA during the login. If the user puts different word(s) to the provided field then the generated word(s), even if the login details are correct such as username and password, the messages appear to warn the user about the wrong words generated and login fails.

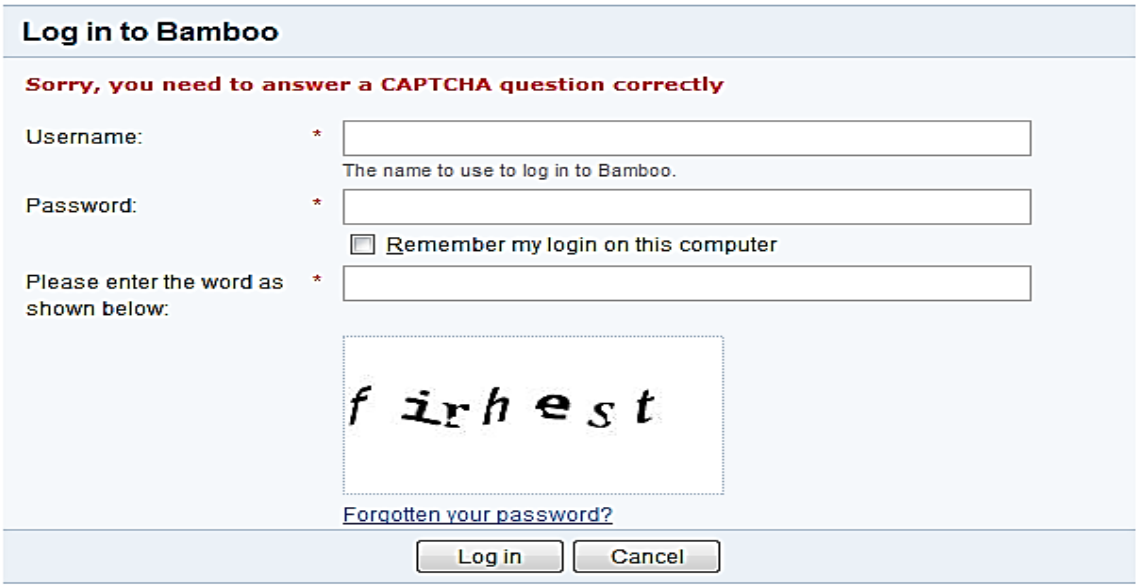

Figure 3.1: Login with CAPTCHA in [44].

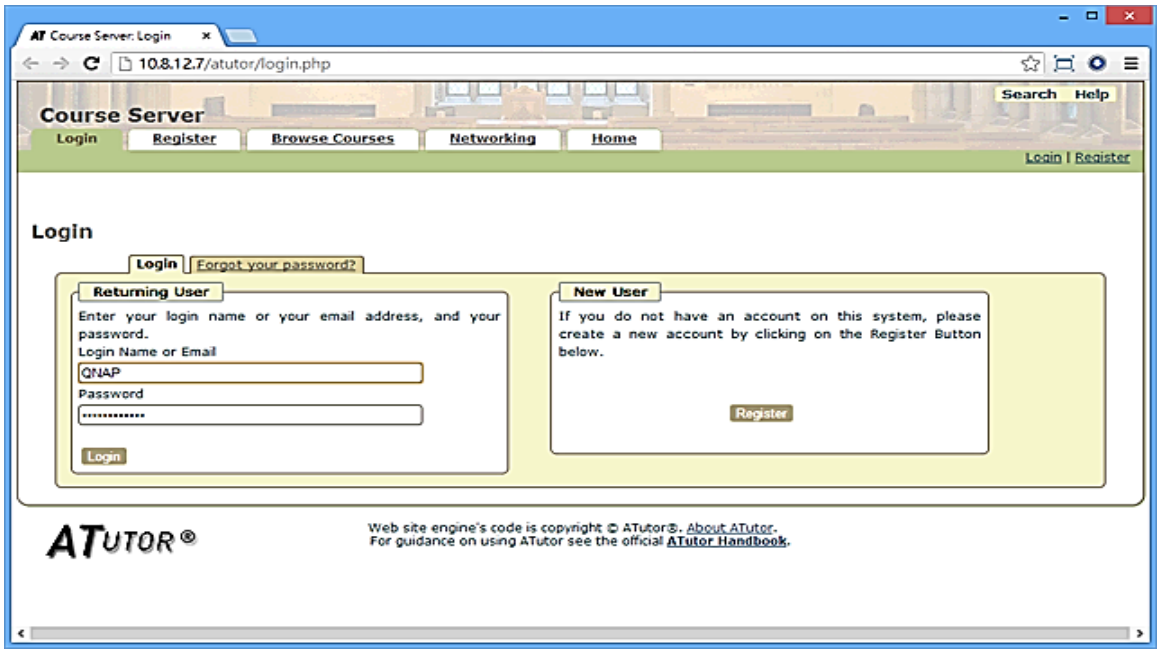

Figure 3.2: Atutor login page.

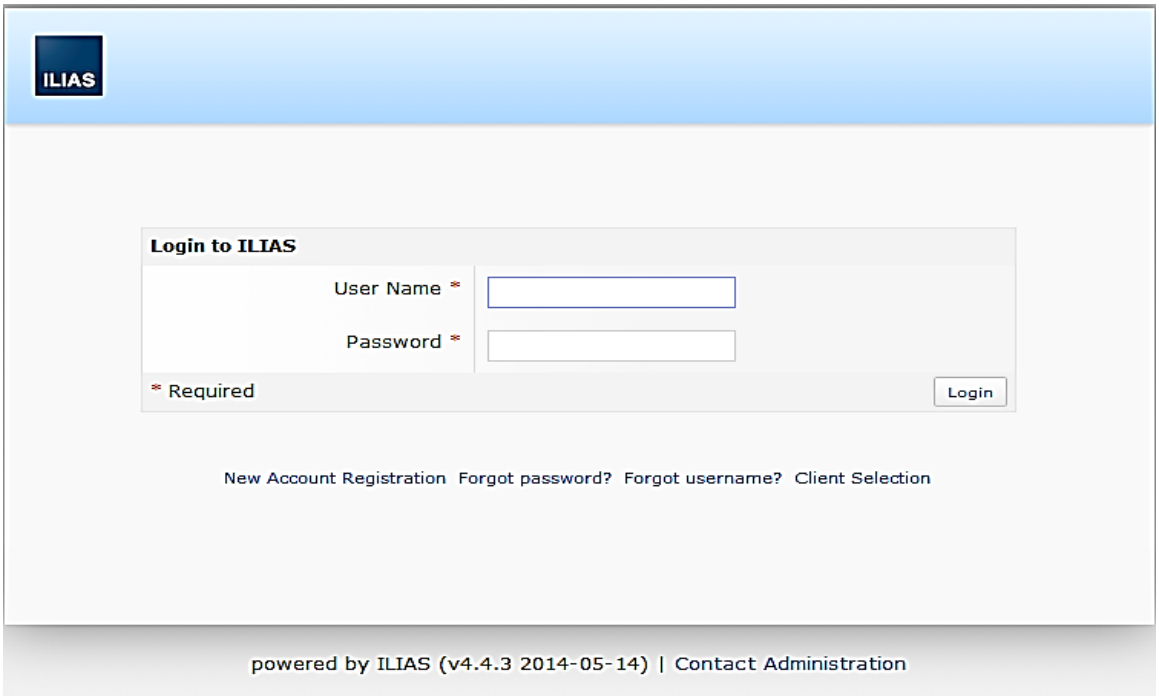

Figure 3.3: Ilias login page.

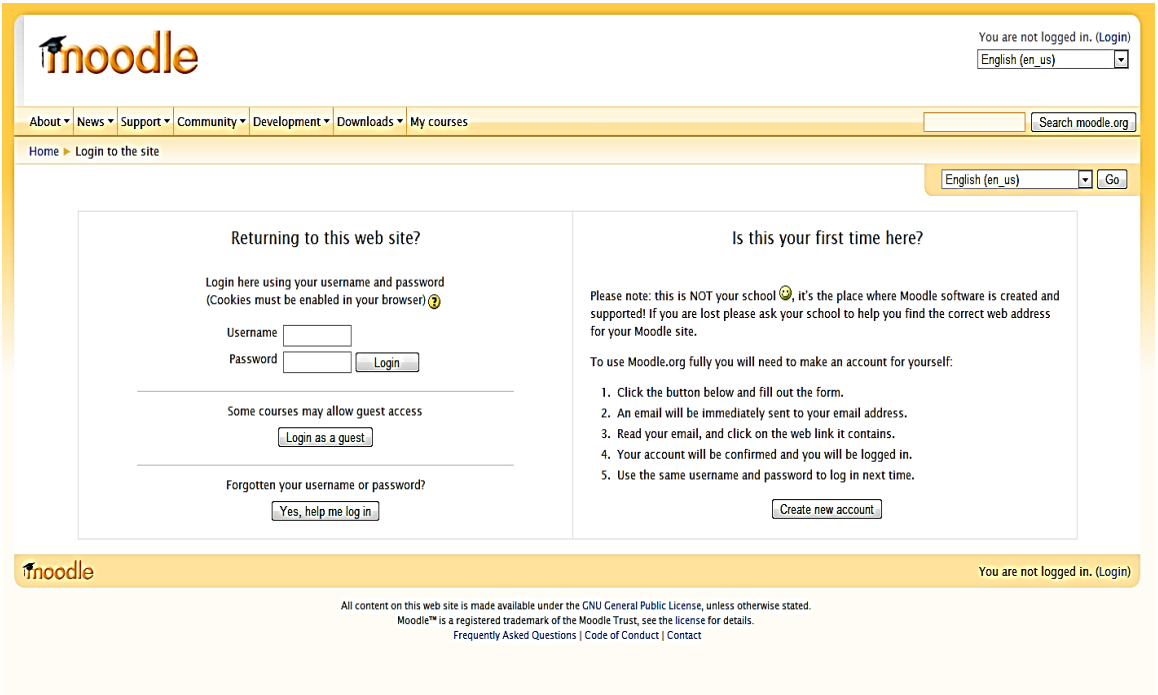

Figure 3.4: Moodle login page.

As it can be seen from the screenshots of Atutor, Ilias and Moodle presented in Figures 3.2-3.4, there is no CAPTCHA implemented on their login pages. When a user attempts to login to Atutor, Ilias and Moodle, there is possibility of brute force

attack that occurs on these LMS's server. If CAPTCHA is implemented, it will generate some random graphics values on the login page that permits the user to put those random generated values in the text area provided on the login page at any time when the user wants to login.

3.3 Logical Test

This section will explain how vulnerabilities of an OSLMS are tested and the tests of three selected LMSs, Atutor, Ilias and Moodle, are conducted based on penetration test in order to check the vulnerabilities of LMSs.

3.3.1 Data Collection

Data collection is the procedure of collecting as well as evaluating evidence based on variables of concentration, in a recognized methodical technique that allows one to response specified investigation questions [62]. In this thesis, two machines are used for collecting data. The first machine is the server while the second machine is scanner.

3.3.1.1 Server (First Machine)

On the first machine that contains windows 7 operating system, the XAMPP server (X ("cross"-platform), Apache HTTP Server, MySQL, PHP and Perl) version 1.8.3 and PHP version 5.5.9 are installed. This machine acts as normal server which allows the user to install web applications on it. Atutor, Ilias and Moodle versions 2.1.1, 4.4.3 and 2.6.1 respectively are installed on the server. For each LMS on this server, a LMS user, and course are created.

3.3.1.2 Scanner (Second Machine)

Here on the second machine, Kali Linux operating system is installed and it is used as host. Kali linux operating system is open source software which contains twenty five web application vulnerability scanners. These twenty five web application

vulnerability scanners are alphabetically ordered as burpsuit, cadaver, davtest, deblaze, fimp, golismero, grabber, joomscan, jsql, nikto, owasp-zap, padbuster, proxystrike, skipfish, sqlmap, uniscan-gui, vega, w3af, wapiti, webscarab, webshag-gui, websploit, whatweb, webscan and xsser. Based on previous researches, there is no specific study which compares or tests all these twenty five scanners. However, there are some previous researches which test or compare some of these scanners. Fernando et al. in [45] examines eighteen web application scanners. Out of these eighteen, four of them are from the aforementioned twenty five. These four scanners are burpsuit, proxystrike, skipfish and w3af. The study shows that skip fish and w3af are the best. Similarly, Djuric in [46] examines seven web vulnerability scanners in order to detect SQL injections. Amongst these seven, five of them are from the twenty five aforementioned scanners which include w3af, nikto, wapiti, vega and owasp-zap. The results of the study recommend w3af. Likewise Saeed in [47] assesses thirty two web application scanners. Ten of them are also from the twenty five above-mentioned scanners while the others are not. These ten are of owasp-zap, sqlmap, w3af, skipfish, vega, proxystrike, wapiti, grabber, webscarab and xsser. The results show that w3af version 1.2 and skipfish version 2.07b are the recommended ones. However to compare the scanners is beyond the scope of this study.

On the other hand in [48] Nikto scanner is applied to perform penetration test for discovering and improving application security. Similarly, Taek et al. in [49] uses Nikto scanner and Open Source Vulnerability Data Base (OSVDB) in their study to examine potential vulnerabilities of web applications victim sites. Finally, Huan-Chung et al. in [50] uses Nikto scanner and OSVDB for their study which is conducted based on observation on cloud-based security susceptibility evaluation.

Since all these tests were successfully performed with Nikto scanner, in this thesis, Nikto is selected to perform the tests of the vulnerabilities of Atutor, Ilias and Moodle. Nikto is an open source (General Public License) web vulnerability scanner and performs comprehensive checks against web application which is designed for manifold applications, including more than 3,200 possibly dangerous CGIs/files, operating systems, on the over 625 different servers which use OSVDB as their database evidence [51]. OSVDB that compromises confidentiality, integrity as well as availability are the main characteristics of information security [52]. More details about OSVDB are given in chapter four.

After the tests are completed, the Nikto report is presented based on newly created S-OSVDB impacts.

3.4 Data Analysis

As mentioned in chapter three, all results are analyzed using qualitative methods through contents analysis. Stempel in [53] explains that content analysis as the general set of methods that is useful for analyzing as well as sympathetic collections of data.

Many researchers such as Zhang and Wildemuth in [54] and Haris in [55] proposed some steps to follow and apply during the analysis of qualitative data using content analysis. Below are the steps to follow during the analysis of the Nikto results:

1. Define coding system.
2. Read over each record as well as making notes in the margins of interesting or related evidence.

3. Link the themes arising from each transcript with corresponding themes in other transcripts.
4. Categorize supporting transcript below the thematic parts.
5. Repeat the steps 1 – 4 to make sure that no theme has been missed.

Chapter 4

RESULTS AND FINDINGS

In chapter four, the results are presented. The results obtained by the scanners are presented that covers classifications of OSVDB impact. Under the introduction of S-OSVDB impact, four newly OSVDB impacts are created as: CoIntibility, AvCotibility, AvIntibility and AvCoIntibility. They are added to existing three CIA, which is called S-OSVDB impacts. Vulnerabilities and their Propose Solutions of an OSLMSs Based on S-OSVDB Impacts is the next section. The results are presented based on S-OSVDB impacts which are found through the tests of the three selected LMSs together with the proposed solutions for each vulnerability. Finally, a general discussion based on the physical observation and logical test are presented.

4.1 Results

Nikto is the general scanner which is used to scan all the entire server, web application and system. Here the aim of the study is to test only the vulnerability of web application on the server that are Atutor, Ilias and Moodle in particular, not the server or operating system. During the analysis of the results, vulnerabilities that do not belong particularly to those three LMSs are eliminated.

4.2 Introduction of Seven Open Source Vulnerability Data Base

OSVDB's objective is to deliver precise, comprehensive, as well as unbiased technical security evidence. The scheme at present covers more than 105,980 vulnerabilities, on both sides of 126,728 products from different 4,735 researchers since 112 years [56].

OSVDB classifies vulnerability impacts into three different categories as confidentiality, integrity and availability. Sometimes, vulnerability might include two or three vulnerability impacts, which meaning intersection in some vulnerability in OSVDB impact. For example, if the vulnerability covers availability and integrity, OSVDB calls that vulnerability impact as “loss of availability, loss of integrity”.

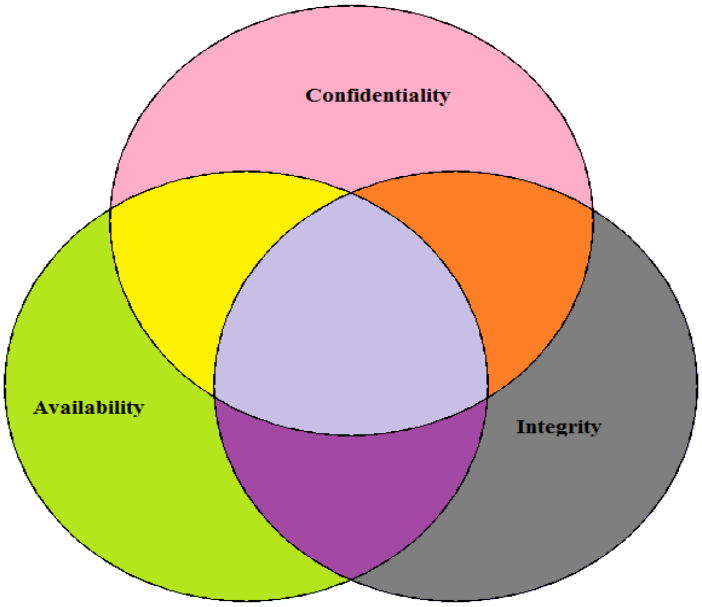

Figure 4.1: Vulnerability impact venn diagram according to OSVDB.

As it is seen from Figure 4.1, there is no standard name given to intersection of vulnerability impacts. If there is vulnerability which falls into one of the intersections, OSVDB uses those names to call this intersection impact.

Since there is no standard name given to any vulnerability found in intersections of three impacts of confidentiality, availability and integrity, new names are created for the intersections in this study. The four new names given to intersections are called as CoIntibility (intersection of confidentiality and integrity), AvCotibility (intersection of availability and confidentiality), AvIntibility (intersection of

availability and integrity) and AvCoIntibility (intersection of availability, confidentiality and integrity). The general name given to OSVDB impact is Seven Open Source Vulnerability Data Base (S-OSVDB) impact. These new names are used during the analysis in this study.

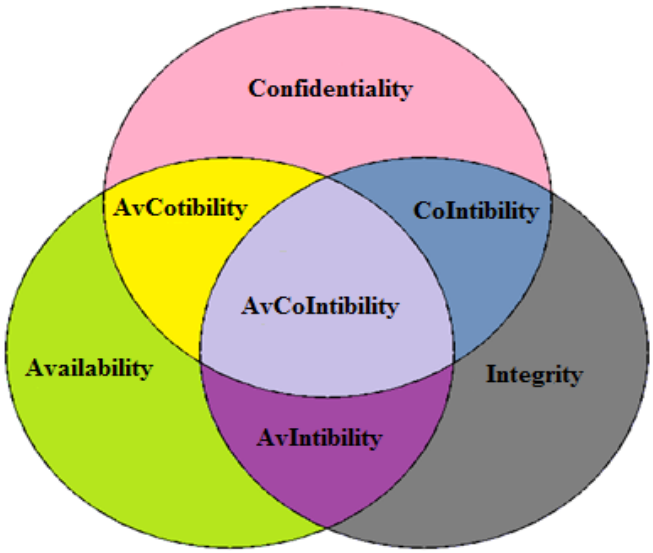

Figure 4.2: New conceptual venn diagram of S-OSVDB impact.

As it is seen from Figure 4.2, the newly created S-OSVDB vulnerability impacts cover seven categories of vulnerabilities as Confidentiality, Availability, Integrity, CoIntibility, AvCotibility, AvIntibility and AvCoIntibility. Four vulnerabilities impacts that are added on the existing OSVDB impacts are explained as followings.

4.3.1 AvCotibility

Whichever vulnerability impact falls into the intersection of availability and confidentiality is called AvCotibility.

4.3.2 AvIntibility

Each vulnerability impact which drops into the intersection of availability and integrity is called AvIntibility.

4.3.3 CoIntibility

Any vulnerability impact which falls into the intersection of confidentiality and integrity is called CoIntibility.

4.3.4 AvCoIntibility

All common vulnerability which falls into the intersection of confidentiality, integrity and availability is called AvCoIntibility.

4.4 Vulnerabilities and Proposed Solutions of an OSLMS Based on S-OSVDB Impacts

The results of scan for three LMSs are discussed here. It is worth to mention at this point that the results of scan for each of the LMS are too much to be presented here. For instance, scan results of the Moodle are around 700 pages. In this section, the results that are related only to the vulnerabilities of the LMSs are summarized. Samples of the nikto scan results are presented in Appendices A, B and C.

4.4.1 Atutor Vulnerabilities

Thirty three findings are found as the result of vulnerability scan but these findings are related with operating systems, server or network (see appendix A). No vulnerability is found as the vulnerability of Atutor.

4.4.2 Ilias Vulnerabilities

Nikto presents five vulnerabilities for the scan of Ilias. However, out of these five vulnerabilities, only one is found to be related with Ilias while the rest are not (see appendix B). S-OSVDB impacts of Ilias presented in Figure 4.3 shows the vulnerability found for Ilias.

Figure 4.3: S-OSVDB impacts of Ilias.

Figure 4.3 shows the vulnerability of Ilias as S-OSVDB 99039 impact that is related to integrity. Table 4.1 also summarizes the results obtained for Ilias.

Table 4.1: Summary of Ilias vulnerability based on S-OSVDB impact.

S-OSVDB Impact	S-OSVDB Number	Vulnerability Type
Confidentiality	N/F	N/F
Availability	N/F	N/F
Integrity	99039	XSS
AvCotibility	N/F	N/F
AvIntibility	N/F	N/F
CoIntibility	N/F	N/F
AvCoIntibility	N/F	N/F

Note: N/F = Not Found.

4.4.2.1 Integrity

Table 4.2 presents the summary of the integrity vulnerabilities of Ilias.

Table 4.2 Integrity impact.

S-OSVDB Impact	Type	Description
99039	XSS	Application does not authenticate the 'note' POST parameter during submission to the ilias.php script

S-OSVDB impact 99039 vulnerability named as Cross Site Scripting (XSS) is one of the vulnerabilities which does not only affect the web applications, but also LCMS and LMS [57]. This vulnerability occurs for the reason that there is lack of validation of 'note' POST parameter on submission to ilias.php which is located in the server. This fault allows an attacker to generate created request, which would execute illogical script code in a user's browsers using the trust connection between user's browser and their server.

4.4.2.2 Proposed solution for S-OSVDB Impact 99039

The vulnerability can be patched-up through validating the input note. If the input field is validated before or during the submission to the 'ilias.php' file which is resided on the server, arbitrary code would not be executed, because only authenticated data is going to be submitted to the server.

4.4.3 Moodle Vulnerabilities

Three vulnerabilities are found related with Moodle after the scan is completed (see appendix C). Figure 4.4 shows the S-OSVDB impacts diagram that presents the vulnerabilities found on Moodle.

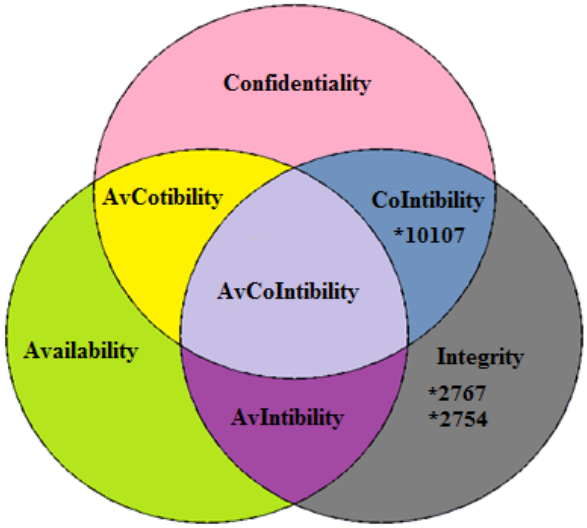

Figure 4.4: S-OSVDB impacts of Moodle.

As it can be seen from S-OSVDB impacts diagram at Figure 4.4 and results summarized in Table 4.3, there is one vulnerability found in CoIntibility impact which is OSVDB 10107, and two vulnerabilities found in integrity impact which are OSVDB 2767 and 2754. On the other hand, there is no vulnerability found in availability, confidentiality, AvCotibility, AvIntibility and AvCoIntibility impacts.

Table 4.3: Summary of Moodle vulnerabilities based on S-OSVDB impact.

S-OSVDB Impact	OSVDB Number	Vulnerability Type
Confidentiality	N/F	N/F
Availability	N/F	N/F
Integrity	2767	XSS
	2754	XSS
AvCotibility	N/F	N/F
AvIntibility	N/F	N/F
CoIntibility	10107	SQL injection
AvCoIntibility	N/F	N/F

4.4.3.1 CoIntibility

Table 4.4 presents the summary of the CoIntibility vulnerabilities of Moodle.

Table 4.4: CoIntibility impact.

S-OSVDB Impact	Type	Description
10107	SQL injection	SQL injection vulnerability in 'complete.php' file. Problem allows the user to execute arbitrary SQL commands remotely.

4.4.3.1.1 S-OSVDB Impact 10107

SQL injection vulnerability allows the user to execute arbitrary SQL commands remotely. Almost every single input field in instructors, guest's and student's user account forms are tested through Nikto scanner. In addition, every related URL parameters are tested in lieu of SQL injection weaknesses. There is one vulnerability found in CoIntibility. According to the research in [58], weaknesses of input validation are the most causes SQL injection attacks.

Below is an example of SQL injection:

$value_search = "ITEC";

*SELECT * from table_course WHERE courses_name = '$value_search';*

The above code is normal, however the attacker can use the following code to attack the web application:

$value_search = " ''; DELETE FROM courses_table WHERE 1 or course_name='' ";

The last SQL query will be present:

*SELECT * from course_table WHERE courses_name ='''; DELETE FROM course_table WHERE 1 or courses_name='';*

As the consequences the injected DELETE query will finally truncate the course table.

4.4.3.1.2 Proposed solution for S-OSVDB impact 10107

To evade this vulnerability, the following is recommended:

- Using the *mysql_real_escape_string()* function which will take the strings that is going to be used in MySQL query and bring back similar string with altogether SQL injection attempts securely escaped. And also to pass variables as parameters to the queries will remove the risk of such attack.
- Sensitive data should be encrypted.
- Error message alerts should be removed especially the ones that are risen for database queries.

4.4.3.2 Integrity

This group comprises vulnerabilities which allow the attacker to create, modify or delete data existing in e-learning. Table 4.5 presents the summary of the vulnerabilities for integrity.

Table 4.5: Integrity impact.

S-OSVDB Impact	Type	Description
2767	XSS	Vulnerability in externallib.php. This script does not correctly handle parameters which will allow remote users to change grade metadata through unnamed courses.
2754	XSS	Weakness in the quiz_question_tostring function in editlib.php allows student to change the time limit of quizzes.

4.4.3.2.1 S-OSVDB Impact 2767

The vulnerability of XSS can cause the attacker to alter browser functionality, and retrieve sensitive data.

A hacker can get the authorized data through presenting the JavaScript program on a web page. Below is an example on how the query executed:

document.write('<img width="2"

height="2"src="http://hackerswebsite.com/savedatainformation.php?datainformation =document.getElementById(' datainformation ').value + '" />');

Through the below example, attacker can use the advantages of a flow which is located in the php script of a web page if there is php code inside a JavaScript. For example:

> echo '<script type="text/javascript">';
>
> echo 'alert('" . $hacker_input . '");' echo '</script>'; the attacker can use $hacker_input = ‘’);
>
> a hacker can make $userinput equal to "); /* Malicious code. */

At the end, the result (code) will be inserted to anything selected variable for the hacker.

4.4.3.2.2 Proposed Solution for S-OSVDB Impact 2767

To avoid this vulnerability, below are the proposed solutions for a Moodle developer:

- Make sure that the web site returns back the user inputs after confirming it for any malicious code.

- Change non alphanumeric characters to html characters before showing the user input especially in search engines as well as forums.

4.4.3.3 S-OSVDB Impact 2754

Time duration is very important in any given quizzes. In Moodle quizzes engine, the structure which enforces to limit the time is a client side JavaScript function. If the student disables the JavaScript on the web browser, it allows the student to bypass the time limit and use more time than given. As mentioned above, Moodle does not use the server time during the quizzes, and JavaScript function is only used. Here the Moodle just uses its JavaScript function to report the quiz starting and finishing time to the instructor. There is no any flag or alert sign which the instructor is notified that the student exceeds the time limit given to him during the quiz.

4.4.3.4 Proposed Solution for S-OSVDB Impact 2754

Below are the recommended solutions for the problems:

- Server time should be used instead of JavaScript function.
- In addition, unique address identifiers such as IP address should be used to confirm that a session has not been hijacked.
- Options should be created which will block concurrent logins using the same user account.
- User account login should be traced instead of session.

4.5 Findings

In this section, the discussions on the results found during the tests are summarized. Only vulnerabilities for Ilias and Moodle are presented since there is no vulnerability found for Atutor.

4.5.1 Ilias General Findings

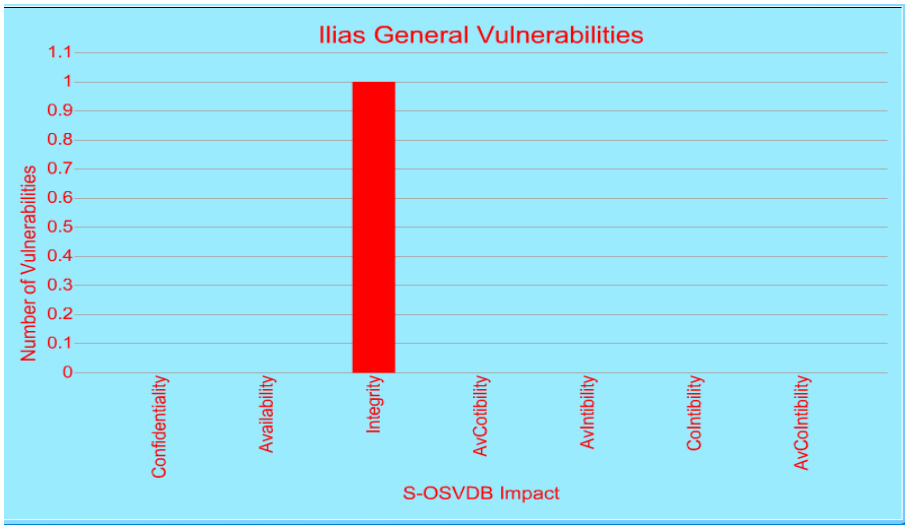

Figure 4.5: Vulnerabilities of Ilias.

Figure 4.5 shows that there is only one vulnerability found for Ilias. This vulnerability is in class of integrity out of S-OSVDB impacts.

4.5.2 Moodle General Findings

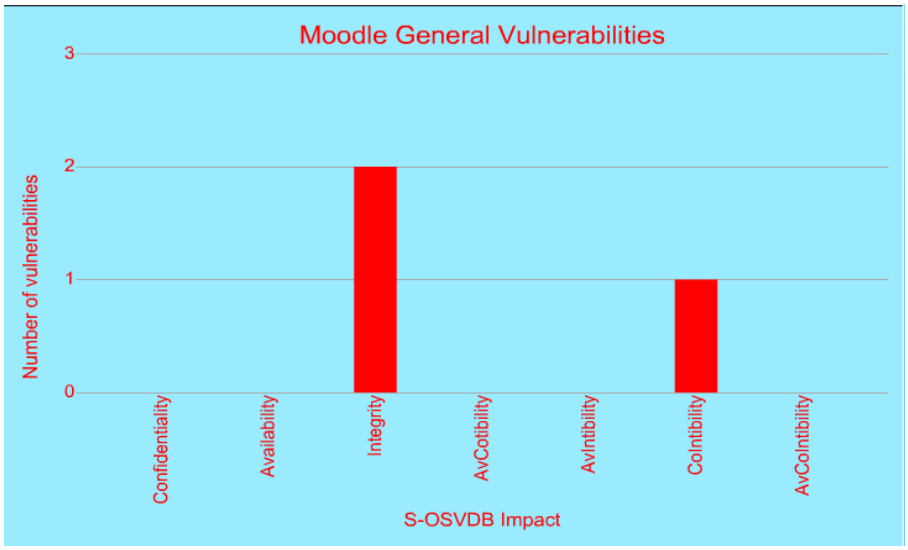

Figure 4.6: Vulnerabilities of Moodle.

As it is seen from Figure 4.6, the vulnerabilities of Moodle are from integrity impact and CoIntibility impact.

4.6 General Discussion

Based on the general results summarized in Table 4.6, it can be stated that Atutor, Ilias and Moodle have some drawbacks. Those are missing implementations of CAPTCHA on their systems. In addition, Moodle has higher vulnerability compared to others. This can prove the statement of previous study as "we found that Moodle has higher number of vulnerabilities compared to its commercial counterpart, Blackboard" in [59]. Ilias has only one vulnerability of loss of integrity impact apart from physical observation. In a previous research Ilias is also analysed and rated as average in terms of accessibility [43]. Atutor has no vulnerability in S-OSVDB impact. This confirms the previous research in [43] which shows that Atutor has an excellent in terms of accessibility.

Table 4.6: General results of the study.

		Atutor	Ilias	Moodle
Physical observation	CAPTCHA	X	X	X
Results of logical test based on S-OSVDB impact	Confidentiality	✓	✓	✓
	Availability	✓	✓	✓
	Integrity	✓	X	X
	AvCotibility	✓	✓	✓
	AvIntibility	✓	✓	✓
	CoIntibility	✓	✓	X
	AvCoIntibility	✓	✓	✓

Based on these findings, learning environment should pay attention in their data integrity, because loosing integrity allows attacker to damage, implement, adapt, hang, copy, reiterate, or interrupt learning environments' assets. But, more attention should be paid to the CoIntibility, because it allows hacker to see or gain confidential information and at the same time the hacker can alter, or damage the information.

As mentioned, loss of CoIntibility is very dangerous in learning environment. For example in 2012, a hacking group called Team Ghost Shell targeted college and universities around the world because of loss of CoIntibilitity. An entire of fifty three college and universities including eleven universities from United State such as Harvard University, Ohio State University, New York University were hacked [60]. Almost all of the data exposed was put publicly available on the website [61], including the usernames and passwords of the students and employees.

Chapter 5

CONCLUSION AND FUTURE WORK

There are two sections in this chapter. The first section presents the conclusions which cover the summary of the thesis. The other section discusses the limitations and future of work. It discusses the boundary of the study and suggests future works that can be carried out in the field of information security in learning environment.

5.1 Conclusion

Majority of the learning environment worldwide use LMSs. In this study, three selected OSLMSs as Atutor, Ilias and Moodle are tested to find their vulnerabilities. Atutor is selected since it is the first LCMS to fulfill the accessibility specifications of completely W3C, WCAG 1.0 at the AA+ level. In addition, Ilias is selected since it is an OSLMS which is used not only in learning environment but also in defense and security organizations. Moodle is selected since it is the most common LMS used worldwide almost in all of the colleges and universities. In the study, the security susceptibilities are classified into two as physical observations and logical tests.

Through physical observations, the study shows that missing CAPTCHA in these three selected LMSs allows the attackers to attack the server, such as brute force attack on the LMSs server.

Through the tests performed through Nikto, three vulnerabilities are found in Moodle, and only one vulnerability in Ilias where recommended solutions for these vulnerabilities are proposed. The outcomes reveal that Atutor is the safest and most secure LMS. The results of this study show that there is possibility to have vulnerability in learning environment even for one of the most known Moodle. The vulnerabilities of Moodle are in CoIntibility and integrity impact.

The significance findings in this study will alert the users especially in education environment about the vulnerabilities of Moodle version 2.6.1 and Ilias version 4.4.3. In addition, the significance of the findings will help the developer of the Moodle and Ilias to update this version based on the recommended solutions in order to make them more secure.

The procedure used to tests three selected LMSs in chapter three (methodology), can be used to test any LMS. This is one of the contributions of this study, not only to the learning environment, but also to LMS penetration testers.

In addition, S-OSVDB impacts are created and used in the study, which will help all the users of OSVDB impact on how to classify the vulnerability impact at intersections. Using the web application scanners which uses OSVDB impact as their data evidence based on CIA triad such as Nikto scanner and apply S-OSVDB impacts will straightforwardly classify the vulnerabilities impact which will allows the tester to see the class of vulnerability impact without complications.

5.2 Limitation and Future Work

This study focuses only in three selected OSLMS, Atutor, Ilias and Moodle. The study does not pay attention on programming language used. Moreover, the study performed within local area network (LAN).

For the future work, this study recommends more study to be focused on commercial LMSs. Moreover, learning environment's server, network settings, as well as their impacts based on security should be considered in terms of CIA.

REFERENCES

[1] Edutech Wiki (2009). Learning Environment. Retrieved at http://edutechwiki.unige.ch/en/Learning_environment (last access June 2014).

[2] Barrie, S. C., & Prosser, M. (2003). An Aligned, Evidence-based Approach to Quality Assurance for Teaching and Learning. *Australian Universities Quality Forum*, pp. 13-15.

[3] Primary National Strategy. (2004). The Learning Environment and its Impact on Learning. Retrieved at http://www.lancsngfl.ac.uk/curriculum/assessment/getfile.php?src=707/10+Learning+Environment.pdf (last accessed May 2014).

[4] Ellis, R. K. (2010). Field Guide to Learning Management Systems, 2009. http://conferenceunctlt.org/proposals/presentations/conf4/900_LMSfieldguide1.pdf, vol. 19, pp. 4 (last accessed June 2014).

[5] Brandon-hall.com. 2003. E-Learning Glossary of Terms. Retrieved at www.brandhall.com/public/pdfs/glossary.pdf (last accessed May 2014).

[6] McIntosh, D. (2014). Vendors of Learning Management and E-learning Products. Retrieved at http://www.trimeritus.com (last accessed April 2014).

[7] ANTA, (2002). Flexible Learning Fellowship Change Management Plan, Strategy 2001, Nancye Stanelis (South Australia), August 2002. Retrieved at www.flexiblelearning.net.au/felloships/docs/NSChangeManagementplan.pdf.

[8] Whitman, M. & Mattord, H. (2011). *Principles of Information Security*, 4th edition, Boston: Course Technology.

[9] Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of Information Security in Theory and Practice*, USA: Elsevier.

[10] IAPP (n.d). Charter of Fundamental Right. Retrieved at https://www.privacyassociation.org/resource_center/privacy_glossary (last accessed January 2014).

[11] Muntjir, M., Aljahdali, S., Asadullah, M., & Haq, J. (2014). Security Issues and Their Techniques in DBMS-A Novel Survey. *International Journal of Computer Applications*, vol. 85.

[12] Joh, H. (2013). Modeling Security Vulnerabilities in Learning Management Systems. *International Journal of Learning Management Systems*, vol. 1, no 2, pp. 1-12.

[13] Moore, R.S. (2001). Information Security Standards: Deluge and Dearth. *Information Systems Security*, vol. 10, no. 1, pp 1-6.

[14] Renaud, K., & Gálvez-Cruz, D. (2010). Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach. *In Information Security for South Africa* (ISSA), pp. 1-8.

[15] Muntjir, M., Aljahdali, S., Asadullah, M., & Haq, J. (2014). Security Issues and their Techniques in DBMS-A Novel Survey. *International Journal of Computer Applications*, vol. 85, no. 13.

[16] The ISO 27000 Directory. (n.d). An Introduction to ISO 27001, ISO 27002....ISO 27008. Retrieved at http://www.27000.org/index.htm (last access April 2014).

[17] Awad, H. A., & Battah, F. M. (2011). Enhancing Information Systems Security in Educational Organizations in KSA through Proposing Security Model. *International Journal of Computer Science*, vol. 8, no. 5.

[18] WhiteHat. (2011). WhiteHat Website Security Statistics Report. Retrieved at https://www.whitehatsec.com/resource/stats.html (last access April 2014).

[19] Tsolis, D., Stamou, S., Christia, P., Kampana, S., Rapakoulia, T., Skouta, M., & Tsakalidis, A. (2010). An Adaptive and Personalized Open Source E-learning Platform. *Procedia-Social and Behavioral Sciences*, vol. 9, pp. 38-43.

[20] Mallon, D., & Clarey, J. (2012). Learning Management Systems 2013: The Definitive Buyer's Guide to the Global Market for Learning Management Solutions, Technical Report.

[21] Kumar, S., & Dutta, K. (2011). Investigation on Security in LMS Moodle. *International Journal of Information Technology and Knowledge Management*, vol. 4, no. 1, pp. 233-238.

[22] Floyd, C., Schultz, T., & Fulton, S. (2012). Security Vulnerabilities in the Open Source Moodle E-learning System. In *Proceedings of the 16th Colloquium for Information Systems Security Education*. Lake Buena Vista, Florida.

[23] Violettas, G. E., Theodorou, T. L., & Stephanides, G. C. (2013). E-Learning Software Security: Tested for Security Vulnerabilities & Issues. *2013 Fourth International Conference on e-Learning Best Practices in Management Design and Development of e-Courses: Standards of Excellence and Creativity*, pp. 233-240.

[24] Sarrab, M., & Rehman, O. M. H. (2014). Empirical Study of Open Source Software Selection for Adoption, Based on Software Quality Characteristics. *Advances in Engineering Software*, vol. 69, pp. 1-11.

[25] Moore, S. A. (2013). Now is the Time to Consider Open Source Learning Management Systems for Enterprise. Retrieved at http://www.ilearning forum.org/fichier/4 (last access May 2014).

[26] Atutor. (n.d). Learning Management Tools. Retrieved at http://www.atutor.ca/ (last access March 2014).

[27] Ruiz Reyes, N., Vera Candeas, P., Galán, S. G., Viciana, R., Canadas, F., & Reche, P. J. (2009). Comparing Open-Source E-learning Platforms from Adaptivity Point of View. In *EAEEIE Annual Conference*, pp. 1-6.

[28] Granite University. (n.d). Retrieved at https://classroom.gsinc.com/login.php (last access May 2014).

[29] Weston University College. (n.d). Retrieved at http://www.westoncollege.edu.gh/demo/eschool/login (last access May 2014).

[30] Sukhothai Thammathirat Open University (n.d). Institutional Profile: Sukhothai Thammathirat Open University. Retrieved at http://www.icde.org/projects/regulatory_frameworks_for_distance_education /institutional_profiles/sukhothai_thammathirat_open_university/ (last access May 2014).

[31] Ilias. (2014). Using ILIAS. Retrieved at http://www.ilias.de/docu/ goto_docu_cat_580.html (last access April 2014).

[32] Dougiamas, M. (2005). Lounge. Retrieved at https://moodle.org/mod/ forum/discuss.php?d=27533&parent=129848 (last access May 2014).

[33] Moodle. (2014). Moodle Statistics. Retrieved at https://moodle.org/stats/ (last access February 2014).

[34] Al-Ajlan, A., & Zedan, H. (2008). Why Moodle. In *Future Trends of Distributed Computing Systems, 2008. FTDCS'08. 12th IEEE International Workshop on*, pp. 58-64.

[35] Eastern Mediterranean University (n.d). Faculty of Education - Online. Retrieved at http://fedumoodle.emu.edu.tr/ (last access April 2014).

[36] Moodle. (2012). Installations 10000 Plus. Retrieved at http://docs.moodle.org/23/en/Installations_10000_plus (last access April 2014).

[37] Athabasca University. (n.d). CDE Moodle Site. Retrieved at http://cde.lms.athabascau.ca/ (last access April 2014).

[38] CoRhodes University. (n.d). RU Connected. Retrieved at http://ruconnected.ru.ac.za/course/view.php?id=71 (last access April 2014).

[39] Open University (n.d). Open Univeristy Moodle. Retrieved at https://msds.open.ac.uk/signon/SAMSDefault/SAMS001_Default.aspx?URL=http://learn1.open.ac.uk/mod/ (last access April 2014).

[40] Smith, J. Bekker, H. & Cheater, F. (2011) 'Theoretical Versus Pragmatic Design in Qualitative Research', *Nurseresearcher*, vol. 18, no. 2, pp. 39-51.

[41] Heyink, J. W., & Tymstra, T. J. (1993). The Function of Qualitative Research. *Social Indicators Research*, vol. 29, no. 3, pp. 291-305.

[42] Joh, H. (2013). Modeling Security Vulnerabilities in Learning Management Systems. *International Journal of Learning Management Systems*, vol. 1, no. 2, pp. 1-12.

[43] Kumar, S., Gankotiya, A. K., & Dutta, K. (2011). A Comparative Study of Moodle with other E-learning Systems. *Electronics Computer Technology (ICECT) 3rd International Conference*, vol. 5, pp. 414-418.

[44] Gaskell, G. (2010). Enabling or Disabling Captcha for Failed Logins. Retrieved at https://confluence.atlassian.com/display/BAMBOO025/Ena bling+or+ Disabling+Captcha+for+ Failed+Logins (last access April 2014).

[45] Muñoz, F. R., & Villalba, L. J. G. (2013). Methods to Test Web Application Scanners. *The 6th International Conference on Information Technology*.

[46] Djuric, Z. (2013). A Black-box Testing Tool for Detecting SQL Injection Vulnerabilities. *Informatics and Applications (ICIA) Second International Conference*, pp. 216-221.

[47] Saeed, F. A., & Elagabar, E. E. (2014). Assessment of Open Source Web Application Security Scanners. *Journal of Theoretical & Applied Information Technology*, vol. 61, no. 2.

[48] Avramescu, G., Bucicoiu, M., Rosner, D., & Tapus, N. (2013). Guidelines for Discovering and Improving Application Security. *Control Systems and Computer Science (CSCS), 19th International Conference,* pp. 560-565.

[49] Lee, T., Kim, D., Jeong, H., & In, H. P. (2014). Risk Prediction of Malicious Code-Infected Websites by Mining Vulnerability Features. *International Journal of Security & its Applications*, vol. 8, no. 1.

[50] Li, H. C., Liang, P. H., Yang, J. M., & Chen, S. J. (2010). Analysis on Cloud-Based Security Vulnerability Assessment. *e-Business Engineering (ICEBE), IEEE 7th International Conference,* pp. 490-494.

[51] Popa, M. (2013). Analysis of Zero-Day Vulnerabilities in Java. *Journal of Mobile, Embedded and Distributed Systems*, vol. 5, no. 3, pp. 108-117.

[52] Rajesh, P., & Narsimha, G. (2013). Privacy Preserving Data Mining by using Implicit Function Theorem *International Journal of Network Security & its Applications*, vol. 5, No. 2.

[53] Fico, F.G. Lacy, S. &Riffe, D (2008). A Content Analysis Guide for Media Economics Scholars, *Journal of Media Economics*, vol. 21, no. 2, pp 114-130.

[54] Zhang, Y., & Wildemuth, B. M. (2009). Qualitative Analysis of Content. *Applications of Social Research Methods to Questions in Information and Library Science*, pp. 308-319.

[55] Harris, H. (2001). Content Analysis of Secondary Data: A Study of Courage in Managerial Decision Making, *Journal of Business Ethics*, vol. 34, no. 3/4, pp. 191-208.

[56] OSVDB. (n.d). Open Sourced Vulnerability Database. Retrieved at http://osvdb.org/ (last access May 2014).

[57] Luminita, D. C. C. (2011). Security Issues in E-learning Platforms. *World Journal on Educational Technology*, vol. 3, no. 3, pp. 153-167.

[58] Matos, R., & Carvalho, F. (2012). Moodlewatcher: One Year Experience of Detecting and Preventing Fraud When using Moodle Quizzes. *Edulearn12 Proceedings*.

[59] Joh, H. (2013). Modeling Security Vulnerabilities in Learning Management Systems. *International Journal Learning Management Systems*, vol. 1, no. 2, pp. 1-12.

[60] TeamGhostShell. (2012). #ProjectWestWind – Today's Education! Retrieved at http://pastebin.com/AQWhu8Ek (last access May 2014).

[61] Privacy Right Clearinghouse, P. R. (2014). Chronology of Data Breaches Security Breaches 2005 - Present. Retrieved at http://www.privacyrights.org/data-breach/admin/www.mass.gov/dia?order=field_breach_total_value&sort=desc&title= (last access April 2014).

[62] Wikipedia (2014). Data collection. Retrieved at http://en.wikipedia.org/wiki/Data_collection (last access June 2014).

APPENDICES

Appendix A: Nikto Results of Atutor

169.254.115.59 / 169.254.115.59 port 80	
Target IP	**169.254.115.59**
Target hostname	169.254.115.59
Target Port	80
HTTP Server	Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9
Site Link (Name)	http://169.254.115.59:80/atutor/login.php
Site Link (IP)	http://169.254.115.59:80/atutor/login.php
URI	/atutor/login.php/atutor/login.php/
HTTP Method	GET
Description	Cookie ATutorID created without the httponly flag
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/ http://169.254.115.59:80/atutor/login.php/atutor/login.php/
OSVDB Entries	OSVDB-0
URI	**/atutor/login.php/atutor/login.php/**
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.5.9
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/ http://169.254.115.59:80/atutor/login.php/atutor/login.php/
OSVDB Entries	OSVDB-0
URI	**/atutor/login.php/atutor/login.php/**
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/ http://169.254.115.59:80/atutor/login.php/atutor/login.php/
OSVDB Entries	OSVDB-0
URI	**/atutor/login.php/atutor/login.php/gb/index.php?login=true**
HTTP Method	GET
Description	/atutor/login.php/gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/gb/index.php?login=true http://169.254.115.59:80/atutor/login.php/atutor/login.php/gb/index.php?login=true
OSVDB Entries	OSVDB-8204
URI	**/atutor/login.php/atutor/login.php/anthill/login.php**
HTTP Method	GET
Description	/atutor/login.php/anthill/login.php: Anthill bug tracking system may be installed.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/anthill/login.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/anthill/l

	ogin.php
OSVDB Entries	OSVDB-0
URI	**/atutor/login.php/atutor/login.php/admin/index.php**
HTTP Method	GET
Description	/atutor/login.php/admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/admin/index.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/admin/index.php
OSVDB Entries	OSVDB-3093
URI	**/atutor/login.php/atutor/login.php/board/index.php**
HTTP Method	GET
Description	/atutor/login.php/board/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/board/index.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/board/index.php
OSVDB Entries	OSVDB-3093
URI	**/atutor/login.php/atutor/login.php/community/index.php?analized=anything**
HTTP Method	GET
Description	/atutor/login.php/community/index.php?analized=anything: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/community/index.php?analized=anything http://169.254.115.59:80/atutor/login.php/atutor/login.php/community/index.php?analized=anything
OSVDB Entries	OSVDB-3093
URI	**/atutor/login.php/atutor/login.php/cutenews/search.php**
HTTP Method	GET
Description	/atutor/login.php/cutenews/search.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/cutenews/search.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/cutenews/search.php
OSVDB	OSVDB-3093

Entries	
URI	**/atutor/login.php/atutor/login.php/modules/Search/index.php**
HTTP Method	GET
Description	/atutor/login.php/modules/Search/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/modules/Search/index.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/modules/Search/index.php
OSVDB Entries	OSVDB-3093
URI	**/atutor/login.php/atutor/login.php/php/gaestebuch/admin/index.php**
HTTP Method	GET
Description	/atutor/login.php/php/gaestebuch/admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/php/gaestebuch/admin/index.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/php/gaestebuch/admin/index.php
OSVDB Entries	OSVDB-3093
URI	**/atutor/login.php/atutor/login.php/prometheus-all/index.php**
HTTP Method	GET
Description	/atutor/login.php/prometheus-all/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
Test Links	http://169.254.115.59:80/atutor/login.php/atutor/login.php/prometheus-all/index.php http://169.254.115.59:80/atutor/login.php/atutor/login.php/prometheus-all/index.php
OSVDB Entries	OSVDB-3093

Appendix B: Nikto Results of Ilias

169.254.115.59 / 169.254.115.59 port 80	
Target IP	**169.254.115.59**
Target hostname	169.254.115.59
Target Port	80
HTTP Server	Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9
Site Link (Name)	http://169.254.115.59:80/ilias/login.php
Site Link (IP)	http://169.254.115.59:80/ilias/login.php
URI	/ilias/login.php/ilias/login.php/
HTTP Method	GET
Description	Cookie PHPSESSID created without the httponly flag
Test Links	http://169.254.115.59:80/ilias/login.php/ilias/login.php/ http://169.254.115.59:80/ilias/login.php/ilias/login.php/
OSVDB Entries	OSVDB-0
URI	**/ilias/login.php/ilias/login.php/**
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.5.9
Test Links	http://169.254.115.59:80/ilias/login.php/ilias/login.php/ http://169.254.115.59:80/ilias/login.php/ilias/login.php/
OSVDB Entries	OSVDB-0
URI	**/ilias/login.php/ilias/login.php/**
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://169.254.115.59:80/ilias/login.php/ilias/login.php/ http://169.254.115.59:80/ilias/login.php/ilias/login.php/
OSVDB Entries	OSVDB-0
URI	**/ilias/login.php/ilias/login.php/**
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://169.254.115.59:80/ilias/login.php/ilias/login.php/ http://169.254.115.59:80/ilias/login.php/ilias/login.php/
OSVDB Entries	OSVDB-0
URI	**/ilias/login.php.**
HTTP Method	GET
Description	The host is vulnerable to XSS. The value is "http:///ilias/ilias.php?target=&client_id=inuwa&auth_stat=".
Test Links	http://169.254.115.59:80/ilias/login.php. http://169.254.115.59:80/ilias/login.php.
OSVDB Entries	OSVDB-99039

Appendix C: Nikto Results of Moodle

192.168.2.101 / 192.168.2.101 port 80	
Target IP	**192.168.2.101**
Target hostname	192.168.2.101
Target Port	80
HTTP Server	Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9
Site Link (Name)	http://192.168.2.101:80/moodle/login/index.php
Site Link (IP)	http://192.168.2.101:80/moodle/login/index.php
URI	/moodle/login/index.php/moodle/login/index.php/
HTTP Method	GET
Description	Cookie MoodleSession created without the httponly flag
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/**
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.5.9
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/**
HTTP Method	GET
Description	Uncommon header 'content-script-type' found, with contents: text/javascript
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/**
HTTP Method	GET
Description	Uncommon header 'content-style-type' found, with contents:

n	text/css
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/**
HTTP Method	GET
Description	Uncommon header 'x-ua-compatible' found, with contents: IE=edge
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/**
HTTP Method	GET
Description	Uncommon header 'x-frame-options' found, with contents: same origin
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/ http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/clientaccesspolicy.xml**
HTTP Method	GET
Description	lines
Test Links	http://192.168.2.101:80/moodle/login/index.php/clientaccesspolicy.xml http://192.168.2.101:80/moodle/login/index.php/clientaccesspolicy.xml
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/crossdomain.xml**
HTTP Method	GET
Description	/crossdomain.xml contains 0 line which should be manually viewed for improper domains or wildcards.
Test Links	http://192.168.2.101:80/moodle/login/index.php/crossdomain.xml http://192.168.2.101:80/moodle/login/index.php/crossdomain.xml
OSVDB	OSVDB-0

Entries	
URI	**/moodle/login/index.php/robots.txt**
HTTP Method	GET
Description	"robots.txt" contains 1 entry which should be manually viewed.
Test Links	http://192.168.2.101:80/moodle/login/index.php/robots.txt http://192.168.2.101:80/moodle/login/index.php/robots.txt
OSVDB Entries	OSVDB-0
URI	**/moodle/login/index.php/moodle/login/index.php/splashAdmin.php**
HTTP Method	GET
Description	/moodle/login/index.php/splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security.
Test Links	http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/splashAdmin.php http://192.168.2.101:80/moodle/login/index.php/moodle/login/index.php/splashAdmin.php
OSVDB Entries	OSVDB-0