Security Vulnerabilities of the Web Based Open Source Information Systems: Adoption Process and Source Codes Screening

Said Ally
The Open University of Tanzania
said.ally@out.ac.tz / said.ally@hotmail.com

Abstract: *This paper exposes security vulnerabilities of the web based Open Source Information Systems (OSIS) from both system angle and human perspectives.It shows the extent of risk that can likely hinder adopting organization from attaining full intended benefits of using OSIS software. To undertake this study, a case study methodology was opted with fifteen public and private organizations being software companies and technology users. The respondents to this study were categorized as top management, software developers, systems administrators and end users. Apart from intensive documentary review, critical investigation of onsite servers running nine web based OSIS systems has been done. The studied systems are MOODLE, OrangeHRM, ATutor, Koha, WebERP, vTigerCRM, OpenDocMan, OpenSIS and Zalongwa software.The study reveals that there are security weaknesses in locally customized OSIS systems and freely downloadable information systems from internet repository. This has been a result of uncoordinated operations and ad hoc performance of key OSIS stakeholders ranging from early stages of sourcing the said software, OSIS selection, adoption, customization, installation, upgrading and routine management.*

Keywords – Open Source Software, Information System, Software Security.

INTRODUCTION

Though application and use of Information and Communication Technologies (ICT) is growing very fast in the world, in developing countries like Tanzania, the use and development of ICT capabilities is still limited and faces a wide range of constraints and challenges (Bakari, 2007). One example of the areas which demonstrates such ICT immobility in Tanzania is the use of web based Open Source Information Systems (OSIS). This has led to extensive Open Source Software (OSS) studies in recent years. As pointed out by Lungo and Kaasbøl (2006), there has been a growing interest among developing countries towards application of OSIS. In Tanzania for example, in the year 2003, the Government carried out participatory review of ICT which consequently resulted into National ICT Policy that places a considerable attention on the use of OSS products (URT, 2003).

Since then, several initiatives have been taken to establish a benchmarking framework for utilizing this technology. In 2003, the Tanzania Free and Open Source Software Association (TAFOSSA) was established to act as a national umbrella with general objective of harnessing the potentials of free and open source software for supporting national developmental goals as spelled in Tanzania's National Vision 2025 and reiterated in Tanzania's National ICT Policy of 2003 aimed at advocating and promoting OSS for rapidly developing access to, and utilization of ICT in Tanzania. In fact, as highlighted by Mitchell (2004) the open source computing is an exclusive technology that has become an essential part of providing the fastest and most efficient organizational solutions in recent years. The organizations that take time to select, evaluate and apply OSS to their specific requirements are likely to realize widespread benefits that are immediate, ongoing and lasting.

Considering that many government institutions are mainly financed by government and are by their very nature not-for-profit organizations, the logical course to take when it comes to choosing software is the OSIS solutions. In Tanzania for instance, the adoption of OSIS products by public sectors has been mainly motivated by its cost effectiveness and presence of National ICT Policy. On the other hand, since many private sectors receive limited software support, the driving factor for OSIS adoption is also based on the software cost. They opt for OSIS to gain business profit as they are either freely or cheaply available.

The recent OSS studies conducted in Tanzania focused only on the experience in the usage and extent of investment. While this sort of technology is fast growing in the country and even in other developing countries, no research has been reported to find the best practices for secure adoption and use of OSIS systems. This has been due to the fact that many scholars who are proponents of OSIS systems rely on the assumption that OSS systems are designed with strong security and therefore not vulnerable to attackers and malicious hackers.

However, from its very nature, the fact that OSIS systems are made available with open source codes and its development being fully depending on community support which is not guaranteed and which constitutes both good guys and bad guys; the OSIS turns to be of high potential risks from malicious attacks that can be introduced due to systems weaknesses and/or through deliberate and accidental actions by users.

The security of these systems is a growing concern for adopters (Schneider, 2000). Security requirements are important to be met since failure to do so may expose critical organizationô's assets specifically information to danger and become susceptible to disclosure risk and, hence, the objectives of organizations might be negatively affected as well.

Therefore the goal of this study was to familiarize with the current applied methods as being practiced by various organizations in Tanzania for the adoption and use of OSIS and discloses the security vulnerabilities of the systems under production.

RESEARCH METHODOLOGY

To undertake this study, a case study methodology was used. As suggested by Yin (1994), a case study refers to an entity, unit of analysis or an empirical inquiry that investigates a contemporary phenomenon within its real life context, using multiple sources of evidence with focus only on a particular issue. With this approach, the problem can be understood and explored from its natural setting by answering ñwhyò and ñhowò questions which are supportive in theory building research.

Figure 1 lists the stages undergone during undertaking this study

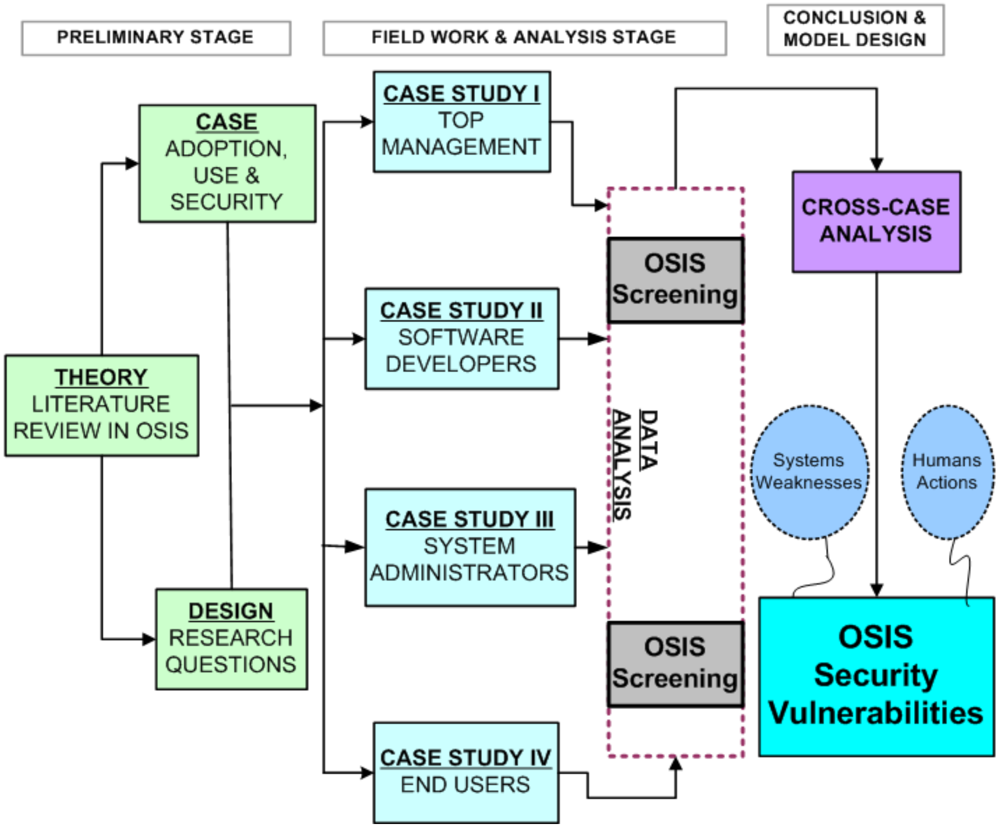
PRELIMINARY STAGE
FIELD WORK & ANALYSIS STAGE
CONCLUSION & MODEL DESIGN
CASE ADOPTION, USE & SECURITY
THEORY LITERATURE REVIEW IN OSIS
DESIGN RESEARCH QUESTIONS
CASE STUDY I TOP MANAGEMENT
CASE STUDY II SOFTWARE DEVELOPERS
CASE STUDY III SYSTEM ADMINISTRATORS
CASE STUDY IV END USERS
OSIS Screening
DATA ANALYSIS
OSIS Screening
CROSS-CASE ANALYSIS
Systems Weaknesses
Humans Actions
OSIS Security Vulnerabilities

Figure 1: The OSIS Research Design

As shown in Figure 1, the first stage of the study was to carry out extensive literature review on the subject; then we conducted interviews with the university academic tutors and professional staff in the field from the selected organizations and performed a deep screening of various running OSIS systems to identify their security vulnerabilities.

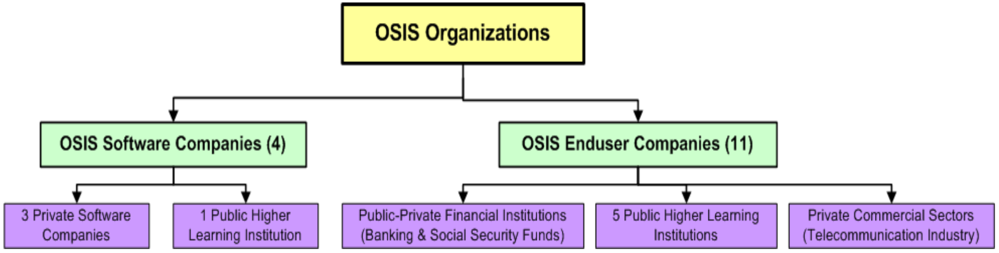
OSIS Organizations
OSIS Software Companies (4)
OSIS Enduser Companies (11)
3 Private Software Companies
1 Public Higher Learning Institution
Public-Private Financial Institutions (Banking & Social Security Funds)
5 Public Higher Learning Institutions
Private Commercial Sectors (Telecommunication Industry)

Figure 2: The OSIS Organizations

Sample and Sampling Techniques

To facilitate the interviewing of the selected respondents, four types of questionnaires were designed purposely for top management (TM), software developers (SD), systems administrators (SA) and end users (EU). The questionnaires formed the raw and primary data from multiple choice, open ended questions and face to face sessions with the use of both unstructured and semi-structured.

In average, each interview session lasted for approximately 40 minutes but interview with software developers and systems administrators took longer than that. This has been due to the fact that the software developers and systems administrators are the two technical groups of the subject under study which are highly involved in OSIS development, upgrading and patching and routine management. They are the only ones with access to source codes.

The top management category involved senior level employees in the organization who assess new OSIS and have the final authority to decide whether a new technology will be adopted by the organization or not.

The category of software developer involved OSIS software engineers who participate in software development project either in the systems designed from scratch or the one customized from free internet sources. The third category of the system administrators involved technical experts who deal with day to day management of OSIS systems. The end-user is defined as the final or ultimate user of OSIS.

In undertaking this study, a total of 200 informants accessed 15 top managers, 24 software developers, 41 OSIS administrators, and 120 end users. The educational qualifications of the respondents were ranging from PhD holders/lecturers (18), Masters/Assistant Lecturers (42), Bachelors/Tutorials Assistants/Advanced Diploma in IT (97) and lastly undergraduate students (43).

Table 1: Academic Profile for Informants

SN	Qualification	TM	SD	SA	EU
1	PhD/Lecturers	11	1	-	6
2	Masters/Assistant Lecturers	4	5	6	27
3	Bachelors/Tutorial Assistants/Advanced Diploma in IT	-	14	35	48
4	Undergraduate Students	-	4	-	39
Total		**15**	**24**	**41**	**120**
Total of **200 informants** were interviewed at all sites					

A total of 15 public and private organizations were visited. Among which, 4 are the software companies while others are just OSIS technology users. As shown in Table 2, in total, the 15 organizations consist of 52 different (i.e. 52 several versions based on 9OSIS systems) OSIS systems with organization Y having highest number of 10 different OSIS running from production servers, followed by organization U with 9

OSIS software. The organizations K and R possess lowest number of OSIS. Each has just one OSIS system in use.

Table 2: Organizations, OSIS in Application and Average Years of Respondents

SN	Organization	OSIS	TM		SD		SA		EU	
			TTL	Avg (Yrs)	TTL	Avg (Yrs)	TTL	Avg (Yrs)	TTL	Avg (Yrs)
1	U	9	1	4	4	4	4	5	13	3
2	V	5	1	3	5	6	5	6	17	3.5
3	X	4	1	5	5	7	5	7	1	6
4	W	2	1	1	-	-	2	1	5	1
5	Z	2	1	2	-	-	2	2	9	1
6	Y	10	1	10	10	8	5	6	5	7
7	G	2	1	1	-	-	2	1	5	1
8	H	2	1	1	-	-	1	1	3	2
9	J	7	1	1	-	-	5	3	21	2
10	K	1	1	1	-	-	1	1	6	1
11	M	2	1	1	-	-	1	1	5	1
12	N	1	1	1	-	-	1	1	8	1
13	Q	2	1	1	-	-	2	1	7	1
14	R	1	1	2	-	-	2	1	6	1
15	I	2	1	1	-	-	3	3	9	2
Total/Average		**52**	**15**	**2.33**	**24**	**6.25**	**41**	**2.67**	**120**	**2.43**

A group of software developers has shown to have more experiences in working with the OSIS systems with average of 6.25 years, followed by group of administrators (2.67 years), then end users (2.43 years). The top managers seem to have experience of average 2.33 years of working with OSIS systems.

The visited organizations (U, V, X, W, Z, Y, G, H, J, K, M, N, Q and R) are purposely left anonymous as the consent to disclose identity was refused in order to protect business interests of such organizations.

Onsite Practical Investigation of OSIS Software

The security vulnerabilities of nine web based OSIS were examined. They include:

(i) Human Resource Management Information System (HRMIS) ï sample software is OrangeHRM-version 2.6.10. This is a PHP-based application for managing human resources. It was started in 2005 and the first beta release was made in January 2006. Due to online adoption, the software is continuously being improved through OSS community.

(ii) Financial Management Information System (FINMIS) ï sample software is webERP-version 4.0.9.1. This is an open-source web-based Enterprise Resource Planning (ERP) system. It is an open source project and no fees associated with using the system. The WebERP has a wide variety of features suitable for managing even complex business processes such as multiple inventory locations, multiple currencies, lot and serial number tracking of inventory. All the features in webERP are integrated with each other and therefore inputs are required just once and everywhere the change is propagated across the system.

(iii) Document Management Information System (DocMIS) ï sample software is OpenDocMan-version1.2.6.2. This is a free PHP web based Document Management System (DMS). It has automated document review process and automated file expiration process. Reviewer can approve or reject a new document or a changed document and e-mail notification options prior to and after a review. In this OSIS, it is possible to add any file type to the system and no File Transfer Protocol (FTP) required i.e. user can upload directly from the browser.

(iv) Customer Relation Management Information System (CRM) ï sample software is vtigerCRM-version5.4.0. This is an open source Customer Relation Management (CRM) that includes sales, service & marketing modules, and ERP modules for inventory and projects.

(v) **Student Management Information System (SMIS)** ï sample software are openSIS-version 4.2 and ZALONGWA. These are the student information systems developed and maintained by Open Solutions for Education (OS4Ed) and Zalongwa Technologies Ltd respectively. They are based in PHP and MySQL platforms and they run in both Microsoft Windows and Linux operating systems.

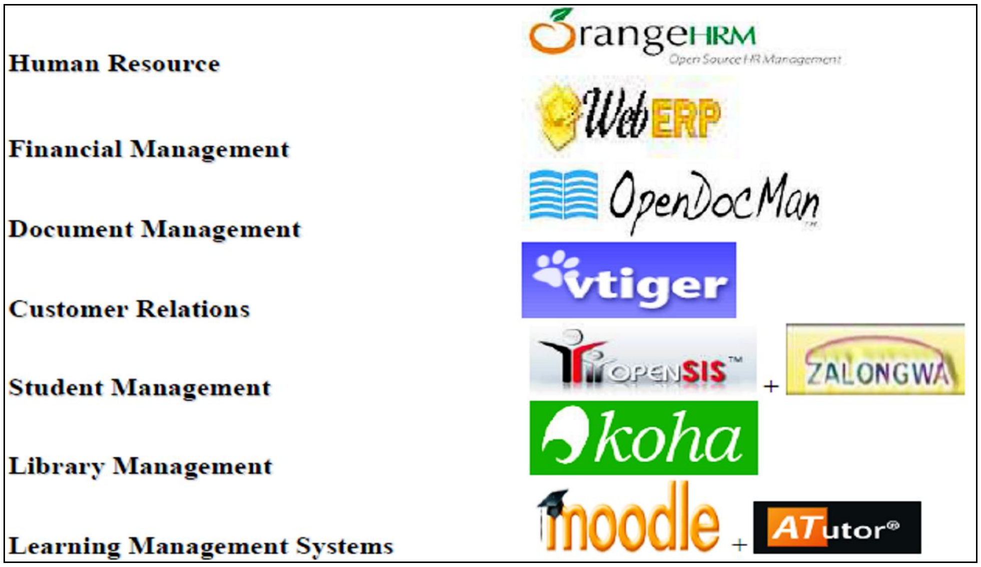

Figure 3: The Investigated OSIS Software

(i) Library Management Information System (LIBMIS) ï sample software is KOHA-version3.10.1. This is an Integrated Library System (ILS) that uses dual database design which utilizes the strengths of the two major industry-standard database types (text-based and Relational Database Management Systems (RDBMS)). It is a web based and truly platform independent solution distributed under the open-source General Public License (GPL), hence no vendor lock-in.

(ii) Learning Management Information System (LMS) ï sample software are MOODLE-version2.4.1 and ATutor-version2.0.3. These are the Open Source Web-based Learning Content Management System (LCMS) used to develop and deliver online courses. They are distributed under the terms of the GNU license. The acronym MOODLE is for Modular Object-Oriented Dynamic Learning Environment.

RESULTS AND DISCUSSION

Driving Factor towards OSIS Adoption

One of the aims of this study was to establish the motivation behind the adoption and use of OSIS systems by organizations in Tanzania. The study revealed that although the low Total Cost of Ownership (TCO) is a major driver for OSIS adoption among adopters, the results, however, suggest that this is not the only deciding factor. For instance, in implementing the project on financial management, the organization U purchased proprietary financial software called ACCPAC from CATS Tanzania Ltd contrary to its ICT policy which clearly advocates the OSIS usage.

The ICT Security Trainings and Software Developments

In this study, we sought to find out if the ICT security trainings are carried out and where the trainings are conducted, we evaluated its contents to determine whether it covers all aspects of ICT security. As part of observation of this study, it has been discovered that the trainings that are targeted to both technical and end users are either completely lack coverage in security or when the security is covered the contents reflect network security only. This has left out most of the OSIS programmers with less or completely lack of software security skills.

One of the reasons that caused this to happen is the tendency of the systems administrators to relax as far as the functional requirements are met and the system is up and running. They do not keep track of further OSIS development, so in such situation, a move and migration to a new and more stable version is not guaranteed. We found that most of the installed OSIS are old, outdated and obsolete from security perspective; therefore they are susceptible to malicious attacks.

Another security aspect is concerning with the OSIS accounts creation and password management among end users. Easy to guess and weak passwords have been common due to lack of security skills among end users. This create critical danger to systems, for instance, if hacker can guess a weak password created by less skilled user (ñteacherò) in a MOODLE Learning Management System, hacker can then be able to acquire administrative privileges using the default settings and can do anything of interest in the system. So for the organizations which are using OSIS systems, the password management should be ensured up to the level of end users as hackers just need a single entry point to the system to gain administrative power.

For some organizations which have developed their own OSIS from scratch using in house expertise, we found that they lack a best practice of the *Many-Eye-Balls Phenomenon* to give chance for security review of their written source codes. This is an important aspect in OSIS security because software is released with source codes.

The practice in some other organizations which opted to outsource their OSIS, have shown that vendors are granted administrative privileges even when the software is already in use and contain very sensitive information. This places a considerable potential risk to organizationôs assets especially when vendors recruit cheap labors who work for them in a temporary basis.

Due to existing technical gap between systems administrators and the software vendors, it has been discovered that some vendors tend to hide configuration tricks for various business reasons which left the systems administrator with little knowledge of what has been put within a system. So, if the vendor is not ethical, there is possibility of hacking and exploiting the system all the time after software delivery to the organization. This is possible through remote access by applying hidden authentication parameters.

Another important security aspect that fall under software development is the security capacity and perception of local software vendors. Most of the local vendors consider security as an add-on feature. While they are designing the software on the first place, the emphasis is always given to the systems functionality and usability properties. The security requirements are only defined at a limited level of authentication where the focus is in usernames, passwords and access rights. However, since OSIS depend on mobile codes which are created by different authors being both ógood guysô and óbadguysô, it becomes challenging for administrators to separate clean codes and be able to incorporate changes into the program. As a result, OSIS systems are left with many security flaws which can attract hackers. To wind up this discussion, the software development requires multidisciplinary skills from both software programming and software security. One of the causes of the existing technical gap between the security experts and software programmers has been due to the poor design of the computer science curricula where the security courses focus only on the network rather than software security. It should be clearly noted that in this new world of open source applications, network is not the only access hackers need to perform malicious activities.

The Staff Ethics and Observance of Professional Codes of Conducts

This aspect is of vital importance especially in the environment where the OSIS are alternative solutions. In that situation, organizations must be confident of the people who are managing the systems since these people are able to play with and manipulate the source codes and therefore can make the software misbehave in a certain period of time. The study revealed that people have been given systems to manage because of their ICT skills and ability and not because they are trusted. It has also been discovered that the seminars on staff ethics and professional codes of conducts are not practiced in most organizations. So, since the source codes are accessible by administrators, the organizations are uncertain whether the codes are manipulated or not.

Untrustworthy of OSIS Sources and Support

From their very nature, the OSIS are publicly developed and therefore one OSIS can be available from multiple sources. It was the interest of this study to understand the capacity of the adopting organization in sourcing the OSIS software. It was however found that the organizations face difficult in finding the secured source of the OSIS software. The practice shows that the URLs (Uniform Resource Locators) are trusted, but who is to say that a certain website exists? Also organizations have no habit of checking the veracity of downloads. It is very possible to download a file named ñwebERPò assuming that it is financial system but in reality it is a malicious code.

In addition to that, based on the fact that the OSIS software supports depend very much on the community which provide sources of the OSIS source codes that cannot be easily verified some systems administrators tend to find their own way to find solutions and support through public internet mailing lists. This creates the possibility of revealing organizational confidential information or receives support from both 'badô and ógood guysô that may introduce new security bugs.

The Adoption of Immature OSIS Software by Organizations

The study informs that 9 out of 15 visited organizations have attempted to download and customize the software which have not reached functional maturity stage. It was also discovered that 38 out of 52 downloaded OSIS systems were just provided as early versions released as technology previews, which are normally intended to experienced technically developed people for software testing and improvement. It has been difficult for the organization to measure fitness for purpose and interoperability of the OSIS software. For instance, the organization U which has already embarked on the use of OrangeHRM faces difficult to integrate it with its other information systems in the organization. The module that support software integration has closed source codes and therefore the implemented system is no more extensible and fail to retain the OSIS fundamental property of open source codes.One of the key lessons here is that the organizations opt to take advantages of readymade OSIS and therefore tend to skip significant software development stages which bring critical risks.

The OSIS Accounts Management - Dead Link between Software Section, HR and User's Departments

This is the general problem observed from most visited organizations where the accounts management is treated in unprofessional way i.e. the requests, issuances and closing of OSIS accounts do not follow proper channel and in most cases is left as an individual task. The consequence of this is that; a staff continues to own username and password even if are already retired, transferred, changed job position or died. This is very dangerous act for information security in the organization.

Organization's Security Considerations

Another facet studied during undertaking this study was the extent of security consideration in the signed contracts between organizations and their consulting firms. The results show that about 8 out of 11 screened Terms of References (ToRs) in the legal contracts and Service Level Agreements (SLAs) for software acquisition and support do not include information security responsibilities. It was even difficult to site the word security in the sampled staff job descriptions of the visited organizations. All 15 organizations lack officer in charge of security. However, 3 organizations have employees with security expertise but their job descriptions do not reflect any security responsibilities.

Technical OSIS Code Reviews and Systems Audit Logs + Data Auditing

In this aspect, the interest was to observe whether organizations perform monitoring and evaluations of its systems and data. It was learnt that all 15 organizations lack procedures to review the source codes. So, the organizations are uncertain on whether the source codes are distorted for illegal purposes or not. However, it was noted from 17 systems administrators practice routine accounts status, privileges and access authorizations. The code reviews are totally left out.

On the systems features, it was observed that apart from famous and publicly downloadable OSIS systems such as KOHA, OrangeHRM and MOODLE, other software which are either in house or locally developed lack audit logs which are vital in tracking each action performed by registered user in the system.

Furthermore, most of the installed OSIS systems have quiescent documentation which does not accommodate any new configurations and code changes which happen regularly as a result of OSIS mobile codes.

The OSIS Preconfigured Default Settings

Normally OSIS comes with preconfigured default settings which must also be customized to suit both functional and security requirements. It was discovered that the systems administrators leave most of the default settings untouched. Through exploitation of these settings, hackers can easily get access into the system.

Security Vulnerabilities of the acquired OSIS Systems by various Organizations in Tanzania

The most common observed security vulnerabilities of the OSIS systems are Cross-Site Scripting (XSS), security bypass, SQL Injection, Cross-Site Request Forgery *(*CSRF) and PHP Code Injection, Authorization Vulnerabilities and Arbitrary File Upload.

Cross Site Scripting (XSS) Security Vulnerabilities

We have found that in the orangeHRM, the public file **jobs.php** of recruitment module is exposed to provide unauthenticated attacker to gain administrative privileges. It has also been discovered in the Employee Social Service (ESS) module, user inputs are not sanitized in such a way that malicious ESS user can also gain administrative privileges.

In some universities which are using MOODLE as their LMS, the MNET access control interface has a persistent XSS vulnerability which happens when server allows extended characters in usernames. This system has also XSS vulnerability in the file**blog/index.php**where some parameters are not being properly cleaned on the blog index page, allowing non-persistent XSS attacks. In the global search engine, MOODLE has a reflexive XSS which is a problem in handling of user submitted data in global search forms. This problem is exploitable only when global search is enabled. However, by default the global search feature is disabled. When using a *login-as* feature in MOODLE, users may trick admins to edit some existing posts which contain XSS exploit code. Apart from MOODLE, another LMS called ATutor has multiple "cid" parameter XSS Vulnerabilities where the system fails to properly sanitize user-supplied input.

On the other hand, the vTigerCRM allows XSS by modifying the parent tab URL parameter value when it is possible to include malicious JavaScript presented to the user. The locally developed Student Academic Register Information System (ZALONGWA-SARIS) seems to fail in validating user input where all sorts of chaos are possible if a user passes unexpected content to a PHP script. The system also fails to validate user inputs in the excel import facility which results into uploading ghost data. However, validation of user inputs through web forms is done through use of java scripts technology from the client side.

Security Bypass Vulnerabilities

In this type of vulnerability, the orangeHRM tends to allow users with 'ESS' privileges to view or modify Time Mod, Benefits Mod, Leave Mod, PIM Mod, or Admin Mod information. The MOODLE has a KSES[1] Security Filter Bypassing vulnerability. This is a critical vulnerability in KSES text cleaning filter which may allow registered users to launch persistent XSS attacks.

SQL Injection Vulnerabilities

In the orangeHRM, the authenticated ESS users can perform SQL injection attacks, leads to unauthorized access to sensitive data, or arbitrary code execution. In WebERP, attacker can inject SQL codes when exploiting CSRF vulnerability especially when the HTTP requests are not filtered. In vtigerCRM, a malicious user may exploit this vulnerability to disclose potentially sensitive information or modify the underlying database. In MOODLE, data may be passed through **add_to_log()**function without being sanitized properly, this could allow SQL injection type attacks if there are any instances of wiki in the courses. ATutor allows 'links' blind SQL injection/admincredentials disclosurewhere remote attackers can inject arbitrary SQL statements into the statements used by the product through the use of the links parameter.

The CSRF and PHP Code Injection Vulnerabilities

The CSRF is a possibility of an attacker to add new administrator in the system. This happens in orangeHRM which does not have security measures implemented in the software against CSRF attacks. The remote attacker can trick an administrator to visit a malicious site; the attacker can perform privileged operations, or exploit PHP code injection vulnerability that can be found in the mail administration module. The successful exploitation of these vulnerabilities can lead to arbitrary code execution.

[1] KSES=òKses Strips Evil Scriptsò (*HTML Filtering Mechanism*)

The CSRF also happens in MOODLE Quiz reportswhere only limited validation is being done for one of the parameters, allowing unauthorized deletion of attempts in some instances.

The Authorization Vulnerabilities

The authorization vulnerability occurs in OrangeHRM in which the timesheet, attendance, HSP, recruitment, and leavemodulescontains bugs in the authorization code; from which the authenticated ESS users can access sensitive information, or perform privileged operations.

The Local File Disclosure and Arbitrary File Upload Vulnerabilities

The local file disclosure has been tested in the vTigerCRM in which the flaw is caused by lack of input validation of the file URL parameter when evaluated in the **CommonAjax.php** file. By modifying the file parameter path, and in turn terminating it with a NULL byte, it is possible to trick **CommonAjax.php** into including files which do not include ó**.php**ô in the file name.

In the same system, a malicious user can upload and execute malicious PHP files. The vtigerCRM has functionality to prevent users from uploading files with a ñ**.php**ò extension but this restriction may be bypassed by uploading a file named in upper case such as **SUPPLY.PHP** or ñ**.phtml**ò which is often associated (by default) with PHP files in many LAMP servers. This vulnerability also happens in KOHA and OpenSIS.

The table 3 summarizes these security vulnerabilities against OSIS software.

Table 3: Security Vulnerabilities against OSIS Systems

SN	Type of OSIS Security Vulnerability	Observed in OSIS System
1	Cross-Site Scripting (XSS)	OrangeHRM, MOODLE, ATutor, vTigerCRM, ZALONGWA
2	Security bypass	OrangeHRM, MOODLE
3	SQL Injection	MOODLE, ATutor, vTigerCRM, WebERP
4	Cross-Site Request Forgery (*CSRF)*	OrangeHRM, MOODLE
5	PHP Code Injection	OrangeHRM, MOODLE
6	Authorization Vulnerabilities	OrangeHRM
7	Local File Disclosure and Arbitrary File Upload	vTigerCRM, KOHA, OpenSIS, OpenDocMan, MOODLE

CONCLUSION

This study focused on the critical evaluation of the existing practices for OSIS adoption, customization and use by organizations. Despite the fact that the rate of investing in OSIS systems is increasing in Tanzania, no security measures are seriously taken to protect these systems. Organizations which have sourced their sensitive information in this kind of technology are exposed to high risks associated with poor OSIS configurations and customizations and/or deliberate and accidental actions by people which are a result of lack of strategies to guide the adoption and usage of web-enabled OSIS systems. This study reveals that although some

Tanzanian organizations have already invested in OSIS systems, there is a possibility of organizations to fail in attaining the intended benefits.

Acknowledgement
I would like to express my sincere gratitude and many thanks to my little growing family for their vital encouragement, the OUT management for support and all other colleagues who contributed in one way or another in undertaking this work.

References

Bakari, J. K. (2007). ñ*A Holistic Approach for Managing ICT Security in Non Commercial Organizations*ò, A Case Study in a Developing Country; PhD Thesis, Stockholm University, Sweden, ISBN - 91-7155-383-8.

Lungo J. H. and Kaasbøl (2006). ñ*Experiences of open source software in institutions: Cases from Tanzania and Norway*ò.

Mitchell, C. (2004). ñ*Understand your open source software options*ò, http://www.cioupdate.com/trends/article.php/3419381, Date Accessed: February 23, 2012

The United Republic of Tanzania (2003). *National ICT Policy*

Schneider, F. B. (2000). "Open Source in Security: Visiting the Bizarre." Proceedings of the 2000 IEEE Symposium on Security and Privacy (the Oakland Conference), Berkeley, CA. Los Alamitos, CA: *IEEE Computer Society*. pp. 126-127.

TAFOSSA (2003). http://www.tafossa.or.tz/, DATE Accessed: Saturday, 29 March 2008

TAFOSSA (2003). www.tanzaniagateway.org/docs/**TAFOSSA**_OverView.pdf ,

DATE Accessed: Monday, 28 January 2013

Viega, J. and McGraw, G. (2002). *Building Secure Software*. Addison-Wesley, ISBN 0201-72152-X.

Yin, R. (1989). ñCase Study Researchò. Sage Publication, California, pp: 22-26.