PENETRATION TESTING FOR LIBYAN GOVERNMENT WEBSITE

Rabia Ihmouda Hassan[1] and Najwa Hayaati Binti Mohd Alwi[2]
[1]Universiti Sains Islam Malaysia, rbhamouda@yahoo.com
[2]Universiti Sains Islam Malaysia, najwa@usim.edu.my

APSTRACT: The study explores the security issues in the Libyan Government websites focusing on assessing the vulnerability and security weaknesses of various websites of the Libyan Government ministries. The study is divided into three stages. In the first stage, literature review was conducted to understand the nature of the problem. Data were collected in the second and third stage of study. In the second stage, three Web application scanner tools were used for checking and evaluate the government websites for common vulnerabilities, and analyzing security level for each of these websites. In the last stage, more insight into the security related issue of the Libyan government websites is obtained through interview with the expert. Using these two methods, a deeper understanding of the status of security level in the Libyan government's websites is presented from the standard security point of view and the need for a research to address and overcome the problem is also asserted.

Keywords: E-government, Information Security, Website Vulnerability

INTRODUCTION

The concept of an e-government is to provide access to government services anywhere at any time over open networks. It has a potential to bring about higher quality and more cost effective government, besides the better relationships between citizens and the government. The purpose of e-government is to set up new internal and external communication channels, to simplify administrative procedures and to enhance the accessibility of services and information (German Development Institute, 2003).It is believed that the implementation and policymaking of governments can be transformed with the help of ICT by replacing traditional services with computerized ones. Since the e-government uses the tools and systems of ICT(Moise & Popa, 2008), therefore the security and protection of privacy is important in the e-government.

The term 'Security' generally refers to the protection of information system assets and control of access to information. Without the assurance of security to the privacy nobody would be prompted to use e-government. According to Cenzic (2009), the web is becoming a dominant threat to computer security. In the second half of 2009, 82% of the reported commercial vulnerabilities were related to web technologies (higher than 78% in the first half of the 2009). According to Maple et al. (2010), in the report of the cases investigated by SAFE UK, 86% of the attacks exploited vulnerability in the web interface, while only 14% targeted other parts of the infrastructure. Attackers know that valuable data passes through the web, and the web interface is accessible to outsiders, thus making the web a logical point of attack. Therefore, websites owner need to pay attention to some high-risk vulnerabilities that may endanger the reliability and integrity of their websites.

According to OWASP (2013), the following vulnerabilities account for the majority of the common web application security breaches:

1. Injection
2. Broken Authentication / Session Management
3. Cross Site Scripting /XSS
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross Site Request Forgery
9. Using Components with known vulnerabilities
10. Invalidated Redirects and Forwards.

Arab countries have been using ICT as well to improve the effectiveness and efficiency in communication and providing services. Gebba & Zakaria (2012), summarizes various e-government challenges in Arab countries. Some of the major challenges faced by the Arab countries include:

1. Limited studies and research on various aspects of the e-government in Arab countries.
2. Lack of trust in accomplishing tasks online amongst the government employees.
3. The security and privacy concerns (the lack of security of information).

Security has been highlighted as one of the main challenges needs to be addressed and implemented for a successful e-government web application, it is expected that the Libyan government and concerned authorities would pay adequate attention to the issue. However, this issue of security is overlooked in Libya by the government website developers. These has led to security threats exposure and some of the Libyan government's websites were attacked. Very recently, the Libyan Prime Minister's website was hacked by Algerian hackers (Alwatan Libya, 2012), and Nic.ly, the site of Libya's top level domain (TLD) name registry, was also defaced by hackers (Schroeder, 2012).

Currently the security status of Libya Government website is unknown. This study aims to investigate this status as well as the security vulnerabilities and weakness that endangers the security of sensitive data and affect the implementation of e-government services in Libya.

This paper consist of three objectives:

- To investigate the current security status in Libyan e-governments.
- To investigate the reasons to such security vulnerabilities and weaknesses.
- To suggest ways to address and overcome these issues.

This paper will focus on the security levels of e-government Web applications and scope of vulnerabilities emphasized is limited to Web sites for Cross Site Scripting (XSS) and SQL injection vulnerabilities. Moen et al., in 2007, had highlighted that the majority of dynamic e-government web applications had vulnerabilities exploitable by XSS or SQL injection. These two vulnerabilities have become the top three security breaches in 2013 (OWASP, 2013).

Due to the time and access limitation, this study focus on the following three Libyan government websites for the study. The selected websites of the Libyan government ministries are listed in Table1.

Table 1. List of the websites under study

No	Name of the Governmental website	Website URL
1	Libyan government – Prime Minister's Office	http://www.pm.gov.ly
2	Ministry of Defence	http://www.defense.gov.ly
3	Ministry of Transportation	http://www.ctt.gov.ly

At the end of this paper, a brief idea about the current status of the Libyan e-government services will be discussed. This includes the nature and the level of the security vulnerabilities and weaknesses found in the Libyan government's websites. In addition, recommendations for approach in addressing and overcoming these security vulnerabilities will be proposed.

LITERATURE REVIEW

E-government Concept

Abramson & Means (2001) defined E-Government as – the electronic interaction (transaction and information exchange) between the government, the public (citizens and businesses) and employees. The term "e-government" refers to the delivery of government information and services via the web, email or other digital sources. E-government consists of the creation of a website where information about political and governmental issues is presented(Alshboul, 2012).

E-Government is a new invention and has been introduced to the developing countries in different ways. It embodies design and implementation characteristics of its original context (Heeks, 2006). The inherent properties determine its success when implemented in different transfer contexts. It is therefore imperative to understand and approach e-Government with respect to the transfer context. Otherwise, e-Government projects may fail because of a large difference between design and contextual reality (Heeks, 2005).

The E-government offers many benefits and opportunities for governments. However, the ability of developing countries to obtain the full benefits of e-government is limited and is largely restricted due to various political, legal, social and economic barriers (Ndou, 2004). It is important to note here the views of Heeks, (2003) who states that most ICT programs such as e-government in developing countries fail with 35% being classified as total failures and 50% partial failures.

Attempts are done at many levels about how technology can be deployed to serve the citizens in better way by the governments. Many research studies exist today on the various issues related to e-government. However, while implementing the e-government, issues of the web security are also becoming increasingly important and many research studies are taking place on the issue to overcome this problem by finding out viable security framework. The following sections of this paper offer a review of these research studies related to the topic of the research in order to understand the problem in better way.

E-government and its Implementations in Libya

E-government is becoming common in most of the countries around the world including developed and developing countries. According to Rorissa & Demissie (2010) the rate of adoption of e-government in developing countries is low due to several factors. The factors include infrastructure, literacy, economic development, and culture. Most of the Arab countries share many similarities on social, political and cultural levels with such developing countries.

As the e-government model was introduced relatively late in most of the developing countries, Libya was no exception to this. Shahahti & Dwivedi (2012) report that before 2005 Libya did not have a notable web presence. But, since then, Libya has implemented several government websites and e-projects, and also has significantly increased its global web ranking.

According to Saadi and Almahjoub (2012) e-government implementation in Libya has not achieved the desired aims and there is a vast scope for the development for such projects. And they conclude that thee-government can be quickly deployed in Libya because of its less population and high literacy rate among the citizens. Thus, a careful planning, intelligent utilization of resources and government-centric focus can boost up the process of making Libya a developed country in this respect.

However, as the implementation of e-government implies providing access to government services from any place and at any time over open networks, this leads to issues of security and privacy in the management of the information systems. And as e-government security is considered one of the crucial factors for achieving the advanced stage of e-government, a lot needs to be done in this field.

Information Security

As the successful implementation of the e-government depends on the viable web security, all the concerns related to it need to be addressed. This is because information security contributes directly to the increase in the level of trust between the government's departments and the citizens by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information. In this regard web security evaluation is considered as an important way for resolving web security related issues and concerns.

Many studies exist today on the issue. In this respect only, Xie and Aiken (2006) proposed a static algorithm to detect the vulnerability on PHP scripting language, used for building server-side web applications most widely. Posthumus and Solms (2004) also introduced a framework for information security for government. They highlighted the importance and the need of protecting business information for the organization by exploring several fundamental concerns that should be taken into consideration in this regard. Hong et al. (2003) also have introduced an integrated system for understanding information security management, explaining information security management strategies, and predicting management outcomes.

The study and methodology proposed by Saha et al. (2010)is also worth mentioning in this respect. They proposed a methodology to formulate the security architecture of the different G2C applications. According to them, this methodology can be used for the development of the G2C applications in a model-driven manner. Thomas et al. (2009) proposed an algorithm called PSR, which aimed to remove SQL injection vulnerability which allows unauthorized hacker to access the database and steal valuable information from the database.

With such studies, it is clear that a lot more research is needed to be done because of the changing parameters of the technology. A viable risk assessment system is a solution which needs to be sought. This is because risk assessment provides organizations with an accurate evaluation of the risks to their assets. It can also help them prioritize and develop a strategy to reduce risks and protect the data.

In computer security, vulnerability is a weakness that allows an attacker to reduce a system's information assurance. Thus, the measure of risk management can determine the effect of such threat. In this regard, web security scanner tools could test web applications automated for common security problems such as XSS, SQL Injection, remote command execution vulnerabilities.

Web Security Scanner Tools

Web security scanners can look for a wide variety of vulnerabilities. These tools are used to assess the security risks in the information systems. A risk exists when there is a possibility of a threat to exploit the vulnerability of a valuable asset. Thus, the following three web security scanner tools need to be mentioned (Shi et al., 2010).

N-Stalker web application Security scanner

N-Stalker web application security scanner 2012 is a web security assessment solution developed by N-stalker.

Acunetix Web Vulnerability Scanner (WVS)

Acunetix WVS is an automated web application security evaluation tool that audits web applications by checking for exploitable hacking vulnerabilities. Acunetix WVS scans a lot of vulnerabilities including the high-risk SQL injection vulnerability and XSS vulnerability.

Nessus vulnerability scanner

Nessus vulnerability scanner has high speed discovery, configuration auditing, sensitive data discovery and vulnerability analysis of security posture. Nessus gives a detailed evaluation report of the vulnerabilities, such as vulnerabilities summary and description, the reason why the sample site has vulnerabilities and their solutions.

METHODOLOGY

This study adopted mixed method. The quantitative method is used to get the data and result from the scanner tools about the vulnerabilities. Data collected is analyzed using descriptive statistics analysis. The qualitative method is used for gaining data from the expert. Interview data is analyzed using brief thematic analysis. Achieving the research aim, this study was conducted in three stages:

The first stage was to collect the data for understanding the nature of the problem by review of the research related literature, that to gain better understanding of the research problem and understand the views of various scholars about the issues related to the selected topic.

The second stage is assessing the vulnerability of the selected websites and their security weaknesses by using web application scanner tools. This stage focused to investigate the security levels of e-government website as listed in Table 1 for XSS and SQL injection vulnerabilities. It is important to note that selecting a vulnerability scanner for web services is a very difficult task as different scanners detect different types of vulnerabilities (Vieira, et al 2009).Three web applications scanner tools were used to investigate the vulnerabilities and weaknesses of these websites, these tools are:

1. N-Stalker web application security scanner,
2. Acunetix web vulnerability scanner (WVS),
3. Nessus vulnerability scanner.

These tools starts with typing the URL of the studied websites, then the tools will analysis it page by page, finally will come out by report that show the vulnerability level of these websites.

The last stage is to understand the security related issues faced by the Libyan Government websites. In this stage data were collected using interview method. An interview was conducted with expert that manage the security issues of the Libyan government’s websites. The interviewee was the e-government program coordinator in the Libyan Prime Minister’s office. This person is in charge for Libyan E-government project for three years. The interview was structured and questions asked included:

[Questions focusing on general information]

1. Where do you work currently?
2. What is your current job title?
3. What are your job responsibilities?
4. How many years of professional experience do you have of the current position and in IT field in general?

[Questions focusing on personal opinions on the security issues]

5. How would you describe the current status of Libyan e-government?
6. How would you describe the security issues faced while implementing the system of e-government in Libya?
7. Do you think that the Libyan government needs to focus more on information security for their e-government websites?
8. How would you describe the importance of information security for the Libyan e-government?

DATA ANALYSIS AND RESULT

The collected data were classified and analyzed. Data collected in the second stage is analyzed using descriptive statistics analysis. In the meanwhile, interview data is analyzed using brief thematic analysis. This included summarizing the important data of the interview and making useful recommendations based on it to solve the security problems in the Libyan E-Government websites for future work.

The results for second stage were fascinating as each of these tools used provided a report showing the overall security posture of the application. The report also provided details of the vulnerabilities classifying them into: low, medium and high severity vulnerabilities at present. The details of the each scanner tool are as follow.

N-Stalker Web application Security Scanner

N-Stalker Web application Security Scanner was applied on the websites under study. The obtained results are presented in the Table2. The table shows three main severity levels of the found vulnerabilities and the total number of each level for each websites.

In Table2, Libyan Government – Prime Minister's Office, the results that had been got was in 16 vulnerabilities which are considered as high severity level.

Table 2. N-Stalker Scanner Results

No	Name of the Website	Total number of severity risks		
		High	Moderate	Low
1	Libyan Government – Prime Minister's Office	16	5	0
2	Ministry of Defence	8	4	10
3	Ministry of Transportation	6	8	11

Acunetix Web Vulnerability Scanner (WVS)

The results obtained from the web vulnerability scanner (WVS) are shown in the Table3.

Table 3. A cunetixWeb Vulnerability Scanner (WVS) Results

No	Name of the Website	Total number of severity risks		
		High	Moderate	Low
1	Libyan Government – Prime Minister's Office	22	11	1
2	Ministry of Defence	0	1	7
3	Ministry of Transportation	9	4	6

In Table3, Libyan Government – Prime Minister's Office, the results that had been got was in 22 vulnerabilities which are considered as high severity level, and 11 vulnerabilities which are considered as moderate severity level.

Nessus Vulnerability Scanner

The results obtained from the Nessus vulnerability scanner tool are shown in the Table: 4.

Table 4. Nessus Vulnerability Scanner Results

No	Name of the Website	Total number of severity risks		
		High	Moderate	Low
1	Libyan Government – Prime Minister's Office	5	0	4
2	Ministry of Defence	2	1	7
3	Ministry of Transportation	0	1	2

In Table4, Libyan Government – Prime Minister's Office, the results that had been got was in 5 vulnerabilities which are considered as high severity level.

It is very clear from the results obtained from the tools that the Libyan government websites are at very high risk. The severity level of risk is quite high and is confirmed by all the three web scanners.

The second phase result

In order to get more insight into the security related risks to the government websites, the data was also collected through interview with the Libyan E-Government program coordinator. The aim was to get insight from the concerned person-in-charge and to know the government approach towards this issue. As expected, the collected data helped to understand the security status and other related issues as well as the Libyan government’s approach towards it from the perspective of the government.

When the concerned interviewed person was asked to describe the current status of Libyan e-government, it was reported that the government web presence is very weak at the present time. The Libyan government’ e-government program coordinator reported that the present government is still in transition phase and faces many challenges. It is not working in effective ways in certain situations due to many security and political instabilities. As the government is in the transition phase after the fall of the previous regime, various instabilities, technical and leadership challenges are creating many problems for in dealing with many issues including the issue of e-government services and system and its security. However, despite this, the new government is doing its best to invest in the e-government sector and implement the services as much as it can for the betterment of its citizens.

This response of the e-government coordinator helped in understanding the current status of the e-government and its security as well as challenges faced by the new Libyan government and its approach towards the e-government.

Focusing on the security related challenges faced by the Libyan government, when the coordinator was asked to describe security issues faced by the government while implementing e-government, it was reported that e-government faces many security risks and challenges. He reported that many governmental portals were subject to hacking. The underlying reasons for this problem and vulnerability were the lack of any national standards or guidelines for developing national websites.

This response of the Libyan e-government program coordinator helped in gaining insight into the security problems and vulnerabilities of the Libyan government websites and reasons underlying them. As the program coordinator acknowledged that the lack of any national standards or guidelines for developing national websites is the main source of the security risks, threats and vulnerabilities, something needs to be done in this regard.

Focusing on this issue, the program coordinator was asked if there was need for the government to focus on these information security issues of the government's websites. To this, the program coordinator replied positively and very strongly.

Because of his positive and strong reply in support of the information security for the government websites, he was asked to explain the importance of such security for the e-government and its websites. The program coordinator reported that the government is speeding up the initiatives for developing its web presence. However, he acknowledged that the government is not paying required attention to the security issues. There have been attacks on governmental portal which prove this fear, concerns and risks. Therefore, there is a strong need to develop a framework of national standard or guidelines for developing national websites.

FINDING AND DISCUSSION

As the study aimed offering insight on the current status of the Libyan E-Government from security perspective, and explaining the importance of security toward it, attempt would be made to summarize these results from security perspective. After looking at all the obtained results from the three selected scanner tools, it is clear that the Libyan government websites have been and are vulnerable to the security threats and risks. The following table offers a general overview of the severity level for the selected websites based on the results of these tools.

Libyan government websites are at very high risk. The severity level of risk is quite high and is confirmed by all the three web scanners result in Table5.

Table 5. The three Scanner tools Results

No	Name of the website	Severity level	N-Stalker	Acunetix	Nessus
1	Libyan Government – Prime Minister's Office	High	16	22	5
		Moderate	5	11	0
		Low	0	1	4
2	Ministry of Defence	High	8	0	2
		Moderate	4	1	1
		Low	10	7	7
3	Ministry of Transportation	High	6	9	0
		Moderate	8	4	1
		Low	11	6	2

This raises the serious information security concerns. Therefore, it is not surprising that these websites were subject to hackers' attacks and can also be due to the security vulnerabilities and weaknesses. Thus, there is very urgent need to address this issue for the protection of the sensitive data. However, from the analysis and the result of the data collected about the security status of the Libyan government websites, it indicated that the Libyan Government – Prime Minister's Office the most vulnerable website due to both high and moderate levels, it has 22 vulnerabilities on high level risk. Whereas the Ministry of Transportation has nine vulnerabilities on high level risk, and the Ministry of Defense has eight vulnerabilities on high level risk. Furthermore, many contradictory and unsatisfactory results were obtained from the tools and the interview. These include:

1. The government web presence is very weak in Libya.

2. The government is investing in speeding up the process of web presence without giving much required attention to the information security issue.
3. Many government websites face high risk vulnerability which endanger the reliability and integrity of these websites and can be prone to hacker attacks.
4. Many governmental portals were subject to hacking because of such security vulnerabilities, supported by Alwatan Libya (2012)& Schroeder(2012).
5. The Libyan government lacks a viable framework of national standards or guidelines for developing national websites which is also concerned as one of the underlying reasons for security issues faced by the government.

CONCLUSION AND FUTURE WORK

This study explored the security status and related issues in the Libyan Government websites. In particular, the vulnerability and security weaknesses in many Libyan Ministries' websites were focused and assessed. Assessing and evaluating the security level in those websites by using three Web application scanner tools; it was found that most of the Libyan government websites have high risk security vulnerability and weaknesses. Therefore, it is not surprising that some of these websites were subject to hackers' attacks due to such security vulnerability and weaknesses.

According to the E-Government program coordinator in the Libyan Prime Minister's office, the lacks a viable framework of national standards or guidelines for developing national websites in Libya is the main underlying reason for security issues faced by the Libyan government.

This security problem and lack of trust on the part of citizens is not limited to Libya only. It is the most common problem faced by many Arab countries as most of them share similar culture, values, education and technical challenges etc. Therefore, a more comprehensive research study needed to be done to investigate these security vulnerabilities and status of the e-government success in the Arab countries. Meanwhile, to conclude, there is an urgent need to address the information security vulnerabilities and weaknesses in the government like that of Libya by developing a security framework of nation standards for government. This framework will help in setting basic standards to be followed to achieve basic or minimum and reasonable and viable requirements of security of e-government.

REFERENCES

Abdallah, S., & Fan, I.-S. (2012). Framework for e-government assessment in developing countries: case study from Sudan. *Electronic Government, an International Journal* , 158 - 177.

Abramson, M., & Means, G. (2001). *E-Government, Pricewaterhouse Coopers endowment for the Business of Government.* Rowman & Littlefield Publishers Inc.

Alfawaz, S., May, L., & Mohanak, K. (2008). E-government security in developing countries: A managerial conceptual framework. *International Research Society for Public Management Conference.* Brisbane.

Almarabeh, T., & AbuAli, A. (2010). A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. *European Journal of Scientific Research* , 29-42.

Al-Shafi, S., & Weerakkody, V. (2009). Factors Affecting E-Government Adoption In The State Of Qatar. *European and Mediterranean Conference on Information Systems.* Abu Dhabi: EMCIS2010.

Alshboul, R. (2012). Security and Vulnerability in the E-Government Society. *Contemporary Engineering Sciences* , 215 - 226.

Alwatan. (2012, September). *News Alwatan Libya*. Retrieved march 10, 2013, from Alwatan Libya http://www.alwatan-libya.com/more.php?newsid=24032&catid=1

Alwi, N. H.M, & Fan, I.S. (2010). E-Learning and Information Security Management. *International Journal of Digital Society (IJDS)* , 1 (2), 148-156.

Bagchi, K., & Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the Association for Information Systems* , 684-700.

BASU, S. (2004). E-Government and Developing Countries: An Overview. *International review of law computers & technology*, 109-132.

Carter, L., & Belanger, F. (2004). The Influence of Perceived Characteristics of Innovating on e-Government Adoption. *Electronic Journal of e-Government* , 11-20.

Cenzic. (2009). *Web Application Security Trends Reoprt q3-q4.* Cenzic Inc.

Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. (2006). E-Government Strategies in Developed and Developing Countries: An Implementation Framework and Case Study. *Journal of Global Information Management* , 23-46.

Commonwealth Telecommunications Organisation. (2002). Success and Failure in eGovernment Projects Retrieved May 10, 2013, from Development Information Exchange Project Website: http://www.egov4dev.org

Gebba, T. R., & Zakaria, M. R. (2012). E-Government in Egypt: An Analysis of Practices and Challenge. *International Journal of Technology and Management* , 11-25.

German Development Institute (2003). E-Government – an Approach to State Reform in Developing Countries? Briefing Paper.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *2004 CSI/FBI Computer Crime and Security Survey.* San Francisco: Computer Security Institute.

Heeks, R. (2006). *Implementing and Managing eGovernment: An International Text.* London: Sage Publications.

Heeks, R. (2005). e-Government as a Carrier of context. *Journal of Public Policy* , 51-74.

Heeks, R. (2003). *Most egovernment-for-development projects fail: How can risks be.* Institute for Development Policy and Management. University of Manchester.

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An Integrated system theory of information security managment. *Information Management & Computer Security* , 243.

ITGI. (2006). *Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd Edition.* Rolling Meadows-USA: IT Governance Institute.

Karokola, G., Yngström, L., & Kowalski, S. (2012a). Secure e-Government Services: A Comparative Analysis of e-Government Maturity Models for the Developing Regions – The Need for Security Services. *International Journal of Electronic Government Research (IJEGR)* , 1-25.

Kessler, K., Hettich, N., Parsons, C., Richardson, C., & Triana, A. (2011). A Framework for Assessing Privacy Readiness of e-Government. *Centre for Development Informatics Institute for Development Policy and Management* .

Maple, Bhala, S., Christodoulides, M., Cornwell, L., Jones, R., & Morris, B. (2010). *UK security breach investigations report: An analysis of data compromise cases security breach.* 7safe Retrieved May 10, 2013 from http:// www.7safe.com/breach_report

Moen, V., Klingsheim, A. N., Simonsen, K. I., & Hole, K. J. (2007). Vulnerabilities in e-governments. *International Journal of Electronic Security and Digital Forensics* , 89-100.

Moise, M., & Popa, V. (2008). Types of methods and researches used in e-government systems/applications. *" National Institute for Research and Development in Informatics Bucharest, Romania Journal of Information Systems & Operations Management* .

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security* , 580–584.

Ndou, V. (2004). E–government for developing countries: opportunities and challenges. *The Electronic Journal on Information Systems in Developing Countries* , 1-24.

WASP. (2013). *OWASP Top 10 - 2013 The Ten Most Critical Web Application Security Risks*. Retrieved March 25, 2013, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Posthumus, S., & Solms, R. v. (2004). A framework for the governance of information security. *Computers & Security* , 638-646.

Rorissa, A., & Demissie, D. (2010). An analysis of African e-Government service websites. *Government Information Quarterly* , 161-169.

Saadi, M., & Almahjoub, A. (2012). E-Governance in Libya – Where we are and Where to Go. *The International Libyan Conference on Electronic Government.* Tripoli – Libya.

Saha, S., Bhattacharyya, D., Kim, T.-h., & Kumar, S. (2010). Model Based Threat and Vulnerability Analysis of E-Governance Systems. *International Journal of u- and e- Service, Science and Technology* , 7-22.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal* , 60-66.

Schroeder, S. (2012). *yahoo news*. Retrieved march 12, 2013, from yahoo: http://news.yahoo.com/libyas-top-level-domain-name-registry-hacked-094014974.html (accessed date 12-3-2013)

Shahahti, S., & Dwivedi, A. (2012). Prospects for Progress: Increasing the efficiency of Libya's E-government through Knowledge Management. *The International Libyan Conference on Electronic Government.* Tripoli – Libya .

Shi, H.-z., Chen, B., & Yu, L. (2010). Analysis of Web Security Comprehensive Evaluation Tools. *Second International Conference on Networks Security, Wireless Communications and Trusted Computing.* (pp. 285- 289). Wuhan, Hubei: Conference Publications.

Singh, S., & Karaulia, D. S. (2011). E-Governance: Information Security Issues. *International Conference on Computer Science and Information Technology (ICCSIT'2011)*, (pp. 120-124).

Thomas, S., Williams, L., & Xie, T. (2009). On automated prepared statement generation to remove SQL injection vulnerabilities. *Information and Software Technology* , . Inform. Software Technol., 51: 589-598.

U.S 'E-Government Act of 2002. (2002, DEC 17). Retrieved MAY 10, 2013, from U.S Government Printing Office (GPO): http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf

UNDESA. (2010). *United Nations E-Government Survey 2010: Leveraging e-government at a time of financial and economic crisis.* New York: United Nations, Department of Economic and Social Affairs avalibale at http://unpan1.un.org/intradoc/groups/public/documents/un/unpan038851.pdf.

Varma, V. (2011). Cloud Computing for E-Governance, A white paper. *IEEE International Conference on Computer Science and Automation Engineering.* Hyderabad, India.

Vieira, M., Antunes, N., & Madeira, H. (2009). Using Web Security Scanners to Detect Vulnerabilities in Web Services. *Dependable Systems & Networks, 2009. DSN '09. IEEE/IFIP International Conference on* (pp. 566- 571). Lisbon: Conference Publications.

Xie, Y., & Aiken, A. (2006). Static Detection of Security Vulnerabilities in Scripting Languages. *15th USENIX Security Symposium* (pp. 179-192). Stanford University: USENIX Association.