Security Assessment of Libyan Government Websites

Abdullah Ahmed Ali, Mohd Zamri Murah
Center for CyberSecurity
Universiti Kebangsaan Malaysia
Malaysia
email: abdullah.alhanash@gmail.com
zamri@ukm.edu.my

Abstract—Many governments organizations in Libya have started transferring traditional government services to e-government. These e-services will benefit a wide range of public. However, deployment of e-government bring many new security issues. Attackers would take advantages of vulnerabilities in these e-services and would conduct cyber attacks that would result in data loss, services interruptions, privacy loss, financial loss, and other significant loss. The number of vulnerabilities in e-services have increase due to the complexity of the e-services system, a lack of secure programming practices, miss-configuration of systems and web applications vulnerabilities, or not staying up-to-date with security patches. Unfortunately, there is a lack of study being done to assess the current security level of Libyan government websites. Therefore, this study aims to assess the current security of 16 Libyan government websites using penetration testing framework. In this assessment, no exploits were committed or tried on the websites. In penetration testing framework (pen test), there are four main phases: Reconnaissance, Scanning, Enumeration, Vulnerability Assessment and, SSL encryption evaluation. The aim of a security assessment is to discover vulnerabilities that could be exploited by attackers. We also conducted a Content Analysis phase for all websites. In this phase, we searched for security and privacy policies implementation information on the government websites. The aim is to determine whether the websites are aware of current accepted standard for security and privacy. From our security assessment results of 16 Libyan government websites, we compared the websites based on the number of vulnerabilities found and the level of security policies. We only found 9 websites with high and medium vulnerabilities. Many of these vulnerabilities are due to outdated software and systems, miss-configuration of systems and not applying the latest security patches. These vulnerabilities could be used by cyber hackers to attack the systems and caused damages to the systems. Also, we found 5 websites didn't implement any SSL encryption for data transactions. Lastly, only 2 websites have published security and privacy policies on their websites. This seems to indicate that these websites were not concerned with current standard in security and privacy. Finally, we classify the 16 websites into 4 safety categories: highly unsafe, unsafe, somewhat unsafe and safe. We found only 1 website with a highly unsafe ranking. Based on our finding, we concluded that the security level of the Libyan government websites are adequate, but can be further improved. However, immediate actions need to be taken to mitigate possible cyber attacks by fixing the vulnerabilities and implementing SSL encryption. Also, the websites need to publish their security and privacy policy so the users could trust their websites.

Index Terms—Libya E-government, Security Assessment, Information Security, Website Vulnerability, Penetration Testing

978-1-5386-7541-0/18/$31.00 ©2018 IEEE

I. Introduction

Internet technology has made a massive contribution to communication and information sharing. There is no doubt that the Internet has made people's lives easier and more convenient. Due to this, many institutions and organizations (both private and government sectors) see the ease in information sharing and offering online services, as an opportunity to improve efficiency, transparency, competitiveness and to survive in the global economy [1] [2]. Many organizations transferred traditional services into e-services. People can access such e-services online from any location, any time and cost-effective.

However, the rise of transferring into e-services brought a new security threat that could affect confidentiality, integrity and availability of information or even threat on the national security of a country. Sharing information by the private sectors could cause threats to a company, but for the government sectors, it could be more catastrophic. Therefore, government sectors need to be more concerned about sharing information and implementing e-services [3] [4].

There are many recent cyber attacks toward governments websites [3]. These attacks exploited various vulnerabilities in the operating systems, network protocol, data encryption, and web applications. As a result, many governments agencies suffered huge losses in term of sensitive data, loss of faith among the users and financial losses [5]. Therefore, there is an urgent need to assess and to evaluate existing government websites as a method to alleviate potential losses from cyber attacks [6].

Libyan government websites are also susceptible to cyber attacks [7]. Current, the is no effort to assess the security level of the websites. This is probably due to lack of security experts in Libya, or lack of security awareness among the government agencies. This situation is not good for Internet security [8].

Due to a lack of security assessment toward Libya government agencies in current literature, in this paper we took the initiative to conduct a passive penetration testing on Libya government websites. We followed a standard penetration testing framework for websites [9], [10], and also, assess the security policy of each website.

II. Methodology

Our security assessment methodology is based on a standard penetration testing guideline [11] [12]. The assessment and data collection were done in May 2018. The assessment was based on 16 Libyan government websites covering the domain gov.ly. The assessment consists of four stages as shown in Figure 1.

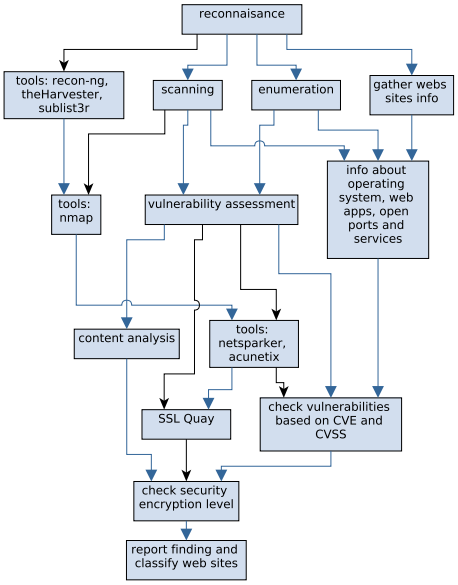

Fig. 1. The security assessment phases. This assessment consists of four major phases; reconnaissance, enumeration and scanning, vulnerability assessment, content analysis.

The first phase (Reconnaissance) is about searching for Libyan government websites under the domain gov.ly. We used an open source tool theHarvester to search for subdomains of gov.ly. The result obtained from theHarvester tool was about 742 subdomains. Based on our analysis, the main domains from 742 gov.ly subdomains were 37 Libyan government websites. After that, we verified these government websites one after the other manually by accessing their main pages. We verified if they were active and whether they were related to the current official government or not. We found that only 16 of the 37 Libyan government websites were active and related to the current Libyan government.

The second phase (Enumeration and Scanning) is about searching for sensitive information about the websites from the 16 Libyan government websites using nmap. This is to determine the security level of the websites. We tried to detect important information such as operating systems type, open ports, services and main IPs.

The third phase (Vulnerability Assessment) consists of two types of vulnerability assessment: web vulnerability scanning and secure socket layer (SSL) encryption evaluating. In web vulnerability scanning, we used two web security scanners namely: Acunetix and Netsparker to scan for web application vulnerabilities in the 16 websites. The scanners reported the vulnerabilities and classified them based on Common Vulnerabilities and Exposures (CVE) categories as: Critical, high, Medium, low and informational.

The second type of vulnerability assessment is evaluating SSL encryption of the 16 websites using Qualys SSL Labs rating. This evaluation classifies the websites into different rating: A,B,T, and No SSL. The rating depends on some factors such as: certificate validation, different protocols support, key exchange strength and cipher strength.

The fourth phase (Content Analysis) searches the websites for their published security and privacy policies. The search includes checking whether the policies are published in the main pages with clear links or not. The search was carried out manually by accessing each of the 16 websites and try to find the links for security and privacy policies. The fourth phase is not in any current security assessment framework, but our extra assessment for the websites.

III. Result and Analysis

A. Reconnaissance phase

In the Reconnaissance phase, we discovered 742 subdomain in gov.ly domain. We pick 16 websites for further analysis.

B. Enumeration and Scanning

In the scanning phase, we discovered operating system for 11 websites, running services from 16 websites, open ports on all 16 websites and IP numbers from 14 websites. Many of the websites are still using outdated operating system such as Linux 2.0 series and old version of Windows operating system.

This information is important because it could be used by cyber attackers to attack the systems. Counter measures should be implemented to hide the operating system, closes all unnecessary ports, stop unnecessary services and use web application firewalls to secure the websites.

C. Security assessment

The vulnerability assessment phase is divided into web vulnerability scanning and SSL encryption evaluation. The web vulnerability scanning used Acunetix and Netsparker to identify web application vulnerabilities. The scanning process would took a long time because the web scanner would crawl the websites and look for vulnerabilities one by one. These vulnerabilities are based on CVE and CVSS [13], [14], a commonly accepted ranking and description of vulnerabilities.

Based on these two scanners we identified 1 critical vulnerability, 24 high vulnerabilities, 139 medium vulnerabilities, 129 low vulnerabilities and 229 informational vulnerabilities from 16 websites. It was important to note that results from Acunetix and Netsparker were different

TABLE I
the vulnerabilities commonly found in the 16 websites and their criticality

vulnerabilities	number of occurance	level of risk
WordPress CMS	5	high
out of date PHP	2	high
Cross-site Scripting (XSS)	5	high
application error messages	78	medium
Cross-Site Request Forgery (CSRF)	4	medium
out of date jQuery	12	medium
PHP information disclosure	3	medium
PHP code execution and DOS	3	medium
User credentials are sent in clear text	2	medium

because each of them used different algorithms to find the vulnerabilities.

We also categorized the 16 websites based on the number of web vulnerabilities found. We have 1 website with 1 critical vulnerability, 7 websites have high vulnerabilities, 15 websites have medium vulnerabilities, and 15 websites have low vulnerability.

We discovered vulnerabilities both based on the web applications and the systems deployed. These vulnerabilities are shown in Table I. The table shows vulnerabilities commonly found on the 16 websites. The vulnerabilities classified by Acunetix and Netsparker into Critical, High, Medium, Low and Informational depending on Common Vulnerabilities and Exposures (CVE) scoring. The CVE is an accepted standard for publicly disclosed of cyber security vulnerabilities and exposures [13].

D. SSL encryption evaluation

The second type of assessment is SSL encryption evaluation using Qualys SSL Labs tool. This assessment rated the websites into 4 rating: A, B, T, No SSL. From the result, we found 3 websites rated A, 7 websites rated B, 1 websites rated T and 5 websites rated No SSL. The websites rated B have weaknesses in key exchange which may affect the encryption by allowing cyber attackers to perform man-in-the-middle attack (MITM) and gain access to the communication channel. We discovered that the T rated websites is one of the important websites that many users utilize in sharing private information. The website is rated T is because the expiration of SSL certificate used on the website, which may lead to a MITM attack.

E. Content Analysis

The Content Analysis phase showed that only 3 of the 16 websites provided links to security and privacy policies. One website indicated only published security policy for the whole organization but did not provide security policy for accessing websites. One website provided links of privacy and security policies, but the links were not working. The other 13 websites did not publish any privacy or security policies.

IV. Discussion and Contribution

Based on our security assessment of 16 Libyan government websites, we conclude that the current security websites of the 16 websites are adequate. There are only 24 high vulnerabilities and 1 critical vulnerabilities among the 16 websites. Also, we found that only 8 websites have critical vulnerabilities and above.

Based on SSL evaluation, we discovered only 3 websites have a proper SSL A-level accreditation while 13 other either have no SSL implementation or low level SSL-accreditation. This is a serious issue for the government agencies especially for government agencies that involves in financial or personal data transactions.

Based on our security assessment results from section III, we proposed a new safety classification matrix for the 16 websites using four safety categories: highly unsafe, unsafe, somewhat unsafe, safe. This classification will combine 3 different results from vulnerabilities analysis, content analysis and SSL encryption evaluation. The purpose of this proposed safety classification is to combine web vulnerabilities with SSL encryption evaluation and come up with a new safety ranking.

The safety classification model was based on Netsparker as a baseline. Our safety classification model is an overall evaluation of the security assessment based on web vulnerabilities, content analysis and SSL evaluation. In this model, a website safety is based on the number and the type of vulnerabilities found, the level of SSL implementation and the security and privacy policies implementation.

To measure a website safely level, we will first analyze each of the vulnerabilities for a website. Then, we determine whether a sensitive information is encrypted or not encrypted during data transaction using at that website. Finally, we determine the level of SSL encryption used on the website. Based on our analysis, we would then determine the safety level based on Table II. As an example, we have a website with 15 vulnerabilities (2 high, 5 medium, 0 low, 8 informational), a B-rated SSL implementation and no security and privacy policy. In this case, we would classify this website as B(unsafe) because the number of high vulnerabilities are low and B-rated SSL implementation.

Based on our analysis on the 16 Libyan government websites, we concluded that;

TABLE II
Classification of a website based on security assessment, SSL encryption evaluation and content analysis. In this classification, there are 4 level of safe. These levels are A(highly unsafe), B(unsafe),C(somewhat unsafe) and D(safe).

risk category	sensitive info	SSL rating A	B	T	no SSL
critical	unencrypted	A	A	A	A
	encrypted	B	B	A	A
high	unencrypted	B	B	B	B
	encrypted	C	C	B	B
medium	unencrypted	C	C	C	B
	encrypted	C	C	C	C
low	unencrypted	C	C	C	C
	encrypted	D	D	C	C
info	unencrypted	D	D	C	C
	encrypted	D	D	D	C

1) 1 website as highly unsafe. This website has 1 critical vulnerability and no SSL implementation.
2) 6 websites as unsafe. These websites have the number of high vulnerabilities more than 3 and B-rated or A-rated SSL implementation.
3) 8 websites as somewhat unsafe. These websites have the number of high vulnerabilities less than 3 and B-rated SSL implementation.
4) 1 website as safe. This website has 0 high and medium vulnerabilities and A-rated SSL implementation.

V. Conclusion

In this paper, we conducted a security assessment of 16 Libyan government websites under the domain gov.ly. This security assessment consists of four phases: Reconnaissance, Scanning and Enumeration, Vulnerabilities Assessment, and Content Analysis. In the reconnaissance phase, we obtained information about websites and verifying them. In the enumeration phase, we detected information about websites environments and network. In the vulnerability assessment, we used two types of assessments: web vulnerability scanning and SSL encryption evaluation. Also, we conducted a manual content analysis to find whether a website has a security and privacy policy, and whether the policy is published or not. Finally, we develop a safety evaluation model that combined vulnerabilities assessment, content analysis and SSL evaluation. The safety ranking would provide another info about the website security status. Based on the results, we highly recommend to the websites with high number of vulnerabilities to keep up to date with the latest security features to mitigate possible hacking attempts on their websites. They should also publish security and privacy policies for the websites in order to increase users trust in the websites.

References

[1] M. H. Othman and R. Razali, "Whole of government critical success factors towards integrated e-government services: A preliminary review," Jurnal Pengurusan (UKM Journal of Management), vol. 53, 2018.

[2] M. M. Yusof and A. Y. A. Yusuff, "Evaluating e-government system effectiveness using an integrated socio-technical and fit approach," Information Technology Journal, vol. 12, no. 5, pp. 894–906, 2013.

[3] J. J. Zhao and S. Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," Government Information Quarterly, vol. 27, no. 1, pp. 49–56, 2010.

[4] H. Kasimin, A. Aman, and Z. M. Noor, "Using evaluation to support organizational learning in e-government system: A case of malaysia government," International Journal of Electronic Government Research (IJEGR), vol. 9, no. 1, pp. 45–64, 2013.

[5] P. M. Tehrani, N. A. Manap, and H. Taji, "Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime," Computer Law & Security Review, vol. 29, no. 3, pp. 207–215, 2013.

[6] M. S. Al-Sanea and A. A. Al-Daraiseh, "Security evaluation of saudi arabia's websites using open source tools," in 2015 First International Conference on Anti-Cybercrime (ICACC). IEEE, 2015, pp. 1–5.

[7] R. Ihmouda, N. H. Alwi Mohd et al., "Penetration testing for libyan government website," in International Conference on Computing and Informatics. Universiti Utara Malaysia-Uum, 2013.

[8] A. R. M. Yusof, M. F. Sukimi, S. B. Ismail, and Z. B. Othman, "The cyber space and information, communication and technology: A tool for westernization or orientalism or both," Journal of Computer Science, vol. 7, no. 12, pp. 1784–1792, 2011.

[9] S. M. Srinivasan and R. S. Sangwan, "Web app security: A comparison and categorization of testing frameworks," IEEE Software, no. 1, pp. 99–102, 2017.

[10] N. Antunes and M. Vieira, "Penetration testing for web services," Computer, vol. 47, no. 2, pp. 30–36, 2014.

[11] G. Weidman, Penetration testing: a hands-on introduction to hacking. No Starch Press, 2014.

[12] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu, and A. Pretschner, "Security testing: A survey," in Advances in Computers. Elsevier, 2016, vol. 101, pp. 1–51.

[13] Y. Makino and V. Klyuev, "Evaluation of web vulnerability scanners," in Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on, vol. 1. IEEE, 2015, pp. 399–402.

[14] V. Basto-Fernandes, I. Yevseyeva, C. Silva-Rabadão, M. Almache-Cueva, and G. Roldán-Molina, "A comparison of cybersecurity risk analysis tools," 2017.