Web Assessment of Libyan Government e-Government Services

Mohd Zamri Murah[1], Abdullah Ahmed Ali[2]
Center for Cybersecurity,
Universiti Kebangsaan Malaysia,
Malaysia

***Abstract*—Libya has started transferring traditional government services into e-government services. The e-government initiative involves the use of websites to offer various services such as civil registration, financial transaction and private information handling. Currently, there has not been many studies about the security assessment of the Libyan government websites. Therefore, in this paper, we did a web security assessment of 16 Libyan government websites. The main purpose of this study is to determine the security level of these websites. The web security assessment was done in four phases: Reconnaissance, Enumeration and Scanning, Vulnerability assessment (web vulnerabilities and SSL encryption evaluation) and Content Analysis(security and privacy policies). The results showed that 9 websites have high and medium level vulnerabilities. Only 3 websites have *A* SSL rating. Also, only 3 websites have published security and privacy policies. We found 1 *highly unsafe* website, 6 *unsafe* websites, 8 *somewhat safe* websites and, 1 *safe* website. Overall, the study indicated the Libyan government websites are adequately secured without major security issues. Since these Libyan government websites deal with sensitive data, adequate security measures should be implemented to reduce the vulnerabilities and to mitigate future cyber security attacks.**

***Keywords*—Libya; e-Government; web security assessment; information security; website vulnerability; penetration testing**

I. Introduction

Internet technology has made a great contribution in changing the global economy. Many governmental and private organization see the opportunity to improve efficiency by providing services online (E-services) through websites or portals[1][2]. The e-services or websites are important to make organization compete and survive in the global economy. Therefore, many governmental and private organization transferred traditional services into e-services which made peoples' lives easier, by getting serve without the constraints of time, location and with less effort and cost[3]. However, the increased usage of websites brought up many new security issues[4]. The websites might have various flaws and weaknesses which they could be exploited by cyber attackers. These security issues are threatening the confidentiality, the integrity of peoples and government information, and threatening availability of the services[5], [6], [7]. According to Edgescan vulnerability statistic report 2018, that both large global organization and governments have faced various breaches. Millions of clients' and employees' records were leaked, and web services are facing various critical and high vulnerabilities.

Libya is one of the countries that have started to transfer traditional government services into e-government such as websites and portals. However, Libya is facing some challenges to implementing these online services. Some main challenges are[8][9]:

1) Lack of studies and researches on the implementations of e-government in Libya.
2) Low trust in e-services from the users.
3) Security and privacy concerns about the websites from the users.

Security of websites is one of the main concerns in Libya today[10][11]. There has been several hacking cases happened in the Libyan government websites due to the lack of security and defensive capabilities[12], [13]. Moreover, not many studies has been done to assess the current security level of Libyan government websites[14]. This is because the Libyan government has only started its e-government in 2013. Therefore, it is important to conduct a study of the current security level of the Libyan government websites. The result of this study might encourage the government to concern more about the importance of web security[15].

II. Related works

Abuzawayda, Y.[16] investigated security issues in Libya by conducting a vulnerability assessment of four Libyan government websites using three vulnerability scanning tools: *N-Stalker*, *Acunetix* and *Nessus*. Also, a survey was carried out to collect data from IT managers. The research results showed that many websites were suffering from various vulnerabilities: critical, high, moderate and low. Ihmouda, R.[14] conducted a web penetration testing on three Libyan government ministries websites using three vulnerability scanning tools: *N-Stalker*, *Acunetix* and, *Nessus*. Moreover, they also interviewed experts to understand the security status of the Libyan government websites in general. The results also showed that many websites have various vulnerabilities and the current security of these websites status need to be improved.

A security assessment was conducted for 51 states government websites in the United States by Zhao(2010)[1]. The assessment was a combination of three methods: web content analysis by searching for security and privacy policies implementation, information security auditing by evaluating SSL encryption, and computer security network mapping using *nmap* scanning tool. The results indicated that many state government websites in the USA were vulnerable to cyber attacks.

Awoleye,W.[17][18] conducted a vulnerability assessment for 64 Nigerian government websites under the domain *gov.ng*.

The assessment carried out using web a web scanner *Acunetix*. The websites were divided into 8 categories which they were evaluated and compared between the categories. The results indicated many Nigerian government websites were open to cyber attacks.

AL-Sanea, M.[3] assessed 150 financial, academic, governmental and commercial websites in Saudi Arabia. The assessment has been done using open-source tools *W3af* and *Skipfish*. Also, they compared between governmental and commercial websites in terms of vulnerabilities numbers. The results indicated some websites are vulnerable to cyber attacks.

We summarized the previous studies with respect to government websites security assessment in Table I. From previous studies, we concluded that many government websites in Saudi Arabia, Nigeria, USA and, Libya are vulnerable to cyber attacks. In this paper, our aim is to determine the current security level of Libyan government websites.

TABLE I. PREVIOUS STUDIES ON SECURITY ASSESSMENT ON GOVERNMENT WEBSITES AND THE TOOLS USED. IN THIS STUDY, WE WILL USE THE SIMILAR TOOLS FOR WEB VULNERABILITIES ASSESSMENT.

Study	Year	Data	Tools
Abuzawayda, Y.	2016	4 Libya government websites	N-Stalker, Acunetix, Nessus
Ihmouda, R.	2013	3 Libya governments websites	N-Stalker, Acunetix, Nessus
Zhao, J	2010	51 United Stated government websites	nmap, SSL, security policy
AL-Sanea, M.	2015	150 financial, academic, governmental and commercial websites is Saudi Arabia	W3af, Skipfish
Awoleye,W.	2012	64 Nigerian government websites	Acunetix

A. Web Application Vulnerabilities

A vulnerability is a security flaws, defects or mistakes in software and system that can be directly exploited by cyber attackers to gain access or to hack the system[19][20]. A good deal of research have found that web applications in general are unsafe[21][22]. There are many types of many types of web vulnerabilities. There are vulnerabilities databases that list all the web vulnerabilities and rank their level of risk. One widely used vulnerabilities' database is CVE and CVSS database[23]. The OWASP Foundation also published top ten web vulnerabilities[24]. Among the OSAWP top vulnerabilities are SQL Injection, Broken Authentication, Sensitive Data exposure, XXL External Entities, Broken Access Control, Security Configuration, Cross-Site Scripting, Insecure Serialization, Using Components with Known Vulnerabilities and, Insufficient Logging and Monitoring[25]. SANS institute also provided 25 top web vulnerabilities[26].

There are many security assessment frameworks to assess websites security. Some methods are manual and others are semi-automated or automated. In recent years, automated web security assessment have become the first choice because its can save time, effort and, covers more security issues. The automated web security assessment consist of three phases: crawl the website and try to list all pages and its links with input vectors, generate specific input values to be submitted to the website and, search for vulnerabilities based on the website responses[27]. Web scanners are different from one another. Some can find more vulnerabilities than others. Therefore, different web scanners will produce slightly different result from one another.

In this study, we use *Acunetix* and *Netsparker* for web scanning. These two tools are considered among the top web scanner available. Other tool that can be used are *AppScan*(IBM), *Arachni*, *Burp Suite*, *WebInspect*(HP) and, *Nessus*[28][29].

B. Secure Socket Layer (SSL)

SSL is a protocol used for securing Internet communication through encryption, decryption and authentication[30]. SSL uses private key to encrypt the transferred data through SSL connection. This allows confidential data such as credit card number, private information and, financial transaction to be transferred through the Internet safely. URLs that uses SSL start with HTTPS, to differentiate its from normal HTTP connection that uses clear text.

SSL protocol establishes secure connection between the website and the user. Its provides authentication between both end points. Also, SSL provides integrity and privacy during the data exchange between the website and the user[31]. Transmitted information between the website and the user is encrypted by SSL, thus ensure high degree of confidentiality.

In general, SSL contains two phases: a hand shake phase and a data transfer phase. During the hand shake phase, a browser will connect to an SSL-based website and request the website to identify itself. In return, the website will send a public key a copy of its SSL certificate. The browser will check the SSL certificate and send an encrypted key back to the website. Finally, the website return an encrypted key with content as a message. The browser will encrypt the message and completes the hand shake phase. After this phase, the browser and the website will continue in a data transfer phase.

It is important for government websites that offer online information and sensitive information transaction to implement secure SSL encryption on their websites. This is important to ensure the security of sensitive information such social security numbers, credit card numbers, private information, health information and, financial information. Sharing information without SSL is a critical risk and may lead to data leakage of sensitive information.

The implementation of SSL can be evaluated using *Qualys SSL* evaluation tool. The tool is an open source software. Other similar tools are *SSL Labs*, *Symantic SSL*, *SSL Analyzer* and, *McAfee SECURE*. This tool check for validity of certificate, protocol version, key exchange, cipher strength and, overall rating.

C. Security and Privacy Policy

The use of government websites involves sharing confidential information between the users and the websites. Users are usually concern with the risk of sharing such information. There are many cases of data leak and data breach where much confidential information is stolen from many websites. Users are less confident in using the government websites if there is no known security policy and privacy policy implemented on the websites[1].

Therefore, in orders to make the users confident in the government websites, the government need to implement and to publish security and privacy policy on the websites. The security policy indicates how secure are the websites and privacy policy indicates how private information is being maintained and used. These policies need to be published and to be make known to all users so that they will trust the websites. If the government websites do not implement or publish their policies, it will be a concern to users to trust the websites and share private information[1].

III. Methodology

The security assessment framework consists of four main phases: Reconnaissance, Enumeration and Scanning, Vulnerability Assessment, and Content Analysis as shown in Fig. 1. We didn't conduct any exploitation or proof-of-concept for any vulnerabilities. The security assessment is based on passive penetration testing[32].

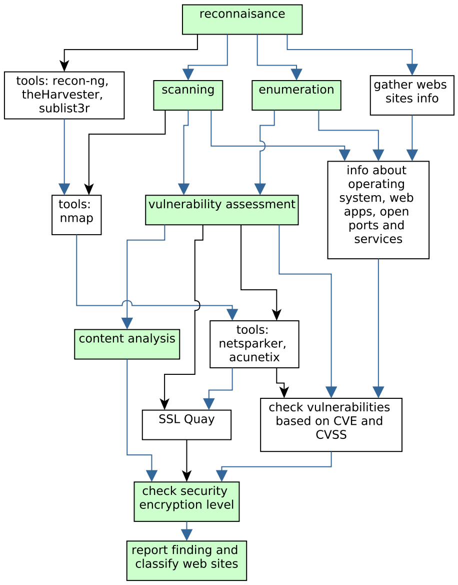
reconnaisance
tools: recon-ng, theHarvester, sublist3r
scanning
enumeration
gather webs sites info
info about operating system, web apps, open ports and services
tools: nmap
vulnerability assessment
content analysis
tools: netsparker, acunetix
SSL Quay
check vulnerabilities based on CVE and CVSS
check security encryption level
report finding and classify web sites

Fig. 1. Security assessment procedures. This procedures consists of four major phases; Reconnaissance, Enumeration and Scanning, Vulnerability Assessment, Content Analysis. The first three phases are the standard procedures. The fourth phase is an additional phase that we proposed.

A. Reconnaissance

Reconnaissance is the stage when we collect as much as possible information about the target from Internet, DNS, and, other public available information. There are two types of reconnaissance: passive and active. Passive reconnaissance is to gather information from search engines and other Internet tools while active reconnaissance is to gather information from a direct contact with the target through social engineering.

This study used passive information gathering by searching for all the Libyan government websites that under the domain *gov.ly*. There are many open source reconnaissance tools that can be used such as *recon-ng*, *sublist3r*, *discovery* and, *theHarvester*[33]. In this study, *TheHarvester* tool have been used to find the sub- domains of *gov.ly* domain. *TheHarvester* is a tool that uses publicly available resources from Internet search engines like Google, Bing, and, Shodan to search for subdomains, hosts, emails and other information. The command that used in this study was:

```
theharvester -d gov.ly -b all > out.txt
```

The command will save the result in the text file `out.txt`.

B. Enumeration

Enumeration is the phase when we gather information about the network and information technology infrastructure such as open ports, operating systems, running services, IPs, status of firewall and, routers[34]. There are also two distinct types of enumeration: active and passive. Passive enumeration is the utilization of the received packets from a website host and it does not require any packets to be sent. Active enumeration is very noisy which requires packets to be sent and waiting for a reply from the website host.

When an active enumeration is conducted, the website or the firewall at the website would detect any attempts from the Internet. Therefore, any active enumerations are logged by the system, thus would alert the website owner of a possible cyber attack. For this reason, enumeration normally done in stealth mode to avoid detection by the websites being scanned.

This study used active enumeration by using *nmap*[35] to scan for open ports, operating systems, running services, and main IPs from the Libyan government websites. The command that has been used in *nmap* scanning is:

```
nmap -iL -F -Pn -sV -A -oX
```

The enumeration phase took a lot of time to be conducted. In this study, we took two working days to enumerate and to scan all 16 websites using *nmap*. One possible issue was the speed of network to reach Libyan websites, and another was probably the websites implemented some security measures to avoid active scanning and enumeration such as throttling the web traffics.

C. Vulnerability Assessment

Vulnerability assessment[36] is the phase where we search for vulnerabilities and flaws in the website's network architecture, operating systems, web applications, content management system and, infrastructures. There are two types of vulnerability scanning: Manual and Automatic. Manual vulnerability scanning requiring advanced skills, experience and may takes a long time. This normally done by experienced hacker and black hats[37][38]. Automatic or semi-automatic vulnerability scanning is much faster than manual. It can be done using open source vulnerabilities scanners like *Vega* and commercial vulnerabilities scanners like *Acunetix* or *Netsparker*. In this study, we used an automatic method to scan for web applications vulnerabilities using *Acunetix* and *Netsparker*.

Different web vulnerabilities scanners would produce different results from one another. This is because each scanner uses different algorithms to detect and to identify vulnerabilities. For example, some vulnerabilities are discovered using web vulnerabilities A but not by web vulnerabilities B, and vice versa. A web vulnerabilities scanning requires a lot of time because of the software need to crawl the website and to verify each vulnerability found. A typical web vulnerability scanning for a typical website will take about 8-15 hour.

In this phase, we also evaluated SSL(Secure Socket Layer) encryption implementation as part of vulnerability assessment using *Qualys SSL.*

1) Web Vulnerability Scanning: In this phase, we used *Acunetix* and *Netsparker* to scan for web vulnerabilities of the 16 Libyan government websites. The time required to scan the websites depends on the websites' security, firewall protections, web application firewall, network speed and network protection. A typical website scanning takes between 2 and 8 hours. The reports from *Acunetix* are very comprehensive, depending on the websites complexity. The reports included vulnerabilities types such as high, medium, low or informational and their CVE/CVSS rating. The reports doesn't indicate any counter-measures for the vulnerabilities. A website scanning using *Netsparker* also takes from 1 to 12 hours. The reports generated were very extensive and includes CVE/CVSS rating. However, *Netsparker* reports give some counter-measures for each vulnerabilities.

This active web vulnerability scan is very noisy and will be logged into the system log file. The scan could also trigger the firewall or (Intrusion Detection System) IDS alarm about a possible cyber attack to the website. Some websites have implemented a counter-measure where it would block connections from Internet that appears to be an active scan[39].

2) Secure Socket Layer (SSL) Encryption Evaluation: During this phase, we used *Qualys SSL* to evaluate SSL encryption implementation at each government website. We assume that it is essential for a government website to implement a secure SSL to protect the data security on the website. If a government website does not implement SSL for data transaction, the data will be at risk. Many government websites deals with highly sensitive and crucial data, and SSL implementation is an important requirement.

The tool *Qualys SSL* checks for SSL validation, certificate expiration, cipher strength and, protocol version of SSL implementation. The results give a detailed and an overall rating for SSL encryption implementation at the websites. The rating levels are: **A**, **A+** for secure encryption, **B**, **C**, **D**, **E**, and **F** means need some updates or improvements, **T** is not trusted, usually because of certificate expiration. If there is no SSL implementation, the evaluation will indicate as such. The SSL evaluation takes between 5 to 10 minutes for each website.

D. Content Analysis

In this phase, we searched for security and privacy policies listed on the 16 Libyan government websites. The idea is that, if the website is serious about security and privacy issues, the website will published the policies on websites for the users. This will indicates that the websites follow the current standard in security and privacy issues. This practice also increase the user trust on the websites. The search was done manually by opening each website and searched for security and privacy policies links in all main page sides. We also checked for the availability of the links provided. Usually, in Arabic websites, security and privacy policies are named by their Arabic links.

E. Safety Level Classification

Based on our experimental previous results, we propose a new safety classification model based on all three factors: vulnerabilities analysis, content analysis and SSL encryption assessment. We called this new classification a website safety level. There are four levels of safety: highly unsafe(A), somewhat unsafe(B), unsafe(C) and safe(D). The basic idea is to combine all security assessment results and to come up with a safety status by combining all three important factors as judged by security experts. The safety classification model is shown in Table II.

TABLE II. A proposed safety classification model for a website based on security assessments, content analysis and SSL encryption evaluation. In this model, there are four levels of *safe*: A(*highly unsafe*), B(*unsafe*),C(*somewhat unsafe*) and D(*safe*).

		SSL rating			
vuln	**data**	**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	B	B
	encrypted	C	C	B	B
low	unencrypted	C	C	B	B
	encrypted	D	D	C	B
info	unencrypted	D	D	C	C
	encrypted	D	D	D	C

IV. Results and Analysis

A. Results from Reconnaissance Phase

We found 742 hosts in the domain and subdomain. The 742 hosts have been copied into Excel file and classified to get only the main domains of the government websites. We also check for live websites, and eliminated dead links and duplicate websites. We identified 37 Libyan government websites under the domain *gov.ly* from our analysis.

We verified the 37 government websites manually using a web browser. This verification was important because there were still some available websites related to the previous government. However, these websites are not used any more due to Libyan government transformation. The verification was conducted by accessing each website to check for availability of the websites. We also checked whether the websites were under the control of the current government "Government of National Accord". The verification process resulted in 16 available websites under the current government. The 16 government websites have been changed and indicated by the letter (w) followed by a number to protect the confidentiality of the websites and to avoid abusing the sensitive information that the experiment might revealed.

B. Results from Enumeration and Scanning phase

In the Enumeration and Scanning phase, we used *nmap*. From *nmap*, we discovered the type of operating system used by the websites, how many open ports were available, the type of running services and the websites IPs number. The information is summarized in Table III.

TABLE III. THE RESULTS FROM *nmap* SCANNING ON 16 LIBYAN GOVERNMENT WEBSITES. WE GET INFORMATION ABOUT OPERATING SYSTEM (YES/NO), THE NUMBER OF OPEN PORTS(COUNT), TYPE OF RUNNING SERVICES(YES/NO) AND, IP NUMBER(YES/NO). THE WEBSITES HAVE BEEN CHANGED USING NAME $w_1 \ldots w_{16}$.

websites	operating system	services	open ports	IP
w_1	yes	yes	10	yes
w_2	no	no	2	no
w_3	yes	yes	10	yes
w_4	yes	yes	10	yes
w_5	yes	no	2	no
w_6	yes	yes	13	yes
w_7	yes	yes	11	yes
w_8	yes	yes	1	yes
w_9	yes	yes	9	yes
w_{10}	no	yes	9	yes
w_{11}	no	yes	10	yes
w_{12}	yes	yes	11	yes
w_{13}	yes	yes	11	yes
w_{14}	yes	yes	13	yes
w_{15}	no	no	3	yes
w_{16}	yes	yes	9	yes

From the results, we obtained information about operating system from 12 websites. Many of these websites used outdated Window XP and Window Server or Linux 2.0 series operating system. The use of outdated operating system could cause a serious risk for the websites. The operating information could be used by cyber attackers to launch cyber attacks based on the outdated operating system vulnerabilities. We discovered 13 websites which disclosed their running services. The information about running services such as *NTP* and *telnet* could be used to launch another type of Internet attacks. We found 11 websites that have the number of open ports larger than 3. Typically, a website only needs to open three required ports (HTTP, HTTP, ssh), and close other ports to reduce attack vectors.

C. Results from Vulnerability Assessment

In this phase, we used web vulnerabilities scanner *Acunetix* and *Netsparker*. These two web scanners are the standard tools in the industry for web scanning. Each tool have its strengths and drawbacks. The results from the web scanning is shown in Table IV.

From the web vulnerabilities scanning, we obtained 1 critical vulnerability, 24 high vulnerabilities, 139 medium, 129 low and, 230 informational from 16 websites. We have 1 website with 1 critical vulnerability, 7 websites with high vulnerabilities, 15 websites with medium and low vulnerabilities. Many of the common vulnerabilities are shown in Table V.

TABLE IV. RESULTS FROM WEB VULNERABILITIES SCANNING USING *Acunetix* AND *Netsparker* THAT INDICATE THE NUMBER OF VULNERABILITIES FOR EACH CATEGORY HIGH(H), MEDIUM(M), LOW(L) AND INFO(I).

	Acunetix				Netsparker			
	H	M	L	I	H	M	L	I
w_1	4	17	45	17	1	2	6	12
w_2	0	1	0	0	0	0	4	14
w_3	0	0	1	1	1	1	2	7
w_4	0	1	3	0	0	0	1	6
w_5	0	0	0	0	0	2	1	8
w_6	0	0	1	0	1	3	11	24
w_7	2	91	4	18	2	2	7	13
w_8	0	0	1	0	0	4	3	10
w_9	0	1	0	0	0	0	2	5
w_{10}	0	0	1	1	1	2	10	24
w_{11}	0	0	0	1	0	1	4	6
w_{12}	0	2	0	1	0	1	0	9
w_{13}	0	1	1	0	0	0	1	7
w_{14}	9	1	2	2	2	3	11	28
w_{15}	0	0	1	0	0	0	0	8
w_{16}	0	1	2	0	1	1	4	8
mean	0.94	7.25	3.86	2.56	0.56	1.38	4.19	11.81
max	9	91	45	18	2	4	11	28

TABLE V. THE COMMON VULNERABILITIES, THEIR RISK LEVEL AND THEIR SECURITY IMPACTS.

vulnerability	**count**	**risk**	**impact**
application error message	78	medium	allow hackers to determine web apps being used
out of date version of JQuery	12	medium	security not patched
out of date wordpress	5	high	security not patches
cross site scripting	5	high	allow hackers to hijack websites
CSRF protection	4	medium	allow hackers to hijack websites
PHP disclosure	3	medium	allow hackers to attack PHP
PHP DOS vulnerability	3	medium	allow hackers to attack PHP
out of date PHP	2	high	security not patches
data in clear text	2	medium	allow hackers to sniff sensitive info

The second vulnerability assessment is SSL encryption evaluation. This step is to determine how a website handle sensitive data such as user data, login information, privacy and, financial transaction. A secure website would use an SSL protocol to encrypt data transaction between the website and the user to ensure the data security. The results is shown in Table VI.

In the Content Analysis phase, we manually searched for security and privacy policies on the 16 websites. Security policy concerns with how secure is the data being used on the website transaction such as login information, personal information, financial data and, sensitive information. Privacy policy concern with whether the website tracks the users that use the websites by extracting IP number, Geo location, time of transaction and, personal information. It was to determine whether the websites informed the users about the security and

TABLE VI. Results from SSL encryption evaluation. The websites were ranked based on their level of SSL implementation. The ranking are A(secure communication), Bneed updates and improvements, T(not trusted, certificate expired) and, no SSL.

	SSL features				
	certificate	protocol support	key exchange	cipher strength	overall rating
w_1,w_7 w_3,w_{11} w_{16}		*no secure protocol*			
w_2, w_5 w_{12}	100%	95%	90%	90%	A
w_4, w_6 w_9, w_{10} w_{13},w_{14} w_{15}	100%	95%	70%	90%	B
w_8	-	90%	70%	90%	T

privacy policies implemented at the websites. From our sample 16 websites, only 3 websites specifically mentioned security and privacy issues. The others didn't have any links to security or privacy issues.

D. Safety Level Classification

The classification criteria in Table II has been used to classify the websites into four main safety categories: highly unsafe, safe, somewhat unsafe, safe. The criteria are based on security assessment, content analysis and SSL encryption evaluation. Each website would be manually assessed by a panel of security experts to determine the safety category of each website. Table VII showed the safety category and previous security assessments. The current approach for safety classification is a heuristic approach. It is derived based on security assessments and, security experts experiences.

V. Discussion

Based on the security assessments results, SSL encryption evaluations and content analysis results, we found that many Libyan government websites have some vulnerabilities issues and do not have good security implementations. Enumeration and Scanning phase has detected a good deal of information about operating systems, open ports, services, and main IPs about the websites. These information might be used by the attacker to find vulnerabilities of the websites. For example, some websites wre detected using operating outdated systems are Windows XP or old versions of Linux (version 2.0 series). These two operating systems have many old vulnerabilities that could be exploited by hackers.

Open ports are another attack vector for cyber hackers. A hardened website only needs 3 essential open ports for data transmission: *HTTP* at port 80, *HTTPS* at port 443 and *SSH* at port 22. All other ports are not important for a website. Port numbers below 100 are reserved for system services such as *ftp*, *telnet* and, *NTP*. We found twelve of the 16 websites have 4 or more open ports and only 4 websites have 3 open ports or fewer. We opined that if a website have more open ports available, the higher the risk of a cyber attack to a website. Services from a website are served using open ports. Cyber hackers can exploit these available services to gain access to the website. Websites should only employed important services such as *HTTP*, *HTTPS* and, *SSH* only to reduce the risk of illegal access to a website. Basic services such as *ftp* and *telnet* could be exploited by cyber attackers if these services are not properly configured.

TABLE VII. Summary of security assessment, SSL encryption evaluation and Content Analysis. For *vulns* column, the number indicate the total number of High(H) and Medium(M) vulnerabilities from web scanning.Content Analysis column indicate whether the website has security policy and has privacy policy(1,1), no security policy but has privacy policy(0,1), has security policy but no privacy policy(1,0), no security policy and no privacy policy(0,0) . Safety category column indicate the safety category: 1(highly unsafe), 2(unsafe), 3(somewhat unsafe), 4(safe)

website	vulns	SSL	Content Analysis	Safety
w_1	21	-	(0,0)	2
w_2	1	A	(1,0)	3
w_3	2	-	(1,1)	2
w_4	1	B	(0,0)	3
w_5	2	A	(0,0)	3
w_6	4	B	(0,0)	2
w_7	99	-	(0,0)	2
w_8	4	T	(0,0)	3
w_9	1	B	(0,0)	3
w_{10}	3	B	(0,1)	2
w_{11}	1	-	(0,0)	3
w_{12}	2	A	(0,0)	3
w_{13}	1	B	(0,0)	3
w_{14}	10	B	(0,0)	1
w_{15}	0	B	(0,0)	4
w_{16}	2	-	(0,0)	2

Using *Acunetix* and *Netsparker*, we found that 9 of the 16 websites have high or medium vulnerabilities as shown in Table IV and, 7 of the 16 websites do not have high or medium vulnerabilities. That security implementation at the 16 Libyan government websites are good but need improvement. There is only 1 website with a critical vulnerability.

The results from *Acunetix* and *Netsparker* are different. This is to be expected since both of them use different algorithms to detect vulnerabilities. Some vulnerabilities were found by *Acunetix* and not by *Netsparker* and, vice versa. *Acunetix* discovered more high and medium vulnerabilities than *Netsparker*. *Netsparker* discovered more low and informational vulnerabilities than *Acunetix*. Therefore, it is good practice to use both web scanners.

The websites with high and medium vulnerabilities might be compromised or might be open to future cyber attacks. Therefore, these high and medium vulnerabilities need to be fixed urgently. Many of these vulnerabilities involve outdated operating systems and web applications. However, The websites with low and informational vulnerabilities are also at risk. Attackers might use this information to find more critical vulnerabilities, to conduct social engineering and, to launch phishing attacks. Many of the web vulnerabilities found at the websites are included in OWASP 2017 top 10 web vulnerabilities: Cross-Site Scripting(XS), Sensitive Data Exposure (lack of SSL, send sensitive data in clear text), Using Components with Known Vulnerabilities (outdated programming language or content management system), Broken Authentication (expired SSL certificate, outdated SSL)and Security Configuration (application error logs).

In SSL encryption evaluations, we found only 3 websites with rating **A**, which indicate the websites implement the latest SSL security measures for data security. We found 7 websites rated **B**, because they have weak SSL exchange keys. The weak keys would allow attackers to do a Man-In-The-Middle (MITM) attack and to access the data communication channel. There are 5 websites with no SSL implementations. These websites would need to implement SSL encryption protocol since government websites normally involves in transferring users credential, private data or sensitive data through the Internet. We found 1 website with an expired SSL certificate. Hackers may take advantage of this website by using MITM attacks or POODLE attacks.

Based our security assessment and content analysis study, we propose a safe classification model that would categorize the websites into 4 *safe* categories: *highly unsafe*, *unsafe*, *somewhat safe*, *safe*. The criteria are based on the web security assessment, the SSL encryption evaluation and the content analysis of security and privacy policies. Based on these criteria, we have 1 *highly unsafe* website because this website involves in handling Libyan citizen private information and have low SSL rating. We have 6 *unsafe* websites with a high number of vulnerabilities and low SSL rating. The websites need to fix their vulnerabilities and improve their SSL implementation. We also have 8 *somewhat unsafe* websites with low numbers of vulnerabilities and low SSL rating. These websites need to improve their SSL implementations. We have 1 *safe* website where its has 0 vulnerabilities and low SSL rating. This website might need some improvement in SSL implementation.

Based on our proposed *safe* classification model, we have 1 *highly unsafe* website, 6 *unsafe* websites, 8 *somewhat unsafe* and 1 *safe* website. For a website to have a safe category, we propose for a website to follow these guidelines;

1) Eliminate critical and high level vulnerabilities. This can be done with regular web vulnerabilities assessment. Also, the website needs to update operating system regularly, to patch securities holes, to updating web apps and, to harden the system.
2) Implement secure SSL and avoid expired certificate. This will make sure the data communication channel is safe.
3) Published policy on privacy and security. This will install confident for users to use the website for sensitive data transactions.

VI. Conclusion

In this paper, we have studied security assessment of 16 Libyan government websites using a four phases framework: Renaissance, Enumeration and Scanning, Vulnerability Assessment and Content Analysis. Our study found 3 websites with more than 9 vulnerabilities and, 12 websites have between 0 and 8 vulnerabilities. Twelve websites implement SSL encryption at different level of implementation with only 3 websites have *A* rating. Only 3 websites have published security and privacy policies on their websites. Based on our *safe* category model, we have 1 *highly unsafe* website due to its SSL implementation and the nature of its operation. It is highly recommended for the websites to keep up-to-date with securities issues, system patches and, cyber attacks vectors. The websites also need to develop security and privacy policies for their users so the users would trust the websites.

Overall, we considered the Libyan government websites are adequately secured without major security issues.We encourage the websites to improve their security implementation by fixing the vulnerabilities, updating security patches, updating system configurations and, improving SSL implementations. For future work, this study can be extended to cover all Libyan government and educational websites. Also, the same study can be conducted on commercial websites. Then, a comparison can be made between these websites from a security assessment perspective.

Acknowledgment

The authors would like to thank Center for Cybersecurity at Universiti Kebangsaan Malaysia for their assistance.

References

[1] 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.

[2] R. Ismail ova, “Web site accessibility, usability and security: a survey of government web sites in Kirghiz republic,” *Universal Access in the Information Society*, vol. 16, no. 1, pp. 257–264, 2017.

[3] C. G. Red dick and M. Turner, “Channel choice and public service delivery in Canada: Comparing e-government to traditional service delivery,” *Government Information Quarterly*, vol. 29, no. 1, pp. 1–11, 2012.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] A. A. Ahmed, S. Dalbir, and M. Ibrahim, “Potential e-commerce adoption strategies for Libyan organization,” *International Journal of Information and Communication Technology Research*, 2011.

[9] O. Elaswad and C. D. Jensen, “Identity management for e-government Libya as a case study,” in *Information Security for South Africa (ISSA), 2016*. IEEE, 2016, pp. 106–113.

[10] T. R. Gebba and M. R. Zakaria, “E-government in Egypt: An analysis of practices and challenges,” *International Journal of Business Research and Development*, vol. 4, no. 2, 2012.

[11] M. M. Elmansori, H. Atan, and A. Ali, “Factors affecting e-government adoption by citizens in Libya: A conceptual framework,” *i-Manager’s Journal on Information Technology*, vol. 6, no. 4, p. 1, 2017.

[12] 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.

[13] 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.

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

[15] Y. B. Forti and M. G. Wynn, "A new model for e-government in local level administrations in Libya," in *The Proceedings of 17th European Conference on Digital Government ECDG 2017*, 2017, p. 315.

[16] Y. I. Abuzawayda, "Security issues on Libya's e-government," *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 1, 2016.

[17] O. M. Awoleye, B. Ojuloge, and W. O. Siyanbola, "Technological assessment of e-government web presence in Nigeria," in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*. ACM, 2012, pp. 236–242.

[18] O. M. Awoleye, B. Ojuloge, and M. O. Ilori, "Web application vulnerability assessment and policy direction towards a secure smart government," *Government Information Quarterly*, vol. 31, pp. S118–S125, 2014.

[19] N. F. Awang, A. A. Manaf, and W. S. Zainudin, "A survey on conducting vulnerability assessment in web-based application," in *International Conference on Advanced Machine Learning Technologies and Applications*. Springer, 2014, pp. 459–471.

[20] 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.

[21] I. Alsmadi and E. Abu-Shanab, "E-government website security concerns and citizens' adoption," *Electronic Government, an International Journal*, vol. 12, no. 3, pp. 243–255, 2016.

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

[23] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, 2006.

[24] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, no. 2, pp. 76–79, 2017.

[25] T. F. OWASP, "Application security risks-2017. open web application security project (OWASP)," 2017.

[26] T. Scholte, D. Balzarotti, and E. Kirda, "Have things changed now? an empirical study on input validation vulnerabilities in web applications," *Computers & Security*, vol. 31, no. 3, pp. 344–356, 2012.

[27] F. R. Munoz and L. G. Villalba, "Methods to test web applications scanners," in *Proceedings of the 6th International Conference on Information Technology*, 2013.

[28] 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.

[29] G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadão, I. Yevseyeva, and V. Basto-Fernandes, "A comparison of Cybersecurity risk analysis tools," *Procedia Computer Science*, vol. 121, pp. 568–575, 2017.

[30] A. Freier, P. Karlton, and P. Kocher, "The secure sockets layer (SSL) protocol version 3.0," Tech. Rep., 2011.

[31] M. A. Alnatheer, "Secure socket layer (SSL) impact on web server performance," *Journal of Advances in Computer Networks*, vol. 2, no. 3, pp. 211–217, 2014.

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

[33] C. Buchanan and V. Ramachandran, *Kali Linux Wireless Penetration Testing Beginner's Guide: Master wireless testing techniques to survey and attack wireless networks with Kali Linux, including the CRACK attack*. Packt Publishing Ltd, 2017.

[34] S. Mehta, G. Raj, and D. Singh, "Penetration testing as a test phase in web service testing a black box pen testing approach," in *Smart Computing and Informatics*. Springer, 2018, pp. 623–635.

[35] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.

[36] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27–49, 2015.

[37] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, and T. Raghu, "Moving toward black hat research in information systems security: an editorial introduction to the special issue," *MIS quarterly*, vol. 34, no. 3, pp. 431–433, 2010.

[38] I. Idris, M. U. Majigi, S. Abdulhamid, M. Olalere, and S. I. Rambo, "Vulnerability assessment of some key Nigeria government websites," *International Journal of Digital Information and Wireless Communications*, vol. 7, no. 3, pp. 143–153, 2017.

[39] D. Stuttard and M. Pinto, *The web application hacker's handbook: Finding and exploiting security flaws*. John Wiley & Sons, 2011.