SECURITY ASSESSMENT FOR EDUCATION WEBSITES IN SAUDI ARABIA

Almirabi Anas Anwar M, Mohd Zamri Murah

CYBER SECURITY, FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY, UNIVERSITI KEBANGSAAN, MALAYSIA

Almirabi.33@hotmail.com , zamri@ukm.edu.my

ABSTRACT: Web applications have become a part of our daily lives and are usually accessible from any internet connection point at any time. This has also had an impact on the education sector, whereby increasing the demand for a reliable, effective, and stable web presence. The institutional websites have helped many educational organisations deliver vital information to potential students without increasing man hours. Due to this, the e-service industry is growing in Saudi Arabia. The creation and delivery of such e-services on the internet however increases the risk of cyber-attack exposure. This could result in the data theft of users and other involved parties. Hence, to maintain the trust of the users, the level of website security must be analyzed, and the vulnerabilities addressed. The research done focuses on four main phases of security assessment framework. This includes Reconnaissance, Enumeration and Scanning, Vulnerability Assessment, and Content Analysis. The study was carried out using 12 education websites in Saudi Arabia. The results indicated that total number of high, intermediate and low vulnerabilities found are 886, 5036 and 604 respectively. Besides this, there were 1965 informational vulnerabilities. These high number of vulnerabilities in the websites without mitigation protocol are at high risk of cyber-attacks and must be patched. The following research would aid the Saudi Arabian institutes in understanding the vulnerabilities and establish protocols in order to mitigate attacks.

1. **INTRODUCTION:** Web applications have become an integral part of everyday life (Mburano & Si 2019). Web applications generally pose only very few constraints regarding the time of use, place, or person for the end-user. They are accessible at any time and from any internet access point normally. This design concept is chosen to provide access to the largest possible group of potential consumers. However, in this case, the qualities making web applications attractive to consumers also render them to interesting targets for web attacks. Additionally, they have few means to differentiate an honest user from a malicious one. Interactions take place by exchanging request/response messages containing only a limited amount of information (Lis & Schmitz 2019).

Security remains one of the major concerns of information systems. The growing connectivity of computers through the internet, the increasing extensibility, and the unbridled growth of the size and complexity of systems have made system security a bigger problem now than in the past (Shah & Mehtre 2015). As a result, web applications became increasingly dynamic and susceptible to vulnerabilities (Lis & Schmitz 2019).

The usage of e-services in Saudi Arabia is growing. such services offer a wide range of benefits and make people's life easier. However, the development and the deployment of these e-services on the internet increase the likelihood of exposure to cyber-attacks. Attackers take advantage of vulnerabilities in these e-services. Vulnerabilities arise as a result of weaknesses in the programming, miss-configuration, or lack of updates. Unfortunately, only a little effort is done to evaluate the security posture of Saudi Arabia's' websites (District 2015).

Nevertheless, most people still don't understand the importance of internet security. People pay no attention to the security of web applications to protect sensitive information. They would realize the importance of security when they experience cyber-attacks. Web applications like government websites contain much sensitive information such as identity card numbers, addresses, telephone numbers, etc. Hence, precautions must be taken to avoid the data being leaked (Ara 2018).

2. **RELATED WORK:** (Montagu 2015) Public education is open to every Saudi citizen from primary school through college. Saudi Arabia's second-largest government spending goes toward education. Saudi Arabia invests 8.8% of its gross national product on education, compared to the global average of 4.6%, which is almost twice the global education average.

List of several Saudi Arabia universities and colleges:

1. King Saud University

2. Princess Nora bint Abdul Rahman University

3. Imam Muhammad bin Saud Islamic University

4. Prince Sultan University

5. College of Telecom & Information

6. Riyadh College of Dentistry and Pharmacy

Nowadays, as online technologies become an integral part of the education procedure, the need for higher education institutes to provide a reliable, efficient, and safe web presence is growing. The institutions of higher education perform a critical part in the growth of society. websites of higher education have various tasks to fill. They need the information to be given to the students to help for enrolling for classes, faculty information, current students statuse, and alumni. Also, they need to provide knowledge reams in a method that makes it easy to understand and it's a major challenge. Digital attackers, however, are turning their attention on universities more and more and they often find prey fairly easy. Universities are desirable goals as they retain a wide amount of personal data on graduates, including contact details, financial information, medical information, and social security numbers (Chan 2016).

3. **PROBLEM STATEMENT:** With the rapid growth in relying on the convenience of using web applications, many organizations focus on the functionality of the web application and overlook the importance of security. In 2011, Sony Pictures was attacked by a group called Lulz Security with a very simple SQLi. The attack had compromised more than a million users' confidential information including passwords, date of birth, home addresses, email addresses, and other personal information (Ames 2018).

The demand for electronic services to university students has grown in Saudi Arabia, with a significantly higher number of government and private universities in the last 10 years (Alotaibi 2013). Therefore, based on the security risks on the internet and the importance of education websites and the need to maintain trust and trust with users, we need to test the security level of the website from actual threats and fix vulnerabilities and analyze the results of current education websites in Saudi Arabia to help us make decisions and understand the main risks that we need to address.

4. **OBJECTIVES:** The purpose of this research is to identify the security level of targeted Saudi Arabia education web applications and identify the existence of vulnerabilities.

5. **METHODOLOGY:** The framework for the security assessment is composed of four main phases: Reconnaissance, Enumeration and Scanning, Vulnerability Assessment, and Content Analysis as given in Figure 1. No proof-of-concept or exploitation was conducted for any vulnerabilities. The assessment of security is based on passive penetration testing.

The figure below shows the methodology for this project.

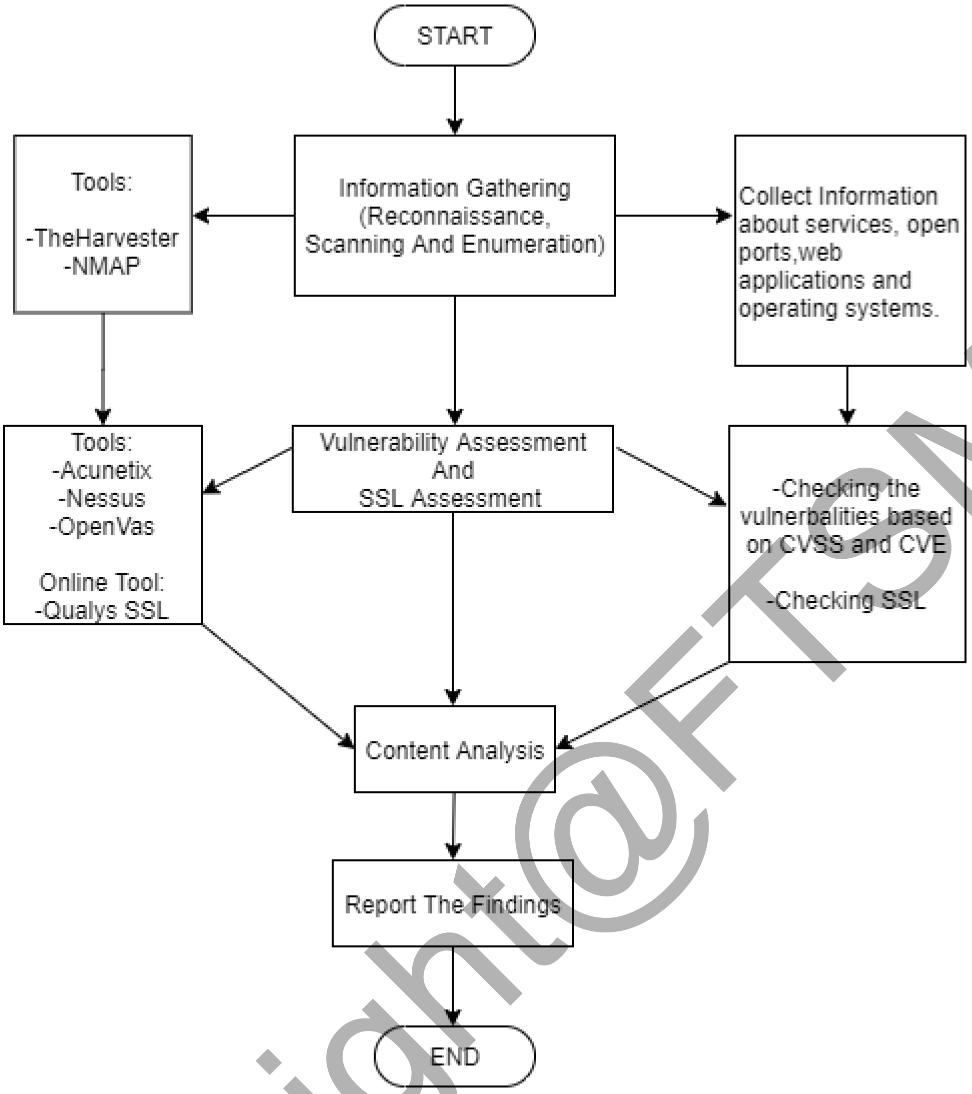

Figure 1 Security assessment procedures.

6. **RESULTS AND DISCUSSION:** In edu.sa, 78 hosts were found within the domain and subdomain. The 78 hosts were copied into a new file and listed to get only the main education websites domains. We checked for live websites however and removed all dead links. For our analysis, we identified 29 websites for Saudi education under the domain edu.sa.

We used a web browser to manually check the 29 Saudi education websites. This verification was important because some websites related to Saudi education were still available, but such websites are no longer used. The verification was performed by opening each website to check the websites' availability. The verification process led to 12 websites being available under edu.sa. The 12 websites of Saudi education have been updated and indicated by letters (wb) followed by a number to protect the websites' confidentiality and to avoid abusing the sensitive details that the experiment could disclose.

6.1 RESULTS OF ENUMERATION AND SCANNING:

We used Nmap in the enumeration and scanning process. Through Nmap, we discovered the type of operating system that the websites obtain, the number of open ports available, types of running services as well as the number of websites IPs. The table below shows us the services, operating systems, and open ports for each website detected by Nmap.

Table 2 Service, operating systems and open ports by Nmap

websites	Operating system	services	Open ports	IP
Wb1	Microsoft IIS 8.5	http, ssl/https	80/tcp, 443/tcp	Yes
Wb2	Microsoft IIS 10.0	http, ssl/https	80/tcp, 443/tcp	Yes
Wb3	Citrix-netscaler, Apache2.4.29(Unix)	http, ssl/https	80/tcp, 443/tcp	Yes
Wb4	No	http-proxy, ssl/https	80/tcp, 443/tcp	Yes
Wb5	Microsoft HTTPAPI/2.0	http, ssl/https	80/tcp, 443/tcp,	Yes
Wb6	No	http, ssl/https, proxy, ssl/https-alt	80/tcp, 443/tcp, 8080/tcp, 8443/tcp,	Yes
Wb7	No	"http, ssl/https, proxy, ssl/https-alt	80/tcp, 443/tcp, 8080/tcp, 8443/tcp,	Yes
Wb8	No	http-proxy, ssl/https	80/tcp, 443/tcp,	Yes
Wb9	Apache(SSL-only mode)	http-proxy, ssl	80/tcp, 443/tcp,	Yes
Wb10	Microsoft IIS 10.0	http-proxy, ssl/https	80/tcp, 443/tcp	Yes
Wb11	No	http, ssl/https	80/tcp, 443/tcp	Yes
Wb12	Microsoft-azureapplication-,Microsoft-IIS/10.0	http, ssl/https	80/tcp, 443/tcp	Yes

From the results, we gathered details from 7 websites on the operating system. Several of these websites are using outdated operating-systems of the Windows IIS 8.5 Server or Linux 2.4 series. Using the outdated operating system might put the websites at serious risk. Cyber attackers may use the operating information to launch cyber-attacks based on outdated vulnerabilities in the operating system. We found some websites which revealed their running services. Information regarding running services like NTP and telnet could then be used to initiate some other kind of web attack. After all, most websites are protected with less than 5 open ports in the matter of attack surface, most of them are HTTP, proxy & https ports. Only three appropriate ports (HTTP, HTTPS, SSH) must be opened by a website and other ports must be closed to reduce attack vectors.

Open ports could be the potential of the attack surface. The daemons mentioned on the port can be susceptible to buffer overflows or other vulnerability which can be remotely exploited. A major security principle is to reduce the attack surface and maintain that the server has a minimum amount of exposed services. (Theisen et al. 2018).

6.2 VULNERABILITY SCANNER: We used the OpenVAS, Nessus, and Acunetix web vulnerability scanners. Such three web scanners are some of the industry standard tools for web scanning. There are strengths and disadvantages of each tool. The results of the three examinations took longer than two months of continuous scanning.

The following tables indicate what the outcomes of OpenVAS, Nessus, and Acunetix are found on each web site. (H) stands for High criticality level, (M) stands for Medium criticality level, (L) stands for Low criticality level, and (I) stands for Informational level.

In OpenVas, Nessus, and Acunetix, "CVE (Common Vulnerabilities Exposure), CWE (Common Weakness Enumeration), and CVSS (Common Vulnerability Scoring System) are included for classification of vulnerabilities.

Table 3 Detected vulnerabilities of all

Tools	**OpenVas**				**Nessus**				**Acunetix**			
Indicators	H	M	L	I	H	M	L	I	H	M	L	I
Websites												
Wb1	-	-	-	-	-	2	1	27	22	58	11	31
Wb2	-	-	-	-	-	2	-	20	0	0	1	2
Wb3	-	-	-	-	-	-	-	2	0	843	2	233
Wb3	-	-	-	-	-	-	-	8	0	3	3	3
Wb4	-	-	-	-	-	-	-	14	0	435	55	703
Wb5	1	-	-	66	-	-	-	72	0	646	45	23
Wb6	1	-	-	66	-	-	-	46	0	0	1	1
Wb7	-	-	-	-	-	1	-	23	4	2	4	7
Wb8	-	-	-	-	-	-	-	8	0	2	1	1
Wb9	-	-	-	-	-	1	1	30	0	18	11	32
Wb10	-	-	-	-	7	6	1	17	0	0	0	1
Wb11	-	-	-	-	-	1	-	25	851	3016	467	504
Wb12	-	-	-	-	-	2	1	27	22	58	11	31

Different scanners of web vulnerabilities will show results differently from one another. This is because each scanner uses different algorithms for detecting and recognizing vulnerabilities. For instance, some vulnerabilities are discovered through web vulnerabilities A, but not B, and likewise. The symbol (-) means that the tools could not detect whether there is a vulnerability in the websites or not while (0) means that vulnerability was detected as zero.

The findings of Acunetix were surprisingly different than OpenVas and Nessus tools. However, the results show, wb12, with Acunetix, but not Nessus, have the largest number of high vulnerabilities and the highest medium vulnerability. The second highest was then the number of medium vulnerabilities in wb3, web6. Then, wb6 and wb7 have high, discovered by OpenVAS and informational vulnerabilities discovered by OpenVAS and

Nessus. Besides, wb3, wb5, wb6, and wb12 have the highest medium vulnerability that Acunetix has found. Generally, most websites have low and informational vulnerabilities, and many have intermediate vulnerabilities.

The overall number of vulnerabilities that were found on all websites is 886 as high vulnerabilities number, discovered by OpenVAS, Nessus and Acunetix, Medium vulnerabilities number is 5036, low vulnerabilities number is 604, finally, the number of informational vulnerabilities is 1965.

6.2.1 Qualys SSL Labs Results:

The second vulnerability assessment is an evaluation of the SSL encryption. This stage is to assess how sensitive data such as user data, login information, confidentiality, and financial transaction are processed by a website. To ensure data protection, a secure website will use an SSL protocol to encrypt data transfers between the website and the user. We searched websites using the free online Qualys SSL Labs tool for an in-depth review of website server SSL configuration. The results are outlined in the table below.

Table **Error! No text of specified style in document.** Qualys SSL labs rating

Website	Certificate %	Protocol Support %	Key Exchange %	Cipher Strength %	Rate %
Wb1	100	70	70	90	“B”
Wb2	100	100	70	90	“B”
Wb3	100	70	70	90	“B”
Wb4	100	70	90	90	“B”
Wb5	100	70	90	90	“B”
Wb6	100	70	90	90	“B”
Wb7	100	100	90	90	“A+”
Wb8	100	100	90	90	“A”
Wb9	100	0	70	90	“F”
Wb10	100	70	70	90	“B”
Wb11	-	-	-	-	-
Wb12	100	70	90	90	“B”

6.2.2 Content Analysis Results:

In this step, we manually searched using google, and by reviewing the websites’ pages, documents, and links to all 12 websites to find out about security and privacy policies. The results are shown in the table below.

Table 5 Content analysis result

Website	Privacy Policy Availability	Security Policy Availability
Wb1	No	No
Wb2	Yes	Yes
Wb3	No	No
Wb4	Yes	Yes
Wb5	No	No
Wb6	Yes	Yes

Wb7	Yes	Yes
Wb8	No	No
Wb9	Yes	Yes
Wb10	Yes	Yes
Wb11	Yes	Yes
Wb12	No	No

Several websites do not offer security or privacy policies in their website pages. Moreover, various websites do not recognize the worth of establishing privacy and security policies on the websites. However, except for the security and privacy policies of seven websites mixed in one page as by the name of the privacy policy. Hence, we suggest that all websites consider establishing security and privacy policy in their website. without security policy, any organization may be exposed in a bad way.

6.2.3 Compliance of Security Standards Results: We conducted a security review to verify that the sites met security standards using the Acunetix tool.

The table below shows us the security standards incompliance alerts for each website using Acuntix. for example, the incompliance alerts count of wb5 for **OWASP** standard is 995.

Table 6 Incompliance alerts count on security standards using Acunetix for all websites.

WebSite	CWE	HIPPA	ISO	NIST	PCI	OWASP	SOX	STIG	WASC
Wb1	138	541	643	285	251	268	167	213	1119
Wb2	1	6	7	3	4	6	5	3	25
Wb3	934	1450	1544	1171	1224	525	1078	1078	9558
Wb4	1	9	8	10	15	22	12	10	74
Wb5	1185	6358	7638	2814	2157	995	1199	1627	10778
Wb6	668	815	839	744	761	203	795	757	6420
Wb7	0	1	1	1	3	5	4	2	17
Wb8	12	49	48	27	23	30	25	22	145
Wb9	0	3	3	4	7	11	6	4	33
Wb10	54	287	349	125	96	95	61	71	546
Wb11	0	1	1	1	2	3	1	1	8
Wb12	5673	10759	13096	8114	5380	2838	6542	6731	43528

Next table shows the High and Medium vulnerabilities that we detect and the number of its occurrence.

Table 7 The high and medium vulnerabilities count of all the 12 education websites of Saudi Arabia

Severity	Vulnerability	Alert count
High	AngularJS client-side template injection	22
High	Cross-site scripting	854
High	Blind SQL Injection	1
Medium	HTML form without CSRF protection	3978

Medium	Source code disclosure	1
Medium	TLS 1.0 enabled	7
Medium	SharePoint exposed web services	482
Medium	Unencrypted __VIEWSTATE parameter	18
Medium	Vulnerable Javascript library	9
Medium	Error message on page	477
Medium	Application error message	44
Medium	Possible social security number disclosed	3
Medium	Backup files	2
Medium	Password field submitted using the GET method	1
Medium	RC4 cipher suites detected	1
Medium	HTTP parameter pollution	1
Medium	Cross site scripting (content-sniffing)	1

There are several vulnerabilities have been detected on the 12 websites. Some of them are rated as high and medium vulnerabilities as shown in Table 1.18. Thus, below are some descriptions of some vulnerabilities and some suggestions for mitigation and prevention.

6.2.4 Suggested mitigations for the 12 education websites in Saudi Arabia.

1. SharePoint exposed web services: Microsoft SharePoint is a web application platform developed by Microsoft. Because of improper configuration an anonymous user has access to the SharePoint Web Services.

Recommendation to prevent attacks: Restrict access to this page.

2. Cross-site scripting: Cross-site Scripting (XSS) refers to a client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Recommendation to prevent attacks: Use context-dependent encoding and/or validation on a page's user input.

7. **CONCLUSION:** Overall, the result shows that there is a variation security level between the 12 education websites. The high number of vulnerabilities in the websites without such mitigation will have a high risk for cyber-attacks. It is necessary for these websites to patch such vulnerabilities. As these education websites hold sensitive data, effective security measures are needed to decrease vulnerabilities and mitigate future cybersecurity attacks.

8. **FUTURE WORK:** Regarding education sites, we analyzed the security problems of education websites in Saudi Arabia. But every website on the internet is still facing a security problem due to some commonalities they share, technical challenges, etc. Therefore, more detailed inquiries and analysis on security issues are

needed on education websites in Saudi Arabia. This can be extended to all education websites in Saudi Arabia in different ways, for example. Therefore, we suggest a future security assessment to range it from assessing vulnerabilities to discovering and identifying false negatives and positives.

In contrast, do a manual assessment and compare the results with an automatic one. It will also be strengthened if the assessed sites are better analyzed and compared to the secured one.

9. REFERENCES

Alotaibi, M. B. 2013. Assessing the usability of university websites in Saudi Arabia: A heuristic evaluation approach. *Proceedings of the 2013 10th International Conference on Information Technology: New Generations, ITNG 2013* (April 2013): 138–142. doi:10.1109/ITNG.2013.26

Ames, M. G. 2018. Hackers, computers, and cooperation: A critical history of logo and constructionist learning. *Proceedings of the ACM on Human-Computer Interaction* 2(CSCW): 1–19. doi:10.1145/3274287

Ara, I. 2018. Growth analysis of cyber security awareness among mass people of Bangladesh : a case study.

Chan, R. Y. 2016. Understanding the purpose of higher education: an analysis of the economic and social benefits for completing a college degree. *Journal of Education Policy, Planning and Administration* 6(5): 1–40.

District, N. 2015. Security Evaluation of Saudi Arabia’s Websites Using Open Source Tools 1–5.

Lis, A. & Schmitz, G. 2019. Comparison and Analysis of Web Vulnerability Scanners.

Mburano, B. & Si, W. 2019. Evaluation of web vulnerability scanners based on OWASP benchmark. *26th International Conference on Systems Engineering, ICSEng 2018 - Proceedings* 1–6. doi:10.1109/ICSENG.2018.8638176

Montagu, A. 2015. Special communication. *JAMA: The Journal of the American Medical Association* 179(11): 887. doi:10.1001/jama.1962.03050110055011

Shah, S. & Mehtre, B. M. 2015. An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques* 11(1): 27–49. doi:10.1007/s11416-014-0231-x