INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 9, Issue 2 - V9I2-1404)
Available online at: https://www.ijariit.com

Penetration testing in several universities in SaudiArabia using black box method

Faisal Hamzah Faisal Al-Ahdal
faisal.a.g.l69@gmail.com
Narotama University, Surabaya, Indonesia

Aryo Nugroho
Aryo.nugroho@narotama.ac.id
Narotama University, Surabaya, Indonesia

ABSTRACT

We live in a very modern era where the presence of the Internet has become one of the necessities of life and to facilitate daily and hard work. The presence of the Internet is important, but not all people use it in the right way. There are those who prevent the appropriation or theft of information be secure through the presence of some gaps in the web, so researcher will do some examinations on some university website in Saudi Arabia and analysis of the types of vulnerabilities using the OWASP ZAP bracket and use Black box method, It's testing the functionality without peering into internal structures. The result from this research is to measure the security of university websites in KSA.

Keywords: Website, OWASP ZAP, Black Box, Secure, Vulnerabilities.

1. Background

The development of technology and information in the current era is very rapid, the internet is an important partin the continuity of activities carried out by today's society. This can be seen with the increasing number ofusers of social media and the internet today. We Are Social noted that 95.7% of Saudi Arabia's population had used the internet as of January 2021. This proportionis the 3rd highest ranking in Asia, after the United ArabEmirates and South Korea (Databoks, 2021) This indicates that almost the entire population of Saudi Arabia is now connected to the internet.

The development of information technology has also touched the process within the scope of the university inorder to increase the effectiveness and efficiency of work. Currently, quite a lot of modern universities use information technology by utilising the internet network,namely the web as a medium for conveying information,connecting the academic community and others.

Creating information systems can improve the quality ofan organisation. The importance of the value of information causes the information generated from the system to be restricted to access by certain people so that the value of the information conveyed maintains itsintegrity. The fall of information to other parties who arenot authorised can cause harm to the organisation so thatthe system created must be able to cope with unwanted actions. Information security is something that must be considered for every agency in order to avoid interference or criminal acts.
Lack of understanding and awareness of system securityissues always threatens at any time, especially for developers.

Data leakage or destruction can threaten at any time as human resources increase. Web security solutions from interference or hacker attacks can be doneby means of security testing carried out to determine thelevel of vulnerability in order to avoid attacks from irresponsible parties.

Software security plays an important role in many aspects of cybersecurity. To protect the web server fromattacks by irresponsible parties, it is recommended that web server testing should be carried out by self-testing the web server system itself using the penetration testingmethod. According to Mulyadi, penetration testing is a procedure and technique to assess the security of acomputer system or network by running attack simulations to find out where the system is vulnerable and to close or repair the gap. Penetration testing is doneas a precaution to prevent hacking of the system (Mulyadi, 2018). One of the penetration testing methodsis Open Web Application Security Project (OWASP) which is a non-profit organisation that focuses on web security (Owasp, 2021). The OWASP risk assessment method is a simple and useful way to calculate and assess the risk vulnerabilities of websites. OWASP has several projects, namely OWASP Top 10, OWASP Proactive Controls, OWASP Application Security Verification Standard (ASVS), OWASP Software Assurance Maturity Model (SAMM), OWASP Zed Attack Proxy (ZAP), and OWASP ModSecurity Core Rule Set (CRS). One that will be used by the author in this research is OWASP Zed Attack Proxy (OWASPZap) is a tool used to find various security holes in web applications when developing and testing web applications (G.Costaner, 2020). The OWASP method is open and collaborative, this method is based on the Black Box Testing approach where the examinerhas very little information on the web to be tested. As a method of application security. This test is expected to determine the quality of websites owned by several universities inSaudi Arabia in maintaining and developing their websites.

Based on the foregoing background and problem formulation, the researcher is interested in taking the topic for this thesis. PENETRATION TESTING INSEVERAL UNIVERSITIES IN SAUDI ARABIAUSING BLACK BOX METHOD.

2. RESEARCH METHOD

In this study using the Black Box method, namely testing on
a website that has used a hosting service The Tool usedin OWASP ZAP is Active scan, active scan rules, alerts, Access control testing, and passive scan rules.
The following is the flow of research methods or steps that will be carried out in this research:

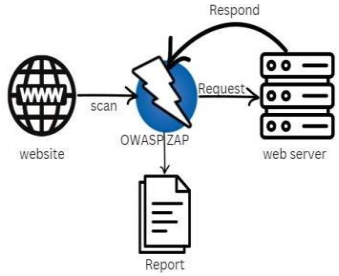


Figure 3.1 Flow or steps of research methodology

2.1 Research methods

Explanation of the flow of research methods in Picture
3.1 The flow or steps of the research methodology basedon the sequence:

2.2.1 website

The initial step is to do an analysis using BLACK BOXto find websites that use BLACK BOX hosting services,as in the case study that will be tested. OWASP ZAP is embedding the search URL university website in KSA in it. with BLACK BOX helps to do an accurate search.

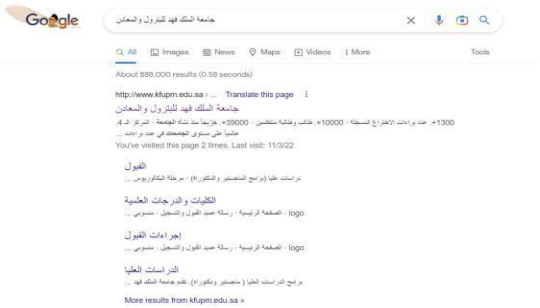


Figure 3.2.1 website

2.2.2 Input URL

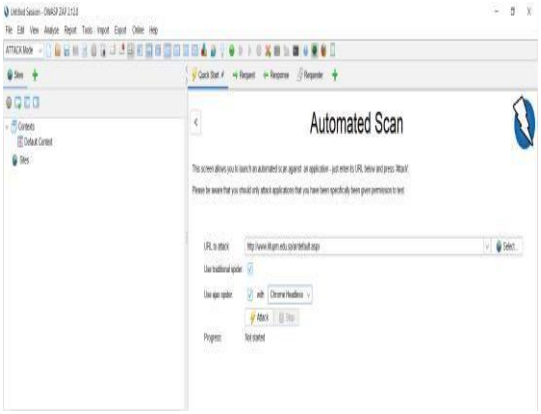


Figure 3.2.2 Input URL website1.Choose Automated Scan.
2.In put the URL of the university website. 3.Checklist Use traditional and Use ajax spider.
4. Choose a browser as a support already installed on thecomputer.
5. Chose attack mode.6.Press Attack.

2.2.3 Proses scanning

Process scanning sends some request access to the web server to find vulnerability by link or URL website in it.

Figure 3.2.3 Result Report

2.2.4 Result report

The report is the response after the attack with a scan using OWASP ZAP to send several request access to theweb server to find several vulnerabilities such as contentsecurity tokens, email viewstate, and cookie attributes.

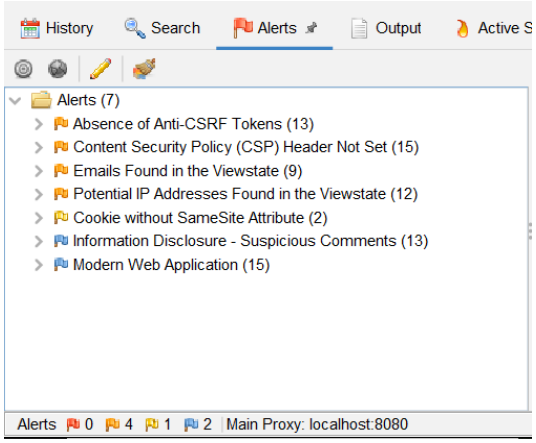


Figure 3.2.4 Result Report

3. Results and Discussion

the results and discussion of the scanning process that has been carried out, the results show that there may be security holes in the targets of several universities in Saudi Arabia, among them as shown in Figure 4.1

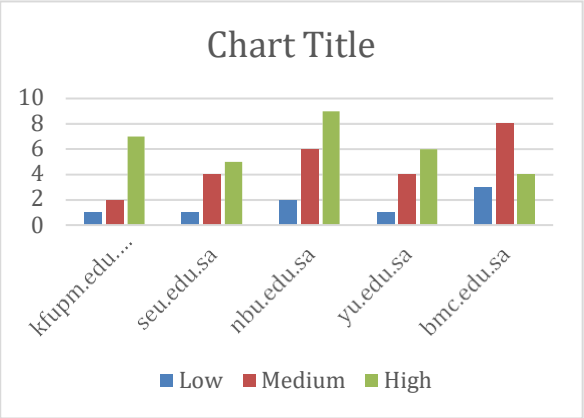


Figure 4.1 Security gap in the domain of several universities in Saudi Arabia

Table 4.1 Security gap in the domain of several universities in Saudi Arabia

	LOW	MEDIUM	HIGH
KFUPM.EDU.SA	1	2	7
SEU.EDU.SA	1	4	5
NBU.EDU.SA	2	6	9
YU.EDU.SA	1	4	6
BMC.EDU.SA	3	8	4

shows a graph of the scan results using the OWASPZapautomation application which shows the number of possible security holes that exist on the target web according to the level of threat here divided into 3categories based on the effects of these security holes, namely High, Medium and Low. Furthermore, the results of the scanning process using the WPScan tool are shown in Figure 4. 2. In Figure 4.2, this explains thenumber of possible types of security holes that exist in each web.

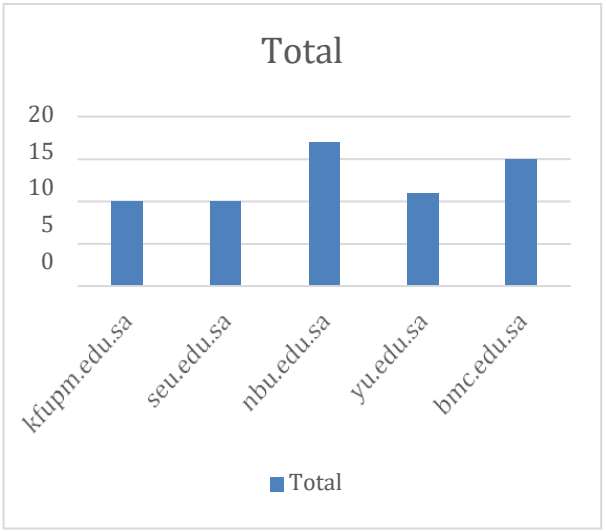


Figure 4.2. Number of threat types scanned fromOWASP

4.1.1. OWASP ZAP automation application

The results of the report issued by the application will show the alertas shown in figure 4.3 it contains the risk

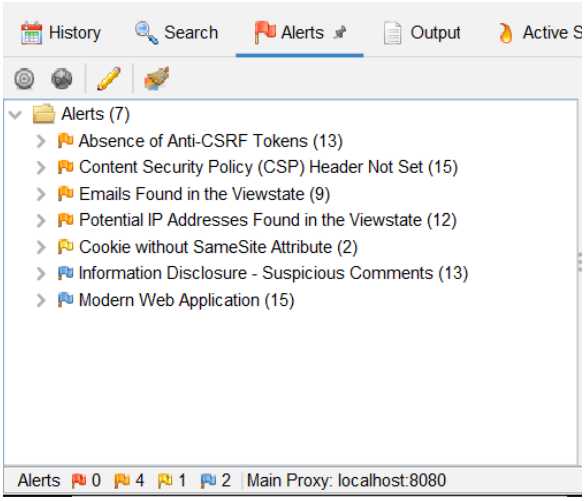


Figure 4.3 Security vulnerabilities report

And beside this bar shown another bar contains the vulnerabilities risk level, category or name of the vulnerabilities, the location of the vulnerabilities,methods, parameters and also the last solution to deal with these vulnerabilities as shown in Figure 4. 3 and Figure 4. 4

Figure 4. 4 Solutions to overcome security holes

Meanwhile, reports with xml format are different in appearance from html but have the same content as

Figure 4.5 below

4.2 Discussion

4.2.1 OWASP ZAP automation application

At this stage, the use of the OWASPZap automation application will be explained. The application display isas shown in Figure 4.6 and figure 4.7.

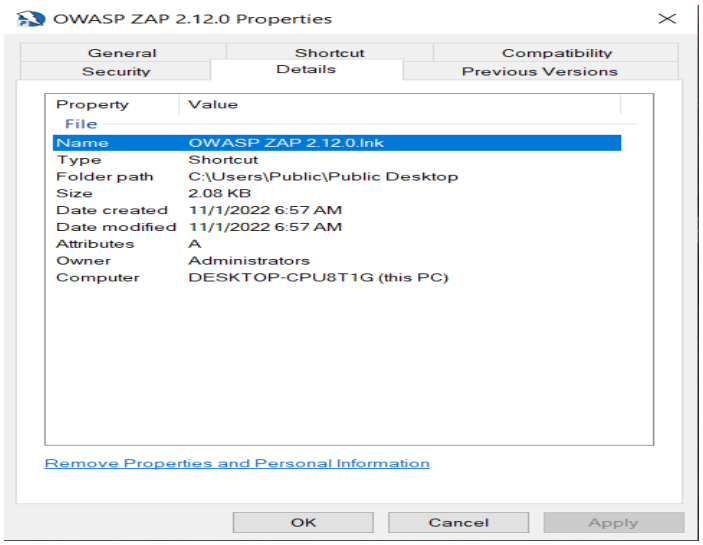
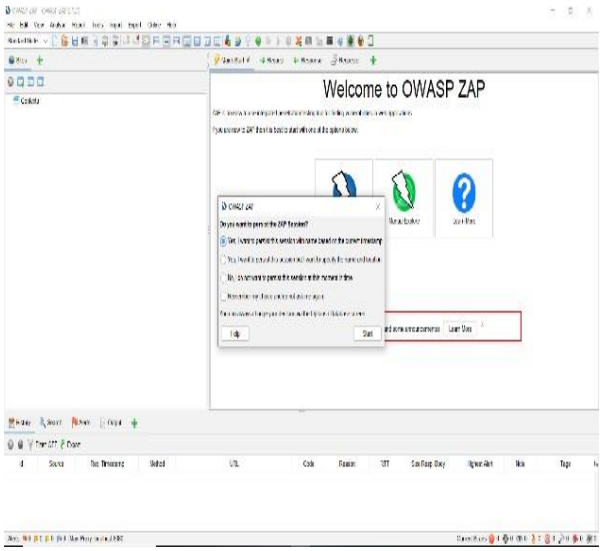


Figure 4.6 OWASP Zap automation application file

Figure 4.7 OWASP Zap automation applicationshortcut

First the user opens the OWASP application and the application will ask how the result want to be saved. Theissued file will be saved in the format of the target nameand the date and time the scanning process was completed as shown in Figure 4.8



For the next step choose Automated Scan as shown in

Figure 4.9

And for the next step enters the target URL to be scannedas shown in Figure 4. 10. Here the author gives an example using the website of a university in SaudiArabia, namely using the web url http://www.kfupm.edu.sa/ar/default. aspx for the scanning process.

Put the checklist Use traditional and Use ajax spider on the bar and Choose a browser as a support alreadyinstalled on the computer as shown in figure 4.10 and choose attack mode and press the attack to run thescanned process

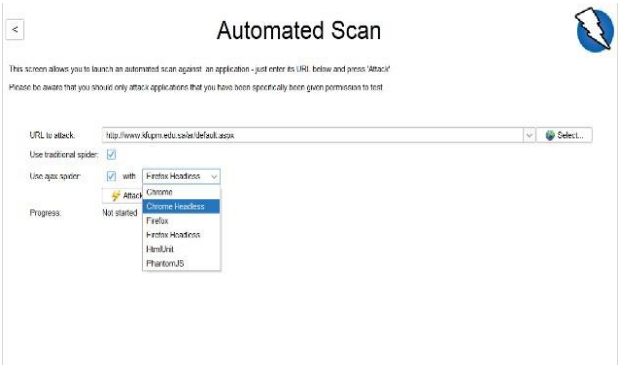


Figure 4.10

will automatically proceed to the next stage, namely thescan progress shown in Figure 4. 11 This stage aims to search for security holes on the target web

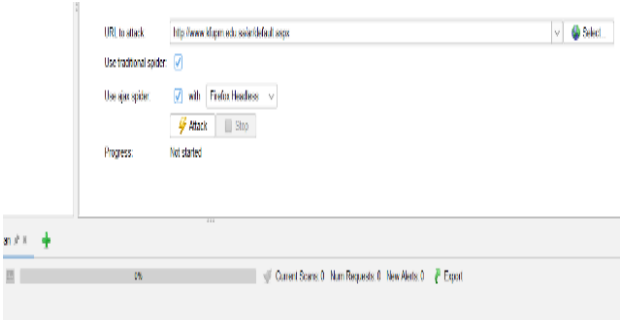


Figure 4. 11

4. 3. Analysis

At this early stage the author uses several tools to find information about the target web that will be tested pentest. By using the search engine, namely Google, as shown in Figure 4. 15. In Figure 4. 15, it is found that several university targets in Saudi Arabia have main websites with the name

4.3.1 kfupm.edu.sa

Figure 4.3.1 King Fahd University ofPetroleum & Minerals.

4.3.2 seu.edu.sa

Figure 4.3.2 Saudi ElectronicUniversity.

4.3.3 nbu.edu.sa

Figure 4.3.3 Northern Border University.

4.3.4 yu.edu.sa

Figure 4.3.4 Al-Yamamah University.

4.3.5 bmc.edu.sa

Figure 4.3.5 Batterjee MedicalCollege.

The results that have been obtained from scanning andtesting using OWASP ZAPare in the form of several security vulnerabilities with Low, medium and high levels. The results will be grouped according to the services that have been used and the number of securityvulnerabilities that have been found on the website willbe calculated, and the total number of security vulnerabilities found on the websitewill be grouped bythe type of service and the level of security vulnerabilities that have been found. The results will bemade into a table like the following:

1. kfupm.edu.sa

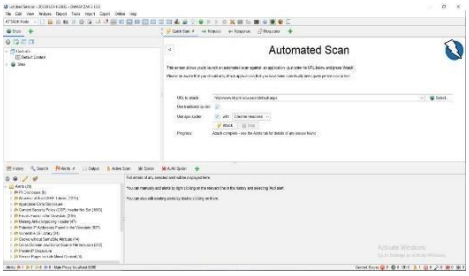


Figure 4.3.6 spider.

On the website kfupm.edu.sa a security vulnerability hasbeen found. A total of 1 security holes that have a Severity risk rating which are categorized assecurity holes with a High level of vulnerability.
A total of 7 security holes that have a Severity risk rating which are categorized assecurity holes with a Medium level of vulnerability.
A total of 6 security holes that have a Severity risk rating which are categorized assecurity holes with a Low level of vulnerability.
It is known that there are a total of 14 secuity holes found, the High category is having a higher priority for immediate fixing or repairs so that the resulting impactcan be reduced or even lost immediately.
It Found 1 High category with the gap name PII Disclosure

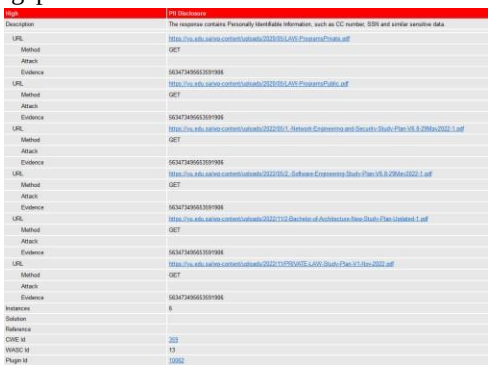


Figure 4.3.7 type of gap.

PII is an extension of Personally Identifiable Information so this response contains Personally Identifiable Information, such as CC number, SSN andsimilar sensitive data. For the solution check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

2. seu.edu.sa

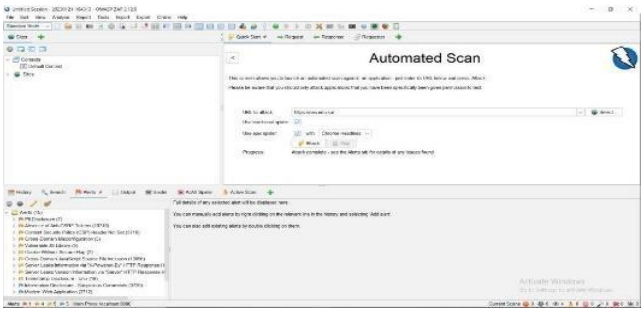


Figure 4.3.8 alerts.

On the website seu.edu.sa a security vulnerability has been found.

A total of 1 security holes that have a Severity risk ratingwhich are categorized assecurity holes with a High levelof vulnerability.

A total of 4 security holes that have a Severity risk ratingwhich are categorized assecurity holes with a Medium level of vulnerability.

A total of 5 security holes that have a Severity risk ratingwhich are categorized assecurity holes with a Low level of vulnerability.

It is known that there are a total of 10 security holes found, the High category is having a higher priority for immediate fixing or repairs so that the resulting impact can be reduced or even lost immediately.

It Found 1 High category with the gap name PII Disclosure

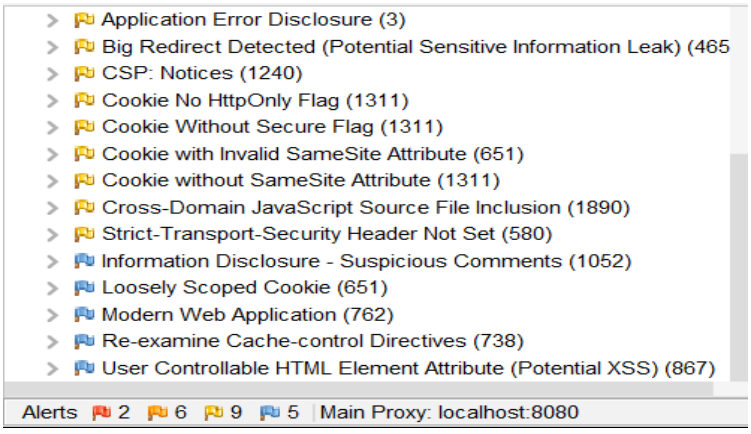


Figure 4.3.9 Alerts

Figure 4.3.10 Describe.

.

On the website nbu.edu.sa a security vulnerability has been found. A total of 2 security holes that have a Severity risk rating which are categorized assecurity holes with a High level of vulnerability. A total of 6 security holes that have a Severity risk rating which arecategorized assecurity holes with a Medium level of vulnerability. A total of 9 security holes that have a Severity risk rating which are categorized assecurity holes with a Low level of vulnerability.

3. yu.edu.sa

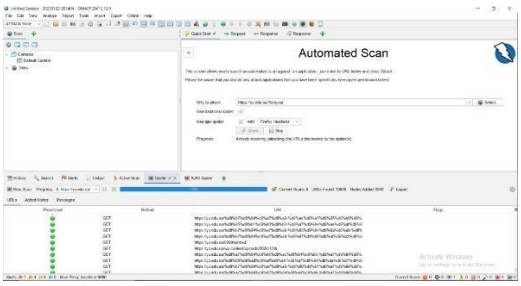


Figure 4.3.11 Spider.

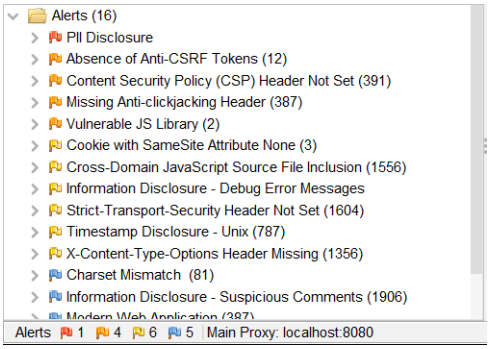


Figure 4.3.12 Alerts

Figure 4.3.13 Describe.

On the website yu.edu.sa a security vulnerability has been found. A total of 1 security holes that have a Severity risk rating which are categorized assecurity holes with a High level of vulnerability.
A total of 4 security holes that have a Severity risk ratingwhich are categorized assecurity holes with a Medium level of vulnerability. A total of 6 security holes that havea Severity risk rating which are categorized assecurity holes with a Low level of vulnerability.

4. bmc.edu.sa

Figure 4.3.14 Alerts.

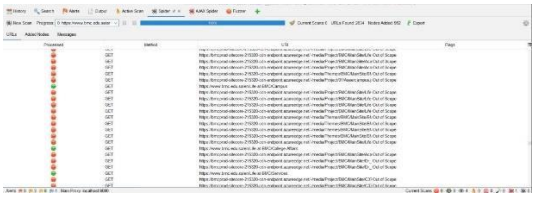


Figure 4.3.15 Spider.

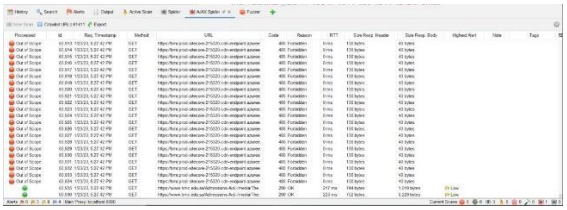


Figure 4.3.16 Ajax spider.

On the website bmc.edu.sa a security vulnerability hasbeen found.
A total of 0 security holes that have a Severity risk rating which are categorized assecurity holes with a High level of vulnerability.
A total of 3 security holes that have a Severity risk rating

which are categorized assecurity holes with a Medium level of vulnerability.

A total of 8 security holes that have a Severity risk rating which are categorized assecurity holes with a Low level of vulnerability.

4. Conclusion and Suggestion

When I already testing from severel website in KSA universitys I found

Table 5.1 total

No.	University	High	Medium	Low	Total
1	King Fahd University of Petroleum & Minerals	1	7	6	14
2	Northern Border University	2	6	9	17
3	Saudi Electronic University	0	4	4	8
4	. Al-Yamamah University	1	4	6	11
5	Batterjee Medical College	0	6	10	16
Total		4	17	35	66

So from the result testing I found in the KSA universitythere is still many low risk and less high risk. The conclusion is the secure website on medium level and make more attention on the low risk level.

5.1 suggestion

For the next researcher I hope use my research for yourstudy and make new adaptions to make the websites more secure especially university.

Reference

[1] A. Verma, A. Khatana, and S. Chaudhary, "A Comparative Study of Black Box Testing and White Box Testing," Int. J. Comput. Sci. Eng., vol. 5, pp. 301–304,Dec. 2017, doi: 10.26438/ijcse/v5i12.301304.

[2] H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in 2018IEEE Long Island Systems, Applications and Technology Conference (LISAT), May 2018, pp. 1–7. doi: 10.1109/LISAT.2018.8378035.

[3] D. Hariyadi and F. E. Nastiti, "AnalisisKeamanan Sistem Informasi Menggunakan Sudomy dan A total of 0 security holes that have a Severity risk rating OWASP ZAP di Universitas Duta Bangsa Surakarta," J. J. Ilm. Inform. Komput., vol. 24, no. 1, Art. no. 1, Aug.2019, doi: 10.35760/ik.2019.v24i1.1988.

[5] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," CESS J. Comput. Eng.Syst. Sci., vol. 6, no. 2, Art. no. 2, Jul. 2021, doi:10.24114/cess.v6i2.24777.

[6] A. Nugroho, D. Rizaludin, S. Soebandhi, L. Junaedi, S. Winardi, and M. N. Al- Azam, "Automatic Sign of Commencement of Work from Enterprise Resource Planning," in 2020 International Conference on Smart Technology and Applications (ICoSTA), 2020, pp. 1–6.

[7] M. Qasaimeh, A. Shamlawi, and T. Khairallah,"BLACK BOX EVALUATION OF WEB APPLICATION SCANNERS: STANDARDS MAPPING APPROACH," J. Theor. Appl. Inf. Technol.,vol. 22, Jul. 2018.

[8] "Black Box Testing on ukmbantul.com Pagewith Boundary Value Analysis and Equivalence Partitioning Methods-IOPscience." https://iopscience.iop.org/article/10.1088/1742- 6596/1823/1/012029/meta (accessed Jan. 31, 2023).

[9]A. Lamba, "Cyber Attack Prevention UsingVAPT Tools (Vulnerability Assessment & Penetration Testing)." Rochester, NY, 2014. Accessed: Jan. 31, 2023. [Online]. Available: https://papers.ssrn.com/abstract=3516069

[10]M. E. Khan, "Different Approaches to Black Box Testing Technique for Finding Errors." Rochester, NY, Jul. 21, 2021. Accessed: Jan. 31, 2023. [Online]. Available: https://papers.ssrn.com/abstract=3890672

[11]D. R. Pratama, K. E. Susilo, and A. Nugroho, "Implementasi Metode Waterfall Pada Sistem InformasiKapasitas Pengoperasian Kapal," J. Ilmu Komput. Dan Bisnis, vol. 13, no. 1, pp. 36–49, 2022.

[12]"IMPLEMENTASI OWASP ZAP UNTUKPENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK | Jurnal Teknologi Informasi: JurnalKeilmuan dan Aplikasi Bidang Teknik Informatika." https://e journal.upr.ac.id/index.php/JTI/article/view/3995(accessed Nov. 03, 2022).

[13]13523025 Adetya Putra Dewanto, "PENETRATTESTING PAD DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10," Sep. 2018, Accessed: Jan. 31, 2023. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/11281

[14]R. Pramudita, "Pengujian Black Box pada AplikasiEcampus Menggunakan Metode Equivalence Partitioning," Inform. Educ. Prof. J. Inform., vol. 4, no.2, pp. 193–202, Jun. 2020, doi: 10.51211/itbi.v4i2.1347.

[15]Amanda and I. R. Widiasari, "'SIASAT' UKSW (UNIVERSITAS KRISTEN SATYA WACANA)WEBSITE SECURITY ANALYSIS USING OWASP (OPEN WEB APPLICATION SECURITY PROJECT)," J. Tek. Inform. Jutif, vol. 3, no. 3, Art. no.3, Jun. 2022, doi: 10.20884/1.jutif.2022.3.3.346.

[16]I. Rosydi, A. Nugroho, and A. Ambarwati, "SistemMonitoring BTS Pada Perusahaan TelekomunikasiSeluler Berbasis Aplikasi Mobile," JOINTECS J. Inf.Technol. Comput. Sci., vol. 7, no. 3, pp. 93–100, 2022. [17]D. Sagar, S. Kukreja, J. Brahma, S. Tyagi, and P.Jain, "STUDYING OPEN SOURCE VULNERABILITY SCANNERS FORVULNERABILITIES IN WEB APPLICATIONS," Comput. Sci., vol. 9, p. 7, 2018.

[18]S. -, I. Riadi, and P. Ananda, "Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 11, 2019, doi: 10.14569/IJACSA.2019.0101118.

[19]D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of WebsiteApplication Using OWASP," Int. J. Comput. Inf. Syst. IJCIS, vol. 3, no. 3, Art. no. 3, Aug. 2022, doi: 10.29040/ijcis.v3i3.90.

[20]I. F. Ashari, M. Alfarizi, M. N. K, and M. A. H, "Vulnerability Analysis And Proven On The neonime.co Website using OWASP Zap 4 and XSpear," JTKSI J. Teknol. Komput. Dan Sist. Inf., vol. 5, no. 2, Art. no. 2,May 2022, doi: 10.56327/jtksi.v5i2.1130.

