

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 <u>faisal.a.g.l69@gmail.com</u> Narotama University, Surabaya, Indonesia Aryo Nugroho <u>Aryo.nugroho@narotama.ac.id</u> 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 of users 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 of an 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 its integrity. The fall of information to other parties who arenot authorised can cause harm to the organisation so that the 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 the level 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 testing method. 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 methods is 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 used nOWASP 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:

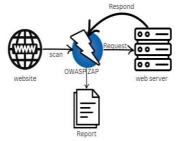


Figure 3.1 Flow or steps of research methodology

#### 2.1 Research methods

Explanation of the flow of research methods in Picture

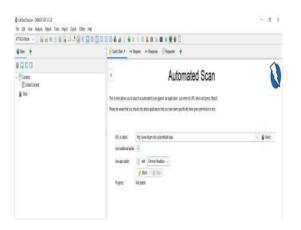
3.1 The flow or steps of the research methodology basedon the sequence:

#### 2.2.1 website

The initial step is to do an analysis using BLACK BOX to 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.

Goggle	جامعه البلك فهد للبترول والمعادن	×	<b>0 0</b>
	Q All 🔄 Images 🖹 News 🖗 Maps 🗈 Videos I More		Tools
	About 888,000 results (0.58 seconds)		
	http://www.kfupm.edu.sa > Translate this page		
	جامعة الملك فهد للبتر ول و المعادن		
	ت الاحتراع السبطة - 10000+, طالب وطالبة استخليق - 99000 - بحريط النا الطبطة - على كار الد له مثلياً على سنوى الطبطان في مدير الات You've visited this page 2 limes. Last visit: 11/3/22	+, هذيراءك	1300
	القبول دراست طبا (برامج الباجشر و التكور 8) - مرحلة التكاور يوس		
	الكليات و الدرجان العليية logo - تصفحه ترتيبيه - رسلة صيد تقول والسجن - مسربي		
	الجر امات القبول - اصلحة الرئيسة - رسلة صيد الفول والشجل - مدوني		
	ير امح التر البلك النقيا ( متصنير ا وتكاور (s): تقدم جمعة النقال فها		
	More results from kfurm edu sa a		

# 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 the computer.
- 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.

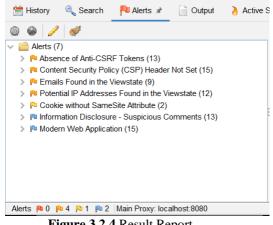


Figure 3.2.4 Result Report

# 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

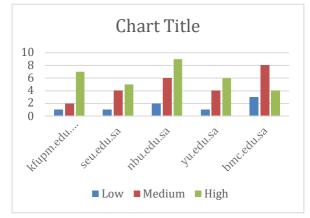


Figure 4.1 Security gap in the domain of several universities in Saudi Arabia

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.

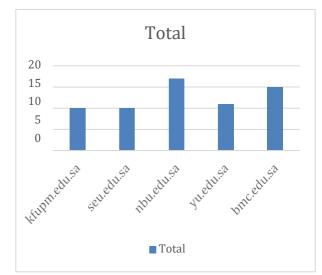


Figure 4.2. Number of threat types scanned fromOWASP

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

🛗 History	🔍 Search	🏴 Alerts 🖈	Output	👌 Active S
0 0 /	1			
✓  → Alerts (7)	')			
> 🏴 Abser	nce of Anti-CSR	F Tokens (13)		
> P Conte	ent Security Poli	cy (CSP) Header	Not Set (15)	
> 🏴 Email	s Found in the \	/iewstate (9)		
> P Poten	tial IP Addresse	s Found in the Vi	ewstate (12)	
> P Cooki	e without Same	Site Attribute (2)		
> 🏴 Inform	nation Disclosur	e - Suspicious Co	omments (13)	
> 🏴 Mode	rn Web Applicat	ion (15)		
Alerts 🎮 0 🖡	4 🎮 1 🎮 2	Main Proxy: loca	alhost:8080	

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

bsence of	Anti-CSRF Tokens	
RL	https://yu.edu.sa/abiut/policies/	
lisk .	P Medum	
orfidence.	Low	
arameter.		
mack:		
aidence:	<form action="https://yu.edu.sa" class="searchform" id="searchform" method="gef" role="search"></form>	
WE D	362	
NASCID:		
Source	Passive (10202 - Absence of Anti-CSRF Tokens)	
put Vector		
Descriptio	*	
	te request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in o gplication functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a we	
Other Info.		
	Arpi-CSRF tokun (anteur), CSRFTokun,Request/wirlicationTokun, cardmiddiewantokun, authenticity, tokun, CWASP, CSRFTOKEH, anore srf_token; was tound in the following HTML form: (Form 1 Tang" %" Search, n., pisze, form " Searchoubrief").	carf, carf_baken, _carf, _confSecret,carf_mage, CSRF,
Solution		
Phase Ar	chilecture and Design	
	ed library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid sle, use anti-CSRF packages such as the OWASP CSRF Guant.	
Reference		
	ntis webspepace.org/Cross-Site-Request-Forgery mitre org/Cata-Metriziane/352.html	

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.

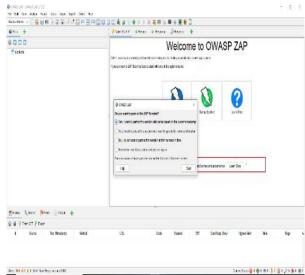
General	Shortcut	Compatib	
Security	Details	Previous Versi	ons
Property File	Value		
Name	OWASP ZAP 2.12.0.lnk		
Туре	Shortcut		
Folder path	C:\Users\Public\Public	Desktop	
Size	2.08 KB		
	11/1/2022 6:57 AM 11/1/2022 6:57 AM		
Attributes	A		
Owner	Administrators		
Computer	DESKTOP-CPU8T1G (th	nis PC)	
emove Proper	ties and Personal Informa	ation	

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

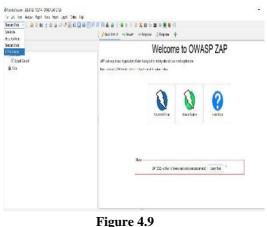


Figure 4.9

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 already installed on the computer as shown in figure 4.10 and choose attack mode and press the attack to run thescanned process

		nated scan against an application - just enter its URL below and press 'Attack' ck applications that you have been specifically been given permission to test	
RL to attack	10.00	Klopm edu sələri defəuli. əsax	🗸 🏙 Select
ise traditional spider.		kupm.edu.sakar.detaun.aspik	V Gelect
ise ajax spider	V with	Firefox Headless V	
Yrogress.	Sector Attack	Convertiendeus Preiss Freiss Freiss Handloo Handloù Freissen	
		T HEROTRO	



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

URL in steck Ute taithoral spu Use sjor sjoler Progress	Itip Jawa digan edu selectidefa il aego ✔ with Fredu Headnes ↓ ✔ Attack 100 3100 Not darted	V Select.
n / 1 +	 ∳ Curret Scenc 0. Hun Reguest: 0. Hen Henc 0. ∦ Esport	

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 of Petroleum & Minerals.

# 4.3.2 seu.edu.sa



# Figure 4.3.2 Saudi ElectronicUniversity.



### Figure 4.3.3 Northern Border University.



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 security vulnerabilities that have been found on the website will be calculated, and the total number of security vulnerabilities found on the websitewill be grouped by the 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

#10 ÷	🖓 tasta / - Houri - Houri - Staure
0 D C D Destrict Destinen 9 Des	Automated Scan
	H & Least reverse they independent age - ♥ Break to a same year ≥ Marcine ♥ (0) (normalisment - ) Marcine ♥ (0) (normalisment - ) Marcine ♥ (0) (normalisment +
	Training ( ) And the pair of the state of th
Time Cost Past Lines &	

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

Description	The response contains. Personally identifiable information, such as CC number, SSN and sensitive data
URL	Ittin, Proceduce and content/uploads/2020/15 LAW, ProgramsPrivate and
Method	0E1
Attack	
Evidence	\$63473495653591994
URL	Http://www.usavo.comm/subrads/2020/05LAW-PropartsPublic.of
Method	QET
Attack	
Evidence	563473495653591934
URL	https://www.edu.tativo.content/ustoads/2022/05/1.Network Engineering and Security Study Plan VK-0.29Max/2022.1.pdf
Method	GET
Attack	
Evidence	563473496653599904
URL.	Hips. Pys. edu. salvo.content/usicada/2022/05/2. Gatavare Engineering Study Plan VEB /29Mav2022-1.adf
Method	GET
Attack	
Evidence	563473495643599994
URL	Https://www.edu.nativo.coment/ur/audio/2022/11/2 Dischelar of Architecture-Term Study-Flam Updated-1 mF
Method	GET
Attack	
Evidence	5634734954535919H
URL.	Https://www.nductaaling.commet/uploadia/2022/11/PRV/ATE-LAW-Study-Plan-V1/Hpv-2022.pdf
Method	OET
Attack	
Evidence	563473495653581996
instances	6
Solution	
Reference	
CWE M	253
WASC M	13
Plugin Id	10952

### 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 and similar 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

eter +	1 # Gant Sant + → Regard → Reserver @Regards
0000	
Consult     En United Counsel     En United Counsel     En United Counsel	Automated Scan
	refeare to water that you that all all all all all all all their street theory and their grant all all all all all all all all all al
	(Autophone) galary 🖸
	the ascigator at the second reading -
	Property Alexandro consider - see the Marta set for costs of any bases fund
Minday Sylmadi Million 4	RADING SANS
00/0	Tail familie of any selected alart will be disalised way
- Contraction (C)	You can measure and even to reproduce the relevance into the relevance and selecting. Add sum
<ol> <li>Ste Almonic of Anko 2008" Training (20192)</li> </ol>	Visi can also addirected allera bir double clisting on them.
Proceedings of the second	

# 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 level f vulnerability.

A total of 4 security holes that have a Severity risk rating which 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

> 5	Application Error Disclosure (3)
> 5	Big Redirect Detected (Potential Sensitive Information Leak) (465
> 5	SP: Notices (1240)
> 5	Cookie No HttpOnly Flag (1311)
> 5	Cookie Without Secure Flag (1311)
> 5	Cookie with Invalid SameSite Attribute (651)
> 5	Cookie without SameSite Attribute (1311)
> 5	Cross-Domain JavaScript Source File Inclusion (1890)
> 5	Strict-Transport-Security Header Not Set (580)
> 5	Information Disclosure - Suspicious Comments (1052)
>	Loosely Scoped Cookie (651)
> 5	Modern Web Application (762)
> 5	Re-examine Cache-control Directives (738)
> 5	User Controllable HTML Element Attribute (Potential XSS) (867)
Alerts	🍽 2 💫 6 🟳 9 🏴 5   Main Proxy: localhost:8080

#### Figure 4.3.9 Alerts

Source. Persona (10055 - CSP) Input Vector Conception		
attacks are used for everything from data theft to site defacement or distribut	of and miggle nation types of allastic holding (but not hinked by Clause Ste Scoping (XSS), and date repoten allastic and makaze. CSP provides a set of standard HTTP facetors that allow website averas to beckere approved sources of c edge GSS, HTVI, frames, forts, images and embeddiatic objects such as Java applets, ActiveS, and to retuides files.	
Otterinle		
style sit includes unsafe inline.		
Salata		
Ensure that your web server, application server, head balancer, etc. is proper	y configured to set the Conten-Security-Pulicy heads	
listenerge		
htp://www.siturg/TROSPD htp://www.siturg/TROSPD htp://www.secont/freexity-policy		
Alert Tage		
Key	Value	
CHARP 201 AN CHARP 2017 AG	Horshave of tel MMC 2015 Seeing Jacobia near titles brook of wave sets to see a first of the 2017 Second y Macrobia de that Activate Windows Chair Self age tradition Windows	(19-5
	Canat Son 🖉 0 🖓 0 🐨 1 🤰 0 🤯 0 🌶	10 <b>*</b> 0 <b>*</b>

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 are categorized 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 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

	Alerts (16) Alerts (16) Alerts (16) Alerts (16) Alerts (16) Content Security Policy (CSP) Header Not Set (391) Kontenticickjacking Header (387) Volinerable JS Library (2) Cooke with SameSite Attribute None (3) Cross-Domain JavaScript Source File Inclusion (1556) Pi Information Disclosure - Debug Error Messages Strict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) K-Content-Type-Options Header Missing (1366) Pi Information Disclosure - Suspicious Comments (1906) Pi Information Disclosure - Suspicious Comments (1906)	00		<
Alerts (16) Alerts (16) Alerts (16) Alerts (16) Alerts (16) Alerts (16) Pl Disclosure Pl Absence of Anti-CSRF Tokens (12) Pc Content Security Policy (CSP) Header Not Set (391) Pk Unlerable JS Library (2) Pc Cookie with SameSite Attribute None (3) Pc Content-Trype-Options Header Not Set (1604) Pi Information Disclosure - Debug Error Messages Pc Strict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) Pc X-Content-Type-Options Header Missing (1366) Pi Information Disclosure - Suspicious Comments (1906) Pi Information Disclosure - Suspicious Comments (1906) Pi Information Disclosure - Suspicious Comments (1906)	Figure 4.3.12 Alerts		<ul> <li>Automated Scan</li> </ul>	
Alerts (16) Alerts (16) Alerts (16) Pi Disclosure Pi Absence of Anti-CSRF Tokens (12) Pi Content Security Policy (CSP) Header Not Set (391) Pi Missing Anti-clickjacking Header (387) Pi Content Steratory Disclosure - Debug Error Messages Pi Stict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) Pi X-Content-Type-Options Header Missing (1356) Pi Consret Mismatch (81) Pi Information Disclosure - Suspicious Comments (1906) Worker Web Analication (287)	Pictorent States (16) Pictorent States (17) Pictorent States (18) Pictorent Sta	El Ses		
Alerts (16) Pi Alosna data and a static and a s	Picture description of the first state state of the first state of the first state of the first state			V . @ 5001
Alerts (16) P Alerts	Providence of the second se			
Alerts (16) Pi Alosna of Anti-CSRF Tokens (12) Pi Content Security Policy (CSP) Header Not Set (391) Pi Missing Anti-clickjacking Header (387) Pi Content Security Policy (CSP) Header Not Set (391) Pi Missing Anti-clickjacking Header (387) Pi Cookie with SameSite Attribute None (3) Pi Cookie with SameSite Attribute None (3) Pi Cross-Domain JavaScript Source File Inclusion (1556) Pi Information Disclosure - Debug Error Messages Stitct-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) Pi X-Content-Type-Options Header Missing (1366) Pi Charset Mismatch (81) Pi Information Disclosure - Suspicious Comments (1906) Worden Web Analication (287)	Context (16) Performance of Anti-CSRF Tokens (12) Performance of Anti-CSRF Tokens (13) Performance of Anti-CSRF Tokens (13) Performance of State of State of Anti-CSRF Tokens (13) Performance of State of Sta		distant bir Ser	
Alerts (16) Pi Abesce of Anti-CSRF Tokens (12) Pi Content Security Policy (CSP) Header Not Set (391) Pi Vulnerable JS Library (2) Pi Content Security Policy (CSP) Header Not Set (391) Pi Vulnerable JS Library (2) Pi Content Security Policy (CSP) Header Not Set (1556) Pi Vulnerable JS Library (2) Pi Consen Jbarestite Attribute None (3) Pi Cross-Domain JavaScript Source File Inclusion (1556) Pi Information Disclosure - Debug Error Messages Pi Strict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) Pi Consent Missing (1356) Pi Charset Missing (136) Pi Charset Missing (137) Pi Vansetamp Disclosure - Suspicious Comments (1906) Modern Web Analization (287)	Alerts (16) P PII Discosure P Volnerable JS Library (2) P Content Security Policy (CSP) Header Not Set (391) P Volnerable JS Library (2) P Content Security Policy (CSP) Header Not Set (391) P Volnerable JS Library (2) P Content Security Policy (CSP) Header Not Set (391) P Volnerable JS Library (2) P Conse-Domain JavaScript Source File Inclusion (1556) P Strict-Transport-Security Header Not Set (1604) P Charset Mismatch (81) P Under Mak Anolication (1267) Alerts P 1 P 4 P 6 P 5 Main Proxy: localhost:8080		culture. Active annual fillenced unit or y managed of a date of	
Merrie Maria	Image: Control of the second secon			
Content Security Policy (CSP) Header Not Set (391)     Pi Missing Anti-clickjacking Header (387)     Pi Content Security Policy (CSP) Header Not Set (391)     Pi Content Security Policy (CSP) Header Not Set (391)     Pi Vulnerable JS Library (2)     Pi Content Security Policy (CSP) Header Not Set (1556)     Pi Information Disclosure - Debug Error Messages     Pi Strict-Transport-Security Header Not Set (1604)     Pi Timestamp Disclosure - Unix (787)     Pi Content-Type-Options Header Missing (1356)     Pi Information Disclosure - Suspicious Comments (1906)     Pi Information (371)	Alerts (16) Pi Discissure Pi Content Security Policy (CSP) Header Not Set (391) Pi Content Security Policy (CSP) Header Not Set (391) Pi Missing Anti-clickjacking Header (387) Pi Vulnerable JS Library (2) Pi Content Security Policy (CSP) Header Not Set (391) Pi Vulnerable JS Library (2) Pi Content Security Policy (CSP) Header Not Set (1604) Pi Strict-Transport-Security Header Not Set (1604) Pi Strict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Debug Error Messages Pi Strict-Transport-Security Header Not Set (1604) Pi Timestamp Disclosure - Unix (787) Pi Charset Mismatch (81) Pi Mismatch (81) Pi Mismatch (81) Pi Mismatch (81) Pi Modern Web Annie etco (287) Alerts Pi 1 Pi 4 Pi 6 Pi 5 Main Proxy: localhost:8080	Acted Soley Verseger		
Content Security Policy (CSP) Header Not Set (391)     Pi Vulnerable JS Library (2)     Pi Content Security Policy (CSP) Header Not Set (391)     Pi Vulnerable JS Library (2)     Pi Content Security Policy (CSP) Header Not Set (391)     Pi Vulnerable JS Library (2)     Pi Content Security Policy (CSP) Header Not Set (391)     Pi Vulnerable JS Library (2)     Pi Content Security Policy (CSP) Header Not Set (1556)     Pi Vulnerable JS Library (2)     Pi Constent Security Header Not Set (1604)     Pi Timestamp Disclosure - Debug Error Messages     Pi Strict-Transport-Security Header Not Set (1604)     Pi Timestamp Disclosure - Unix (787)     Pi Conset Missing (1356)     Pi Information Disclosure - Suspicious Comments (1906)     Pi Information Disclosure - (387)	Content Security Policy (CSP) Header Not Set (391) Provide Security Policy (CSP) Header Not Set (1604) Provide Security Policy Security Header Not Set (1604) Provide Security Policy (282) Provide Security Policy (282) Provide Security Header Not Set (1604) Provide Security Policy (282) Provide Security Policy (282) Provide Security Header Not Set (1604) Provide Security Policy (282) Provide Security Header Not Set (1604) Provide Security Policy (282) Provide Security Header Not Set (1604) Provide Security Policy (282) Provide Security Policy (282) Prov		the second	
Alerts (16)     Per PII Disclosure     Per Absence of Anti-CSRF Tokens (12)     Per Content Security Policy (CSP) Header Not Set (391)     Per Missing Anti-clickjacking Header (387)     Per Vulnerable JS Library (2)     Pe Consie with SameSite Attribute None (3)     Pe Cross-Domain JavaScript Source File Inclusion (1556)     Pi Information Disclosure - Debug Error Messages     Pe Strict-Transport-Security Header Not Set (1604)     Pi Timestamp Disclosure - Unix (787)     Pi CArset Missindt (81)     Pi Charset Missindt (81)     Pi Information Disclosure - Suspicious Comments (1906)     Modern Web Analization (387)	Cross-Domain JavaScript Source File Inclusion (1556)     P Strict-Transport-Security Header Not Set (1604)     P Strict-Transport-Security Header Not S	2 047 047	ang un nyu da u an tach o Shaithe na chuaithean a Chaithean Ann An Anna An Anna An Anna An Anna An Anna An Anna Migu nyu da u an tach a Shaithean Anna Anna Anna Anna Anna Anna Anna A	
Alerts (16)     Pu PII Disclosure     Pubsence of Anti-CSRF Tokens (12)     Pubsence of Anti-CSRF Tokens (13)     Pubsence of Anti-CSRF Tokens (136)     Pubsence of Anti-CSRF Tokens (12)     Pubsence of Anti-CSRF Tokens (12)     Pubsence of Anti-CSRF Tokens (1366)     Pubsence of Anti-CSRF Tokens (137)     Pubsence of Anti-CSRF (137)     Pubsen			mpunyuka kabaliya Nadiserin Ina Nadiserin Antonin Kabaliya Kabaliya Kabaliya Kabaliya Kabaliya Kabaliya Kabaliy Mpunyuka kabaliya Kab Mpunyuka Kabaliya Kab	
Alerts (16) Absence of Anti-CSRF Tokens (12) Pi Pil Disclosure Pi Absence of Anti-CSRF Tokens (12) Pi Content Security Policy (CSP) Header Not Set (391) Pi Missing Anti-clickjacking Header (387) Pi Vulnerable JS Library (2) Pi Cookie with SameSite Attribute None (3) Pi Cross-Domain JavaScript Source File Inclusion (1556) Pi Information Disclosure - Debug Error Messages Pi Strict-Transport-Security Header Not Set (1804) Pi Timestamp Disclosure - Unix (787) Pi CAnset Mismatch (81) Pi Information Disclosure - Suspicious Comments (1906) Mindem Web Analication (387)	Alerts (16)  Aler			
Figure 4.3.11 Spider.	Figure 4.3.11 Spider.			
<ul> <li>Pi Cookie with SameSite Attribute None (3)</li> <li>Pi Cross-Domain JavaScript Source File Inclusion (1556)</li> <li>Pi Information Disclosure - Debug Error Messages</li> <li>Pi Strict-Transport-Security Header Not Set (1604)</li> <li>Pi Timestamp Disclosure - Unix (787)</li> <li>Pi X-Content-Type-Options Header Missing (1356)</li> <li>Pi Charset Mismatch (81)</li> <li>Pi Information Disclosure - Suspicious Comments (1906)</li> </ul>	<ul> <li>Pa Cookie with SameSite Attribute None (3)</li> <li>Pa Cross-Domain JavaScript Source File Inclusion (1556)</li> <li>Pa Information Disclosure - Debug Error Messages</li> <li>Pa Strict-Transport-Security Header Not Set (1604)</li> <li>Pa Timestamp Disclosure - Unix (787)</li> <li>Pa X-Content-Type-Options Header Missing (1356)</li> <li>Pa Information Disclosure - Suspicious Comments (1906)</li> <li>Pa Information Disclosure - Suspicious Comments (1906)</li> <li>Pa Information Disclosure - Suspicious Comments (1906)</li> <li>Pa Modern Web Analization (287)</li> <li>Alerts Pa 1 Pa 4 Pa 6 Pa 5 Main Proxy: localhost:8080</li> </ul>	<ul> <li>P Content Sect</li> <li>Missing Anti-</li> </ul>	urity Policy (CSP) Header Not Set (391) clickjacking Header (387)	
<ul> <li>Pel Information Disclosure - Debug Error Messages</li> <li>Pel Strict-Transport-Security Header Not Set (1604)</li> <li>Pel Timestamp Disclosure - Unix (787)</li> <li>Pel X-Content-Type-Options Header Missing (1356)</li> <li>Pel Charset Mismatch (81)</li> <li>Pel Information Disclosure - Suspicious Comments (1906)</li> <li>Pel Information (287)</li> </ul>	Pol Information Disclosure - Debug Error Messages     Pol Strict-Transport-Security Header Not Set (1604)     Pol Timestamp Disclosure - Unix (787)     Pol X-Content-Type-Options Header Missing (1356)     Pol Charset Mismatch (81)     Pol Information Disclosure - Suspicious Comments (1906)     Dot Modern Web Analication (187) Alerts Pol 1 Pol 6 Pol 5 Main Proxy: localhost:8080	🔉 Ҏ Cookie with S	SameSite Attribute None (3)	1
	Po Strict-Transport-Security Header Not Set (1664)     Po Timestamp Disclosure - Unix (787)     Po X-Content-Type-Options Header Missing (1356)     Po Charset Mismatch (81)     Po Information Disclosure - Suspicious Comments (1906)     Dotter Web Application (287) Alerts Po 1 Po 4 Po 6 Po 5 Main Proxy: localhost.8080			
Rev X-Content-Type-Options Header Missing (1356)     Rev Charset Mismatch (81)     Rev Information Disclosure - Suspicious Comments (1906)     Rev Medern Web Application (387)	<ul> <li>         Pi X-Content-Type-Options Header Missing (1356)     </li> <li>         Pi Charset Mismatch (81)     </li> <li>         Pi Information Disclosure - Suspicious Comments (1906)     </li> <li>         Modern Web Analication (387)     </li> <li>         Alerts Pi 1 Pi 4 Pi 6 Pi 5 Main Proxy: localhost:8080      </li> <li>         Figure 4.3.12 Alerts     </li> </ul>		• •	
Pi Charset Mismatch (81)     Pi Information Disclosure - Suspicious Comments (1906)     Bi Modern Web Application (387)	Pi Charset Mismatch (81) Pi Information Disclosure - Suspicious Comments (1906) Disclosure - Suspicious Comments (1906) Disclosure - Modern Web Analication (287) Alerts Pi 1 Pi 4 Pi 6 Pi 5 Main Proxy: localhost:8080  Figure 4.3.12 Alerts			
Pu Information Disclosure - Suspicious Comments (1906)     Mudern Web Application (387)	Pi Information Disclosure - Suspicious Comments (1906)  New Modern Web Analication (387)  Alerts Pi 1 Pi 4 Pi 6 Pi 5 Main Proxy: localhost:8080  Figure 4.3.12 Alerts			
Modern Web Application (387)	Alerts P 1 P 4 P 6 P 5 Main Proxy: localhost.8080			
Alerts Pu 1 Pu 4 Pu 6 Pu 5 Main Proxy: localhost:8080	Figure 4.3.12 Alerts		Sciesdie Caspicious Comments (1000)	
	insues of MonCOM Filesen URI: Intelligence of MonCommentation and American Decimal Commentation and American American American American Conference Store	> 🎮 Information D	Application (387)	
	Assessed Moto-Caller Transm 1981 - Standard Assessed Asses 1986 - Robert Assessed			
	Confidence: Low	> P Information D Modern Web Alerts P 1 P 4 P	6 📭 5   Main Proxy: localhost:8080	
181 mps/garacsobarperes		> P Information D Modern Web Alerts P 1 P 4 P Fig	6 📭 5   Main Proxy: localhost:8080	

Excence:	-tom rolen" search" methodningen" (dim"searchDorm" classin"searchDorm" accomfitted viguadu sal"-	
UNE LL	112	
WASC D.		
Seeres	Perceve) (1992 - Advence-or Anti-COUL Educed)	
band Visits		
Dennitive		
Acress	CHM laters was have an eff the activities in the site respect largery is an attack that invites funcing a sictim to send on HTTP request to a target destination without application to have been predicted as 110 Januar states on a secondation and . The invites of the stark is the 22111	her knowledge of intent in order to perform an action as the victim. The underging sophole the model has a used where the score of a constant, orders whe scoping.
Oterint	N	
	n kei-25 tii sisamaataat (25 tii teken). Hagaattaanataat een connakteensisan aaturiset, teen (20 Catijoket eastaastin teitskeig Pitte tem, Panelli Say "S"saastuju jakke (soo "seestaaste").	REP OSE ICHER announ, cal laters, cel, stattions, cel mage, CER,
Neas-		
Likeste	Aufliciture and Decign nind Barry, or transition from doer not active this seekness to prease or provides the statement that make the seekness a right case and colorid packages each as the CONSET CODE States.	AN SAFE AND T
Falance		
	pets webspree and Costs for Request Eastery	

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 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.

#### 4. bmc.edu.sa



Figure 4.3.14 Alerts.

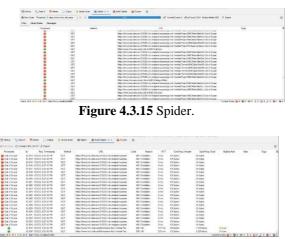


Figure 4.3.16 Ajax spider.

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

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

Table 5.1 total

So from the result testing I found in the KSA university there 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." <u>https://e</u> journal.upr.ac.id/index.php/JTI/article/view/3995(accessed Nov. 03, 2022).

[13]13523025AdetyaPutraDewanto, "PENETRATTESTINGPADDOMAINUII.AC.IDMENGGUNAKANOWASP10,"Sep.2018,Accessed: Jan.31,2023.[Online].Available:https://dspace.uii.ac.id/handle/123456789/11281Sep.2018,Accessed: Jan.31,2023.[Online].Available:

[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 TelekomunikasiSelulerBerbasis 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 SOURCEVULNERABILITYSCANNERSFORVULNERABILITIES 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.