# BAB V

# HASIL DAN PEMBAHASAN

# 5.1. Hasil

Hasil audit yang telah dilakukan berdasarkan metode OWASP *Testing v* 4 didapatkan hasil pada ketiga *website* UMP tidak lolos uji pada 31 kontrol uji dari 65 kontrol uji di 8 sub kategori standar ditandai dengan tanda  $\mathbf{E}$  dapat dilihat pada tabel 5.1 dan penjelasan masing masing hasil kontrol terlampir.

No	Tahapan Kontrol	Website	Website	Website
		Portal	Simak	Journal
1	OTG-INFO-001			
2	OTG-INFO-002	×	×	×
3	OTG-INFO-003	×		×
4	OTG-INFO-004			
5	OTG-INFO-005	×		×
6	OTG-INFO-006	×	×	X
7	OTG-INFO-007	×	×	×
8	OTG-INFO-008		×	
9	OTG-INFO-009	×		×
10	OTG-INFO-010			×
11	OTG-CONFIG-001	×	×	X
12	OTG-CONFIG-002			
13	OTG-CONFIG-003			
14	OTG-CONFIG-004			×
15	OTG-CONFIG-005	×		
16	OTG-CONFIG-006	×	×	×

Tabel 5.1	Hasil	audit 3	website	UMP
-----------	-------	---------	---------	-----

No	Tahapan Kontrol	Website Portal	Website Simak	Website Journal
17	OTG-CONFIG-007	×	×	×
18	OTG-CONFIG-008			
19	OTG-IDENT-001		×	
20	OTG-IDENT-002			×
21	OTG-IDENT-003			
22	OTG-IDENT-004			
23	OTG-IDENT-005		×	
24	OTG-IDENT-006			
25	OTG-IDENT-007			
26	OTG-AUTHN-001	×	×	×
27	OTG-AUTHN-002	×	×	×
28	OTG-AUTHN-003	×		
29	OTG-AUTHN-004			
30	OTG-AUTHN-005	×	×	×
31	OTG-AUTHN-006		×	×
32	OTG-AUTHN-007		×	×
33	OTG-AUTHN-008			
34	OTG-AUTHN-009			
35	OTG-AUTHN-010			
36	OTG-AUTHZ-001			
37	OTG-AUTHZ-002		×	
38	OTG-AUTHZ-003		×	
39	OTG-AUTHZ-004		×	
40	OTG-SESS-001		×	×
41	OTG-SESS-002			
42	OTG-SESS-003			

No	Tahapan Kontrol	Website	Website	Website
		Portal	Simak	Journal
43	OTG-SESS-004			
44	OTG-SESS-005			
45	OTG-SESS-006			
46	OTG-SESS-007			
47	OTG-SESS-008		×	
48	OTG-INVAL-001			
49	OTG-INVAL-002			
50	OTG-INPVAL-003		×	×
51	OTG-INPVAL-004		×	
52	OTG-INVAL-006			
53	OTG-INVAL-007			
54	OTG-INVAL-008			
55	OTG-INVAL-009			
56	OTG-INVAL-010			
57	OTG-INVAL-011			
58	OTG-INVAL-012			
59	OTG-INVAL-013			
60	OTG-INVAL-014			
61	OTG-INVAL-015			
62	OTG-INVAL-016			
63	OTG-INVAL-017			
64	OTG-ERR-001	×	×	×
65	OTG-ERR-002		×	

# 5.1.1 Temuan Audit

# a. Website Portal

Hasil audit yang telah dilakukan berdasarkan metode OWASP *Testing version* 4 didapatkan hasil pada *website* portal http://um.palembang.ac.id tidak lolos uji pada 15 kontrol uji dari 65 kontrol uji di 8 sub kategori standar dapat dilihat pada tabel 5.1.1

OTC INFO 001 Mangatahui Analisa agaka Googla Hanya di	
GIG-INFO-001 Mengetaliui Aliansa cuche Google Haliya ul	temukan
informasi desain google <i>hacking cache</i> pada g	oogle
dan konfigurasi database	
sensitive	
OTG-INFO-002 Memeriksa Analisa HTTP Netcat Adanya i	nformasi
fingerprint web header versi sistem	operasi
server Ubuntu ver	si 1.4.6
dan PHP 5.5.	9
OTG-INFO-003 Memeriksa adakah Direct Browser Terdapat	file
metafile webserver searching Mozilla robots.txt	yang
Firefox mengidentifil	casi wp-
admin dan di	temukan
meta tag	versi
wordpress 4.9	9.1
OTG-INFO-004 Memeriksa adakah Analisa <i>port</i> dan Zenmap Tidak di	temukan
non-standard port IP WHOIS adanya por	t yang
service DNSStuff terbuka	
OTG-INFO-005 Memeriksa adakah Analisa source WGET Hanya di	temukan
<i>tag</i> komentar & <i>code</i> html CURL informasi ve	rsi CMS
informasi <i>meta</i> - Wordpress 4.	9.1
adia	11
OIG-INFO-006 Melakukan Manual Browser Menermukan	bebrapa
identifikasi <i>entry identification</i> Mozilia entry point	berupa
OTC INFO 007 Metabolicar commission OWASD Measurelear	
OIG-INFO-007 Melakukan scanning Ow ASP- Menemukan	
den memohami	resource domina
uan memanani UKL dan spia	uering
OTG-INFO-008 Memeriksa adakah Analisa HTTP Whatwah Tidak di	temukan
fingerprint web Header dan framework	icinukali
application source code	
framework	
OTG-INFO-009 Memeriksa adakah Analisa HTTP Whatweb Menggunaka	n CMS
fingerprint web Header dan Wordpress ve	ersi 4.9.1
application source code	
OTG-INFO-010 Mendeteksi web Scanning Nmap Menggunaka	n WAF

Tabel 5.1.1 Temuan audit website portal

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	<i>firewall</i> (WAF)			
OTG-CONFIG-001	Memeriksa	Scanning	Zenmap	Ditemukan port
	konfigurasi			remote terbuka yaitu
	application			port 321,322,323
OTG-CONFIG-002	Memeriksa ekstensi	Scanning	Dirb , ZAP,	Tidak ditemukan <i>log</i>
	sensitive		Nikto	
OTG-CONFIG-003	Memeriksa <i>file</i>	Scanning	Dirb , ZAP,	Tidak ditemukan
	sensitive		N1kto	informasi file
OTC CONFIC 004	M	с :	NUL ZAD	sensitive
01G-CONFIG-004	Memeriksa adakan	Scanning	N1Kto, ZAP	lidak ditemukannya
	directory listing			directory <i>cache</i> nanya
OTG CONFIG 005	Mamarikaa adakah	Moninulaci	Drouwor	Ditomukan robots.txt
010-000	input bertine hidden	hidden value	Mozilla	bertine hidden
	input bertipe niaden	niuuen vuiue	Firefox	berupe niaden
OTG-CONFIG-006	Memeriksa Allowed	Scanning	Nikto	Hanya ditemukan
	HTTP method	Securiting	1 (likto	<i>method</i> GET dan
				POST
OTG-CONFIG-007	Memeriksa adakah	Analisa HTTP	Browser	Tidak ditemukan
	HTTP Strict	Header	Mozilla	HTTP Strict
	Transport security		Firefox	Transport Security
	header			Header
OTG-CONFIG-008	Memeriksa adakah	Scanning	Nikto	Tidak didapatkan
	RIA Cross Domain			adanya RIA cross
	Policy			domain policy
OTG-IDENT-001	Memvalidasi hak	Browsing user	Browser	Hak akses telah ter-
	akses website	Policy CMS	Mozilla	mangement dengan
OTC IDENT 002	Mananii analash ada	Wordpress, OJS	Firefox	Daik Tidala tandanat fan asi
01G-IDEN1-002	menguji apakan ada	Manual testing	Browser	rogistrosi rogistrosi
	proses registrasi		Firefox	hanva dapat
	user		THEIOX	dilakukan oleh
				administrator
OTG-IDENT-003	Menguji apakah	Manipulasi http	Browser	Tidak bisa membuat
	penyerang dapat	request	Mozilla	akun tanpa melalui
	membuat akun	1	Firefox	aplikasi
	valid tanpa melalui			-
	aplikasi			
OTG-IDENT-004	Memeriksa semua	Manual input	Browser	Hanya ditemukan
	form login dan		Mozilla	username coadmin
	mencoba guessable		Firefox	dan superadmin pada
	password			setiap postingan pada
OTC IDENT 005	Manauii analaah	Information	Secret	Website Tidalt ditamultan
010-IDEN1-003	terdapat kelemahan	Injormation Gathering	Engine	kelementen nede
	nada pengaturan	Guinering	Lingine	pengaturan nama
	nama pengguna			pengguna
OTG-IDENT-006	Menguii kerentanan	Information	Browser	Tidak ditemukan
	akun <i>training</i> atau	Gathering	Mozilla	
	guess	0	Firefox	
OTG-IDENT-007	Memvalidasi proses	Information	Browser	Tidak ditemukan
	registrasi	Gathering	Mozilla	
			Firefox	

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-AUTHN-001	Memverifikasi	Analisa	Wireshark	Ditemukan bahwa
	data pengguna	header		oleh <i>tools</i> berupa
	ditransfer melalui			clear text
	saluran terenkripsi			dikarenakan masih
				protocol HTTP
OTG-AUTHN-002	Memverifikasi	Bruteforce dan	WPScan,	Ditemukan hanya tiga
	adakah penggunaan	dictionary	Hydra	username yaitu
	(weak password)	иниск		dan bora. Ini
	(			diakibatkan karena
				website portal telah
				Retter security
OTG-AUTHN-003	Memverifikasi	Mencoba	Browser	Hanya terdeteksi
	apakah ada	invalid login	Mozilla	plugin better security,
	mekanisme penguncian akun	beberapa kali	Firefox	sehingga website
	poligunolun ultun			pesan kesalahan <i>login</i>
				ke email admin.
				Namun tidak sampai
OTG-AUTHN-004	Memverifikasi	Direct page	Dirb,	Tidak ditemukan
	direct page request	request,	Sqlmap	celah bypass
	tanpa proses login	Parameter modification		
		session ID		
		prediction,SQL		
OTG-AUTHN-005	Memverifikasi	Injection Analisa form	Browser	Terdanat kerentanan
010 //01110 005	bahwa password	login	Mozilla	akan remember me
	tidak disimpan		Firefox	karena form input
	dalam bentuk <i>text</i>			login tidak di setting
	serta menemukan			unocompicie-ojj
	kerentanan dari			
	fungsi remember			
OTG-AUTHN-006	Memeriksa apakah	Analisa browser	Browser	Tidak ditemukan
	aplikasi	history dan	Mozilla	
	menginstruksikan browser untuk tidak	browser cache	Firefox, Notepad ++	
	ingat data		riotepud ++	
OTG-AUTHN-007	Menguji kerentanan	Melakukan	Browser	Tidak ditemukan
	otentikasi password	beberapa percobaan <i>login</i>	Mozilla Firefox	
OTG-AUTHN-008	Menguji kerentanan	Manual testing	Browser	Tidak ditemukan
	pertanyaan dan	_	Mozilla	
	jawaban pada		Firefox	
OTG-AUTHN-009	Menguji terhadap	Information	Browser	Tidak ditemukan
	fungsi ubah	Gathering	Mozilla	
	password/reset		Firefox	

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	password			
OTG-AUTHN-010	Menguji kerentanan otentikasi melalui jalur alternatif	Information Gathering	Search engine	Tidak ditemukan
OTG-AUTHZ-001	Menguji apakah aplikasi tahan terhadap <i>malicious</i> <i>string</i>	Scanning	OWASP- ZAP,Nikto, Dirb	Tidak ditemukan
OTG-AUTHZ-002	Percobaan akses ke dalam fungsi administrasi tanpa <i>login</i>	Scanning	OWASP- ZAP,Nikto dan Sqlmap	Tidak ditemukan
OTG-AUTHZ-003	Mencoba mendapatkan akses <i>admin</i> dari <i>user</i>	Memanipulasi http request header	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHZ-004	Mencoba mengakses data tanpa <i>login</i>	Scanning	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-001	Memerika apakah token pada <i>cookies</i> dan sesinya dibuat dalam cara yang aman dan <i>unpredictable</i>	Analisa <i>cookies</i>	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-002	Memeriksa apakah cookie menyimpan informasi masa expired di harddisk client	Analisa <i>cookie</i>	Browser Mozilla Firefox, OWASP- ZAP	Tidak ada <i>expired</i> <i>attribute</i> pada <i>cookie</i> <i>website</i> portal
OTG-SESS-003	Memeriksa apakah session yang diberikan pada client selalu diperbarui setelah authentifikasi	Analisa <i>cookie</i>	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-004	Memeriksa pada <i>cookies</i> apakah attribute <i>cookies</i> terlihat jelas	Analisa <i>cookie</i>	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-005	Memeriksa POST dan GET <i>request</i> pada halaman <i>login</i> apakah terimplementasi dengan baik	Scanning	OWASP CSRF Tester	Tidak ditemukan
OTG-SESS-006	Memeriksa adakah kerentanan pada fungsi <i>logout</i>	Analisa <i>cookie</i>	OWASP- ZAP	Tidak ditemukan
OTG-SESS-007	Memeriksa fungsi session timeout	Analisa <i>cookie</i>	OWASP- ZAP	Tidak ditemukan
OTG-SESS-008	Memeriksa session yang teridentifiksasi untuk validasi user	Analisa <i>cookie</i>	Browser Mozilla Firefox	Tidak ditemukan

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-INVAL-001	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	vurnerability		ZAP	
	reflected XSS			
OTG-INVAL-002	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	vurnerability stored		ZAP	
	XSS	a .	NT1 /	
OIG-INPVAL-003	Memeriksa adakah	Scanning	Nikto	I idak ditemukan
	POST dan GET			
	vang bisa di			
	explotasi			
OTG-INPVAL-004	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	HTTP Parameter		ZAP	
	Pollution			
OTG-INVAL-006	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	cela SQL Injection,		ZAP	
	Oracle, SQL Server			
OTG-INVAL-007	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	LDAP Injection	<i>a</i> .	ZAP	
OTG-INVAL-008	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
OTC INVAL 000	ORM Injection	Commino		Tidalı ditamultan
010-INVAL-009	XMI Injection	scanning		I luak ultemukan
OTG-INVAL-010	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	SSI Injection	Seaming	ZAP	Track anomakan
OTG-INVAL-011	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	XPath Injection	0	ZAP	
OTG-INVAL-012	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	IMAP/SMTP	_	ZAP	
	Injection			
OTG-INVAL-013	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	Code Injection, LFI		ZAP	
	dan RFI	<i>c</i> ·	OWAGD	<b>T1 1 1 1</b>
01G-INVAL-014	Command Injection	Scanning		Пак анетикап
OTG INVAL 015	Memeriksa anakah	Scanning		Tidak ditemukan
010-IIIVAL-015	dapat dilakukan	Scanning	ZAP	
	Buffer Heap Stack		2/11	
	overflow dan			
	Format string			
OTG-INVAL-016	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	incubated		ZAP	
	vulnerability			
OTG-INVAL-017	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	HTTP G I'w /G		ZAP	
OTC EDD 001	Splitting/Smugging	Commins	OWASD	Ditomulton
010-EKK-001	wenganansis kode	scanning	74P	kesalahan 404 arror
	Kosalallall			no input file specified
				dan menampilkan
				versi server & PHP
OTG-ERR-002	Menganalisis Stack	Scanning	OWASP	Tidak ditemukan
	Traces	Ĩ	ZAP	

# b. Website Simak

Hasil audit yang telah dilakukan berdasarkan metode OWASP *Testing version* 4 didapatkan hasil pada *website* simak http://mahasiswa.um.palembang.ac.id tidak lolos uji pada 23 kontrol uji dari 65 kontrol uji di 8 sub kategori standar dapat dilihat pada tabel 5.1.2.

Tabel 5.1.	.2 Hasil	audit	website	simak
------------	----------	-------	---------	-------

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-INFO-001	Mengetahui informasi	Analisa	Google	Hanya ditemukan
	desain dan konfigurasi	cache	hacking	cache pada google
	sensitive	google	database	
OTG-INFO-002	Memeriksa <i>fingerprint web</i>	Analisa	Netcat	Adanya informasi
	server	HIIP		versi sistem operasi
		neuaer		Microsoft US vorsi
				8 Odan ASP Net versi
				4 0 30319 dan
				menggunakan
				framework ASP.Net
				MVC 5.2
OTG-INFO-003	Memeriksa adakah	Direct	Browser	Tidak ditemukan file
	metafile webserver	searching	Mozilla	robots.txt
			Firefox	
OTG-INFO-004	Memeriksa adakah non-	Analisa	Zenmap	Tidak ditemukan
	standard port service	<i>port</i> dan IP	WHOIS	adanya port yang
OTC NEO 005	Manage 1 and 1 at 1	A	DNSStuff	terbuka
01G-INFO-005	Memeriksa adakan <i>tag</i>	Analisa	WGEI	lidak ditemukan tag
	mata data	source	CURL	informasi mata data
OTG-INFO-006	Melakukan identifikasi	Manual	Browser	Menermukan bebrana
010 110 000	entry point	identificati	Mozilla	entry point berupa
		on	Firefox	parameter
OTG-INFO-007	Melakukan pemetaan	scanning	OWASP-	Menemukan beberapa
	website dan memahami	Ũ	ZAP	resource URL dari
	prinsip kerja			spidering
OTG-INFO-008	Memeriksa adakah	Analisa	Whatweb	Ditemukan framework
	fingerprint web application	HTTP		ASP.Net 4.0.30319
	framework	Header		MVC 5.2
		dan <i>source</i>		
OTC INFO 000	Mamarikaa	code	W/la a tana a la	Tidala managementary
010-111-009	fingerprint web application	Analisa	whatweb	ridak menggunakan
	Jingerprini web application	Header		CIVIS
		dan <i>source</i>		
		code		
OTG-INFO-010	Mendeteksi web	Scanning	Nmap	Menggunakan WAF
	application firewall(WAF)	Ũ		BigIP

OTG-CONFIG-001         Memeriksa application         konfigurasi application         Scanning         Zenmap         Ditemukan remote terbuka yaitu port 321,322,323           OTG-CONFIG-002         Memeriksa sensitive         Scanning         Dirb         ZAP, Nikto         Tidak ditemukan informasi         Tidak ditemukan informasi           OTG-CONFIG-003         Memeriksa file sensitive         Scanning         Dirb         ZAP, Nikto         Tidak ditemukan informasi         Tidak ditemukan informasi           OTG-CONFIG-004         Memeriksa directory listing         Mamipulasi         Scanning         Nikto         Tidak ditemukan input beripe hidden           OTG-CONFIG-005         Memeriksa adakah input beripe hidden         Manipulasi         Browser         Tidak ditemukan input beripe hidden           OTG-CONFIG-006         Memeriksa adakah Hirpu header         Analisa         Browser         Tidak ditemukan port           OTG-CONFIG-007         Memeriksa dakah RITP header         Analisa         Browser         Tidak ditemukan didaya RIA cross domain policy           OTG-CONFIG-008         Memeriksa dakah RIA Cross Domain Policy         Scanning         Nikto         Tidak ditemukan didaya RIA cross domain policy           OTG-IDENT-001         Memavalidasi hak akses vebsite         Browser         Tidak terdapat fungsi registrasi user           OTG-IDENT-003         Menguji a	Tahapan Kontrol	Objective	Technique	Tool	Hasil
applicationremote terbuka yaitu port 321.322.323OTG-CONFIG-002 sensitiveMemeriksa ekstensi sensitiveScanningDirb , ZAP, NiktoTidak ditemukan log NiktoOTG-CONFIG-003Memeriksa file sensitiveScanningDirb , ZAP, NiktoTidak ditemukan informasis ensitiveOTG-CONFIG-004Memeriksa adakah directory listingScanningNiktoTidak ditemukan input beripe hidden valueOTG-CONFIG-005Memeriksa adakah input beripe hiddenManipulasi hiddenBrowserTidak ditemukan input beripe hiddenOTG-CONFIG-006Memeriksa adakah HTTP headerAnalisa HTTP methodScanningNiktoDitemukan method OPTION, TRACE, GET.HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah RIA Strict Transport security headerScanningNiktoTidak ditemukan idak ditemukan intak didapatkan adapatka dapatkan adanya RIA cross domain policyOTG-IDENT-001Meneriksa inak akses websiteBrowsingBrowser word meriksi adakah RIA ScanningOTG-IDENT-002Menguji apakah ada proses registrasi userManual terifoxBrowserTidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administrator oleh administratorOTG-IDENT-003Menguji apakah terdapat dapat memboat akun vulta dapat memboat akun vulta dapat memboat akun vulta httpBrowser Hak atsesTidak terdapat fungsi registrasi hanya dapat dilakukan oleh administrator oleh administrator oleh administratorOTG-IDENT-004Menguji apakah terdapat napasword admin gestav	OTG-CONFIG-001	Memeriksa konfigurasi	Scanning	Zenmap	Ditemukan port
OTG-CONFIG-002Memeriksa sensitiveScanning sensitiveDirb scanningZAP, NiktoTidak ditemukan log niktoOTG-CONFIG-003Memeriksa file sensitiveScanning directory listingDirbZAP, NiktoTidak ditemukannya directory cache.OTG-CONFIG-004Memeriksa directory listingScanning directory listingNiktoTidak ditemukannya directory cache.OTG-CONFIG-005Memeriksa directory listingManipulasi valueBrowserTidak ditemukannya directory cache.OTG-CONFIG-006Memeriksa HTTP methodScanning valueNiktoDitemukan method OPTIDA, TRACE, GET.HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah HTTP headerAnalisa ScanningBrowserTidak ditemukan method OPTIDA, TRACE, GET.HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah RIA Cross Domain PolicyScanning NiktoNiktoTidak ditemukan directory cache.OTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning NiktoNiktoTidak ditemukan didapatkan condity headerOTG-IDENT-001Memeriksa semau form egistrasi userBrowser registrasi userTidak terdapat fungsi registrasi, registrasi hanya dapat fungsi registrasi userOTG-IDENT-004Meneriksa semua form dapat membuat akun valida dapat membuat akun valida inputManual firefoxBrowser tidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan pengaturan nama pengguna ging dan mencoba guessable passwordManual an pasbew of servit ada napassword abl		application			remote terbuka yaitu
OTG-CONFIG-003       Memeriksa       ekstensi       Scanning       Dirb , ZAP,       Irdak ditemukan log         OTG-CONFIG-003       Memeriksa       adakah       Scanning       Dirb , ZAP,       Tidak ditemukan linformasi       file         OTG-CONFIG-004       Memeriksa       adakah       Scanning       Nikto       Tidak ditemukan jife         OTG-CONFIG-005       Memeriksa       adakah       Scanning       Nikto       Tidak ditemukan jife         OTG-CONFIG-006       Memeriksa       Allowed       Scanning       Nikto       Ditemukan method         OTG-CONFIG-006       Memeriksa       Allowed       Scanning       Nikto       Ditemukan method         OTG-CONFIG-007       Memeriksa       Allowed       Scanning       Nikto       Ditemukan method         OTG-CONFIG-007       Memeriksa       adakah       RIA       Scanning       Nikto       Ditemukan method         OTG-CONFIG-008       Memeriksa       adakah       RIA       Scanning       Nikto       Tidak ditemukan jipt         OTG-IDENT-001       Memeriksa       adakah RIA       Scanning       Nikto       Tidak kases       mainya terdiri         OTG-IDENT-001       Menguji apakah ada proses       Marual       Browser       Tidak kases       mainhanya terdi			<i>a</i> .		port 321,322,323
OTG-CONFIG-003         Memeriksa file sensitive         Scanning         Nikto         Tidak ditemukan informasi file sensitive           OTG-CONFIG-004         Memeriksa adakah directory listing         Scanning         Nikto         Tidak ditemukan input directory cache.           OTG-CONFIG-005         Memeriksa adakah input bertipe hidden         Manipulasi hidden         Browser hidden         Tidak ditemukan input bertipe hidden           OTG-CONFIG-006         Memeriksa adakah HTTP         Analisa         Browser         Tidak ditemukan input bertipe hidden           OTG-CONFIG-007         Memeriksa adakah HTTP         Analisa         Browser         Tidak ditemukan method OPTION, TRACE, GET.HEAD,dan POST           OTG-CONFIG-006         Memeriksa adakah RIA         Scanning         Nikto         Tidak ditemukan danya RIA cross domain Policy           OTG-CONFIG-008         Memeriksa adakah RIA         Scanning         Nikto         Tidak didapatkan adanya RIA cross domain policy           OTG-IDENT-001         Memeriksa adakah ada proses registrasi user         Firefox         Tidak terdapat fungsi registrasi user           OTG-IDENT-002         Menguji apakah ada proses registrasi user         Maniul tanya dapat dilakukan oleh administrator           OTG-IDENT-003         Menguji apakah penyerang dapat dilakukan oleh administrator         Tidak terdapat fungsi napasword seperi admin           OTG-IDENT-004	OTG-CONFIG-002	Memeriksa ekstensi	Scanning	Dirb , ZAP,	Tidak ditemukan log
OTG-CONFIG-003       Memeriksa jile sensitive       Scanning       Diff v. ZAF, informasis informasis informasis informasis informasis ensitive         OTG-CONFIG-004       Memeriksa adakah input bertipe hidden       Scanning       Nikto       Tidak ditemukaniya directory cache.         OTG-CONFIG-005       Memeriksa adakah input bertipe hidden       Manipulasi       Browser       Tidak ditemukan input bertipe hidden         OTG-CONFIG-006       Memeriksa adakah HITP       Analisa       Browser       Tidak ditemukan method         OTG-CONFIG-007       Memeriksa adakah RIA       Scanning       Nikto       Ditemukan method         OTG-CONFIG-008       Memeriksa adakah RIA       Scanning       Nikto       Tidak ditemukan adanya RIA cross         OTG-IDENT-001       Memvalidasi hak akses westie       Browsing       Browser       Hak akses masih         OTG-IDENT-002       Menguji apakah ada proses       Manual       Browser       Hak akses masih         OTG-IDENT-004       Menerikas aseus form dapat dilakukan oleh administrator       Browser       Tidak bias membuat akun valid http         OTG-IDENT-004       Menguji apakah terdapat ngas apat dilakukan oleh administrator       Browser       Tidak bias membuat akun valid http         OTG-IDENT-004       Menguji apakah terdapat ngas apat dilakukan oleh administrator       Browser n       Tidak ditemukan dikarenakan username dan	OTC CONFIC 002	sensitive	Saannina	Nikto	Tidalı ditamultan
OTG-CONFIG-004Memcriksa directory lisingScanning directory lisingNikto, ZAPTidak ditemukanya directory corp.OTG-CONFIG-005Memeriksa beripe hiddenManipulasi hiddenBrowser walaeTidak ditemukan input beripe hiddenOTG-CONFIG-006Memeriksa HTTP methodManipulasi hiddenBrowserTidak ditemukan methodOTG-CONFIG-007Memeriksa AladerAllowed HTTP methodScanningNiktoDitemukan methodOTG-CONFIG-008Memeriksa adakahAlakak RIA Cross Domain PolicyAnalisa BrowserBrowserTidak didapatkan adanya RIA cross domain policyOTG-IDENT-001Memeriksa adakah proses registrasi userBrowsing user Policy Wordpress, OTG-IDENT-002Menguji apakah ada proses registrasi userManual testing hada proses testingBrowser firefoxTidak ditapatkan adanya RIA cross domain policyOTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Manual testingTidak terdapat fungsi registrasi, registrasi hup a dapat dilakukan registrasi tapa melalui aplikasiBrowser tidak terdapat fungsi registrasiOTG-IDENT-004Menguji apakah terdapat registrasi tapa melalui aplikasiInformatio n menikak bernasid normBrowser mozilla firefoxTidak ditemukan adhasiswa dan oleh administrator oleh administratorOTG-IDENT-005Menguji apakah terdapat registrasi registrasiInformatio n n data bisa membuat dian mencoba nManual menguna adapa <t< td=""><td>010-000</td><td>Memeriksa jue sensuive</td><td>Scanning</td><td>Diro , ZAP, Nikto</td><td>informasi file</td></t<>	010-000	Memeriksa jue sensuive	Scanning	Diro , ZAP, Nikto	informasi file
OTG-CONFIG-004 directory listing directory listing OTG-CONFIG-005         Memeriksa directory listing directory listing bertipe hidden         Scanning hidden value         Nikto, ZAP Browser Mozilla         Tidak ditemukan input bertipe hidden           OTG-CONFIG-006         Memeriksa adakah input bertipe hidden         Manipulasi hidden         Browser Mozilla         Tidak ditemukan input bertipe hidden           OTG-CONFIG-006         Memeriksa adakah HTTP strict Transport security header         Scanning         Nikto         Ditemukan method OPTION, TRACE, GET,HEAD,dan           OTG-CONFIG-007         Memeriksa adakah RIA cross Domain Policy         Scanning         Nikto         Tidak ditemukan HTTP Strict Transport security Header           OTG-CONFIG-008         Memeriksa adakah RIA cross Domain Policy         Scanning website         Nikto         Tidak didapatkan diapatkan da kross domain policy           OTG-IDENT-001         Memuyai apakah ada proses registrasi user         Browser website         Browser Manual testing         Browser Mozilla Firefox         Tidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administrator           OTG-IDENT-003         Menguji apakah penyerang dapat membuat akun volid tapat membuat akun volid tapat menbuat akun volid dapat menbuat dapat menbuat dapat menbuat dapat menbuat dapat menbuat dapat menbuat dapat menbuat hutp apasword adalah nomor         Browser Mozilla Firefox         Tidak bisa membuat akun tapa melalui aplikasi           OTG-IDENT-005         Menguji apakah terdapat kelem				TTIKto	sensitive
directory listingdirectory cache.OTG-CONFIG-005Memeriksa adakah input bertipe hiddenManipulasi hidden valueBrowser hidden FirefoxTidak ditemukan input bertipe hiddenOTG-CONFIG-006Memeriksa HTTP methodScanningNiktoDitemukan method OPTION, TRACE, GET_HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah HTTP strict Transport security headerAnalisa HTTP HeaderBrowser HeaderTidak ditemukan HTTP Strict Transport Security HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning NiktoNiktoTidak ditemukan adany RIA cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy CMSBrowser Mozilla FirefoxHak akses masih memiliki kekurangan. FirefoxOTG-IDENT-002Menguji apakah penyerang dapat membuat akun valid tanp a melalui aplikasiManual registrasi userBrowser tirefoxTidak ditakukan adany dapat dilakukan oleh administratorOTG-IDENT-004Menguji apakah penyerang dapat membuat akun valid hogin dan mencoba guessable passwordManual inputBrowser firefoxTidak berhasil mengunakan guessable username dan password seperti administratorOTG-IDENT-005Menguji apakah terdapat registrasiInformatio n firefoxScarch firefoxDitemukan kelemahan noror induk mabaiswa (NIM)OTG-IDENT-006Menguji apakah terdapat kelemahan registrasiInformatio n firefoxBrowser n firefoxTidak ditemukan mengunakan guessabl	OTG-CONFIG-004	Memeriksa adakah	Scanning	Nikto, ZAP	Tidak ditemukannya
OTG-CONFIG-005Memeriksa adakah input bertipe hiddenManipulasi hidden valueBrowser Mozilla FirefoxTidak ditemukan input bertipe hiddenOTG-CONFIG-006Memeriksa HTTP methodAllowed HTTP methodScanningNiktoDitemukan method OPTION, TRACE, GET,HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah HTTP headerAnalisa HTTP headerBrowser HEU HeaderTidak ditemukan diapatian diapatian diapatian diapatian diapatian diapatian get seriesTidak ditemukan method OPTION, TRACE, GET,HEAD,dan POSTOTG-CONFIG-008Memeriksa adakah RIA Cross Domain Policy websiteScanning user Policy CMSTidak ditemukan diapatian diapatian diapatian diapatian dari Mahasiswa dan oDISTidak sees masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan OTG-IDENT-002Menguji apakah ada proses registrasi userBrowser Mozilla FirefoxHak akses masih memiliki kekurangan. Tidak terdapat fungsi registrasi userOTG-IDENT-004Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser Mozilla FirefoxTidak berhasil memiliki kelemahan guessable passwordOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n n GatheringSearch Browser Mozilla FirefoxDitemukan kelemahan dan password adalah nom induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun registrasiInformatio n A GatheringBrowser Mozilla FirefoxTidak ditemukan <td></td> <td>directory listing</td> <td>0</td> <td>,</td> <td>directory cache.</td>		directory listing	0	,	directory cache.
bertipe hiddenhidden valueMozilla Firefoxbertipe hiddenOTG-CONFIG-006Memeriksa HTTP methodScanningNiktoDitemukan 	OTG-CONFIG-005	Memeriksa adakah input	Manipulasi	Browser	Tidak ditemukan input
OTG-CONFIG-006Memeriksa HTTP methodAllowed ScanningNiktoDitemukan method OPTION, TRACE, GET,HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah HTTP Strict Transport security headerAnalisa HeaderBrowser HeaderTidak ditemukan diapatkan adamy RIA cross Domain PolicyOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning WebsiteTidak ditapatkan adamy RIA cross Wordpress, OISOTG-IDENT-001Memvalidasi hak akses websiteBrowser WerkerBrowser Wordpress, OISOTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser testingOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tapa melalui aplikasiManual registrasi userBrowser testingOTG-IDENT-004Menguji apakah terdapat kelemahan penguta agu melalui aplikasiInformatio n n mengunakan testingBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui apasword agu messord sessordOTG-IDENT-004Menguji apakah terdapat kelemahan padapInformatio n n mengunakan guessable password nSearch more miduk mahasiswa (MIM)OTG-IDENT-007Menguji kerentanan akun registrasiInformatio n n Menguji kerentanan akun n more induk mahasiswa (NIM)Ditemukan kelemahan dikarenakan username dan password adalah nomor n miduk mahasiswa (NIM)OTG-IDENT-007Menguji kerentanan akun registrasiInformatio n Menyu ikasi bahwa otentikasi data penguna dit		bertipe hidden	hidden	Mozilla	bertipe hidden
OTG-CONFIG-006Memeriksa HTTPAllowed MemeriksaScanning ScanningNiktoDiremukan OPTION, TRACE, GET,HEAD,dan HTTPOTG-CONFIG-007Memeriksa strict headerMemeriksa trict transport security headerAnalisa HTTPBrowser HeaderTidak HTTP Strict Transport Security HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyNiktoTidak didapatkan adanya RIA cross OTG-IDENT-001Memvalidasi hak aksesBrowsing user Policy CMS Wordpress, OJTG-IDENT-002Browser testingHak akses memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orang tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat tingsi registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManual inputBrowser Mozilla FirefoxTidak berhasil mengunakan guessable passwordOTG-IDENT-004Menguji apakah terdapat kelemahan pengaturan nama pengguna and mengguna and pengaturan nama penggunaInformatio n GatheringScarch Browser Mozilla FirefoxTidak ditemukan dita mengunakan genesable username data password seperti adminOTG-IDENT-006Menguji apakah terdapat registrasiInformatio n Mozilla GatheringBrowser Mozilla FirefoxTidak ditemukan ditarenakan username ditarenakan username data password adalah momor iduk mahasiswa (NIM) <td></td> <td></td> <td>value</td> <td>Firefox</td> <td></td>			value	Firefox	
HTTP methodOPTION, TRACE, GET,HEAD,dan POSTOTG-CONFIG-007Memeriksa adakah HTTP headerAnalisa HTTP headerBrowser HTTP MozillaTidak HTTP Strict Transport security HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning user PolicyNiktoTidak didapatkan adaya RIA cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy OTG-IDENT-002Browsing websiteBrowsing user Policy OTG-IDENT-002Browsing userBrowser user Policy MozillaHak akses memiliki kekurangan. Orang tu asaja.OTG-IDENT-002Menguji apakah ada proses registrasi userManipulasi registrasi userBrowser testingTidak terdapat fungsi registrasi, registrasi naya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid poin dan mencoba guessable passwordManipulasi hunual registrasiBrowser referoxTidak bisa membuat akun tanpa melalui apilikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n n GatheringSearch Mozilla FirefoxTidak ditemukan menggunakan guessable username dan password adalah n n menggunakanOTG-IDENT-006Menguji kerentanan akun rauiring atu guess registrasiInformatio n n MozillaBrowser mengunakan EngineOTG-IDENT-007Menguji kerentanan akun registrasiInformatio n n n nBrowser n Mozilla GatheringTidak ditemukan ditak ditemu	OTG-CONFIG-006	Memeriksa Allowed	Scanning	Nikto	Ditemukan method
OTG-CONFIG-007Memeriksa adakah HTTP Strict Transport security headerAnalisa HeaderBrowser HeaderTidak MozillaTidak ditemukan HTTP Strict Transport Security HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning HeaderNiktoTidak adanya RIA Cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy Wordpress, OJSBrowser MozillaHak akses masih memiliki ketvaragan. Orang tu asja.OTG-IDENT-002Menguji apakah ada proses dapat membuat akun valid tanpa melalui aplikasi aupa melalui aplikasiManual registrasi userBrowser testingTidak terdapat fungsi registrasi, registrasi, registrasiOTG-IDENT-004Menguji apakah penyerang login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat hegin dan mapa negguna registrasiInformatio n n MozillaScarch BriefoxDitemukan kelemahan diatkana nomor induk massword seperti admini dan hassiswa (NIM)OTG-IDENT-005Menguji kerentana akun registrasiInformatio n n MozillaScarch BriefoxDitemukan kelemahan diatemakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentana akun registrasiInformatio n n MozillaScarch Browser n MozillaTidak ditemukan ditaktana nomor malket yang tercapture dot horebacOTG-IDENT-007Memverifikasi bahwa<		HIIP method			OPTION, IRACE,
OTG-CONFIG-007Memeriksa adakah HTTP Strict Transport security headerAnalisa HTTP HeaderBrowser Mozilla FirefoxTidak Mozilta adaya RIA adaya RIA cross domain policyOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning NiktoTidak Mozilla Browser Mozilla FirefoxTidak ditemukan HTTP Strict Transport Security HeaderOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy Wordpress, OTG-IDENT-002Browser Menguji apakah ada proses registrasi userBrowser Mozilla FirefoxHak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orang tua saja.OTG-IDENT-002Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi registrasi, registrasi, registrasiBrowser Tidak terdapat fungsi registrasi, registrasi userOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManipulasi inputBrowser mozilla FirefoxTidak berhasil menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n n n GatheringSearch Browser MozillaDitemukan kelemahan massword adalah n dari password seperti adminOTG-IDENT-007Menguji kerentanan akun raining atua guessInformatio n n n datheringBrowser FirefoxTidak ditemukan dikarenakan username dan password adalah n datheringOTG-IDENT-007Menyuji kerentanan akun rigistrasiInformatio n n<					POST
Strict Transport security headerHTTP HeaderMozilla FirefoxHTTP Strict Transport Security HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning user PolicyNiktoTidak didapatkan adanya RIA cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy CMSBrowser Wordpress, OJSHak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orag tua saja.Browser memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orag tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi registrasi, registrasi naya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi n registrasiBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form pengaturan nama pengguna pengaturan nama penggunaInformatio n n MozillaSearch EngineDitemukan kelemahan dikarenakan username dan password seperti adminOTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n MozillaBrowser FirefoxTidak ditemukan dikarenakan username da password seperti adminOTG-IDENT-007Memvalidasi proses registrasiInformatio n n MozillaBrowser firefoxTidak ditemukan dikarenakan username data preser n nOTG-IDENT-007Memvalidasi proses <td>OTG-CONFIG-007</td> <td>Memeriksa adakah HTTP</td> <td>Analisa</td> <td>Browser</td> <td>Tidak ditemukan</td>	OTG-CONFIG-007	Memeriksa adakah HTTP	Analisa	Browser	Tidak ditemukan
headerHeaderFirefoxSecurity HeaderOTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanningNiktoTidakdidapatkan adanya RIAOTG-IDENT-001Memvalidasi hak akses websiteBrowser 		Strict Transport security	HTTP	Mozilla	HTTP Strict Transport
OTG-CONFIG-008Memeriksa adakah RIA Cross Domain PolicyScanning andanya RIATidak adanya RIA cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy CMS Wordpress, OISBrowser Mozilla FirefoxHak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orag tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi registrasi, registrasi, registrasi nanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManual tequestBrowser FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama pengguna registrasiInformatio n n fortheringSearch firefoxDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun registrasiInformatio n n massword adalah nomor induk mahasiswa (NIM)Browser n firefoxTidak ditemukan maketOTG-IDENT-007Memguji kerentanan akun registrasiInformatio n n massial firefoxBrowser m Mozilla firefoxTidak ditemukan maketOTG-IDENT-007Memguji kerentanan akun registrasi <td< td=""><td></td><td>header</td><td>Header</td><td>Firefox</td><td>Security Header</td></td<>		header	Header	Firefox	Security Header
Cross Domain Policyadanya RIA cross domain policyOTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy CMS Wordpress,Browser Mozilla FirefoxHak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orang tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memerikas semua form login dan mencoba guessable passwordManual inputBrowser Hozilla FirefoxTidak berhasil menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama pengguna Renguji kerentanan akun registrasiInformatio n m Mozilla FirefoxDitemukan kelemahan dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun registrasiInformatio n m Mozilla GatheringBrowser FirefoxTidak ditemukan massword adalah nomorOTG-IDENT-007Memyulidasi registrasiproses n n Memyulidasi pengaturan nama pengguna ada adat adateringInformatio Mozilla FirefoxBrowser Tidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memyulidasi registrasiproses n n Mozilla FirefoxTidak ditem	OTG-CONFIG-008	Memeriksa adakah RIA	Scanning	Nikto	Tidak didapatkan
OTG-IDENT-001Memvalidasi hak akses websiteBrowsing user Policy CMS Wordpress, OJSBrowsner Mozilla FirefoxHak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orag tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManual testingBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak berhasil mengunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama pengguna registrasiInformatio n n GatheringSearch Mozilla FirefoxDitemukan kelemahan nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun raining atau guessInformatio n n mor matistic n n n n morBrowser mowser Mozilla FirefoxTidak ditemukanOTG-IDENT-007Memverifikasi bahwa otentikasi data pengguna ditransfer melalui aplanzan n melalui aplanzan a dat pengguna otentikasi data pengguna otentikasi data pengguna otentikasi data pengguna otentikasi data pengguna otentikasi data pengguna otentikasi data pengguna oleh tools beruma clearSoarch matetOTG-AUTHN-001Memverifikasi data pengguna <b< td=""><td></td><td>Cross Domain Policy</td><td></td><td></td><td>adanya RIA cross</td></b<>		Cross Domain Policy			adanya RIA cross
OTG-IDENT-001Memvaildasi memvaildasi hak websiteBrowsing user Policy Wozilla OJSBrowser Mozilla FirefoxHak memiliki kekurangan. Mozilla dari Mahasiswa dan Orang tua saja.OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tapat menduu akun valid tapat menduu akun valid pengetsManipulasi registrasiBrowser Mozilla FirefoxTidak terdapat dilakukan oleh administratorOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual requestBrowser FirefoxTidak berhasil menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n n Mozilla FirefoxSearch Mozilla FirefoxDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n mor midukBrowser Mozilla FirefoxOTG-IDENT-007Memvalidasi registrasiInformatio n n noorBrowser mozilla GatheringTidak ditemukan morOTG-IDENT-007Memvalidasi registrasiInformatio n n n noorBrowser Mozilla FirefoxTidak ditemukan mengunakan guessableOTG-IDENT-007Memvalidasi registrasiproses n n n n n <td< td=""><td></td><td></td><td><b>D</b> ·</td><td>D</td><td>domain policy</td></td<>			<b>D</b> ·	D	domain policy
Websitediserlaser PolicyMoziliaInterminit kekunalgan. Karena hanya terdiri dari Mahasiswa dan OISOTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser MozillaTidak terdapat fungsi registrasi, registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi requestBrowser FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser MozillaTidak berhasil menggunakan guessable username daminOTG-IDENT-005Menguji apakah terdapat kelemahan pada pengaturan nama penggunaInformatio n n GatheringSearch NozillaDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n nBrowser moserTidak ditemukan mengunakan guessableOTG-IDENT-007Memvalidasi prosesproses Informatio n nBrowser moserTidak ditemukan moror induk mahasiswa (NIM)OTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna otentikasi data pengg	OTG-IDENT-001	Memvalidasi hak akses	Browsing	Browser	Hak akses masih
OTG-IDENT-002Menguji apakah ada proses registrasi userManual Wordpress, OJSBrowser Manual testingTidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi requestBrowser FirefoxTidak terdapat fungsi registrasi, registrasi, registrasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser MozillaTidak berhasil menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pada pengaturan nama pengguna GatheringInformatio n GatheringSearch FirefoxDitemukan kelemahan n an password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentana akun registrasiInformatio n n Menguji kerentana akun registrasiInformatio n MozillaBrowser FirefoxOTG-IDENT-007Menguji kerentana akun registrasiInformatio n n MozillaBrowser MozillaTidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memverifikasi proses registrasiInformatio n n MozillaBrowser MozillaTidak ditemukan mahasiswa (NIM)OTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna otentikasi data pengguna otentikasi data pengguna paketAnalisa maketWireshark paket yang tercapture oleh tools berma clear		website	user Policy	Firefox	Karana hanya terdiri
OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Herif MozillaTidak terdapat fungsi registrasi, registrasi naya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser HittpTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak bisa akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n n GatheringSearch Mozilla FirefoxDitemukan kelemahan diarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atu guessInformatio n n MozillaBrowser FirefoxTidak ditemukan mengunakan guessable username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-007Menguji kerentanan akun training atu guessInformatio n n MozillaBrowser FirefoxTidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memvalidasi proses registrasiInformatio n MozillaBrowser MozillaTidak ditemukan mahasiswa (NIM)OTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa captured n aket capturedDitemukan bahwa paket yang tercapture oleh tools beruma clear			Wordpress.	THEIOX	dari Mahasiswa dan
OTG-IDENT-002Menguji apakah ada proses registrasi userManual testingBrowser Mozilla FirefoxTidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n GatheringSearch mozilla FirefoxDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n datheringBrowser Mozilla FirefoxTidak ditemukan mengunakan guessable username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-007Memguji kerentanan akun training atau guessInformatio n n MozillaBrowser FirefoxTidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memverifikasi bahwa otentikasi data pengguna dittansfer melalui saluran dittansfer melalui saluranInformatio n n Analisa capturedBrowser Mozilla FirefoxTidak ditemukan bahwa paket yang tercapture oleh tols berupa clear			OJS		Orang tua saja.
registrasi usertestingMozilla Firefoxregistrasi, negistrasi hanya dapat dilakukan oleh administratorOTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Mozilla FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n GatheringSearch firefoxDitemukan kelemahan dikarenakan username dan password adalah nomor n MozillaOTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n Menverifikasi bahwa otentikasi data penggunaBrowser n n MozillaTidak ditemukan mengunakan grierfoxOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluran ditransfer melalui saluranInformatio n n Analisa capturedDitemukan bahwa paket yang tercapture oleh tools beruma clear	OTG-IDENT-002	Menguji apakah ada proses	Manual	Browser	Tidak terdapat fungsi
OTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi nequestBrowser FirefoxTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser MozillaTidak berhasil mengunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio Rather at a mengunaSearch mengene dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n mBrowser mTidak ditemukan massword adalah nomor miduk mahasiswa (NIM)OTG-IDENT-007Menguji kerentanan akun training atau guessInformatio n n mBrowser mTidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memvalidasi registrasiInformatio n n mBrowser mTidak ditemukan mahasiswa (NIM)OTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditansfer melalui saluran ditansfer melalui saluran ditansfer melalui saluran ditansfer melalui saluran paket yang tercapture oleh tools berma clear		registrasi user	testing	Mozilla	registrasi, registrasi
OTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser MozillaTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser MozillaTidak berhasil menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio n nSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n n MozillaBrowser ErefoxTidak ditemukan menggunakan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-007Menguji kerentanan akun training atau guessInformatio n n MozillaBrowser MozillaTidak ditemukan mahasiswa (NIM)OTG-IDENT-007Memverifikasi bahwa otentikasi data pengguna otentikasi data pengguna dittansfer melalui saluran dittansfer melalui saluran dittansfer melalui saluranInformatio n Analisa captured paket paketDitemukan bahwa paket paket oleh tools berma clear				Firefox	hanya dapat dilakukan
OTG-IDENT-003Menguji apakah penyerang dapat membuat akun valid tanpa melalui aplikasiManipulasi httpBrowser MozillaTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser menggunakan guessable username dan password seperti adminTidak bisa membuat akun tanpa melalui aplikasiOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio RatheringSearch menguneDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n nBrowser mor induk mahasiswa (NIM)OTG-IDENT-007Memvalidasi prosesInformatio n n Memvalidasi registrasiBrowser n n AnalisaTidak bisa membuat akun tanpa melalui aplikasiOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranInformatio n n naketBrowser maketTidak ditemukan bahwa oleh tools berupa clear				D	oleh administrator
OTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser Manual inputTidak menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pada pengaturan nama penggunaInformatio RatheringSearch BrowserDitemukan kelemahan dikarenakan username dan password adalah nOTG-IDENT-006Menguji kerentanan akun training atau guessInformatio RatheringSearch BrowserDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n NoziliaBrowser MoziliaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiInformatio n NoziliaBrowser MoziliaTidak ditemukan mahasiswa (NIM)OTG-AUTHN-001Memverifikasi bahwa ditansfer melalui saluran ditansfer melalui aguranInformatio n n naketDitemukan bahwa paket yang tercapture oleh tools berupa clear	OTG-IDENT-003	Menguji apakah penyerang	Manipulasi	Browser	Tidak bisa membuat
OTG-IDENT-004Memeriksa semua form login dan mencoba guessable passwordManual inputBrowser MozillaTidak menggunakan guessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pada pengaturan nama penggunaInformatio RatheringSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio n nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses registrasiInformatio n NBrowser MozillaTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa captured naketDitemukan bahwa paket yang tercapture oleh tools berupa clear		tanna melalui anlikasi	nup	Firefox	akun tanpa merarun anlikasi
OTG-IDENT-005Instantial dam mencoba guessable passwordinputMozilla inputmenggunakan guessable username 	OTG-IDENT-004	Memeriksa semua form	Manual	Browser	Tidak berhasil
guessable passwordIFirefoxguessable username dan password seperti adminOTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio nSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser Mozilla FirefoxTidak ditemukanOTG-IDENT-007Menguji kerentanan akun training atau guessInformatio nBrowser Mozilla FirefoxTidak ditemukanOTG-IDENT-007Memvalidasi registrasiInformatio nBrowser MozillaTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa capturedWireshark paketDitemukan bahwa paket oleh tools berupa clear		login dan mencoba	input	Mozilla	menggunakan
OTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio nSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio nBrowser MozillaTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa captured paketWireshark paketDitemukan bahwa paket paket		guessable password	1	Firefox	guessable username
OTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio nSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses n NInformatio MozillaBrowser FirefoxTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa captured paketWireshark paketDitemukan bahwa paket					dan password seperti
OTG-IDENT-005Menguji apakah terdapat kelemahan pengaturan nama penggunaInformatio nSearch EngineDitemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio nBrowser MozillaTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan bahwa paket					admin
kelemanan pengaturan nama penggunanEnginedikarenakan username dan password adalah nomor induk mahasiswa (NIM)OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio MozillaBrowser FirefoxTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan bahwa paket	OTG-IDENT-005	Menguji apakah terdapat	Informatio	Search	Ditemukan kelemahan
Defigituran nama penggunaGatheringdan password adatan nomorOTG-IDENT-006Menguji kerentanan akun training atau guessInformatioBrowser nTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio MozillaBrowser FirefoxTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio MozillaBrowser FirefoxTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan bahwa paket		kelemahan pada	n Cath anim a	Engine	dikarenakan username
OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi 		pengaturan nama pengguna	Gainering		nomor induk
OTG-IDENT-006Menguji kerentanan akun training atau guessInformatio nBrowser MozillaTidak ditemukanOTG-IDENT-007Memvalidasi registrasiproses nInformatio NocillaBrowser FirefoxTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan bahwa paket					mahasiswa (NIM)
training atau guessnMozillaGatheringFirefoxOTG-IDENT-007Memvalidasi registrasiprosesInformatio registrasiBrowserOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan paket	OTG-IDENT-006	Menguji kerentanan akun	Informatio	Browser	Tidak ditemukan
GatheringFirefoxOTG-IDENT-007Memvalidasi proses registrasiInformatioBrowser MozillaTidak ditemukanOTG-AUTHN-001Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluranAnalisa paketWireshark paketDitemukan bahwa paket oleh tools berupa clear		training atau guess	n	Mozilla	
OTG-IDENT-007       Memvalidasi proses       Informatio       Browser       Tidak ditemukan         registrasi       n       Mozilla       Mozilla       Mozilla         OTG-AUTHN-001       Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluran       Analisa       Wireshark       Ditemukan bahwa paket			Gathering	Firefox	
registrasi     n     Mozilla       Gathering     Firefox       OTG-AUTHN-001     Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluran     Analisa     Wireshark paket     Ditemukan paket     bahwa paket	OTG-IDENT-007	Memvalidasi proses	Informatio	Browser	Tidak ditemukan
Gathering     Firefox       OTG-AUTHN-001     Memverifikasi bahwa otentikasi data pengguna     Analisa captured     Wireshark     Ditemukan     bahwa paket yang tercapture       ditransfer melalui saluran     paket     oleh tools berupa clear		registrasi	n G	Mozilla	
otentikasi data pengguna captured paket oleh tools berupa clear	OTC AUTUN 001	Mamuanifikasi hahaa	Gathering	Firefox Wincelses	Ditamultan hal
ditransfer melalui saluran naket oleh tools beruna clear	010-AUTHN-001	otentikasi data pengguna	Analisa cantured	w nesnark	paket yang tercanture
		ditransfer melalui saluran	paket		oleh tools berupa clear

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	terenkripsi	header		text dikarenakan
				masih menggunakan
OTC AUTUN 002	Mamuarifikasi adalah	Duritofouse	WDCoon	protocol H11P
01G-AUTHN-002	penggupaan <i>default</i>	<i>Brutejorce</i>	WPScan, Hydra	Ditemukan delault
	penggunaan uejuun password (weak password)	dictionary	Tryuta	password adalah NIM
	pussiona (weak pussiona)	attack		Mahasiswa
OTG-AUTHN-003	Memverifikasi apakah ada	Mencoba	Browser	Tidak ada mekanisme
	mekanisme penguncian	invalid	Mozilla	penguncian akun
	akun	login	Firefox	
		beberapa		
		kali	D'1	<b>TT: 1 1 1'</b> 1
OTG-AUTHN-004	Memverifikasi direct page	Direct	Dirb,	Tidak ditemukan
	request tanpa proses <i>login</i>	page	Sqimap	celan bypass
		Parameter		
		modificatio		
		n, session		
		ID		
		prediction,		
		SQL		
OTC AUTUN 005	Mamuarifikasi bahwa	Apolico	Drougor	Tardanat karantanan
010-A01HN-003	password tidak disimpan	form login	Mozilla	akan remember me
	dalam bentuk <i>text</i>	jorni togin	Firefox	karena form input
	melainkan <i>hash</i> serta			login tidak di setting
	menemukan kerentanan			autocomplete=off
	dari fungsi <i>remember me</i>			
OTG-AUTHN-006	Memeriksa apakah aplikasi	Analisa	Browser	Website simak men-
	menginstruksikan browser	browser	Mozilla Eirofori	cache seluruh data
	untuk tidak ingat data	history dan	Firefox, Notepad $\pm\pm$	sensitive separti data
		cache	Notepad ++	diri mahasiswa
OTG-AUTHN-007	Menguji kerentanan	Melakukan	Browser	Ada beberapa karakter
	otentikasi password	beberapa	Mozilla	yang dilarang,
		percobaan	Firefox	pengguna bisa
		login		melakukan perubahan
			<b>D</b>	password
UIG-AUTHN-008	Nienguji kerentanan	Manual testine	Browser	1 Idak ditemukan
	pada forgot password	iesting	Firefox	
OTG-AUTHN-009	Menguji terhadap fungsi	Informatio	Browser	Tidak ditemukan
	ubah password/reset	n	Mozilla	
	password	Gathering	Firefox	
OTG-AUTHN-010	Menguji kerentanan	Informatio	Search	Tidak ditemukan
	otentikasi melalui jalur	n	engine	
	alternatif	Gathering	OWACD	TT: 1.1 1'4 1
UIG-AUTHZ-001	tahan terhadan maliaiana	scanning	OWASP-	i idak ditemukan
	string		Dirh	
OTG-AUTHZ-002	Percobaan akses ke dalam	Scannino	OWASP-	Ditemukan link
	fungsi administrasi tanpa	Securiting	ZAP,Nikto	http://mahasiswa.um-
	login		dan Sqlmap	palembang.ac.id
	-			Account/ResetPassw

Tahapan Kontrol	Objective	Technique	Tool	Hasil
				ord dapat digunakan
				untuk merubah
				password mahasiswa
				lain tanpa mengetahui
				password lama
				korban.
OTG-AUTHZ-003	Mencoba mendapatkan	Memanipu	Browser	Menemukan hidden
	akses admin dari user	lasi http	Mozilla	parameter nim pada
		request	Firefox	halaman
		neaaer		ResetPassword, dapat
				usor lain morubah
				profil user lain
OTG-AUTHZ-004	Mencoba mengakses data	Scanning	Browser	Berhasil mendanatkan
	tanna login	Seanning	Mozilla	informasi pembayaran
	unpu togin		Firefox	user lain dengan
				mengubah value pada
				parameter GET
				Cost_Sched_Id
OTG-SESS-001	Memerika apakah token	Analisa	Browser	Set_cookies tidak
	pada cookies dan sesinya	cookies	Mozilla	secure, tidak
	dibuat dalam cara yang		Firefox	terenkripsi,tidak
	aman dan <i>unpredictable</i>			adaSet Expire pada
			-	cookies
OTG-SESS-002	Memeriksa apakah <i>cookie</i>	Analisa	Browser	Tidak ada expired
	menyimpan informasi	cookie	Mozilla Eirofore	attribute pada cookie
	masa expired di nardalsk		FIFEIOX,	website portai
	client		ZAP	
OTG-SESS-003	Memeriksa apakah session	Analisa	Browser	Tidak ditemukan
	yang diberikan pada <i>client</i>	cookie	Mozilla	
	selalu diperbarui setelah		Firefox	
	authentifikasi			
OTG-SESS-004	Memeriksa pada cookies	Analisa	Browser	Tidak ditemukan
	apakah attribute cookies	cookie	Mozilla	
	terlihat jelas		Firefox	
OTG-SESS-005	Memeriksa POST dan	Scanning	OWASP	Tidak ditemukan
	GET request pada halaman		CSRF Tester	
	login apakah			
	terimplementasi dengan			
OTG-SESS 006	Vaik Memeriksa adakab	Analica	OWASP	Tidak ditamukan
010-5255-000	kerentanan pada fungsi	cookie	74P	I luak ultelliukali
	logout	COOKIE		
OTG-SESS-007	Memeriksa fungsi session	Analisa	OWASP-	Tidak ditemukan
	timeout	cookie	ZAP	suit or of the full
OTG-SESS-008	Memeriksa session yang	Analisa	Browser	Ditemukan session
	teridentifiksasi untuk	cookie	Mozilla	NIM dan session
	validasi <i>user</i>		Firefox	Student_Id
OTG-INVAL-001	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	vurnerability reflected		ZAP	
	XSS			
OTG-INVAL-002	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	vurnerability stored XSS		ZAP	

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-INPVAL-003	Memeriksa adakah method	Scanning	Nikto	Ditemukan method
	selain POST dan GET			OPTION, TRACE
	yang bisa di <i>explotasi</i>			dan HEAD
OTG-INPVAL-004	Memeriksa adakah HTTP	Scanning	OWASP	Adanya authorization
	Parameter Pollution		ZAP	bypass yang dapat
				digunakan untuk
				mengubah password
				dan biodata
				mahasiswa lain
OTG-INVAL-006	Memeriksa adakah cela	Scanning	OWASP	Tidak ditemukan
	SQL Injection, Oracle,		ZAP	
	SQL Server,			
	PostgreSQL,Ms Access			
	dan NoSQL			
OTG-INVAL-007	Memeriksa adakah LDAP	Scanning	OWASP	Tidak ditemukan
	Injection	_	ZAP	
OTG-INVAL-008	Memeriksa adakah ORM	Scanning	OWASP	Tidak ditemukan
	Injection	0	ZAP	
OTG-INVAL-009	Memeriksa adakah XML	Scanning	OWASP	Tidak ditemukan
	Injection	0	ZAP	
OTG-INVAL-010	Memeriksa adakah SSI	Scanning	OWASP	Tidak ditemukan
	Injection	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ZAP	
OTG-INVAL-011	Memeriksa adakah XPath	Scanning	OWASP	Tidak ditemukan
	Injection		ZAP	
OTG-INVAL-012	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	IMAP/SMTP Injection	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ZAP	
OTG-INVAL-013	Memeriksa adakah Code	Scanning	OWASP	Tidak ditemukan
	Injection, LFI dan RFI	0	ZAP	
OTG-INVAL-014	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	Command Injection	0	ZAP	
OTG-INVAL-015	Memeriksa apakah dapat	Scanning	OWASP	Tidak ditemukan
	dilakukan Buffer Heap		ZAP	
	.Stack overflow dan			
	Format string			
OTG-INVAL-016	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	incubated vulnerability		ZAP	
OTG-INVAL-017	Memeriksa adakah HTTP	Scanning	OWASP	Tidak ditemukan
	Splitting/Smugging	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	ZAP	
OTG-ERR-001	Menganalisis kode	Scanning	OWASP	Ditemukan pesan
	kesalahan	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	ZAP	kesalahan 404, 405
				dan informasi versi
				server IIS 8.0 terlihat
OTG-ERR-002	Menganalisis Stack Traces	Scanning	OWASP	namun error ini
	6		ZAP	merupakan pesan
				pencegahan dari
				serangan SOL
				injection.SSI. RFLLFI
				vang terdeteksi oleh
				WAF BigIP

# c. Website Jurnal

Hasil audit yang telah dilakukan berdasarkan metode OWASP *Testing version* 4 didapatkan hasil pada *website* jurnal http://jurnal.um.palembang.ac.id tidak lolos uji pada 20 kontrol uji dari 65 kontrol uji di 8 sub kategori standar dapat dilihat pada tabel 5.1.3.

Tahapan Kontrol	Objective	Techniqu e	Tool	Hasil
OTG-INFO-001	Mengetahui informasi desain dan konfigurasi sensitive	Analisa <i>cache</i> google	Google hacking database	Hanya ditemukan cache pada google
OTG-INFO-002	Memeriksa fingerprint web server	Analisa HTTP <i>header</i>	Netcat	Adanya informasi versi server apache 2.4.26 dengan plugin SSL versi 1.0.21 dan terinstall PHP versi 5.6.31
OTG-INFO-003	Memeriksa adakah metafile webserver	Direct searchin g	<i>Browser</i> Mozilla Firefox	Menemukan robots.txt yang mengarah pada directory cache, serta menggunakan CMS Open Journal System versi 2.4.5
OTG-INFO-004	Memeriksa adakah non- standard port service	Analisa <i>port</i> dan IP	Zenmap WHOIS DNSStuf f	Tidak ditemukan adanya port yang terbuka
OTG-INFO-005	Memeriksa adakah <i>tag</i> komentar & informasi <i>meta-data</i>	Analisa <i>source</i> <i>code</i> html	WGET CURL	Hanya ditemukan versi CMS Open Journal System 2.4.5
OTG-INFO-006	Melakukan identifikasi entry point	Manual identifica tion	Browser Mozilla Firefox	Menermukan bebrapa entry point berupa parameter
OTG-INFO-007	Melakukan pemetaan website dan memahami prinsip kerja	scanning	OWASP- ZAP	Menemukan beberapa resource URL dari spidering
OTG-INFO-008	Memeriksa adakah fingerprint web application framework	Analisa HTTP Header dan source code	Whatweb	Tidak ditemukan framework
OTG-INFO-009	Memeriksa adakah fingerprint web application	Analisa HTTP Header &source code	Whatweb	Menggunakan CMS OJS

Tabel 5.1.3 Hasil audit website jurnal

Tahapan Kontrol	Objective	Techniqu e	Tool	Hasil
OTG-INFO-010	Mendeteksi web application firewall WAF	Scanning	Nmap	Tidak menggunakan WAF
OTG-CONFIG-001	Memeriksa konfigurasi application	Scanning	Zenmap	Menemukan port yang terbuka pada port 321,322,323
OTG-CONFIG-002	Memeriksa ekstensi sensitive	Scanning	Dirb , ZAP, Nikto	Tidak ditemukan log
OTG-CONFIG-003	Memeriksa <i>file sensitive</i>	Scanning	Dirb , ZAP, Nikto	Tidak ditemukan extension file sensitif
OTG-CONFIG-004	Memeriksa adakah directory listing	Scanning	Nikto, ZAP	Ditemukan directory listing pada path /cache
OTG-CONFIG-005	Memeriksa adakah input bertipe <i>hidden</i>	Manipula si <i>hidden</i> value	Browser Mozilla Firefox	Tidak ditemukan input bertipe hidden
OTG-CONFIG-006	Memeriksa Allowed HTTP method	Scanning	Nikto	Method yang didukung adalah POST, GET dan TRACE
OTG-CONFIG-007	Memeriksa adakah HTTP Strict Transport security header	Analisa HTTP <i>Header</i>	Browser Mozilla Firefox	Tidak ditemukan HTTP Strict Transport Security Header
OTG-CONFIG-008	Memeriksa adakah RIA Cross Domain Policy	Scanning	Nikto	Tidak ditemukan RIA cross domain policy
OTG-IDENT-001	Memvalidasi hak akses website	Browsing user Policy CMS Wordpre ss, OJS	Browser Mozilla Firefox	Hak akses website telah diconfigurasi dengan baik
OTG-IDENT-002	Menguji apakah ada proses registrasi <i>user</i>	Manual testing	Browser Mozilla Firefox	Ditemukan adanya proses registrasi user sebagai anggota
OTG-IDENT-003	Menguji apakah penyerang dapat membuat akun <i>valid</i> tanpa melalui aplikasi	Manipul asi http request	Browser Mozilla Firefox	Tidak memungkinkan membuat akun valid tanpa melalui aplikasi
OTG-IDENT-004	Memeriksa semua form login dan mencoba guessable password	Manual input	Browser Mozilla Firefox	Tidak ditemukan
OTG-IDENT-005	Menguji apakah terdapat kelemahan pada pengaturan nama pengguna	Informati on Gatherin g	Search Engine	Tidak ditemukan
OTG-IDENT-006	Menguji kerentanan akun training atau guess	Informati on Gatherin g	Browser Mozilla Firefox	Tidak ditemukan
OTG-IDENT-007	Memvalidasi proses registrasi	Informati on Gatherin 8	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-001	Memverifikasi bahwa otentikasi data pengguna	Analisa <i>captured</i>	Wireshar k	Ditemukan bahwa paket yang tercapture oleh

Tahapan Kontrol	Objective	Techniqu e	Tool	Hasil
	ditransfer melalui saluran terenkripsi	paket <i>header</i>		tools berupa clear text dikarenakan masih menggunakan protocol HTTP
OTG-AUTHN-002	Memverifikasi adakah penggunaan <i>default</i> password (weak password)	Bruteforc e dan dictionar y attack	WPScan, Hydra	Ditemukan username beberapa user terlihat dari directory /public/site/image dan hanya mendapatkan satu akun valid gilang dengan password gilang123
OTG-AUTHN-003	Memverifikasi apakah ada mekanisme penguncian akun	Mencoba <i>invalid</i> <i>login</i> beberapa kali	Browser Mozilla Firefox	Tidak ada mekanisme penguncian akun
OTG-AUTHN-004	Memverifikasi direct page request tanpa proses <i>login</i>	Direct page request, Paramet er modificat ion, session ID predictio n,SQL Injection	Dirb, Sqlmap	Tidak ditemukan celah bypass
OTG-AUTHN-005	Memverifikasi bahwa password tidak disimpan dalam bentuk text melainkan hash serta menemukan kerentanan dari fungsi remember me	Analisa form login	Browser Mozilla Firefox	Terdapat kerentanan akan remember me karena form input login tidak di setting autocomplete=off
OTG-AUTHN-006	Memeriksa apakah aplikasi menginstruksikan <i>browser</i> untuk tidak ingat data	Analisa browser history dan browser cache	Browser Mozilla Firefox, Notepad ++	Cache control diset public sehingga data tersimpan pada folder cache
OTG-AUTHN-007	Menguji kerentanan otentikasi password	Melakuk an beberapa percobaa n <i>login</i>	Browser Mozilla Firefox	Tidak ada karakter yang dilarang
OTG-AUTHN-008	Menguji kerentanan pertanyaan dan jawaban pada <i>forgot password</i>	Manual testing	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-009	Menguji terhadap fungsi ubah password/reset password	Informati on Gatherin g	Browser Mozilla Firefox	Tidak ditemukan

Tahapan Kontrol	Objective	Techniqu e	Tool	Hasil
OTG-AUTHN-010	Menguji kerentanan otentikasi melalui jalur alternatif	Informati on Gatherin g	Search engine	Tidak ditemukan
OTG-AUTHZ-001	Menguji apakah aplikasi tahan terhadap <i>malicious</i> <i>string</i>	Scanning	OWASP- ZAP,Nik to, Dirb	Tidak ditemukan
OTG-AUTHZ-002	Percobaan akses ke dalam fungsi administrasi tanpa <i>login</i>	Scanning	OWASP- ZAP,Nik to dan Sqlmap	Tidak ditemukan
OTG-AUTHZ-003	Mencoba mendapatkan akses <i>admin</i> dari <i>user</i>	Memanip ulasi http request header	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHZ-004	Mencoba mengakses data tanpa <i>login</i>	Scanning	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-001	Memerika apakah token pada <i>cookies</i> dan sesinya dibuat dalam cara yang aman dan <i>unpredictable</i>	Analisa cookies	Browser Mozilla Firefox	Menggunakan cookie tetap dengan nama OJJSID
OTG-SESS-002	Memeriksa apakah cookie menyimpan informasi masa expired di harddisk client	Analisa <i>cookie</i>	Browser Mozilla Firefox, OWASP- ZAP	Tidak ada expired attribute pada cookie website portal
OTG-SESS-003	Memeriksa apakah <i>session</i> yang diberikan pada <i>client</i> selalu diperbarui setelah authentifikasi	Analisa cookie	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-004	Memeriksa pada <i>cookies</i> apakah attribute <i>cookies</i> terlihat jelas	Analisa <i>cookie</i>	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-005	Memeriksa POST dan GET <i>request</i> pada halaman <i>login</i> apakah terimplementasi dengan baik	Scanning	OWASP CSRF Tester	Tidak ditemukan
OTG-SESS-006	Memeriksa adakah kerentanan pada fungsi <i>logout</i>	Analisa <i>cookie</i>	OWASP- ZAP	Tidak ditemukan
OTG-SESS-007	Memeriksa fungsi session timeout	Analisa <i>cookie</i>	OWASP- ZAP	Tidak ditemukan
OTG-SESS-008	Memeriksa <i>session</i> yang teridentifiksasi untuk validasi <i>user</i>	Analisa <i>cookie</i>	Browser Mozilla Firefox	Tidak ditemukan
OTG-INVAL-001	Memeriksa adakah vurnerability reflected XSS	Scanning	OWASP ZAP	Tidak ditemukan
OTG-INVAL-002	Memeriksa adakah vurnerability stored XSS	Scanning	OWASP ZAP	Tidak ditemukan

Tahapan Kontrol	Objective	Techniqu	Tool	Hasil
		e		
OTG-INPVAL-003	Memeriksa adakah method	Scanning	Nikto	Ditemukan method
	selain POST dan GET			TRACE
OTO DIDUAL 004	yang bisa di <i>explotasi</i>	<i>a</i> .	ONLAGE	
OTG-INPVAL-004	Memeriksa adakah HTTP	Scanning	OWASP	Tidak ditemukan
OTC INVAL 000	Parameter Pollution	<u>с</u> .		T' 1.1 1' ( 1
UIG-INVAL-000	SOL Injection Oracle	Scanning	UWASP ZAD	Пак анетикап
	SQL Injection, Oracle,		ZAI	
	PostgreSOL Ms Access			
	dan NoSOL			
OTG-INVAL-007	Memeriksa adakah LDAP	Scanning	OWASP	Tidak ditemukan
	Injection	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	ZAP	
OTG-INVAL-008	Memeriksa adakah ORM	Scanning	OWASP	Tidak ditemukan
	Injection	, i i i i i i i i i i i i i i i i i i i	ZAP	
OTG-INVAL-009	Memeriksa adakah XML	Scanning	OWASP	Tidak ditemukan
	Injection		ZAP	
OTG-INVAL-010	Memeriksa adakah SSI	Scanning	OWASP	Tidak ditemukan
	Injection		ZAP	
OTG-INVAL-011	Memeriksa adakah XPath	Scanning	OWASP	Tidak ditemukan
OTO DULL 010	Injection	<i>a</i> .	ZAP	
OTG-INVAL-012	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
OTC INVAL 012	IMAP/SMTP Injection	c ·		TP: 1.1. 1'4
UIG-INVAL-013	Memeriksa adakan <i>Code</i>	Scanning	OWASP	I idak ditemukan
OTG INVAL 014	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
010-110741-014	Command Injection	Scanning		Tidak uttenlukan
OTG-INVAL-015	Memeriksa anakah danat	Scanning	OWASP	Tidak ditemukan
	dilakukan Buffer Hean	Seanning	ZAP	Truck uterhukun
	<i>Stack overflow</i> dan			
	Format string			
OTG-INVAL-016	Memeriksa adakah	Scanning	OWASP	Tidak ditemukan
	incubated vulnerability		ZAP	
OTG-INVAL-017	Memeriksa adakah HTTP	Scanning	OWASP	Tidak ditemukan
	Splitting/Smugging		ZAP	
OTG-ERR-001	Menganalisis kode	Scanning	OWASP	Ditemukan kesalahan
	kesalahan		ZAP	scripting pada fuction
				import() yang harusnya
				tidak ditampilkan, dan
				adanya error
				404,403,403 dali 301
				server versi PHP
OTG-FRR-002	Menganalisis Stack Traces	Scanning	OWASP	Tidak ditemukan
010 ERR 002	Mongunansis Stack Traces	Seanning	ZAP	Truck uterhukun

# 5.1.2. Hasil Optimalisasi E-Jurnal UMP

Hasil Optimalisasi yang telah dilakukan berdasarkan metode OWASP *Testing version* 4 didapatkan hasil pada *website* http://jurnal.um-palembang.ac.id Universitas Muhammadiyah Palembang yang telah dioptimalisasi ditandai dengan tanda ☑ dapat dilihat pada tabel 5.1.4.

No	Tahapan Kontrol	Hasil	Hasil
		Audit	Optimalisasi
1	OTG-INFO-001		
2	OTG-INFO-002	×	$\overline{\mathbf{A}}$
3	OTG-INFO-003	×	$\square$
4	OTG-INFO-004		
5	OTG-INFO-005	X	
6	OTG-INFO-006	X	
7	OTG-INFO-007	X	
8	OTG-INFO-008		
9	OTG-INFO-009	X	
10	OTG-INFO-010	X	
11	OTG-CONFIG-001	X	
12	OTG-CONFIG-002		
13	OTG-CONFIG-003		
14	OTG-CONFIG-004	×	

Tabel 5.1.4 Hasil Optimalisasi website jurnal

15	OTG-CONFIG-005		
16	OTG-CONFIG-006	×	$\mathbf{\overline{N}}$
17	OTG-CONFIG-007	×	$\overline{\mathbf{N}}$
18	OTG-CONFIG-008		
19	OTG-IDENT-001		
20	OTG-IDENT-002	×	$\mathbf{N}$
21	OTG-IDENT-003		
22	OTG-IDENT-004		
23	OTG-IDENT-005		
24	OTG-IDENT-006		
25	OTG-IDENT-007		
26	OTG-AUTHN-001	X	$\mathbf{N}$
27	OTG-AUTHN-002	×	$\mathbf{\overline{N}}$
28	OTG-AUTHN-003		
29	OTG-AUTHN-004		
30	OTG-AUTHN-005	×	Ń
31	OTG-AUTHN-006	×	$\mathbf{\overline{N}}$
32	OTG-AUTHN-007	×	$\overline{\mathbf{N}}$
33	OTG-AUTHN-008		
34	OTG-AUTHN-009		
35	OTG-AUTHN-010		
36	OTG-AUTHZ-001		
37	OTG-AUTHZ-002		
38	OTG-AUTHZ-003		
39	OTG-AUTHZ-004		
40	OTG-SESS-001	×	$\mathbf{\overline{A}}$
41	OTG-SESS-002		
·			

43       OTG-SESS-004       □       □         44       OTG-SESS-005       □       □         45       OTG-SESS-006       □       □         46       OTG-SESS-007       □       □         47       OTG-SESS-008       □       □
44       OTG-SESS-005       □       □         45       OTG-SESS-006       □       □         46       OTG-SESS-007       □       □         47       OTG-SESS-008       □       □
45       OTG-SESS-006       □       □         46       OTG-SESS-007       □       □         47       OTG-SESS-008       □       □         48       OTG-DWAL_001       □       □
46     OTG-SESS-007     □     □       47     OTG-SESS-008     □     □
47 OTG-SESS-008
49 OTG-INVAL-002
50 OTG-INPVAL-003
51 OTG-INPVAL-004
52 OTG-INVAL-006
53 OTG-INVAL-007
54 OTG-INVAL-008
55 OTG-INVAL-009
56   OTG-INVAL-010
57 OTG-INVAL-011
58         OTG-INVAL-012 <td< td=""></td<>
59         OTG-INVAL-013
60 OTG-INVAL-014
61 OTG-INVAL-015
62 OTG-INVAL-016
63 OTG-INVAL-017
64 OTG-ERR-001
65 OTG-ERR-002

Optimalisasi yang dilakukan pada *website* jurnal memuat *point-point* antara lain :

a. Melakukan upgrade versi CMS OJS terlihat pada gambar 5.1.1.

System Information	× +				a farii shina ana	and the second second
(←) → C <sup>2</sup>	🗢 🐠 🎉 🕕 jurnal.um	-palembang.ac.id/inde	x/admin/syst	.emInfo		
	E-Jurnal	Unive	rsita	ıs Mı	uham	madiyah Pa
	Home > User > Site Administration > Sy System Informatic	rstem Information				
	OJS Version					
	Current version					
	2.4.8.2 (January 5, 2018 - 08:46 AM)					
	Check for updates					
	Version history					
	VERSION	MAJOR	MINOR	REVISION	BUILD	DATE INSTALLED
	2.4.8.2	2	4	8	2	2018-01-05
	2.4.8.0	2	4	8	0	2018-01-05
	2.4.5.0	2	4	5	0	2015-01-31

Gambar 5.1.1 Hasil upgrade version CMS OJS website jurnal UMP

b. Merubah isi *file* DisPatcher.inc.php yang berada pada lokasi "C:\xampp\htdocs\jurnal\_ojs\lib\pkp\classes\core\DisPatcher.inc.php". Di bagian *error* 403 dan 404 menjadi jadi 403 *hacking not allowed* diubah seperti ini gambar 5.1.2 dan gambar 5.1.3



Gambar 5.1.2 Patch script Dispacher.inc.php 1



Gambar 5.1.3 Patch script Dispacher.inc.php 2

c. "C:\xampp\htdocs\jurnal\_ojs\lib\pkp\classes\template\PKPTemplateMana ger.inc.php" adalah *file* yang akan diubah untuk *setting cache-control* seperti terlihat pada gambar 5.1.4 dan gambar 5.1.5, dimana penulis menambahkan *script cache private* pada line 31, dan mengubah *response server* menjadi "*Cache-Control*: *private*, *no-cache*, *no-store*, *mustrevalidate*" pada halaman yang bersifat pribadi.

28	define('CACHEABILITY_NO_CACHE', 'no-cache');
29	<pre>define('CACHEABILITY_NO_STORE', 'no-store');</pre>
30	<pre>define('CACHEABILITY_PUBLIC', 'public');</pre>
31	<pre>define('CACHEABILITY_PRIVATE', 'private');</pre>
32	<pre>define('CACHEABILITY_MUST_REVALIDATE', 'must-revalidate');</pre>
33	<pre>define('CACHEABILITY_PROXY_REVALIDATE', 'proxy-revalidate');</pre>
34	

Gambar 5.1.4 Patch script PKPTemplateManager.inc.php 1

92	
93	// Assign common variables
94	<pre>\$this-&gt;styleSheets = array();</pre>
95	<pre>\$this-&gt;assign_by_ref('atvlazhata', \$this-&gt;styleSheets);</pre>
96	
97	<pre>\$this-&gt;javaScripts = array();</pre>
98	
99	<pre>// \$this-&gt;cacheability = CACHEABILITY_NO_STORE; // Safe default</pre>
100	// Set Secure Cache-Control
101	<pre>\$this-&gt;cacheability = CACHEABILITY_PRIVATE .", ". CACHEABILITY_NO_CACHE</pre>
102	.", ". CACHEABILITY_NO_STORE .", ". CACHEABILITY_MUST_REVALIDATE ;
103	
104	<pre>\$this-&gt;assign('defaultCharset', Config::getVar('i18n', 'client_charset'));</pre>
105	<pre>\$this-&gt;assign('basePath', \$this-&gt;request-&gt;getBasePath());</pre>
106	<pre>\$this-&gt;assign('baseUrl', \$this-&gt;request-&gt;getBaseUrl());</pre>
107	<pre>\$this-&gt;assign('requiresFormRequest', \$this-&gt;request-&gt;isPost());</pre>
	•

Gambar 5.1.5 Patch script PKPTemplateManager.inc.php 2

d. Edit *file* untuk *filter file Upload* dengan ekstensi yang berbahaya seperti php, exe, phtml, inf, bat, cgi, dan beberapa ekstensi lainnya yang dapat dilihat pada gambar 5.1.6. Perubahan ini dilakukan pada *file*"C:\xampp\htdocs\jurnal\_ojs\lib\pkp\classes\*file\File*Manager.inc.php"

532	Ģ	function parseFileExtension(\$fileName) {
533		<pre>\$fileParts = explode('.', \$fileName);</pre>
534	Ģ	if (is array(\$fileParts)) {
535		<pre>\$fileExtension = \$fileParts[count(\$fileParts) - 1];</pre>
536	~	
537		
538		// FIXME Check for evil
539		if (!isset(\$fileExtension)    stristr(\$fileExtension, 'exe')
540		<pre>stristr(\$fileExtension, 'phtml')    stristr(\$fileExtension, 'shtml')   </pre>
541		<pre>stristr(\$fileExtension, 'xhtml')    stristr(\$fileExtension, 'sh')   </pre>
542		<pre>stristr(\$fileExtension, 'py')    stristr(\$fileExtension, 'bat')   </pre>
543		<pre>stristr(\$fileExtension, 'inf')    stristr(\$fileExtension, 'pl')   </pre>
544		<pre>stristr(\$fileExtension, 'ggi')    stristr(\$fileExtension, 'asp')   </pre>
545		<pre>stristr(\$fileExtension, 'aspx')    stristr(\$fileExtension, 'jsp')   </pre>
546		<pre>stristr(SfileExtension, 'git')    stristr(SfileExtension, 'json')   </pre>
547		<pre>stristr(\$fileExtension, 'lock')    stristr(\$fileExtension, 'yaml')   </pre>
548	9	<pre>stristr(SfileExtension, 'php')    strlen(SfileExtension) &gt; 6    'preg match('/^\w+\$/', SfileExtension)) {</pre>
540		SfileFytengion = ityri:

Gambar 5.1.6 Patch script FileManager.inc.php

e. Mengganti nilai "*restful\_urls*" dari off menjadi on untuk menghilang index.php/ pada url bar ketika membuka *website*, ini juga berpengaruh terhadap segi keamanan CMS *Journal*, karena telah memiliki *custom response* 403 dan 404 seperti yang telihat pada Gambar 5.1.2 dan Gambar 5.1.3, perubahan dilakukan pada *file* config.inc.php seperti terlihat pada gambar 5.1.7.

```
90 ; See FAQ for more details.
91 restful_urls = On
92
93 ; Allow the X_FORWARDED_FOR
```

Gambar 5.1.7 Menghidupkann *restful\_urls* pada config.inc.php

Konfigurasi .htaccess untuk dapat menjalankan restful\_urls seperti terlihat

pada gambar 5.1.8 file .htaccess ini diletakan di directory root.

13	# Start URL RestFul
14	RewriteRule ^admin(.*)\$ index.php/index/admin\$1 [L]
15	RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} !-d
16	RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} !-f
17	RewriteCond %{REQUEST_FILENAME} !-d
18	RewriteCond %{REQUEST_FILENAME} !-f
19	<pre>#RewriteRule ^(.*)\$ index.php/\$1 [L]</pre>
20	RewriteRule ^(.*)\$ index.php/\$1 [QSA,L]
21	# End URL RestFul

Gambar 5.1.8 Konfigurasi restful\_urls pada .htaccess

f. Meng-enable kan httpd-default.conf untuk penambahan dan pengeditan beberapa konfigurasi pada apache website tersebut. Seperti terlihat pada Gambar 5.1.9 penulis menghapus tanda pagar pada Include "conf/extra/httpd-default.conf"

527	# Implements a proxy/gateway for Apache.
528	Include "conf/extra/httpd-proxy.conf"
529	# Various default settings
530	Include "conf/extra/httpd-default.conf"
531	# XAMPP settings
532	Include "conf/extra/httpd-xampp.conf"

Gambar 5.1.9 Enable httpd-default.conf pada httpd.conf

g. Mengganti ServeTokens Menjadi Prod dari yang semula Full dan ServerSignature yang semula On menjadi Off terlihat pada gambar 5.1.10. hal ini dilakukan untuk disable versi Apache yang digunakan. Sehingga hanya akan tampil "Server: Apache" pada response HTTP Header.

```
52
    # Set to one of: Full | OS | Minor | Minimal | Major | Prod
53
    # where Full conveys the most information, and Prod the least.
54
    ŧ.
55
    ServerTokens Prod
56
57
58
    # Optionally add a line containing the server version and virtual host
59
    # name to server-generated pages (internal error documents, FTP directory
    # listings, mod status and mod info output etc., but not CGI generated
60
    # documents or custom error documents).
61
    # Set to "EMail" to also include a mailto: link to the ServerAdmin.
62
63
    # Set to one of: On | Off | EMail
64
    ±
65
    ServerSignature Off
```

### Gambar 5.1.10 Konfigurasi pada httpd-default.conf

h. Mengkonfigurasikan form input Login dengan attribute autocomplete="off" seperti terlihat pada Gambar 5.1.11 yang terletak di "C:\xampp\htdocs\jurnal\_ojs\lib\pkp\templates\user\Login.tpl" dan 5.1.12 gambar yang terletak dilokasi "C:\xampp\htdocs\jurnal\_ojs\plugins\blocks\user\block.tpl". hal ini dilakukan guna mencegah pengisian username dan password secara otomatis ketika pengguna menyimpan username dan password mereka pada website jurnal.

52	$\Theta$	
53		<label for="loginUsername">{translate</label>
		key="user.username"}
54		<input id="loginUsername" name="&lt;/th" type="text"/>
		"username" value="{\$username escape}" size="20" maxlength="32"
		<pre>class="textField" autocomplete="off" /&gt;</pre>
55		
56	$\dot{\ominus}$	
57		<label for="loginPassword">{translate</label>
		key="user.password"}
58		<input <="" id="loginPassword" th="" type="password"/>
		name="password" value="{\$password escape}" size="20" class=
		"textField" autocomplete="off" />
59	-	

Gambar 5.1.11 Patch script Login.tpl



Gambar 5.1.12 Patch script block.tpl

i. Mengkonfigurasikan HTTP Header dan disable kan trace method untuk

securing website pada .htaccess terlihat pada gambar 5.1.13

99	# Menonaktifkan Method Trace
100	TraceEnable off
101	<pre># Mengedit Set-Cookie Dengan Tambahan Value HttpOnly Only</pre>
102	Header edit Set-Cookie ^(.*)\$ \$1;HttpOnly
103	# Mengedit HTTP Header For Better Security
104	Header set X-Frame-Options SAMEORIGIN
105	Header set X-XSS-Protection "1; mode=block"
106	Header set X-Content-Security-Policy "allow 'self';"
107	Header set X-Content-Type-Options "nosniff"

Gambar 5.1.13 Konfigurasi HTTP Header dan disable method trace

j. Menambahkan konfigurasi untuk disable akses dari HTTP/1.0 pada

.htaccess terlihat pada gambar 5.1.14

```
7 # Start Disable HTTP 1.0 Protocol
8 RewriteCond %{THE_REQUEST} !HTTP/1.1$
9 RewriteRule .* - [F]
10 # End Disable HTTP 1.0 Protocol
```

Gambar 5.1.14 Konfigurasi disable akses dari HTTP/1.0 pada htaccess

k. Menghidupkan plugin rewrite engine dan mengatur base url / pada

.htaccess terlihat pada gambar 5.1.15



### Gambar 5.1.15 Menghidupkan plugin rewrite engine pada htaccess

1. Disable directory listing dan server side include serta membuat redirect

untuk directory cache ke folder webroot pada .htaccess terlihat pada

gambar 5.1.16

Gambar 5.1.16 Men-disable directory listing dan server side include

m. Custom errordocument dengan htaccess terlihat pada gambar 5.1.17

29	# Custom ErrorD	Docu	ument	
30	ErrorDocument 5	500	" <script>alert('500:</th><th>Internal Server Error (Hacking Not Allowed)');location.href='/';</script> "	
31	ErrorDocument 5	501	<pre>"<script>alert('501:</pre></th><th>Not Implemented (Hacking Not Allowed)');location.href='/';</script>"</pre>	
32	ErrorDocument 5	502	<pre>"<script>alert('502:</pre></th><th>Bad Gateway (Hacking Not Allowed)');location.href='/';</script>"</pre>	
33	ErrorDocument 5	503	<pre>"<script>alert('503:</pre></th><th>Service Unavailable (Hacking Not Allowed)');location.href='/';</script>"</pre>	
34	ErrorDocument 5	504	<pre>"<script>alert('504:</pre></th><th>Gateway Timeout (Hacking Not Allowed)');location.href='/';</script>"</pre>	
35	ErrorDocument 5	505	<pre>"<script>alert('505:</pre></th><th>HTTP Version Not Supported (Hacking Not Allowed)');location.href='/';</script>"</pre>	
36	ErrorDocument 4	104	<pre>"<script>alert('404:</pre></th><th>Server Not Found (Hacking Not Allowed)');location.href='/';</script>"</pre>	
37	ErrorDocument 4	103	<pre>"<script>alert('403:</pre></th><th>Forbidden (Hacking Not Allowed)');location.href='/';</script>"</pre>	
38	ErrorDocument 4	102	<pre>"<script>alert('402:</pre></th><th>Payment Required Error (Hacking Not Allowed)');location.href='/';</script>"</pre>	
39	ErrorDocument 4	101	<pre>"<script>alert('401:</pre></th><th>Server Nauthorized (Hacking Not Allowed)');location.href='/';</script>"</pre>	
40	ErrorDocument 4	100	<pre>"<script>alert('400:</pre></th><th><pre>Bad Request (Hacking Not Allowed)');location.href='/';</script>"</pre>	

Gambar 5.1.17 Custom error document pada htaccess

n. Mengkonfigurasikan HTTP *Header* sebagai pengganti "robots.txt" di *directory cache* pada httpd-default.conf terlihat pada gambar 5.1.18. dalam kasus ini penulis menghapus *file* "robots.txt" yang telah digantikan dengan HTTP Header yang digunakan seperti terlihat pada gambar 5.1.18.

93	# Custom HTTP Header
94	# Penambahan header untuk pengganti robots.txt
95	<directory "c:="" cache"="" htdocs="" jurnal="" ojs="" xampp=""></directory>
96	Header set X-Robots-Tag "noindex, nofollow, noarchive"
97	

Gambar 5.1.18 Konfigurasi http Header pengganti robot.txt

o. Menambahkan *redirect* dari IP *address* ke *domain* jurnal.umpalembang.ac.id pada .htaccess terlihat pada gambar 5.1.19

```
29 # Redirect IP Address[103.99.214.16] Ke DNS jurnal.um-palembang.ac.id
30 RewriteCond %{HTTP_HOST} ^103\.99\.214\.16$
31 RewriteRule ^(.*)$ http://jurnal.um-palembang.ac.id/$1 [L,R=301]
```

### Gambar 5.1.19 Menambahkan redirect IP address ke domain

p. Memperbaiki error 500 di file seperti terlihat pada gambar 5.1.20 pada file

"C:\xampp\htdocs\jurnal\_ojs\plugins\gateways\resolver\ResolverPlugin.in

c.php" dan *file* 

"C:\xampp\htdocs\jurnal\_ojs\plugins\gateways\metsGateway\MetsGatewa

yPlugin.inc.php" seperti terlihat pada gambar 5.1.21

118	// Failure.
119	<pre>header("HTTP/1.1 500 Internal Server Error");</pre>
120	<pre>\$templateMgr =&amp; TemplateManager::getManager();</pre>
121	AppLocale::requireComponents(LOCALE_COMPONENT_APPLICATION_COMMON);
122	<pre>\$templateMgr-&gt;assign('message', 'pluging.gateways.resolver.errors.errorMessage');</pre>
123	<pre>\$templateMgr-&gt;display('common/message.tpl');</pre>
124	exit;
125	

Gambar 5.1.20 Patch script ResolverPlugin.inc.php

130	// Failure.
131	header("HTTP/1.1 500 Internal Server Error");
132	AppLocale::requireComponents(LOCALE_COMPONENT_APPLICATION_COMMON);
133	<pre>\$templateMgr =&amp; TemplateManager::getManager();</pre>
134	<pre>\$templateMgr-&gt;assign('message', 'pluging.gateways.metsGateway.errors.errorMessage');</pre>
135	<pre>\$templateMgr-&gt;display('common/message.tpl');</pre>
136	exit;

Gambar 5.1.21 Patch script MetsGatewayPlugin.inc.php

q. Memperbaiki *form* pencarian jurnal yang *error* pada *file* "C:\xampp\htdocs\jurnal\_ojs\*plugins*\blocks\navigation\block.tpl" terlihat pada gambar 5.1.22 dan pada gambar 5.1.23 memperbaiki *form* pencarian "C:\xampp\htdocs\jurnal\_ojs\templates\search\search.tpl" dengan menambahkan *method post* dan *patch error upgrade* OJS 2.4.8.2 pada pencarian jurnal. Pada *file* block.tpl penulis menambahkan *page="search"* dan *method="post"* dan menambahkan *method="post"* pada *file* search.tpl

14	
15	{prl assign:"searchFormUrl" page="search" op="search" escape=false}
16	
	{\$searchFormUrl parse_url:\$smarty.const.PHP_URL_QUERY parse_str:\$formU
	rlParameters}
17 (	<pre><form ?<="" action="{\$searchFormUrl strtok:" id="simplesearchForm" pre=""></form></pre>
	"[escape]" method="post">

Gambar 5.1.22 Patch script Block.tpl

23		{url assign:"searchFormUrl" op="search" escape=false}
24		
		<pre>{\$searchFormUrl parse_url:\$smarty.const.PHP_URL_QUERY parse_str:\$form UrlParameters}</pre>
25	¢	<form ?" escape}"<br="" action="{\$searchFormUrl strtck:" id="searchForm">method="post"&gt;</form>

Gambar 5.1.23 Patch script Search.tpl

- r. Patch autocomplete="off" pada beberapa form yang berisikan form password, seperti terlihat pada gambar 5.1.24, gambar 5.1.25, gambar 5.1.26, gambar 5.1.27, gambar 5.1.28, gambar 5.1.29, gambar 5.1.30 dan gambar 5.1.31.
  - 1. C:\xampp\htdocs\jurnal\_ojs\plugins\generic\dataverse\templates\datav

erseAuthForm.tpl



Gambar 5.1.24 Patch script dataverseAuthForm.tpl

2. C:\xampp\htdocs\jurnal\_ojs\*plugins*\generic\lucene\templates\*settingsF* 

orm.tpl

40	Ó		
41		{fieldLabel name="password" required="true"	
		<pre>key="plugins.generic.lucene.settings.password"}</pre>	
42	(	<input id="&lt;/th" name="password" type="password"/>	
		"password" value="{\$password escape}" size="15" maxlength="25"	
		class="textField" autocomplete="off" />	
43		 	
44		<pre><span class="instruct">{translate</span></pre>	
		<pre>key="plugins.generic.lucene.settings.passwordInstructions"}</pre>	
45	L .		
46	-		

Gambar 5.1.25 Patch script settingsForm.tpl

3. C:\xampp\htdocs\jurnal\_ojs\plugins\importexport\crossref\templates\s

## ettings.tpl



Gambar 5.1.26 Patch script settings.tpl plugin importexport crossref

4. C:\xampp\htdocs\jurnal\_ojs\plugins\importexport\datacite\templates\se

## ttings.tpl



Gambar 5.1.27 Patch script settings.tpl plugin importexport datacite

5. C:\xampp\htdocs\jurnal\_ojs\plugins\importexport\medra\templates\sett

ings.tpl



Gambar 5.1.28 Patch script script settings.tpl plugin importexport medra

6. C:\xampp\htdocs\jurnal\_ojs\templates\manager\people\usrProfileForm

158		{if !\$implicitAuth    \$implicitAuth ===
		<pre>\$smarty.const.IMPLICIT_AUTH_OPTIONAL}</pre>
159	$\Theta$	
160		{fieldLabel name="password"
		required=\$passwordRequired key="user.password"}
161	- Q	
162		<pre><input <="" id="password" name="password" pre="" type="password"/></pre>
		<pre>value="{\$password escape}" size="20" class="textField"</pre>
		autocomplete="off"/>
163		 
164		<span class="instruct">{translate</span>
		key="user.register.passwordLengthRestriction"
		length=\$minPasswordLength}
165	~	
166	C	
167	φ	
168		{fieldLabel name="password2"
		required=\$passwordRequired key="user.repeatPassword"}
169		<input <="" name="password2" th="" type="password"/>
		id="password2" value="{\$password2 escape}" size="20" class=
		"textField" autocomplete="off" />
170		

Gambar 5.1.29 Patch script usrProfileForm.tpl

7. C:\xampp\htdocs\jurnal\_ojs\templates\user\changePassword.tpl



Gambar 5.1.30 Patch script changePassword.tpl

8. C:\xampp\htdocs\jurnal\_ojs\templates\user\register.tpl

77	Θ	
78		{fieldLabel name="password" required="true"
		key="user.password"}
79		<input name="password" type="password" value="&lt;/td"/>
		"{Spassword[escape]" id="password" size="20" class="textField"
		autocomplete="off" />
80		
81		
01		(if l'eviating Haar)
02		{II !\$existingoser}
83	$\Theta$	
84		
85		{translate
		key="user.register.passwordLengthRestriction"
		length=\$minPasswordLength}
86	-	
87	0	
88		{fieldLabel name="password2"
		required="true" key="user.repeatPassword"}
89		<input <="" name="password2" td="" type="password"/>
		id="password2" value="{\$password2 escape}" size="20" class=
		"textField" autocomplete="off"/>
90	6	

Gambar 5.1.31 Patch script register.tpl

s. Memperbaiki script pemanggilan google api dan google analytic merubah

dari src="//www.google.com/jsapi" menjadi src="https://www.google.com/jsapi" dan menambahkan "https:" juga pada *link* menuju *google analytic, file* yang diperbaiki seperti terlihat pada gambar 5.1.32, gambar 5.1.33, gambar 5.1.34, gambar 5.1.35, gambar 5.1.36, gambar 5.1.37 dan gambar 5.1.38.

34		Base Jguery		
35		{if \$allowCDN} <script src="&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;&lt;u&gt;https://www.google.com/jsapi&lt;/u&gt;" type="text/javascript"></script>		
36	φ	<script type="text/javascript"></script>		

# Gambar 5.1.32 Patch script common Header.tpl

2. C:\xampp\htdocs\jurnal\_ojs\lib\pkp\templates\help\Header.tpl

30		Base Jquery			
31	{if \$allowCDN} <mark><script< mark=""> type="text/javascript" src="</script<></mark>				
		https://www.google.com/jsapi"×/script>			
32 🤅	₽	<script type="text/javascript"></script>			

Gambar 5.1.33 Patch script help Header.tpl

3. C:\xampp\htdocs\jurnal\_ojs\plugins\generic\googleAnalytics\pagetagU

rchin.tpl

11	Google Analytics
12	⊖ <script src="https://www.google-analytics.com/urchin.js" type="&lt;/th"></tr><tr><th></th><th>"text/javascript"></th></tr><tr><th>13</th><th></script>

# Gambar 5.1.34 Patch script pagetagUrchin.tpl

4. C:\xampp\htdocs\jurnal\_ojs\plugins\generic\googleAnalytics\pagetagA

nalytics.tpl bisa dilihat pada gambar 5.1.34

17	<pre>}) (window, document, 'script', '</pre>
	https://www.qoogle-analytics.com/analytics.js','ga');
18	

# Gambar 5.1.35 Patch script pagetagAnalytics.tpl

5. C:\xampp\htdocs\jurnal\_ojs\templates\article\Header.tpl

```
48 <!-- Base Jquery -->
49 {if $allowCDN}<script type="text/javascript" src="
https://www.google.com/jsapi"></script>
```

# Gambar 5.1.36 Patch script article Header.tpl

6. C:\xampp\htdocs\jurnal\_ojs\templates\rt\Header.tpl

31	Base Jguery	
32	<pre>{if \$allowCDN}<script pre="" s<="" type="text/javascript"></th><th>src="</th></tr><tr><th></th><th><pre>https://www.google.com/jsapi"></script></pre>	

# Gambar 5.1.37 Patch script rt Header.tpl

7. C:\xampp\htdocs\jurnal\_ojs\templates\Submission\comment\Header.tp



Gambar 5.1.38 Patch script comment Header.tpl

t. Pemasangan captcha pada config.inc.php seperti terlihat pada gambar

5.1.39. penulis mengganti *captcha* dari *off* menjadi *on*, *recaptcha* dari *off* menjadi *on* dan memasukkan *private* dan *public key* yang didapat dari *google recaptcha*.



Gambar 5.1.39 Pemasangan captcha pada config.inc.php

Input google recaptcha v1 yang berhasil penulis tambahkan terlihat pada

gambar 5.1.40

Profil	
Nama Pengguna *	
	Nama pengguna hanya bisa terdiri dari huruf kecil, nomor, da ketiganya.
Kata Sandi *	
	Kata sandi minimal 6 karakter.
Ulangi Kata Sandi *	
Validasi *	Meadows ROAT
	Ketik teks



- u. Pemasangan Modsecurity
  - 1. penulis mengunduh *modules* modsecurity2 di

http://www.apachelounge.com/download/

- memasukan library libcurl.dll dan yajl.dll pada *directory* "C:/xampp/apache/bin"
- setelah itu penulis memasukkan *module* mod\_security2.so pada directory "C:/xampp/apache/modules"
- lalu penulis mengganti nama *file* modsecurity.conf.example menjadi modsecurity.conf dan memasukan modsecurity.conf pada *directory* "C:/xampp/apache/conf"
- penulis melakukan konfigurasi terlihat pada gambar 5.1.41 pada *file* httpd.conf yang terletak di folder "C:/xampp/apache/conf" dengan pengubahan sebagai berikut;
  - a. menambahkan *module* "LoadModule *modules*/mod\_security2.so"
  - b. Enable "LoadModule unique\_id\_module

modules/mod\_unique\_id.so" dengan menghilangkan tanda pagar

563 # menambahkan module mod\_security2 dan meng enable kan module mod\_unique\_id 564 LoadModule security2\_module modules/mod\_security2.so 565 LoadModule unique\_id\_module modules/mod\_unique\_id.so

## Gambar 5.1.41 penambahan *module* pada httpd.conf

6. menambahkan rule modsecurity bawaan seperti terlihat pada gambar

5.1.42.

567 **#** menambahkan konfigurasi mod\_security bawaan 568 Include conf/modsecurity.conf

#### Gambar 5.1.42 menambahkan *rule* modsecurity pada httpd.conf

7. melakukan penambahan konfigurasi bawaan modsecurity pada *file* 

modsecurity.conf seperti terlihat pada gambar 5.1.43.

1	<ifmodule security2_module=""></ifmodule>
2	# merubah SecRuleEngine dari DetectionOnly menjadi On
3	SecRuleEngine On
4	# <u>mengubah nama</u> server <u>menjadi</u> IT-UMP
5	SecServerSignature IT-UMP
6	# Mengatur Response ketika terdeteksi melakukan penyerangan, response
	berupa error 403
7	SecDefaultAction "deny, phase: 2, status: 403"
8	
9	SecRequestBodyAccess On
10	# Rule Untuk Anti LFI Standard
11	SecRule ARGS "\.\./"
	"t:normalizePathWin,id:50904,severity:4,t:none,t:urlDecodeUni,t:htmlEntit
	yDecode,t:lowercase,msg:'Drive Access'"

Gambar 5.1.43 perubahan pada modsecurity.conf

8. Disable Unicode Code Point dikarenakan xampp mengirmkan pesan

error dan tidak dapat dijalankan ketika memanggil fungsi tersebut,

seperti telihat pada gambar 5.1.44

#### 221 # Specify your Unicode Code Point. 222 # This mapping is used by the t:urlDecodeUni transformation function 223 # to properly map encoded data to your language. Properly setting 224 # these directives helps to reduce false positives and negatives. 225 # 226 #SecUnicodeMapFile unicode.mapping 20127

Gambar 5.1.44 Disable rule SecUnicodeMapFile

9. Mengganti lokasi SecTmpdir dan SecDataDir seperti gambar 5.1.45



Gambar 5.1.45 perubahan lokasi directory pada file modsecurity.conf 1

10. Mengganti lokasi SecAuditLog ke tmp pada xampp seperti telihat pada

gambar 5.1.46.

```
193 SecAuditLogType Serial
194 SecAuditLog "C:/xampp/tmp/modsec_audit.log"
```



- 11. mengunduh *rule* modsecurity dari owasp pada *link* https://github.com/SpiderLabs/owasp-modsecurity-crs/tree/v3.0/master kemudian memindahkan seluruh *file* dengan ekstensi \*.data ke folder "C:/xampp/apache/conf" dan menyalin seluruh *rule* pada *file* dengan ekstensi \*.conf pada baris akhir *file* modsecurity.conf (hal ini dikarenakan ketika melakukan dengan pemanggilan include terjadi *error* pada saat menjalankan apache pada xampp)
- 12. Menghapus "<meta name="generator" content="{\$applicationName} {\$currentVersionString|escape}" />" dibaris 26 pada *file* C:\xampp\htdocs\jurnal\_ojs\lib\pkp\templates\common\header.tpl". Untuk menghilangkan tampilan versi OJS yang ada pada *website*.
- 13. Hasil optimalisasi terlihat pada gambar 5.1.47 hasil scan nikto menunjukan pesan berisikan informasi nama server dan beberapa HTTP Header yang tidak terpasang, informasi ini merupakan informasi palsu yang berasal dari konfigurasi pada costume modsecurity csr owasp yang penulis pasang.

<pre>root@kali:~# nikto -    Nikto v2.1.6</pre>	h jurnal.um-palembang.ac.i	.d -C All
+ Target IP: + Target Hostname: + Target Port: + Start Time:	103.99.214.16 jurnal.um-palembang.ac.i 80 2018-01-06 11:05:09 (GMT	.d <sup>-</sup> -5)
<pre>+ Server: IT-UMP + The anti-clickjack + The X-XSS-Protecti agent to protect aga + The X-Content-Type to render the conte + 8341 requests: 0 e + End Time:</pre>	king X-Frame-Options header on header is not defined. hinst some forms of XSS e-Options header is not set ent of the site in a differ error(s) and 3 item(s) repo 2018-01-06 11:09:12 (GMT	is not present. This header can hint to the user This could allow the user agent ent fashion to the MIME type orted on remote host -5) (243 seconds)
+ 1 host(s) tested		

Gambar 5.1.47 Hasil Scan Nikto Setelah Optimalisasi

Seperti terlihat pada gambar 52.48 *HTTP Header* pada *browser* mozilla yang penulis gunakan terlihat bahwa *server* sudah memasang *HTTP Header* seperti *X-Frame-Options, X-XSS-Protection* dan *X-Content-Type-Options,* serta konfigurasi lainya seperti *cache control* yang telah penulis konfigurasikan sedemikian rupa untuk menghindari terjadinya penyimpanan *cache* pada perangkat pengunjung *website* untuk halaman yang tidak perlu di *cache*.



Gambar 5.1.48 Hasil HTTP Header Setelah Optimalisasi

Pengujian hasil optimalisasi dengan menggunakan modsecurity adalah mencoba melakukan penyerangan pada *website* seperti XSS,LFI RFI, RCE, dan *File Upload*. Pengujian dilakukan baik menggunakan *automatic scanning tools* dan secara manual dengan berpedoman pada buku *OWASP Testing* yang penulis gunakan. Dari hasil pengujian ditemukan hasil bahwa percobaan penyerangan mendapatkan balasan pesan *error* 404 berdasarkan hasil konfigurasi pada modsecurity.conf sebelumnya. Adapun tampilan *error* 403 yang telah dimodifikasi pada konfigurasi .htaccess terlihat pada Gambar 5.1.49.



Gambar 5.1.49 Hasil Response pada percobaan penyerangan

*Response* ini berlaku baik melalui *input form*, manual url maupun Upload file yang dianggap sebuah penyerangan terhadap *website* oleh WAF modsecurity.

Adapun optimalisasi OTG-AUTHN-001 dengan mengganti protokol http ke https, tidak bisa dilakukan karena dana yang belum pasti kapan akan keluar dari rektor UMP, sehingga kami menyarankan untuk memasang protokol https pada *website* jurnal untuk kedepannya. Selain itu perlu adanya pemasangan *host based* IDS/IPS untuk meningkatkan keamanan *website*.

## 5.2 Pembahasan

Berdasarkan jurnal yang ditulis oleh Purnama dan Budi (2016) Peneliti membuktikan bahwa dengan menggunakan *tools* nikto peneliti juga menemukan beberapa vurnerablity pada website simak yaitu link http://mahasiswa.um-palembang.ac.id/Account/ResetPassword dapat digunakan untuk merubah password mahasiswa lain tanpa mengetahui password lama korban.

Berdasarkan jurnal yang ditulis oleh Hidayatullah dan Priadi (2016). Peneliti juga menggunakan teknik yang sama dalam melakukan upload webshell exploit ke dalam form input file jurnal pada website http://jurnal.umpalembang.ac.id . Walaupun peneliti berhasil mengupload file exploit, namun peneliti tidak menemukan directory tempat menyimpan file exploit tersebut. Setelah peneliti melakukan optimalisasi ditemukan bahwa directory file upload tersebut berada di drive D:/.

Berdasarkan jurnal yang ditulis oleh Muhsin dan Fajaryanto (2015) Peneliti juga menggunakan standar audit yang sama yaitu OWASP Testing versi 4. Sedangkan untuk tools yang dipakai kesamaan hanya terletak pada tools OWASP ZAP, dirb, dan OWASP CSRF Tester.

Berdasarkan jurnal yang ditulis oleh Cobantoro, Adi Fajaryanto (2016). Peneliti juga menemukan bukan hanya manajemen otentifikasi, otorisasi dan menajemen sesi yang belum diimplementasi dengan baik di ketiga website universitas muhammadiyah Palembang, namun manajemen informasi, konfigurasi, identifikasi, input validasi, penanganan pesan kesalahan juga belum dioptimalisasi.

Adapun optimalisasi yang dilakukan oleh peneliti hanya pada website jurnal dikarenakan adanya perjanjian kontrak kerja antara Universitas Muhammadiyah Palembang dengan Universitas Muhammadiyah Yogyakarta (UMY), Berdasarkan surat dengan nomor 047/F-10/UMP/I/2018 pihak UMP menolak mengizinkan akses ke kedua *webserver* portal dan simak. Dikarenakan masih adanya kontrak kerjasama antara pihak UMP dengan pihak UMY yang masih bertanggung jawab atas kedua *website* tersebut.

Penulis melakukan Optimalisasi pada 19 dari 20 kontrol audit yang ditemukan pada website jurnal. Sedangkan kontrol audit OTG-AUTHN-001 dengan mengganti protokol http ke https, tidak bisa dilakukan karena dana yang belum pasti kapan akan keluar dari rektor UMP, sehingga kami menyarankan untuk memasang protokol https pada *website* jurnal untuk kedepannya. Selain itu perlu adanya pemasangan *host based* IDS/IPS untuk meningkatkan keamanan *website*.

Adapun hasil dari diskusi penulis dengan pihak staff IT UMP Bapak Taufik yang menyatakan bahwa cukup memberikan laporan mengenai perbaikan apa saja yang harus dilakukan pada *website* tersebut dan dari laporan yang telah diberikan telah dilakukan beberapa perbaikan pada website simak oleh pihak UMY. Laporan perbaikan pada *website* simak dan portal terlampir.

## **BAB VI**

## SIMPULAN DAN SARAN

## 6.1 Simpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Audit dan Optimalisasi *Website* Universitas Muhammadiyah Palembang, maka dapat disimpulkan bahwa :

- Hasil audit yang telah dilakukan berdasarkan metode OWASP *Testing* version 4 didapatkan hasil pada ketiga website Universitas Muhammadiyah Palembang tidak lolos uji pada 31 kontrol uji dari 65 kontrol uji di 8 sub kategori standar.
- 2. Optimalisasi hanya bisa dilakukan pada website http://jurnal.umpalembang.ac.id, mencakup perbaikan seperti, upgrade CMS OJS, patch script baik pada aplikasi, konfigurasi apache, konfigurasi php dan juga memasang google recaptha pada form registration, comments, dan notification mailing list registration serta penambahan modsecurity2 pada apache sebagai web application firewall (WAF).
- 3. Metode *OWASP Testing version* 4 dapat digunakan untuk melakukan audit keamanan *website*, dikarenakan didalam metode tersebut menjelaskan caracara mengetahui celah keamanan dan memperbaiki celah keamanan *website* tersebut.

## 6.2 Saran-saran

Hasil penelitian ini memberikan kontribusi saran perbaikan celah keamanan pada *website* UMP. Untuk itu peneliti menyarankan sebagai berikut :

- 1. Agar website ini dapat diamankan dengan optimal maka diperlukan adanya dukungan perangkat keras dan perangkat lunak yang *up to date*.
- 2. Agar audit dan optimalisasi ini lebih sempurna diperlukan penelitian lebih lanjut di kemudian hari, mengingat masih begitu banyak teknik pengujian yang belum dicobakan (pengujian *OWASP Testing* tidak dilakukan secara keseluruhan) pada penelitian ini dan itu berarti belum semua celah keamanan yang didapatkan.
- 3. Guna mendapatkan hasil audit yang lebih optimal diharapkan penelitian selanjutnya dapat menggunakan hasil penelitian ini sebagai referensi dan tidak menutup kemungkinan menggunakan standar audit yang lain.