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 ☒ dapat dilihat pada tabel 5.1 dan penjelasan masing masing hasil kontrol terlampir.

Tabel 5.1 Hasil audit 3 website UMP

No	Tahapan Kontrol	Website Portal	Website Simak	Website 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	☒	☒	☒
7	OTG-INFO-007	☒	☒	☒
8	OTG-INFO-008	☐	☒	☐
9	OTG-INFO-009	☒	☐	☒
10	OTG-INFO-010	☐	☐	☒
11	OTG-CONFIG-001	☒	☒	☒
12	OTG-CONFIG-002	☐	☐	☐
13	OTG-CONFIG-003	☐	☐	☐
14	OTG-CONFIG-004	☐	☐	☒
15	OTG-CONFIG-005	☒	☐	☐
16	OTG-CONFIG-006	☒	☒	☒

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 Portal	Website Simak	Website 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

Tabel 5.1.1 Temuan audit website portal

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-INFO-001	Mengetahui informasi desain dan konfigurasi *sensitive*	Analisa *cache* google	Google *hacking database*	Hanya ditemukan *cache* pada google
OTG-INFO-002	Memeriksa *fingerprint web server*	Analisa HTTP *header*	Netcat	Adanya informasi versi sistem operasi Ubuntu versi 1.4.6 dan PHP 5.5.9
OTG-INFO-003	Memeriksa adakah *metafile webserver*	*Direct searching*	*Browser* Mozilla Firefox	Terdapat *file* robots.txt yang mengidentifikasi wp-admin dan ditemukan *meta* tag versi wordpress 4.9.1
OTG-INFO-004	Memeriksa adakah *non-standard port service*	Analisa *port* dan IP	Zenmap WHOIS DNSStuff	Tidak ditemukan adanya port yang terbuka
OTG-INFO-005	Memeriksa adakah *tag* komentar & informasi *meta-data*	Analisa *source code* html	WGET CURL	Hanya ditemukan informasi versi CMS Wordpress 4.9.1
OTG-INFO-006	Melakukan identifikasi *entry point*	*Manual identification*	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* dan *source code*	Whatweb	Menggunakan CMS Wordpress versi 4.9.1
OTG-INFO-010	Mendeteksi *web application*	Scanning	Nmap	Menggunakan WAF *BigIP*

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	firewall(WAF)			
OTG-CONFIG-001	Memeriksa konfigurasi *application*	*Scanning*	Zenmap	Ditemukan *port remote* terbuka yaitu *port* 321,322,323
OTG-CONFIG-002	Memeriksa ekstensi *sensitive*	*Scanning*	Dirb , ZAP, Nikto	Tidak ditemukan *log*
OTG-CONFIG-003	Memeriksa *file sensitive*	Scanning	Dirb , ZAP, Nikto	Tidak ditemukan informasi *file sensitive*
OTG-CONFIG-004	Memeriksa adakah *directory listing*	*Scanning*	Nikto, ZAP	Tidak ditemukannya directory *cache* hanya ditemukan robots.txt
OTG-CONFIG-005	Memeriksa adakah input bertipe *hidden*	Manipulasi *hidden value*	Browser Mozilla Firefox	Ditemukan input bertipe *hidden*
OTG-CONFIG-006	Memeriksa *Allowed* HTTP *method*	*Scanning*	Nikto	Hanya ditemukan *method* GET dan POST
OTG-CONFIG-007	Memeriksa adakah HTTP *Strict Transport security header*	Analisa HTTP *Header*	Browser Mozilla Firefox	Tidak ditemukan HTTP *Strict Transport Security Header*
OTG-CONFIG-008	Memeriksa adakah RIA *Cross Domain Policy*	*Scanning*	Nikto	Tidak didapatkan adanya RIA *cross domain policy*
OTG-IDENT-001	Memvalidasi hak akses *website*	*Browsing user Policy* CMS Wordpress, OJS	Browser Mozilla Firefox	Hak akses telah ter-mangement dengan baik
OTG-IDENT-002	Menguji apakah ada proses registrasi *user*	*Manual testing*	Browser Mozilla Firefox	Tidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administrator
OTG-IDENT-003	Menguji apakah penyerang dapat membuat akun *valid* tanpa melalui aplikasi	*Manipulasi* http *request*	Browser Mozilla Firefox	Tidak bisa membuat akun tanpa melalui aplikasi
OTG-IDENT-004	Memeriksa semua form login dan mencoba *guessable password*	*Manual input*	Browser Mozilla Firefox	Hanya ditemukan username coadmin dan superadmin pada setiap postingan pada *website*
OTG-IDENT-005	Menguji apakah terdapat kelemahan pada pengaturan nama pengguna	*Information Gathering*	Search Engine	Tidak ditemukan kelemahan pada pengaturan nama pengguna
OTG-IDENT-006	Menguji kerentanan akun *training* atau *guess*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-IDENT-007	Memvalidasi proses registrasi	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-AUTHN-001	Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluran terenkripsi	Analisa *captured* paket *header*	Wireshark	Ditemukan bahwa paket yang tercapture oleh *tools* berupa *clear* text dikarenakan masih menggunakan *protocol* HTTP
OTG-AUTHN-002	Memverifikasi adakah penggunaan *default password* (*weak password*)	*Bruteforce* dan *dictionary attack*	WPScan, Hydra	Ditemukan hanya tiga username yaitu superadmin, coadmin dan bora. Ini diakibatkan karena website portal telah ter-*install plugin Better security*
OTG-AUTHN-003	Memverifikasi apakah ada mekanisme penguncian akun	Mencoba *invalid login* beberapa kali	Browser Mozilla Firefox	Hanya terdeteksi *plugin better security*, sehingga website akan mengirimkan pesan kesalahan *login* ke *email admin*. Namun tidak sampai mengunci akun
OTG-AUTHN-004	Memverifikasi direct page request tanpa proses *login*	*Direct page request*, *Parameter modification*, *session* ID *prediction*,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 *browser* untuk tidak ingat data	Analisa *browser history* dan *browser cache*	Browser Mozilla Firefox, Notepad ++	Tidak ditemukan
OTG-AUTHN-007	Menguji kerentanan *otentikasi password*	Melakukan beberapa percobaan *login*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-008	Menguji kerentanan pertanyaan dan jawaban pada *forgot password*	*Manual testing*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-009	Menguji terhadap fungsi ubah *password*/*reset*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan

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 *malicious string*	*Scanning*	OWASP-ZAP,Nikto, Dirb	Tidak ditemukan
OTG-AUTHZ-002	Percobaan akses ke dalam fungsi administrasi tanpa *login*	*Scanning*	OWASP-ZAP,Nikto dan Sqlmap	Tidak ditemukan
OTG-AUTHZ-003	Mencoba mendapatkan akses *admin* dari *user*	Memanipulasi http *request header*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHZ-004	Mencoba mengakses data tanpa *login*	*Scanning*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-001	Memerika apakah token pada *cookies* dan sesinya dibuat dalam cara yang aman dan *unpredictable*	Analisa *cookies*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-002	Memeriksa apakah *cookie* menyimpan informasi masa *expired* di *harddisk client*	Analisa *cookie*	Browser Mozilla Firefox, OWASP-ZAP	Tidak ada *expired attribute* pada *cookie website* portal
OTG-SESS-003	Memeriksa apakah *session* yang diberikan pada *client* selalu diperbarui setelah authentifikasi	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-004	Memeriksa pada *cookies* apakah attribute *cookies* terlihat jelas	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-005	Memeriksa POST dan GET *request* pada halaman *login* apakah terimplementasi dengan baik	*Scanning*	OWASP CSRF Tester	Tidak ditemukan
OTG-SESS-006	Memeriksa adakah kerentanan pada fungsi *logout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-007	Memeriksa fungsi *session timeout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-008	Memeriksa *session* yang teridentifiksasi untuk validasi *user*	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan

Tahapan Kontrol	Objective	Technique	Tool	Hasil
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
OTG-INPVAL-003	Memeriksa adakah *method* selain POST dan GET yang bisa di *explotasi*	*Scanning*	Nikto	Tidak ditemukan
OTG-INPVAL-004	Memeriksa adakah HTTP *Parameter Pollution*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-006	Memeriksa adakah cela SQL *Injection*, Oracle, SQL *Server*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-007	Memeriksa adakah LDAP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-008	Memeriksa adakah ORM *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-009	Memeriksa adakah XML *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-010	Memeriksa adakah SSI *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-011	Memeriksa adakah XPath *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-012	Memeriksa adakah IMAP/SMTP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-013	Memeriksa adakah *Code Injection*, LFI dan RFI	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-014	Memeriksa adakah *Command Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-015	Memeriksa apakah dapat dilakukan *Buffer* ,*Heap* ,*Stack overflow* dan *Format string*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-016	Memeriksa adakah *incubated vulnerability*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-017	Memeriksa adakah HTTP *Splitting*/*Smugging*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-ERR-001	Menganalisis kode kesalahan	*Scanning*	OWASP ZAP	Ditemukan pesan kesalahan 404, *error no input file specified* dan menampilkan versi server & PHP
OTG-ERR-002	Menganalisis *Stack Traces*	*Scanning*	OWASP ZAP	Tidak ditemukan

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 desain dan konfigurasi *sensitive*	Analisa *cache* google	Google *hacking database*	Hanya ditemukan cache pada google
OTG-INFO-002	Memeriksa *fingerprint web server*	Analisa HTTP *header*	Netcat	Adanya informasi versi sistem operasi windows server Microsoft IIS versi 8.0dan ASP.Net versi 4.0.30319 dan menggunakan framework ASP.Net MVC 5.2
OTG-INFO-003	Memeriksa adakah *metafile webserver*	*Direct searching*	*Browser* Mozilla Firefox	Tidak ditemukan file robots.txt
OTG-INFO-004	Memeriksa adakah *non-standard port service*	Analisa *port* dan IP	Zenmap WHOIS DNSStuff	Tidak ditemukan adanya port yang terbuka
OTG-INFO-005	Memeriksa adakah *tag* komentar & informasi *meta-data*	Analisa *source code* html	WGET CURL	Tidak ditemukan tag komentar dan informasi meta data
OTG-INFO-006	Melakukan identifikasi *entry point*	*Manual identification*	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	Ditemukan framework ASP.Net 4.0.30319 MVC 5.2
OTG-INFO-009	Memeriksa adakah *fingerprint web application*	Analisa HTTP *Header* dan *source code*	Whatweb	Tidak menggunakan CMS
OTG-INFO-010	Mendeteksi *web application firewall*(WAF)	Scanning	Nmap	Menggunakan WAF BigIP

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-CONFIG-001	Memeriksa konfigurasi *application*	*Scanning*	Zenmap	Ditemukan port remote terbuka yaitu port 321,322,323
OTG-CONFIG-002	Memeriksa ekstensi *sensitive*	*Scanning*	Dirb , ZAP, Nikto	Tidak ditemukan log
OTG-CONFIG-003	Memeriksa *file sensitive*	Scanning	Dirb , ZAP, Nikto	Tidak ditemukan informasi file sensitive
OTG-CONFIG-004	Memeriksa adakah *directory listing*	*Scanning*	Nikto, ZAP	Tidak ditemukannya directory cache.
OTG-CONFIG-005	Memeriksa adakah input bertipe *hidden*	Manipulasi *hidden value*	Browser Mozilla Firefox	Tidak ditemukan input bertipe hidden
OTG-CONFIG-006	Memeriksa *Allowed* HTTP *method*	*Scanning*	Nikto	Ditemukan method OPTION, TRACE, GET,HEAD,dan POST
OTG-CONFIG-007	Memeriksa adakah HTTP *Strict Transport security header*	Analisa HTTP *Header*	Browser Mozilla Firefox	Tidak ditemukan HTTP Strict Transport Security Header
OTG-CONFIG-008	Memeriksa adakah RIA *Cross Domain Policy*	*Scanning*	Nikto	Tidak didapatkan adanya RIA cross domain policy
OTG-IDENT-001	Memvalidasi hak akses *website*	*Browsing user Policy* CMS Wordpress, OJS	Browser Mozilla Firefox	Hak akses masih memiliki kekurangan. Karena hanya terdiri dari Mahasiswa dan Orang tua saja.
OTG-IDENT-002	Menguji apakah ada proses registrasi *user*	*Manual testing*	Browser Mozilla Firefox	Tidak terdapat fungsi registrasi, registrasi hanya dapat dilakukan oleh administrator
OTG-IDENT-003	Menguji apakah penyerang dapat membuat akun *valid* tanpa melalui aplikasi	*Manipulasi* http *request*	Browser Mozilla Firefox	Tidak bisa membuat akun tanpa melalui aplikasi
OTG-IDENT-004	Memeriksa semua form login dan mencoba *guessable password*	*Manual input*	Browser Mozilla Firefox	Tidak berhasil menggunakan guessable username dan password seperti admin
OTG-IDENT-005	Menguji apakah terdapat kelemahan pada pengaturan nama pengguna	*Information Gathering*	Search Engine	Ditemukan kelemahan dikarenakan username dan password adalah nomor induk mahasiswa (NIM)
OTG-IDENT-006	Menguji kerentanan akun *training* atau *guess*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-IDENT-007	Memvalidasi proses registrasi	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-001	Memverifikasi bahwa otentikasi data pengguna ditransfer melalui saluran	Analisa *captured* paket	Wireshark	Ditemukan bahwa paket yang tercapture oleh tools berupa clear

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	terenkripsi	*header*		text dikarenakan masih menggunakan protocol HTTP
OTG-AUTHN-002	Memverifikasi adakah penggunaan *default password* (*weak password*)	*Bruteforce* dan *dictionary attack*	WPScan, Hydra	Ditemukan default susername dan password adalah NIM Mahasiswa
OTG-AUTHN-003	Memverifikasi apakah ada mekanisme penguncian akun	Mencoba *invalid login* beberapa kali	Browser Mozilla Firefox	Tidak ada mekanisme penguncian akun
OTG-AUTHN-004	Memverifikasi direct page request tanpa proses *login*	*Direct page request*, *Parameter modification*, *session* ID *prediction*, 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 *browser* untuk tidak ingat data	Analisa *browser history* dan *browser cache*	Browser Mozilla Firefox, Notepad ++	Website simak men-cache seluruh data termasuk onformasi sensitive seperti data diri mahasiswa
OTG-AUTHN-007	Menguji kerentanan *otentikasi password*	Melakukan beberapa percobaan *login*	Browser Mozilla Firefox	Ada beberapa karakter yang dilarang, pengguna bisa melakukan perubahan password
OTG-AUTHN-008	Menguji kerentanan pertanyaan dan jawaban pada *forgot password*	*Manual testing*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-009	Menguji terhadap fungsi ubah *password*/*reset password*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-010	Menguji kerentanan otentikasi melalui jalur alternatif	*Information Gathering*	Search engine	Tidak ditemukan
OTG-AUTHZ-001	Menguji apakah aplikasi tahan terhadap *malicious string*	*Scanning*	OWASP-ZAP,Nikto, Dirb	Tidak ditemukan
OTG-AUTHZ-002	Percobaan akses ke dalam fungsi administrasi tanpa *login*	*Scanning*	OWASP-ZAP,Nikto dan Sqlmap	Ditemukan link http://mahasiswa.um-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 akses *admin* dari *user*	Memanipulasi http *request header*	Browser Mozilla Firefox	Menemukan hidden parameter nim pada halaman ResetPassword, dapat merubah password user lain, merubah profil user lain
OTG-AUTHZ-004	Mencoba mengakses data tanpa *login*	*Scanning*	Browser Mozilla Firefox	Berhasil mendapatkan informasi pembayaran user lain dengan mengubah value pada parameter GET Cost_Sched_Id
OTG-SESS-001	Memerika apakah token pada *cookies* dan sesinya dibuat dalam cara yang aman dan *unpredictable*	Analisa *cookies*	Browser Mozilla Firefox	Set_cookies tidak secure, tidak terenkripsi,tidak adaSet Expire pada cookies
OTG-SESS-002	Memeriksa apakah *cookie* menyimpan informasi masa *expired* di *harddisk client*	Analisa *cookie*	Browser Mozilla Firefox, OWASP-ZAP	Tidak ada expired attribute pada cookie website portal
OTG-SESS-003	Memeriksa apakah *session* yang diberikan pada *client* selalu diperbarui setelah authentifikasi	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-004	Memeriksa pada *cookies* apakah attribute *cookies* terlihat jelas	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-005	Memeriksa POST dan GET *request* pada halaman *login* apakah terimplementasi dengan baik	*Scanning*	OWASP CSRF Tester	Tidak ditemukan
OTG-SESS-006	Memeriksa adakah kerentanan pada fungsi *logout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-007	Memeriksa fungsi *session timeout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-008	Memeriksa *session* yang teridentifiksasi untuk validasi *user*	Analisa *cookie*	Browser Mozilla Firefox	Ditemukan session NIM dan session Student_Id
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	Technique	Tool	Hasil
OTG-INPVAL-003	Memeriksa adakah *method* selain POST dan GET yang bisa di *explotasi*	*Scanning*	Nikto	Ditemukan method OPTION, TRACE dan HEAD
OTG-INPVAL-004	Memeriksa adakah HTTP *Parameter Pollution*	*Scanning*	OWASP ZAP	Adanya authorization bypass yang dapat digunakan untuk mengubah password dan biodata mahasiswa lain
OTG-INVAL-006	Memeriksa adakah cela SQL *Injection*, Oracle, SQL *Server*, PostgreSQL,Ms *Access* dan NoSQL	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-007	Memeriksa adakah LDAP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-008	Memeriksa adakah ORM *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-009	Memeriksa adakah XML *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-010	Memeriksa adakah SSI *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-011	Memeriksa adakah XPath *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-012	Memeriksa adakah IMAP/SMTP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-013	Memeriksa adakah *Code Injection*, LFI dan RFI	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-014	Memeriksa adakah *Command Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-015	Memeriksa apakah dapat dilakukan *Buffer* ,*Heap* ,*Stack overflow* dan *Format string*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-016	Memeriksa adakah *incubated vulnerability*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-017	Memeriksa adakah HTTP *Splitting*/*Smugging*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-ERR-001	Menganalisis kode kesalahan	*Scanning*	OWASP ZAP	Ditemukan pesan kesalahan 404, 405 dan informasi versi server IIS 8.0 terlihat
OTG-ERR-002	Menganalisis *Stack Traces*	*Scanning*	OWASP ZAP	namun error ini merupakan pesan pencegahan dari serangan SQL injection,SSI, RFI,LFI yang 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.

Tabel 5.1.3 Hasil audit website jurnal

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-INFO-001	Mengetahui informasi desain dan konfigurasi *sensitive*	Analisa *cache* google	Google *hacking database*	Hanya ditemukan cache pada google
OTG-INFO-002	Memeriksa *fingerprint web server*	Analisa HTTP *header*	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 searching*	*Browser* 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 *port* dan IP	Zenmap WHOIS DNSStuff	Tidak ditemukan adanya port yang terbuka
OTG-INFO-005	Memeriksa adakah *tag* komentar & informasi *meta-data*	Analisa *source code* html	WGET CURL	Hanya ditemukan versi CMS Open Journal System 2.4.5
OTG-INFO-006	Melakukan identifikasi *entry point*	*Manual identification*	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

Tahapan Kontrol	Objective	Technique	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 *file sensitive*	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 *hidden*	Manipulasi *hidden 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 *Header*	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 Wordpress, OJS	Browser Mozilla Firefox	Hak akses website telah diconfigurasi dengan baik
OTG-IDENT-002	Menguji apakah ada proses registrasi *user*	*Manual testing*	Browser Mozilla Firefox	Ditemukan adanya proses registrasi user sebagai anggota
OTG-IDENT-003	Menguji apakah penyerang dapat membuat akun *valid* tanpa melalui aplikasi	*Manipulasi* 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	*Information Gathering*	Search Engine	Tidak ditemukan
OTG-IDENT-006	Menguji kerentanan akun *training* atau *guess*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-IDENT-007	Memvalidasi proses registrasi	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-001	Memverifikasi bahwa otentikasi data pengguna	Analisa *captured*	Wireshark	Ditemukan bahwa paket yang tercapture oleh

Tahapan Kontrol	Objective	Technique	Tool	Hasil
	ditransfer melalui saluran terenkripsi	paket *header*		tools berupa clear text dikarenakan masih menggunakan protocol HTTP
OTG-AUTHN-002	Memverifikasi adakah penggunaan *default password* (*weak password*)	*Bruteforce* dan *dictionary 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 *invalid login* beberapa kali	Browser Mozilla Firefox	Tidak ada mekanisme penguncian akun
OTG-AUTHN-004	Memverifikasi direct page request tanpa proses *login*	*Direct page request, Parameter modification, session* ID *prediction*,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 *browser* 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*	Melakukan beberapa percobaan *login*	Browser Mozilla Firefox	Tidak ada karakter yang dilarang
OTG-AUTHN-008	Menguji kerentanan pertanyaan dan jawaban pada *forgot password*	*Manual testing*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHN-009	Menguji terhadap fungsi ubah *password*/*reset password*	*Information Gathering*	Browser Mozilla Firefox	Tidak ditemukan

Tahapan Kontrol	Objective	Technique	Tool	Hasil
OTG-AUTHN-010	Menguji kerentanan otentikasi melalui jalur alternatif	*Information Gathering*	Search engine	Tidak ditemukan
OTG-AUTHZ-001	Menguji apakah aplikasi tahan terhadap *malicious string*	*Scanning*	OWASP-ZAP,Nikto, Dirb	Tidak ditemukan
OTG-AUTHZ-002	Percobaan akses ke dalam fungsi administrasi tanpa *login*	*Scanning*	OWASP-ZAP,Nikto dan Sqlmap	Tidak ditemukan
OTG-AUTHZ-003	Mencoba mendapatkan akses *admin* dari *user*	Memanipulasi http *request header*	Browser Mozilla Firefox	Tidak ditemukan
OTG-AUTHZ-004	Mencoba mengakses data tanpa *login*	*Scanning*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-001	Memerika apakah token pada *cookies* dan sesinya dibuat dalam cara yang aman dan *unpredictable*	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 *cookie*	Browser Mozilla Firefox, OWASP-ZAP	Tidak ada expired attribute pada cookie website portal
OTG-SESS-003	Memeriksa apakah *session* yang diberikan pada *client* selalu diperbarui setelah authentifikasi	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-004	Memeriksa pada *cookies* apakah attribute *cookies* terlihat jelas	Analisa *cookie*	Browser Mozilla Firefox	Tidak ditemukan
OTG-SESS-005	Memeriksa POST dan GET *request* pada halaman *login* apakah terimplementasi dengan baik	*Scanning*	OWASP CSRF Tester	Tidak ditemukan
OTG-SESS-006	Memeriksa adakah kerentanan pada fungsi *logout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-007	Memeriksa fungsi *session timeout*	Analisa *cookie*	OWASP-ZAP	Tidak ditemukan
OTG-SESS-008	Memeriksa *session* yang teridentifiksasi untuk validasi *user*	Analisa *cookie*	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	Technique	Tool	Hasil
OTG-INPVAL-003	Memeriksa adakah *method* selain POST dan GET yang bisa di *explotasi*	*Scanning*	Nikto	Ditemukan method TRACE
OTG-INPVAL-004	Memeriksa adakah HTTP *Parameter Pollution*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-006	Memeriksa adakah cela SQL *Injection*, Oracle, SQL *Server*, PostgreSQL,Ms *Access* dan NoSQL	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-007	Memeriksa adakah LDAP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-008	Memeriksa adakah ORM *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-009	Memeriksa adakah XML *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-010	Memeriksa adakah SSI *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-011	Memeriksa adakah XPath *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-012	Memeriksa adakah IMAP/SMTP *Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-013	Memeriksa adakah *Code Injection*, LFI dan RFI	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-014	Memeriksa adakah *Command Injection*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-015	Memeriksa apakah dapat dilakukan *Buffer* ,*Heap* ,*Stack overflow* dan *Format string*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-016	Memeriksa adakah *incubated vulnerability*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-INVAL-017	Memeriksa adakah HTTP *Splitting/Smugging*	*Scanning*	OWASP ZAP	Tidak ditemukan
OTG-ERR-001	Menganalisis kode kesalahan	*Scanning*	OWASP ZAP	Ditemukan kesalahan scripting pada fuction import() yang harusnya tidak ditampilkan, dan adanya error 404,403,405 dan 501 yang menampilkan versi server, versi PHP
OTG-ERR-002	Menganalisis *Stack Traces*	*Scanning*	OWASP ZAP	Tidak ditemukan

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.

Tabel 5.1.4 Hasil Optimalisasi website jurnal

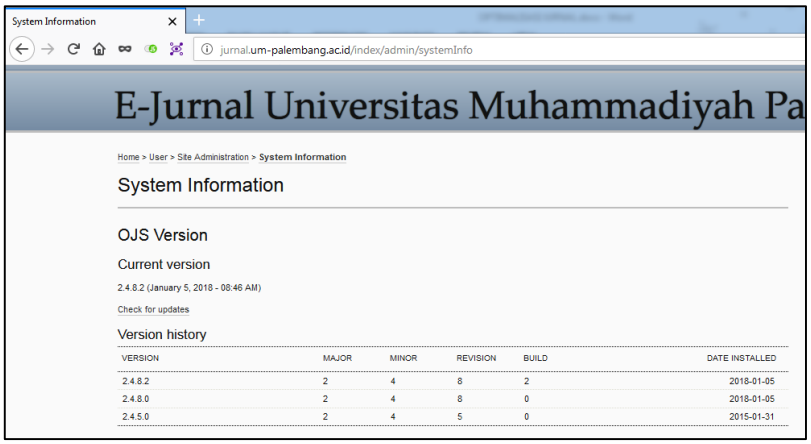
No	Tahapan Kontrol	Hasil Audit	Hasil Optimalisasi
1	OTG-INFO-001	☐	☐
2	OTG-INFO-002	☒	☑
3	OTG-INFO-003	☒	☑
4	OTG-INFO-004	☐	☐
5	OTG-INFO-005	☒	☑
6	OTG-INFO-006	☒	☑
7	OTG-INFO-007	☒	☑
8	OTG-INFO-008	☐	☐
9	OTG-INFO-009	☒	☑
10	OTG-INFO-010	☒	☑
11	OTG-CONFIG-001	☒	☑
12	OTG-CONFIG-002	☐	☐
13	OTG-CONFIG-003	☐	☐
14	OTG-CONFIG-004	☒	☑

15	OTG-CONFIG-005	☐	☐
16	OTG-CONFIG-006	☒	☑
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	☐	☐
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	☐	☐

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

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



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

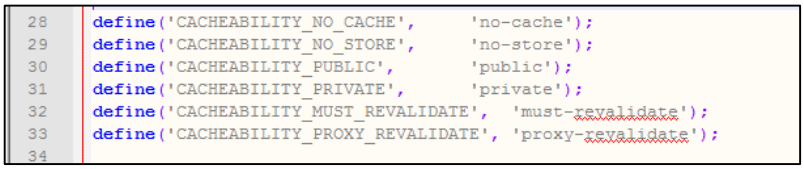
```
if (isset($_SERVER['HTTP_X_MOZ']) && $_SERVER['HTTP_X_MOZ'] == 'prefetch') {
    header('HTTP/1.1 403 Hacking Not Allowed');
    echo '403: Hacking Not Allowed<br><br>Pre-fetching not allowed.';
    exit;
}
```

Gambar 5.1.2 *Patch script* Dispacher.inc.php 1

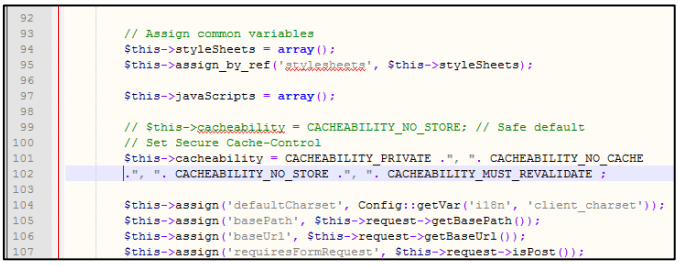
```
240
241     /**
242      * Handle a 404 error (page not found).
243      */
244     function handle404() {
245         PKPRequest::_checkThis();
246
247         header('HTTP/1.1 403 Hacking Not Allowed');
248         fatalError('403: Hacking Not Allowed');
249     }
250 }
251
```

Gambar 5.1.3 *Patch script* Dispacher.inc.php 2

c. "C:\xampp\htdocs\jurnal_ojs\lib\pkp\classes\template\PKPTemplateManager.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*, *must-revalidate*" pada halaman yang bersifat pribadi.

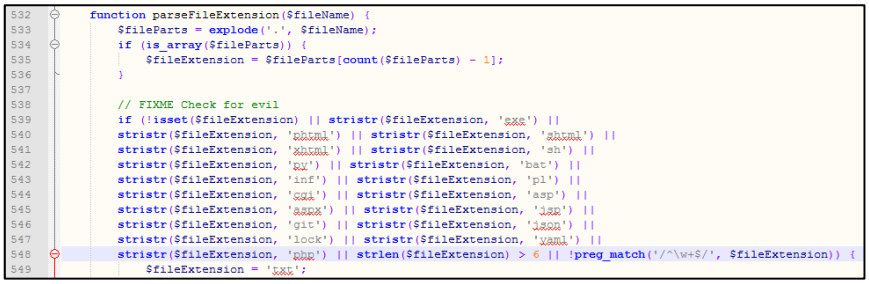


Gambar 5.1.4 *Patch script* PKPTemplateManager.inc.php 1



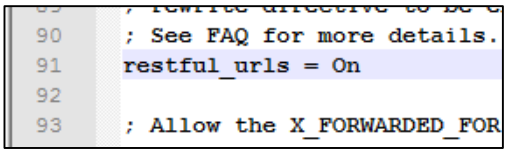
Gambar 5.1.5 *Patch script* PKPTemplateManager.inc.php 2

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"



Gambar 5.1.6 *Patch script File*Manager.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.



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.*

```
# Start URL RestFul
RewriteRule ^admin(.*)$ index.php/index/admin$1 [L]
RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} !-d
RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f
#RewriteRule ^(.*)$ index.php/$1 [L]
RewriteRule ^(.*)$ index.php/$1 [QSA,L]
# End URL RestFul
```

Gambar 5.1.8 Konfigurasi *restful_urls* pada .htaccess

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

```
# Implements a proxy/gateway for Apache.
Include "conf/extra/httpd-proxy.conf"
# Various default settings
Include "conf/extra/httpd-default.conf"
# XAMPP settings
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  #
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
60  # listings, mod_status and mod_info output etc., but not CGI generated
61  # documents or custom error documents).
62  # Set to "EMail" to also include a mailto: link to the ServerAdmin.
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 gambar 5.1.12 yang terletak dilokasi "C:\xampp\htdocs\jurnal_ojs*plugin*s\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      <tr>
53          <td class="label"><label for="loginUsername">{translate
            key="user.username"}</label></td>
54          <td class="value"><input type="text" id="loginUsername" name=
            "username" value="{$username|escape}" size="20" maxlength="32"
            class="textField" autocomplete="off" /></td>
55      </tr>
56      <tr>
57          <td class="label"><label for="loginPassword">{translate
            key="user.password"}</label></td>
58          <td class="value"><input type="password" id="loginPassword"
            name="password" value="{$password|escape}" size="20" class=
            "textField" autocomplete="off" /></td>
59      </tr>
```

Gambar 5.1.11 *Patch script Login*.tpl

```
45                      <tr>
46                          <td><label for="sidebar-username">
                            {translate key="user.username"}</label></td>
47                          <td><input type="text" id=
                            "sidebar-username" name="username" value=""
                             size="12" maxlength="32" class="textField"
                             autocomplete="off" /></td>
48                      </tr>
49                      <tr>
50                          <td><label for="sidebar-password">
                            {translate key="user.password"}</label></td>
51                          <td><input type="password" id=
                            "sidebar-password" name="password" value=
                            "{$password|escape}" size="12" class=
                            "textField" autocomplete="off" /></td>
52                      </tr>
```

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  # Mengedit Set-Cookie Dengan Tambahan Value HttpOnly Only
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

```
3   # Turn mod_rewrite on
4   RewriteEngine On
5   RewriteBase /
```

Gambar 5.1.15 Menghidupkan *plugin* rewrite engine pada htaccess

l. *Disable directory listing* dan *server side include* serta membuat *redirect* untuk *directory cache* ke *folder webroot* pada .htaccess terlihat pada gambar 5.1.16

```
23  # Disabled Directory Listing dan Server Side Includes
24  Options -Indexes -Includes
25
26  # Redirect Otomatis Saat Akses Folder Cache
27  Redirect 301 /cache http:
```

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 ErrorDocument
30  ErrorDocument 500 "<script>alert('500: Internal Server Error (Hacking Not Allowed)');location.href='/';</script>"
31  ErrorDocument 501 "<script>alert('501: Not Implemented (Hacking Not Allowed)');location.href='/';</script>"
32  ErrorDocument 502 "<script>alert('502: Bad Gateway (Hacking Not Allowed)');location.href='/';</script>"
33  ErrorDocument 503 "<script>alert('503: Service Unavailable (Hacking Not Allowed)');location.href='/';</script>"
34  ErrorDocument 504 "<script>alert('504: Gateway Timeout (Hacking Not Allowed)');location.href='/';</script>"
35  ErrorDocument 505 "<script>alert('505: HTTP Version Not Supported (Hacking Not Allowed)');location.href='/';</script>"
36  ErrorDocument 404 "<script>alert('404: Server Not Found (Hacking Not Allowed)');location.href='/';</script>"
37  ErrorDocument 403 "<script>alert('403: Forbidden (Hacking Not Allowed)');location.href='/';</script>"
38  ErrorDocument 402 "<script>alert('402: Payment Required Error (Hacking Not Allowed)');location.href='/';</script>"
39  ErrorDocument 401 "<script>alert('401: Server Nauthorized (Hacking Not Allowed)');location.href='/';</script>"
40  ErrorDocument 400 "<script>alert('400: Bad Request (Hacking Not Allowed)');location.href='/';</script>"
```

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:/xampp/htdocs/jurnal_ojs/cache">
96      Header set X-Robots-Tag "noindex, nofollow, noarchive"
97  </Directory>
```

Gambar 5.1.18 Konfigurasi http *Header* pengganti *robot*.txt

o. Menambahkan *redirect* dari IP *address* ke *domain* jurnal.um-palembang.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*plugin*s\gateways\resolver\Resolver*Plugin*.inc.php" dan *file* "C:\xampp\htdocs\jurnal_ojs*plugin*s\gateways\metsGateway\MetsGateway*Plugin*.inc.php" seperti terlihat pada gambar 5.1.21

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

Gambar 5.1.20 *Patch script* Resolver*Plugin*.inc.php

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

Gambar 5.1.21 *Patch script* MetsGateway*Plugin*.inc.php

q. Memperbaiki *form* pencarian jurnal yang *error* pada *file* "C:\xampp\htdocs\jurnal_ojs*plugin*s\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      {url|assign:"searchFormUrl" page="search" op="search" escape=false}
16
        {$searchFormUrl|parse_url:$smarty.const.PHP_URL_QUERY|parse_str:$formU
        rlParameters}
17      <form id="simplesearchForm" action="{$searchFormUrl|strtok:"?
        "|escape}" method="post">
```

Gambar 5.1.22 *Patch script* Block.tpl

```
23      {url|assign:"searchFormUrl" op="search" escape=false}
24
        {$searchFormUrl|parse_url:$smarty.const.PHP_URL_QUERY|parse_str:$form
        UrlParameters}
25      <form id="searchForm" action="{$searchFormUrl|strtok:"?"|escape}"
        method="post">
```

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

```
44              <tr valign="top">
45                  <td class="label">{fieldLabel name="password"
                    required="true" key="user.password"}</td>
46                  <td class="value">
47                      <input type="password" name="password" id=
                        "password" value="{$password|escape}" size="20"
                        maxlength="90" class="textField" autocomplete="off"
                        />
48                  </td>
49              </tr>
```

Gambar 5.1.24 *Patch script* dataverseAuth*Form*.tpl

2. C:\xampp\htdocs\jurnal_ojs*plugins*\generic\lucene\templates*settingsF orm*.tpl

```
40      <tr valign="top">
41          <td class="label">{fieldLabel name="password" required="true"
            key="plugins.generic.lucene.settings.password"}</td>
42          <td class="value"><input type="password" name="password" id=
            "password" value="{$password|escape}" size="15" maxlength="25"
            class="textField" autocomplete="off" />
43              <br />
44              <span class="instruct">{translate
                key="plugins.generic.lucene.settings.passwordInstructions"}
                </span>
45          </td>
46      </tr>
```

Gambar 5.1.25 *Patch script settingsForm*.tpl

3. C:\xampp\htdocs\jurnal_ojs*plugins*\im*portexport**cross*ref\templates*settings*.tpl

```
79          <tr valign="top">
80              <td width="20%" class="label">{fieldLabel
                name="password"
                key="plugins.importexport.common.settings.form.password"
                }</td>
81              <td width="80%" class="value">
82                  <input type="password" name="password" value=
                    "{$password|escape}" size="20" maxlength="50" id=
                    "password" class="textField" autocomplete="off" />
83                  <br />{translate
                    key="plugins.importexport.common.settings.form.passw
                    ord.description"}
84              </td>
85          </tr>
```

Gambar 5.1.26 *Patch script settings*.tpl *plugin* im*portexport* *cross*ref

4. C:\xampp\htdocs\jurnal_ojs*plugins*\im*portexport*\datacite\templates*settings*.tpl

```
38          <tr valign="top">
39              <td width="20%" class="label">{fieldLabel
                name="password"
                key="plugins.importexport.common.settings.form.password"
                }</td>
40              <td width="80%" class="value">
41                  <input type="password" name="password" value=
                    "{$password|escape}" size="20" maxlength="50" id=
                    "password" class="textField" autocomplete="off" />
42              </td>
43          </tr>
```

Gambar 5.1.27 *Patch script settings*.tpl *plugin* im*portexport* datacite

5. C:\xampp\htdocs\jurnal_ojs*plugins*\im*portexport*\medra\templates*settings*.tpl

```
88          <tr valign="top">
89              <td width="20%" class="label">{fieldLabel
                name="password"
                key="plugins.importexport.common.settings.form.password"
                }</td>
90              <td width="80%" class="value">
91                  <input type="password" name="password" value=
                    "{$password|escape}" size="20" maxlength="50" id=
                    "password" class="textField" autocomplete="off"/>
92              </td>
93          </tr>
```

Gambar 5.1.28 *Patch script script settings*.tpl *plugin* im*portexport* medra

6. C:\xampp\htdocs\jurnal_ojs\templates\manager\people\usr*ProfileForm*.tpl

```
158     {if !$implicitAuth || $implicitAuth ===
        $smarty.const.IMPLICIT_AUTH_OPTIONAL}
159         <tr valign="top">
160             <td class="label">{fieldLabel name="password"
                required=$passwordRequired key="user.password"}</td>
161             <td class="value">
162                 <input type="password" name="password" id="password"
                    value="{$password|escape}" size="20" class="textField"
                    autocomplete="off"/>
163                 <br />
164                 <span class="instruct">{translate
                    key="user.register.passwordLengthRestriction"
                    length=$minPasswordLength}</span>
165             </td>
166         </tr>
167         <tr valign="top">
168             <td class="label">{fieldLabel name="password2"
                required=$passwordRequired key="user.repeatPassword"}</td>
169             <td class="value"><input type="password" name="password2"
                id="password2" value="{$password2|escape}" size="20" class=
                "textField" autocomplete="off" /></td>
170         </tr>
```

Gambar 5.1.29 *Patch script* usr*ProfileForm*.tpl

7. C:\xampp\htdocs\jurnal_ojs\templates*user*\change*Password*.tpl

```
27  <table class="data" width="100%">
28  <tr valign="top">
29      <td width="20%" class="label">{fieldLabel name="oldPassword"
        key="user.profile.oldPassword"}</td>
30      <td width="80%" class="value"><input type="password" name=
        "oldPassword" id="oldPassword" value="{$oldPassword|escape}" size=
        "20" class="textField" /></td>
31  </tr>
32  <tr valign="top">
33      <td class="label">{fieldLabel name="password"
        key="user.profile.newPassword"}</td>
34      <td class="value"><input type="password" name="password" value=
        "{$password|escape}" id="password" size="20" class="textField"
        autocomplete="off"/></td>
35  </tr>
36  <tr valign="top">
37      <td></td>
38      <td><span class="instruct">{translate
        key="user.register.passwordLengthRestriction"
        length=$minPasswordLength}</span></td>
39  </tr>
40  <tr valign="top">
41      <td class="label">{fieldLabel name="password2"
        key="user.profile.repeatNewPassword"}</td>
42      <td class="value"><input type="password" name="password2" id=
        "password2" value="{$password2|escape}" size="20" class="textField"
         autocomplete="off"/></td>
43  </tr>
```

Gambar 5.1.30 *Patch script* change*Password*.tpl

8. C:\xampp\htdocs\jurnal_ojs\templates*user**register*.tpl

```
77      <tr valign="top">
78          <td class="label">{fieldLabel name="password" required="true"
            key="user.password"}</td>
79          <td class="value"><input type="password" name="password" value=
            "{$password|escape}" id="password" size="20" class="textField"
            autocomplete="off" /></td>
80      </tr>
81
82      {if !$existingUser}
83          <tr valign="top">
84              <td></td>
85              <td class="instruct">{translate
                key="user.register.passwordLengthRestriction"
                length=$minPasswordLength}</td>
86          </tr>
87          <tr valign="top">
88              <td class="label">{fieldLabel name="password2"
                required="true" key="user.repeatPassword"}</td>
89              <td class="value"><input type="password" name="password2"
                id="password2" value="{$password2|escape}" size="20" class=
                "textField" autocomplete="off"/></td>
90          </tr>
```

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.

1. C:\xampp\htdocs\jurnal_ojs\lib\pkp\templates\common*Header*.tpl

```
34      <!-- Base Jquery -->
35      {if $allowCDN}<script type="text/javascript" src="
        https://www.google.com/jsapi"></script>
36          <script type="text/javascript">{literal}
37              <!--
38              // Provide a local fallback if the CDN cannot be reached
39              if (typeof google == 'undefined') {
```

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}<script type="text/javascript" src="
        https://www.google.com/jsapi"></script>
32      <script type="text/javascript">{literal}
33          <!--
34          // Provide a local fallback if the CDN cannot be reached
```

Gambar 5.1.33 *Patch script* help *Header*.tpl

3. C:\xampp\htdocs\jurnal_ojs*plugins*\generic\googleAnalytics\pa*get*agUrchin.tpl

```
11  <!-- Google Analytics -->
12  <script src="https://www.google-analytics.com/urchin.js" type=
    "text/javascript">
13  </script>
```

Gambar 5.1.34 *Patch script* pa*get*agUrchin.tpl

4. C:\xampp\htdocs\jurnal_ojs*plugins*\generic\googleAnalytics\pa*get*agAnalytics.tpl bisa dilihat pada gambar 5.1.34

```
17  })(window,document,'script','
    https://www.google-analytics.com/analytics.js','ga');
18
```

Gambar 5.1.35 *Patch script* pa*get*agAnalytics.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 Jquery -->
32      {if $allowCDN}<script type="text/javascript" src="
        https://www.google.com/jsapi"></script>
```

Gambar 5.1.37 *Patch script* rt *Header*.tpl

7. C:\xampp\htdocs\jurnal_ojs\templates\Submission\comment\Header.tpl

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

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*.

```
393  [captcha]
394
395  ; Whether or not to enable Captcha features
396  captcha = on
397
398  ; Whether or not to use Captcha on user registration
399  captcha_on_register = on
400
401  ; Whether or not to use Captcha on user comments
402  captcha_on_comments = on
403
404  ; Whether or not to use Captcha on notification mailing list registration
405  captcha_on_mailinglist = on
406
407  ; Font location for font to use in Captcha images
408  font_location = /usr/share/fonts/truetype/freefont/FreeSerif.ttf
409
410  ; Whether to use reCaptcha instead of default Captcha
411  recaptcha = on
412
413  ; Public key for reCaptcha (see http://www.google.com/recaptcha)
414  recaptcha_public_key = 6Ld7kD8UAAAAAE6kxbx-67mCMyJkjdGbFNsVXVx2
415
416  ; Private key for reCaptcha (see http://www.google.com/recaptcha)
417  recaptcha_private_key = 6Ld7kD8UAAAAACB9tzs3zVpOGKk_LVRGIdRmL2c9
```

Gambar 5.1.39 Pemasangan *captcha* pada config.inc.php

Input google *recaptcha* v1 yang berhasil penulis tambahkan terlihat pada gambar 5.1.40

Gambar 5.1.40 Tampilan *input captcha* pada *form Login*

u. Pemasangan Modsecurity

1. penulis mengunduh *modules* modsecurity*2* di http://www.apachelounge.com/download/

2. memasukan library libcurl.dll dan yajl.dll pada *directory* "C:/xampp/apache/bin"
3. setelah itu penulis memasukkan *module* mod_security2.so pada *directory* "C:/xampp/apache/*module*s"
4. lalu penulis mengganti nama *file* modsecurity.conf.example menjadi modsecurity.conf dan memasukan modsecurity.conf pada *directory* "C:/xampp/apache/conf"
5. 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 *module*s/mod_security2/mod_security2.so"
   b. *Enable* "LoadModule unique_id_*module* *module*s/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
566
```

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.

```
<IfModule security2_module>
# merubah SecRuleEngine dari DetectionOnly menjadi On
SecRuleEngine On
# mengubah nama server menjadi IT-UMP
SecServerSignature IT-UMP
# Mengatur Response ketika terdeteksi melakukan penyerangan, response
berupa error 403
SecDefaultAction "deny,phase:2,status:403"

SecRequestBodyAccess On
# Rule Untuk Anti LFI Standard
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

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

Gambar 5.1.44 *Disable rule* SecUnicodeMap*File*

9. Mengganti lokasi SecTmpdir dan SecDataDir seperti gambar 5.1.45

```
# -- Filesystem configuration --------------------------------------------------

# The location where ModSecurity stores temporary files (for example, when
# it needs to handle a file upload that is larger than the configured limit).
#
# This default setting is chosen due to all systems have /tmp available however,
# this is less than ideal. It is recommended that you specify a location that's private.
#
SecTmpDir "C:/xampp/tmp/"

# The location where ModSecurity will keep its persistent data.  This default setting
# is chosen due to all systems have /tmp available however, it
# too should be updated to a place that other users can't access.
#
SecDataDir "C:/xampp/tmp/"

```

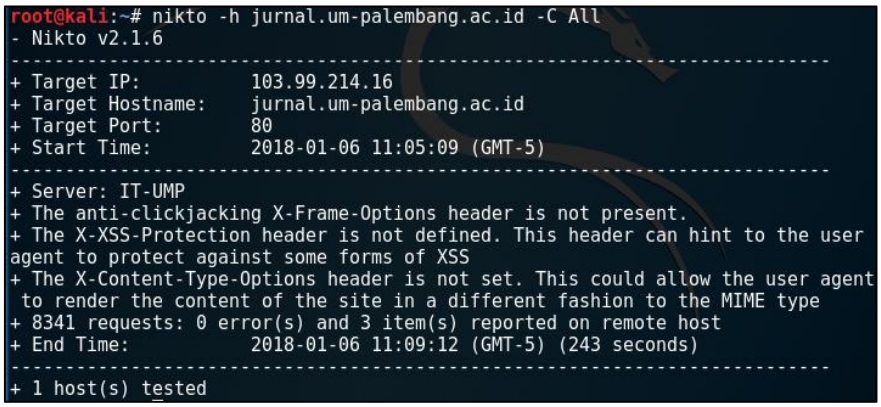
Gambar 5.1.45 perubahan lokasi *directory* pada *file* modsecurity.conf 1

10. Mengganti lokasi SecAuditLog ke tmp pada xampp seperti telihat pada gambar 5.1.46.

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

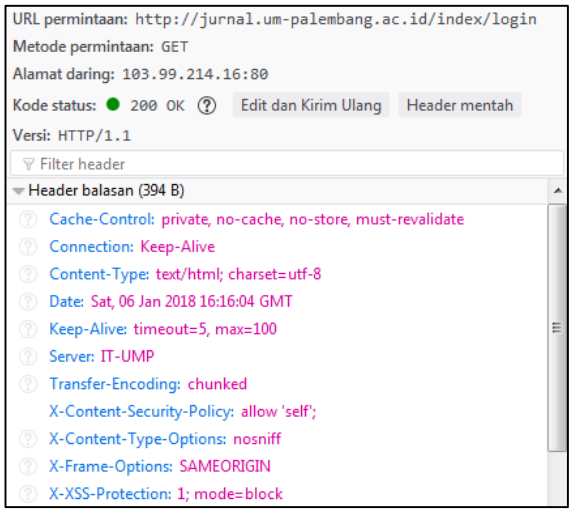
Gambar 5.1.46 perubahan lokasi *directory* pada *file* modsecurity.conf 2

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.



Gambar 5.1.47 Hasil *Scan* Nikto Setelah **Optimalisasi**

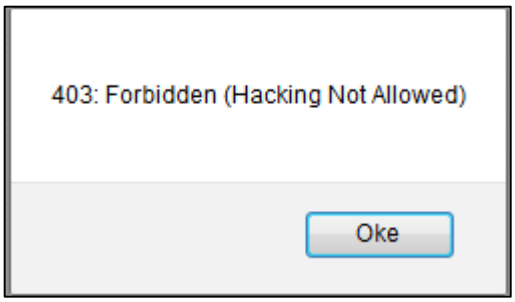
Seperti terlihat pada gambar 52.48 *HTTP Header* pada *browser* mozilla yang penulis gunakan terlihat bahwa *server* sudah memasang *HTTP Header* seperti *X-Frame-Options*, *X-XSS-Protection* dan *X-Content-Type-Options*, serta konfigurasi lainya seperti *cache control* yang telah penulis konfigurasikan 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.um-palembang.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 :

1. 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.um-palembang.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 cara-cara 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.