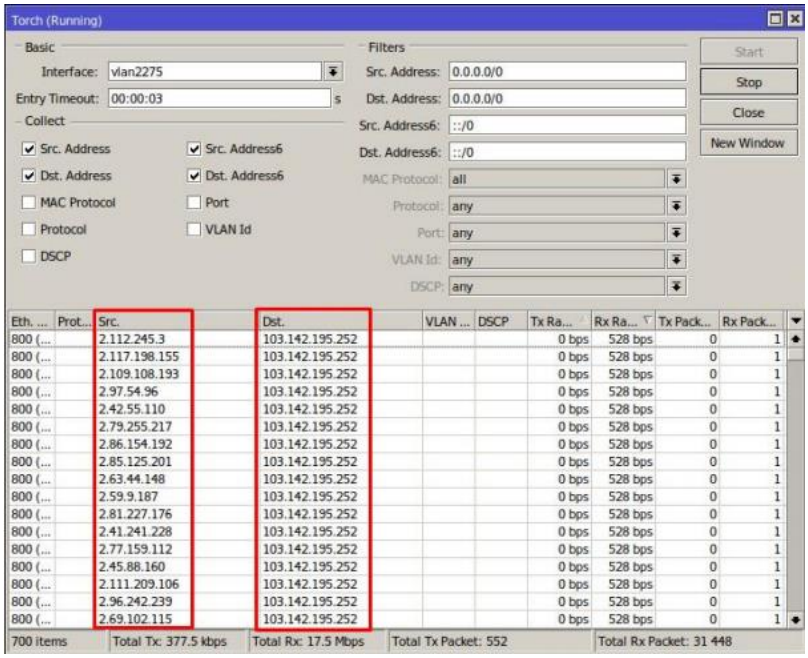
BAB IV
HASIL DAN PEMBAHASAN

4.1 Evaluasi Keamanan Layanan Teknologi Informasi

Evaluasi keamanan layanan teknologi informasi dilakukan dengan menganalisis kerentanan yang terdapat pada keamanan layanan teknologi informasi Untirta. Evaluasi keamanan dilakukan dengan forensik jaringan menggunakan *log* jaringan yang didapatkan saat serangan terjadi, serta dilakukan *vulnerability assessment* pada beberapa layanan teknologi informasi Untirta.

4.1.1 Analisis Forensik Jaringan

Pada forensik jaringan, dilakukan analisis mendalam terhadap *log* jaringan pada saat terkena serangan. Pada *log* jaringan, terdapat beberapa informasi yang didapatkan. Salah satu informasi tersebut diantaranya adalah IP *address*. Dari IP *address* tersebut, dapat diketahui lokasi penyerang. *Server* UPT Data dan Informasi sempat mendapatkan serangan DDoS pada tanggal 12 Agustus 2022. Data *log* jaringan didapatkan dari pihak ketiga yang bekerja sama dengan UPT Data dan Informasi Untirta. *Log* jaringan saat serangan DDoS terjadi dijelaskan pada Gambar 4.1.



Gambar 4.1 *Log* Jaringan Saat Serangan DDoS

Pada Gambar 4.1, *log* jaringan didapatkan dari aplikasi Winbox Router OS pada menu Torch. Dari data *log* tersebut didapatkan informasi bahwa IP *Address Server* UPT Data dan Informasi Untirta adalah 103.142.195.252, sementara itu IP *Address* penyerang bervariasi. Berikut adalah daftar IP *Address* yang menyerang *server* UPT Data dan Informasi Untirta yang diuraikan pada Tabel 4.1.

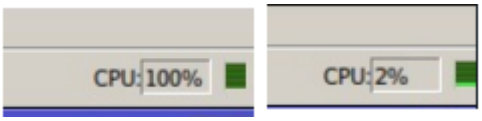
Tabel 4.1 IP *Address* Penyerang

IP Address	**Lokasi**
2.112.245.3	Italia
2.117.198.155	Italia
2.109.108.193	Denmark
2.97.54.96	Britania Raya
2.42.55.110	Italia
2.79.255.217	Kazakhstan
2.86.154.192	Yunani
2.85.125.201	Yunani
2.63.44.148	Rusia

IP Address	**Lokasi**
2.59.9.187	Rumania
2.81.227.176	Portugal
2.41.241.228	Italia
2.77.159.112	Kazakhstan
2.45.88.160	Italia
2.111.209.106	Denmark
2.96.242.239	Britania Raya
2.69.102.115	Swedia

Dari Tabel 4.1, dapat dilihat bahwa lokasi IP *Address* bervariasi. Informasi lokasi IP *Address* penyerang didapatkan melalui pencarian melalui *website* www.whatismyip.com/ip-address-lookup/. Semua IP *Address* penyerang berlokasi di benua Eropa dan sebagian besar serangan berasal dari IP *Address* yang berlokasi di Italia. Hal ini merupakan salah satu karakteristik serangan DDoS dimana serangan dilakukan menggunakan *botnet* sehingga IP Address penyerang bervariasi. Semua oktet awal pada IP *Address* penyerang merupakan angka 2.

Selain itu, terdapat kondisi beban CPU pada saat serangan dan sesudah serangan terjadi yang terdapat pada Gambar 4.2.



(a) (b)

Gambar 4.2 Kondisi Beban CPU, (a) Saat Serangan, (b) Sesudah

Pada Gambar 4.2 (a) didapatkan bahwa beban CPU pada saat serangan adalah 100%. Hal tersebut berdampak pada terputusnya koneksi internet ke seluruh layanan dan *server* milik UPT Data dan Informasi Untirta. UPT Data dan Informasi Untirta melalui pihak ketiga melakukan aksi sementara untuk mengurangi dampak dari serangan yang ditimbulkan. Aksi yang dilakukan adalah melakukan *blackhole* IP *Address server* Untirta ke arah internet internasional. Hasil dari aksi yang telah dilakukan adalah beban CPU kembali normal seperti pada Gambar 4.2 (b). Namun, dampak dari aksi sementara tersebut adalah *server* Untirta tidak dapat diakses oleh beberapa *provider* internet dikarenakan *blackhole* yang telah dilakukan.

4.1.2 Analisis *Vulnerability Assessment*

Pada *vulnerability assessment*, dilakukan uji kerentanan pada beberapa layanan teknologi informasi Untirta. *Vulnerability assessment* dilakukan dalam dua tahapan, yaitu *network scanning*, dan *vulnerability scanning*. Layanan teknologi informasi yang akan dilakukan penetration test adalah SIAKAD Untirta, SPADA Untirta, Website Untirta, dan eAdministrasi Untirta.

1. *Network Scanning*

Tahap awal pada *vulnerability assessment* adalah *network scanning*. Hal ini dilakukan untuk mengetahui beberapa informasi terkait dengan layanan teknologi informasi diantaranya adalah IP *address server* layanan, *port* yang terbuka, serta memperkirakan sistem operasi yang digunakan oleh *server* layanan. *Tool* yang digunakan pada *network scanning* adalah nmap. Berikut adalah salah satu contoh *network scanning* menggunakan nmap yang terdapat pada Gambar 4.3.

```
┌──(root㉿DESKTOP-EP29EPG)-[/home/dell]
└─# nmap siakad.untirta.ac.id
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-15 12:30 +07
Nmap scan report for siakad.untirta.ac.id (103.142.195.98)
Host is up (0.013s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3306/tcp open     mysql
5678/tcp filtered rrac

Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
```

Gambar 4.3 Hasil *Network Scanning* Menggunakan nmap

Pada Gambar 4.3 merupakan hasil *network scanning* pada layanan SIAKAD Untirta menggunakan aplikasi nmap. Pada hasil scan tersebut, didapatkan beberapa informasi terkait layanan SIAKAD Untirta. Informasi tersebut diantaranya adalah IP *Address* layanan yaitu 103.142.195.98. Selanjutnya, didapatkan informasi beberapa *port* layanan yang terbuka. Salah satu contohnya adalah layanan Mysql yang terdapat pada port 3306 dengan protokol TCP. Layanan Mysql sering digunakan untuk manajemen *database*.

Pada Lampiran B.1 sampai Lampiran B.4 merupakan hasil *network scanning* seluruh layanan yang diuji. Dari hasil-hasil tersebut, didapatkan rekap keseluruhan pada Tabel 4.2.

Tabel 4.2 Hasil *Network Scanning*

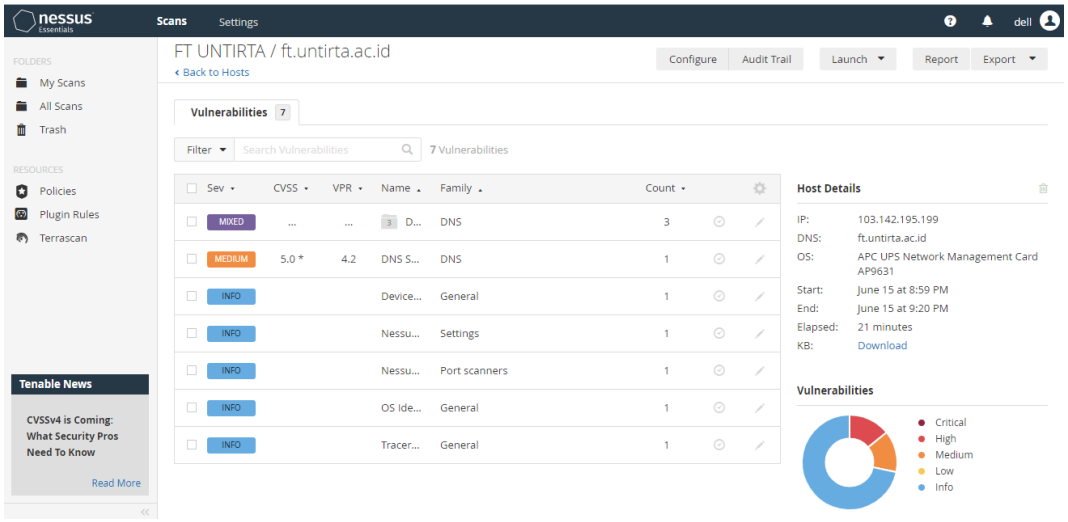
Layanan	**IP *Host***	**Sistem Operasi**	**Jumlah *Port* Terdeteksi**
SIAKAD Untirta (siakad.untirta.ac.id)	103.142.195.98	OpenBSD 4.0 (86%)	8
SPADA Untirta (spada.untirta.ac.id)	103.142.195.106	OpenBSD 4.0 (86%)	12
eAdministrasi Untirta (eadministrasi.untirta.ac.id)	103.142.195.194	OpenBSD 4.0 (86%)	6
Website Untirta dan FT Untirta (untirta.ac.id dan ft.untirta.ac.id)	103.142.195.199	FreeBSD 6.2-RELEASE (87%)	14

Pada Tabel 4.2, didapatkan bahwa layanan Untirta memiliki IP *Host* yang sama dan berbeda tergantung pada layanan, serta *port* yang terdeteksi pada tiap layanan jumlahnya berbeda-beda. Pada layanan web Untirta dan FT Untirta memiliki IP *Host* yang sama serta memiliki jumlah *port* terdeteksi paling banyak di antara layanan yang lainnya.

2. *Vulnerability Scanning*

Pada *vulnerability scanning*, dilakukan pemindaian kerentanan yang terdapat pada layanan teknologi informasi Untirta. *Vulnerability scanning* dilakukan menggunakan *tools* Nessus. *Tools* tersebut dapat memberikan *report*

pada hasil pemindaian yang telah dilakukan. Berikut adalah contoh hasil pemindaian menggunakan Nessus yang terdapat pada Gambar 4.4.



Gambar 4.4 Hasil *Vulnerability Scanning* Menggunakan Nessus

Pada Gambar 4.4, hasil *vulnerability assessment* pada layanan web FT Untirta yang didapatkan pada aplikasi Nessus. Aplikasi Nessus memberikan *report* kerentanan yang ada pada layanan berdasarkan tingkat *risk* serta terdapat nilai kerentanan berdasarkan *Common Vulnerability Scoring System* (CVSS). Selain itu, terdapat informasi IP *Address*, DNS, sistem operasi, serta grafik kerentanan yang terdapat pada layanan. Berikut adalah contoh dari hasil *vulnerability scanning* pada Gambar 4.4 yang dijelaskan pada Tabel 4.3.

Tabel 4.3 Hasil *Vulnerability Scanning*

Domain Name	ft.untirta.ac.id	
IP *Host*	103.142.195.199	
Sistem Operasi	APC UPS *Network Management Card*	
Tingkat Kerentanan	**Celah Keamanan**	**Skor**
HIGH	DNS *Server Spoofed Request Amplification* DDoS	7,5
MEDIUM	DNS *Server Recursive Query Cache Poisoning Weakness*	5,0

Pada Tabel 4.3 merupakan hasil *vulnerability scanning* pada layanan *website* FT Untirta. Hasil tersebut didapatkan bahwa terdapat dua kerentanan pada *website* FT Untirta yaitu DNS *server spoofed request amplification DDoS* dengan tingkat

kerentanan *High* dan DNS *server recursive query cache poisoning weakness* dengan tingkat kerentanan *Medium*.

DNS *server spoofed request amplification DDoS* merupakan kerentanan ketika *server* DNS jarak jauh menjawab permintaan apa pun, memungkinkan untuk meminta *name server* (NS) dari *root zone* ('.') dan mendapatkan jawaban yang lebih besar dari permintaan awal. *Spoofing* alamat IP sumber menyebabkan penyerang jarak jauh dapat memanfaatkan 'amplifikasi' ini untuk meluncurkan serangan *Denial of Service* (DoS) terhadap *host* pihak ketiga menggunakan *server* DNS jarak jauh. Solusi untuk kerentanan ini adalah dengan membatasi akses ke *server* DNS dari jaringan publik atau konfigurasi ulang *server* DNS untuk menolak permintaan tersebut.

Sementara itu, DNS *server recursive query cache poisoning weakness* merupakan kerentanan ini memungkinkan penyerang untuk melakukan serangan *cache poisoning* terhadap NS. Solusi untuk kerentanan ini adalah dengan membatasi *recursive queries* ke host yang harus menggunakan NS.

Pada Lampiran C.1 sampai Lampiran C.4 merupakan hasil *vulnerability scanning* seluruh layanan yang diuji. Dari hasil-hasil tersebut, didapatkan rekap jumlah *vulnerability* pada Tabel 4.4.

Tabel 4.4 Rekap Jumlah *Vulnerability Scanning*

Layanan	**Tingkat Kerentanan**				**Jumlah**
	Critical	***High***	***Medium***	***Low***	
SIAKAD Untirta (siakad.untirta.ac.id)	9	16	19	6	50
SPADA Untirta (spada.untirta.ac.id)	1	1	6	1	9
eAdministrasi Untirta (eadministrasi.untirta.ac.id)	1	4	5	1	11
Website Untirta (untirta.ac.id)	0	1	2	2	5
Website FT Untirta (ft.untirta.ac.id)	0	1	1	0	2

Pada Tabel 4.4, didapatkan bahwa tiap layanan Untirta memiliki jumlah kerentanan yang berbeda-beda. Layanan yang memiliki jumlah kerentanan paling banyak adalah SIAKAD Untirta. Sementara itu, layanan yang memiliki jumlah

kerentanan paling sedikit adalah *website* FT Untirta. Kerentanan tersebut memiliki dampak yang berbeda-beda terhadap layanan. Keseluruhan kerentanan beserta tingkat kerentanan dijelaskan pada Tabel 4.5

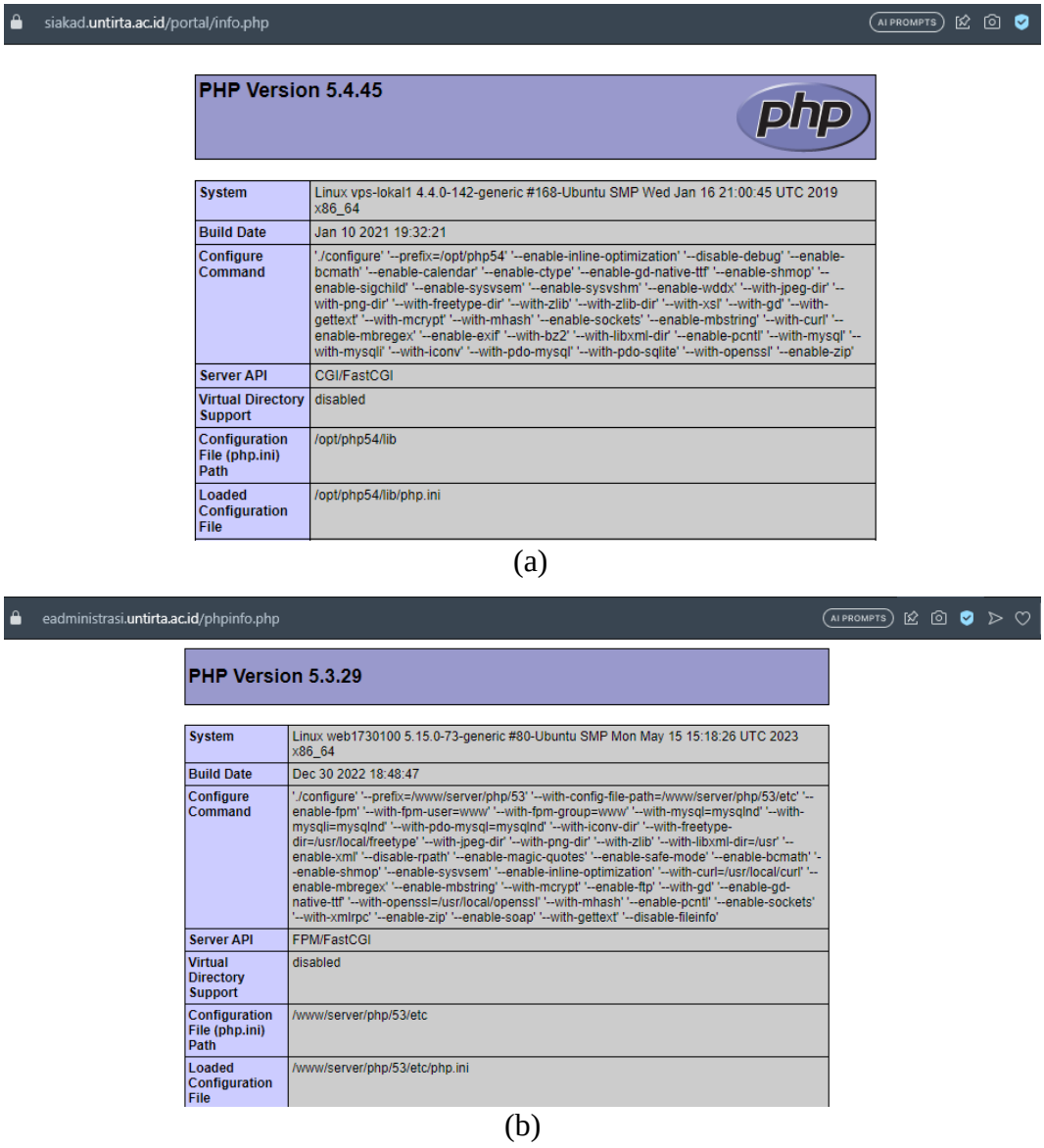
Tabel 4.5 Keseluruhan Kerentanan Layanan Teknologi Informasi Untirta

No.	Kerentanan	Tingkat Kerentanan
1.	PHP *Multiple Vulnerabilities*	*Critical, High, Medium, Low*
2.	SSL/TLS *Version Vulnerabilities*	*Critical, High, Medium*
3.	SNMP *Agent Default Community Name* (*public*)	*High, Medium*
4.	SNMP 'GETBULK' *Reflection* DDoS	
5.	SSH *Weak Algorithms Supported*	*Medium, Low*
6.	SSH *Weak* MAC *Algorithms Enabled*	
7.	SSH *Weak Key Exchange Algorithms Enabled*	
8.	SSH *Server* CBC *Mode Ciphers Enabled*	
9.	DNS *Server Spoofed Request Amplification DDoS*	*High*
10.	ADOdb tmssql.php *do Parameter Arbitrary* PHP *Function Execution*	*HIgh*
11.	CGI *Generic* SQL *Injection* (*blind*)	*High*
12.	nginx < 1.17.7 *Information Disclosure*	*Medium*
13.	Web *Server* info.php / phpinfo.php *Detection*	*Medium*
14.	DNS *Server Recursive Query Cache Poisoning Weakness*	*Medium*
15.	*Web Application Potentially Vulnerable to Clickjacking*	*Medium*
16.	JQuery 1.2 < 3.5.0 *Multiple* XSS	*Medium*
17.	DNS *Server Cache Snooping Remote Information Disclosure*	*Medium*
18.	*Browsable Web Directories*	*Medium*
19.	Git *Repository Served by Web Server*	*Medium*
20.	*Web Server Transmits Cleartext Credentials*	*Low*
21.	*Web Server Allows Password Auto-Completion*	*Low*

Pada Tabel 4.5, merupakan keseluruhan *vulnerability* yang ada pada layanan teknologi informasi Untirta. Terdapat sekitar 21 kerentanan yang terdeteksi pada keseluruhan layanan UPT Data dan Informasi Untirta, dengan tingkat kerentanan paling tinggi adalah PHP dan SSL/TLS. Berikut penjelasan beberapa kerentanan yang ada pada layanan UPT Data dan Informasi Untirta.

a. PHP *multiple vulnerabilities*

Kerentanan ini disebabkan oleh versi PHP yang sudah kadaluwarsa atau sudah tidak didukung. Versi yang sudah tidak didukung ini memiliki banyak kerentanan, beberapa diantaranya adalah dapat menyebabkan DoS, *buffer overflow*, dan kebocoran informasi. Kerentanan tersebut dapat dilihat pada Gambar 4.5.



Gambar 4.5 Versi PHP Layanan Untirta (a) SIAKAD (b) e-Administrasi

Pada Gambar 4.5 merupakan infomasi PHP yang digunakan SIAKAD Untirta dengan mengakses *file* info.php pada https://siakad.untirta.ac.id/portal dan https://eadministrasi.untirta.ac.id. Berdasarkan *file* tersebut, didapatkan pada Gambar 4.5 (a) bahwa PHP yang digunakan SIAKAD Untirta adalah PHP versi

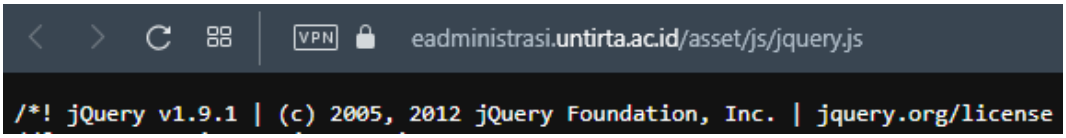
5.4.45, sedangkan pada Gambar 4.5 (b) PHP yang digunakan e-Administrasi Untirta adalah PHP versi 5.3.29 dimana dua versi tersebut merupakan versi PHP yang cukup lawas. Sementara itu, PHP terbaru yang telah dirilis saat ini adalah versi 8.2.7. Untuk menghindari kerentanan tersebut, perlu dilakukan *upgrade* PHP ke versi terbaru.

b. SSL/TLS *version vulnerabilities*

Protokol keamanan juga menjadi masalah pada layanan teknologi informasi Untirta. Hal tersebut dikarenakan beberapa layanan Untirta terdeteksi masih menggunakan protokol *Secure Socket Layer* (SSL) yang merupakan protokol keamanan yang cukup lawas. Protokol SSL sendiri memiliki beberapa kelemahan kriptografi. Disarankan menggunakan protokol *Transport Layer Security* (TLS) yang memiliki tingkat keamanan lebih tinggi dari SSL untuk menghindari kerentanan tersebut.

c. Jquery 1.2 < 3.5.0 *multiple* XSS

Jquery merupakan pustaka JavaScript yang digunakan untuk menyederhanakan *client-side scripting* pada HTML. Jquery yang digunakan oleh e-Administrasi Untirta dapat dilihat pada Gambar 4.6.

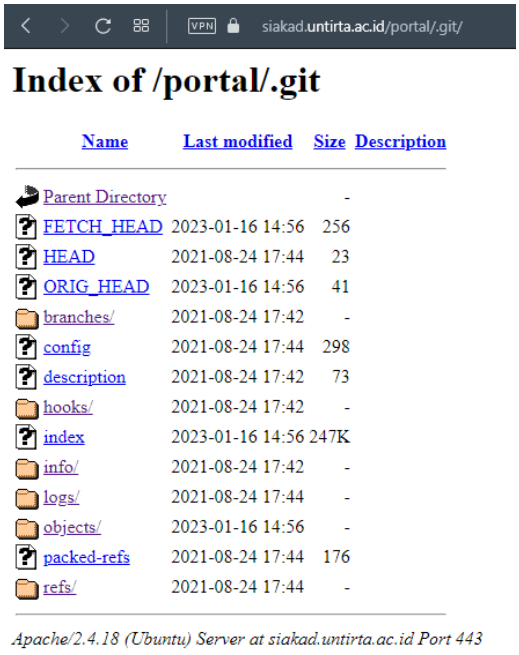


Gambar 4.6 Jquery e-Administrasi Untirta

Pada Gambar 4.6 didapatkan versi Jquery yang digunakan pada layanan e-Administrasi Untirta yaitu versi 1.9.1. Hal tersebut dapat diketahui dengan mengakses file jquery.js pada asset https://eadministrasi.untirta.ac.id. Jquery versi terbaru yang dirilis adalah versi 3.7.0. Versi dibawah 3.5.0 memiliki kerentanan *Cross-Site Scripting* (XSS). XSS sendiri merupakan kerentanan yang dapat dieksploitasi dengan menginjeksi kode berbahaya pada skrip. Diperlukan *update* Jquery minimal ke versi 3.5.0 untuk menghindari hal tersebut.

d. *Information disclosure*

Pada sebuah *website* terdapat beberapa informasi di dalamnya. Informasi terbuka pada sebuah *website* dapat menjadi sebuah bahaya jika informasi tersebut bersifat sensitif. Contohnya adalah *backup file* SQL, foto *user*, atau *file* penting lainnya. *Information disclosure* pada layanan Untirta dapat dilihat pada Gambar 4.7.



(a)

(b)

Gambar 4.7 *Information Disclosure* (a)Web *Directories* (b)Git *Repository*

Pada Gambar 4.7 merupakan informasi terbuka pada SIAKAD Untirta yang dapat diakses pada laman https://siakad.untirta.ac.id. Gambar 4.7 (a) merupakan *git repository* web SIAKAD website SIAKAD Untirta. Sementara itu, pada Gambar 4.7 (b) merupakan direktori website SIAKAD Untirta. Dua hal tersebut berisi *file* yang digunakan, dijelajah, dan diakses pada website SIAKAD Untirta. Sebaiknya

file yang dapat dijelajah tersebut tidak mengandung informasi yang bersifat sensitif. Jika diperlukan, batasi akses atau menonaktifkan indeks direktori website.

e. DNS *spoofing* dan *poisoning*

DNS *spoofing* dan *poisoning* juga merupakan celah kerentanan yang terdapat pada layanan teknologi informasi Untirta. Hal ini dapat menyebabkan pengguna dialihkan ke alamat palsu. Kerentanan tersebut perlu diperbaiki oleh UPT Data dan Informasi supaya layanan teknologi informasi Untirta dapat diakses pengguna dengan aman.

4.2 Evaluasi Manajemen Layanan Teknologi Informasi

Evaluasi manajemen layanan teknologi informasi dilakukan untuk mengetahui sejauh mana manajemen layanan teknologi informasi Untirta. Evaluasi manajemen dilakukan dengan menyebar kuesioner pada beberapa staff UPT Data dan Informasi Untirta yang menangani layanan teknologi informasi Untirta.

Kuesioner yang digunakan adalah kuesioner UCISA ITIL v3 Service Operation Readiness berjumlah 81 pertanyaan yang dibagi menjadi dua sub-domain. Pertanyaan untuk sub-domain *service operation process* berjumlah 53 pertanyaan, sedangkan untuk sub-domain *common service operation activities* berjumlah 28 pertanyaan.

Perhitungan kuesioner menggunakan perhitungan *maturity* model serta *gap analysis*. Dari hasil perhitungan tersebut, didapatkan analisis *maturity* model serta *gap analysis* pada tiap sub-domain pada service operation UPT Data dan Informasi Untirta.

4.2.1 Analisis *Service Operation Process*

Pada sub-domain *service operation process* dilakukan evaluasi manajemen layanan teknologi informasi pada tiap proses yang ada dalam domain *service operation*. *Service operation* memiliki 5 proses utama, yaitu *event management*, *incident management*, *request fullfilment*, *problem management*, dan *access management*. Hasil kuesioner *service operation process* dapat dilihat pada Tabel 4.6.

Tabel 4.6 Hasil Kuesioner *Service Operation Process*

Service Operation Process									
No	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-1	3	4	4	5	16	4	4	1
2	SOP-2	3	4	5	5	17	4	4,25	0,75
3	SOP-3	3	4	3	5	15	4	3,75	1,25
4	SOP-4	3	4	4	5	16	4	4	1
5	SOP-5	3	4	5	4	16	4	4	1
6	SOP-6	3	3	3	4	13	4	3,25	1,75
7	SOP-7	3	4	2	5	14	4	3,5	1,5
8	SOP-8	3	4	5	4	16	4	4	1
Skor		24	31	31	37	123	32	3,84	1,16

Tabel 4.6 merupakan hasil kuesioner bagian awal pada *service operation process*. Bagian awal berisi pernyataan yang diajukan untuk setiap proses secara keseluruhan. Dari hasil kuesioner didapatkan nilai maturity pada bagian awal *service operation process* adalah 3,84 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-6 dikarenakan memiliki nilai *maturity* paling kecil. SOP-6 menyatakan bahwa UPT Data dan Informasi telah menetapkan Indikator Kinerja Utama (IKU) serta metrik dari setiap proses pada *service operation*. Saran untuk UPT Data dan Informasi Untirta dalam *service operation process* adalah meningkatkan peran, fungsi, kebijakan, serta faktor keberhasilan terutama indikator kinerja utama pada *service operation process* yang dimiliki oleh UPT Data dan Informasi Untirta.

1. *Event management*

Proses *event management* merupakan proses dalam mengelola *event* atau peristiwa sepanjang siklus hidup layanan. Pengelolaan ini mencakup kegiatan untuk mendeteksi dan memahami persitiwa yang terjadi serta menentukan tindakan pengendalian yang tepat. Hasil kuesioner pada proses *event management* dapat dilihat pada Tabel 4.7.

Tabel 4.7 Hasil Kuesioner *Event Management*

***Service Operation Process* (*Event Management*)**									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-9	3	3	4	4	14	4	3,5	1,5
2	SOP-10	3	4	4	3	14	4	3,5	1,5
3	SOP-11	3	3	4	4	14	4	3,5	1,5
4	SOP-12	3	3	5	4	15	4	3,75	1,25
5	SOP-13	3	3	3	4	13	4	3,25	1,75
6	SOP-14	3	3	4	4	14	4	3,5	1,5
7	SOP-15	3	3	5	4	15	4	3,75	1,25
8	SOP-16	3	3	3	4	13	4	3,25	1,75
9	SOP-17	3	4	4	4	15	4	3,75	1,25
Skor		27	29	36	35	127	36	3,53	1,47

Tabel 4.7 merupakan hasil kuesioner bagian *event management* pada *service operation process*. Pada proses *event management* berisi pernyataan terkait penanganan terhadap suatu peristiwa. Dari hasil kuesioner didapatkan nilai *maturity* pada *event management* adalah 3,53 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-16 dikarenakan memiliki nilai maturity paling kecil. SOP-16 menyatakan bahwa UPT Data dan Informasi melakukan tinjauan dari hasil tanggapan yang diberikan pada peristiwa yang terjadi dari layanan teknologi informasinya. Saran untuk UPT Data dan Informasi Untirta dalam *event management* adalah meningkatkan pengelolaan peristiwa terutama dalam peninjauan setiap peristiwa yang ada pada layanan teknologi informasi Untirta.

2. *Incident management*

Proses *incident management* merupakan proses dalam pemulihan layanan dari insiden yang secara tidak terduga terdegradasi atau terganggu. Proses ini mencakup kegiatan identifikasi, dokumentasi, diagnosa, dan pemulihan terhadap suatu insiden yang terjadi pada layanan teknologi informasi. Hasil kuesioner pada proses *incident management* dapat dilihat pada Tabel 4.8.

Tabel 4.8 Hasil Kuesioner *Incident Management*

***Service Operation Process* (*Incident Management*)**									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-18	3	4	4	3	14	4	3,5	1,5
2	SOP-19	3	3	4	5	15	4	3,75	1,25
3	SOP-20	3	4	5	4	16	4	4	1
4	SOP-21	3	3	3	4	13	4	3,25	1,75
5	SOP-22	3	3	3	4	13	4	3,25	1,75
6	SOP-23	3	3	4	4	14	4	3,5	1,5
7	SOP-24	3	4	4	4	15	4	3,75	1,25
8	SOP-25	3	4	3	4	14	4	3,5	1,5
9	SOP-26	3	4	5	4	16	4	4	1
10	SOP-27	3	4	3	4	14	4	3,5	1,5
11	SOP-28	3	4	4	5	16	4	4	1
12	SOP-29	3	4	4	4	15	4	3,75	1,25
Skor		36	44	46	49	175	48	3,65	1,35

Tabel 4.8 merupakan hasil kuesioner bagian *incident management* pada *service operation process*. Pada proses *incident management* berisi pernyataan terkait penanganan serta pemulihan terhadap suatu insiden yang terjadi. Dari hasil kuesioner didapatkan nilai *maturity* pada *incident management* adalah 3,65 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-21 dan SOP-22. SOP-21 menyatakan bahwa UPT Data dan Informasi memiliki aktivititas pengidentifikasian insiden yang terjadi pada layanan teknologi informasi. Sementara itu, SOP-22 menyatakan bahwa UPT Data dan Informasi melakukan *logging* pada setiap insiden yang terjadi pada layanan teknologi informasi. Saran untuk UPT Data dan Informasi Untirta dalam *incident management* adalah meningkatkan penanganan insiden terutama dalam pengidentifiksian insiden serta mendokumentasikan insiden yang terjadi pada layanan teknologi informasi Untirta.

3. *Request fullfilment*

Proses *request fullfilment* merupakan proses dalam pemenuhan permintaan pada layanan. Proses ini mencakup pemenuhan kebutuhan yang diperlukan pada layanan teknologi informasi. Hasil kuesioner pada proses *request fullfilment* dapat dilihat pada Tabel 4.9.

Tabel 4.9 Hasil Kuesioner *Request Fullfilment*

***Service Operation Process* (*Request Fullfilment*)**									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-30	3	3	3	4	13	4	3,25	1,75
2	SOP-31	3	4	3	3	13	4	3,25	1,75
3	SOP-32	3	4	3	3	13	4	3,25	1,75
4	SOP-33	3	4	3	3	13	4	3,25	1,75
5	SOP-34	3	4	4	4	15	4	3,75	1,25
Skor		15	19	16	17	67	20	3,35	1,65

Tabel 4.9 merupakan hasil kuesioner bagian *request fullfilment* pada *service operation process*. Pada proses *request fullfilment* berisi pernyataan terkait permintaan pemenuhan kebutuhan yang diperlukan untuk layanan teknologi informasi. Dari hasil kuesioner didapatkan nilai *maturity* pada *request fullfilment* adalah 3,35 atau *defined*. UPT Data dan Informasi Untirta perlu meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.

4. *Problem management*

Proses *problem management* merupakan proses dalam mencegah masalah yang ada dalam layanan. Proses ini mencakup penyelesaian akar masalah dari suatu insiden serta melakukan pendeteksian dan pencegahan masalah atau insiden di masa depan. Hasil kuesioner pada proses *problem management* dapat dilihat pada Tabel 4.10.

Tabel 4.10 Hasil Kuesioner *Problem Management*

***Service Operation Process* (*Problem Management*)**									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-35	3	3	4	5	15	4	3,75	1,25
2	SOP-36	3	3	3	5	14	4	3,5	1,5
3	SOP-37	3	3	4	4	14	4	3,5	1,5
4	SOP-38	3	4	3	4	14	4	3,5	1,5
5	SOP-39	3	4	4	4	15	4	3,75	1,25
6	SOP-40	3	4	5	3	15	4	3,75	1,25
7	SOP-41	3	3	5	3	14	4	3,5	1,5
8	SOP-42	3	4	4	4	15	4	3,75	1,25
9	SOP-43	3	4	3	4	14	4	3,5	1,5

No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	*Maturity Level*	Gap
		1	2	3	4				
10	SOP-44	3	4	4	4	15	4	3,75	1,25
11	SOP-45	3	3	3	4	13	4	3,25	1,75
12	SOP-46	3	3	5	3	14	4	3,5	1,5
13	SOP-47	3	3	3	4	13	4	3,25	1,75
Skor		39	45	50	51	185	52	3,56	1,44

Tabel 4.10 merupakan hasil kuesioner bagian *problem management* pada *service operation process*. Pada proses *problem management* berisi pernyataan terkait pendeteksian serta pencegahan masalah yang terdapat pada suatu layanan. Dari hasil kuesioner didapatkan nilai maturity pada *problem management* adalah 3,65 atau *defined*. Bagian yang perlu ditingkatkan adalah pernyataan SOP-45 dan SOP-47. SOP-45 menyatakan bahwa UPT Data dan Informasi melakukan pendeteksian kesalahan dalam lingkungan pengembangan. Sementara itu, SOP-47 menyatakan bahwa UPT Data dan Informasi memiliki database kesalahan yang diketahui (*known error database*) untuk memungkinkan diagnosis dan resolusi yang lebih cepat. Saran untuk UPT Data dan Informasi Untirta dalam *problem management* adalah meningkatkan pencegahan masalah yang ada pada layanan terutama pada pendeteksian kesalahan serta membuat *known error database* untuk memudahkan diagnosis serta resolusi pada suatu masalah.

5. *Access management*

Proses *Access Management* merupakan proses dalam pemberian akses terhadap pengguna yang berwenang untuk menggunakan layanan. Proses ini mencakup permintaan, verifikasi, pemantauan, serta penelusuran terhadap akses layanan. Hasil kuesioner pada proses *access management* dapat dilihat pada Tabel 4.11.

Tabel 4.11 Hasil Kuesioner *Access Management*

***Service Operation Process* (*Access Management*)**									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	SOP-48	3	4	3	3	13	4	3,25	1,75
2	SOP-49	3	4	3	4	14	4	3,5	1,5
3	SOP-50	3	4	4	3	14	4	3,5	1,5
4	SOP-51	3	4	4	4	15	4	3,75	1,25
5	SOP-52	3	4	4	5	16	4	4	1
6	SOP-53	3	4	4	3	14	4	3,5	1,5
Skor		18	24	22	22	86	24	3,58	1,42

Tabel 4.11 merupakan hasil kuesioner bagian *access management* pada *service operation process*. Pada proses *access management* berisi pernyataan terkait permintaan, verifikasi, pemantauan, serta penelusuran terhadap akses layanan. Dari hasil kuesioner didapatkan nilai *maturity* pada *problem management* adalah 3,58 atau defined. Bagian yang perlu ditingkatkan adalah pernyataan SOP-48. SOP-48 menyatakan bahwa UPT Data dan Informasi memiliki aktivitas permintaan untuk mengakses layanan. Saran untuk UPT Data dan Informasi Untirta dalam *access management* adalah meningkatkan manajemen dalam pemberian akses terhadap layanan teknologi informasi Untirta. Hasil keseluruhan kuesioner *service operation process* dapat dilihat pada Tabel 4.12.

Tabel 4.12 Rekap Hasil Kuesioner *Service Operation Process*

No.	**Proses**	***Maturity Level***	**Gap**
1	*Service Operation Process in General*	3,84	1,16
2	*Event Management*	3,53	1,47
3	*Incident Management*	3,65	1,35
4	*Request Fullfilment*	3,35	1,65
5	*Problem Management*	3,56	1,44
6	*Access Management*	3,58	1,42
Skor		3,60	1,40

Tabel 4.12 merupakan hasil keseluruhan kuesioner *service operation process*. Dari hasil kuesioner didapatkan nilai *maturity* keseluruhan *service operation process* adalah 3,60 atau *defined* dengan gap 1,40. Nilai *maturity* tersebut menunjukkan bahwa manajemen layanan teknologi informasi UPT Data dan

Informasi Untirta pada domain *service operation* telah terdefinisi serta memiliki prosedur yang jelas. Tahap selanjutnya adalah bagaimana UPT Data dan Informasi meningkatkan nilai *maturity* manajemen layanan teknologi informasi ke level 4 (*Managed*). Bagian yang menjadi perhatian pada *service operation process* adalah proses *request fullfilment*. UPT Data dan Informasi harus meningkatkan bagaimana permintaan untuk pemenuhan kebutuhan dapat terpenuhi untuk pengembangan layanan teknologi informasi.

4.2.2 Analisis *Common Service Operation Activities*

Pada *common service operation activities* dilakukan evaluasi aktivitas umum yang terdapat dalam proses atau fungsi pada domain *service operation*. Aktivitas umum tersebut berdasarkan pada proses dan fungsi yang ada dalam *service operation*. Hasil kuesioner *common service operation activities* dapat dilihat pada Tabel 4.13.

Tabel 4.13 Hasil Kuesioner *Common Service Operation Activities*

Common Service Operation Activities									
No.	**Kode Pernyataan**	**Responden**				**Total Bobot**	**Jumlah Responden**	***Maturity Level***	**Gap**
		1	**2**	**3**	**4**				
1	CSOA-1	3	4	4	2	13	4	3,25	1,75
2	CSOA-2	3	4	3	2	12	4	3	2
3	CSOA-3	3	4	4	4	15	4	3,75	1,25
4	CSOA-4	3	4	3	4	14	4	3,5	1,5
5	CSOA-5	3	4	4	4	15	4	3,75	1,25
6	CSOA-6	3	4	4	3	14	4	3,5	1,5
7	CSOA-7	3	2	4	5	14	4	3,5	1,5
8	CSOA-8	3	4	3	4	14	4	3,5	1,5
9	CSOA-9	3	4	4	4	15	4	3,75	1,25
10	CSOA-10	3	4	4	3	14	4	3,5	1,5
11	CSOA-11	3	4	4	4	15	4	3,75	1,25
12	CSOA-12	3	4	4	3	14	4	3,5	1,5
13	CSOA-13	3	3	3	2	11	4	2,75	2,25
14	CSOA-14	3	3	5	2	13	4	3,25	1,75
15	CSOA-15	3	4	5	4	16	4	4	1
16	CSOA-16	3	4	4	2	13	4	3,25	1,75
17	CSOA-17	3	4	2	5	14	4	3,5	1,5
18	CSOA-18	3	4	4	4	15	4	3,75	1,25
19	CSOA-19	3	4	4	4	15	4	3,75	1,25

No.	Kode Pernyataan	Responden				Total Bobot	Jumlah Responden	*Maturity Level*	Gap
		1	2	3	4				
20	CSOA-20	3	4	4	4	15	4	3,75	1,25
21	CSOA-21	3	4	4	4	15	4	3,75	1,25
22	CSOA-22	3	4	4	4	15	4	3,75	1,25
23	CSOA-23	3	4	4	4	15	4	3,75	1,25
24	CSOA-24	3	4	4	4	15	4	3,75	1,25
25	CSOA-25	3	4	4	4	15	4	3,75	1,25
26	CSOA-26	3	4	4	3	14	4	3,5	1,5
27	CSOA-27	3	4	4	3	14	4	3,5	1,5
28	CSOA-28	3	4	4	4	15	4	3,75	1,25
Skor		84	108	108	99	399	112	3,56	1,44

Tabel 4.13 merupakan hasil keseluruhan kuesioner *common service operation activities*. Dari hasil kuesioner didapatkan level *maturity* keseluruhan *service operation process* berada pada nilai 3,56 atau *defined* dengan *gap* 1,44. Nilai maturity tersebut menunjukkan bahwa manajemen layanan teknologi informasi UPT Data dan Informasi Untirta pada aktivitas umum *service operation* telah terdefinisi serta memiliki prosedur yang jelas. Tahap selanjutnya adalah bagaimana UPT Data dan Informasi meningkatkan nilai *maturity* manajemen layanan teknologi informasi ke level 4 (*Managed*).

Bagian yang perlu menjadi perhatian adalah pernyataan CSOA-2. CSOA-2 menyatakan bahwa UPT Data dan Informasi memastikan bahwa kondisi tertentu dipenuhi atau tidak terpenuhi dan jika tidak, maka akan menaikkan peringatan ke grup yang sesuai. UPT Data dan Informasi Untirta harus meningkatkan manajemen pada aktivitas umum *service operation* dengan melakukan pemantauan dan *service control*, melakukan audit *service operation*, serta mengukur ketersediaan dari perspektif teknologi informasi dan organisasi.

4.3 Rekomendasi

Setelah dilakukan analisis keamanan dan manajemen terhadap layanan teknologi informasi Untirta, hasil analisis tersebut digunakan untuk membuat rekomendasi. Hal tersebut dilakukan supaya layanan teknologi informasi Untirta dapat berkembang menjadi lebih baik.

4.3.1 Rekomendasi Keamanan Layanan Teknologi Informasi

Rekomendasi untuk keamanan layanan teknologi informasi UPT Data dan Informasi adalah memperbaiki layanan dari kerentanan yang ada pada layanan. Rekomendasi untuk keamanan layanan teknologi informasi Untirta dijelaskan pada Lampiran D.1.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran D.1, sebagian besar yang perlu dilakukan UPT Data dan Informasi Untirta untuk meningkatkan keamanan layanan teknologi informasi adalah mengupgrade aplikasi yang digunakan dalam layanan. Aplikasi tersebut diantaranya adalah PHP, SSL/TSL, nginx, dan Jquery. Selain itu, perlu dilakukan perubahan pada kueri dan menambahkan atribut pada aplikasi tertentu.

4.3.2 Rekomendasi Manajemen Layanan Teknologi Informasi

Rekomendasi untuk manajemen layanan teknologi informasi UPT Data dan Informasi adalah meningkatkan pengelolaan manajemen pada proses dan aktivitas umum pada *service operation*. Rekomendasi untuk manajemen layanan teknologi informasi Untirta dijelaskan pada Lampiran D.2.

Berdasarkan rekomendasi yang telah dijelaskan pada Lampiran D.2, sebagian besar yang perlu dilakukan UPT Data dan Informasi Untirta untuk meningkatkan manajemen layanan teknologi informasi ialah meningkatkan manajemen pada tiap proses yang ada pada *service operation*. Sementara itu, pemantauan dan pengelolaan layanan juga perlu ditingkatkan supaya layanan teknologi informasi dapat digunakan dan dimanfaatkan oleh civitas akademika Untirta dengan baik.