SURVEI CELAH KEAMANAN WEBSITE SISMIK FAKULTAS TEKNIK UNIVERSITAS PATTIMURA MENGGUNAKAN METODE SNIFFING

Ain Nurhayati Idi¹⁾, A. Y. Leiwakabessy²⁾, Benjamin G. Tentua³⁾

 ¹⁾S1 Teknik Mesin, Fakultas Teknik Universitas Pattimura Email:aku188764@gmail.com
 ²⁾Jurusan Teknik Mesin, Fakultas Teknik, Universitas Pattimura Email: arthur.leiwakabessy.@gmail.com
 ³⁾Jurusan Teknik Mesin, akultas Teknik, Universitas Pattimura Email:benjamin.tentua@fatek.unpatti.ac.id

Abstrak

Website memiliki peran yang sangat terkenal di zaman era globalisasi. Instansi-instansi baik pemerintah maupun swasta telah menggunakan website sebagai salah satu system informasi, Fakultas Kedokteran merupakan salah satu instansi yang menggunakan system website dengan nama SISMIK. Website SISMIK mengunakan system keamanan HTTP. System keamanan ini belum mencapai standar keamanan sehingga sering terjadi pencurian informasi dalam di dalam lalu lintas jaringan. Tujuan dari penelitian ini yakni untuk mengetahui celah keamanan pada penggunaan website SISMIK Fakultas Kedokteran yang masih menggunakan keamanan HTTP. Metode yang digunakan dalam penelitian ini yakni metode sniffing dengan menggunakan aplikasi wireshark untuk merekam aktifitas yang terjadi di dalam website SISMIK pada Fakultas Kedokteran. Dari hasil penelitian yang telah dilakukan maka dapat diketahui tingkat keamanan website Sismik Universitas Pattimura masih perlu ditingkatkan. Hal ini dibuktikan dengan penyerangan menggunakan aplikasi wireshark dengan menerapkan metode sniffing yang dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Username dan password yang didapat dari hasil perekaman tersebut berupa plain-text bukan berupa kode yang telah di enkripsi. Hal tersebut yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mengubah maupun menjual data tersebut. Mencegah hal itu terjadi maka website SISMIK fakultas kedokteran harus menggunakan SSL untuk meningkatkan keamanan website yang awalnya HTTP menjadi HTTPS sehingga username dan password tersebut tidak berupa plain-text.

Kata Kunci : Keamanan, Wireshark, Metode Sniffing

1. PENDAHULUAN

Pada saat ini kita hidup di zaman era globalisasi. Zaman era globalisasi yang terjadi di Indonesia yaitu kemajuan infrastruktur trasnportasi dan telekomunikasi ditandai dengan perkembangan teknologi. Seperti munculnya berbagai teknologi baru dan lebih maju. Pada saat ini jaringan internet sangat berperan dalam kehidupan manusia. Dengan adanya jaringan internet kita dapat melakukan berbagai hal, mulai dari mencari informasi, berkomunikasi dengan orang lain, transaksi jual beli dan lain sebagainya. Salah satunya dengan menggunakan website

Website adalah suatu kumpulan-kumpulan halaman yang menampilkan berbagai macam informasi teks, data, gambar diam maupun bergerak, data animasi, suara, video maupun gabungan dari semuanya, baik itu bersifat statis maupun yang dinamis, dimana membentuk satu rangkaian bangunan yang saling berkaitan dimana masing-masing dihubungkan dengan jaringan halaman atau hyperlink (Lestari T. S. M,dkk:2021). Sehingga untuk keamanan pada sebuah website menjadi salah satu hal yang paling penting karena dengan adanya kemana

Pada sebuah web artinya informasi dari user yang menggunakan web tersebut bisa menjadi lebih aman Namun perlu juga untuk selalu diperhatikan bahwa kemanan pada web harus selalu di kontrol dan diperhatikan karena jika tidak maka sistem keamanan tersebut dapat ditemukan kelemahannya oleh para hacher atau cracker yang ingin mencuri informasi pada web tersebut (Hae Y & Wiwin Sulistyo : 2021). Pencurian informasi pada lalu lintas data suatu jaringan komputer disebut dengan sniffing.

Sniffing dalam pengertian berarti mengendus, sedangkan dalam ilmu keamanan jaringan sniffing merupakan aktifitas menangkap paket-paket data yang lewat dalam sebuah jaringan. Serangan sniffing sangat berbahaya jika penyadap melakukan tindakan-tindakan atau perubahan paket data di jaringan karena data dapat dicuri. Pencurian data tersebut dapat berdampak pada pihak tertentu. Beberapa aksi sniffing lebih menakutkan jika cracker melakukan sniffing ditempat rawan, misalnya seorang user melakukan sniffing di universitas tempat belajar, atau seorang cracker melakukan sniffing untuk mencuri password email, bahkan mencuri data transaksi melalui kartu kredit maupun hal lainnya. Pada kenyataanya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas sniffing ini.

Universitas Pattimura Ambon khususnya Fakultas Kedokteran telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data atau informasi pelayanan umum maupun akademik dan informasi lainnya. Fakultas Kedokteran memiliki website yang digunakan salah satunya yaitu SISMIK. SISMIK adalah sistem informasi akademik yang digunakan oleh mahasiswa untuk melakukan registrasi dan dosen untuk melakukan proses peninputan nilai dan untuk SISMIK Fakultas Kedokteran sendiri menggunakan HTTP yang memiliki protokol keamanan yang belum mencapai standar keamanan sebuah website, sehingga data pada website yang menggunakan HTTP belum bisa dikatakan aman dari para hacker maupun cracker.

Serangan sniffing dapat terjadi baik website menggunakan HTTP ataupun HTTPS tergantung keamanan dari website itu sendiri. Penerapan serangan sniffing pada website di fakultas kedokteran dan gmail yaitu ingin mengetahui penangkapan data apa yang terjadi ketika terjadi serangan sniffing. Jika terjadi penangkapan data dari kedua website tersebut tahap selanjutnya bagaimana penulis memberikan solusi untuk mengatasi masalah yang terjadi.

2. HASIL DAN PEMBAHASAN

Hasil penelitian ini menjelaskan tentang keamana website yang dapat dilihat pada gambar berikut ini

Protkol	192.168.5.131	192.168.5.139
ТСР	86	0
HTTP	6	0
ICMP	0	8

Tabel 1 Hasil Pengintaian Capture Protokol SISMIK



Gambar 1 Hasil Pengintaian Capture

Dari gambar 1 dapat dilihat bahwa pada hasil capture menggunakan wireshark menghasilkan 3 protocol pada SISMIK. Dengan sumbu X merupakan jumlah banyaknya data dan sumbu Y merupakan protocol yang terdapat pada saat capture.

Terdapat dua alamat IP yang melakukan komunikasi dengan alamat IP SISMIK. Alamat IP 192.168.5.139 merupakan alamat IP perangkat yang mana dijadikan sebagai perangkat untuk sniffing. Komunikasi yang terekam dari peranagkat ini menghasikan protokol ICMP. Sedangkan alamat IP 192.168.5.131 merupakan alamat IP yang dijadikan target oleh sniffer. Komunikasi yang terekam dari perangkat ini menghasilkan protokol TCP dan HTTP.

A. Capturing Sismik

- 1. Capturing Pertama pada website sismik fakultas kedokteran universitas pattimura menggunakan akun yang memiliki info sebagai berikut
 - ✤ Username : 20228xxxx
 - ✤ password : 12071xxx
- 2. login pada halaman website sismik fakultas kedokteran universitas pattimura mengunakan akun diatas
- 3. merekam aktifitas yang terjadi menggunakan software wireshark



Gambar 2 Hasil Rekaman Paket Data

Pada gambar 2 merupakan tampilan hasil rekaman serangan packet sniffing pada software wireshark yang telah merekam seluruh aktifitas yang terjadi pada jaringan untuk melihat paket yang berasal dari website sismik fakultas teknik universiats pattimura, maka diharuskan melakukan penyaringan dahulu dari paket yang telah direkam.

Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui IP address dari website sismik fakultas teknik universitas pattimura yang memiliki DNS "sismik.fkunpatti.com" dengan cara membuka terminal kemudian memasukan perintah "ping sismik.fkunpatti.com" lalu menekan "enter" pada keyboard, maka akan muncul IP address dari sismik.fkunpatti.com pada gambar berikut.



Gambar 3 IP addresss sismik.fkunpatti.com

Pada Gambar 3 dapat diterangkan bahwa angka yang diberi tanda persegi panjang biru merupakan IP address dari website sismik fakultas kedokteran universitas pattimura. Setelah mengetahui IP address dari sismik.fkunpatti.com yaitu "103.247.11.125", maka selanjutnya melakukan penyaringan paket pada address bar filter yang ada dbawah kumpulan icon aplikasi Wireshark dengan memasukan perintah "ip.add==103.247.11.125" maka akan tampil paket-paket yang memiliki IP address tersebut.



Gambar 4 Hasil Penyaringan Paket Data Sismik.fkunpatti.com

Pada Gambar 4 merupakan seluruh paket data yang memiliki IP Address103.247.11.125 yang terdapat pada Source ataupun pada Destination.

Dapat dilihat dari Source dan Destination yang selalu bertukar tempat. Dari 492 paket data yang ditampilkan terdapat 2 jenis protokol yang digunakan yaitu protocol Transmission Control Protocol (TCP) dan Hypertext Transfer Protocol (HTTP). Karena koneksi internet kebanyakan menggunakan protocol TCP maka hasilnya akan banyak paket TCP yang terekam.

Dapat dilihat pula warna dari paket data, terdapat paket yang memiliki warna hijau muda, menunjukan bahwa paket tersebut menggunakan protokol HTTP dan protocol TCP yang menggunakan port 80. Sendangkan paket yang memiliki warna hitam dengan tulisan merah, menunjukan bahwa paket tersebut bermasalah dan paketdata harus dikirim ulang.

Untuk menganalisis paket data, dapat dilihat pada panel detail packet data. Berikut adalah salah satu tampilan detail packet data protocol TCP.



Gambar 5 Detail Paket Data TCP sismik.fkunpatti.com

Pada Gambar 5 merupakan detail dari packet Transmission Control Protocol yang diberi tanda persegi panjang biru. Dari detail paket data tersebut, penulis dapat menganalisis

informasi sebagai berikut :

- 1. Source Port : 36320
 - menunjukan port yang digunakan client adalah 36320
- 2. Destination Port : http (80) menunjukan port yang digunakan server adalah 80 yaitu http
- 3. Flags : 0x010 (ACK)
- 4. menunjukan client ingin meminta data dari server

Karena dalam penelitian ini hanya menganalisis keamanan website, maka penulis melakukan penyaringan lagi dengan mengetik perintah "ip.add==103.247.11.125&&http" maka akan tampil paket-paket yang memilikiprotokol HTTP seperti pada gambar berikut

				*wlar0	- 0
le Edit <u>View</u> G	o Capture Analyze	Statistics	Telephony Wireless To	iols <u>H</u> elp	
	s 🗎 🕅 🙆	a, e e	n ++ ++ 🔜 🔳		
p.addr==103.247.	11.1258&http				8 0 •
1000	2014/10		Lesuperio 0	Protocol Length	nfo
20 6.31228	7167 192.168.5	.231	103.247.11.125	HTTP 805	POST /fca5c1db0969ca021fdb451e94eb601f HTTP/1.1 (application/x-w_
07.0.47855	0384 103.247.1	1.125	192 108 5 131	HTTP 151	(TCP Previous segment not captured) Continuation
70 6.48223	2382 192.108.5	.131	103.247.11.125	HTTP 902	POST /login/proceed HTTP/1.1 (application/x-waw-form-urlencoded)
183 6.97749	8789 103.247.1	1.125	192.168.5.131	HTTP 594	(TTP/1.1 303 See Other
189 7.00123	3580 192.188.5	.131	103.247.11.125	HTTP 691	ET /student HTTP/1.1
					TCP Previous segment not captured] Continuation
223 1 19983	1401 103,241	1.125	192,168,5,131	HTTP: 1514	TCP Previous segment not captured] continuation
225 7.20002	7098 103.247.3	1.125	192.108.5.131	HTTP 1514	Int Indat ion
255 7 43707	7670 100.201.3	1.1.2.0	192.100.0.131	WTTO 540	ST (ann (controllers (min*ontroller in 1967 HTTD/1 1
271 7 04010	0005 102 100 5	101	103 247 11 125	NTTP 555	ET /master/arodi/listerodi MTTP/1 1
205 0 11331	0104 103 247 1	1 195	102 168 5 191	ATTD 505	(TTD/1 1 202 Temperary Badiract
289 8.12456	4549 192 168 5	0.04	101 247 11 125	NTTP 533	ET / HTTP/1 5
360 8.28577	2058 103.247.1	1.125	1002010010001011	HTTP: 1914	tcP Previous comment ante cuptured i Continuation
362 8,28738	3420 103.247.1	1,125	192.108.5.131	HTTP 1514	continuation
363 8.28730	3454 103.247.1	1.125	192.168.5.131	HTTP 1514	Continuation
304 0.20730	G487 163.247.1	1.125	102,100.5,131	HTTP 1814	TCP Previous segment not captured] Continuation
366 8.28834	3921 103.247.1	1.125	192.168.5.131	HTTP 1514	Continuation
367 8.28834	3006 103.247.1	1.125	192.168.6.131	HTTP 158	Continuation
rane 367: 158	bytes on wire i	1264 bit	s), 158 bytes capture	d (1264 bits) on i	nterface wlan0, id 0
thernet II, S	irc: Routerbo_fc:	:88:44 (c	4:ad:34:fc:80:44), D:	t: LiteonTe_9d:df:	8b (10:63:c8:9d:df:6b)
nternet Proto	col Version 4, 5	irc: 103.	247.11.125, Det: 192.	168.5.131	
ransmission C	control Protocol,	Src Par	t: 80, Dst Port: 4203	18, Seq: 27398, Ack	: 2892, Len: 92
ypertext Tran	isfer Protocol				
10 10 63 c8 1	be be de 76 be	M fc 80	44 98 99 45 a0 c	D E	
0 00 90 84 4	c7 40 00 38 06	70 61 67	f7 6b 7d c8 a8	@ 8)ag	

Gambar 6 Paket Data Sismik.fkunpatti.com dengan Protokol HTTP

Pada Gambar 6 merupakan paket data dari website sismik fakultas kedokteran unpatti yang memiliki protokol HTTP. Setelah melakukan penyaringan protokol HTTP, maka sisa paket data yang ditampilkan pada Gamabr 4.5 adalah sebanyak 21 paket. Pada menu "info" terdapat beberap keterangan seperti GET,HTTP/1,1, dan POST.

Untuk menganalisis paket data tersebut dapat dilakukan dengan cara mengklik kanan paket data pada listing packet panel yang ingin dianalisis kemudian pilih follow HTTP Stream. Berikut adalah salah satu tampilan detail paket data protokol HTTP yang memiliki info "POST"

Wire Wire	shark · Follow TCP Stream	(tcp.stream eq 5) ·	sismik.fkunpatti.co	om.pcapng			\times
POST /fca5cit Host: sismik. Connection: I Content-Lengi Accept: appl: X-Requested-V User-Agent: N (KHTML, like Origin: http: Content-Type: Origin: http: Accept-Langua Cookie: csrf. sessions-Bdbb usr=fca5cidbb	ibb909ca021fdb45i fkunpati.com eeep-alive lat bio/json, tex distrom/json, tex distrome/l0 ecko) chrome/l0 ecko) chrome/l0 ecko) chrome/l0 ecko) chrome/l0 ecko) chrome/l0 ecko) chrome/l0 application/x-w //sismik.fkunpat ing: gzlp, deflat ung: gzlp, deflat sobdf2d99ea765ab26: 9065ca021fdb451e9.	e94eb661f HT est x; Android J y.0.0.0 Mob ww-form-urle ti.com ti.com/ ej c1db969ca62 c1db969ca62 4eb661f&user	TP/1.1 , */*; q=0. .0; M2006G3L le Safari/5 mcoded; cha t1fdb451e94e le996edd4 mame=202283	01 G) AppleWe 37.36 rset=UTF-8 b661f; 999&passwo	ebKit/537	. 36 991&ak	
r=0HTTP/1.1 2 Date: Sat, 22 Server: Apach X-Powered-By: Expires: Thu, Cache-Control	200 OK L Jan 2023 04:22:3 ne PHP/5.5.38 19 Nov 1981 08:3 L: no-store, no-ca	30 GMT 52:00 GMT ache, must-r	evalidate,	post-check	<=0, pre-	check=	Ð
1 client pkt, 2 server pi	kts, 1 turn.						
Entire conversati	on (2,190 bytes)	 Show date 	ta as ASCII		* S	tream 5	
Find:						Find N	lext
	Filter Out This Stre	am Print	Save as	Back	Close	Hel	P

Gambar 7 Detal Paket Data POST sismik.fkunpatti.com

Gambar 7 dapat diterangkan bahwa dari detail paket data protokol HTTP terdapat dua warna teks. Teks yagng berwarna biru merupakan HTTP request sedangkan teks yang berwarna biru merupakan HTTP respons.

Isi dari salah satu paket data yang memiliki info POST berisikan berbagai informasi, diantaranya terdapat informasi sensitif yaitu username dan passowrd yang dogunakan. Selain itu dalam detail paket data tersebut penulis dapat menganalisis beberapa informasi sebegai berikut:

1. POST

Menunjukan bahwa client melakukan sebuah permintaan dengan memanfaatkan badan

pesan untuk mengirim data ke server web.

- Host: sismik.fkunpatti.com Menunjukan bahwa client sedang terhubung dengan sismik.fkunpatti.com
- 3. Conecction: keep-alive merupakan parameter yang mendefinisikan untuk batas waktu koneksi terputusdan jumlah permintaan maksimun
- 4. Content-Type: application/x-www-form-urlencoded;charset=UTF-8 Menunjukan bahwa client mengirim data melalui Form Uniform ResourceLocator (URL)
- User-Agent: Mozilla/5.0 (Linux; Android 10 id-id; M2006C3LG)AppleWebKit/537.36 (KHTML, like Gecko) Version/109.0.0.0 Mobile Safari/53 7. 36. Menunjukkan kemungkinan Web browser yang digunakan oleh client.
- 6. Accept-Encoding: gzip,deflate Menunjukkan metode kompresi yang diinginkan oleh client yaitu gzip atau eflate.
- Accept-Language: en-US Menunjukkan bahasa yang digunakan web browser yang dapat di terima serveradalah bahasa Inggris british dan bahasa inggris amerika
- 8. HTTP/1.1 200 OK. Menunjukkan permintaan telah berhasil dilakukan.
- 9. Date: Sat, 28 Apr 2018 19:44:35 GMT.

Menunjukkan waktu pada saat server megirim data tersebut.

10. Server: Apache

Menunjukkan jenis server yang dipakai yaitu Apache.

Untuk melihat proses komunikasi data pada saat korban mengakses website Simak Unismuh dapat dilakukan dengan cara mengklik "Statistik" pada menu bar kemudian pilih "Flow Graph" berikut ini adalah tampilannya.



Gambar 8 Proses Komunikasi Data sismik.fkunpatti.come

Pada Gambar 8 menunjukkan proses komunikasi data antara client yang memiliki IP address 192.168.43.121 sedangkan simak.unismuh.ac.id memiliki IP address 36.89.54.122.

Hasil dengan dilakukannya analisis uji coba dalam penelitian ini menunjukkan bahwa website Sismik Universitas Pattimura rentan terhadap pencurian data dengan menggunakan metode serangan sniffing pada jaringan nirkabel. Hal ini terjadi karena pada website Universitas Pattimura masih menggunakan protokol HTTP

Pada saat target mengakses website Sismik Universitas Pattimura menggunakan browser, kemudian browser meminta data pada server, server langsung mengirim data yang di

minta dalam bentuk teks biasa melalui TCP tanpa adanya perlindungan lebih. Sehingga pada saat melakukan proses sniffing, seluruh data yang melewati komputer penyerang akan tercapture pada aplikasi wireshark dan data tersebut dapat dibaca langsung oleh penyerang seperti yang terlihat pada Gambar 4.6.

Pada saat client melakukan sebuah permintaan dengan menentukan paramater di bagian URL dari permintaan maka metode permintaan HTTP tersebut berisikan opsi GET, contohnya yaitu URL yang terdapat pada halaman website. Sedangkan jika client melakukan sebuah permintaan dengan memanfaatkan badan pesan untuk mengirim data ke server web maka metode permintaan HTTP tersebut berisikan opsi POST, contohnya yaitu form pengisian username dan password pada halaman website. Setelah itu server mengirimkan HTTP response ke client yang berisikan datayang diminta dalam bentuk plain-text.



Berbeda halnya dengan https yang dapat dilihat pada gambar berikut

Gambar 9 capturing https

Dari gambar 9 dapat kita lihat bahwa komunikasi yang terjadi antara client dan server di lindungi dengan TLS1.2 yang merupakan keamanan standar sehingga data yang terekam pada wireshark tidak berupa plain-text. ketika kita akses website username dan password yang kita punya tidak terekam dalam bentuk teks biasa. Ini merupakan perbedaan pada HTTP dan HTTPS.

Karena ketika sniffer mendapat password dan username untuk mengakses website SISMIK yang masih http, kemungkinan data yang dicuri dapat mencangkup informasi indentifikasi pribadi mahasiswa, informasi pendaftaran mahasiswa, infromasi pengenal pribadi mahasiswa maupun staff, informasi nilai-nilai akademik mahasiswa. Yang lebih buruknya adalah peretas memiliki akses ke server yang memungkinkan mereka mengubah data dalam sistem. Hal tersebut dapat dikutip dari (Waka,2018) bahwa dari 500 juta pengguna 100 juta data mahasiswa dicuri. Dampak dari hal tersebut peretas menjual data pribadi, melakukan pemasaran spam, penipuan, meminta uang tembusan untuk pengembalian data serta mengubah informasi sistem akademik mahasiswa.

Hal ini sangat berbahaya sehingga untuk mencegah adanya penipuan, penjualan data, pengubahan data dan lain sebagainya website yang berkaitan dengan Sistem Informasi Akademik harus meningkatkan keamanan dari website tersebut, yang mana ketika website itu masih http harus di updated menjadi https yang memiliki standar SSL.

B. Solusi untuk Mencagah Serangan Paket Sniffing

Step 1. Install SSL di Server IIS

a. Untuk melakukan generate CSR silahkan akses dahulu aplikasi IIS yangdigunakan kemudian klik pada menu server certificat



Gambar 10 Halaman Beranda IIS

b. Kemudian klik link create certificate request pada sidebar sebelah kanan.

9			Internet informatio	in Services (IIS) Manager		- 0	x	
() () + (211/0+/79/04)	t *					$\omega = 0$	R.+	
For New Esti-								
Connections	GH S	erver Certil	licates			Actions		
0,-14111116	10.0					linger.	_	
5 4 Di 1686/719/862 (2019/80/11	Use this fea SSL	share to request an	of manage certificates that t	he Web server can use with website	configured for	Create Certificate Request.	-	
	Fiter		• 🐨 51 - 💽 Stow (11	Group by: No Grouping +		Create Damas Certificate		
	Name		Insued To	Insued By	Loi-	Create Self-Signed Certificate		
						Enable Automatic Rebend of Renewed Certificate		
	1				[8]			
1 1	- Feature:	Vew Costen	tView					
Fredy							41	
	_						-	

Gambar 11 Create Certificate Request

c. Kemudian akan muncul file seperti gambar berikut

	Request Certificate	?	x
Distinguished	i Name Properties		
Specify the required inforr official names and they ca	nation for the certificate. State/province and City/locality must be specified as nnot contain abbreviations.		
Common name:			
Organization:			
Organizational <u>u</u> nit:			
City/Jocality			
State/province:			
Country/region:	US v		
			_
	Previous <u>N</u> ext Einish	Cancel	

Gambar 12 Request Certificate

Step 2. Download Sertifikat SSL

Sertifikat SSL yang telah terbit bisa di download melalui halaman Clientzone. Langkahnya sebagai berikut:

- 1. Login ke Clientzone.
- 2. Klik menu SSL > Klik tombol Manage > Manage SSL.
- 3. Setelah itu akan masuk ke Produk Details. Klik download untuk mengunduh sertifikat SSL.

Domain	namadomain.com	Silahkan download sertifikat		
ackage	Sectigo PositiveSSL DV Wildcard	L CRI	Intermediate	+ ROOT
Periode	1 Tahun			
vetode Validasi	EMAIL	Jika Anda kehilangan private key CSR, silahk ta Re-issue	an generate ulang CSR dan lakuko	an re-issue dengan klik butto
	Contract Contract Contract Contract			

Gambar 13 Download Certificate SSL

Setelah file sertifikat di download, langkah selanjutnya adalah melakukaninstalasi SSL di cPanel. Berikut tahapannya

Step 2. Install SSL cPanel

- Berikut kami sampaikan cara install SSL di cPanel Rumahweb:
- 1. Login ke cPanel.
- 2. Masuk ke menu 'SSL/TLS' pada cPanel.

cPa	inel		n 1996 - N - N			
	SECURITY					-
	IP Blocker	SSL/TLS	Hotlink Protection	Leech Protection	SSL/TLS Status	
	Let'sEncrypt					

Gambar 14 Menu SSL/TLS

3. Masuk ke 'Install and Manage SSL for your site (HTTPS)' klik 'Manage SSL sites' seperti pada gambar.

DEFAULT SSL/TLS KEY TYPE	Show Help Text 🕲	PRIVATE KEYS (KEY)
The default key type for SSL/TLS certificates and <u>CSR</u> s. Use the system's default key type, <u>Recommended</u> <u>Current</u> Current value: RSA, 2,048-bit RSA, 2,048-bit ECDSA, P-384 (secp384r1) ECDSA, P-256 (prime256v1) RSA, 4,096-bit		Generate, view, upload, or delete your private keys. CERTIFICATE SIGNING REQUESTS (CSR) Generate, view, or delete SSL certificate signing requests. CERTIFICATES (CRT)
B Save		Generate, view, upload, or delete SSL certificates. INSTALL AND MANAGE SSL FOR YOUR SITE (HTTPS) GManage SSL sites.

Gambar 15 Manage SSL Sites

4. Lalu masukkan kode sertifikat SSL di kolom Certificate (CRT) seperti gambarberikut.

Joinain		
demorw.	my.id (+ subdomains: cpanel, cpcalendars, cpc 🗸 🗸	
P Address		
03.247.11.	121	
Certificate:	(CRT)	
MIFLZCCBBB MDIxCZAJBgN EwJSMZAFW0 DiouZGVtb3J vCU6E2SqJ31 ZQn98XKBYk5 umZL3pVN1k1 nmPPNG7yJ3X0 ow1V0Tj0Rd	EIRT 11 LOT 12	Autofill by Certificate
Domains:	*.demorw.my.id	
lssuer: Kev:	Let's Encrypt RSA, 2.048-bit (bc253a13)	

Gambar 16 Sertifikat SSL di Kolom CRT

5. Selain kolom CRT, Anda juga perlu mengisi kolom Private Key dan CA Bundle yang berada tepat dibawah kolom Certificate. Tampilannya sebagai berikut:

y to retrieve the
i public

- Gambar 17 Pengisian Private Key dan CA Bundle
- 6. Di cPanel, Anda bisa menggunakan fitur 'Autofill by Certificate' agar kolom Private key dan CA Bundle dapat terisi secara otomatis. Contohnya sebagai berikut.

lutfi.web	.id (+ subdomains: cpanel, cpcalendars, cpcontacts, 🗸 🗸	
IP Address		
Certificate	: (CRT)	
2N5KYX32Lm dG2pLnd1Y11 Lm1kghR32kk HSAERTBDHAg dHRwG1BvY31 BQB3A7Qgv8d AEgxRgThAP pTeoGK2nD9 Dhg3fy5q12 B34Td504043 vvQwDQY3Ko3	Ladipium 1792 TTXYN 392897000 SYN Ladiwiddiad Color TTXYN 2000 Color Col	Autofill by Certificate
Domains	c cpanel.lutfi.web.id cpcalendars.lutfi.web.id lutfi.web.id mall.utfi.web.id webdisk.lutfi.web.id webmall.utfi.web.id	ney dan ca bundle otomatis
	contraction and the last	

Gambar 18 Konfigurasi Autofill by Certificate

Hasilnya kolom Key dan CA Bundle akan terisi seperti screenshot berikut.

BEGIN RSA PRIVATE KEY	-
MIIEpAIBAAKCAQEAvCU6E25qJ31sDTjLSYnqXjQnqywu4wgooJ20kIjoqtP21A/7	
XzUlbroibnunKfMhZQn98XKBYk5j+Ez3ZaBGo5LVirnEXbr5qzQPe8YfIucfC74c	
I9VbCV283WPBe1NoumZL3pVW1k1oDW242s8C5OR1eYH8ZBrmnutphYPeUbg/Qjtt	
I8SGNgIdr2ztMlH4nmPPNG7yJaXGz16mxSSRV1w1V7g3j1w/Ep31dULX8ULS3TFM	
JHR140024C59R0510R1401J1000117CC5A040088A0003204053A701C04R0P2000	
d1R4N041F9r1n16PhVoN2MF1M/MHD4WU310nH1F4V645x501oxRe4M91wB1e38Wv	
XnHOMwgIl4Rmnet01zvCOgFsVdljVsKs/bTv6/I0H1IzuGEHreluRfTlLlCjE80W	*
MNoNxbzJ6rHfD+Xb5DTndpVVMVPHY1Xu/fu38bu+JdNtVTDm18KTW1yp3RP2gY4A	
MD0TADXAusea10aaAuCct1uEX85KabiKa07AWKu00C3LEEm00caAba7LET033ablaE	
ine private key inay aneady be on your server, nou can ender passe the private natching key for your certificate.	
Inte private key integrated be on your server, nou can entitle paste the private matching key for your certificate.	A
The private key intra-an easily be on your server, nou can ensure passe the private matching key for your certificate. Certificate Authority Bundle: (CABUNDLE) The private magnature certres intra status operations and	
Interprivate key integrateato/ De on your server, nou can entitier paste the private activing key for your certificate. Certificate Authority Bundle: (CABUNDLE) 	
Interprivate key inag aneady be on your server, nou can entitle paste the private atching key for your certificate. Sertificate Authority Bundle: (CABUNDLE) 	
Interprivate Avy Inay an early De On You's even to use reinter passe the private activing key for your certificate. Certificate Authority Bundle: (CABUNDLE) 	
Ine private key inay aneady be on your server. You can entrie paste the private aratching key for your certificate. erificate Authority Bundle: (CABUNDLE) 	
Inter private key inga an early be on your server. You can entrie passe the private activity by your certificate. eretificate Authority Bundle: (CABUNDLE) TITTF:Cockegantagetagetagetagetagetagetagetagetagetage	
Interprivate Avery Imag all early the only your server. You can entrie private arching key for your certificate certificate Authority Bundle: (CABUNDLE)	
Inter private key inga an early be on your server. You can entitle paste the private activity by your certificate. ertificate Authority Bundle: (CABUNDLE)	
Inter private Ander Arey Tingy an early the on you're level. Tou'r can einifer paste the private arching key for you'r cerfficate certificate Authority Bundle: (CABUNDLE)	fetch if from a public
Transformation (Construction) Transformation (Construction) Transformation (Construction) Transformation (Construction) Transformation T	fetch it from a public

Gambar 19 Hasil Kolom Key dan CA Bundle

7. Langkah terakhir adalah klik tombol 'Install Certificate'.

Sampai tahap ini, install SSL telah selesai. Anda bisa mencoba akses namadomain anda untuk mengetahui hasilnya karena domain anda sudah menjadi HTTPS

3. SIMPULAN

Dari hasil penelitian yang telah dilakukan maka dapat ditarik simpulannya, yaitu: Tingkat keamanan website Sismik Universitas Pattimura masih perlu ditingkatkan. Hal ini dibuktikan dengan penyerangan packet sniffing yang dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Username dan password yang didapat tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mengubah maupun menjual data tersebut. Mencegah hal itu terjadi maka website SISMIK fakultas kedokteran harus menggunakan SSL untuk meningkatkan keamanan website yang awalnya HTTP menjadi HTTPS sehingga username dan password tersebut tidak berupa plain-text.

DAFTAR PUSTAKA

- [1] Adriant, M.F., & Mardianto, I. (2015). Seminar Nasional Cendekiawan. Implementasi Wireshark untuk Penyadapan (Sniffing) Paket Data Jaringan, 2, 224-228. Retrieved from http://www.trijurnal.lemlit.trisakti.ac.id/index.php/semnas/article/view/139.
- [2] Basri. (2015). Jurnal Ilmu Komupter. Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan), 1(2). Retrieved from https://ejournal.fikomunasman.ac.id/index.php/jikom/ article/view/34.
- [3] Dewi, R., Rimra, I.L., & Vitria, R. (2012). Poli Rekayasa. Analisis Komunikasi Data Pada Aplikasi Percakapan Suara Menggunakan Perangkat Lunak Wireshark, 8(1), 32-41. Retrieved from <u>http://repo.polinpdg.ac.id/273/</u>.
- [4] Fatimah, Thomson Mary., & Anggri Yulio Pernanda. (2022). Analisis Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing di Universitas PGRI Sumatera Barat. Jurnal Teknologi Informasi.. vol 1, No. 2. 7-11.
- [5] Hamid. (2017). Teknoin. Analisis Keamanan Aplikasi Email Bawaan Android dan Gmail Pada Jaringan Nirkabel, 23(2), 125-136. Retrieved from <u>http://jurnal.uii.ac.id/jurnal-teknoin/article/view/8923</u>.
- [6] Nazwita, & Ramadhani. S. (2017). Seminar Nasional Teknologi Informasi, Komunikasi dan Industri (SNTIKI). Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata, 9, 308-317. Retrieved from http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/ view/3368
- Rerung, R.R. (2018). Program Web Dasar. Deepublish. Yogyakarta
- [7] Singh, A. (2013). Instant Wireshark Starter, Packt Publishing Ltd, Birmingham B3 2PB.
- [8] Tia Siti Maulidda Lestari dkk., 2021. Perancangan Sistem Informasi Berbasis Web Melalui Whatsapp Gateway Studi Kasus Sekolah Luar Biasa-BC Nurani. Jurnal Informasi dan komunikasi. Vol 9, No. 1
- [9] Wikipedia. (2018). Wireshark Go Deep. Wireshark User's Guide, Diakses pada 15:45, Februari 15, 2018, dari https://www.wireshark.org/docs/wsug_html/.
- [9] Yacob Hae & Wiwin Sulistyo., 2021. Analisis Keamanan Jaringan Pada Web Daei Serangan sniffing Dengan Metode Eksperimen. Jurnal Teknik Informatika dan Sistem Informasi. Vol 8, No. 4, Hal 2095-2105