HARDENING CLOUDFRI DENGAN METODE *SECURITY HARDENING* PADA APLIKASI BERBASIS *WEBSITE* TAP2GO.CLOUDFRI.ID

CLOUDFRI HARDENING WITH SECURITY HARDENING METHOD ON *WEBSITE*-BASED APPLICATION TAP2GO.CLOUDFRI.ID

Rifqi Zain Naufal[1], Umar Yunan kurnia Septo Herdianto[2], Muhammad Fathinuddin[3]

[1,2,3] Universitas Telkom, Bandung

[1]**rifqizn@student.telkomuniversity.ac.id,** [2]**umaryunan@telkomuniversity.ac.id,**

[3]**muhammadfathinuddin@telkomuniversity.ac.id**

Abstrak

Hardening merupakan metode untuk meminimalisir celah keamanan pada sistem, dan metode ini dapat dilakuan diberbagai sistem. Dengan berkembang pesatnya teknologi pada saat ini tidak menutup kemungkinan akan terjadinya tidak kriminal untuk mengekpoitasi celah keamanan yang terdapat pada suatu sistem. Penelitian ini bertujuan untuk mengetahui seberapa tingginya tingkat keamanan dan celah keamanan yang terdapat pada aplikasi berbasis *website* tap2go.cloudfri lalu menentukan rekomendasi apa yang harus dilakukan dalam melakukan *hardening* dan meminimalisir celah keamanan dengan metode *security hardening* yang dilakukan hingga tahap *remediate*. Pada penelitian ini simulasi yang dilakukan yaitu *vulnerability scanning* dan *penetration testing* dengan OWASP sebagai pedoman dalam pemilihan tools *vulnerability scanning* dan dalam melakukan *penetration testing*. Hasil penelitian ini berupa analisis *vulnerability scanning* dan *penetration testing*. Kerentanan yang ditemukan yaitu kerentanan terhadap serangan DoS, komunikasi yang tidak terenkripsi, dan penggunaan SSl/TLS yang telah usang. *Penetration testing* yang dilakukan yaitu simulasi penyerangan SQL *injection*, DoS, *Session hijacking*, dan *Interception.* Hasil *penetration testing* didapati sistem tersebut telah aman dari serangan SQL *injection* karena sudah terdapatnya *firewall* untuk menahan serangan tersebut sebaliknya untuk jenis serangan lainnya sistem tersebut belum aman dan perlu dilakukan konfigurasi ulang pada *web server* untuk meminialisir celah keamanan yang terdapat pada aplikasi berbasis *website* tap2go.cloudfri.

Kata Kunci: *Hardening, Vulnerability Scanning, Penetration testing, OWASP*

Abstract

Hardening is a method to minimize security holes in the system, and this method can be done in various systems. With the rapid development of technology at this time, criminals can exploit security gaps in a system. This study aims to find out how high the level of security and security gaps are contained in the tap2go.cloudfri website-based application and then determine what recommendations should be made in hardening and minimizing security gaps with the security hardening method carried out to the remediate stage. In this study, simulations were carried out, namely vulnerability scanning and penetration testing with OWASP as a guide in selecting vulnerability scanning tools and in performing penetration testing. The results of this study are analysis of vulnerability scanning and penetration testing. The vulnerabilities identified were vulnerability to DoS attacks, unencrypted communications, and outdated use of SSL/TLS. Penetration testing carried out is a simulation of SQL injection, DoS, Session hijacking, and Interception attacks. The results of the penetration testing found that the system was safe from SQL injection attacks because there was already a firewall to withstand these attacks. On the other hand, for other types of attacks, the system was not secure and needed to be reconfigured on the webserver to minimize the security holes in the tap2go.cloudfri website-based application.

Keywords: Hardening, Vulnerability Scanning, Penetration testing, OWASP

1. Pendahuluan

*Cloud*FRI merupakan sebuah *website* yang penting di Fakultas Rekayasa Industri Telkom University. *Cloud*FRI berisi kumpulan aplikasi web yang digunakan oleh keseluruhan entitas Fakultas Industri baik Dosen, mahasiswa maupun karyawan yang terdapat di Fakultas Rekayasa Industri, kurang lebih terdapat sembilan aplikasi didalamnya dengan fungsi yang berbeda seperti aplikasi administrasi.cloudfri.id, ingram.cloudfri.id, labrecuirement.cloudfri.id dsb[1]. Dengan berkembang pesatnya teknologi pada saat ini tidak menutup kemungkinan akan terjadinya tidak kriminal untuk mengekpoitasi celah keamanan yang terdapat di CloudFRI seperti pencurian data, perusakan data, interupsi layanan yang dapat berakibat *server down*, dan berbagai serangan lainnya yang sangat merugikan seluruh entitas yang terdapat di Fakultas Rekayasa Industri. Untuk mengatasi hal itu maka harus dilakukan suatu metode keamanan yaitu dengan melakukan *Hardening* pada *Cloud*FRI. *Hardening* merupakan metode untuk meminimalisir celah keamanan pada sistem, dan metode ini dapat dilakuan diberbagai sistem , terdapat berbagai metode dalam melakukan *hardening* seperti membatasi akses pada jaringan ke sistem dengan menonaktifkan layanan jaringan yang tidak terpakai atau tidak perlu , lalu ada juga dengan menggunakan *firewall* yaitu dengan menggunakan *rule* yang ada pada *firewall* atau dengan mem*filter* akses data yang akan masuk kedalam jaringan dan *filter* yang terdapat di *firewall* dapat berdasarkan *IP address*, *protocol*, *port*, *interface*, Mac *address*, dsb. Dalam melakukan *hardening* terdapat empat tahapan, tahap pertama yaitu *Access*, *Access* adalah proses untuk mengidentifikasi celah – celah keamanan yang terdapat dalam CloudFRI yaitu dengan melakukan simulasi atau percobaan penyerangan (*attacking)* kedalam sistem CloudFRI untuk mengetahui celah keamanan yang terdapat didalamnya. Tahap selanjutnya yaitu *Analyze* yang berfungsi untuk menganalisa seberapa besar dampak yang akan diperoleh dari celah – celah keamanan tersebut jika celah tersebut berhasil di eksploitasi oleh penyerang lalu mengklasifikasikan tingkat resikonya. Setelah tahap *Analyze* terdapat tahap *Remediate*, pada tahap ini berfungsi untuk mencari solusi dan metode apa yang akan digunakan untuk menutup celah – celah keamanan yang ada atau memperbaiki konfigurasi yang ada pada *website* CloudFRI yang menyebabkan terdapatnya celah keamanan pada sistemnya. Tahap terakhir yaitu Manage pada tahap ini sistem yang sudah ditutup celahnya atau diperbaiki konfigurasinya pada tahap sebelumnya, selanjutnya dilakukan pemantauan dan pengelolaan apakah yang dilakukan sebelumnya sudah cukup untuk mencegah terjadinya serangan[2]. Dengan dilakukannya *Hardening* pada *Cloud*FRI diharapkan dapat menambah wawasan atau pengalaman bagi peneliti dalam bidang *host hardening* dan juga mencegah terjadinya hal-hal yang dapat merugikan seluruh entitas yang ada di Fakultas Rekayasa Industri seperti pencurian data, perusakan data, interupsi layanan yang dapat mengakibatkan *server down* dana berbagai serangan lainnya serta menutup celah – celah keamanan yang terdapat di *Cloud*FRI.

2. Landasan Teori

2.1 *Web Hosting*

Web hosting adalah jasa penyewaan tempat penyimpanan data di internet yang diperlukan oleh sebuah *website*. Ukuran yang digunakan dalam suatu *web hosting* adalah kapasitas dan *bandwith*. Kapasitas adalah ukuran besarnya kemampuan sebuah *web hosting* untuk menyimpan data-data *website*. Semakin besar kapasitas dari *web hosting*, maka semakin besar kapasitas penyimpanan data yang diberikan. *Bandwith* adalah ukuran maksimal dari jumlah *volume* data yang diperbolehkan untuk diakses dari *web hosting* setiap bulannya[3].

2.2 *Cloud Computing*

Cloud computing adalah utilitas yang menyediakan jasa komputasi (*Computing services*). Dalam utilitas komputasi (*utility computing*), perangkat keras dan sumber daya perangkat lunak terkonsentrasi dalam pusat data yang besar. Pengguna *computing services* membayar saat mereka menggunakan komputasi, penyimpanan, dan sumber daya komunikasi. Sementara utilitas komputasi sering membutuhkan infrastruktur seperti *cloud*, fokus dari *cloud computing* adalah ada pada model bisnis untuk menyediakan layanan komputasi.[4]

Cloud computing memiliki tiga layanan yang ditawarkan kepada penggunanya, diantaranya[5]:

1. *Software as a Service* (SaaS)

SaaS adalah layanan dari *Cloud Computing* dimana kita tinggal memakai software (perangkat lunak) yang telah disediakan. Kita cukup tahu bahwa perangkat lunak bisa berjalan dan bisa digunakan dengan baik. Contohnya yaitu layanan email publik (Gmail, YahooMail, Hotmail) media sosial (Facebook, Twitter) instant messaging (YahooMessenger, Skype, Gtalk) dan masih banyak lagi yang lain.

2. *Platform as a Service* (PaaS)
   PaaS adalah layanan dari Cloud Computing dimana kita menyewa rumah berikut lingkungan-nya (*operating system, network, database engine, framework* aplikasi), untuk menjalankan aplikasi yang kita buat. Pengembang membuat aplikasi pada platform penyedia melalui *Internet*. Penyedia PaaS dapat menggunakan *API*, *port*al situs web atau perangkat lunak gateway di install pada komputer pelanggan.

3. *Infrastructure as a Service* (IaaS)

   IaaS adalah layanan dari *Cloud Computing* dimana kita bisa menyewa infrastruktur IT (komputasi, *storage, memory, network* dsb). Kita bisa definisikan berapa besar-nya unit komputasi (CPU), penyimpanan data (s*torage*) , memori (RAM), *bandwith*, dan konfigurasi lain-nya yang akan kita sewa. Mudahnya, IaaS ini adalah menyewa komputer virtual yang masih kosong, dimana setelah komputer ini disewa kita bisa menggunakannya terserah dari kebutuhan kita. IaaS terletak satu *level* lebih rendah dibanding PaaS.

2.3 *Security hardening*

Security Hardening merupakan metode untuk meminimalisir celah keamanan pada sistem, dan metode ini dapat dilakuan diberbagai sistem. Dalam melakukan *Security Hardening* terdapat empat tahapan yaitu *Access, Access* adalah proses untuk mengidentifikasi celah – celah keamanan yang terdapat dalam suatu sistem. Tahap selanjutnya yaitu *Analyze* yang berfungsi untuk menganalisa seberapa besar dampak yang akan diperoleh dari celah – celah keamanan yang ada. Tahap selanjutnya yaitu tahap *Remediate*, pada tahap ini berfungsi untuk mencari solusi dan metode apa yang akan digunakan untuk menutup celah – celah keamanan yang ada. Tahap terakhir yaitu tahap *Manage* pada tahap ini dilakukan penutupan celah keamanan yang telah ditemukan pada sistem[2].

2.4 *Penetration Testing/Exploit*

Penetration testing/Exploit merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan kegitan *security* audit. Simulasi serangan yang dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin terjadi karena kelemahan sistem[6].

Jenis atau metode *Penetration testing* terbagi menjadi tiga yakni :

1. Metode *Black-box*, merupakan jenis *penetration testing* yang serupa dengan *hacker* aslinya, karena penguji diberikan nama perusahaan dan informasi mengenai jaringan maupun informasi lainnya harus dicari sendiri oleh penguji. Cara ini cara yang menghabiskan banyak waktu serta biaya yang sangat besar.
2. Metode *White-box* merupakan jenis pengujian yang berbalikan dengan *black-box* karena semua informasi secara lengkap diberitahukan di depan serta infrasuktur mana saja yang perlu diuji, pengujian ini mirip denga tindakan karyawan perusahaan cara pengujin ini dibagi menjadi dua bagian yakni yang diberitahukan dengan kerjasama sepenuhnya oleh karyawan IT maupun tidak diberitahukan dimana tanpa sepengetahuan staff IT.
3. Metode *Grey-box*, dimana campuran keduanya melibatkan informasi yang terbatas serta pengujian secara internal, selain itu setiap program diteliti untuk di celahnya. Simulasi yang digunakan di *grey-box* berdasarkan pengujian *black-box* serta pengetahuan yang ada untuk dapat menganalisa secara menyeluruh.

2.5 *Vulnerability*

Vulnerability adalah kelemahan sebuah sistem akibat dari berbagai jenis pola serangan. Pada setiap sistem dan jaringan tentu akan mempunyai *vulnerability* (kerentanan) dan dapat mengakibatkan kerusakan pada sistem bahkan data perusahaan sehingga menimbulkan kerugian. *Vulnerability* dapat

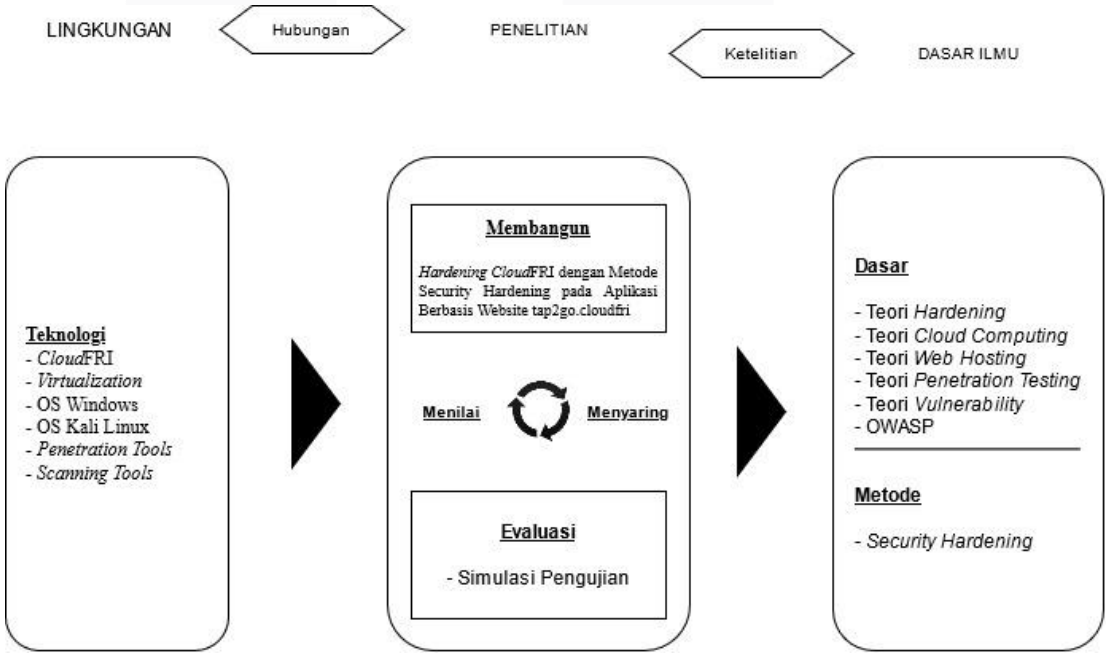
terjadi pada perangkat keras(*hardware*), perangkat lunak(*software*), aplikasi yang dikembangkan perusahaan bahkan kelemahan dari sisi user itu sendiri. *Vulnerability* atau kelemahan ini kemudian memiliki peluang digunakan sebagai pintu masuk di mana penyerang akan menyerang sistem yang terdapat *vulnerability* tersebut. Dengan melakukan *penetration testing* setelah dilakukannya *vulnerability scanning* dapat mengidentifikasi *vulnerability* yang ada, mencoba masuk melalui *vulnerability* dan memberikan rekomendasi untuk menutup *vulnerability* yang ada sehingga sistem menjadi aman[7].

2.6 OWASP

Open Web Application Security Project (OWASP) adalah sebuah organisasi internasional yang bersifat non-profit, didirikan oleh OWASP foundation pada 21 April 2004 di Ameriaka Serikat. Keanggotaan OWASP berasal dari para ilmuwan, peneliti, dan sektor swasta yang menerbitkan laporan artikel, Penerapan *Framework* OWASP dan *Network Forensics* untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi *Host-Based* 10 alat/peralatan, dan dokumen yang bersifat *open source*. OWASP fokus pada peningkatan keamanan perangkat lunak dan didedikasikan untuk memungkinkan organisasi dalam mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi terpercaya untuk menjamin keamanan yang dibuat atau dikembangkan. OWASP memiliki misi untuk mengamankan *software*, sehingga orang-orang dan organisasi dapat membuat keputusan terhadap resiko keamanan yang benar. OWASP merupakan vendor netral yang tidak berafiliasi dengan perusahaan teknologi manapun, tidak mendukung atau merekomendasikan produk atau layanan komersial. Proyek yang sudah dibuat dan dipublikasikan ada 363 proyek dan semua berkaitan dengan keamaan aplikasi, diantara proyek tersebut yaitu *OWASP Top Ten Project, OWASP ASVS Assessment tool, OWASP Zed Attack Proxy Project, OWASP Testing Guide*[8].

3. Metodologi Penelitian

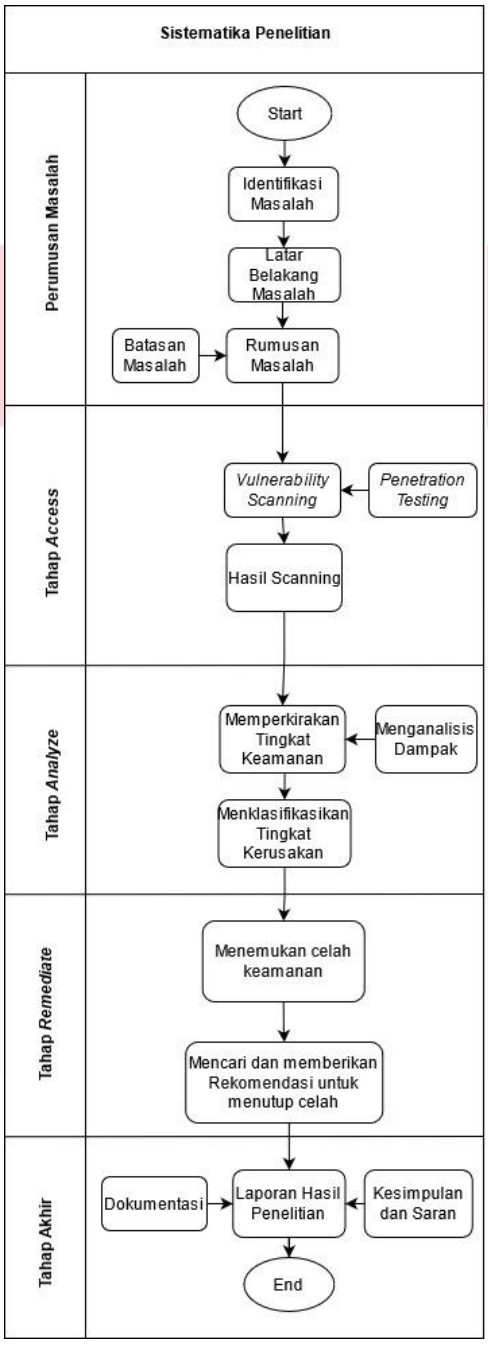
Model konseptual merupakan gambaran untuk memahami, melaksanakan, dan mengevaluasi penelitian sistem informasi. Tujuan utama dari model ini dapat digunakan untuk mewujudkan sebuah kerangka terstruktur yang digunakan untuk memahami tujuan dari sebuah penelitian[11].



Gambar 3. 1 Model Konseptual

3.1 Sistematika Penelitian

Sistematika Penelitian merupakan pemecahan masalah, sebuah proses terencana yang mana dilkakukan untuk mencapai tujuan penelitian. Berikut adalah sistematika pemecahan masalah yang dilakukan :



Gambar 3. 2 Sistematika Penelitian

4. Hasil dan Analisis

4.1 Hasil dan Analisis *vulnerability scanning* dari Nessus

Data yang diambil dari Nessus antara lain *vulnerability*, CVSS, VPR (*Vulnerability Priority Rating)*, *services*, dan *threat level.* Pada *vulnerability scanning* yang telah dilakukan, didapatkan hasil dari jenis – jenis kerentanan yang ada pada aplikasi berbasis *website* tap2go.cloudfri, pada hasil dari

kategori *service* didapatkan *port* yang terbuka pada jenis kerentanan masing – masing, hasil CVSS pada tap2go.cloudfri yang didapatkan dari aplikasi Nessus mengacu pada standar NVD (*National Vulnerability Database*) dengan rentang score 0.0 – 10.0, dan *threat* yang didapatkan memiliki kategori antara lain *Low, Medium, dan High.* Dapat diketahui rincian *vulnerability* dengan rincian sebagai berikut:

Tabel 4. 1 Hasil *Vulnerability Scanning* Nessus

No	*Threat level*	*Vulnerability*	CVSS	*Service* (*Port*)
1	*High*	SSL *Medium Strength Cipher Suites Supported* (SWEET32)	7.5	143 / tcp / imap 995 / tcp / pop3
		DNS *Server Spoofed Request Amplification* DDoS	7.5	53 / udp / dns
2	*Medium*	TLS *Version* 1.0 *Protocol Detection*	6.5	110 / tcp /pop3 993 / tcp / imap
		HSTS *Missing From* HTTPS *Server* (RFC 6797)	6.5	2088 / tcp /www 2083 / tcp /www
		DNS *Server Recursive Query Cache Poisoning Weakness*	5.0	53 / udp / dns
		SSL *Anonymous Cipher Suites Supported*	5.9	21 / tcp / ftp
3	*Low*	POP3 *Cleartext Logins Permitted*	2.6	110 / tcp /pop3

4.2 Hasil dan Analisis *vulnerability scanning* dari Burp Suite

Pada *vulnerability scanning* yang telah dilakukan pada alamat *ip* target dengan aplikasi Burp suite akan diperoleh hasil berupa detail dari *vulnerability* berikut dengan solusi untuk mengatasi *vulnerability* yang ada, dan threat yang didapatkan memiliki kategori antara lain *Low, Medium, dan High*. Aplikasi ini juga berfungsi sebagai tools untuk melakukan penyerangan *man in the middle, fuzzing*, dan secara ekstensif menguji kerentanan OWASP dan mengkategorikan tingkat kerentanan yang ada. Dapat diketahui rincian *vulnerability* dengan rincian sebagai berikut:

Tabel 4. 2 Hasil *Vulnerability Scanning* Nessus

No	*Threat level*	*Vulnerability*
1	*High*	*Cleartext submission of password*
2	*Medium*	TLS *certificate*
3	*Low*	*Unencrypted communications*
		Strict transport security not enforced
		Vulnerable JavaScript dependency
		Password field with autocomplete enable

4.3 Hasil dan Analisis *vulnerability scanning* dari Nmap

Pada *vulnerability scanning* yang telah dilakukan pada alamat *IP* target dengan aplikasi Nmap versi GUI (*Graphical User Interface***)** pada sistem operasi Windows 10 akan diperoleh hasil berupa detail dari *state*, *services*, *dan version* dari target yaitu aplikasi berbasis *website* tap2go.cloudfri. Hasil dari *services* yang terbuka dan fungsinya pada *website* tap2go.cloudfri adalah sebagai berikut:

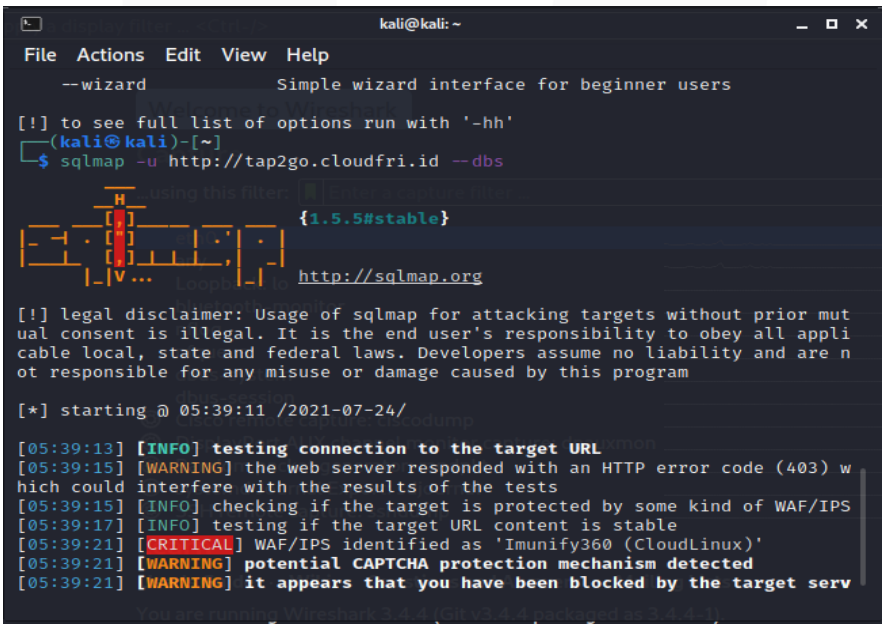
Tabel 4. 3 Hasil *Vulnerability Scanning* Nmap

Port	Fungsi
80	Terbuka : *Port* ini digunakan untuk web *server*, paling umum digunakan untuk mengakses internet atau bisa disebut HTTP *port server* Tertutup : *Port* ini akan menutup jalan atau akses ke internet
53	Terbuka : *Port* ini adalah *port Domain Name Server* (DNS). Untuk menjawab pertanyaan yang terkait dengan penerjemahan nama domain ke *IP Address*. Tertutup : *Port* ini menjadi tidak bisa membaca DNS atau menerjemahkan DNS ke alamat *IP*.
21	Terbuka : *Port* ini digunakan untuk mengkoneksi FTP *Server*. FTP (File Transmission Protocol) untuk dapat saling menghubungkan komputer satu dengan komputer lainnya. Tertutup : *Port* ini tidak akan terkoneksi dengan FTP *Server* dan tidak bisa menggunakan hal berbagi file.
22	Terbuka : *Port* ini merupakan *port* yang digunakan untuk mengaktifkan SSH atau *Secure Shell* pada jaringan komputer dan memberikan kerahasiaan atau integritas dalam pengiriman data Tertutup : Jika *port* ini tertutup menyebabkan rentan terhadap intersepsi dan menggunakan penganalisa paket sehingga tidak terjaga kerahasiaan data saat sedang berbagi file.
25	Terbuka : *Port* ini merupakan *port* yang digunakan untuk SMTP (*Simple mail Transfer Protocol*), *port* SMTP digunakan untuk mengirimkan data dari computer klien pengirim email ke *server* si penerima email. Tertutup : Tidak tersedianya layanan SMTP (*Simple mail Transfer Protocol*).
110	Terbuka : *Port* ini merupakan *port* yang digunakan untuk menjalankan protokol POP3 (Post Office Version 3). POP3 adalah protokol yang berfungsi sebagai tempat sementara untuk email sebelum diteruskan ke penerima. Tertutup : Tidak tersedianya layanan protokol POP3 (*Post Office Version* 3).
143	Terbuka : *Port* ini merupakan *port* yang digunakan untuk IMAP4 (*Internet Message Access Protocol*). IMAP adalah protokol yang berfungsi untuk mengakses email yang dikirim ke *server* maupun dari *server*. Tertutup : Tidak dapat mengakses atau mengambil email menggunakan *server* IMAP4
443	Terbuka : *Port* ini merupakan *port* yang digunakan untuk HTTPS. Dengan protookol HTTPS perintah ataupun data telah dilindungi dengan sistem enkripsi sehingga dokumen yang dikirimkan dengan HTTPS lebih aman. Tertutup : Jika *port* ini tertutup maka memungkinkan akan terjadinya serangan karena saat proses pertukaran data tidak melalui proses enkripsi.
587	Terbuka : *Port* ini merupakan *port* yang digunakan untuk menjalankan *Mail Submission Agent* (MSA). MSA adalah software untuk menerima email dari *Mail*

	User Agent (MUA) dan bekerja sama dengan *Mail Transfer Agent* (MTA) untuk mengirimkan sebuah email. Tertutup : Tidak dapat melakukan koneksi SMTP
993	Terbuka : *Port* ini merupakan *port* yang digunakan untuk *Port* ini merupakan *port* yang digunakan untuk *Secure Internet Mail Access Protocol* (SIMAP). SIMAP adalah protokol yang berfungsi untuk pengamanan dalam mengakses email dari *server* dengan komunikasi yang lebih aman. Tertutup : Jika *port* ini tertutup maka dalam mengakses email dari *server* menjadi tidak aman.
995	Terbuka : *Port* ini merupakan *port* yang digunakan untuk *Port* ini merupakan *port* yang digunakan POP3 untuk menjalankan SSL/TLS. *Port* ini digunakan untuk menjalankan layanan POP3 yang terenkripsi, dan digunakan oleh *server* email. Tertutup : Jika *port* ini tertutup maka dalam mengakses email dari *server* menjadi tidak aman.
3306	Terbuka : *Port* ini merupakan *port* yang digunakan untuk *port* default dari protokol MySQL. *Port* ini digunakan sebagai penghubung dengan klien MySQL dan utilitas seperti mysqldump. Tertutup : Tidak dapat mengakses *database* karena tidak dapat terhubung dengan MYSQL

4.4 Hasil dan Analisis *Penetration Testing* SQl *Injection*

Pada pengujian ini menjelaskan hasil *penetration testing* SQL *Injection* yang termasuk kedalam OWASP 10 top risks menggunakan aplikasi SQLMap pada sistem operasi Kali Linux. SQL *Injection* adalah kegiatan menyerang sebuah *website* dengan memasukkan perintah-perintah SQL melalui url untuk dieksekusi oleh database, dimana penyerang dapat mengambil alih database[9]. Hasil dari pengujian penyerangan SQL *Injection* menggunakan SQLMap terhadap aplikasi berbasis *website* tap2go.cloudfri dengan memasukan perintah "sqlmap -u http://tap2go.cloudfri.id/ --dbs" sperti pada gambar berikut.

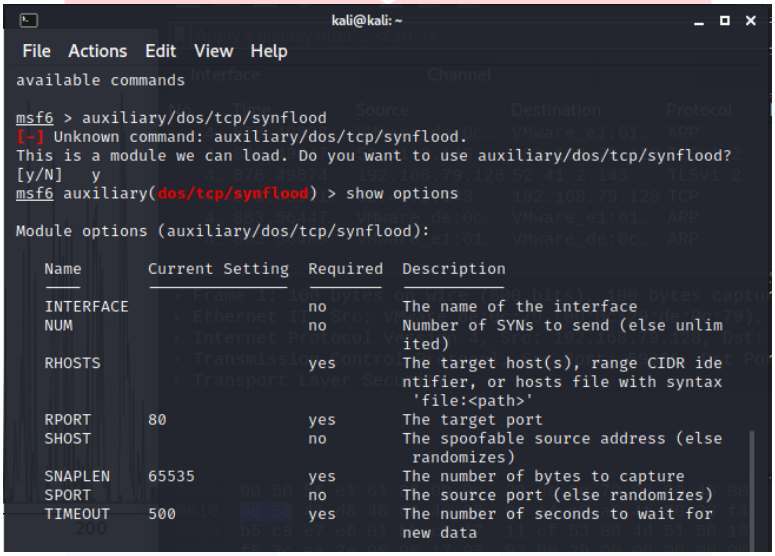


Gambar 4. 1 *Penetration Testing* SQl *Injection*

Dapat dilihat bahwa pada proses penyerangan SQL *Injection* menggunakan SQLMap dapat digagalkan karena *website* telah dilindungi oleh WAF/IPS. Pada Gambar V.6 terdapat pernyataan "WAF/IPS *identified as* Imunify 360 (CloudLinux) yang berarti imunify 360 merupakan sebuah WAF/IPS yang disediakan layanan hosting untuk melindungi *website* terhadap penyerangan SQL *Injection*.

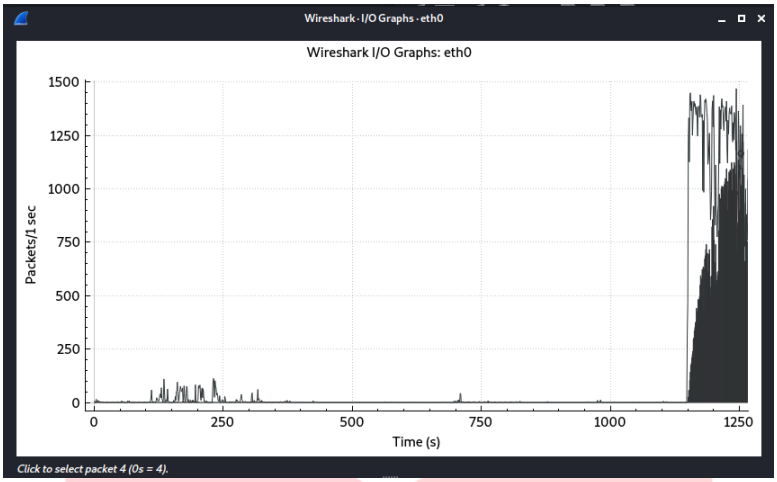
4.5 Hasil dan Analisis *Penetration Testing* DoS

Pada subbab ini menjelaskan implementasi *penetration testing* DoS yang termasuk kedalam OWASP 10 *top risks* menggunakan aplikasi yang dijalankan pada sistem operasi Kali Linux yaitu Metasploit *Framework* dan Wireshark sebagai alat untuk menganalisis detail lalu lintas jaringan pada saat proses eksploitasi DoS. Ekploitasi DoS yang dilakukan dengan aplikasi Metasploit adalah DoS SYN *Flooding*. DoS SYN *Flooding* adalah serangan yang bertujuan untuk mendistrupsi *traffic* dari sebuah *server*, layanan, atau jaringan, yang mengeksploitasi *three-way handshake* dari rangkaian koneksi TCP[10].



Gambar 4. 2 *Penetration Testing* DoS

Pada proses *penetration testing* DoS pada Metasploit Framework sudah terdapat modul untuk melakukan penyerangan DoS seperti yang terlihat pada Gambar V.7 dengan memasukan perintah "auxiliary/dos/tcp/synflood" untuk masuk kedalam modul tersebut. Sebelum menjalankan proses penyerangan perlu dilakukannya konfigurasi alamat IP target dan *port* yang dituju dengan memasukan perintah "set RHOSTS 193.1668.194.15" untuk konfigurasi alamat IP target, lalu memasukan perintah "set R*PORT* 53" untuk konfigurasi *port* target yang dituju, dalam pengujian penyerangan ini dilakukan terhadap *port* 53 dan 80 untuk menguji hasil *vulnerability* scanning yang telah dilakukan sebelumnya.

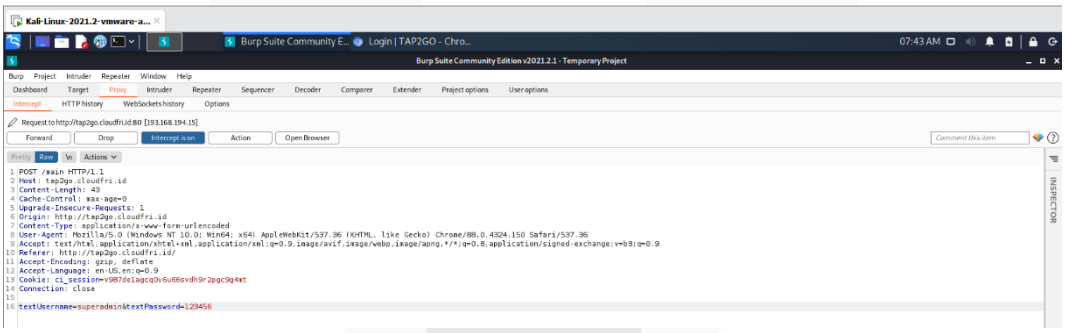


Gambar 4. 3 *Traffic* Saat Pengujian

Pada Gambar V.9 dapat dilihat bahwa setelah dilakukannya proses penyerangan rentang paket per detiknya mencapai kurang lebih 1000-1400 paket per detik, dengan perbedaan yang cukup signifikan tersebut dapat beresiko untuk menyebabkan *website* sulit untuk diakses oleh pengguna dan lumpuh karena kehabisan sumber daya selama penyerangan tersebut berlangung.

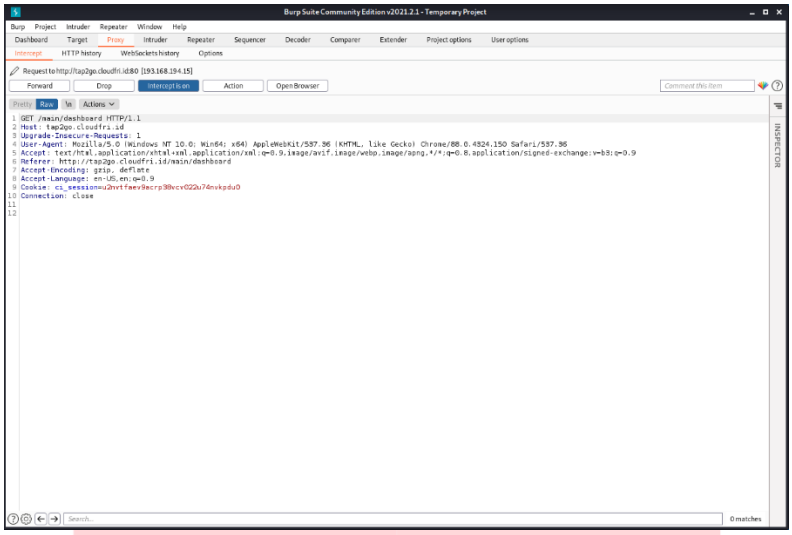
4.6 Hasil dan Analisis *Penetration Testing Interception* dan *Session Hijacking*

Pada subbab ini menjelaskan hasil implementasi *penetration testing Interception* menggunakan aplikasi Burp suite pada sistem operasi Kali Linux. *Interception* merupakan bentuk sebuah ancaman terhadap kerahasiaan data yang memungkinkan akan terjadinya kebocoran data, yang mana pihak yang tidak berhak berhasil mendapatkan hak akses untuk membaca suatu data atau informasi dari suatu sistem komputer. *Session Hijacking* adalah serangan yang pada dasarnya digunakan untuk mendapatkan akses tidak sah antara koneksi sesi resmi.



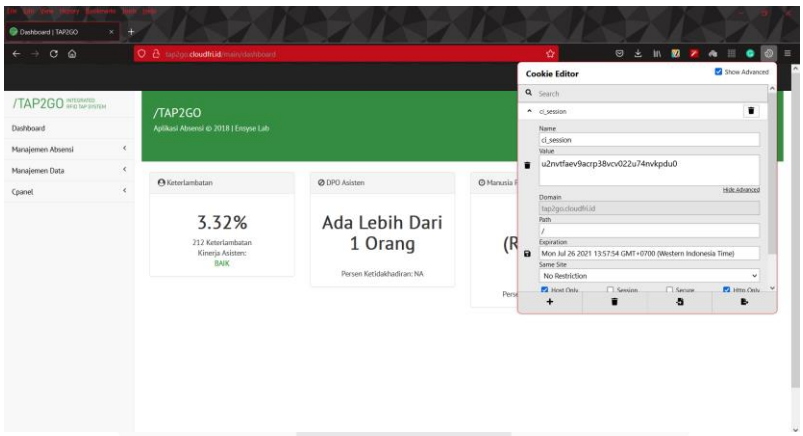
Gambar 4. 4 *Penetration Testing Interception*

Pada Gambar 4. 4 dapat terlihat setelah dilakukanya *intercept* dengan aplikasi Burp Suite terdapat informasi mengenai username dan password yang digunakan pada proses *login* tidak terenkripsi.



Gambar 4. 5 *Penetration Testing Session Hijacking*

Pada Gambar 4. 5 dapat terlihat bahwa *session cookie* pada url http://tap2go.cloudfri.id/main/dashboard dari percobaan *login* yang telah dilakukan sebelumnya pada saat proses *intercept.* Selanjutnya dilakukan percobaan login dengan *session cookie* yang telah didapat.



Gambar 4. 6 Percobaan *login* dengan *Session Cookie*

Pada Gambar 4. 6 dapat dilihat bahwa percobaan *login* pada web *browser* Main OS Windows 10 menggunakan *session cookie* yang diperoleh dari serangan *intercept* berhasil dilakukan.

5 Kesimpulan

Berdasarkan hasil dari pengujian dan analisis dapat disimpulkan beberapa hal berikut:

1. *Vulnerability scanning* yang dilakukan dengan *scanning tools* pada aplikasi berbasis *website* tap2go.cloudfri ditemukan beberapa celah keamanan yang memungkinkan untuk menjadi ancaman bagi *website* untuk kedepannya. Celah - celah keamanan yang ditemukan dari hasil *vulnerability scanning* yaitu kerentanan terhadap serangan DoS, komunikasi yang tidak terenkripsi yang memungkinkan terjadinya serangan MIM dan *session hijacking*, dan kerentanan berupa penggunaan SSL/TLS yang telah usang. Data yang didapat dari hasil *Vulnerability scanning* berupa *vulnerability*, *services*, dan *threat level* pada aplikasi berbasis *website* tap2go.cloudfri .
2. Dari hasil *penetration testing* yang telah dilakukan terhadap *vulnerability* yang terdapat pada aplikasi berbasis *website* tap2go.cloudfri memiliki dampak yang cukup merugikan bagi *website.* Pada pengujian penyerangan DoS SYN *Flooding* berhasil membuat *website* untuk sulit diakses sehingga layanan yang terdapat pada *website* menjadi terganggu. Pada

pengujian Interception didapati dalam komunikasi antara klien dengan server tidak melalui proses enkripsi sehingga memungkinkan akan terjadinya tindakan pencurian data seperti *username* dan *password.* Pada pengujian session hijacking berhasil melakukan proses login tidak sah pada *main* OS kedalam *website* menggunakan session cookie yang didapat dari pengujian intercept sebelumnya. Terdapat pula pengujian penyerangan SQL *Injection* yang gagal akibat adanya *firewall* imunify360 yang berjalan pada aplikasi berbasis *website* tap2go.cloudfri.

3. Prosedur *hardening* yang dilakukan pada pengujian ini sampai dengan tahap *remediate* dengan memberikan rekomendasi untuk meminimalisir celah keamanan yang terdapat aplikasi berbasis *website* tap2go.cloudfri. Rekomendasi yang dilakukan untuk meminimalisir celah keamanan ditemukan yaitu dengan mengkonfigurasi ulang web server seperti mematikan versi SSL/TLS yang telah usang, dan menggaktifkan fitur HSTS agar *website* memaksa *browser* untuk menggunakan koneksi HTTPS. Terdapatnya firewall imunify 360 pada aplikasi berbasis *website* tap2go.cloudfri sudah cukup untuk menahan serangan karena terdapat proses pemblokiran alamat *IP* jika terindikasi terdapat tindakan mencurigakan yang akan dilakukan kedalam *website*.

Referensi

[1] FRI. (2020, October 19). *CloudFRI Web Applications*. Diambil kembali dari CLOUDFRI: http://cloudfri.id/

[2] Laurensius Faleddo Giri Retza, A. (2016). SECURITY HARDENING DENGAN CLOUD WEB SERVICE UNTUK PENGAMANAN WEBSITE BERBASIS WORDPRESS. 4-7.

[3] Kristanto, A. (2014). *Panduan cPanel Web Hosting.* Jakarta: Elex Media.

[4] Kusnanto, Y. (2016). ANALISIS KERENTANAN DAN KEHANDALAN LAYANAN JARINGAN CLOUD BERBASIS PLATFORM EUCALYPTUS. *Jurnal Sistem Informasi*.

[5] Lee Badger, T. G.-C. (2012). Cloud Computing Definition. Dalam T. G.-C. Lee Badger, *Cloud Computing Synopsis and Recommendations.* Gaithersburg: NIST Special.

[6] David Harjowinoto, A. N. (t.thn.). Vulnerability Testing pada Sistem Administrasi . 2.

[7] Wardaya, M. S. (2019). Penetration Testing Terhadap Website Asosiasi Pekerja Professional Informasi Sekolah Indonesia. 28-31.

[8] Kurniawan, A. (2019). Penerapan Framework OWASP dan Network . *Jurnal Telematika*, 12.

[9] Andria. (2020). Analisis Celah Keamanan Website Menggunakan . *Generation Journal*.

[10] Nikhil Tripathi, B. M. (2013). DoS and DDoS Attacks: Impact, Analysis and. 1-5.

[11] Alan Hevner, S. C. (2004). Design Research in Information Systems Theory and Practice. Dalam S. C. Alan Hevner, *Design Research in Information Systems* (hal. Volume 22). New York: Springer.