BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi khususnya jaringan komputer pada saat ini telah menjadi hal yang *fundamental*. Teknologi informasi ditandai dengan lahirnya komputer dan perkembangannya yang sangat cepat Andrew R Molnar (1997:63). Seiring berjalannya waktu, teknologi telah berkembang menjadi lebih canggih. Ini dapat membantu dalam setiap kehidupan sehari-hari, baik dalam kegiatan industri maupun rumah tangga. Teknologi Informasi memiliki banyak manfaat ada untuk transportasi, komunikasi, pendidikan, dll. Semakin cepatnya perkembangan suatu informasi menyebabkan banyaknya kemungkinan aksi *hacking* dan *data-sniffing*. Serangan–serangan tersebut perlu dihindari untuk menghindari kerusakan ataupun kehilangan data pada *website*. Salah satu upaya untuk membangun keamanan data dalam jaringan internet adalah dengan menggunakan Metode *Hardening*

Penggunaan *Hardening* dibutuhkan untuk pengamanan sistem. *Hardening* berguna untuk menutup celah–celah yang rentan diserang oleh para *hacker*. Penutupan celah–celah inilah yang membuat sistem jadi sulit untuk diserang. *Hardening* bisa digunakan pada semua sistem, termasuk sistem *cloud*fri Telkom University.

*Cloud*fri merupakan sistem yang berisi kumpulan aplikasi yang digunakan oleh seluruh entitas Fakultas Rekayasa Industri Universitas Telkom yang mana didalamnya terdapat beberapa *web applications* seperti administrasi.cloudfri.id, ingram.cloudfri.id, labrecruitment.cloudfri.id, tap2go.cloudfri.id, dst. Penggunaan metode *Hardening* pada *cloudfri* dinilai bisa untuk menghindari kerusakan, pengubahan, atau pencurian data pada aplikasi yang terdapat pada sistem *cloudfri***.** Hal ini dilakukan untuk menjaga stabilitas dan kinerja sistem *cloudfri***.**

Metode *hardening* yang dilakukan pada *cloud*fri menggunakan metode *security hardening*. Dimana *security hardening* ini memiliki empat tahapan, yaitu *access, analyze, remediate,* dan *manage*. Tahapan ***access*** berguna untuk mencari suatu

celah keamanan yang masih terdapat di dalam suatu sistem, tahap ***analyze*** berguna untuk mencari tingkat keamanan dan menganalisis dampak yang terjadi pada celah keamanan tersebut, kemudian mengelompokan tingkat kerusakan yang diakibatkan oleh celah keamanan tersebut. tahap ***remediate*** berguna untuk menemukan celah keamanan pada sistem yang diuji dan mencari cara untuk menutup celah keamanan tersebut untuk mengamankan sistem, dan tahap ***manage*** yang berguna untuk menutup lubang keamanan dan mencegah serangan masuk, serta mencegah terbukanya celah keamanan lain.

Tujuan dari metode *hardening* yang dilakukan pada c*loud*fri adalah untuk menegakkan keamanan data, membersihkan file sampah, menutup *port* yang tidak digunakan, dan menutup lubang keamanan lainnya. maka sistem tersebut akan sulit diserang karena celah–celah yang ada pada sistem sudah ditutup. Hal ini membuat sistem ***cloudfri*** akan lebih stabil karena tidak ada gangguan terhadap sistem tersebut.

I.2 Perumusan Masalah

Berdasarkan masalah yang telah uraian dari latar belakang sebelumnya, maka rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana mengindetifikasi apa saja *vulnerability* yang terdapat pada *website TAP2GO (Cloud FRI)*?
2. Bagaimana cara memperkuat keamanan pada *website TAP2GO (Cloud FRI)*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui *vulnerability* apa saja yang terdapat pada *website Tap2go (Cloud FRI)*.
2. Merekomendasikan bagaimana cara untuk menutup celah atau *vulnerability* yang ditemukan pada *website Tap2go (Cloud FRI)*.

I.4 Batasan Penelitian

Adapun batasan masalah pada penelitian ini adalah sebagai berikut :

1. Penelitian ini hanya berfokus kepada keamanan data yang terdapat dalam aplikasi yang disediakan *Cloud*FRI.
2. Penelitian ini menggunakan metode *security hardening* untuk mengidentifikasi celah keamanan pada website *Tap2go* (*cloud*FRI)
3. Penelitian ini melakukan identifikasi dan rekomendasi pada celah keamanan yang terdapat di *Cloud*FRI.

I.5 Manfaat Penelitian

1. Untuk Institusi

Dari hasil penelitian yang telah dilakukan, Instansi akan mendapatkan manfaat dari aplikasi web yang aman.

2. Untuk Pengguna

Manfaat yang diperoleh pengguna adalah terciptanya rasa aman dari pencurian data.

3. Untuk Peneliti

Penelitian ini dapat menambah wawasan bagi peneliti, dan peneliti dapat mengimplementasikan ilmu yang didapat dan dipelajari dari perkuliahan.