# BAB I PENDAHULUAN

## I.1 Latar Belakang

Perkembangan jumlah dan penggunaan *website* pada era teknologi informasi saat ini menunjukan peningkatan yang pesat. Banyak *website* digunakan untuk saling berbagi informasi antara satu sama lain. *Website* banyak digunakan karena *flexible* dan mudah pemakaiannya. Seseorang hanya membutuhkan waktu beberapa menit untuk membuat maupun membuka suatu *website*. Hal inilah yang menyebabkan perkembangan *website* meningkat.

Dengan mudahnya pembuatan dan penggunaan *website*, maka akan mudah juga suatu website *diretas* (*hack*) oleh *hacker*. Banyak ribuan *website* telah diretas oleh *hacker*. *Website* Pemerintahan dan Pendidikan menjadi target yang diminati oleh para *hacker* untuk dilakukan *deface*.


Gambar I.1 Statistik Web *Deface* Zone-H pada Domain ID (Doel, 2016)

Melihat dari Gambar I.1, maka bisa diketahui banyak website yang sudah di-*deface* oleh para *hacker*. Dengan banyaknya peretasan pada *website* maka dibutuhkan pengamanan data.

Pengamanan data ini perlu dilakukan untuk menghindari serangan dari *hacker*, *cracker*, dan sejenisnya yang bermaksud untuk mencuri atau merubah data yang ada pada *website*. Terdapat banyak serangan yang bisa dilakukan kepada *website*, contohnya seperti: Phising, DoS, Bruteforce Attack, Defacing, dan masih banyak lagi.

Serangan – serangan tersebut perlu dihindari untuk menghindari kerusakan ataupun kehilangan data pada website. Untuk menghindari suatu serangan, banyak cara yang dapat dilakukan, seperti: menggunakan Firewall, Two Step Authentication, SSL, atau melakukan *Hardening*.

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

Cloudfri merupakan sistem yang berisikan kumpulan aplikasi yang digunakan oleh keseluruhan entitas Fakultas Rekayasa Industri Telkom University. Melakukan *hardening* pada cloudfri diperlukan untuk menghindari pengerusakan, perubahan, maupun pencurian data pada aplikasi yang terdapat pada sistem cloudfri. Hal ini dilakukan untuk menjaga kestabilan dan kinerja dari sistem cloudfri.

*Hardening* yang dilakukan pada cloudfri bisa menggunakan metode *security hardening*. Dimana *security hardening* ini memiliki empat tahapan, yaitu *access*, *analyze*, *remediate*, dan *manage*. Tahapan *access* berguna untuk mencari celah keamanan pada sistem, tahap *analyze* berguna untuk menganalisis tingkat keamanan dan dampak dari celah pada sistem, tahap *remediate* berguna untuk mencari cara untuk menutup celah yang ditemukan pada sistem, dan tahap *manage* yang berguna untuk menutup celah yang ada pada sistem. Cara ini digunakan untuk menghindari serangan terhadap cloudfri yang dapat memberikan kerugian kepada Fakultas Rekayasa Industri.

Untuk menemukan celah – celah yang terdapat pada cloudfri bisa dilakukan dengan cara melakukan *scanning vulnerability*. *Scanning* ini bertujuan untuk memberikan informasi *vulnerability* apa saja yang terdapat pada cloudfri. Setelah *vulnerability* diketahui, maka selanjutnya dapat dilakukan analisis *vulnerability* berdasarkan *threat level* pada *vulnerability* tersebut. Hasil analisis yang didapat bisa dijadikan sebagai acuan dalam melakukan *hardening* pada cloudfri.

Setelah melakukan *hardening* pada sistem cloudfri dengan mengacu pada *vulnerability* yang didapat, maka sistem cloudfri akan sulit diserang karena celah –

celah yang ada pada sistem sudah ditutup. Penutupan celah yang terdapat pada cloudfri akan menghasilkan keamanan lebih pada cloudfri. Hal ini dikarenakan cloudfri sudah menutup jalur yang kemungkinan akan dilakukan penyerangan oleh hacker. Hal ini juga membuat sistem cloudfri akan lebih stabil karena tidak ada gangguan terhadap sistem tersebut.

## I.2 Perumusan Masalah

Berdasarkan uraian dari latar belakang di atas, maka rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana mengetahui celah yang ada pada sistem *cloudfri*?
2. Bagaimana cara melakukan penutupan celah yang terdapat pada sistem *cloudfri*?
3. Bagaimana cara melakukan *hardening* pada celah yang terdapat pada sistem *cloudfri*?

## I.3 Tujuan Tugas Akhir

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

1. Mengetahui celah yang terdapat pada sistem *cloudfri* Fakultas Rekayasa Industri Telkom University.
2. Melakukan penutupan celah yang terdapat pada sistem *cloudfri*.
3. Melakukan *hardening* pada sistem yang sudah dilakukan penutupan untuk pengamanan data di *cloudfri*.

## I.4 Batasan Tugas Akhir

Adapun batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini melakukan *hardening* pada *website* savsoftquiz.cloudfri.id.
2. Penelitian ini hanya berfokus pada keamanan data yang terdapat dalam aplikasi yang disediakan *cloudfri*.
3. Pada penelitian ini pembahasan *cloud computing* hanya pada *cloud hosting*.

4. Pada penelitian ini *hardening* yang dilakukan hanya sampai tahap *remediate*.
5. Standar keamanan yang digunakan adalah OWASP.

## I.5 Manfaat Tugas Akhir

1. Bagi institusi

   Hasil dari penelitian diharapkan dapat memberikan manfaat pada Fakultas Rekayasa Industri Telkom University terhadap keamanan data di sistem *cloudfri*.

2. Bagi Masyarakat

   Hasil dari penelitian diharapkan dapat menambah pengetahuan tentang pentingnya mengamankan suatu sistem dengan menggunakan metode *hardening* untuk menghindari perusakan, perubahan, ataupun pencurian data.

3. Bagi Peneliti

   Hasil dari penelitian ini dapat menambah pengetahuan dan pengalaman di bidang Keamanan Data dan berguna sebagai referensi untuk penelitian selanjutnya.

## I.6 Sistematika Penulisan

Adapun sistematika penulisan dari penelitian adalah sebagai berikut:

**Bab I Pendahuluan**

Berisi mengenai uraian latar belakang, perumusan masalah, tujuan tugas akhir, batasan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

**Bab II Tinjauan Pustaka**

Berisi tentang penjelasan dan kutipan yang relevan dengan permasalahan yang dihadapi dan juga teori – teori yang digunakan seperti *hosting*, *cloud computing*, keamanan data, dan *security hardening*.

**Bab III Metodologi Penelitian**

Berisikan model untuk merumuskan solusi dari permasalahan yang ada serta penjelasan secara rinci mengenai tahapan – tahapan dari penelitian ini.

**Bab IV Perancangan Sistem**

Berisikan penjelasan mengenai *hardware*, *software*, dan skenario praktik yang dilakukan saat penelitian.

**Bab V Analisa Hasil dan Evaluasi**

Berisikan penjelasan mengenai setiap hasil yang diperoleh dari penelitian disertai dengan analisis.

**Bab VI Kesimpulan dan Saran**

Berisikan kesimpulan serta saran untuk penelitian selanjutnya.