BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Di era modern ini, teknologi sangat berkembang pesat dan bertumbuh dari jam ke jam. Maupun itu teknologi di bagian *Software* atau *Hardware*. Di internet sendiri kita bisa menjumpai *traffic* dari pentrasferan data-data privasi dari *user* pada web-web besar, katakanlah amazon, facebook, google, dan web besar lainnya. Tentu semakin banyak data yang mereka simpan, semakin besar juga tanggung jawab yang harus terima untuk menjaga data dari pelanggan atau yang biasa kita sebut *user*. Informasi tidak boleh bocor atau di akses oleh orang yang tidak bertanggung jawab. Jika bocor, itu akan merugikan dari pihak pengelola web dan *user* itu sendiri. Khususnya kata sandi atau *password* dari para user. Salah satu serangan yang biasa di gunakan dalam eksploitasi *password* yaitu dengan *Rainbow Table attack*. Dan di area login web biasanya menggunkan *CSRF attack*. Maka dari itu kita membutuhkan sebuah konsep atau skema keamanan data untuk melindungi web itu dari serangan-serangan dari luar web.

Guru ngaji merupakan sebuah komunitas lokal di sleman yang bertujuan untuk mengumpulkan para pengajar ngaji. Secara umum para pengajar akan mendaftarkan diri di dalam web tersebut. Tentu saja *password* mereka yang merupakan suatu hal yang sensitif harus di jaga kerahasiannya. Karena jikalau *password* mereka di curi, bisa saja di manfaatkan oleh oknum yang tidak bertanggung jawab. Di mana biasanya *password* seorang yang telah di curi akan di manfaatkan, seperti kata sandi akan di ubah, data akan di ambil dan di manfaatkan untuk melakukan penipuan atas nama kan user yang datanya telah di curi tersebut.

Di butuhkan sebuah keamanan data untuk menjaga data tersebut aman oleh serangan dari pihak luar yang tidak berwenang. Kriptografi adalah ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Dalam ilmu kriptografi terdapat proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan atau informasi yang asli(*plaintext)* menjadi suatu pesan dalam bahasa sandi yang susah di baca atau tidak di kenali oleh manusia(*ciphertext)*, sedangkan dekripsi adalah sebuah proses mengubah atau mengembalikan pesan yang sudah di enkripsi menjadi pesan aslinya.

Upaya untuk meningkatkan keamanan data pada website guru ngaji ini untuk mencegah dari serangan *Rainbow Table* dan *CSRF*, salah satunya dengan menerapkan *Algoritma RSA, Secure Hash Algorithm, dan Token based Mitigation*. Pencegahan ini di ketahui dapat menghambat dari kedua serangan tersebut. Sehingga *password* dan hak akses dari login dapat terjaga kemanannya oleh pihak yang tidak berwenang. Berdasarkan beberapa sumber kenapa kita harus menggunkan Algoritma RSA,Secure Hash Algorithm, dan Token-based Mitigation untuk keamanan web ini yaitu :

1. *Algoritma RSA* merupakan kriptografi asimetris yang menggunakan sebuah sepasang kunci, yaitu kunci publik dan kunci pribadi. Kemanan *Algoritma RSA* terletak pada sulitnya memfaktorkan bilangan prima.

2. *Secure Hash Algorithm* merupakan salah satu fungsi hash yang di nyatakan oleh NIST sebagai fungsi hash yang masih layak di gunakan untuk standar keamanan data. Fungsi hash adalah fungsi yang bekerja secara satu arah, yaitu dengan mudah dapat menghitung hash value dari pre-image, tetapi sangat sukar untuk menghitung pre-image dari hash value.

3. *Token-based Mitigation* adalah konsep yang sangat sederhana untuk mengurangi risiko diserang melalui *CSRF*. Di sebagian besar aplikasi web, server menggunakan objek sesi HTTP untuk mengidentifikasi pengguna yang masuk. Dalam hal ini, sesi dibuat di sisi server dan memberikan ID

sesi kepada klien. ID sesi ini adalah sebagian besar file cookie sisi klien. Karena sesi ini ID disimpan di file cookie sisi klien, jika cookie tidak dilindungi dengan konfigurasi lanjutan (httponly, samesite, secure, dll), dimungkinkan untuk mengakses cookie ini dari halaman lain yang memiliki browser terbuka.

1.2 RUMUSAN MASALAH

Dari latar belakang yang telah di jelaskan di atas bisa kita simpulkan rumusan masalahnya yaitu :

- Bagaimana menerapkan *Algoritma RSA dan Secure Hash Algorithm* untk mengamankan login dan password.
- Bagaimana menerapkan *Token-Based Mitigtion* pada login page.

1.3 BATASAN MASALAH

Dari rumusan di atas, terdapat beberapa batasan dalam menyelesaikan skripsi ini yaitu :

- Penerapan sistem keamanan hanya pada *Login Page* dan *Password*
- Panjang kunci yang di gunakan dalam Algoritma RSA yaitu 2048 bit.
- Fungsi Hash yang di gunakan adalah SHA2 yang mempunyai panjang bit 256 bit.
- Otentikasi yang diamanin hanya pada sisi admin.

1.4 TUJUAN PENELITIAN

Tujuan dari penelitian ini yaitu:

- Password yang di simpan dalam database menjadi lebih aman dengan menggunakan kriptografi.

- Hak akses dari Login Page menjadi lebih aman.

- Meningkatkan nilai *confidentiality* dan *Data Integrity* pada website ini.

1.5 MANFAAT PENELITIAN

Di harapkan dengan penerapan kriptografi ini pada sistem login dan password, bisa meningkatkan mutu keamanan pada web tersebut.

1.6 METODE PENILITIAN

Metode penelitian di gunakan untuk memudahkan kita untuk melakukan pencarian data-data maupun teori-teori pendukung skripsi ini. Dengan penerapan metode penelitian ini, skripsi lebih terarah sesuai tujuan dan rumusan masalahnya.

1.6.1 Metode Pengumpulan Data

Metode pengumpulan informasi dan data yang di gunakan dalam penelitian ini di antaranya :

1.6.1.1 Metode Observasi

Di tahap ini saya melakukan pengamatan secara langsung pada objek tentang keamanan login dan password yang telah di terapkan di dalam web tersebut untuk pengembangan selanjutnya.

1.6.1.2 Metode Literatur

Pada tahap ini dilakukan untuk mencari dan mempelajari sumber-sumber ilmu dari buku, jurnal, dan internet yang berkaitan dengan penerapan kriptografi ini.

1.6.2 Metode Perancangan

Merupakan tahapan dalam merancang proses yang terjadi Didalam sistem. Adapun metode perancangannya yang dilakukan adalah sbg berikut: Merancang *flowchart* untuk mem-visualisasikan proses yang terjadi dalam sistem.

1.7 SISTEMATIKA PENULISAN

Untuk memperoleh gambaran yag mudah di mengerti dan komperehensif mengenai isi dari penulisan skripsi ini , secara garis besar dapat di lihat dari penulisan di bawah ini :

BAB I : PENDAHULUAN

Pada BAB I membahas tentang kerangka penuisan dan meliputi latar belakang masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada BAB II berisi tentang tinjauan pustaka serta teori-teori yang berasal dari studi literatur seperti buku, jurnal, buku, dan internet yang mengacu pada standarisasi keaman di kriptografi. Di mana ini akan menjadi panduan atau landasan teori yang akan di pakai untuk membuat keamanan data pada web ini.

BAB III: ANALISIS DAN PERANCANGAN

Pada BAB III berisi tentang bagaimana menganalisa dan membangun keamanan pada *Login Web* dan *Password*.

BAB IV: HASIL DAN PEMBAHASAN

Pada BAB IV berisi tentang tata cara pembuatan dan urutan- urutan dalam kriptografi ini, dan juga hasil yang di peroleh dari proses pembuatan ini.

BAB V : PENUTUP

Pada BAB V, ini adalah bab terakhir dan berisi tentang kesimpulan, saran, dan daftar pustaka untuk hasil dari kriptografi ini.