# **BAB I PENDAHULUAN**

## Latar Belakang Masalah

*Website* atau yang kita kenal dengan situs web merupakan sarana yang digunakan untuk menyebarkan informasi melalui internet, baik berupa teks, gambar, suara, maupun video. Seiring penggunaan situs web yang semakin luas, dapat menimbulkan banyak macam tindak kejahatan seperti pencurian, manipulasi data atau informasi penting oleh orang yang tidak bertanggung jawab yang mana merupakan ancaman kebocoran pada suatu situs web tersebut. Sehingga dibutuhkan pengamanan lebih untuk menjaga data atau informasi penting tersebut.

Dokumen-dokumen informasi yang terdapat pada situs web dihubungkan melalui alamat *URL (Uniform Resource Locator)*. Di dalam *URL*, terdapat alamat server, lokasi, dan nama-nama dokumen yang terdapat pada situs web tersebut. *URL* situs web dapat digunakan untuk memberikan berbagai macam perintah terhadap basis data yang terdapat pada server situs web tersebut. Oleh karena itu, *URL* situs web sering digunakan sebagai media untuk melakukan tindak kejahatan terhadap suatu situs web tersebut. Berbagai macam cara dapat dilakukan untuk meretas suatu situs web, cara yang banyak digunakan adalah dengan menggunakan metode *SQL (Sequence Query Language) Injection*. *SQL Injection* menjadi sangat terkenal di Indonesia semenjak dibobolnya situs Komisi Pemilihan Umum (KPU) pada Pemilihan Umum (Pemilu) tahun 2004 lalu.

Metode *SQL Injection* digunakan untuk memasukkan perintah *SQL* sebagai input pada suatu situs web untuk mendapatkan hak akses ke dalam basis data. Jika basis data situs web dapat diakses, maka seorang *hacker* dapat dengan mudah mencuri berbagai data rahasia, bahkan dapat memanipulasi atau merusak data pada situs web tersebut. Salah satu cara yang dapat digunakan untuk mengamankan suatu situs web dari serangan *SQL Injection* adalah dengan ilmu kriptografi. Ilmu kriptografi adalah ilmu yang digunakan untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Banyak sekali metode dari ilmu kriptografi tersebut, dan setiap metode memiliki keunikan tersendiri antara satu dengan yang lainnya. Dengan ilmu tersebut, *URL* pada situs web dapat disamarkan menjadi kode atau sandi yang tidak dapat dibaca oleh sembarang orang, sehingga dapat mencegah serangan *SQL Injection* pada suatu situs web.

Kriptografi yang digunakan adalah kriptografi *BASE64* yang mana akan digunakan sebagai sistem keamanan untuk mengatasi ancaman terhadap serangan SQL Injection yang menggunakan metode *Union Based SQL Injection* dan *Blind SQL Injection*. Kriptografi ini dapat menyamarkan kode atau sandi dengan cepat, dan juga mudah untuk digunakan agar pengamananan terhadap situs web menjadi lebih maksimal.

Setelah melihat latar belakang di atas, maka penulis tertarik dengan topik *security* yang menggunakan kriptografi untuk menciptakan sistem keamanan yang lebih terjamin untuk menjaga data-data agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

## Identifikasi Masalah

Berdasarkan uraian latar belakang di atas, maka dapat disebutkan beberapa permasalahan yang dapat diidentifikasi adalah sebagai berikut :

1. Banyak pengembang situs yang masih kurang *aware* terhadap keamanan suatu situs.
2. Kurangnya pengetahuan pengembang situs mengenai keamanan situs webnya.
3. Pihak yang tidak berkepentingan dapat menggunakan hak akses dan penyalahgunaan data.
4. Banyaknya data konfidensial yang terancam kebocorannya, dalam hal ini dapat dilihat dari bobolnya situs web KPU pada tahun 2004.
5. Penggunaan kriptografi yang masih belum banyak digunakan pada *URL* situs web yang mana kriptografi yang digunakan adalah *BASE64*.
6. Menangani serangan *Union Based* *SQL Injection* dan *Blind SQL Injection* terhadap *database* situs web tersebut.

## Batasan Masalah

Berdasarkan hasil identifikasi masalah dan agar penelitian ini dapat dilakukan lebih fokus dan mendalam, penelitian ini dibatasi pada :

1. Penggunaan kriptografi yang masih belum banyak digunakan pada *URL* situs web yang mana kriptografi yang digunakan adalah *BASE64*.
2. Banyaknya data konfidensial yang terancam kebocorannya, dalam hal ini dapat dilihat dari bobolnya situs web KPU pada tahun 2004.
3. Menangani serangan *Union Based* *SQL Injection* dan *Blind SQL Injection* terhadap *database* situs web tersebut.

## Tujuan Penelitian

Setiap penelitian pasti memiliki tujuan yang ingin dicapai. Hal ini dimaksudkan agar pelaksanaan penelitian ini dapat memiliki target yang jelas, maka tujuan dalam penelitian ini yaitu :

1. Mengetahui tingkat keamanan dari situs yang diuji.
2. Menerapkan metode kriptografi *BASE64* untuk meningkatkan proteksi sistem keamanan.

## Manfaat Penelitian

Penulis berharap agar penelitian ini dapat bermanfaat bagi para instansi / perusahaan, penulis, dan pembaca.

1. Instansi / perusahaan :
   * + 1. Instansi dapat memahami bahwa terdapatnya kerentanan pada *URL Website*.
       2. Instansi dapat memperbaiki dan memperkuat keamanan situs web dengan menerapkan kriptografi *BASE64.*
2. Penulis :

Penulis dapat membantu mengingatkan kepada semua pihak bahwa data itu sangat penting dan lebih diperketat keamanannya.

* + 1. Penulis dapat belajar lebih dalam, dan menemukan cara untuk lebih meningkatkan keamanan data.

1. Pembaca :
   * + 1. Pembaca dapat sadar akan bahaya dari risiko yang ada, sehingga akan lebih waspada dan berhati-hati dalam menggunakan situs tersebut.
       2. Pembaca dapat lebih memahami mengenai *IT Security* dan metode yang ada.
       3. Pembaca dapat lebih memahami peningkatan keamanan dengan metode kriptografi *BASE64.*