BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan menjadi salah salah satu bagian penting dari sebuah sistem yang harus menjadi prioritas, karena jika sistem keamanan diabaikan akan memungkinkan serangan mudah dilakukan terhadap sebuah sistem. Hal demikian pula berlaku pada sistem informasi berbasiskan pada aplikasi *web*. Aplikasi *web* adalah sebuah sistem yang dapat berjalan pada platform *webbrowser* yang menggunakan *webserver* untuk memproses permintaan dan sebuah bahasa *scripting* yang digunakan untuk melakukan proses bisnis sebuah sistem. Umumya komponen dari sebuah sistem aplikasi *web* sangat menyesuaikan dengan kebutuhan, bisa tidak menggunakan *webserver*, bisa tidak menggunakan *databaseserver*, bisa menggunakan bahasa *scripting* php atau yang lainya.

Dalam tampilanya, aplikasi *web* dalam sebuah *browser* pasti terdapat URL yang menandakan alamat dari sistem atau alamat dari sebuah proses. Karena pengembangan dari aplikasi *web* ini sangat *custom* dan metode pengembangan mengikuti kebiasaan dari pengembang, maka dari itu ada pengembang yang memang sengaja menyembunyikan alamat URL dari sebuah proses dan ada juga yang secara terang-terangan tetap menampilkan URL utuh dari sebuah proses bisnia. Akan tetapi keamanan dari sebuah apliasi *web* tidak bisa diukur hanya dari terlihat atau tidak terlihatnya sebuah URL utuh sebuah proses.

Banyak kasus serangan terhadap sebuah layanan aplikasi *web* yang memanfaatkan kelemahan dari parameter URL yang tingkat keamananya belum dimaksimalkan.Contoh serangan yang bisa memanfaatkan celah dari parameter URL ini adalah *SQL Injection*.*SQL Injection* adalah salah satu jenis serangan terhadap sebuah sistem dengan mengubah parameter URL secara langsung untuk memanipulasi data, diantaranya dapat mengakses *database* secara langsung maupun mengambil kontrol atau hak akses yang sebenarnya tidak diperbolehkan.

Salah satu metode untuk mengamankan parameter URL adalah dengan melakukan *hashing, encoding,* enkripsi, maupun kombinasi dari ketiganya. Banyak orang salah dalam menganggap ketiga istilah tersebut, karena ketiganya mempunyai fungsi yang hampir sama, yaitu terkait dengan fungsi penyandian sebuah data. Enkripsi adalah penyandian sebuah data menjadi bentuk yang tidak bisa dibaca secara langsung dan mempunyai kunci untuk membukanya.*Encoding* adalah penyandian sebuah data menjadi bentuk yang tidak bisa dibaca secara langsung, tetapi tidak membutuhkan kunci untuk membukanya.Sedangkan *hashing* adalah penyandian sebuah data menjadi bentuk yang tidak bisa dibaca secara langsung dan tidak bisa dikembalikan menjadi data asli. Pada *hashing* ini, perubahan satu karakter akan berdampak banyak pada hasil akhirnya. Contoh dari enkripsi adalah *caesar* dan lain sebagainya, contoh dari *encoding* adalah *base64*, dan contoh dari *hashing* adalah *MD5*.

1.2 Rumusan Masalah

Berisi tentang kalimat yang menegaskan apa yang menjadi masalah dalam penyelesaian penelitian. penulisan diawali dengan kalimat pengantar dan masalah dituliskan dalam pointer.

Rumusan masalah yang dapat didefinisikan dalam penelitian ini diantaranya adalah sebagai berikut:

1. URL dapat dimanipulasi untuk merubah data atau merubah proses bisnis dari sebuah sistem
2. URL dapat dimanipulasi untuk melihat halaman yang tidak boleh diakses oleh user tertentu
3. URL dapat dimanipulasi untuk melihat atau mengubah data yang tidak boleh dilihat oleh user tertentu

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengimplementasikan algoritma *base64* yang dikombinasikan dengan *hashing MD5* untuk mengamankan sebuah URL aplikasi berbasis *web*.

1.4 Manfaat Penelitian

Manfaat penelitian ini secara umum adalah untuk meningkatkan keamanan dari sebuah sistem aplikasi berbasis *web*.Keamanan yang ditingkatkan adalah berfokus pada keamanan manipulasi URL untuk tujuan yang dilarang oleh sistem.Adapun manfaat penelitian secara khusus diantaranya adalah sebagai berikut.

1. *Website* akan menampilkan error atau data tidak tampil atau akan dialihkan jika URL salah. Ini akan mengurangi resiko tidak aman dari aplikasi berbasis *web* dimana pengguna dapat melihat halaman yang tidak diperbolehkan untuk dilihat.
2. *Website*tidak bisa diubah proses bisnisnya. Misalnya dalam URL terdapat aksi untuk melakukan *edit* terhadap data dengan id tertentu, maka aksi itu tidak dapat diubah menjadi aksi *delete* atau tambah data.
3. Data pada *website* tidak bisa diubah tanpa melalui prosedur yang disediakan. Misalnya dalam aksi *edit* data dengan id tertentu, pengguna tidak bisa mengubah id tersebut untuk diubah.

1.4 Batasan Masalah

Dalam penelitian ini tidak semua berlaku atau tidak semua dapat diterapkan pada berbagai kasus. Batasan-batasan dalam penelitian ini adalah:

1. Penelitian ini hanya bertujuan untuk mengamankan URL dari injeksi URL
2. Penelitian ini tidak sampai pada penanganan keamanan database maupun *server*
3. Penelitian ini dilakukan dengan menggunakan data user sebagai bahan uji
4. Penelitian ini mengimplementasikan algoritma yang sudah ada dengan menambahkan beberapa teknik pengamanan.