BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era sekarang internet sudah bukan menjadi hal baru atau asing, dari anak kecil sampai orang tua pun sudah mengetahui, *website* atau situs yang merupakan salah satu bagian dari internet juga telah menjadi bagian bagi manusia, karena *website* dapat menyediakan sebuah in*form*asi yang dapat dijangkau dengan mudah bagi yang memiliki akses layanan internet.

Website adalah sebuah layanan di suatu domain internet yang terdiri dari 1 atau lebih halaman untuk tujuan tertentu yang dapat diakses oleh orang di dunia maya (Waryanto, 2018). Perkembangan *website* sampai sekarang telah meluas fungsinya, tidak hanya menyediakan in*form*asi namun kita dapat berinteraksi di dalamnya yaitu adanya aplikasi yang dibangun berbasis *website* atau biasa disebut *web application*. *Web application* di dalamnya memuat sebuah proses dinamisasi dengan cara mengambil in*form*asi dari database yang kemudian ditampilkan ke dalam halaman web. Dalam *web application* ini terkadang di dalamnya terdapat sebuah data – data yang dilindungi bahkan dirahasiakan, dan data tersebut hanya bisa diakses oleh orang yang diberi hak akses khusus untuk mengaksesnya.

Namun sebuah *website* bisa juga rentan terhadap serangan – serangan yang terjadi pada sistem keamanan yang ada pada sebuah *website*, jikalau *website* tidak mempunyai sistem keamanan atau sistem keamanan yang dimiliki *website* itu lemah maka ancaman dapat terjadi sewaktu waktu, ancaman ini dapat merugikan karena orang lain dapat mengetahui *user* dan *password* dari admin lalu masuk dan bisa saja merusak *website* bahkan mencuri data – data rahasia. Orang lain yang dapat masuk ke halaman admin tentu memanfaatkan celah keamanan yang ada pada sebuah *website*. Masalah keamanan ini sering tidak mendapat perhatian dari pengelola sistem in*form*asi bahkan kadang terabaikan dan bahkan berada di urutan kedua atau urutan

terakhir dari daftar hal hal yang dianggap penting (Ariyus, 2009).

Celah yang terdapat pada sistem disebut dengan *vulnerability* yaitu suatu celah pada sistem yang menyebabkan terjadinya orang lain yang masuk dengan mengeksploitasi sistem tersebut. Maka dari itu perlu adanya sistem sebagai peringatan dini ketika situs yang dimiliki diserang oleh peretas.

Masalah yang terdapat pada penelitian ini yaitu bagaimana membuat mekanisme keamanan *system server* sehingga penanganan berada di awal bukan lagi di belakang menunggu *system* rusak atau dieksploitasi, maka di sini peneliti akan membuat sebuah mekanisme keamanan dimana apabila seseorang mengaskses situs asli yang diserang maka akan diarahkan pada situs palsu namun berisi hal yang sama.

Cross-site scripting atau disebut xss, salah satu teknik serangan pada *website* ini yaitu xss merupakan serangan yang dilakukan pada *website* yang tidak perlu melakukan sebuah validasi dan sanitasi (Syaifuddin, Diah dan Hanugra. 2018), peretas dapat memanfaatkan hal itu dengan memasukan sebuah kode atau *script* yang dikirimkan pada *server*, salah satu *script* tersebut bila bekerja dapat mem-*bypass* akun serta keamanan.

Intrusion Detection System (IDS), Menurut Onno Purbo(2010), IDS adalah usaha untuk mengidentifikasi adanya peretas yang memasuki sistem tanpa adanya hak akses atau totrisasi (misal cracker) atau seorang pengguna yang legal namun sumberdaya sistemnya di salah gunakan. IDS dalam penelitian ini akan digunakan sebagai pendeteksi serangan xss.

Selain itu untuk penelitian ini juga mengevaluasi tingkat kerentanan situs terhadap serangan xss dengan mengukur seberapa besar dampak serangan xss pada *website* dengan perhitungan CVSS *(Common Vulnerability Scoring System)* versi 2 dengan kelompok *base metric*. *Base metric* ini hasilnya dapat menunjukkan *base score, base score* inilah yang menjadi acuan tingkat dampak serangan dari kerentanan sebuah situs apakah *low, medium*, bahkan *high* dengan rentang nilai 0-10. Penentuan *base score* tentunya terdapat perhitungan di dalamnya, perhitungan tersebut ditentukan dari beberapa variabel penentu tingkat *vulnerability*. Pada CVSS v.2 parameter penentuan

nilai *base score* terdapat 6 kategori lebih sedikit dari CVSS v.3 yang mempunyai 8 kategori sehingga penggunaan CVSS v.2 lebih simpel untuk melakukan pengamatan. Untuk itu penelitian ini akan meneliti bagaimana nilai *base score* tersebut dihasilkan untuk menentukan seberapa besar kerentanan situs terhadap serangan xss.

Situs yang digunakan pada penelitian ini adalah situs berjenis blog dan situs sistem in*form*asi akademik MAN 1 Jember, dua situs yang memiliki karakteristik berbeda sehingga diharapkan dapat memunculkan hasil dan dampak yang berbeda. Pada situs blog hanya menampilkan sebuah in*form*asi berupa artikel dan fitur komentar dan siapapun dapat mengaksesnya, pada situs sistem in*form*asi akademik menampilkan sebuah in*form*asi akademik berupa nilai siswa, jadwal siswa, profil siswa dan lain lain, serta untuk mengaksesnya harus mempunyai hak akses seperti guru atau siswa maka apabila seseorang yang tidak berhak mengakses namun dapat masuk sebagai *admin* yang diakibatkan adalah dapat merubah semua isi tabel pada *database*.

Berdasarkan uraian di atas maka permasalahan tersebut diangkat sebagai bahan penelitian untuk skripsi. Adapun judul yang dipilih yaitu "Mekanisme Keamanan dan Evaluasi Situs Terhadap Serangan *Cross-Site Scripting* (XSS) Berdasarkan *Base Metric* CVSS V.2".

1.2 Rumusan Masalah

Adapun rumusan masalah yang sesuai pada uraian di atas dan menjadi acuan dalam penelitian ini yaitu:

1. Berapa serangan xss yang dapat ditahan pada situs palsu dari 16 serangan xss yang diberikan?
2. Berapakah tingkat kerentanan situs blog dan sistem in*form*asi akademik terhadap serangan xss dari hasil perhitungan *base metric* cvss v.2 melalui skenario pengujian?

1.3 Tujuan

Tujuan penelitian ini yaitu:

1. Membuat mekanisme keamanan agar situs yang dilindungi dapat aman dari serangan xss.
2. Mengetahui *level* pada kerentanan situs blog dan sistem in*form*asi akademik terhadap serangan xss berdasarkan *base metric* cvss v.2.

1.4 Manfaat

1. Situs asli menjadi aman dari *client* yang ingin mengeksploitasi mengggunakan serangan xss.
2. Memberikan pengetahuan bagaimana mengamankan situs yang dimiliki.
3. Memberikan pengetahuan untuk menentukan nilai kerentanan dari situs yang dimiliki terhadap serangan xss.
4. Dapat dijadikan referensi untuk melakukan penelitian lebih lanjut dengan mencari tingkat *level* kerentanan pada *vulnerability* yang lain.

1.5 Batasan Masalah

1. Situs yang dipakai adalah situs yang suda teruji dapat diserang xss.
2. Terdapat dua situs yang dibuat sebagai uji coba serangan dan masing masing situs memiliki karakteristik yang berbeda yaitu situs berjenis blog dan situs SIA MAN 1 Jember.
3. Situs uji coba tidak di *hosting*.
4. Jumlah serangan pada mekanisme keamanan situs adalah 16 *payload*.
5. Terdapat 4 skenario untuk menentukan *level* kerentanan pada masing – masing situs dengan jenis serangan berjenis *alert* dan *bypass cookie*.
6. Evaluasi situs dilakukan setelah dibuatnya mekanisme keamanan
7. Nilai parameter *base metric* hanya fokus pada nilai yang ditemukan pada dua situs tersebut.
8. *Router* yang dipakai adalah *router* mikrotik.