BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pada saat ini perkembangan teknologi sangatlah cepat dan tidak dapat dibendung lagi. Dimana pada saat ini hampir disemua sektor memerlukan teknologi yang dimana teknologi tersebut digunakan untuk menggantikan pekerjaan manusia serta memfasilitasi dan juga mengikuti perkembangan jaman yang mulai menerapkan digitalisasi pada semua sektor dengan begitu banyak hal yang akan tergantikan dan juga terbaharui. Seperti contohnya zaman sekarang teknologi juga merambah ke sektor bisnis dan komerisal dengan ditandai banyak munculnya *website* jualan sebuah produk , barang , ataupun jasa. Dengan menggunakan *website* sebagai tempat berjualan otomatis pedagang tidak terlalu membutuhkan toko fisik , mereka hanya membuat toko *online* kemudian ditoko tersebutlah para pedagang menjual dan memasarkan produknya kekonsumen. Dan konsumen hanya perlu mengakses toko tersebut melalui perangkat yang terhubung oleh koneksi internet. Dikarenakan para pedagang dan penjual tidak perlu membuka toko fisik maka banyak orang yang tertarik untuk membuka toko onlinenya sendiri.

Dengan begitu banyak para pedagang atau pengusaha yang tertarik untuk membangun dan membuat website masing - masing. Akan tetapi banyak dari pembuat *website* tersebut yang melalaikan atau kurang paham tentang keamanan *website* itu sendiri. Dimana banyak pembuat *website* yang tidak menerapkan sistem keamanan yang berstandar pada lembaga tertentu yang sudah teruji. Misalnya adalah standarisasi dari *Open Web Application Security Project* (OWASP) dimana didalam OWASP tersebut ada beberapa kriteria yang diharuskan untuk para pembuat *website* memenuhi beberapa kriteria tersebut. Seperti menerapkan beberapa fitur yang telah disediakan untuk mencegah beberapa serangan tertentu. Dan disana juga terdapat halaman yang mengedukasi bagaimana cara metode hacking itu menyerang dan apa yang harus

dilakukan untuk mencegah *hacking* itu terjadi. Sehingga diharapakan nantinya diharapkan dapat meminimalisir terjadinya *hacking* pada *website* tersebut.

Dikarenakan jaman sekarang semakin banyak munculnya *website* baru maka tingkat *traffic* akan peretasan atau hacking akan semakin meningkat juga. Seperti contoh teknik *hacking* yang sering umum dipakai adalah teknik *Cross Site Scripting* (XSS) , *Cross Site Scripting* merupakan serangan pada halaman website atau website aplikasi. *Cross Site Scripting* pada umumnya digunakan untuk mengambil atau mencuri *session cookies user* , yang membuat penyerang menyamar atau berkamuflase sebagai korban atau target. Dengan begitu peretas bisa mendapat informasi data sensitif dari pada korban atau target tersebut. Berdasarkan artikel *writeup* (Jake Miler 2018, hlm.1) yang terjadi ditahun 2018 dimana pada bulan Juni dimana laman *Google Docs* Tepatnya *SpreadSheet* tedapat *vulnerability* XSS yakni dalam kolom dokumenya ketika diinject sebuah *script* kode maka laman tersebut merefleksikan dokumen *cookies* dimana dokumen tersebut berisi tentang *cookies user* dan informasi lainya. Dimana *cookies* itu bisa digunakan oleh *hacker* untuk mencuri data *user* tersebut dengan menyamar sebagai *user* tersebut dengan mengganti *cookies hacker* ini menjadi *cookies user* yang menjadi targetnya. Kemudian *hacker* tersebut akan melakukan hacking terhadap *website* tersebut dengan menggunakan identitas sebagai *user* korban tadi.

Kasus lainya adalah berdasarkan artikel *writeup* (Anas Mahmood 2018, hlmn.1) *Zoho Office Suite* pada bulan september tahun 2019 , dimana pada *website* tersebut tedapat *vulnerability* XSS dimana pada mail *user* dapat ditanamkan *stored* XSS yang nanti akan memunculkan dokumen *cookies* dari pada *user* tersebut. Dari sini kita dapat informasi bahwa *bug* XSS masih ada dibeberapa *website* yang bahkan cukup terkenal seperti *Google Documents* tadi. Ini membuktikan bahwa beberapa pemilik *website* masih lengah akan keamanan *website*nya sendiri , padahal *OWASP* telah membuat 10 daftar teknik yang masih dipakai untuk mencari suatu *vulnerability* atau *bug* yang ada pada suatu *website*.

OWASP juga membuat bagaimana cara mengamankan *website* dari serangan - serangan tersebut.

Dari beberapa contoh kasus diatas terdapat beberapa solusi yang ditawarkan sebelumnya salah satunya adalah penggunaan metacharacter untuk memfilter inputan yang merupakan sebuah *payload* untuk *mentrigger error* yang merefleksikan *bug* XSS. Metacharacter sendiri banyak digunakan dikarenakan kefektifanya dalam mengatasi *bug* ini dan juga penggunaanya yang cukup mudah dengan menggunakan beberapa *statement* yang telah tersedia. Metacharacter juga dapat dipadukan dengan *filter* dari HTML sehingga membuat *filter* menjadi berlapis - lapis. Sehingga sangat meminimalisir terjadinya *bug* XSS tersebut , untuk menjaga keamanan *website* perlu diaplikasikan disetiap *page* atau halaman yang mempunyai inputan seperti kolom *search* atau pencarian , *form upload* , *form* komentar dan lain - lain.

Akan tetapi metacharacter masih ada kelemahan atau kekurangan dimana metacharacter hanya akan menangkap injeksi kode XSS yang sesuai dengan pola yang dibentuk , dengan demikian diperlukan banyak pola - pola kode injeksi untuk menangkal itu semua maka akan terjadi pemborosan kode dan resource. Misalnya pola untuk mendeteksi inputan <script></script> tidak dapat menangkal jika yang diinput adalah <img onerror=' '>, untuk itu penulis akan menggunakan metode tambahan yakni form validation dimana hasil dari inputan user akan dicek apakah inputan tersebut sesuai dengan form atau tidak , misalnya user menginput email maka dengan form validation akan melakukan pengecekan apakah inputan tersebut benar email atau bukan. Jika bukan maka akan dilakukan sebuah tindakan tetapi jika benar struktur inputan emailnya maka inputan tersebut benar dan akan diproses sesuai prosess di *web*nya.

Dikarenakan beberapa faktor dan alasan tersebut dimana *Cross Site Scripting* (XSS) masih masuk kedalam 10 daftar teknik yang masih sering dipakai serta dari beberapa contoh kasus tersebut oleh karena itu penulis mengambil topik penelitian ini dengan judul " Peningkatan Keamanan *Website*

Dari Serangan *Cross Site Scripting* (XSS) Dengan Metode Metacharacter Dan *Form Validation*".

1.2 Rumusan Masalah

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis merumuskan masalah sebagai berikut :

1) Apa bahaya yang ditimbulkan oleh serangan *Cross Site Scripting* ?
2) Apakah dengan menggabungkan metode *form validation* dan metacharacter untuk mem*filter* inputan dapat mencegah serangan *Cross Site Scripting*?

1.3 Tujuan Penelitian

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis membuat tujuan sebagai berikut :

1) Untuk mengetahui apa saja dampak dari serangan *Cross Site Scripting.*
2) Untuk mengetahui bagaimana cara serangan *Cross Site Scripting bekerja*.
3) Untuk mengetahui hasil dari menggunakan dua *filter* inputan *form validation* dan metacharacter terhadap *payload* serangan *Cross Site Scripting*.

1.4 Manfaat Penelitian

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis mengharapkan manfaat sebagai berikut :

1) Dapat menjadikan penelitian ini sebagai salah satu cara untuk menghindari resiko terhadap serangan *Cross Site Scripting* (XSS).
2) Dapat dijadikan sebagai referensi untuk penelitian terkait dengan pembahasan pada tulisan ini.

1.5 Ruang Lingkup

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas, maka ruang lingkup penelitian sebagai berikut :

1) *Website* yang dibuat menggunakan bahasa pemograman *web* PHP dan HTML.
2) *Website* menggunakan *hosting localhost* xampp.
3) Membahas proses teknik ekploitasi *Cross Site Scripting* (XSS) pada *website* dan menggunakan 10 kode injeksi.
4) Membahas jenis teknik *Cross Site Scripting* (XSS) *stored* dan *self reflected* yang digunakan untuk mengeksploitasi *website* yang menggunakan bahasa pemrograman *web* PHP.
5) *Website* hanya dapat melakukan *login* saja dan hanya terdapat *user dummy* untuk simulasi *stealing cookies* dan *session* saja.
6) *Website dummy* hanya berisi fitur *login* , halaman artikel dan halaman *home* saja.
7) Pengamanan *website* hanya menggunakan 2 *filter* yakni metacharacter dan *form validation*

1.6 Luaran Yang Diharapkan

Bedasarkan latar belakang masalah yang telah penulis uraikan diatas maka penulis mengharapkan luaran sebagai berikut :

1) Menginformasikan kepada para pembuat *website* bagaimana caranya mengamankan *website* dari serangan *Cross Site Scripting*.
2) Mengedukasi pembaca bagaimana cara kerja dari serangan *Cross Site Scripting* dan dampaknya pada sisi klien.

1.7 Sistematika Penulisan

Penulis akan memaparkan gambaran sistematika penulisan laporan penelitian ini yang terdiri dari beberapa bagian sebagai berikut :

BAB 1 Pendahuluan

Pendahuluan yang berisi latar belakang penelitian, tujuan, permasalahan, ruang lingkup penelitian, sistematika penulisan.

BAB 2 Landasan Teori

Landasan teori (kajian pustaka) berisi mengenai teori-teori, metode, prosedur dan tools yang digunakan dalam penelitian.

BAB 3 Metodologi Penelitian

Metodologi Penelitian berisi antara lain langkah-langkah apa yang dilakukan dalam penelitian serta motode/teknik/prosedur yang digunakan dalam setiap langkah penelitian berikut keluaran yang diharapkan.

BAB 4 Pembahasan

Pembahasan berisi penjelasan tentang rumusan masalah yang sudah dibuat sebelumnya dan melakukan pengujian penelitian.

BAB 5 Penutup

Penutup berisi tentang kesimpulan dan saran dari hasil penelitian yang telah dilakukan sebelumnya.

Daftar Pustaka

Lampiran