BAB 1 PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi khususnya internet semakin hari semakin berkembang dengan pesat dan mencakup berbagai bidang kehidupan masyarakat. Internet bisa dikatakan sebagai penghubung antara satu manusia dengan yang lainnya tanpa dibatasi oleh ruang dan waktu. Hal tersebut menjadikan beberapa pekerjaan menjadi lebih mudah untuk dilakukan dan membuat kehidupan bersosialisasi menjadi lebih luas lagi. Biasanya kita untuk melakukan pekerjaan dan bersosialisasi di internet menggunakan sebuah aplikasi, baik aplikasi berbasis *mobile* maupun aplikasi berbasis *website*. Seiring perkembangan internet yang semakin maju maka berbanding lurus dengan bertambahnya pengguna pada aplikasi berbasis *mobile* dan *website*. Berdasarkan data yang didapatkan dari laman artikel (Simon Kemp 2020, hlm.1) jumlah pengguna internet pada tahun 2020 dimana saat statistik tersebut dirilis pada bulan Juli 2020 sudah mencapai 4,57 miliar pengguna atau 59% total populasi dunia yang dimana hampir setiap tahun mengalami peningkatan penggunanya dimana pada tahun 2020 terjadi peningkatan sebanyak 8.2% atau sebanyak 346 juta pengguna.

Peran dari aplikasi tersebut khususnya aplikasi berbasis *website* yaitu sebagai sarana penghubung, pekerjaan, pendidikan, hiburan dan sebagainya yang menghubungkan antara pengguna satu dengan yang lainnya. Sehingga hal tersebut membuat adanya pertukaran atau perpindahan data atau informasi yang cukup signifikan yang terjadi pada *website* tersebut. Sehingga dengan adanya hal tersebut maka diperlukanya sebuah jaminan keamanan bagi penggunanya dalam sebuah *website*. Keamanan data atau informasi pengguna merupakan sebuah prioritas yang harus diutamakan oleh para pengguna maupaun para pengembang. Oleh karenanya perlu diperhatikan beberapa hal penting dalam proses perancangan dan pengembangan sebuah website. Beberapa hal yang harus diperhatikan dalam melakukan perancangan sebuah website adalah dengan

menghindari adanya *bug* atau celah yang dapat menimbulkan kerentanan pada website yang dikembangkan. Sebuah *bug* atau celah tersebut bisa muncul karena berbagai macam faktor yang ada. Faktor yang cukup menjadi alasan dalam munculnya kerentanan tersebut adalah dalam melakukan penulisan kode bahasa pemrograman. Banyak kerentanan yang muncul dari adanya ketidaksempurnaan dalam melakukan penulisan atau penyusunan bahasa pemrograman pada sebuah website. Sehingga dengan munculnya kerentanan pada website, maka kerentanan tersebut bisa diekploitasi yang bisa memungkinkan orang yang tidak memiliki kewenganan dapat mengakses sistem yang ada melalui kerentanan yang ada tersebut. Hal ini bisa memungkinan data atau informasi yang terdapat didalamnya dapat dilihat dan diakses sehingga bisa disalahgunakan oleh orang yang tidak memiliki kepentingan atau kewenangan.

Berdasarkan laporan yang didapatkan dari website berikut, (2020 Security Vulnerability, 2021., hlm.1) sepanjang tahun 2020 sejauh ini terdapat 17002 kerentanan (CVEs) diumukan. Dari antara kerentanan tersebut teradapat sekitar 205 laporan untuk *Unrestricted File Upload*. Berdasarkan dari laporan kerentanan yang ditemukan, kita bisa melihat cukup banyak sebuah *bug* atau celah yang dapat mengakibatkan munculnya kerentanan yang bisa mengakibatkan ancaman terhadap sebuah sistem dikarenakan ketidaksempurnaan penulisan bahasa pemrograman, salah satunya adalah *File Upload Vulnerability*. Kerentanan tersebut memungkinkan orang yang tidak memiliki kewenangan untuk memasukan sebuah *file* yang berisikan *payload* atau *backdoor* kedalam system melalui website tersebut. Sehingga jika *file* tersebut berhasil masuk kedalam sebuah website maka bukan tidak mungkin orang tersebut menjadikan file tersebut sebagai jalan masuk kedalam sistem dan melakukan beberapa Tindakan yang dapat mengancam keamanan sistem maupun kerahasiaan data atau informasi.

Bedasarkan latar belakang diatas, maka penulis akan melakukan penelitian terhadap *File Upload Vulnerability* pada sebuah website dan mencoba menerapkan keamanan pada aplikasi berbasis website untuk

melakukan pencegahan dari *File Upload Vulnerability* menggunakan bahasa pemrograman php dengan menerapkan *filtering file upload* dengan cara melakukan validasi pada *file* yang akan diupload sehingga menghindari masuknya *file* yang berisi *payload* atau *backdoor* yang dapat dapat membahayakan sebuah sistem. Jika *file* yang divalidasi tidak berhasil melewati filtering, maka file tersebut tidak akan bisa masuk kedalam system tersebut. Sehingga dengan melakukan hal tersebut maka akan mencegah masuknya file berbahaya ke dalam sebuah sistem melalui website tersebut. Oleh karena itu, maka penulis akan memberi judul. "Analisis *File Upload Vulnerability* dan Pencegahan dengan File Content Validation" pada penelitian yang akan dilakukan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya maka penulis melakukan perumusan masalah tersebut sebagai berikut:

1. Bagaimana pengaruh *File Upload Vulnerability* pada sebuah website?
2. Bagaimana cara mengamankan sebuah website dari *File Upload Vulnerability*?
3. Bagaimana pencegahan File Upload Vulnerability dengan cara validasi *file content*?

1.3. Tujuan Penelitian

Berdasarkan latar belakang yang telah dijelaskan sebelumnya maka tujuan dari dilakukannya penelitian ini yaitu sebagai berikut:

1. Dapat mengetahui hal terkait *File Upload Vulnerability*
2. Dapat membuat aplikasi berbasis website yang bisa mencegah masuknya backdoor kedalam sistem.
3. Dapat menjadikan referensi untuk penelitian terkait

1.4. Manfaat Penelitian

Berdasarkan latar belakang yang telah dijelaskan sebelumnya maka manfaat dari dilakukannya penelitian ini yaitu sebagai berikut:

1. Untuk mengetahui apa saja dampak yang ditimbulkan dari *File Upload Vulnerability*
2. Untuk mengetahui cara kerja *backdoor* yang masuk kedalam sistem melalui *File Upload Vulnerability*
3. Dapat mengetahui pencegahan dari *File Upload Vulnerability*

1.5. Ruang Lingkup

Berdasarkan latar belakang yang telah dijelaskan sebelumnya maka ruang lingkup penelitian ini sebagai berikut:

1. Membahas proses *filtering* dalam sebuah aplikasi berbasis *website.*
2. Membahas langkah dalam mengeksploitasi *file upload vulnerability* menggunakan *backdoor* pada *website* melalui *form upload* pada *website*.
3. Aplikasi *Website* dirancang menggunakan bahasa pemrograman *PHP*.
4. Server yang digunakan pada website menggunakan *virtual machine* sistem operasi linux ubuntu.
5. Jaringan yang digunakan pada pengujian menggunakan jaringan lokal.

1.6. Luaran

Luaran yang diharapkan adalah sebuah aplikasi berbasis website yang bisa mencegah masuknya payload atau program berbahaya kedalam sebuah system.

1.7. Sistematika Penulisan

Pada bagian ini penulis menjelaskan sistematika penulisan yag digunakan pada penelitian ini. Hal ini dimaksudkan supaya memudahkan dalam melakukan penyusunan laporan penelitaian. Berikut merupakan susunan sistematika penulisan laporan penelitian :

BAB 1 PENDAHULUAN

Pada bagian ini menjelaskan mengenai latar belakang dari penelitian ini, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, luaran yang diharapkan, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bagian ini menjelaskan mengenai kumpulan teori-teori, definisi dari metode beserta beberapa hal yang digunakan dalam penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Pada bagian ini berisi mengenai metode yang digunakan dalam penelitian ini beserta apa saja yang digunakan sebagai sarana dalam melakukan penelitian ini.

BAB 4 PEMBAHASAN

Pada bagian ini menjelaskan dan membahas mengenai hasil dari penelitian yang telah dilakukan beserta apa hasil yang telaj didapatkan dari penelitian ini.

BAB 5 KESIMPULAN DAN SARAN

Pada bagian ini berisi kesimpulan dari penelitian dan hasil yang didapatkan, beserta juga saran untuk penelitian kedepannya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN