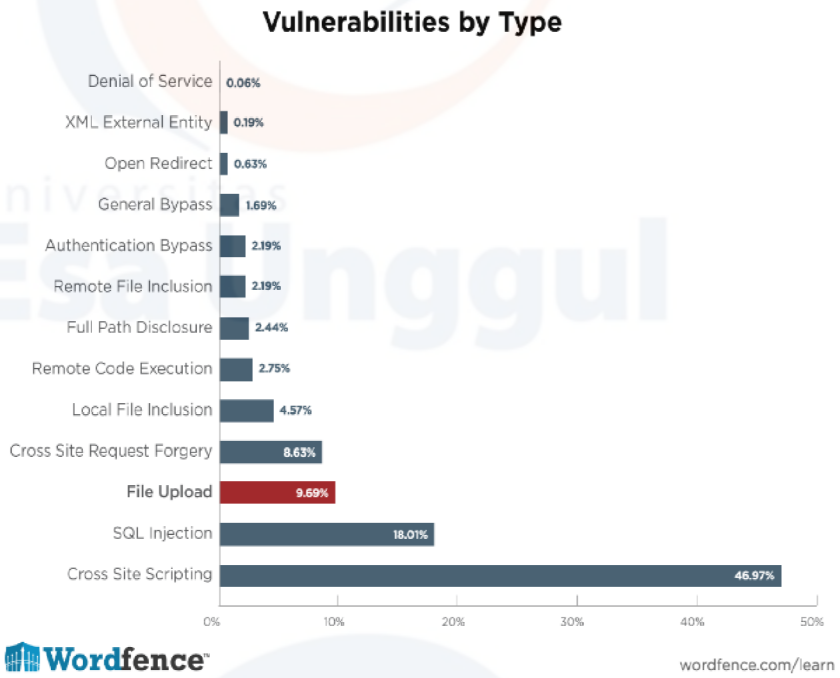
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan pada *website* saat ini sudah semakin berkembang dengan sangat pesat, *website* yang terhubung dengan internet semakin mempermudah masyarakat untuk mengkases setiap informasi dari setiap penjuru dunia. penggunaan *website* menjadi sebuah kebutuhan utama dalam menjalankan sebuah bisnis di era saat ini, Namun, seiring perkembangan *website*, semakin berkembang juga usaha *exploitation* dari *hacker* untuk mencuri informasi – informasi penting dengan memanfaatkan celah keamanan. *Wordpress* merupakan CMS yang bersifat *Open source*, hal ini dapat mempermudah *hacker* untuk melakukan *exploitation* karena *source code* program yang bersifat terbuka dan dapat diunduh secara gratis di *Internet*.



Gambar 1.1 Persentase jenis serangan terhadap Wordpress.

Pada gambar 1.1 menunjukan hasil *survey* yang dilakukan oleh situs wordfence.com terhadap jenis serangan file *upload* pada *Wordpress* memiliki persentase sebesar 9.96% dan diposisi teratas adalah jenis serangan *Cross Site Scripting* dengan persentase sebesar 46.97%. *Unrestricted File upload* merupakan salah satu jenis serangan file *upload,* serangan ini menjadi sebuah ancaman yang serius karena *hacker* dapat menyisipkan kode berbahaya kedalam file yang di upload untuk mendapatkan akses ilegal kedalam *webserver*. konten berita dan keamanan data merupakan hal yang harus dijaga oleh pengembang *website*.

Pada tahun 2020 terdapat serangan terhadap *website* berbasis *Wordpress* dengan memanfaatkan celah keamanan pada plugin bernama *wp file manager*. Sekitar 700.000 *website* berhasil diserang oleh *hacker* dan diantaranya menanamkan *backdoor* atau pintu masuk illegal kedalam *webserver* dengan memanfaatkan celah keamanan file upload [1]. *wp file manager* merupakan plugin yang digunakan oleh *administrator* untuk melakukan *upload ,edit ,delete* file kedalam CMS *Wordpress*. Kerentanan ini terdaftar sebagai CVE-2020-25213.

Dari permasalahan tersebut penulis tertarik untuk melakukan penelitian tugas akhir untuk mengetahui celah keamanan *Unrestricted File Upload* berdasarkan CVE-2020-25213 pada *website* berbasis *Wordpress* dengan melakukan pengujian atau biasa disebut dengan *penetration testing*. *Penetration testing* adalah sebuah metode yang dilakukan untuk menilai keamanan dari sistem yang akan diuji berdasarkan metode yang telah ditentukan. Pada penelitian ini penulis akan melakukan pengujian atau *penetration testing* terhadap website berbasis *Wordpress* dengan menggunakan teknik *Dork* untuk menentukan *target* dan menggunakan metode OWASP Top 10 tahun 2017 sebagai referensi *penetration testing*. Penerapan *penetration testing* bertujuan untuk menemukan celah keamanan dan melihat dampak yang ditimbulkan dari serangan *Unrestricted File Upload* yang terdapat pada *website* berbasis *Wordpress.* Hasil pengujian akan dituliskan dalam bentuk laporan yang nantinya akan digunakan sebagai referensi perbaikan website yang terdampak celah keamanan CVE-2020-25213.

Maka dari itu penulis mengajukan judul " **ANALISA CELAH KEAMANAN PADA *WORDPRESS* TERHADAP SERANGAN *UNRESTRICTED FILE UPLOAD (* STUDI KASUS : WEBSITE XYZ *)*** " yang diharapkan dapat memberikan solusi dari masalah yang ada.

1.2 Identifikasi Masalah

Berdasarkan latar masalah di atas permasalahan yang akan dibahas adalah,

1. Bagaimana menemukan celah keamanan *plugin* pada *Wordpress*?
2. Apa dampak yang dapat dilakukan dari serangan *Unrestricted file upload?*
3. Bagaimana perbaikan untuk mencegah terjadinya serangan *Unrestricted file upload* pada *website* XYZ?

1.3 Tujuan Masalah

Adapun tujuan dari penelitian tugas akhir ini adalah,

1. Melakukan pengujian situs *Wordpress* terhadap serangan *Unrestricted file upload.*
2. Mengetahui dampak yang ditimbulkan dari serangan *Unrestricted file upload.*
3. Membantu melakukan analisa dan memberikan saran perbaikan situs *Wordpress* terhadap serangan *Unrestricted file upload* .

1.4 Batasan Masalah

Batasan Masalah terdiri dari tahapan – tahapan sebagai berikut :

1. Melakukan implementasi serangan terhadap plugin yang memiliki celah keamanan *Unrestricted file upload* pada *Wordpress.*
2. perancangan dan pembuatan *malicious code* dengan menggunakan bahasa pemrograman PHP.
3. Menggunakan metodologi *OWASP Penetration Testing* dalam proses pengujian celah keamanan.
4. Penelitian ini berfokus pada kerentanan CVE-2020-25213.

1.5 Manfaat Penelitian

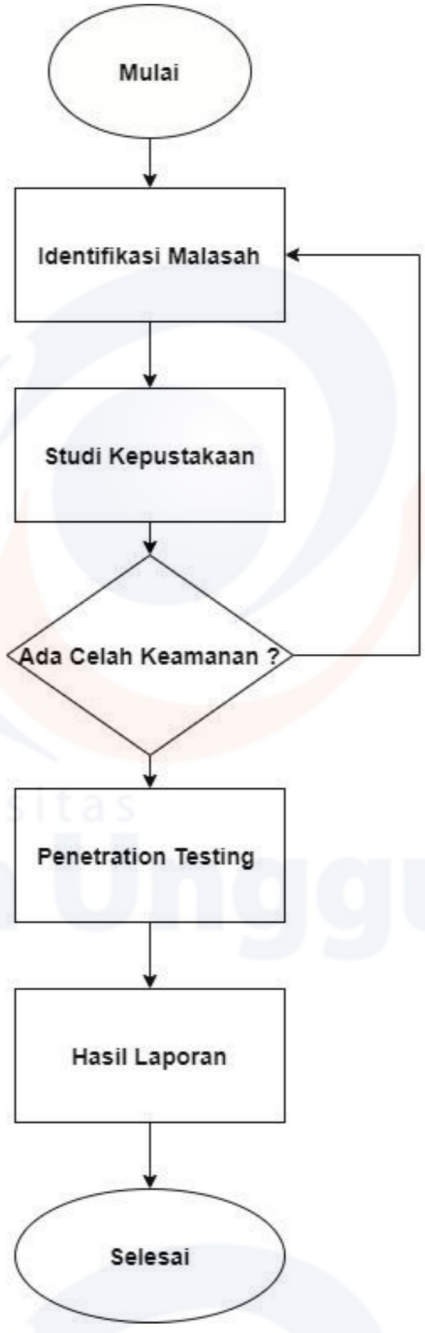
Manfaat penelitian yang dapat diambil sebagai berikut:

1. Dapat menambah pengetahuan dan pemahaman mengenai celah keamanan pada *Wordpress* terutama celah keamanan *Unrestricted file upload.*
2. Membantu administrator dalam melakukan perbaikan dan pengujian sistem secara berkala.
3. Membantu meningkatan *awareness* terhadap dampak yang ditimbulkan dari serangan *Unrestricted file upload.*

1.6 Kerangka Berfikir

Dalam kerangka berpikir terdapat sebuah gambaran untuk penelitian yang membahas tentang pendekatan dari permasalahan sehingga dapat menghasilkan yaitu pengujian celah keamanan pada website berbasis *Wordpress*. Dalam penilitian ini dibagi menjadi tiga tahap yaitu *Pre-Attack phase*, *Attack Phase*, dan yang terakhir *Post-Attack Phase*. dimulai dari mengidentifikasi latar belakang dimana latar belakang yang ingin dibuat yaitu Analisa Celah Keamanan pada *Wordpress* Terhadap Serangan *Unrestricted File Upload* dan menggunakan studi kepustakaan dari kerentanan CVE-2020-25213, dari latar belakang tersebut akan dilakukan analisa permasalahan yang bertujuan untuk mengumpulkan informasi terhadap sistem yang berjalan dengan melakukan identifikasi dengan Teknik *information gathering* dan menggunakan tool WPScan, ini bertujuan untuk mengumpulkan data, serta menganalisis permasalahan yang dihadapi. Setelah data di dapatkan maka langkah selanjutnya yaitu melakukan implementasi serangan menggunakan metodologi *OWASP Penetration Testing* Tahap ini merupakan sebuah proses *exploitation* dimana proses perancangan *exploit code* dibatasi menggunakan bahasa pemrograman, PHP yang ditujukan untuk celah keamanan file upload.,

berdasarkan dari hasil pengujian akan dilakukan proses pembuatan *reporting*. adapun gambar kerangka berpikir pada penelitian ini dapat dilihat dibawah ini :



Gambar 1. 2 Kerangka Berfikir.

1.7 Sistematika Penulisan

Berikut sistematika penulisan yang disusun dalam laporan ini:

BAB I PENDAHULUAN

Dalam bab ini dijelaskan mengenai hal yang terdiri dari latar belakang, identifikasi masalah , tujuan dan manfaat penelitian, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini dijelaskan mengenai hal yang berisi tentang teori – teori yang berhubungan dengan tugas akhir ini. Terdapat beberapa definisi atau teori pada penelitian ini seperti : Definisi *Unrestricted file upload, Wordpress*, *Malicious Code,* dan *Plugin*.

BAB III METODE PENELITIAN

Bab ini membahas mengenai langkah-langkah pengerjaan yang akan ditempuh dalam rangka pencapaian tujuan penelitian

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang pembahasan berupa uraian, penjelasan, dan hasil pengujian celah keamanan yang telah ditentukan sebelumnya. Pengujian dilakukan untuk memastikan bahwa hasil akhir yang dibuat sesuai dengan kebutuhan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang uraian kesimpulan yang dapat diambil berdasarkan hal yang telah dilakukan serta saran yang berguna untuk perbaikan selanjutnya.