BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada tahun-tahun saat ini telah mengalami perkembangan sangat pesat dalam dunia teknologi dan sistem informasi, sehingga mengalami perubahan cukup besar dalam penyebaran informasi yang dimana tidak lagi menggunakan media konvensional melainkan menggunakan website. sehingga perkembang teknologi informasi tersebut juga mengambil peranan yang bisa dibilang sangat penting dalam dunia serba digital saat ini. Dengan menggunakan *website* memudahkan dalam mengakses informasi kapanpun tanpa adanya batasan tempat dan waktu. yang membuat masyarakat akan bergantung pada internet dalam kehidupan sehari-hari untuk mendapatkan informasi. Menurut survei yang telah dilakukan oleh Asosiasi Penyelenggara Jasa Indonesia (APJII), di tahun 2018 pengguna internet di Indonesia telah mencapai 171,17 juta orang atau lebih tepatnya sekitar 64,8% dari total jumlah penduduk di Indonesia sebanyak 264,16 juta orang, yang dimana pengguna internet yang ada di Indonesia mengalami peningkatan sekitar 10,12% atau sekitar 27,9 juta orang dari tahun sebelumnya yaitu 143,26 juta orang. Dengan meningkatnya pengguna internet, situs web yang sebagai tempat mencari segala jenis informasi harus terjamin keamanannya. Menurut *Open Web Application Security Project* (OWASP) tahun 2017, terdapat sepuluh kerentanan yang sering terjadi yaitu kelemahan injeksi, otentikasi rusak, data sensitif yang terpajang (terekspos), *XML Extenal Entities* (XXE), kontrol akses yang rusak, kesalahan konfigurasi keamanan, kelemahan *Cross-Site Scripting* (XSS), *insecure deserialization*[1]. Dari kerentanan tersebut dapat dimanfaatkan untuk melakukan eksploitasi sistem dan mengambil informasi atau data penting dalam aplikasi web tersebut.

Menurut laporan dari *Asia Pasific Computer Emergency Response Team (*APCERT*)*[2] pada tahun 2018 Indonesia *Computer Emergency Reponse Team* (ID-CERT) menerima jumlah laporan insiden sekitar 144,620 dan juga menerima

laporan *bruce force attack*, web yang di sisipkan *malware* dan pencurian data terhadap web sekitar 18.210 pengaduan.[3]

Berdasarkan permasalahan yang telah dijelaskan pada paragraf sebelumnya, penelitian pada kali ini akan menggunakan metode Kualitatif dengan menggunakan Redhawk, dengan melakukan beberapa tahapan seperti mengumpulkan informasi, investigasi, pengujian dan pelaporan dari hasil yang ditemukan pada web target, agar pembaca dapat mengetahui Langkah awal bagaimana seorang attacker mencoba menerobos melalui website dengan mengetahui bugs atau vulnerability yang bisa di manfaatkan untuk masuk secara illegal, sehingga sesuai judul penelitian ini "Analisis Kerentanan Keamanan Pada *Website* Menggunakan Redhawk" akan melakukan analisis atau menguji coba dalam menemukan celah apa saja yang di temukan pada *website* target tersebut dengan menggunakan *Redhawk*.

Teknologi ini di pilih karena mampu dan sesuai serta dapat melakukan beberapa fungsi dalam melakukan analisis terhadap keamanan *website* dalam menemukan kerentanan *website*. *Redhawk* sendiri merupakan alat yang *OpenSource* yang di rilis pada forum *Github* yang berfokus dalam melakukan pemindaian situs web serta mampu dalam melakukan pengumpulan informasi. *Redhawk* di tulis dengan Bahasa peprograman *PHP*. Pada *RedHawk* terdapat fitur yang sangat penting seperti:1) mendeteksi informasi *Cloudflare*, 2) mendeteksi catatan *webserver*, 3) mencari *sql injection* berbasis kesalahan, 4) mampu deteksi website yang di bangun menggunakan *Wordpress, Joomla, Drupal*, dan *Magento*.

1.2 Perumusan masalah

Berdasarkan Latar belakang masalah seperti yang sudah dijelaskan pada pada paragraph sebelumnya, sehingga penelitian ini dapat dirumuskan sebuah permasalahan diantaranya:

1.) Bagaimana cara melakukan analisis kerentanan keamanan pada *website* dengan *Redhawk*, guna mempermudah teknisi keamanan pada perusahaan untuk mengetahui tipe kerentanan apa yang ada pada *website* yang di kelola?

2.) Bagaimana hasil atau kerentanan serta informasi apa yang di dapatkan

dari analisis menggunakan *Redhawk*?

1.3 Tujuan Penelitian

Adapun tujuan yang ingin di capai pada penelitian ini adalah:

1) Membantu menyelesaikan permasalahan dalam menemukan celah keamanan *website* terhadap organisasi dengan *Tools Redhawk*.
2) Dari hasil analisis tersebut peneliti dapat memberikan rekomendasi terhadap teknisi keamanan data dalam perusahaan untuk melakukan evaluasi serta perbaikan keamanan aplikasi *website*.

1.4 Batasan Masalah

Adapun batasan-batasan yang telah ditetapkan pada penelitian yang akan dianalisis, diantaranya adalah.

1) Dalam menggunakan *Redhawk* akan di butuhkan *username* dan *password* login ke sistem operasi sebelum menjalankan *Redhawk*.
2) Yang di analisis hanya berupa dalam mencari kerentanan terhadap website serta informasi apa yang bisa didapatkan tanpa melakukan publikasi ke public.
3) Target yang akan dijadikan pengujian *Tool Redhawk* dalam mencari kerentanan pada *website* dibangun sendiri dengan *Wordpress*.
4) Penelitian kali berfokus untuk sampai tahap melakukan analisis, serta saran dari hasil analisis yang telah dilakukan. tidak sampai proses melakukan penyerangan terhadap celah yang ditemukan.

1.5 Manfaat Penelitian

Adapun manfaat yang akan di rasakan oleh objek dari hasil penelitian ini sebagai berikut:

1) Mempermudah admin perusahaan dalam melakukan analisis untuk menemukan tipe serangan apa yang rentan terhadap *website* perusahaan dengan alat bantu *Redhawk*.
2) Mempermudah admin untuk melakukan pengecekan *vulnerability website* secara berkala.