BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pertumbuhan teknologi saat ini semakin berkembang dan inovatif dalam penyampaian informasi hingga pengelolaan data yaitu *website*. *Website* memiliki fungsi dalam penyampaian informasi dan mengelola data secara luas sehingga masyarakat dapat dengan mudah menggunakannya. Hanya dengan jaringan internet dapat diakses oleh siapa saja melalui perangkat komputer dan *smartphone* [1].

Pada tahun 2018, Indonesia memiliki jumlah pengguna internet sebesar 132,7 juta pengguna dan meningkat setiap tahunnya. Pada tahun 2022, pengguna internet sudah mencapai 204,7 juta pengguna dan akan terus meningkat, dimana jumlah tersebut melonjak sebesar 54,25% dari tahun-tahun sebelumnya sehingga menjadikan Indonesia sebagai salah satu negara dengan pengguna internet terbesar di dunia [2]. Seiring dengan meningkatnya jumlah pengguna internet, maka hal itu juga mempengaruhi peningkatan jumlah pengguna *website*. Hal tersebut dapat berdampak adanya kerentanan *website* yang memiliki resiko diserang oleh oknum tidak bertanggungjawab sebab terdapat celah keamanan *website* yang tidak diperhatikan admin *website* tersebut sehingga timbul adanya peretasan [1].

Website penerimaan peserta didik baru (PPDB) merupakan *website* yang menyediakan berbagai informasi terkait pendaftaran siswa baru. Dengan melakukan PPDB secara *online*, maka pendaftar dapat memanfaatkan teknologi informasi dari rumah sehingga tidak perlu datang di tempat untuk melakukan pengisian data hingga melakukan pembayaran pendaftaran [3].Seiring dengan meningkatnya jumlah siswa di sekolah XYZ, maka semakin meningkat juga penggunaan *website* PPDB tersebut. Hal ini menjadi peran penting, dimana banyak data calon siswa baru hingga nomor rekening pendaftaran yang harus dijaga sedemikian rupa. Hal tersebut pernah terjadi ketika saat hilangnya data calon siswa sehingga pihak lembaga sekolah XYZ harus melakukan *back-up* data kembali. Pengujian keamanan sistem informasi perlu dilakukan untuk mengantisipasi ancaman peretasan yang diterima oleh pihak administrasi sekolah, dimana hal tersebut berdampak pada kebocoran informasi yang dapat mengakibatkan serangan *cyber* seperti *phising, deface,* hingga hilangnya data pribadi calon siswa [3].

Dalam pengujian keamanan sistem informasi, terdapat dua jenis metode pengujian kerentanan pada *website* PPDB, yaitu *vulnerability testing* dan *penetration testing*. *Vulnerability testing* merupakan proses pemindaian sistem salah satunya pada *website* yang bertujuan untuk mengetahui titik kelemahan di dalam *website* tersebut. Sedangkan, *penetration testing* merupakan pengujian dengan melakukan serangan ke dalam sistem *website* tersebut yang bertujuan untuk mengetahui kemungkinan titik sistem yang mudah terdapat serangan. Dari kedua metode tersebut merupakan metode yang baik dalam menguji keamanan sistem *website*. Namun *penetration testing* memiliki peran besar dan disarankan untuk melakukan pengujian keamanan sistem [4].

Information system security assesment framework (ISSAF) merupakan kerangka kerja dalam melakukan *penetration testing*, dimana memiliki beberapa fungsi terkait kontrol keamanan, struktur intuitif yang memberikan arahan melalui langkah-langkah yang kompleks. ISSAF terikat pada pedomannya menjelaskan bahwa *penetration testing* dilakukan untuk memberikan arahan pengujian secara benar, hingga menghindari adanya kesalahan dengan metode serangan yang dilakukan secara acak [4]. *Framework* ISSAF memiliki kelebihan yaitu penggunaan ISSAF memiliki kesesuaian untuk memenuhi persyaratan penilaian keamanan organisasi dan dapat dijadikan acuan untuk memenuhi persyaratan keamanan informasi lainnya. ISSAF mencakup aspek utama pemrosesan dan penilaian keamanan informasi, membantu mendapatkan gambaran lengkap tentang potensi kerentanan [5].

Penelitian ini berfokus terhadap pengujian keamanan sistem *website* PPDB yang dilakukan dengan metode *penetration testing* berdasarkan *framework* ISSAF. Penelitian ini bertujuan untuk mengetahui sisi kerentanan pada *website* berdasarkan *framework* ISSAF, sehingga dalam penelitian ini dapat memberikan rekomendasi agar terjadi peningkatan keamanan pada *website* sekolah XYZ [4].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dipaparkan, maka terdapat rumusan masalah dalam penelitian ini, yakni sebagai berikut:

1. Bagaimana kondisi keamanan sistem informasi pada *website* PPDB sekolah XYZ?
2. Bagaimana langkah *penetration testing* dapat bekerja berdasarkan *framework* ISSAF untuk proses keamanan sistem informasi pada *website* PPDB sekolah XYZ?
3. Apa saja rekomendasi keamanan sistem informasi yang harus dilakukan sekolah XYZ untuk meningkatkan keamanan pada *website* PPDB?

1.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang sudah dipaparkan sebelumnya, maka terdapat tujuan penelitian, yakni sebagai berikut:

1. Mengetahui kondisi keamanan *website* PPDB sekolah XYZ setelah melakukan *penetration testing* berdasarkan ISSAF.
2. Mengetahui langkah-langkah *penetration testing* dapat bekerja berdasarkan ISSAF untuk proses keamanan sistem informasi pada *website* PPDB sekolah XYZ.
3. Menyusun rekomendasi berdasarkan hasil *testing* keamanan sistem informasi untuk meningkatkan keamanan pada *website* PPDB sekolah XYZ.

Namun terdapat manfaat dari penelitian ini, yaitu:

1. Dapat mengantisipasi kebocoran informasi data pribadi calon siswa baru dan bukti pembayaran yang tersimpan pada sistem *website* PPDB sekolah XYZ.
2. Dapat memberikan rekomendasi terkait keamanan sistem informasi pada pihak lembaga sekolah XYZ.
3. Dapat mengetahui bagaimana letak keamanan pada *website* PPDB sekolah XYZ.

1.4 Batasan Masalah

Berdasarkan latar belakang yang sudah dipaparkan, maka terdapat batasan masalah dalam penelitian ini, yaitu:

1. Studi kasus dalam penelitian ini yaitu *website* PPDB sekolah XYZ.
2. Penggunaan metode *penetration testing* berdasarkan *framework* ISSAF.
3. Metode *penetration testing* dilakukan dengan cara uji *black box.*