BAB I PENDAHULUAN

Tugas Akhir merupakan sebuah karya ilmiah yang harus dapat dipertanggung jawabkan terutama oleh mahasiswa dan pembimbing terkait. Struktur penulisan tugas akhir dibagi menjadi beberapa bab, diawali dengan bab pendahuluan dan diakhiri dengan daftar pustaka, atau jika diperlukan dapat ditambahkan lampiran-lampiran. Jumlah bab tidak ditentukan, tergantung kepada kajian penelitian sesuai dengan diskusi melalui bimbingan antara mahasiswa dengan pembimbing tugas akhir.

1.1 Latar Belakang

Dengan perkembangan Teknologi yang semakin canggih, situs *web* menjadi media baru untuk mengirimkan informasi. Teknologi ini sangat penting untuk menyebarkan informasi secara luas tanpa batas. Sistem penggunaan *web* sederhana yang dapat digunakan pada perangkat komputer dan *smartphone*. Informasi adalah data yang disusun atau diinterpretasikan sehingga memiliki nilai bagi penerima. Penjabaran informasi melibatkan proses menjelaskan atau menguraikan informasi agar lebih jelas, lengkap, dan mudah dipahami oleh orang lain. Salah satu cara mengakses informasi dapat melalui media apapun salah satunya adalah informasi (Prasetyo & Hassanah, n.d., 2021).

Informasi merupakan jenis layanan informasi yang sering diakses oleh pengguna yang terhubung ke Internet. Berdasarkan fungsi informasi sebagai sarana penyampaian informasi, maka diperlukan pengamanan agar penerima informasi menerima informasi secara lengkap. Jika pemilik situs informasi mengabaikan keamanan, peretas dapat membuat keuntungan mereka sendiri dan merusak informasi. Beberapa contoh kasus yang dilakukan peretas antara lain virus, pencurian kartu kredit, pencurian rekening bank, pencurian *password server email*/*server web*. Peretas mendapatkan data-data penting dari sebuah informasi bahkan merusak tampilannya di informasi suatu organisasi, instansi, dan sekolah (Mulyanto et al., 2022).

Informasi telah berkembang menjadi cara baru untuk menyebarkan informasi termasuk dalam media Pendidikan. Selain itu, lembaga pendidikan menggunakan *platform* informasi untuk berbagi informasi terbaru dan memberi tahu orang-orang tentang penerimaan siswa baru dan beasiswa yang tersedia. Pengguna dapat mengakses pembelajaran dan pertanyaan yang terkait dengan institusi melalui informasi institusi (Uji et al., 2023).

PT.XYZ adalah Lembaga Amil Zakat Nasional yang dikukuhkan oleh Menteri Agama Republik Indonesia . PT.XYZ berfokus pada kemanusiaan dan berusaha untuk menggunakan dana yang mereka kumpulkan secara Syar'i, efisien, efektif, dan produktif. PT.XYZ memiliki beberapa anak perusahaan salah satunya yaitu Xyz yang bergerak sebagai *platform crowdfunding* berbasis informasi dengan tujuan mengajak bergerak bersama untuk bisa peduli dengan problem masyarakat, agar kebaikan yang dihasilkan bersama akan terus dirasakan kebermanfaatanya.

Berdasarkan hasil observasi dan wawancara, informasi Xyz.Id adalah *platform* yang bertujuan untuk menghimpun dana dari masyarakat dalam bentuk zakat, infaq, dan sedekah. Mengingat bahwa informasi ini menangani informasi yang sangat penting, seperti data pengguna, laporan keuangan, detail program dan penerima donasi, serta riwayat transaksi donasi, keamanan menjadi faktor yang sangat krusial. Transaksi yang melibatkan uang memerlukan perlindungan ekstra agar tidak terjadi kebocoran data atau penyalahgunaan. Oleh karena itu, penting untuk melakukan pencarian celah keamanan pada informasi melalui *Penetration Testing*. Pendekatan ini melibatkan pemindaian sistem atau jaringan untuk menemukan kelemahan yang ada, serta eksploitasi sistem untuk menguji seberapa rentan terhadap serangan. Dalam pengujian penetrasi, para penguji diberi wewenang untuk mengeksploitasi sistem guna menemukan celah keamanan yang dapat dieksploitasi. Meskipun ada berbagai metode untuk menguji keamanan sistem, *Penetration Testing* menawarkan keunggulan khusus dan sangat disarankan untuk memastikan keamanan sistem secara menyeluruh, terutama karena adanya transaksi keuangan yang sensitif di dalamnya.

Menurut penelitian terdahulu *framework* yang direkomendasikan untuk *Penetration Testing* adalah ISSAF (*The Information System Security Assessment Framework*). ISSAF merupakan kerangka kerja yang digunakan untuk melakukan penilaian keamanan pada sistem informasi. ISSAF memberikan pedoman dan metode untuk melakukan penilaian risiko, mengidentifikasi celah keamanan, dan mengembangkan strategi perlindungan yang tepat untuk sistem informasi. Ini membantu para profesional keamanan untuk memahami, mengevaluasi, dan meningkatkan keamanan sistem informasi dengan pendekatan yang terstruktur. Panduan ISSAF menjelaskan dengan jelas bagaimana proses pengujian penetrasi harus dilakukan agar memberikan arahan yang tepat dan menyeluruh kepada penguji, serta mencegah kesalahan umum terkait dengan metode serangan acak (Ary et al., 2020).

Penelitian ini menggunakan pengujian *Black Box*, Pengujian *Black Box* adalah metode pengujian yang fokus pada memastikan bahwa semua fitur perangkat lunak beroperasi sesuai dengan kebutuhan fungsional yang telah ditetapkan, tanpa mendapatkan informasi mengenai data internal atau struktur programnya terlebih dahulu (Magdalena, 2011).

Penelitian ini memiliki fokus pada pengujian keamanan beserta rekomendasinya untuk situs Xyz.id. Pengujian keamanan dilakukan melalui metode penetrasi dengan menggunakan kerangka kerja ISSAF. Harapannya, penelitian ini dapat mengungkapkan potensi kerentanan keamanan pada situs *web* dengan memanfaatkan uji penetrasi ISSAF, dan hasilnya dapat digunakan sebagai dasar penyusunan rekomendasi untuk meningkatkan keamanan informasi Xyz.id. Melalui pendekatan ini, diharapkan situs Xyz.id dapat menjadi lebih aman dan dapat diandalkan (Ary et al., n.d., 2020).

1.2 Perumusan Masalah

Adapun rumusan masalah dari permasalahpenelitian ini adalah sebagai berikut:

1. Bagaimana identifikasi kerentanan keamanan yang ada pada informasi Xyz.id menggunakan metode uji penetrasi berdasarkan *Framework* ISSAF?
2. Apa saja kerentanan yang terdapat pada *website* Xyz.id?
3. Apa saja rekomendasi perbaikan yang dapat disarankan untuk meningkatkan keamanan *website* Xyz.id

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan, penelitian ini bertujuan untuk mencapai tujuan antara lain:

1. Mengidentifikasi kelemahan keamanan berdasarkan standar yang dijelaskan dalam kerangka kerja ISSAF.
2. Dapat menganalisis kerentanan keamanan yang ada pada informasi Xyz.id.
3. Merumuskan rekomendasi perbaikan berdasarkan hasil uji penetrasi (*Penetration Testing*) untuk meningkatkan tingkat keamanan pada *web*site Xyz.Id.

Adapun Manfaatnya sebagai berikut:

1. Penelitian ini memberikan manfaat bagi *web*site Xyz.Id dengan membantu mengidentifikasi serta memperbaiki kelemahan keamanan, sehingga meningkatkan perlindungan terhadap data dan informasi yang terdapat di *web*site.

2. Penelitian ini memberikan peneliti kesempatan untuk memperdalam wawasan dan keterampilan dalam bidang *Penetration Testing* serta keamanan informasi, sekaligus menghadirkan pengalaman berharga yang menjadi nilai tambah di dunia kerja.

1.4 Batasan Penelitian

Adapun batasan penelitian ini adalah, sebagai berikut:

1. Penelitian ini hanya di lakukan dengan Metode *penetration testing* menggunakan *framework* ISSAF dengan pengujian *Black Box* dari sisi *User website* Xyz.id.
2. Penelitian ini akan dilakukan dalam kurun waktu tertentu agar relevan dengan tujuan penelitian, serta untuk memastikan fokus dan kedalaman analisis yang optimal.
3. Hasil penelitian berupa rekomendasi perbaikan dengan menganalisis kerentanan dan risiko keamanan yang terdapat pada informasi Xyz.id.

1.5 Manfaat Penelitian

Berdasarkan latar belakang yang telah diuraikan sebelumnya maka dapat dituliskan manfaat dari penelitian ini adalah:

1. Penelitian ini bermanfaat bagi universitas Telkom dalam memperkaya literatur dan studi kasus di bidang keamanan siber, terutama dalam penerapan uji penetrasi menggunakan kerangka ISSAF. Temuan dari penelitian ini dapat dijadikan acuan untuk kegiatan pembelajaran, penelitian, dan pengembangan kurikulum terkait keamanan informasi, sehingga berkontribusi pada peningkatan wawasan akademik dan mencetak lulusan yang kompeten di bidang tersebut.
2. Penelitian ini memberikan manfaat bagi perusahaan dengan membantu mengidentifikasi potensi kelemahan keamanan pada situs *web* Xyz.id melalui uji penetrasi menggunakan kerangka ISSAF. Temuan dari penelitian ini dapat dijadikan dasar dalam merumuskan rekomendasi perbaikan untuk meningkatkan keamanan informasi pada situs tersebut. Melalui langkah ini, diharapkan Xyz.id menjadi lebih aman, andal, dan mampu menjaga data pengguna secara optimal.