BAB I PENDAHULUAN

I.1 Latar Belakang

Seiring dengan perkembangan teknologi, informasi sangat mudah untuk diperoleh dan disebarluaskan serta menjadi salah satu aset penting bagi perusahaan (Nurul et al., 2022). Perusahaan harus memiliki kemampuan untuk menyediakan informasi yang akurat dan cepat, sehingga sistem informasi menjadi bagian penting bagi perusahaan karena dapat mendukung berbagai kegiatan di perusahaan. Tetapi, sistem informasi dapat menyebabkan munculnya ancaman dan risiko dari penggunaan teknologi karena dimanfaatkan oleh pihak yang tidak bertanggung jawab(Chazar, 2015)**.** Berdasarkan data dari laporan Positive Technologies yang telah dirangkum oleh Kompas.id, tercatat selama periode bulan januari sampai dengan bulan september tabun 2020 telah terjadi sebanyak 123 kejadian serangan cyber yang menargetkan layanan kesehatan. Berdasarkan data yang telah dirangkum sebagian besar penyerangan dilakukan dengan malware dengan presentase sebesar 61%, kemudian serangan berupa rekayasa sosial sebesar 46%, serangan berusa peretasan sebesar 30%, serangan *credential compromise* sebesar 17% dan serangan pada situs kesehatan sebesar 7%(Indraswari, 2021). Permasalahan keamanan sistem informasi dapat menimbulkan kerugian bagi perusahaan, sehingga perlu dilakukan tindakan untuk mencegah dan memperbaiki keamanan sistem informasi(Chazar, 2015).

Keamanan sistem informasi menjadi salah satu masalah utama dalam perkembangan teknologi. Sistem informasi harus memastikan kerahasiaan, ketersediaan, dan integritas pada semua sumber daya informasi. Organisasi perlu memastikan bahwa aset informasi dapat dilindungi dari berbagai resiko yang mungkin terjadi(Mu'min et al., 2022). Berdasarkan data pada tekno.kompas.com terjadi kasus peretasan data yang terjadi pada Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan tahun 2021. Data yang berhasil dicuri berupa Nomor Kartu, NIK, Nomor Ponsel, E-mail, alamat dan gaji dari 279 juta penduduk indonesia yang terdaftar pada BPJS Kesehatan. Data tersebut dijual oleh akun peretas yang bernama "kotz" pada forum online(Pertiwi & Yusuf, 2021). Karena permasalahan tersebut mendorong organisasi untuk membangun keamanan sistem, tidak

terkecuali sistem keamanan pada *website*. Website adalah sebuah halaman yang menyediakan informasi atau data yang dapat diakses saat terkoneksi dengan internet. Website sangat dibutuhkan untuk menyebarkan data dan informasi secara lebih luas(Ariyadi et al., 2023). Seperti pada instansi kesehatan contohnya juga menerapkan sistem informasi berbasis website.

Instansi XYZ Surabaya adalah salah satu instansi kesehatan yang menggunakan sistem informasi berbasis *website* untuk media informasi kesehatan. Terdapat dua *website* yang digunakan pada instansi XYZ, yaitu *website* instansixyz.com yang berisi informasi terkait UGD, Rawat Inap, Rawat jalan, Jadwal Dokter, dan juga informasi lainnya dan *website* antrianinstansixyz.com yang berisi form bagi pasien yang ingin mendaftar seperti nama poli, jadwal dokter, dan juga identitas pasien seperti NIK, KTP, Alamat, nomor telpon, dll. Berdasarkan kasus serangan *cyber* pada BPJS Kesehatan maka *website* pada rumah sakit juga beresiko menjadi sasaran dari serangan *cyber*, hal ini didukung dengan hasil wawancara kepada koordinator IT pada instansi XYZ yang menyatakan bahwa *website* instansixyz.com pernah terjadi tindakan peretasan dengan mengganti tampilan *website* utama yakni pada tahun 2023, walaupun dampak dari serangan tidak mempengaruhi operasional kerja pada instansi, karena segera diperbaiki oleh pihak IT instansi XYZ Surabaya. Hal ini membuktikan bahwa *website* instansixyz.com rentan terhadap serangan, serta *website* antrianinstansixyz.com yang berisi data sensitif pasien seperti KTP, NIK, Alamat, nomor telpon, dll, juga berpotensi mendapatkan serangan serupa seperti instansixyz.com, sebab angka penggunaan *website* antrianinstansixyz.com perbulan mencapai angka 8400 sampai 9600 pemakaian perbulan, maka perlu dilakukan pengujian keamanan untuk meminimalisir celah kerentanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Berdasarkan dari wawancara, pihak instansi XYZ juga belum pernah melakukan analisis kerentanan pada kedua *website*, apabila tidak dilakukan analisis kerentanan maka *website* berpotensi terjadi tindakan peretasan yang dapat menimbulkan kerugian materil dan non materil yang dialami oleh instansi XYZ. Kerugian materil berupa kehilangan data pasien, gangguan layanan medis (pasien tidak bisa daftar *online*), biaya keamanan tambahan (pemasangan *firewall*), kehilangan reputasi, sedangkan kerugian non materil berupa pelanggaran privasi

(data pasien bocor), ketidaknyamanan dan kecemasan pada pasien, gangguan operasional. Cara terbaik untuk mengetahui tingkat kemanan suatu sistem yatu dengan mencoba *penetration testing*(Riandhanu, 2022). *Penetration testing* merupakan pengujian untuk mengidentifikasi kerentanan baru, menguji keamanan dan menetapkan kontrol untuk mengurangi resiko dari sistem informasi(Mu'min et al., 2022).

Pada penerepan penetration testing pada *website*, terdapat panduan atau *framework* yang digunakan dalam pengujian dan analisis keamanan pada *website*, panduan yang dimaksud yaitu (*Open Web Application Security Project*) OWASP. OWASP merupakan organisasi yang mempunyai visi untuk menjaga kseamanan *website* dengan menyediakan *resource*(Dharmawan et al., 2022). Pada penelitian ini pengujian keamanan *website* dilakukan dengan *penetration testing* dan menggunakan metode OWASP yang bertujuan untuk mencari celah keamanan yang ada pada *website* Instansi XYZ Surabaya. Hasil dari penelitian ini dapat digunakan oleh pengelola atau pengembang *website* untuk memperbaiki celah kerentanan dan meningkatkan keamanan pada kedua *website* agar kasus serangan yang pernah terjadi tidak terulang kembali pada kedua *website*.

I.2 Rumusan Masalah

Berdasarkan latar belakang yang disampaikan, terdapat beberapa rumusan masalah yang didapat sebagai berikut :

1. Bagaimana menerapkan teknik *penetration testing* dan *framework* OWASP untuk meningkatkan keamanan pada *website* instansixyz.com dan antrianinstansixyz.com?
2. Bagaimana hasil dari pengujian kerentanan keamanan *website* instansixyz.com dan antrianinstansixyz.com berdasarkan *framework* OWASP?
3. Apa saja rekomendasi untuk meningkatkan keamanan *website* instansixyz.com dan antrianinstansixyz.com?

I.3 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang disampaikan, maka tujuan dari penelitian ini adalah sebagai berikut :

1. Melakukan analisis kerentanan keamanan pada *website* instansixyz.com dan antrianinstansixyz.com dengan menggunakan teknik *penetration testing* dan *framework* OWASP.
2. Memberikan hasil dari pengujian kerentanan keamanan website instansixyz.com dan antrianinstansixyz.com berdasarkan framework OWASP.
3. Memberikan rekomendasi perbaikan dari hasil yang sudah didapatkan untuk meningkatkan keamanan *website* instansixyz.com dan antrianinstansixyz.com.

Dari tujuan diatas, manfaat dari penelitian ini sebagai berikut :

Bagi penulis :

1. Menambah pengetahuan terkait proses analisis keamanan sistem informasi berdasarkan *framaework* OWASP.
2. Mampu melakukan pengujian keamanan dengan menggunakan teknik penetration testing.

Bagi pengembang sistem :

1. Mengetahui kerentanan pada *website* instansixyz.com dan antrianinstansixyz.com.
2. Dapat meningkatkan keamanan pada website instansixyz.com dan antrianinstansixyz.com berdasarkan hasil analisis.

I.4 Batasan Masalah

Berdasarkan rumusan masalah yang telah dipaparkan di atas, maka terdapat beberapa batasan permasalahan sebagai berikut :

1. Pengujian difokuskan pada *website* instansixyz.com dan antrianinstansixyz.com.
2. Teknik yang digunakan yaitu *penetration testing* dengan *framework* yang digunakan yaitu OWASP.

I.5 Metodologi Penelitian

Berikut ini adalah metode penelitian dalam penelitian ini sebagai berikut :

- **Identifikasi Masalah**

Pada tahap ini mengidentifikasi permasalahan yang terjadi pada *website* instansixyz.com dan antrianinstansixyz.com dengan melakukan observasi terhadap target pengujian.

- **Tinjauan Pustaka**

  Tahap ini melakukan tinjauan pustaka dengan cara mengumpulkan artikel dan jurnal yang sesuai dengan topik penelitian sebagai sumber acuan dalam melakukan pengujian dan penyusunan laporan.

- **Wawancara**

  Wawancara dilakukan kepada divisi IT pada Instansi XYZ Surabaya untuk menegtahui kondisi eksisting *website* yang akan dijadikan target pengujian serta mengumpulkan informasi yang akan dibutuhkan saat peroses pengujian.

- **Analisis Kebutuhan**

  Pada tahap ini, dilakukan analisis terkait apa saja yang dibutuhan sebelum melakukan pengujian keamanan *website*. Kebutuhan ini dapat berupa informasi dan juga *tools* yang akan digunakan.

- **Implementasi**

  Pada tahap implementasi ini, peneliti melakukan pengujian keamanan *website* sesuai dengan teknik *penetration testing* dan *framework* OWASP yang digunakan sebagai acuan pedoman dalam pengujian.

- **Evaluasi Hasil**

  Tahap terakhir ini yaitu tahapan evaluasi dari hasil pegujian. Peneliti menyimpulkan hasil dari pengujian keamanan untuk meperbaiki kerentanan sesuai hasil analisis.