BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang berkembang pesat telah mendorong berbagai sektor untuk melakukan transformasi digital, termasuk pada bidang pendidikan tinggi. Penerapan ini juga termasuk pada Website berbasis web di kampus yang dimana web ini digunakan sebagai layanan akademik dan administrasi. Website ini diharapkan digunakan untuk mempermudah dan efisiensi pengajuan dan penerbitan berbagai jenis surat, seperti surat pengantar, rekomendasi, maupun surat lainnya. Melalui sistem ini menjadi langkah penting untuk mendukung kegiatan administrasi kampus dan meningkatkan kualitas layanan kepada civitas akademika.

Namun, Perkembangan teknologi informasi ini juga membawa sebuah tantangan baru, yaitu dalam bidang keamanan informasi. Di Indonesia sendiri pada tahun 2021 “BSSN sebut ada 1.6 milliar serangan siber” diantara serangan tersebut yang tercatat oleh BSSN adalah malware, trojan, dan pengumpulan data [1]. Contoh kasus yang ada di Indonesia pada tahun 2021 adalah peretasan situs BPJS Kesehatan yang menyebabkan sekitar 279 juta dari data penduduk bocor dan dijual [2], Sekitar 2 juta data nasabah BRI Life diduga bocor dan dijual secara online [2], dan Puluhan mahasiswa UNUD di terror spam diduga data bocor dari kampus [3]. Oleh karena itu pentingnya perlindungan keamanan terhadap sistem maupun data sensitif yang merupakan bagian penting yang tidak bisa diabaikan. Maka dari itu analisis keamanan dibutuhkan untuk memastikan apakah Website web yang telah dibuat sudah masuk dalam kategori aman tidaknya dari ancaman serangan siber. Tanpa adanya analisis keamanan ini, sistem bisa saja berjalan dengan normal tetapi dapat menyimpan celah keamanan yang berpotensi di eksploitasi oleh pihak pihak yang tidak bertanggung jawab sehingga analisis keamanan bukan hanya tambahan tetapi merupakan kebutuhan utama. [4][5]

SIPATCA adalah website fakultas yang digunakan untuk layanan surat-menyurat yang dimana hal ini juga berpotensi untuk mengalami serangan siber apabila tidak dilengkapi dengan mekanisme keamanan yang memadai. Serangan

tersebut dapat berupa penyusupan malware, modifikasi konten, maupun akses yang tidak sah oleh pihak yang tidak bertanggung jawab. Maka kondisi ini akan menimbulkan kerentan terhadap ancaman siber, seperti pencurian data, maupun manipulasi isi surat bahkan yang akan memungkinkan manipulasi data dan informasi, hingga penyalahgunaan identitas digital. Risiko ini dapat berdampak serius, tidak hanya bagi pengguna individu, tetapi juga terhadap kepercayaan civitas akademik terhadap layanan digital tersebut [1], [2], [3].

Meskipun website di fakultas yang digunakan untuk layanan surat-menyurat sudah melalui uji fungsionalitas guna memastikan fitur berjalan sesuai kebutuhan tetapi itu tidak cukup menjamin dari segi keamanan sistem karena pada pengujian fungsionalitas hanya berfokus dalam kinerja Website dari sisi pengguna, seperti pencatatan data, penyimpanan, dan pembuatan laporan namun tidak mampu mendeteksi potensi kerentanan keamanan. Sehingga juga dalam banyak kasus aspek keamanan website sering kali dilupakan selama proses pengembangan. Rata-rata Website web tersebut dibuat oleh tim. Fokus utama pengembangannya sendiri biasanya tertuju pada fungsionalitas dan kenyamanan pengguna dan terkadang developer web tersebut menunda keamanan dikarenakan kurang nya sumber daya, baik dari segi budget dan SDM. Sehingga elemen penting seperti keamanan pada web tidak dilakukan pengujian secara menyeluruh bahkan terkadang tidak ada keamanan[6]. Hal ini lah yang membuka celah terhadap berbagai potensi serangan siber yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Meskipun belum jelas sejauh mana data pribadi disimpan di Website web ini, web ini berpotensi mengelola data sensitive yang berkaitan dengan data pribadi mahasiswa. Data tersebut meliputi informasi identitas mahasiswa seperti nama lengkap, tempat dan tanggal lahir, serta Alamat domisili, hingga informasi orang tua seperti nama, instansi atau tempat bekerja, jabatan atau pangkat, dan data pendukung lainnya. Hal ini juga berkaitan dengan data yang dilindungi oleh UU PDP (Perlindungan data pribadi) sehingga Website web tersebut harus dapat memastikan aman sesuai dengan regulasi yang ada. Untuk itu pentingnya dilakukan analisis keamanan terhadap Website web fakultas, guna memastikan bahwa sistem tersebut memiliki keamanan yang baik terhadap ancaman eksternal seperti kebocoran data sensitif. Salah satu metode yang efektif untuk melakukan evaluasi

keamanan adalah *penetration testing* (pengujian penetrasi). Metode ini mensimulasikan serangan nyata yang dilakukan oleh pihak luar dengan tujuan untuk mengidentifikasi dan mengevaluasi kerentanan yang terdapat dalam sistem [7]. Selain memberikan gambaran tingkat keamanan, *pentest* juga membantu memetakan kerentanan berdasarkan tingkat resiko dari celah keamanan. Hal ini juga memungkinkan menentukan prioritas dalam menangani perbaikan.

Pentest juga tidak hanya berfungsi sebagai alat evaluasi tetapi juga dasar strategi mitigasi resiko keamanan. Pendekatan pentest juga sudah banyak digunakan dalam berbagai industri, termasuk bidang pendidikan karena sesuai dengan standar internasional. Dengan penerapan metode ini hasil yang diperoleh dapat memberikan validasi nyata terhadap keamanan Website sekaligus rekomendasi teknis yang dapat diimplementasikan secara praktis oleh pengembang maupun pihak pengelola sistem.

Dalam penelitian ini, metode pentest akan dilakukan menggunakan ISSAF (*Information System Security Assessment Framework*) dan *OWASP Testing Guide v4.2.* ISSAF sendiri adalah sebuah metodologi terbuka yang menyediakan tahapan sistematis dalam melakukan pengujian keamanan terhadap sistem informasi. ISSAF juga dirancang dalam bentuk yang terstruktur [8] dan juga menyediakan standar untuk setiap domain. Domain ini mencakup proses dari perencanaan, pengumpulan informasi, identifikasi kerentanan, eksploitasi, hingga pelaporan, dan dapat disesuaikan dengan pendekatan black box, Sehingga metode ini juga menjadi salah satu pendekatan yang efisien saat melakukan uji penetrasi [7].

Untuk melengkapi hal tersebut maka digunakan nya *OWASP testing guide v4.2* untuk mengklasifikasikan hasil temuan yang dimana kompehensif untuk pengujian keamanan Panduan ini mencakup berbagai metode pengujian untuk mengidentifikasi kerentanan dalam proses autentikasi, otorisasi, manajemen sesi, validasi input, serta aspek penting lainnya dalam keamanan web [9]. Penggunaan *OWASP testing guide v4.2* bertujuan untuk memberikan pemetaan risiko yang lebih terarah dan mudah dipahami, baik oleh pengembang maupun pihak manajemen [10][11][12].

OWASP Testing Guide v4.2 digunakan sebagai pelengkap metode ISSAF yang dimana metode tersebut berperan sebagai kerangka kerja utama yang mengatur perencanaan, pelaksanaan, hingga pelaporan pengujian, kerangka ini tidak memberikan klasifikasi kerentanan yang distandarisasi dan mudah dipahami. Oleh karena itu digunakannya OWASP Testing Guide yang menyediakan daftar pengujian yang komprehensif dan daftar kerentanan yang diakui secara internasional, mencakup autentikasi, otorisasi, manajemen sesi, validasi input, serta aspek penting lainnya dalam keamanan web. Dengan mengacu pada OWASP Testing Guide v4.2, hasil temuan dari proses pengujian dapat diklasifikasikan secara sistematis sehingga memudahkan pengembang dan manajemen dalam memahami tingkat risiko, menentukan prioritas perbaikan, serta mengambil keputusan strategis. Pendekatan kombinasi ISSAF dan OWASP Testing Guide memungkinkan penelitian ini tidak hanya memvalidasi keberadaan kerentanan secara terstruktur, tetapi juga memberikan pemetaan risiko yang jelas, terarah, dan sesuai dengan praktik terbaik industri, sehingga hasilnya lebih mudah diinterpretasikan dan ditindaklanjuti.

Melalui penelitian ini diharapkan juga dapat ditemukannya potensi kerentanan keamanan yang nyata pada website fakultas. Hasil pengujian ini juga diharapkan akan memberikan gambaran tingkat keamanan website serta disusun rekomendasi teknis yang relevan untuk perbaikannya. Dengan demikian, penelitian ini tidak hanya memberikan kontribusi akademik, tetapi juga berdampak langsung pada peningkatan keamanan dan keandalan layanan digital.

1.2 Rumusan Masalah

1. Apa saja kerentanan keamanan yang terdapat pada website Fakultas Sipatca.
2. Bagaimana hasil analisis kerentanan keamanan pada website Fakultas Sipatca menggunakan metode ISSAF dengan pendekatan black box?
3. Apa rekomendasi teknis yang dapat diberikan untuk meningkatkan keamanan website berdasarkan hasil pengujian dengan ISSAF dan *OWASP testing guide v4.2*?

1.3 Batasan Masalah

Batasan masalah pada pembahasan skripsi ini, yaitu :

1. Ruang lingkup sistem yang diuji dibatasi pada Website web yang diakses melalui domain https://sipatca.igsindonesia.org/ tanpa menyertakan sistem pendukung lain.
2. Pengujian hanya sampai tahap verifikasi kerentanan (proof of concept) tanpa melakukan eksploitasi penuh yang dapat merusak data atau mengganggu layanan
3. Pendekatan pengujian keamanan yang digunakan adalah black box, black box adalah pengujian yang dilakukan dari sudut pandang pihak eksternal tanpa mengetahui akses kode, sumber informasi internal ataupun sistem lainnya.
4. Penelitian ini hanya menyajikan hasil eksploitasi dan rekomendasi dari teknis-teknis tanpa melakukan perbaikan langsung pada sistem.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengidentifikasi dan menganalisis kerentanan keamanan pada Website SIPATCA menggunakan metode ISSAF, serta memberikan rekomendasi teknis untuk meningkatkan keamanan website berdasarkan hasil pengujian yang dilakukan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan pemahaman mengenai penerapan metode OWASP dalam pengujian keamanan website, menambah literatur akademik terkait analisis keamanan aplikasi web, serta membantu instansi dan pengembang sistem dalam mengetahui, menangani, dan memperbaiki kerentanan keamanan agar aspek keamanan website dapat lebih diperhatikan dalam proses pengembangan aplikasi.

1.6 Sistematika Penulisan

Penulisan skripsi ini disusun dengan sistematika penulisan untuk mempermudah melihat dan mengetahui pembahasan yang ada secara menyeluruh. Adapun sistematika penulisannya sebagai berikut :

BAB I PENDAHULUAN

Bagian ini menguraikan latar belakang yang mendasari dilakukannya penelitian, rumusan masalah yang menjadi fokus penelitian, batasan masalah, tujuan penelitian, serta sistematika penulisan skripsi secara keseluruhan.

BAB II TINJAUAN PUSTAKA

bagian ini memuat kajian terhadap penelitian terdahulu yang memiliki keterkaitan dengan topik yang diangkat, serta landasan teori yang digunakan sebagai dasar dalam mendukung pelaksanaan penelitian.

BAB III METODE PENELITIAN

Bagian ini menjelaskan tahapan-tahapan yang dilakukan dalam proses penelitian, mulai dari perencanaan hingga pelaksanaan, serta metode penetration testing berbasis ISSAF dan OWASP WSTG V4.2 yang digunakan sebagai pendekatan dalam melakukan pengujian keamanan sistem.

BAB IV HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil yang diperoleh selama proses pengujian serta pembahasan terhadap temuan yang dihasilkan. Selain itu, dilakukan analisis terhadap kerentanan yang ditemukan berdasarkan acuan OWASP WSTG v4.2.

BAB V PENUTUP

Bagian ini berisi kesimpulan yang diperoleh dari keseluruhan hasil penelitian serta saran yang dapat dijadikan sebagai bahan pertimbangan untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

Bagian ini mencantumkan literatur yang digunakan sebagai referensi dalam penyusunan skripsi, memberikan dasar yang kuat bagi argumen dan analisis yang disajikan

LAMPIRAN

Bagian ini berisi data tambahan atau informasi pendukung yang berkaitan dengan penelitian, seperti test case, test reporting, serta dokumentasi percobaan yang dilakukan selama proses pengujian keamanan sistem.