BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Teknologi terdiri dari pengembangan perangkat lunak (*software*) dan perangkat keras (*hardware*) yang didasarkan pada ilmu pengetahuan dan disesuaikan dengan kebutuhan pengguna saat ini. Dengan kemajuan teknologi, pengguna masih dapat melakukan tugas-tugas yang sebelumnya membutuhkan bantuan tangan sekarang dilakukan dengan bantuan alat elektronik. Misalnya, meskipun pengguna masih menggunakan tangan untuk membuat laporan keuangan dan surat menyurat, pengguna dapat membuat laporan keuangan dengan komputer dan aplikasi (Ahmad Taufik et al., 2022). Pada saat ini, teknologi berkembang dengan sangat cepat. Hal ini dapat dilihat dari jumlah pengguna web yang semakin meningkat untuk memenuhi kebutuhan organisasi, institusi pendidikan, atau individu. Asosiasi Penyelenggara Jasa Internet Indoensia (APJII) melaporkan bahwa jumlah pengguna internet di Indonesia akan naik mencapai 210,03 juta pada tahun 2021-2022, naik 3,32% dari tahun sebelumnya (Asosiasi Penyelenggara Jasa Internet Indonesia, 2022). *Website* merupakan salah satu tujuan utama bagi pengguna internet khususnya dalam memanfaatkannya untuk melakukan aktifitas baik untuk keperluan bisnis mupun mengakses sebuah informasi (Hidayatulloh & Saptadiaji, 2021). Terdapat banyak ancaman yang sering terjadi pada saat pengguna menggunakan akses internet, salah satunya yaitu yang terjadi pada aplikasi *website* (Yusuf DM et al., 2022). Salah satu elemen penting dalam segala hal adalah keamanan komputer. Seiring dengan meningkatnya jumlah orang yang terhubung ke internet, kebutuhan akan sistem keamanan komputer meningkat karena hal ini dapat mencegah tindak kejahatan *cyber* oleh individu yang tidak bertanggung jawab.

Kerentanan keamanan informasi adalah awal serangan pada *website*, dari celah keamanan yang ada, penyerang akan memanfaatkan celah-celah yang ada untuk dapat memasuki sistem *website* dan menggunakan celah untuk merusak atau

mencuri data pada *website* tersebut. Selain masalah keamanan data, celah keamanan juga berdampak pada reputasi sebuah *website*, semakin banyak celah keamanan yang ditemukan di sebuah *website*, reputasinya akan menurun, dan pengunjung akan merasa ragu untuk mengunjungi *website* dengan reputasi buruk karena mereka takut data pribadi mereka tidak aman. Serangan yang sering diimplementasikan dalam pengujian penetrasi termasuk *SQL Injection, Cross-Site Scripting (XSS), Denial of Service (DOS), Brute Force Attack, Sniffing, Clickjacking, dan Cross-Site Request Forgery (CSRF)* dan autentikasi atau sesi yang rusak (Ujung & Nasution, 2023). Karena itu, pengujian keamanan dibutuhkan dalam upaya identifikasi dan evaluasi terhadap celah keamanan serta fungsi sistem yang telah berjalan. Tinjauan keamanan sistem menjadi elemen penting dalam deteksi masalah keamanan serta evaluasi menyeluruh terhadap kelangsungan operasional. Proses pengujian keamanan menjadi kunci untuk memahami secara mendalam kesalahan dan kelemahan yang mungkin termanifestasi baik dalam desain maupun operasionalitas sistem yang bersangkutan. *Open Web Application Security Project* (OWASP) merupakan organisasi yang bertugas menangani dan mencegah masalah keamanan sistem web. OWASP Top 10 adalah daftar kerentanan yang dibuat oleh komunitas OWASP yang mencakup sepuluh kerentanan terpenting yang dapat mengancam keamanan web. Tujuannya adalah agar keamanan perangkat lunak terlihat oleh individu dan organisasi sehingga mereka dapat membuat keputusan yang tepat tentang ancaman keamanan perangkat lunak mereka. Serangan aplikasi berbasis web sering terkena berbagai serangan yang sering dimanfaatkan oleh penyerang, seperti *SQL Injection, Cross-Site Scripting (XSS), Denial Of Service (DOS), Brute Force Attacks, Sniffing, Clickjacking, Cross-Site Request Forgery (CSRF),* dan sesi atau autentikasi yang rusak (Edy Listartha et al., 2022). Dalam konteks ini, penting untuk melakukan evaluasi dan pengujian keamanan secara teratur. Metode yang tepat dan terstruktur diperlukan untuk mengidentifikasi, mengevaluasi, dan mengatasi potensi celah keamanan dalam sistem informasi calon mahasiswa baru. Berbagai metodologi pengujian keamanan seperti *Open Web Application Security Project* (OWASP), *Penetration Testing Execution Standard* (PTES), *Information System Security Assessment Framework* (ISSAF), dan NIST SP 800-115 dapat

digunakan sebagai panduan dan landasan untuk melakukan evaluasi keamanan sistem (Aryanti et al., 2021). Adapun untuk metodologi yang digunakan di penelitian ini ialah NIST SP 800-115 karena metode tersebut sangat membantu dalam melakukan perencanaan dan pengujian teknikal keamanan informasi. Selain itu, NIST SP 800-115 menyediakan metode *penetration testing* yang dibutuhkan dalam penelitian ini. Dalam konteks SICAMA, pendekatan ini memungkinkan identifikasi dan penanganan potensi celah keamanan yang ada. Evaluasi keamanan sistem informasi SICAMA di Universitas Jenderal Achmad Yani Yogyakarta bertujuan untuk mengidentifikasi, mengevaluasi, dan memberikan saran perbaikan celah keamanan berdasarkan OWASP TOP 10 Tahun 2021. Dengan melakukan evaluasi ini, diharapkan sistem informasi ini dapat terlindungi dengan baik, memberikan kontribusi positif dalam mendukung proses penerimaan mahasiswa baru, serta mempertahankan integritas data dan kepercayaan masyarakat pada universitas.

Sistem Informasi Calon Mahasiswa Baru (SICAMA) di Universitas Jenderal Achmad Yani Yogyakarta adalah *platform* vital yang mengelola proses pendaftaran, informasi, dan layanan yang berkaitan dengan penerimaan mahasiswa baru. Sistem ini mengintegrasikan informasi-informasi terkait penerimaan mahasiswa, proses administrasi, dan berbagai layanan yang diperlukan calon mahasiswa, seperti informasi program studi, prosedur pendaftaran, dan panduan administrasi. Dalam menghadapi perkembangan teknologi yang pesat, perlindungan keamanan sistem informasi menjadi aspek krusial. Karena jumlah pengguna internet terus meningkat, perlindungan terhadap sistem ini menjadi semakin penting untuk mencegah ancaman *cyber* yang dapat merugikan baik bagi integritas data maupun reputasi universitas. Kerentanan keamanan informasi pada sistem seperti SICAMA adalah titik awal serangan terhadap sistem tersebut. Serangan dapat dimulai dari celah keamanan yang ada dan dimanfaatkan untuk mengakses sistem, merusak data, atau bahkan mencuri informasi penting. Keberhasilan operasional sistem informasi dan kepercayaan masyarakat pada universitas tergantung pada seberapa kuatnya perlindungan keamanan yang diterapkan.

1. Selain kerentanan terhadap serangan yang dapat mengganggu integritas dan operasionalitas sistem, Sistem Informasi Calon Mahasiswa Baru (SICAMA) juga harus berhati-hati terhadap potensi ancaman terhadap data dan informasi pribadi calon mahasiswa. Dalam konteks ini, keamanan informasi menjadi aspek krusial yang harus dijaga dengan ketat. Serangan yang berhasil pada sistem seperti SICAMA dapat mengakibatkan akses tidak sah terhadap data pribadi calon mahasiswa, seperti informasi identitas, riwayat akademik, dan informasi keuangan. Hal ini dapat mengakibatkan pencurian identitas, penyalahgunaan informasi pribadi, atau bahkan penggunaan informasi tersebut untuk tujuan kriminal seperti penipuan atau pemerasan. Oleh karena itu, penilaian keamanan *website* menjadi langkah yang sangat penting dalam upaya mencegah bahaya-bahaya tersebut. Dengan melakukan penilaian keamanan secara teratur menggunakan metodologi yang sesuai seperti NIST SP 800-115, tim pengembang dan pengelola SICAMA dapat mengidentifikasi celah keamanan potensial dan mengambil langkah untuk memperkuat sistem. Ini dapat melibatkan penerapan langkah-langkah pengamanan seperti enkripsi data, autentikasi yang kuat, penggunaan protokol keamanan yang tepat, dan pemantauan aktif terhadap aktivitas yang mencurigakan. Dengan mengutamakan keamanan *website* melalui penilaian yang cermat, SICAMA dapat memastikan bahwa data dan informasi pribadi calon mahasiswa tetap aman dan terlindungi. Selain itu, tindakan ini juga akan membantu mempertahankan reputasi universitas dalam hal perlindungan privasi dan keamanan data, yang merupakan faktor penting dalam membangun kepercayaan masyarakat dan calon mahasiswa terhadap institusi tersebut. Pentingnya penilaian keamanan dalam mengelola Sistem Informasi Calon Mahasiswa Baru (SICAMA) tak terbantahkan, karena hal ini memungkinkan celah keamanan potensial yang dapat dieksploitasi oleh pihak tidak bertanggung jawab.

1.2 PERUMUSAN MASALAH

Berdasarkan penjelasan latar belakang terdapat data dan informasi yang bersifat krusial pada *website* SICAMA Universitas Jenderal Achmad Yani Yogyakarta sehingga diperlukan sistem keamanan yang dapat melindungi data dan informasi. Rumusan masalah penelitian ini adalah menerapkan proses pengujian penilaian kerentanan yang mengacu pada standar *framework Open Web Application Security Project (OWASP) TOP 10* menggunakan metode NIST SP 800-115. Penelitian ini menekankan betapa pentingnya melakukan evaluasi terhadap kerentanan keamanan yang ada dalam *website* untuk melindungi data dan informasi yang tersimpan.

1.3 PERTANYAAN PENELITIAN

Beberapa pertanyaan yang menjadi dasar penelitian ini sebagai berikut :

1. Bagaimana cara mengidentifikasi kerentanan sistem pada *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta menggunakan *Open Web Application Security Project (*OWASP*) TOP 10* dan NIST SP 800-115?
2. Bagaimana hasil penilaian dan analisis kerentanan pada *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta?

1.4 TUJUAN PENELITIAN

Tujuan yang akan dicapai dalam penelitian ini adalah sebagai berikut :

1. Mengidentifikasi kerentanan sistem pada *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta.
2. Mengetahui hasil analisis kerentanan pada *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta dengan menggunakan *Open Web Application Security Project* (OWASP) TOP 10 dan metode NIST SP 800-115.

1.5 MANFAAT HASIL PENELITIAN

Manfaat yang diperoleh dengan adanya penelitian ini adalah sebagai berikut:

1. Mengetahui celah kerentanan dan hasil penilaian yang ada pada *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta menggunakan *Open Web Application Security Project (*OWASP*) TOP 10* dan NIST SP 800-115
2. Sebagai evaluasi untuk pengelola *website* layanan Sistem Informasi Calon Mahasiswa Baru (SICAMA) Universitas Jenderal Achmad Yani Yogyakarta untuk meningkatkan keamanan sistem, mengatasi ancaman keamanan serangan cyber, dan memastikan ketersediaan layanan publik secara *online*.