BAB I
PENDAHULUAN

1.1 Latar Belakang

Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengumukan jumlah pengguna internet Indonesia tahun 2024 mencapai 221.563.479 jiwa dari total populasi 278.696.200 jiwa penduduk Indonesia tahun 2023. Semakin maju Indonesia dalam bidang teknologi dan informasi semakin cepat pula kita dalam mengakses sebuah informasi dengan cepat. Hal ini yang menjadi salah satu fasilitas terutama bagi seorang mahasiswa, penggunaan teknologi informasi adalah syarat utama untuk meningkatkan efektifitas waktu dan hasil yang terbaik (Ngantung & Pakereng, 2021).

Dalam dunia pendidikan modern, sistem informasi akademik kampus berbentuk sebuah *website*. *Website* adalah kumpulan komponen yang terdiri dari teks, gambar, suara animasi merupakan media informasi yang menarik dan diminati digunakan sebagai media berbagai informasi (Arief & Sugiarti, 2022). Dan hal tersebut menjadi salah satu elemen kunci yang memfasilitasi berbagai aktivitas kegiatan akademik dan administratif di kampus tersebut. *Website* tersebut tidak hanya menjadi sumber informasi penting bagi mahasiswa, dosen, dan staf administrasi, tetapi juga menjadi *platform* vital untuk pengelolaan data mahasiswa, jadwal kuliah, registrasi kursus, dan informasi lainnya yang berkaitan dengan kegiatan akademik.

Namun dengan kelebihan tersebut, *website* sistem informasi akademik kampus juga menghadapi berbagai ancaman keamanan yang kompleks dan berkembang pesat. Kesalahan pada penulisan kode program dalam pembuatan aplikasi berbasis *website* sering dimanfaatkan oleh penyerang, dalam hal ini serangan yang sering dimanfaatkan oleh penyerang diantaranya serangan siber seperti injeksi *SQL*, *cross-site scripting* (XSS), serangan *brute force*, dan serangan *DDoS* (Ghozali et al., 2019). Hal tersebut dapat mengancam keamanan dan stabilitas *website*, serta mengakibatkan kebocoran data sensitif atau gangguan pada layanan penting.

Untuk melindungi *website* sistem informasi akademik kampus dari serangan-serangan ini, diperlukan pendekatan proaktif yang mencakup identifikasi, evaluasi, dan penanganan potensi kerentanan keamanan. Salah satu metode yang telah diakui secara luas dalam melakukan analisis keamanan *website* adalah menggunakan OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*). OWAPS adalah komunitas non-profit yang bertujuan untuk meningkatkan keamanan perangkat lunak. Metode OWASP sendiri telah digunakan pada penelitian sebelumnya dengan judul "*Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP*" (Priyawati et al., 2022). Salah satu *software* yang dikembangkan oleh OWASP dan digunakan untuk penelitian ini adalah ZAP. ZAP adalah *scan tool* yang digunakan untuk menemukan celah keamanan pada aplikasi *website* saat pengembangan dan pengujian aplikasi *website*.

Tujuan dari penelitian ini adalah untuk mengidentifikasi celah-celah keamanan pada sistem informasi akademik kampus, serta menganalisis tingkat risiko keamanan berdasarkan klasifikasi standar OWASP TOP 10 terbaru. Studi dilakukan pada situs Sistem Informasi Akademik (SIAKAD) Universitas Merdeka Malang. Hasil identifikasi yang dilakukan melalui pengujian keamanan kemudian digunakan untuk memberikan rekomendasi kepada institusi agar dapat melakukan peningkatan keamanan sistem. Melalui penelitian ini diharapkan dapat memberikan kontribusi positif dalam peningkatan keamanan serta kualitas pelayanan *website* sistem informasi akademik kampus, serta memperkaya pemahamanan tentang analisis keamanan website menggunakan metode OWASP ZAP.

1.2 Rumusan Masalah

Dalam penggunaan OWASP ZAP sebagai metode analisis keamanan sebuah *website*, terdapat beberapa hal yang dapat dijadikan sebuah pertanyaan seperti:

- Bagaimana penggunaan metode OWASP ZAP dalam mendeteksi kerentanan keamanan pada *website* sistem informasi akademik kampus?

- Bagaimana hasil pengujian keamanan dan rekomendasi dari kerentanan keamanan yang berhasil teridentifikasi?

1.3 Tujuan

Tujuan dari penelitan penggunaan metode OWASP ZAP untuk analisis keamanan sebuah *website* sistem akademik kampus, sebagai berikut :

1. Menerapkan langkah-langkah penggunaan metode OWASP ZAP dalam mendeteksi dan mengidentifikasi kerentanan keamanan sebuah *website* sistem informasi akademik kampus.
2. Menganalisis hasil pengujian kemananan dan rekomendasi dari kerentanan keamanan yang berhasil teridentifikasi.

1.4 Manfaat Penelitian

Beberapa manfaat dari penelitian metode OWASP ZAP sebagai analisis keamanan sebuah *website* sistem akademik kampus, sebagai berikut :

1.4.1 Manfaat bagi peneliti

1. Penambahan dan Pengembangan Wawasan: Peneliti akan mendapatkan pengalaman praktis saat melakukan analisis keamanan *website* dengan metode OWASP ZAP. Hal ini akan membantu peneliti dalam pengembangan dan penambahan wawasan secara teknis dalam bidang keamanan siber.
2. Pemahaman Mendalam: Peneliti akan memeperoleh pemahaman yang lebih mendalam tentang ancaman keamanan yang mungkin akan dihadapi sebuah *website* sistem informasi akademik kampus, beserta cara-cara untuk mengidentifikasi, mengevaluasi, dan mengatasi kerentanan tersebut.

1.4.2 Manfaat bagi Institusi Perguruan Tinggi

1. Peningkatan Keamanan Website: Institusi perguruan tinggi akan memperoleh pemahaman yang lebih baik tentang keamanan *website* sistem informasi akademik kampus mereka dan dapat mengambil langkah-langkah yang sesuai untuk memperkuat keamanannya. Hal ini juga membantu melindungi data sensitif mahasiswa, dosen, dan staf.
2. Kepatuhan Regulasi Perlindungan Data: Diharapkan penelitian ini dapat membantu institusi perguruan tinggi untuk memenuhi persyaratan keamanan data sesuai regulasi yang ada, seperti GDPR (*General Data Protection Regulation*) atau peraturan perlindungan data di Indonesia.

1.5 Batasan Masalah

Dalam penelitian analisis ancaman keamanan menggunakan metode OWASP ZAP pada *website* sistem informasi akademik kampus, terdapat beberapa batasan masalah yang perlu diperhatikan untuk menjaga fokus dan keakuratan penelitian. Berikut adalah batasan-batasan masalah yang ditetapkan:

- Analisis ini hanya mencakup *website* sistem informasi akademik kampus dan tidak termasuk aplikasi atau sistem lain yang mungkin terhubung secara langsung atau tidak langsung.
- Pengujian dilakukan menggunakan alat OWASP ZAP yang fokus pada identifikasi kerentanan keamanan berbasis *website*.
- Analisis kerentanan terbatas pada OWASP Top 10 2021, yang mencakup 10 kategori risiko keamanan aplikasi *website* yang paling umum.
- Hanya kerentanan yang teridentifikasi oleh OWASP ZAP dalam ruang lingkup pengujian yang akan dibahas.