BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin canggih telah memberikan kemudahan dalam hal penyimpanan, pengolahan, hingga pengamanan data[1]. Selain itu, teknologi informasi seperti internet dan aplikasi *website* menjadi perpaduan penting untuk menggantikan kebiasaan lama yang tidak terkomputerisasi[2][3]. Saat ini, aplikasi *website* menjadi jenis teknologi yang banyak digunakan oleh berbagai organisasi, termasuk institusi pendidikan untuk menyampaikan informasi. Namun, pemilik atau pengelola sistem seringkali mengabaikan masalah keamanan[4].

Menurut Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada tahun 2021 terdapat laporan serangan siber dengan 10 peringkat besar yang terjadi di Indonesia (data lengkap tersedia di situs cloud.bssn.go.id). Adapun berikut beberapa ancaman aplikasi *website* yang umum terjadi antara lain SQL *Injection*, *Cross Site Scripting* (XSS), *Cookie/Session Poisoning*, *Form Tampering*, *Code Injection*, dan *Defacement*[5].

Keamanan pada sistem informasi memiliki tingkat yang berbeda-beda antara satu organisasi dengan organisasi lainnya, hal ini bertujuan untuk mencegah, mendeteksi kerusakan pada sistem, dan terhindar dari serangan siber[6][7][8]. Keamanan sistem informasi dapat dicapai dengan melakukan sebuah pengujian yang berkaitan dengan keamanan siber, contohnya adalah *penetration testing*. *Penetration testing* adalah suatu kegiatan untuk melakukan eksploitasi sistem dengan cara legal yang bertujuan untuk mendapatkan akses ke data sensitif[9]. Seorang penguji harus memiliki izin yang sudah disetujui institusi terkait untuk melakukan *penetration testing*[10].

Salah satu metode yang digunakan dalam *penetration testing* adalah *Open Web Application Security Project* (OWASP) Top 10 2021. OWASP adalah sebuah *framework* yang bersifat *open source* dan memiliki tujuan dalam memperbaiki sistem aplikasi *website*[11]. OWASP menggunakan 10 daftar risiko keamanan aplikasi *website* paling populer yang digunakan untuk menyelidiki potensi ancaman dan risiko[12]. OWASP menggunakan *vulnerability scanner tools* dengan menggabungkan beberapa

security project tools dalam mencari celah keamanan, kemudian melakukan pengujian pada kerentanan yang didapatkan untuk mengetahui keamanan suatu aplikasi *website*[13][14].

Universitas AMIKOM Yogyakarta merupakan salah satu institusi pendidikan di Indonesia yang memanfaatkan teknologi informasi berupa aplikasi *website* yang terkoneksi pada jaringan internet sebagai media dalam menyampaikan informasi kepada civitas akademik maupun non akademik guna memudahkan aktivitas penyampaian informasi. Meskipun pertukaran informasi hanya dapat diakses oleh orang-orang tertentu, namun tetap saja masih ada kemungkinan pihak-pihak yang tidak bertanggung jawab dapat mengaksesnya dan menyalahgunakannya yang menyebabkan kerugian bagi institusi terkait.

Berdasarkan latar belakang yang sudah dijelaskan, salah satu upaya yang dapat dilakukan adalah melakukan analisis dan pengujian celah keamanan. Dalam hal ini aplikasi *website dashboard* mahasiswa di Universitas AMIKOM Yogyakarta akan dijadikan sebagai target dalam menemukan celah keamanan dengan *domain* yang akan diuji yaitu mhs.amikom.ac.id yang berfokus pada pengumpulan informasi dan pengujian sistem menggunakan metode *Open Web Application Security Project* (OWASP) dengan standar keamanan Top 10 2021. Hasil analisis keamanan berupa laporan dokumentasi pertanggung jawaban yang berisi daftar celah keamanan dan rekomendasi perbaikan pada sistem aplikasi *website*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dijelaskan, adapun rumusan masalah dari penelitian ini adalah bagaimana melakukan analisis dan pengujian celah keamanan pada sistem aplikasi *website* di Universitas AMIKOM Yogyakarta berdasarkan Top 10 *Web Application Security Risks* 2021?

1.3 Batasan Masalah

Berdasarkan rumusan masalah sebelumnya, maka batasan masalah sebagai berikut:

1. Aplikasi *website dashboard* yang akan diuji yaitu *domain* mhs.amikom.ac.id di Universitas AMIKOM Yogykarta.
2. Sistem operasi yang digunakan dalam pengujian yaitu menggunakan Kali Linux dan *penetration testing tools* yang digunakan antara lain Whois,

Harvester, Whatweb, Google *Database*, Nmap, OWASP ZAP, Acunetix, Burp Suite, Cookie Editor, dan XXS Hunter.

3. Laporan berupa dokumen pertanggung jawaban yang berisi rekomendasi perbaikan akan diserahkan sepenuhnya pada institusi terkait dalam hal ini Universitas AMIKOM Yogyakarta.

1.4 Tujuan Penelitian

Berdasarkan latar belakang yang sudah dijelaskan, adapun tujuan dari penelitian ini adalah analisis dan pengujian celah keamanan dapat digunakan sebagai bahan perbaikan sistem aplikasi *website* di Universitas AMIKOM Yogyakarta.

1.5 Manfaat Penelitian

Berdasarkan hasil analisis keamanan aplikasi website yang telah dilakukan, adapun manfaat dari penelitian ini sebagai berikut.

1. Bagi Institusi
   a. Sebagai acuan untuk bahan evaluasi dan perbaikan keamanan sistem pada aplikasi *website*.
   b. Sebagai acuan untuk meningkatkan keamanan sistem pada aplikasi *website*.
   c. Sebagai acuan untuk mencegah terjadinya serangan dalam dunia maya.
2. Bagi penelitian selanjutnya
   a. Sebagai acuan untuk memberikan gambaran tentang keamanan sistem pada aplikasi *website*.
   b. Sebagai referensi terhadap penelitian keamanan sistem pada aplikasi *website* selanjutnya.

1.6 Sistematika Penelitian

Sistematika penelitian dengan judul implementasi *Open Web Application Security Project* untuk *Penetration Testing* pada *website* Institusi Pendidikan sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan

masalah, tujuan penelitian, manfaat penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang penelitian-penelitian sebelumnya yang menjadi studi literatur dan dasar teori yang berkaitan dengan pembahasan dalam penelitian ini seperti *penetration testing*, keamanan sistem informasi, OWASP, dan aplikasi *website*.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang metode pengujian sistem serta langkah-langkah yang dilakukan dalam penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan hasil pengujian dan analisis sistem berdasarkan metode OWASP Top 10 2021 sebagai acuan standar keamanan aplikasi *website* dan rekomendasi perbaikan sistem.

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil dan pembahasan penelitian ini serta saran yang membangun agar penelitian selanjutnya dapat menjadi lebih baik lagi.