# BAB I. PENDAHULUAN

## 1.1. Latar Belakang

Pada era yang canggih dan serba maju seperti jaman sekarang, semua orang pasti sudah mengenal dengan yang namanya internet mulai dari anak muda hingga orang dewasa. Internet dapat dikatakan sebagai bagian dari kehidupan manusia yang tidak dapat dilepaskan. Laporan bertajuk "Digital 2021" yang dirilis oleh layanan manajemen koten Bernama *HootSuite* mengatakan bahwa pada awal tahun 2021 Indonesia memiliki pengguna internet sebanyak 202,6 juta jiwa. Jumlah tersebut mengalami peningkatan sebanyak 27 juta jiwa atau setara dengan 15,5 persen dibandingkan dengan awal tahun 2020 lalu. Hal tersebut tentunya terjadi karena pandemi COVID-19 yang terjadi pada tahun 2020 lalu. Masyarakat dipaksa untuk menggunakan internet dan melakukan semuanya secara daring mulai dari sekolah *online* hingga bekerja atau dapat disebut dengan *Work From Home* (WFH).

Pelaksanaan sekolah atau kuliah yang dilakukan secara *online* tentunya dilengkapi dengan fasilitas-fasilitas yang mendukung situasi belajar mengajar sehingga fasilitas *online* tersebut memiliki fungsionalitas yang sama dengan fasilitas *offline*. Fasilitas tersebut dapat berupa *website* atau aplikasi yang dapat digunakan dalam proses pembelajaran. Fasilitas tersebut juga dapat digunakan untuk mengumpulkan tugas, mengikuti perkuliahan secara daring, mengakses informasi mengenai kampus dan informasi mengenai materi yang mendukung perkembangan siswa. Akan tetapi hal-hal positif yang ditawarkan oleh teknologi, terdapat pula hal-hal yang negative salah satunya adalah peretasan atau *hacking* yang dilakukan oleh oknum-oknum yang tidak bertanggung jawab yang sengaja dilakukan untuk memperoleh data-data sensitif.

Keamanan aplikasi web menjadi hal yang penting dalam menjaga informasi yang berada didalamnya. Terjadi sebanyak 88.414.296 serangan siber atau *cyber attack* pada bulan 1 Januari hingga 12 April 2020 yang dicatat oleh Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN). Dampak dari serangan siber atau *cyber attack* dapat bervariasi sesuai dengan skalanya, mulai dari pengaturan lampu pada lalu lintas hingga peretasan kode nuklir berbahaya. Intinya jika keamanan aplikasi web tidak dijaga maka suatu

informasi yang tidak dapat diakses oleh suatu orang dapat diakses dan disalahgunakan jika jatuh ke tangan orang yang tidak bertanggung jawab.

Sistem Informasi Kemahasiswaan atau yang dikenal oleh mahasiswa Universitas Atma Jaya Yogyakarta sebagai SIKMA merupakan salah satu web informasi kemahasiswaan yang dapat diakses oleh seluruh mahasiswa UAJY. Pada web tersebut mahasiswa dapat mendaftar beberapa acara yang tersedia di UAJY, konseling dengan romo atau suster dan fitur yang paling sering dipakai oleh mahasiswa UAJY yaitu SPAMA. Jika keamanan web SIKMA tersebut tidak dijamin maka seseorang yang tidak berhak dapat mengatur data-data sertifikat dan poin SPAMA yang dimiliki oleh mahasiswa dan dapat disalahgunakan. Maka dari itu penulis ingin melakukan pentest pada aplikasi *website* tersebut sehingga hal-hal tersebut tidak terjadi. Karena proses pentest ini memerlukan adanya peretasan dan pencarian celah-celah yang terdapat pada *website*, maka dari itu aktivitas ini dapat disebut dengan serangan siber. Maka dari itu juga diperlukan adanya persetujuan dengan pihak yang terkait dengan pemilik *website*.

Pada penelitian ini juga digunkan *framework* ISSAF sebagai metodologi dari kegiatan pentest. *Framework* merupakan sebuah kerangka dalam suatu aplikasi atau *website*, jadi *framework* ISSAF (*Information System Security Assessment Framework*) merupakan suatu kerangka pentest yang memiliki struktur teratur berfungsi untuk memberikan arahan kepada penguji. *Framework* ISSAF juga memiliki keunggulan dalam kontrol keamanan suatu sistem dan dapat menghindari kesalahan umum yang terjadi karena metode serangan yang acak. Penguji mengharapkan bahwa celah keamanan yang terdapat pada *website* SIKMA dapat ditemukan dan dianalisa dan perbandingan mengenai aplikasi yang digunakan untuk menemukan celah-celah tersebut. Maka dari itu pengujian ini penting dan layak menjadi kajian skripsi. Pada pengujian ini digunakan aplikasi Nessus, Burp Suite dan Metasploit untuk mencari kelemahan atau kerentanan target *website* dan dibandingkan antar satu dengan yang lainnya.

## 1.2. Rumusan Masalah

Terdapat beberapa rumusan masalah yang terdapat pada penelitian ini berdasarkan latar belakang:

1. Bagaimana cara melakukan pengujian keamanan pada *website* sikma.uajy.ac.id Universitas Atma Jaya Yogyakarta?
2. Celah keamanan apa saja yang ada pada *website* sikma.uajy.ac.id Universitas Atma Jaya Yogyakarta?
3. Bagaimana perbandingan dari hasil pemindaian situs sikma.uajy.ac.id menggunakan Nessus, Burp Suite dan Metasploit pengujian celah keamanan yang digunakan?

## 1.3. Batasan Masalah

Adapun batasan-batasan masalah yang terdapat pada pengujian ini:

1. Pengujian yang dilakukan terbatas pada keamanan *website* sikma.uajy.ac.id menggunakan *framework* ISSAF.
2. Identifikasi kerentanan website menggunakan *tool* Nessus, Burp Suite dan Metasploit.
3. Metode *vulnerability test* diterapkan pada *website* situs sikma.uajy.ac.id.

## 1.4. Tujuan Penelitian

Tujuan dari penelitian yang dilakukan adalah:

1. Menganalisa celah keamanan yang terdapat pada *website* sikma.uajy.ac.id Universitas Atma Jaya Yogyakarta.
2. Mengetahui tingkat keamanan *website* sikma.uajy.ac.id Universitas Atma Jaya Yogyakarta.
3. Mengetahui aplikasi yang sesuai untuk melakukan aktifitas pemindaian berdasarkan framework ISSAF dalam pencarian celah keamanan terhadap situs sikma.uajy.ac.id.

## 1.5. Metode Penelitian

Beberapa metode atau tahapan yang digunakan dalam ISSAF (*Information*

*System Security Assessment Framework*):

*A. Information Gathering*

Pada tahap ini, sesuai dengan namanya yaitu pengumpulan informasi atau *information gathering* maka dilakukan pengumpulan informasi target yaitu *website* yang akan diteliti. Informasi tersebut dapat berupa DNS, IP *lookup* dan informasi umum *website* lainnya.

*B. Network Mapping*

Pada tahap *network mapping*, dilakukan pengumpulan informasi yang lebih spesifik dibandingkan dengan tahap sebelumnya mengenai jaringan target. Informasi tersebut merupakan *port-port* yang digunakan oleh target.

*C. Vulnerability Identification*

Setelah itu adalah tahap *vulnerability identification* atau identifikasi kerentanan. Pada tahap ini akan dilakukan pemindaian pada *website* target untuk melihat apakah *website* memiliki kerentanan atau tidak.

## 1.6. Sistematika Penulisan

Sistematika penulisan akan memberikan gambaran secara umum mengenai topik yang akan dibahas pada tiap bab. Adapun penjelasannya sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan laporan *vulnerability testing* pada subdomain sikma.uajy.ac.id.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penelitian yang telah dilakukan oleh orang lain yang akan diadikan pembanding terhadap penguian ini.

BAB III LANDASAN TEORI

Bab ini berisi teori-teori yang akan diterapkan pada *vulnerability testing*. Di dalam bab ini juga dielaskan tentang metode dan alat yang akan digunakan untuk pengujian.

BAB IV ANALISIS DAN PERANCANGAN PENGUJIAN

Bab ini berisi tentang hasil dari analisis dan perancangan pengujian.

BAB V HASIL DAN PEMBAHASAN PENGUJIAN

Bab ini berisi tentang hasil yang diperoleh dari proses pengujian keamanan yang dilakukan terhadap web target.

BAB VI PENUTUP

Bab ini berisi kesimpulan yang diambil dari hasil penelitian dan saran untuk membangun pengembangan penelitian selanjutnya.