BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem informasi telah menjadi elemen kunci dalam operasi bisnis modern. Sistem ini digunakan untuk menyimpan, mengelola, dan mengakses data penting yang berperan dalam pengambilan keputusan, produktivitas, dan efisiensi perusahaan. Namun, dengan meningkatnya kompleksitas teknologi informasi dan meningkatnya ancaman siber, keamanan sistem informasi menjadi salah satu aspek yang paling vital. Organisasi dihadapkan pada berbagai tantangan keamanan, termasuk serangan siber yang semakin canggih seperti peretasan, *malware*, *phishing*, dan banyak lagi.

Universitas Pembangunan Nasional "Veteran" Jawa Timur memiliki beberapa website yang digunakan untuk menunjang proses perkuliahan. Pada tanggal 15 Februari 2022 beberapa website UPN "Veteran" Jawa Timur diretas oleh kelompok *hacker*. Peretas melakukan deface atau mengubah tampilan visual dari situs website yang berhasil diretas (Alfarizy, 2022). Untuk itu diperlukan pengujian keamanan pada website UPN "Veteran" Jawa Timur agar tidak terjadi lagi peretasan yang dilakukan oleh orang yang tidak bertanggung jawab. Salah satunya adalah Sistem Informasi Akademik (SIAMIK), sistem yang berisi informasi perkuliahan dan mengatur akademik mahasiswa. Celah keamanan yang ada dalam SIAMIK dapat menyebabkan kerugian finansial yang signifikan, merusak reputasi instansi, bahkan melanggar kebijakan privasi data mahasiswa. Oleh karena itu, diperlukan pengujian keamanan SIAMIK untuk evaluasi tingkat keamanannya.

Ada beberapa standar keamanan yang dapat digunakan untuk menjadi landasan uji penetrasi antara lain ISO Standart, ISSAF, NIST CSF, OWASP, dan beberapa standar lainnya. Pada tesis yang disusun (Burkan & Tanase, 2021) membahas Analisis dan Kerangka Keamanan Siber untuk Perusahaan TI, terdapat analisis terhadap kerangka kerja OWASP, ISO 27000/27001, dan NIST. Dalam analisis tersebut, terlihat bahwa OWASP merupakan satu-satunya kerangka kerja yang

bersifat open source dan dapat diakses oleh siapa pun. Hal ini menjadikannya unggul, terutama bagi perusahaan dengan keterbatasan ekonomi, karena dapat digunakan tanpa biaya yang besar. Keunggulan lainnya dari OWASP adalah daftar Top 10 yang selalu diperbarui secara rutin oleh sebuah tim yang terdiri dari pakar-pakar keamanan website di seluruh dunia. Terdapat tiga kategori baru, empat kategori dengan penamaan dan perbuahan ruang lingkup, dan beberapa konsolidasi baru di Top 10 untuk 2021 (OWASP, 2021). Dengan demikian, perusahaan yang menggunakan kerangka kerja ini dapat terhindar dari menggunakan pedoman yang sudah usang. OWASP Top 10 lebih berfokus pada keamanan aplikasi web, OWASP Top 10 membantu dalam memperbaiki celah keamanan spesifik di aplikasi web mereka, sedangkan NIST CSF memberikan panduan yang lebih luas untuk meningkatkan keamanan informasi secara menyeluruh dalam organisasi.

Berdasarkan tesis tersebut, evaluasi keamanan Sistem Akademik (SIAMIK) UPN "Veteran" Jawa Timur menggunakan teknik *penetration testing* berdasarkan standar keamanan OWASP TOP 10, karena OWASP Top 10 menyajikan daftar sepuluh kerentanan keamanan yang paling umum di aplikasi web, membantu organisasi untuk fokus pada aspek-aspek penting yang harus diprioritaskan dalam pengembangan dan pengujian website SIAMIK. Studi Kasus yang akan menjadi objek penelitian ini yaitu website Sistem Akademik (SIAMIK) milik UPN "Veteran" Jawa Timur. SIAMIK adalah sistem informasi berbasis web yang berguna untuk mengelola Kartu Rencana Studi (KRS) atau beberapa mata kuliah yang akan diambil oleh mahasiswa, melihat nilai dari semua mata kuliah yang telah diambil dalam 1 semester pada Kartu Hasil Studi (KHS), melihat transkrip untuk jumlah SKS dan daftar mata kuliah yang telah diambil beserta nilainya.

Dari pengujian ini diharapkan dapat mengetahui tingkat keamanan yang ada pada website Sistem Akademik (SIAMIK) UPN "Veteran" Jawa Timur dan melakukan analisis mengenai celah keamanan pada website tersebut. Maka dengan demikian *penetration testing* ini dianggap penting dan layak untuk dijadikan kajian skripsi.

1.2 Rumusan Masalah

Dengan latar belakang yang telah diuraikan di atas, maka permasalahan dapat dirumuskan sebagai berikut:

1. Bagaimana cara melakukan pengujian keamanan terhadap website SIAMIK milik UPN “Veteran” Jawa Timur?
2. Celah keamanan apa saja yang terdapat pada website SIAMIK milik UPN “Veteran” Jawa Timur?
3. Bagaimana cara mencegah celah keamanan yang terdapat pada website SIAMIK milik UPN “Veteran” Jawa Timur?

1.3 Tujuan

Tujuan yang ingin dicapai oleh penulis dari penelitian ini adalah sebagai berikut:

1. Mengetahui tingkat keamanan yang ada pada website SIAMIK.
2. Melakukan analisis keamanan pada website SIAMIK apakah terdapat celah keamanan pada website yang berisi data mahasiswa.
3. Melakukan analisis untuk mencegah celah keamanan pada website SIAMIK milik UPN “Veteran” Jawa Timur.

1.4 Manfaat

Manfaat yang bisa diambil menurut penelitian ini adalah sebagai berikut:

1. Mengetahui implementasi penetration pada pengujian keamanan web yaitu mengidentifikasi dan mengeksplorasi kerentanan sebelum penyerang jahat melakukannya.
2. Mengetahui standar keamanan untuk mencegah 10 daftar risiko keamanan teratas yang telah disusun OWASP.
3. Dapat menemukan celah dan risiko keamanan pada SIAMIK.
4. Hasil penelitian dapat digunakan untuk evaluasi pengelola sistem untuk memperbaiki celah keamanan SIAMIK.

1.5 Batasan Masalah

Batasan masalah yang penulis gunakan untuk melakukan penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan menggunakan metode Gray-Box dikarenakan penguji tidak diberi hak akses penuh terhadap website SIAMIK.
2. Pengelola SIAMIK hanya memberi hak akses sebagai mahasiswa.
3. Pengujian hanya dilakukan pada celah keamanan yang berstatus/*level high* dan *medium*.
4. Penelitian ini hanya membahas sampai perencanaan perbaikan celah keamanan web SIAMIK.