# **BAB I**

# **PENDAHULUAN**

## **Latar Belakang Masalah**

Era internet saat ini, informasi sangat mudah diperoleh dan disebar luaskan. Informasi menjadi aset yang sangat berharga baik bagi perseorangan, pemerintah maupun swasta. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi.

Informasi sangat berharga karena jika suatu informasi tersebut berada di tangan pihak yang tidak berhak, bisa disalah gunakan. Sebagai contoh, jika data suatu perusahaan bisa diambil oleh pesaing bisnis bisa digunakan sebagai alat untuk menjatuhkan perusahaan tersebut. Namun sampai saat ini organisasi atau perusahaan belum sepenuhnya menyadari pentingnya perlindungan informasi, karena masih banyak yang menganggap informasi bukan bagian dari aset.

Survei terbaru perusahaan keamanan siber Trend Micro yang bekerja sama dengan Ponemon Institute, Amerika Serikat, mengungkap bahwa 81 persen perusahaan di Indonesia kemungkinan bisa mengalami kebocoran data pelanggan dalam 12 bulan ke depan. Country Manager Trend Micro, Laksana Budiwiyono, menerangkan, temuan itu merupakan hasil dari laporan Cyber Risk Index (CRI) yang dilakukan dua kali setahun. Laporan mengukur gap antara kesiapan keamanan siber para responden dan kemungkinan akan mengalami serangan. “Pada semester pertama 2021, CRI melakukan survei ke lebih dari 3.600 bisnis dari berbagai ukuran dan industri di 24 negara, termasuk Indonesia,” ujar dia dalam acara virtual, Kamis, 2 September 2021.

Universitas Banten Jaya merupakan perguruan tinggi swasta yang memiliki sistem informasi berbasis *web* yang dapat diakses oleh mahasiswa, dosen, dan pihak-pihak lainnya yang berkepentingan. Sistem informasi berbasis *web* tersebut memuat tentang informasi terkait pembelajaran kampus, kegiatan-kegiatan yang ada di kampus, data-data dosen, data-data mahasiswa dan yang lainnya. Sistem tersebut masih sangat rentan dari segi keamanannya terhadap ancaman dari para *hacker* atau pihak yang ingin sekedar melihat atau mengubah sumber data atau informasi tersebut. Terbatasnya tenaga kerja yang memadai untuk pemeliharaan sistem tersebut, menjadi salah satu penyebab sistem sering mengalami *down*. Dalam hal ini dapat dimanfaatkan oleh para *hacker* untuk mengakses sistem informasi dan mengambil data-data yang penting pada sistem tersebut.

Berkaitan dengan perkembangan ini maka keamanan informasi dalam sebuah *website* menjadi sangat penting. Dalam mengamankan *web server* dari serangan seorang *hacker* maka sebaiknya para pemilik *web server* melakukan *self test* terhadap *website* mereka sendiri. Salah satu metode *self test* yang ampuh yaitu dengan mengunakan *penetration test*. *Penetration testing* pada aplikasi *web* hanya memfokuskan evaluasi keamanan aplikasi *web* dengan tujuan menemukan celah keamanan sebelum titik tersebut dieksploitasi para *cracker*.

Berdasarkan hal tersebut, dapat dilakukan suatu pengetesan keamanan *website* mengunakan Metode OWASP (*Open Web Application Security*) versi 4. Dari hasil pengetesan tersebut akan diperoleh berbagai macam kerentanan-kerentanan seorang *attacker* masuk dalam sistem *website*. Kemudian memberikan rekomendasi pencegahan / penanggulangan atas permasalahan yang terjadi.

Penelitian ini bertujuan untuk menganalisis faktor-faktor keamanan *website* yang terdapat di *domain* http://sikadu.unbaja.ac.id dari adanya kemungkinan terjadi kembali ancaman dan gangguan, agar keamanan data yang disimpan dalam *website* terhindar dari akses illegal yang dilakukan oleh pihak yang tidak bertanggung jawab.

Dengan adanya permasalahan diatas, maka dari itu akan dirancang pemecahan masalah yang berjudul **“PENERAPAN OWASP VERSI 4 UJI KERENTANAN SERTA PENANGGULANGAN *WEB* BERBASIS *KALI LINUX*”**. Dengan adanya sistem ini, diharapkan dapat dimanfaatkan sebagai sarana keamanan sistem informasi, untuk keamanan data dan informasi.

## **Identifikasi Masalah**

Dari latar belakang diatas dapat diambil kesimpulan identifikasi masalahnya adalah :

1. Adanya celah keamanan pada *web* Sikadu UNBAJA.
2. Kurangnya sumber daya manusia yang memadai untuk *maintenance* sistem sikadu.
3. Sistem sikadu yang masih rentan terhadap kebocoran data dan informasi mahasiswa.

## **Batasan Masalah**

Berdasarkan point-point diatas, maka dapat ditetapkan batasan masalah seperti berikut:

1. Penelitian dilakukan pada Aplikasi *web* Sikadu Universitas Banten Jaya.
2. Menerapkankegiatan *penetration testing* untuk mengamankan sistem.
3. Sistem yang digunakan adalah *Kali Linux*.

## **Perumusan Masalah**

Berdasarkan latar belakang dan identifikasi masalah diatas maka dapat

dirumuskan beberapa point masalah sebagai berikut :

1. Apa saja risiko celah keamanan yang ada pada aplikasi *web* Sikadu UNBAJA?
2. Bagaimana cara *maintenance* sistem sikadu dengan keterbatasan sumber daya manusia?
3. Apa tindakan yang dapat dilakukan untuk mencegah dampak yang ditimbulkan dari celah keamanan tersebut?

## **Tujuan dan Manfaat Penelitian**

### **Tujuan Penelitian**

Tujuan dari penelitian ini adalah:

1. Mengimplementasikan sistem *kali linux* pada *web server*.
2. Menguji dan menganalisis kerentanan pada *web server* http://sikadu.unbaja.ac.id menggunakan metode *penetration testing*.
3. Mendapatkan solusi atas permasalahan yang ditemukan berdasarkan hasil analisis mengunakan *OWASP* versi 4.

### **Manfaat Penelitian**

1. **Bagi Mahasiswa**

Hasil dari penelitian ini dapat mengetahui kelemahan *web server domain* http://sikadu.unbaja.ac.id apakah rentan terhadap serangan *hacker*.

1. **Bagi Universitas**

Hasil dari penelitian ini dapat dijadikan acuan agar lebih seksama dalam memperbaiki dari segi keamanan informasi *website* Universitas Banten Jaya.

1. **Bagi Pemilik Sistem Informasi**

Hasil dari penelitian ini dapat dijadikan untuk bahan evaluasi dari keamanan sistem informasi yang ada pada organisasi perangkat daerah atau perusahaan swasta.

## **Sistematika Penulisan**

Adapun sistematika penelitian penulisan skripsi ini di uraikan menjadi 5 bab yaitu :

**BAB I PENDAHULUAN**

Pada bab ini menjelaskan dan menguraikan latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

**BAB II DESKRIPSI TEORITIK DAN KERANGKA BERPIKIR**

Pada bab ini menjelaskan dan menguraikan landasan teori yang berhubungan dengan topik/judul dan digunakan dalam pembahasan proposal penelitian termasuk pemodelan pengembangan sistem yang digunakan misal Diagram Arus Data (DAD), *Unified Modeling Language (UML), Flowchart*. Serta menjelaskan secara ringkas tentang penelitian yang pernah dilakukan (Jurnal/Paper/Tesis), terutama jurnal yang telah di publish minimal 5 judul terbitan tahun terakhir.

**BAB III ANALISIS SISTEM**

Pada bab ini menjelaskan dan menguraikan metode-metode yang digunakan dalam pengembangan sistem, dan menjelaskan tentang perancangan sistem yang berisi prototype dan Layout program serta pemodelan sistem menggunakan terstruktur model atau pemodelan berorientasi objek model.

**BAB IV RANCANGAN DAN IMPLEMENTASI SISTEM**

Pada bab ini membahas tentang pembahasan berupa uraian, penjelasan, dan hasil pembuatan aplikasi yang telah dibuat sebelumnya. Pengujian dilakukan untuk memastikan bahwa hasil akhir yang dibuat sesuai dengan kebutuhan pengguna.

**BAB V PENUTUP**

Pada bab ini berisi kesimpulan dan saran yang menjelaskan tujuan penelitian dapat tercapai serta menjelaskan kelebihan dan kekurangan yang terdapat pada aplikasi yang telah dibuat. Sedangkan saran berisi hal-hal yang dapat dikembangkan lagi mengenai kekurangan dari aplikasi yang telah dibuat.