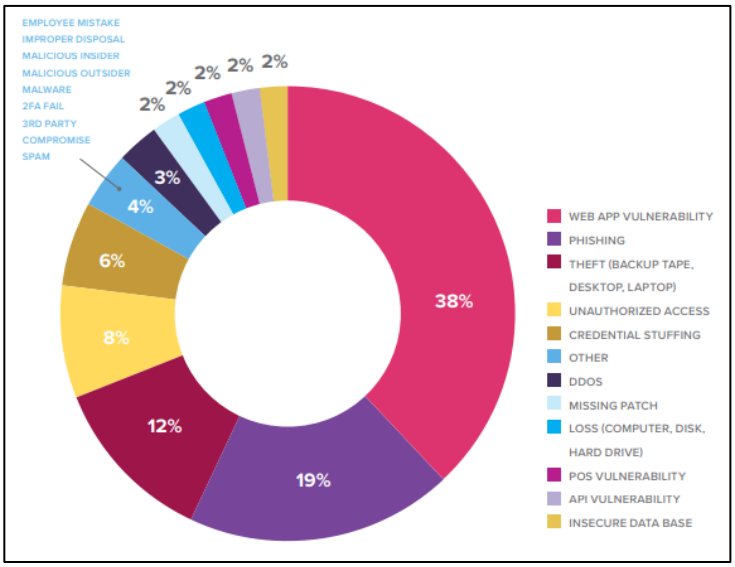
BAB I PENDAHULUAN

I.1 Latar Belakang

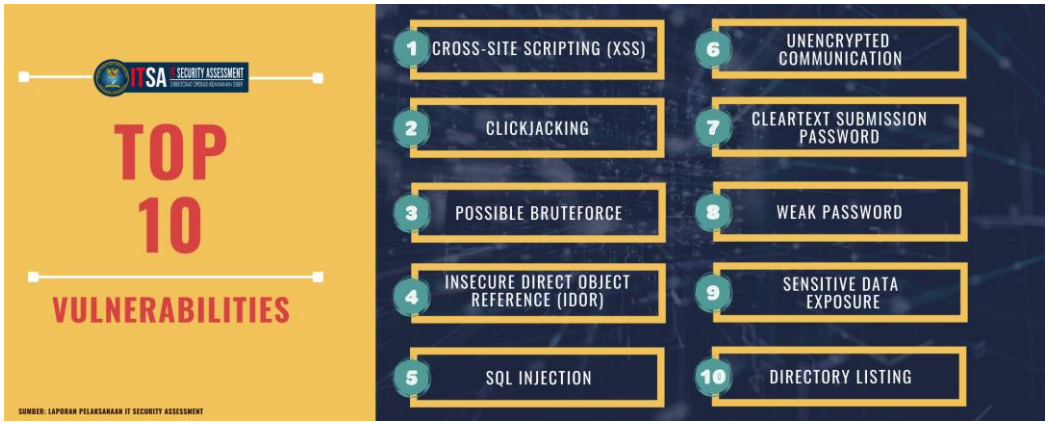
Perkembangan teknologi dan IT saat ini sudah sangat pesat, salah satunya adalah dengan adanya penggunaan *website* sebagai penunjang berbagai aktivitas manusia. Dengan adanya penggunaan *website* ini dapat memberikan dampak positif, khususnya untuk membantu kegiatan dan pekerjaan manusia yang awalnya masih bersifat manual menjadi terotomatisasi dengan sistem, selain itu dengan penggunaan *website* memungkinkan informasi dapat diakses dimana saja dan kapan saja tanpa adanya batasan tempat dan waktu. Berdasarkan kemudahan tersebut hampir seluruh perusahaan, industri, pemerintahan, hingga institusi pendidikan memiliki *website* untuk menunjang proses bisnis beserta aktivitas yang ada didalamnya. Dengan penggunaan aplikasi berbasis *website* tentunya didalamnya terdapat data-data penting dan sensitif tentang pengguna. Namun dengan berbagai kelebihan dan kemudahan dari penggunaan aplikasi berbasis *website* pasti memiliki celah kerentanan atau *vulnerability* yang memungkinkan untuk dieksploitasi oleh *hacker*. Hal ini akan menjadi ancaman terhadap data-data sensitif pengguna yang tersimpan pada aplikasi. Jika celah kerentanan atau *vulnerability* tersebut ditemukan oleh *hacker* jahat (*black hat*) kemungkinan besar data-data tersebut akan disalahgunakan maupun dijual untuk mendapatkan keuntungan bagi *hacker* tersebut, dan jika celah kerentanan ditemukan oleh *hacker* baik (*white hat*) maka celah kerentanan yang ditemukan biasanya akan di informasikan kepada pihak *developer* agar dilakukan perbaikan. Dengan adanya ancaman tersebut maka situs *website* harus dijamin keamanannya.

Berdasarkan pada artikel "*Lesson Learned from A Decade Data Breach*" oleh F5 Labs disebutkan bahwa penyebab utama adanya insiden kebocoran data adalah adanya *web application vulnerability* (Boddy & Pompon, 2017). Representasi penyebab utama kebocoran data tersebut dapat dilihat pada Gambar I.1 berikut.



Gambar I.1 Data Penyebab Kebocoran Data

Dari Gambar I.1 diatas dapat dilihat bahwa *web application vulnerability* menjadi penyebab terbanyak adanya insiden kebocoran data yaitu mencapai 38% dari keseluruhan penyebab kebocoran data. Terkait dengan *web application vulnerability* berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), terdapat 10 jenis celah kerentanan yang banyak ditemukan. Daftar jenis kerentanan ini diambil berdasarkan hasil *Information Technology Security Assessment* (ITSA) yang dilakukan pada tahun 2021 yang dapat dilihat pada Gambar I.2 berikut.



Gambar I.2 *Top* 10 Jenis Celah Kerentanan menurut BSSN

Pada Gambar I.2 merupakan data 10 jenis celah kerentanan yang banyak ditemui. Jenis kerentanan tersebut adalah *Cross-Site Scripting* (XSS), *clickjacking*, *posible bruteforce*, *Insecure Direct Object Reference* (IDOR), *SQL injection*, *uncrypted communication*, *cleartext submission password*, *weak password*, *sensitive data exposure*, dan *directory listing* (Badan Siber dan Sandi Negara, 2022).

Celah-celah kerentanan tersebut dapat dimanfaatkan oleh *hacker* untuk melakukan eksploitasi terhadap *website*, seperti mendapatkan informasi dan data-data sensitif yang ada pada *website*. Jenis celah kerentanan yang umum terjadi pada aplikasi berbasis *website* adalah *Cross-Site Scripting* (XSS), *clickjacking*, dan SQL *injection*. *Cross-Site Scripting* (XSS) merupakan jenis injeksi yang menargetkan halaman web sebuah situs atau aplikasi web, *hacker* akan mengirimkan *side-script* kepada *end-user* sehingga *hacker* dapat mengakses *cookie*, *session token*, atau informasi sensitif pengguna. *Clickjacking* merupakan kerentanan dimana *hacker* dapat memasukkan elemen kedalam *website* agar diklik oleh pengguna, dan apabila elemen tersebut diklik maka akan memicu fungsi jahat yang akan merugikan pengguna. Sedangkan SQL *injection* merupakan jenis injeksi yang menargetkan *database* dan mempengaruhi eksekusi *command* SQL, dimana *hacker* akan mengubah data, menjalankan operasi administasi, serta mengeluarkan perintah melalui *database* tersebut (Badan Siber dan Sandi Negara, 2022).

Fakultas Rekayasa Industri (FRI) merupakan salah satu fakultas yang ada di Universitas Telkom, dimana fokus jurusan yang ini meliputi bidang bisnis, industri, teknologi, dan informasi. Untuk menunjang berbagai kegiatan dan proses administratif yang ada, Fakultas Rekayasa Industri (FRI) memanfaatkan teknologi *website* agar kegiatan dan proses administratif menjadi lebih terorganisir, efektif, dan efisien. Salah satu kegiatan administratif di Fakultas Rekayasa Industri (FRI) yang memanfaatkan teknologi *website* adalah proses rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI). Dalam *website* tersebut menunjang proses pendaftaran calon asisten praktikum dan laboratorium dari mulai pemilihan laboratorium, pengisian data pribadi, hingga melampirkan berkas-berkas yang diperlukan seperti *curriculum vitae*, *motivation letter*, hingga transkrip nilai.

Dari informasi diatas *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) memiliki banyak data-data sensitif mahasiswa Fakultas Rekayasa Industri (FRI). Maka dalam penelitian ini akan dilakukan proses *vulnerability assessment* pada *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) untuk melihat apa saja celah kerentanan yang ada pada *website*. Hal ini berguna untuk mengamankan *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) dari pihak-pihak yang tidak bertanggung jawab sebelum menimbulkan kerusakan dan kerugian bahkan kebocoran data baik kepada Fakultas Rekayasa Industri (FRI) maupun mahasiswa yang menggunakan *website* tersebut.

Untuk melakukan *vulnerability assessment*, pada penelitian ini menggunakan dua *tools* utama yaitu Nikto dan Nessus. Nikto merupakan sebuah *software* pemindai kerentanan yang bersifat *open source* dan berfokus pada keamanan aplikasi web, sedangkan Nessus merupakan *software* yang bersifat otomatis dalam melakukan pemindaian kerentanan, Nessus juga menyediakan pemindaian untuk aplikasi berbasis web. Dalam dokumentasi dari laman resmi kedua *tools* ini, menyatakan bahwa kedua *tools* ini dapat diintegrasikan satu sama lain. Dengan mengimplementasikan kedua *tools* ini dalam melakukan *vulnerability assessment*, diharapkan mampu mengidentifikasi celah kerentanan yang ada dan mengurangi ancaman keamanan terhadap *website*, sehingga dapat dijadikan acuan untuk perbaikan sebagai antisipasi sebelum menyebabkan kerusakan, kerugian, dan terganggunya kinerja serta layanan yang ada didalam *website*.

I.2 Perumusan Masalah

Adapun rumusan masalah yang mendasari penelitian ini diantaranya adalah sebagai berikut:

a. Bagaimana hasil dan analisis *vulnerability scan* pada *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) menggunakan *tools* Nikto dan Nessus?
b. Bagaimana perbandingan *tools* Nessus dan Nikto dalam proses *vulnerability analysis* yang telah dilakukan?

I.3 Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini diantaranya adalah sebagai berikut:

a. *Vulnerability scan* pada *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) menggunakan Nikto dan Nessus untuk menemukan celah kerentanan pada *website*.
b. Analisis hasil *vulnerability scan* dari kedua *tools* yang digunakan yaitu Nikto dan Nessus untuk mendapatkan rekomendasi solusi atas kerentanan yang ditemukan.

I.4 Batasan Penelitian

Agar penelitian ini tidak keluar dari ruang lingkupnya, pada proses penelitian ini diberikan beberapa batasan diantaranya terbatas pada hal-hal berikut:

a. Objek penelitian ini terbatas pada *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) Universitas Telkom yang berjalan pada *Virtual Private Server* (VPS) FRI.
b. Pada penelitian ini, dalam proses *vulnerability scan* terbatas pada penggunaan *tools* Nikto dan Nessus.
c. Parameter yang diukur dalam penelitian ini adalah tingkat kerentanan dan solusi berdasarkan hasil *vulnerability scan* yang dihasilkan menggunakan *tools* Nikto dan Nessus.
d. Penelitian ini tidak mencakup proses *penetration testing*.

I.5 Manfaat Penelitian

Adapun manfaat yang didapat dari adanya penelitian ini adalah sebagai berikut:

a. Bagi Fakultas Rekayasa Industri Universitas Telkom, peneliti ini bermanfaat untuk mengetahui celah kerentanan yang ada pada *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI) yang dapat digunakan sebagai acuan dan bahan pertimbangan dalam melakukan perbaikan. Dari hasil penelitian ini juga dapat meminimalisisr potensi ancaman yang akan terjadi dan bisa ditangani sebelum berakibat fatal terhadap *website* tersebut.

b. Bagi peneliti lain yang bergerak dalam sistem informasi pendidikan tinggi, penelitian ini dapat menjadi referensi dalam melakukan proses analisis celah kerentanan pada aplikasi berbasis *website*, serta memberikan informasi mengenai *tools* yang digunakan yaitu Nikto dan Nessus.

I.6 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari enam bab, adapun uraian dari keenam bab tersebut disusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai hal yang melatarbelakangi pembuatan sebuah karya tulis ilmiah. Dalam pembahasannya digambarkan melalui latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan mengenai literatur yang relevan dengan permasalahan yang diambil, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sedang dilakukan, serta berisi penjelasan mengenai teori-teori pendukung yang digunakan dalam penelitian ini

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan mengenai model konseptual yang digunakan untuk merumuskan solusi dari permasalahan yang diambil, menjelaskan alur penelitian yang akan dilakukan yang disusun dalam sistematika penelitian dari tahap awal hingga akhir.

BAB IV RANCANGAN PENGUJIAN

Bab ini membahas mengenai instrumen *hardware* dan *software* yang digunakan dalam penelitian, serta penjelasan skenario rancangan pengujian yang akan dilakukan menggunakan *tools* Nikto dan Nessus.

BAB V HASIL DAN ANALISIS PENGUJIAN

Bab ini membahas mengenai hasil yang telah didapatkan pada proses pengujian yang telah dilakukan, serta berisi analisis dari hasil pengujian yang didapatkan menggunakan *tools* Nikto dan Nessus. Pada bab ini juga, dijelaskan bagaimana perbandingan hasil pengujian yang telah dilakukan menggunakan kedua *tools* tersebut.

BAB VI KESIMPULAN DAN SARAN

Bab ini menyimpulkan mengenai keseluruhan isi karya tulis ilmiah. Didalam bab ini juga menjawab dari rumusan masalah yang telah ditentukan, serta berisi saran untuk penelitian yang akan dilakukan selanjutnya.