BAB I PENDAHULUAN

I.1 Latar Belakang

Internet menjadi salah satu kebutuhan yang tidak akan pernah lepas dari kehidupan masyarakat saat ini. Internet menjadi media yang digunakan masyarakat untuk berkomunikasi, mencari data atau informasi, menyalurkan kreativitas, mendukung kegiatan ekonomi dan bisnis, serta masih banyak lagi. Internet sudah menjadi hal penting pada dunia yang serba digital seperti saat ini, banyak aktivitas ataupun kegiatan yang memiliki ketergantungan terhadap internet dan tidak akan bisa berjalan apabila tidak adanya sambungan internet tersebut. Menurut data yang dimuat dalam laporan yang dirilis oleh layanan manajemen konten *HootSuite*, dan agensi pemasaran media sosial *We Are Social* dalam laporan "*Digital* 2021", terdapat 202,6 juta jiwa pengguna internet di Indonesia

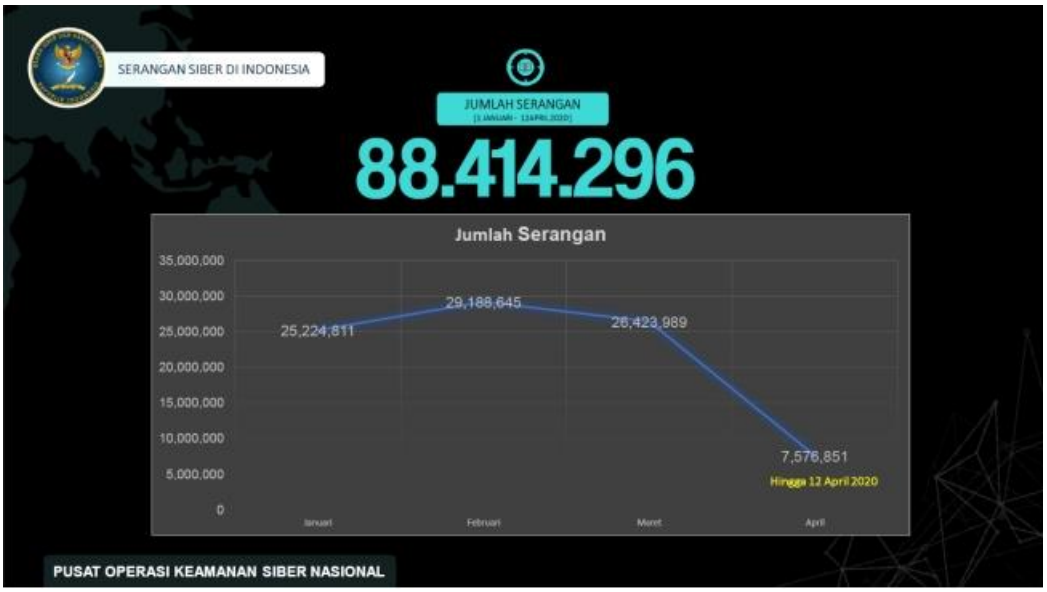
Gambar I.1 Pengguna internet per Januari 2021 (Hootsuite, 2021)

Gambar I.2 Pertumbuhan pengguna internet per Januari 2021 (Hootsuite, 2021)

Pada Gambar I.1 dapat dilihat bahwa pengguna internet per Januari 2021 mencapai 202,6 juta jiwa dari keseluruhan populasi Indonesia yang mencapai 274,9 juta jiwa. Lalu, pada Gambar I.2 menyajikan data pertumbuhan pengguna internet di Indonesia yang meningkat 15,5% atau bertambah 27 juta dibandingkan pada Januari 2020. Maka dari itu internet menjadi sangat penting dan tidak bisa dipisahkan dari kehidupan masyarakat yang serba digital seperti saat ini. Saat masyarakat melakukan akses ke internet salah satu unsur dari internet yang akan selalu diakses adalah situs web. Setiap informasi yang diberikan di internet dari sumber manapun akan memiliki situs web masing-masing yang pemiliknya buat untuk menampilkan informasi atau data yang diperlukan. Situs web atau *website* itu sendiri adalah halaman informasi yang dapat diakses oleh khalayak umum melalui internet tanpa batasan ruang dan waktu, halaman informasi ini dapat berupa teks, gambar, video dan lain-lain (Tania dkk, 2018).

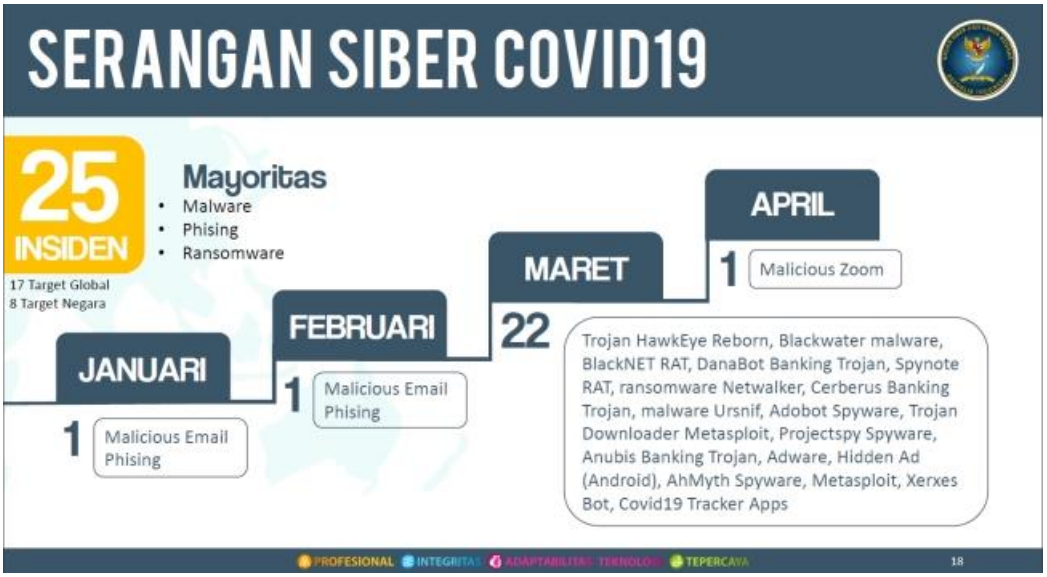
Dengan tingginya penggunaan akses internet dan situs web, ancaman keamanan terhadap integritas dan kerahasiaan suatu informasi serta sumber daya yang ada pada situs web menjadi masalah besar. Banyak kasus peretasan dan eksploitasi yang terjadi di Indonesia maupun di dunia (Shinde & Ardhapurkar, 2016). Indonesia merupakan salah satu negara yang perlu untuk memperhatikan keamanan siber karena Indonesia memiliki catatan kritis dengan banyaknya kasus *cybercrime*

(Almaarif & Lubis, 2020). Menurut data yang dimuat dalam dokumen "Rekapitulasi Insiden *Web Defacement*" yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, terdapat banyak serangan siber yang terjadi



Gambar I.3 Serangan siber di Indonesia per Januari - April 2020 (BSSN, 2020)

Pada Gambar I.3 dapat dilihat bahwa pada Januari - April 2020 telah terjadi 88.414.296 kasus serangan siber di Indonesia. Data yang dirilis oleh BSSN ini membuktikan bahwa Indonesia cukup banyak mengalami serangan siber pada rentang waktu tersebut, ini menjadi hal yang harus diperhatikan agar dapat menjamin keamanan informasi bagi seluruh pengguna internet. Dalam dokumen yang dirilis oleh BSSN tersebut terdapat juga data serangan siber dengan latar belakang isu pandemi COVID-19



Gambar I.4 Serangan siber dengan latar belakang isu pandemi COVID-19

Gambar I.4 menginformasikan data serangan siber yang terjadi dengan latar belakang isu pandemi Covid-19. Terdapat 25 insiden yang terjadi dalam rentang waktu Januari - April 2020 dengan rincian 17 serangan dengan target global dan 8 serangan dengan target suatu negara. Serangan yang terjadi berasal dari berbagai jenis serangan, dengan mayoritas serangan berjenis *Malware*, *Phising*, dan *Ransomware*. Data-data yang dirilis oleh BSSN tersebut menjadi gambaran bahwa pentingnya analisis pengujian kerentanan serta keamanan aplikasi *online* terutama situs web. Pengujian kerentanan dan keamanan dapat mencegah terjadinya insiden siber pada situs web terkait. Insiden siber merupakan kejadian yang mengganggu berjalannya sistem elektronik misalnya serangan virus, pencurian data, informasi pribadi, hak kekayaan intelektual perusahaan, *web defacement* dan gangguan akses terhadap layanan elektronik (BSSN, 2020).

Pada penelitian ini menggunakan metode *black box testing*, metode ini digunakan ketika melakukan pengujian terhadap sebuah aplikasi tanpa mengetahui informasi internal program aplikasi tersebut. Penelitian ini melakukan analisis pengujian kerentanan dan keamanan menggunakan standar dari *National Institute of Standards and Technology* dengan kode publikasi 800-115 atau dapat disebut NIST SP 800-115. Standar NIST SP 800-115 ini dipilih berdasarkan hasil literatur yang menurut penulis lebih sesuai dengan rencana penelitian yang dirancang dengan empat tahapnya yang dapat dilakukan sesuai dengan standar serta tahap pada fase

penetration testing yang digambarkan secara jelas dibandingkan dengan PTES (*Penetration Testing Execution Standard*) yang memiliki tujuh tahap yang tidak keseluruhan tahapnya dapat dilakukan pada penelitian ini serta dengan OSSTMM (*Open Source Security Testing Methodology Manual*) yang kurang memfokuskan pada tahap-tahap fase *penetration testing*. Penggunaan metode *black box testing* dan standar NIST SP 800-115 dapat membantu proses pengujian kerentanan pada situs web yayasan kesehatan XYZ dengan menggunakan bantuan beberapa *tools* untuk melakukan pengujian terhadap situs web tersebut. Pengujian kerentanan ini dapat dijadikan acuan dalam memperbaiki serta meningkatkan penanganan keamanan pada situs web yayasan kesehatan XYZ.

I.2 Perumusan Masalah

Dalam penelitian ini dilakukan penelitian mengenai pengujian kerentanan situs web organisasi serta melakukan analisis kerentanan terdasarkan hasil kerentanan yang diperoleh dari sistem organisasi tersebut. Adapun rumusan masalah yang akan diteliti pada penelitian ini yaitu:

a. Bagaimana hasil analisis kerentanan pada situs web yayasan kesehatan XYZ?
b. Bagaimana evaluasi dan rekomendasi yang bisa diberikan pada situs web yayasan kesehatan XYZ berdasarkan hasil analisis yang dilakukan?

I.3 Tujuan Penelitian

Dari rumusan masalah tersebut, terdapat beberapa tujuan penelitian yang akan dicapai, sebagai berikut:

a. Menganalisis kerentanan pada situs web yayasan kesehatan XYZ.
b. Mengevaluasi hasil uji kerentanan dan memberikan rekomendasi berdasarkan hasil analisis yang telah dilakukan pada situs web yayasan kesehatan XYZ.

I.4 Batasan Penelitian

Adapun batasan masalah dalam penelitian ini, adalah sebagai berikut:

a. Penelitian ini merupakan kajian dalam analisis kerentanan yang ditemukan pada situs web yayasan kesehatan XYZ.

b. Penggunaan standar NIST SP 800-115 sebagai panduan untuk melakukan pengujian kerentanan pada situs web.
c. Pengujian kerentanan pada penelitian ini menggunakan *tools* Zenmap, OWASP ZAP, dan Burp Suite yang berjalan pada sistem operasi Windows.
d. Pengujian mengunakan metode/pendekatan *black box testing*.
e. Penelitian ini tidak mengimplementasikan rekomendasi/usulan yang diberikan.
f. Hanya melakukan eksploitasi/*attack* pada satu jenis kerentanan yang memungkinkan.

I.5 Manfaat Penelitian

Adapun manfaat yang dapat diambil dari penelitian ini, sebagai berikut:

a. Secara teoritis, hasil dari penelitian ini dapat menjadi referensi untuk penelitian lain dalam bidang pengujian kerentanan khususnya penelitian dengan metode dan standar yang serupa.
b. Secara praktis, hasil dari penelitian ini dapat menjadi acuan dan membantu instansi terkait dalam melakukan evaluasi keamanan.

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 penelitian. 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* Zenmap, OWASP ZAP, dan Burp Suite.

Bab V Hasil Pengujian dan Analisis

Bab ini membahas mengenai hasil yang telah didapatkan pada proses pengujian yang telah dilakukan, serta berisi analisis dari hasil pengujian yang didapatkan dari penggunaan *tools* Zenmap, OWASP ZAP, dan Burp Suite. Pada bab ini juga, diberikan rekomendasi terkait kerentanan yang ditemukan pada tahap pengujian.

Bab VI Kesimpulan dan Saran

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