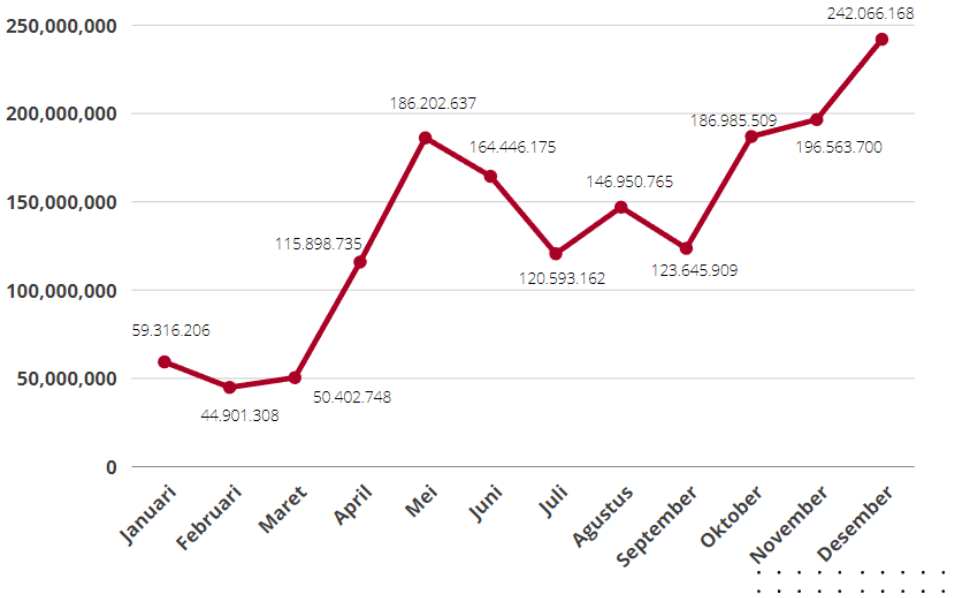
BAB I PENDAHULUAN

I.1 Latar Belakang

Pada saat ini, *website* merupakan salah satu hal yang pasti ada pada sebuah organisasi atau perusahaan bahkan lembaga negara untuk membantu dalam keperluan bisnis atau membantu masyarakat untuk mendapatkan info info penting yang tertera pada *website* tersebut. *Website* bisa menampilkan gambar, teks, dan berbagai macam hal lainnya yang memungkinkan untuk diakses oleh siapapun yang terhubung dengan internet.

Pada *website* juga terdapat informasi informasi atau dokumen dokumen penting yang tersimpan didalam database *website* tersebut. Dokumen dokumen yang seharusnya tidak boleh diakses oleh siapapun sering kali bocor atau dapat diakses oleh peretas karena Dalam pengerjaan *website* banyak hal-hal penting yang kurang diperhatikan dan menjadi celah keamanan yang dapat dimanfaatkan oleh orang-orang yang tidak bertanggung jawab.

Peretasan *website* yang terjadi sudah sangat banyak di alami oleh berbagai negara, begitupun di indonesia sudah beberapa kali situs situs pemerintah mengalami kebobolan seperti situs BSSN, situs KPAI, dan juga situs sekretariat kabinet yang telah mengalami kebobolan bulan juli lalu. Elsam mengemukakan bahwa Rentetan serangan terhadap sistem elektronik pemerintah, khususnya BSSN, berpotensi pada semakin turunnya tingkat kepercayaan *public*, terhadap keseriusan pemerintah dalam melindungi keamanan *sistem* informasi nasional (Jemadu L, 2021).



Gambar I. 1 Jumlah Serangan Siber Nasional

Seperti yang bisa dilihat pada Gambar I.1 pada tahun 2021 berdasarkan laporan tahunan monitoring keamanan siber 2021 terdapat jumlah serangan siber nasional sebesar 1.637.973.022 serangan dalam kurun waktu satu tahun. Serangan terbanyak terjadi pada bulan desember yaitu sebesar 242.066.168 serangan dan serangan paling sedikit terjadi pada bulan februari yaitu sebesar 44.901.308 serangan.

Maka dari itu dapat dilihat dengan maraknya serangan siber atau peretasan situs yang dilakukan oleh beberapa orang tidak bertanggung jawab maka sangat pentingnya melakukan pengetesan kerentanan pada *website* yang dimiliki sehingga dapat mengetahui dimana letak kelemahan *website* tersebut dan bisa melakukan pembenahan pada *website* tersebut. Salah satu cara melakukan pengetesan tersebut adalah dengan melakukan *vulnerability assessment* dan *penetration testing*.

Website milik Dinas Kependudukan dan Catatan Sipil XYZ yaitu xyz.xyz.go.id akan menjadi objek penelitian ini. *Website* xyz.xyz.go.id merupakan situs yang menyimpan dan memberikan informasi mengenai administrasi kependudukan seperti pembuatan KTP, akta kelahiran, kartu keluarga, dan lain sebagainya. Informasi yang dimiliki *website* xyz.xyz.go.id sangat rentan untuk disalahgunakan oleh pihak yang tidak bertanggung jawab.

Pengetesan kerentanan dapat dilakukan dengan berbagai macam metode seperti PTES, NIST dan ISSAF. *Penetration Testing Execution Standard* (PTES) yaitu sebuah standar baru yang menggunakan bahasa umum untuk melakukan *penetration testing* dan terbagi menjadi 7 tahap (Syarif Revelino & Jatmiko Andri, 2018). Sedangkan *National Institute of Standards and Technology* (NIST) adalah metodologi yang dibuat untuk membantu melakukan tes keamanan informasi (Silaban Christian & Wijaya, 2018). Sementara itu *Information System Security Assessment Framework* (ISSAF) adalah metodologi *penetration testing* yang memiliki langkah langkah pengujian yang kompleks dibandingkan dengan metode lainnya dan juga ISSAF memberikan arahan pengujian yang jelas dan lengkap sehingga dapat menghindari kesalahan dalam melakukan pengujian.

Pada penelitian ini menggunakan *framework* ISSAF untuk melakukan pengujian kerentanan dan keamanan pada situs web Dinas Kependudukan dan Catatan Sipil XYZ dengan bantuan beberapa *tools* yaitu zenmap, netcraft, burpsuite dan owasp zap. Pengujian kerentanan ini dapat dijadikan acuan dalam memperbaiki serta meningkatkan penanganan keamanan pada situs web Disdukcapil XYZ.

Pada Penulisan Tugas Akhir ini dilakukan untuk membantu meningkatkan keamanan *website* Disdukcapil XYZ dengan cara mendapatkan celah keamanan dan memberikan rekomendasi untuk mengatasinya.

I.2 Perumusan Masalah

Berdasarkan Latar Belakang yang telah dijelaskan diatas, maka rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana hasil dan analisi pengujian keamanan pada *website* Dinas Kependudukan dan Catatan Sipil XYZ?
2. Bagaimana rekomendasi yang bisa diberikan pada *website* Dinas Kependudukan dan Catatan Sipil XYZ mengenai celah keamanan?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan yang ingin dicapai adalah sebagai berikut:

1. Mengetahui hasil dan analisi pengujian celah keamanan pada *website* Dinas Kependudukan dan Catatan Sipil XYZ.
2. Mengetahui rekomendasi yang bisa diberikan pada *website* Dinas Kependudukan dan Catatan Sipil XYZ mengenai celah keamanan.

I.4 Batasan Penelitian

Adapun Batasan masalah yang dilakukan pada penelitian ini yaitu:

1. Penelitian ini merupakan kajian dalam analisis kerentanan yang ditemukan pada situs web Disdukcapil
2. Penelitian ini menggunakan framework ISSAF.
3. Pengujian ini menggunakan tools zenmap, BurpSuite, owasp zap.
4. Tahap pengujian hanya dilakukan sampai pada tahap keempat yaitu *penetration* dari sembilan tahapan yang ada
5. Analisis celah keamanan hanya bisa dilakukan pada dua celah keamanan saja

I.5 Manfaat Penelitian

Hasil Penelitian ini diharapkan dapat memberikan beberapa manfaat, yaitu:

1. Dapat menjadi bahan pertimbangan dan Evaluasi bagi pengembang *website*
2. Dapat bermanfaat untuk mengedukasi dan pembelajaran pembaca dalam meningkatkan keamanan *website*

I.6 Sistematika Penulisan

Penelitian ini dikerjakan dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, dan sistematika penulisan penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan teori teori pendukung beserta penelitian penelitian terdahulu yang berkaitan dengan penelitian yang dilakukan

BAB III METODOLOGI PENELITIAN

Bab ini terdiri dari model konseptual dan langkah langkah penelitian mulai dari tahap awal hingga tahap akhir

BAB IV RANCANGAN PENGUJIAN

Pada Bab ini berisi penjelasan mengenai *hardware* dan *software* yang digunakan pada penelitian ini dan juga pada bab ini memberikan penjelasan skenario pengujian yang akan dilakukan

BAB V HASIL PENGUJIAN DAN ANALISIS

Bab ini berisikan hasil pengujian dan analisis pengujian yang dilakukan beserta memberikan rekomendasi.

BAB IV KESIMPULAN DAN SARAN

Bab ini terdiri dari kesimpulan dan saran pada penelitian yang telah dilakukan.