BAB I PENDAHULUAN

I.1 Latar Belakang

Peraturan Pemerintah Nomor 30 Tahun 2021 tentang Penyelenggaraan Bidang Lalu Lintas dan Angkutan Jalan, pada pasal 1 menyatakan bahwa jalan adalah seluruh bagian jalan, termasuk bangunan pelengkap dan perlengkapannya yang diperuntukkan bagi Lalu Lintas umum, yang berada pada permukaan tanah, di atas permukaan tanah, di bawah permukaan tanah dan/atau air, serta di atas permukaan air, kecuali jalan rel dan jalan kabel. Di dalam Undang-Undang Nomor 22 Tahun 2009 tentang Lalu Lintas dan Angkutan Jalan, pada pasal 1 angka 2 dijelaskan bahwa lalu lintas adalah gerak kendaraan dan orang di ruang Lalu Lintas Jalan. Lebih lanjut pada pasal 1 angka 3 dijelaskan bahwa angkutan adalah perpindahan orang dan/atau barang dari satu tempat ke tempat lain dengan menggunakan Kendaraan di Ruang Lalu Lintas Jalan. Dengan demikian dapat diartikan bahwa di jalan itu tempat pergerakan lalu lintas, sehingga agar para pengguna jalan dapat menggunakannya secara aman perlu adanya pengawasan sehingga akan dapat menekan angka kecelakaan.

Berdasarkan data dari Badan Pusat Statistika (BPS) kasus kecelakaan di jalan masih tinggi. Pada tahun 2019 jumlah kasus kecelakaan lalu lintas tergambar dalam Tabel I.1

Tabel I.1 Jumlah kasus kecelakaan tahun 2019

Tabel 3.5. **Jumlah Kecelakaan, Korban, dan Kerugian Materi, Tahun 2015-2019/** ***Number of Traffic Accident, Casualties, and Material Losses,*** **2015-2019**

Table

Rincian/ *Description*	2015	2016	2017	2018	2019	Pertumbuhan per Tahun/ *Annually Increase* (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)
Jumlah Kecelakaan (kasus)/*Number of Accident (Case)*	96 233	106 644	104 327	109 215	116 411	4,87
Korban Meninggal (Orang)/*Killed (Person)*	24 275	31 262	30 694	29 472	25 671	1,41
Luka Berat (Orang)/ *Seriously Injured (Person)*	22 454	20 075	14 559	13 315	12 475	-13,67
Luka Ringan (Orang)/ *Slight Injured (Person)*	107 743	120 532	121 575	130 571	137 342	6,26
Kerugian Materi (Juta Rp)/ *Material Loss (Million Rupiahs)*	215 892	229 137	217 031	213 866	254 779	4,23

Sumber/*Source:* Kepolisian Republik Indonesia/*Indonesia State Police*

Pada tahun-tahun sekarang pekerjaan manusia semakin dipermudah dengan adanya *website*. *Website* merupakan fasilitas Internet yang menghubungkan dokumen dalam lingkup lokal maupun jarak jauh. Dokumen pada *website* disebut dengan *web page* dan *link* dalam *website* memungkinkan pengguna bisa berpindah dari satu *page* ke *page* lain (*hypertext*), baik diantara *page* yang disimpan dalam *server* yang sama maupun *server* di seluruh dunia. *Pages* diakses dan dibaca melalui *browser* seperti Netscape Navigator, Internet Explorer, Mozila Firefox, Google Chrome dan aplikasi *browser* lainnya (Lukmanul, 2004).

Indonesia memiliki catatan kritis yang perlu diperhatikan yang disikapi dengan banyaknya kasus *cyber crime* (Almaarif, A dan Lubis, M, 2020). Catatan yang dikemukakan oleh A. Almaarif dan M. Lubis tersebut menegaskan bahwa *cybecrime* merupakan kejadian yang harus mendapatkan perhatian serius demi keamanan sebuah *website*. Catatan ini memperkuat juga perlunya analisis kerentanan dan pengujian keamanan terhadap sebuah *website*, termasuk terhadap *website* XYZ yang merupakan target penelitian.

Pada era digitalisasi saat ini Ilmu Pengetahuan dan Teknologi (IPTEK) menjadi tulang punggung dari kehidupan. Perkembangan yang pesat dari IPTEK membuat sektor publik mengalami reformasi birokrasi dalam mengejar ketertinggalan IPTEK. Pesatnya perkembangan Teknologi Informasi dan Komunikasi (TIK) akan membuka peluang dan tantangan untuk menciptakan (*to create*), mengakses (*to access*), mengolah (*to process*), dan memanfaatkan (*to utilize*) informasi secara tepat dan akurat. Informasi merupakan suatu komoditi yang sangat berharga pada era globalisasi untuk dikuasai dalam rangka meningkatkan daya saing suatu organisasi (termasuk Pemda) secara berkelanjutan.

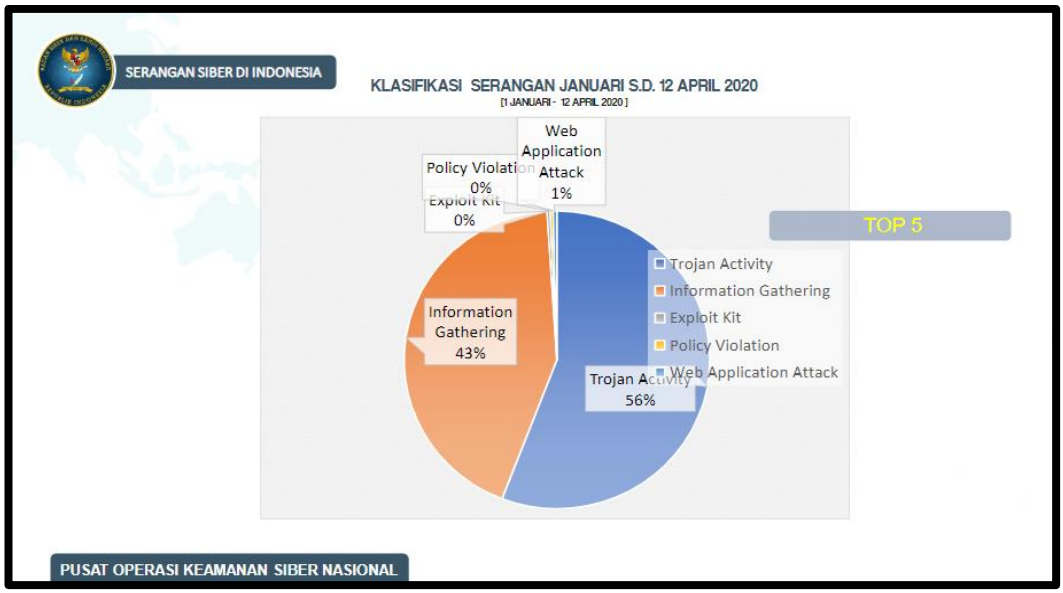
Perkembangan teknologi informasi yang terus berkembang telah memberikan perubahan signifikan mengenai konsep keamanan, kini ruang interaksi tidak bisa hanya dibatasi seara fisik (*physic*) tetapi juga meluas ke dunia maya (*cyber*). Konsekuensinya, negara harus beradaptasi dengan perkembangan konsep keamanan dunia maya (*cyber security*). Ini sudah saatnya ditetapkan sebagai salah satu “wilayah” negara yang dijaga keamanannya sebagaimana kewajiban negara mengamankan teritorialnya. Apalagi, serangan *cyber* tidak hanya terjadi pada

institusi publik saja, namun juga menyerang institusi pemerintah. Keamanan *cyber* mencakup segala sesuatu berhubungan dengan pengawasan komputer, *monitoring* sampai kontrol yang sangat ketat (Triwahyuni dan Wulandari, 2016).

Menurut data Badan Siber dan Sandi Negara Republik Indonesia (BSSN) jumlah serangan dari bulan Januari – April 2020 terjadi puncak serangan pada bulan Februari seperti Gambar I.1

Gambar I.1 Grafik jumlah serangan *cyber* Januari – April 2020 (BSSN,2020)

Pada Gambar I.1 dapat dilihat bahwa angka serangan *cyber* pada kurun waktu Januari-April 2020 mencapai angka 88.414.296 . Hal ini merupakan angka yang tinggi. Dengan demikian dapat disimpulkan bahwa pentingnya menjaga sebuah *website* dari ancaman. selain itu BSSN juga merilis top 5 serangan yang sering terjadi di bulan Januari – April 2020, dan Trojan *activity* adalah serangan yang paling tinggi dan mencapai 56% seperti data pada Gambar I.2



Gambar I.2 Grafik klasifikasi serangan per Januari – April 2020

Dari Gambar I.1 dan Gambar I.2, dapat diketahui betapa tinggi serangan terhadap *website*, sehingga beberapa data nasional yang diperoleh dari BSSN menjadi acuan untuk melakukan menggambarkan bahwa pentingnya analisis kerentanan dan pengujian keamanan sebelum suatu *website* dirilis pada publik. Dengan demikian membuat pemilik *website* memiliki data untuk melakukan suatu tahap penguatan (*hardening)* maupun penundaan perilisan suatu *website* ke publik sebelum *website* yang akan diluncurkan benar-benar aman dari serangan orang yang tidak bertanggung jawab.

Aplikasi *website* rentan terhadap serangan dari luar. Adanya insiden *ransomware* dan serangan lainya yang mengganggu layanan publik menyebabkan perlunya pengujian keamanan terhadap *website* publik. Untuk itu diperlukan pengujian keamanan dilakukan dengan menggunakan standar tertentu seperti NIST 800-115.

Penelitian ini melakukan analisis kerentanan dan pengujian keamanan menggunakan standar yang dikeluarkan oleh *National Institute of Standards and Technology* dengan kode dokumen 800-115 yang secara ringkas disebut standar NIST 800-115. Standar ini yang dipilih mengingat menyediakan metode yang dapat digunakan untuk melakukan *Penetration Testing* dan ada tahapan yang dapat memberikan rekomendasi.

Pengujian keamanan dengan menggunakan standar NIST 800-115 ini dapat digunakan sebagai acuan untuk memperbaiki keamanan *website* sehingga menjadi lebih aman dari serangan. Pada penelitian ini, dilakukan analisis celah dan uji keamanan terhadap *website* XYZ menggunakan standar NIST 800-115 untuk mendapatkan celah yang dapat digunakan sebagai acuan untuk memperbaiki dan membuat *website* XYZ lebih aman.

I.2 Perumusan Masalah

Rumusan masalah pada tugas akhir ini terkait dengan keamanan suatu *website*. Masalah ini terfokus pada keamanan *website* XYZ. Pentingnya keamanan suatu *website* menjadikan keharusan untuk melakukan analisis celah pada sebuah *website*. Adapun rumusan masalah yang akan diselesaikan pada tugas akhir ini adalah:

a. Bagaimana menemukan kerentanan pada *website* XYZ?
b. Bagaimana cara melakukan eksploitasi dan menghasilkan control/rekomendasi pada *website* XYZ?

I.3 Tujuan Penelitian

Tujuan penelitian tugas akhir ini sesuai dengan rumusan masalah yang ada. Hal ini berkaitan dengan *website* XYZ untuk melakukan analisis kerentanan pada *website* XYZ. Adapun tujuan penelitian pada tugas akhir ini adalah:

a. Mengetahui kerentanan pada *website* XYZ.
b. Melakukan ekplotasi dan menghasilkan control atau rekomendasi pada *website* XYZ.

I.4 Batasan Penelitian

Ruang lingkup pada tugas akhir ini memiliki batasan – batasan yang bertujuan untuk mempermudah pengerjaan dan lebih memfokuskan terhadap masalah yang dikerjakan atau dianalisis. Adapun ruang lingkup dalam laporan tugas akhir ini adalah:

a. Pengujian kerentan tidak menguji pada *level medium* dan *low*.
b. Tidak melakukan implementasi *hardening* pada *website* XYZ.
c. Pengujian mengunakan metode/ pendekatan *black box testing*.

I.5 Manfaat Penelitian

Manfaat penelitian yang didapat dari pengujian pada *website* XYZ. Setiap hasil analisis kerentanan dapat dijadikan pedoman sebagai perbaikan *website* XYZ. Oleh karena itu analisis kerentanan pada *website* XYZ membantu pihak pemilik *website* XYZ untuk melakukan evaluasi terhadap yang dimiliki. Adapun manfaat tugas akhir ini adalah:

1. Secara teoritis, hasil penelitian ini berguna sebagai sarana edukasi dan juga penelitian tentang kerentanan pada suatu *website* XYZ. Selain itu mendapatkan informasi kerentanan pada *website* XYZ.
2. Secara praktis, hasil penelitian ini menghasilkan rekomendasi *hardening website* XYZ untuk dilakukan pengkajian lebih lanjut.

I.6 Sistematika Penulisan

Pada penelitian ini menggunakan sistemati penulisan yang dibagi menjadi beberapa bab. Sistematika juga akan mempermudah dalam penyusunhan suatu pengerjaan Tugas Akhir. Sistematika penulisan ini sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Pada bab ini dipaparkan hasil studi literatur terkait dengan permasalahan yang diteliti sebagai dasar keilmuannya.

Tinjauan Pustaka ini memaparkan hal-hal pokok terkait dengan *website*, *website XYZ* yang merupakan *website* yang diteliti, NIST 800-115, Virtualbox, Kali Linux, *Motode Black box*, SQL *Injection*, *Penetration Testing*, Burp Suite, OWASP ZAP, Foxyproxy, dan beberapa hasil penelitian sebelumnya yang relevan.

Bab III Metodologi Penelitian

Metodologi penelitian merupakan strategi dan langkah-langkah yang akan dilakukan dalam penelitian untuk menjawab rumusan masalah yang disusun sebelumnya.

Dalam Bab ini diuraikan tentang Pengembangan Model Koseptual yang digunakan dan Sistematika Penelitian yaitu langkah-langkah yang akan dilakukan dalam penelitian.

Bab IV Rancangan Pengujian

Pada bab ini, disajikan uraian terkait dengan langkah-langkah yang akan dilakukan dalam penelitian. Selain itu menjelaskan skenario – skenario umum dalam penggunaan *tools* terkait dengan penelitian.

Bab V Hasil Pengujian dan Analisis

Pada bab ini, disajikan hasil pengujian dan analisis terhadap *website* XYZ sebagai *website* yang diteliti. Menguraikan hasil penelitian yang dilakukan kepada *website* XYZ.

Secara keseluruhan bab ini membahas secara mendetail mengenai hasil dari penelitian dan refleksinya terhadap tujuan penelitian.

Bab VI Kesimpulan dan Saran

Pada bab ini dijelaskan kesimpulan dari penelitian yang dilakukan serta jawaban dari pertanyaan penelitian yang disajikan di pendahuluan. Selain menyajikan kesimpulan dalam bab ini juga disajikan saran untuk penelitian selanjutnuya.