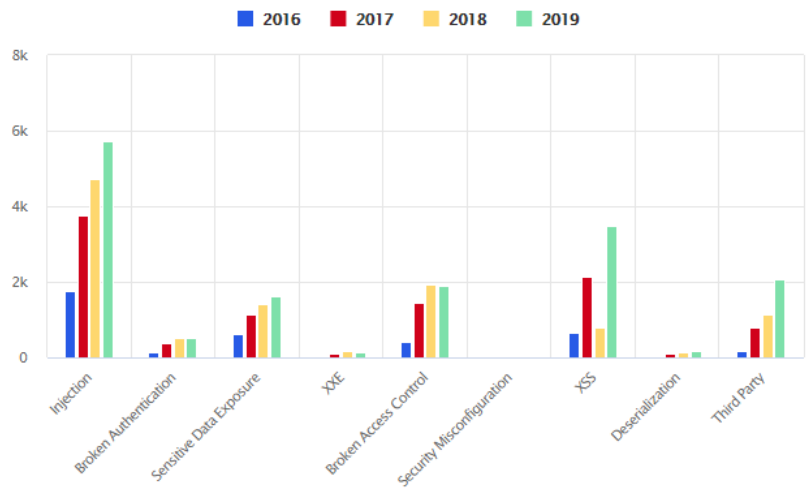
Bab I PENDAHULUAN

I.1 Latar Belakang

Dalam dunia sistem informasi, tentunya keamanan merupakan salah satu hal yang sangat penting. Sumber dari informasi adalah sebuah data. Data-data ini akan diolah menjadi bentuk yang berguna sehingga dapat digunakan bagi penerimanya yang biasanya disebut dengan informasi. Data ini menggambarkan suatu kejadian-kejadian nyata yang terjadi pada saat tertentu (Asmara, 2016). Karena informasi adalah hal yang sangat penting, oleh karena itu hanya orang tertentu saja yang dapat mengakses data informasi. Apabila informasi jatuh kepada pihak yang kurang bertanggung jawab, hal itu dapat membuat pemilik informasi tersebut merasa dirugikan. Maka dari itu keamanan sistem informasi sangat penting dan wajib terjamin kerahasiaannya dalam batas yang dapat diterima (Praptomom, 2016).

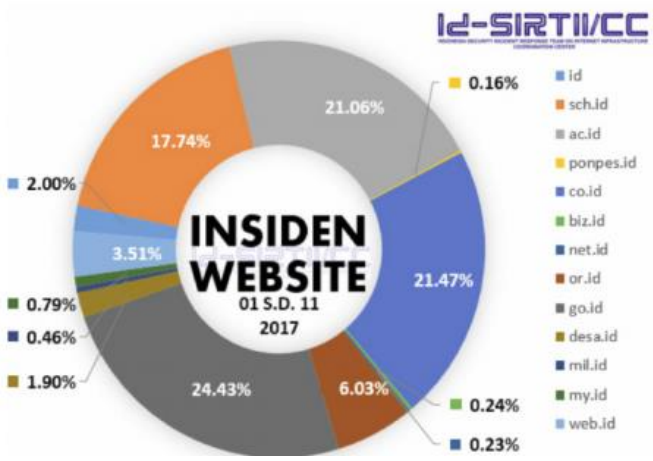
Jika membahas mengenai teknologi pastinya tidak dapat terlepas dari Internet. Internet dapat mempermudah untuk mangakses apa saja, salah satunya ialah mengakses web. Web adalah kumpulan dari beberapa dokumen yang terletak pada komputer *server* (web *server*). Web dapat digunakan untuk mendapatkan berbagai informasi, tidak hanya berbentuk bacaan, tetapi bisa juga dalam bentuk suara, gambar, video, dan animasi (Prasetiadi, 2011).

Semakin berkembangnya aplikasi berbasis web saat ini, maka semakin tinggi juga serangan keamanan dengan berbagai teknik ancaman yang akan menyerang *website*. Tentunya *vulnerabilities* pada tiap *website* berbeda-beda dan mengakibatkan faktor serangan yang berbeda pula. Pada Gambar I.1 kerentanan paling banyak terjadi ialah *injection*. Setiap tahunnya terjadi peningkatan, pada tahun 2019 terjadi peningkatan sebanyak 1.001 *vulnerabilities* dari tahun 2018 (4.729 *vulnerabilities*). Pada tahun 2017 sebanyak 3.770 *vulnerabilities* dan 2016 sebanyak 1.744 *vulnerabilities*. Kemudian disusul dengan kerentanan XSS, sebanyak 3.490 *vulnerabilities* pada tahun 2019, 804 *vulnerabilities* pada tahun 2018, 2.145 *vulnerabilities* pada tahun 2017, dan 646 *vulnerabilities* pada tahun 2016 (Bakeman & Yerushalmi, 2020).



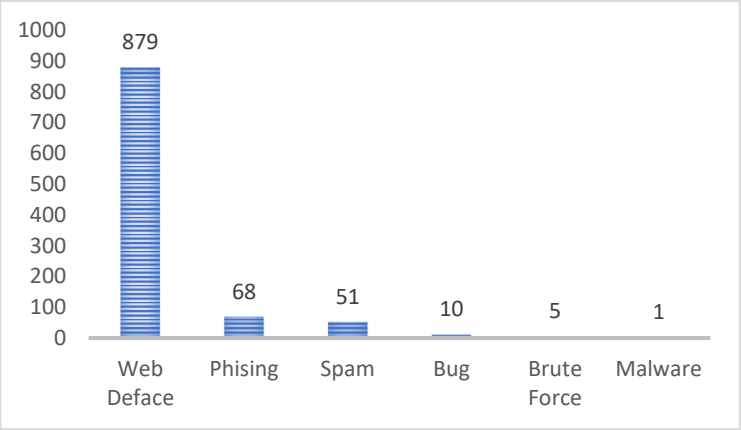
Gambar I.1 *Vulnerabilities* dalam kategori OWASP (www.imperva.com, 2020)

Insiden keamanan *website* saat ini sudah sangat sering terjadi. Banyak *domain website* yang menjadi sasaran untuk melakukan serangan. Data dari Laporan Tahunan Direktorat Jenderal Aplikasi Informatika mengemukakan bahwa ada 5 peringkat besar insiden *website* ditahun 2017 yang terjadi di Indonesia. Pada Gambar I.2 peringkat pertama dalam insiden *website* yaitu *domain* .go.id sebanyak 3.783 kasus (24,43%) kemudian *domain* .co.id sebanyak 3.324 kasus (21,47%) kemudian *domain* .ac.id sebanyak 3.260 kasus (21,06%) selanjutnya *domain* .sch.id sebanyak 2.746 kasus (17,74%), dan yang terakhir adalah *domain* .or.id sebanyak 934 kasus (6,03%) (Direktorat Jendral Aplikasi Informatika Kemenkominfo, 2017). Dari data pada Gambar I.2 menunjukkan peringkat pertama insiden keamanan *website* ialah pada *domain* .go.id dan insiden dalam *domain* .go.id ini memiliki beberapa kasus.



Gambar I.2 Insiden *website* (Id-SIRTII/CC, 2017)

Data dari Laporan Tahunan Direktorat Jenderal Aplikasi Informatika, mengemukakan jika ada beberapa kasus yang sering dijumpai pada insiden keamanan *website domain* .go.id. Pada Gambar I.3 serangan yang paling banyak dilakukan pada *domain* go.id adalah *web deface* sebanyak 879 kasus (86,3%) kemudian *phising* sebanyak 68 kasus (6,7%), kemudian *spam* sebanyak 51 kasus (5,5%) selanjutnya *bug* sebanyak 10 kasus (1%), kemudian *brute force* sebanyak 5 kasus (0,4%), dan serangan yang terakhir *malware* sebanyak 1 kasus (0,1%) (Direktorat Jendral Aplikasi Informatika Kemenkominfo, 2017). Dikarenakan banyaknya insiden keamanan yang terjadi pada *domain* go.id dan ada beberapa kasus yang sering terjadi pada insiden *website domain* go.id, oleh karena itu penelitian ini akan menggunakan salah satu *website* dengan *domain* .go.id sebagai upaya untuk mengamankan *website* tersebut. *Website* dengan *domain* .go.id yang akan digunakan pada penelitian ini ialah situs layanan terpadu pemerintahan daerah XYZ. Situs ini layanan terpadu ini digunakan untuk membantu pelayanan masyarakat dengan menyediakan surat-surat layanan publik, pengurusan administrasi kependudukan, dan lainnya.



Gambar I.3 Serangan insiden *website* (Id-SIRTII/CC, 2017)

Data-data yang ada pada Gambar I.1, I.2, dan I.3 tentunya akan dilakukan upaya untuk memecahkan suatu masalah keamanan dalam *website*. Upaya yang bisa digunakan untuk mengurangi masalah keamanan pada *website* ialah dengan *vulnerability assessment* dan *penetration testing*. *Vulnerability assessment* merupakan kegiatan yang berisikan proses pemindaian sebuah celah atau kerentanan dari suatu *web application* (Ridho, 2015).

Penetration testing dilakukan dengan cara memasuki keamanan kontrol dari suatu perusahaan yang dilakukan dengan melakukan simulasi seorang pengguna yang tidak berwenang untuk melakukan penyerangan pada sistem target dengan menggunakan metode otomatis, manual, dan keduanya. Kegiatan ini dapat membantu suatu perusahaan untuk mengetahui kemugkinan celah keamanan yang ada pada sistemnya dan mengukur dampak dari serangan yang bisa terjadi (Tarigan dkk., 2017).

Pada penelitian ini menggunakan *black box testing* dalam melakukan *penetration testing*. *Black box testing* ini digunakan pada saat semua informasi mengenai *website* target tidak diketahui. Penelitian ini juga memerlukan standar yang akan digunakan. Pada penelitian *penetration testing* ini akan digunakan *Penetration Testing Execution Standard* (PTES) pada situs layanan terpadu pemerintahan daerah XYZ. *Penetration Testing Execution Standard* (PTES) terdiri dari tujuh tahap. Tahap-tahap ini mencakup semua yang terkait dengan *penetration testing*, mulai dari komunikasi awal dan alasan dilakukannya pengujian ini, fase pengumpulan informasi, melakukan pemodelan ancaman, melakukan pencarian

celah keamanan hingga melakukan eksploitasi terhadap kerentanan tersebut, dan akan dilakukan pelaporan hasil dari *penetration testing* yang dilakukan (Adrian & Setiyadi, 2018). PTES ini digunakan karena penilaiannya menggunakan *level-level* yang dapat lebih dipahami oleh *user* (Syarif Revolino & Jatmiko Andri, 2018).

Penggunaan *black box testing* dan *Penetration Testing Execution Standard* (PTES) untuk melakukan pengujian kerentanan dari *website* dapat membantu menemukan kerentanan yang ada pada situs layanan terpadu pemerintahan daerah XYZ dengan mencoba menggunakan beberapa *tools* untuk melakukan beberapa serangan ke dalam *website*. Setalah dilakukan pengujian serangan pada *website* maka akan ditemukan celah keamanan yang ada pada *website* tersebut dan kemudian nantinya akan bisa dilakukan penanganan dalam mengahadapi celah keamanan pada situs layanan terpadu pemerintahan daerah XYZ.

I.2 Perumusan Masalah

Dari uraian latar belakang di atas, rumusan masalah yang dibahas pada penelitian ini, sebagai berikut:

1. Bagaimana hasil dan analisis pengujian celah keamanan pada situs layanan terpadu pemerintahan daerah XYZ menggunakan PTES?
2. Bagaimana rekomendasi yang bisa diberikan pada situs layanan terpadu pemerintahan daerah XYZ mengenai pengujian celah keamanan?

I.3 Tujuan Penelitian

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

1. Mengetahui hasil dan analisis pengujian celah keamanan pada situs layanan terpadu pemerintahan daerah XYZ menggunakan PTES.
2. Mengetahui rekomendasi apa yang akan diberikan pada situs layanan terpadu pemerintahan daerah XYZ mengenai pengujian celah keamanan.

I.4 Batasan Penelitian

Adapun batasan masalah dalam penelitian kali ini, ialah sebagai berikut:

1. Pemindaian kerentanan pada penelitian ini menggunakan *tools* OWASP ZAP, Acunetix, dan Paros.
2. Analisis kerentanan hanya pada kerentanan tingkat risiko *high* dan *medium*, sesuai dengan OWASP *Top* 10 *Vulnerabilites.*
3. Tahap *post exploitation* tidak dilakukan secara keseluruhan, hanya memberikan rekomendasi pada kerentanan yang ditemukan.
4. Penelitian ini tidak mengimplementasikan rekomendasi kerentanan yang telah diberikan.
5. Hanya memprioritaskan kerentanan dengan tingkat *high*.

I.5 Manfaat Penelitian

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

1. Secara teoritis, penelitian ini dapat menjadi referensi dalam bidang *Vulnerability Assessment and Penetration Testing (VAPT)* khususnya mencari kerentanan yang ada pada suatu *website* dengan menggunakan *Penetration Testing Execution Standard* (PTES).
2. Secara praktis, penelitian ini dapat membantu instansi maupun individu dalam mengamankan *website* yang dimiliki dari celah keamanan dan serangan yang bisa merusak *website*.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini berisikan tentang latar belakang penelitian, rumusan masalah dalam penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan dalam penelitian.

Bab II Tinjauan Pustaka

Bab ini berisikan tentang literatur yang sesuai dengan permasalahan dari penelitian ini dan menjelaskan teori-teori yang berkaitan dengan penelitian.

Bab III Metodologi Penelitian

Bab ini berisikan tentang metode yang akan digunakan dalam penelitian. Menjelaskan langkah-langkah yang akan digunakan dalam penelitian, model konseptual yang akan digunakan penulis untuk menyelesaikan tahapan pengujian, tahapan analisis, dan tahapan pemberian solusi dari penelitian ini dan memberikan sistematika penyelesaian masalah dari penelitian yang dilakukan.

Bab IV Rancangan Pengujian

Bab ini berisikan tentang rancangan mengenai *software* dan *hardware* yang akan digunakan dalam melakukan *vulnerability assessment* dan *penetration testing* pada situs layanan terpadu pemerintahan daerah XYZ dan menjelaskan skenario yang akan dilakukan dalam penelitian.

Bab V Hasil Pengujian dan Analisis

Bab ini berisikan tentang penjelasan hasil pengujian yang sudah dilakukan dalam penelitian dan melakukan analisis dari hasil yang sudah diuji berdasarkan literatur yang sudah ditetapkan pada penelitian serta memberikan rekomendasi.

Bab VI Kesimpulan dan Saran

Bab ini berisikan tentang penjelasan intisari dari keseluruhan hasil analisis pengujian celah keamanan pada situs layanan terpadu pemerintahan daerah XYZ dan penjelasan mengenai saran yang akan diberikan kepada penelitian selanjutnya.