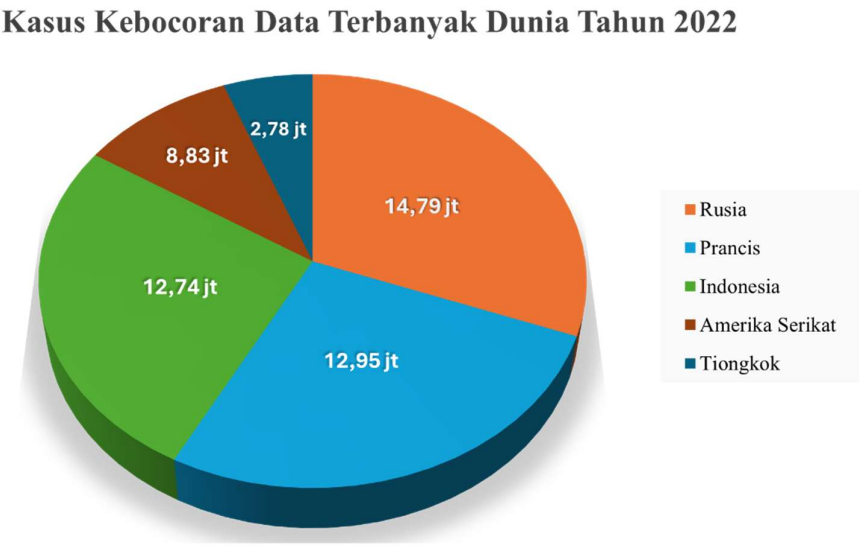
BAB I
PENDAHULUAN

1.1 Latar Belakang

Menurut data yang diterbitkan oleh perusahaan keamanan siber Surfshark, secara global, jumlah akun yang mengalami kebocoran data pada kuartal ketiga tahun 2022 mencapai 72,45 juta akun. Seperti pada gambar 1.1, Indonesia menduduki peringkat ke-3 negara dengan jumlah kebocoran data tertinggi. dunia. Tercatat 12,74 juta akun mengalami pembobolan data di Indonesia per 13 September 2022[1].

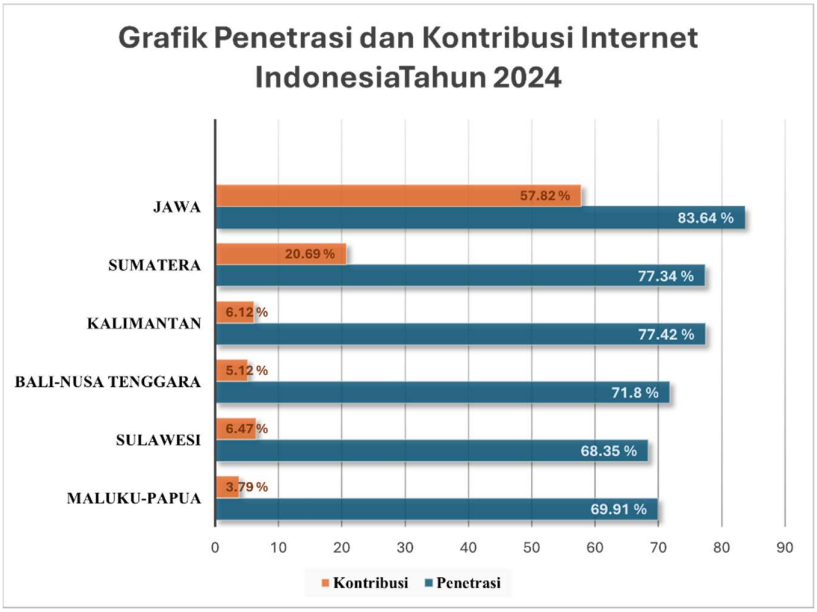


Gambar 1.1 Kasus Kebocoran Data Terbanyak Dunia Tahun 2022[1]

Website adalah salah satu sarana informasi yang sering diakses oleh pengguna dalam dunia teknologi informasi yang terhubung ke internet. Namun, dalam ekosistem website masih terdapat berbagai kerentanan keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab atau peretas.[2]. Tingginya tingkat penggunaan website sejalan dengan munculnya berbagai kerentanan dalam teknologi web. Kerentanan ini dapat dimanfaatkan oleh peretas untuk mengeksploitasi celah keamanan yang kurang diperhatikan oleh administrator,

sehingga berpotensi menyebabkan peretasan website. *Hacker* dapat dengan mudah mengakses data sensitif pada *website* yang tingkat keamanannya yang rendah[3]. Namun disamping itu kemajuan teknologi dapat menjadi tantangan yang baru, termasuk ancaman terhadap situs *website* yang dimiliki oleh pemerintah.

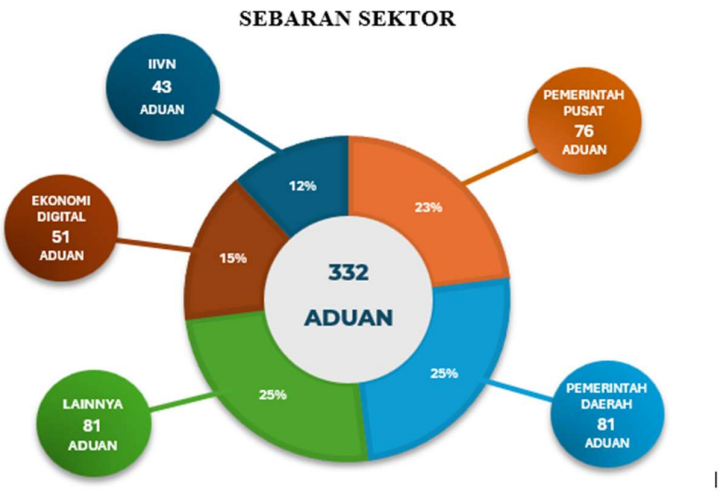
Dalam dunia siber yang terus berkembang, upaya penetrasi merupakan langkah penting untuk menjamin keamanan aplikasi web. Metode analisis kerentanan harus diperbarui secara teratur untuk tetap relevan seiring dengan peningkatan kecerdasan serangan siber. Sebuah laporan dari *Agency for Cybersecurity and Infrastructure Security (CISA, 2022)* menunjukkan bahwa upaya penetrasi yang dilakukan secara rutin memberikan manfaat besar bagi organisasi atau perusahaan. Praktik ini memungkinkan identifikasi kerentanan sebelum dieksploitasi oleh pihak yang tidak berwenang, sehingga dapat mengurangi risiko keamanan serta dampak yang mungkin timbul.[4]



Gambar 1.2 Grafik Penetrasi dan Kontribusi Internet Indonesia Tahun 2024[5]

Berdasarkan gambar 1.2 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melakukan analisis terhadap tingkat penetrasi dan kontribusi internet di pulau-pulau besar Indonesia pada awal 2024 menunjukkan bahwa Jawa memiliki

tingkat penetrasi serta kontribusi internet tertinggi dibandingkan dengan lima pulau besar lainnya di Indonesia. Dalam rincian, tingkat penetrasi internet di Jawa mencapai 83,64%, dan kontribusi internet sebesar 57,82%. Peningkatan tingkat penetrasi internet pada tahun 2024 mencapai 1,31% atau 6 juta pengguna, yang meningkat dari 78,19% pada tahun 2023[5].



Gambar 1.3 Grafik Sebaran Sektor Aduan Siber Tahun 2021[6]

Laporan monitoring keamanan siber tahunan tahun 2021 yang disajikan pada gambar 1.3 menunjukkan bahwa sektor pemerintahan menjadi area yang paling sering diserang oleh peretas. Baik dari pemerintah pusat maupun pemerintah daerah, dimana pemerintah daerah menerima total 81 pengaduan atau 25% dari total 332 pengaduan. Hal ini menunjukkan bahwa pemerintah daerah perlu meningkatkan keamanan *website* untuk mengurangi serangan siber[6].

Dikutip dari *website* CNN Indonesia, Situs *website* administrasi pemerintah dibobol terbanyak. BSSN (Badan Siber dan Sandi Negara) telah menemukan 207 dugaan pelanggaran *database* sepanjang 2023, dengan 55% terjadi di situs administrasi pemerintahan. Oleh karena itu, jelas bahwa keamanan siber adalah keharusan dan bukan lagi pilihan[7].

Website Pengadilan Negeri X, sebagai bagian dari administrasi pemerintahan, tentu tidak terlepas dari risiko keamanan siber yang kerap menjadi

target serangan. Mengingat laporan dari BSSN bahwa lebih dari separuh pelanggaran database di tahun 2023 terjadi pada situs administrasi pemerintahan, website ini juga berpotensi menjadi sasaran peretasan yang dapat mengganggu layanan publik dan mengancam kerahasiaan data. Oleh karena itu, analisis keamanan terhadap website Pengadilan Negeri X menjadi penting untuk memastikan bahwa sistem informasi yang tersedia tidak hanya memberikan kemudahan akses bagi masyarakat, tetapi juga memiliki perlindungan yang memadai terhadap potensi ancaman siber.

Website Pengadilan Negeri X merupakan *website* yang menyediakan sistem informasi tentang pelayanan publik yang berkaitan dengan pelayanan hukum. Hal ini mencakup prosedur pengaduan dan biaya perkara, prosedur permintaan informasi, pengaduan pelayanan publik dan prosedur lainnya. Pada *website* ini juga terdapat sistem informasi pelacakan kasus, sehingga dapat melacak proses kasus yang sedang berjalan atau sudah selesai. Peneliti menggunakan *website* pemerintah Pengadilan Negeri X yang digunakan untuk sempel penelitian pengujian PTES dimana *website* tersebut sudah menggunakan *Hypertext Transfer Protocol Secure* (HTTPS*)*. Peneliti menguji *website* Pengadilan Negeri X, hal ini dilakukan karena banyaknya *website* pemerintah yang kurang aman dan rentan terhadap serangan hacker.

Merujuk pada penelitian sebelumnya yang dilakukan oleh Bita Parga Zen, Rudy A.G. Gultom, dan Agus H.S. Reksoprodjo pada tahun 2021, dengan judul Analisis *Security Assessment* Menggunakan Metode *Penetration Testing* Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. Pada penelitian tersebut Penelitian ini bertujuan untuk memperkuat keamanan sistem komputer dari ancaman pencurian data ilegal yang disebabkan oleh pelanggaran keamanan pada jaringan. Selain itu, penelitian ini juga berfokus pada pengujian untuk meningkatkan perlindungan sistem, termasuk *firewall*, *router*, dan *server*. Pada tahap *scanning* keamanan menggunakan *framework* OWASP *(Open Web Application Security Project)* dan CVSS *(Common Vulnerability Scoring System).* Hasil penelitian menunjukkan bahwa beberapa kerentanan dapat dimanfaatkan oleh *hacker* atau pihak yang tidak bertanggung jawab[8]

Penelitian ini menjawab kebutuhan mendesak untuk pemahaman yang lebih mendalam tentang cara melindungi *website* dengan baik dengan menggunakan praktik analisis kerentanan dan upaya penetrasi yang efektif. Implementasi praktik ini dapat memberikan solusi yang kokoh dan proaktif untuk melawan ancaman keamanan yang terus berkembang di dunia siber. Terlebih lagi pada sektor pemerintahan yang sering terjadi kebocoran data dan peretasan yang lainnya.

Dari masalah tersebut, penelitian ini akan menguji keamanan situs *website* pemerintah dengan tujuan untuk mengidentifikasi celah keamanan dan tingkat kerentanan pada situs *website* Pengadilan Negeri X.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, diperlukannya analisis kerentanan *(vulnerability)* pada sistem informasi *website* Pengadilan Negeri X yang memiliki data bersifat kredensial. Diharapkan metode *Penetration Testing Execution Standard* (PTES) dapat membantu dalam melakukan analisis dan penetrasi terhadap keamanan pada *website* Pengadilan Negeri X.

1.3 Pertanyaan Penelitian

Adapun pertanyaan penelitian sebagai berikut:

1. Bagaimana penerapan metode *Penetration Testing Execution Standard* (PTES) dalam menganalisis keamanan *website* Pengadilan Negeri X?
2. Bagaimana hasil dari pengujian dan analisis keamanan pada *website* Pengadilan Negeri X?
3. Bagaimana memberikan rekomendasi perbaikan berdasarkan hasil analisis menggunakan metode PTES untuk meningkatkan keamanan situs *website* Pengadilan Negeri X?

1.4 Batasan Masalah

Agar penelitian ini tetap terarah pada permasalahan yang akan dibahas, ditetapkan beberapa batasan penelitian sebagai acuan:

1. *Website* yang digunakan untuk melakukan penelitian yaitu *website* Pengadilan Negeri X.
2. Hanya menggunakan metode *Penetration Testing Execution Standard.*

3. Peneliti melakukan seluruh rangkaian tahapan PTES, tetapi nama dan seluruh hal yang berkaitan dengan Pengadilan Negeri X tidak dipublikasikan.
4. Memberikan rekomendasi berdasarkan kerentanan yang ada berdasarkan standarisasi dai BSSN dan OWASP.

1.5 Tujuan Penelitian

Mengacu pada pertanyaan sebelumnya, penelitian ini bertujuan untuk :

1. Dapat mengetahui penerapan metode *penetration testing execution standard* dalam pengujian keamanan *website* Pengadilan Negeri X.
2. Dapat mengetahui hasil dari pengujian dan analisis keamanan pada situs *website* Pengadilan Negeri X.
3. Dapat memberikan rekomendasi perbaikan keamanan pada *website* Pengadilan Negeri X berdasarkan analisis yang dilakukan dengan menggunakan metode *Penetration Testing Execution Standard*.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah, batasan masalah, dan tujuan penelitian di atas, manfaat penelitian ini dapat diidentifikasi sebagai berikut:

1. Sebagai bahan pertimbangan untuk evaluasi sistem keamanan data yang ada di situs *website* Pengadilan Negeri X.
2. Membantu meningkatkan keamanan *website* dari penyusupan oleh pihak yang tidak bertanggung jawab yang mengubah tampilan situs *website* pemerintahan atau kebocoran data.