BAB 1 PENDAHULUAN

1.1 Latar Belakang

Di era digital yang semakin berkembang, sistem informasi berbasis web telah menjadi tulang punggung berbagai layanan publik, termasuk di sektor pemerintahan. Website resmi instansi pemerintah seperti Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas digunakan sebagai sarana penyebaran informasi, pelayanan publik, hingga pengelolaan data internal. Namun, tingginya tingkat ketergantungan terhadap teknologi informasi ini juga meningkatkan risiko terhadap serangan siber. Berbagai insiden kebocoran data dan serangan terhadap situs web pemerintah di Indonesia menunjukkan urgensi penerapan keamanan siber yang kuat, salah satunya melalui kegiatan penetration testing secara berkala.

Pemilihan Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas sebagai objek studi kasus didasarkan pada peran strategis instansi ini dalam pengelolaan infrastruktur digital dan penyediaan layanan informasi publik di wilayah Kabupaten Banyumas. Selain itu, website resmi Dinkominfo Banyumas menjadi salah satu pintu utama interaksi antara pemerintah daerah dan masyarakat, sehingga keberadaannya sangat vital. Berdasarkan observasi awal dan minimnya publikasi terkait pengujian keamanan siber terhadap sistem informasi milik instansi tersebut, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan ketahanan siber pada sektor pemerintahan daerah, khususnya dalam konteks perlindungan data dan pelayanan digital yang aman.
Sebagai bagian dari proses pengumpulan data, penulis juga telah melakukan wawancara langsung dengan pihak internal Dinkominfo Banyumas yaitu kepala bidang APTIKA. Hasil wawancara tersebut mengungkapkan adanya dugaan insiden kebocoran data pada sistem informasi internal, yang menunjukkan adanya celah keamanan yang belum sepenuhnya tertangani. Fakta ini memperkuat urgensi dilakukannya penetration testing secara metodologis guna mengidentifikasi dan memitigasi kerentanan sebelum berdampak lebih luas terhadap layanan publik dan kepercayaan masyarakat.

Insiden-insiden tersebut menunjukkan lemahnya penerapan kebijakan dan sistem keamanan siber yang tepat di sektor publik. Berdasarkan temuan laporan lembaga keamanan nasional serta studi terdahulu, sebagian besar serangan terhadap website instansi pemerintah memanfaatkan kerentanan umum seperti injeksi SQL, pengungkapan direktori, konfigurasi keamanan yang tidak tepat, hingga autentikasi yang gagal. Sebagai contoh, penelitian [1] mengungkapkan enam kerentanan utama pada website Dinas Sosial Surabaya, termasuk Browsable Web Directories dan Content Security Policy (CSP) Header Not Set, yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengeksploitasi sistem. Hal ini menegaskan pentingnya penerapan penetration testing untuk mengidentifikasi dan mengatasi kerentanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab. Fakta di lapangan menunjukkan bahwa sektor publik sering menjadi target empuk serangan karena lemahnya mekanisme pertahanan siber dan minimnya audit keamanan secara berkala. Serangan terhadap website pemerintahan tidak hanya menyebabkan kebocoran data pribadi masyarakat, tetapi juga dapat melumpuhkan sistem layanan publik, memicu disinformasi, dan menciptakan distrust terhadap lembaga pemerintah. Lebih buruk lagi, serangan semacam ini berpotensi melanggar Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mewajibkan instansi publik untuk menjamin keamanan data warganya dalam setiap proses digital. Tanpa pengujian keamanan yang sistematis dan metodologis, instansi seperti Dinkominfo Banyumas berisiko tinggi menjadi korban serangan siber yang berdampak sistemik.

Penetration testing atau uji penetrasi merupakan pendekatan proaktif dalam mengidentifikasi kerentanan keamanan pada sistem informasi dengan mensimulasikan serangan dari pihak luar. Keberhasilan kegiatan ini sangat bergantung pada metodologi yang digunakan untuk memastikan pengujian dilakukan secara menyeluruh, sistematis, dan sesuai dengan standar industri. Dua kerangka kerja yang umum digunakan adalah PTES (Penetration Testing Execution Standard) dan OWASP (Open Web Application Security Project). PTES menyusun proses penetration testing ke dalam tujuh tahap utama, yaitu: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Tahapan-tahapan ini membantu

peneliti atau praktisi keamanan dalam menjaga konsistensi dan cakupan selama proses pengujian berlangsung. Sementara itu, OWASP menyediakan panduan yang lebih spesifik untuk keamanan aplikasi web, dengan fokus pada identifikasi dan mitigasi sepuluh jenis kerentanan paling umum yang dijabarkan dalam OWASP Top 10, serta strategi pengujian terstruktur melalui OWASP Testing Guide. Kedua pendekatan ini telah diterapkan dalam berbagai studi kasus dan terbukti efektif dalam mendeteksi celah keamanan kritis. Sebagai contoh, penelitian [2] menggunakan metode PTES untuk menguji keamanan situs web milik instansi pemerintah dan berhasil mengidentifikasi 13 kerentanan signifikan, termasuk Clickjacking, SQL Injection, dan Cross Site Scripting (XSS), yang menunjukkan bahwa pendekatan sistematis PTES mampu mengungkap risiko keamanan yang tersembunyi. Temuan ini menunjukkan pentingnya penggunaan metode yang tepat dalam kegiatan penetration testing, terutama pada sistem informasi publik yang memproses data sensitif dan bersifat krusial bagi pelayanan masyarakat.

PTES (Penetration Testing Execution Standard) merupakan kerangka kerja komprehensif yang mencakup seluruh proses pengujian keamanan, mulai dari perencanaan, pengumpulan informasi, pemodelan ancaman, analisis kerentanan, eksploitasi, pasca-eksploitasi, hingga pelaporan. PTES menekankan pendekatan menyeluruh dengan dokumentasi yang mendalam untuk setiap tahap pengujian. Sebagai contoh dalam penelitian [3], metode PTES digunakan untuk menganalisis kerentanan pada situs web pemerintah daerah XYZ. Hasilnya menunjukkan adanya 42 peringatan keamanan yang dikategorikan ke dalam empat tingkat risiko: 9 kerentanan dengan tingkat risiko tinggi, 13 kerentanan dengan tingkat risiko sedang, 11 kerentanan dengan tingkat risiko rendah, dan 9 kerentanan dengan tingkat risiko informasional. Di sisi lain, OWASP (Open Web Application Security Project) menyediakan panduan yang lebih spesifik untuk aplikasi web, seperti OWASP Testing Guide dan OWASP Top 10, yang berfokus pada jenis-jenis kerentanan paling umum dan cara pengujiannya. Dalam penelitian [4] penerapan OWASP Testing Guide versi 4.2 pada sebuah situs web pemerintah berhasil mengidentifikasi 32 kerentanan, dengan beberapa di antaranya memiliki tingkat risiko tinggi hingga kritis. Kedua metodologi ini memiliki kelebihan dan kekurangan masing-masing, sehingga penting untuk dilakukan analisis

perbandingan dalam konteks penggunaannya di lingkungan instansi pemerintah. Pemilihan metodologi yang tepat tidak hanya menentukan kedalaman dan cakupan analisis keamanan, tetapi juga efektivitas dalam mendeteksi dan menanggulangi ancaman siber. Dengan mempertimbangkan karakteristik sistem informasi pemerintahan yang kompleks dan memiliki tingkat sensitivitas data yang tinggi, pemilihan framework yang tepat menjadi faktor penting untuk mendukung kebijakan keamanan siber yang berkelanjutan.

Dalam konteks Dinas Komunikasi dan Informatika (Dinkominfo) Banyumas, yang memiliki peran vital dalam pengelolaan informasi publik dan sistem digital daerah, penerapan penetration testing yang efektif menjadi sangat krusial. Pemilihan metodologi yang tepat tidak hanya menentukan tingkat kedalaman analisis keamanan, tetapi juga efektivitas dalam mengidentifikasi dan memitigasi kerentanan. Studi kasus serupa telah dilakukan oleh Diskominfo Magelang terhadap sistem informasi "Pusaka Magelang", di mana penerapan framework OWASP berhasil mengidentifikasi 27 kerentanan dengan rincian 5 berisiko tinggi, 5 sedang, 11 rendah, dan 7 bersifat informasional. Selain itu, pengujian menggunakan metode PTES berhasil menemukan celah berupa sensitive data exposure melalui file info.php() yang dapat diakses publik. Hasil tersebut menunjukkan bahwa kombinasi kedua metodologi dapat memberikan gambaran menyeluruh mengenai kondisi keamanan sistem informasi pemerintah. Dengan demikian, studi kasus pada Dinkominfo Banyumas diharapkan dapat memberikan pemahaman yang lebih konkret mengenai implementasi dan efektivitas PTES dan OWASP dalam konteks dunia nyata, khususnya pada sistem website instansi pemerintahan [5].

Melalui analisis perbandingan antara PTES dan OWASP pada sistem website Dinkominfo Banyumas, penelitian ini tidak hanya berupaya mengevaluasi efektivitas masing-masing kerangka kerja dalam mendeteksi kerentanan, tetapi juga menyusun rekomendasi strategis yang dapat diterapkan oleh instansi pemerintahan serupa. Dengan mempertimbangkan karakteristik sistem informasi pemerintahan yang cenderung kompleks dan memiliki tingkat sensitivitas data yang tinggi, pendekatan hybrid atau pemanfaatan keunggulan kedua framework secara bersamaan menjadi opsi yang layak untuk ditelusuri. Sejumlah studi menyebutkan

bahwa penggunaan kombinasi metodologi dapat meningkatkan cakupan deteksi kerentanan secara signifikan dibandingkan penggunaan satu framework tunggal. Hal ini membuktikan pentingnya penelitian komparatif seperti ini dalam mendukung penguatan kebijakan keamanan siber, terutama di lingkungan sektor publik yang kian terdigitalisasi [6].

Dalam kondisi tersebut, penetration testing (uji penetrasi) menjadi langkah yang tidak hanya penting, tetapi mendesak untuk dilakukan. Penelitian ini mencoba menjawab tantangan tersebut dengan membandingkan dua pendekatan standar industri, yaitu PTES (Penetration Testing Execution Standard) dan OWASP (Open Web Application Security Project), dalam menguji kerentanan keamanan sistem informasi web. Keduanya menawarkan struktur dan fokus yang berbeda: PTES memberikan pendekatan menyeluruh dari sisi jaringan, sistem, hingga eksploitasi lanjutan, sedangkan OWASP fokus pada sepuluh kerentanan aplikasi web paling kritis dan cara mengujinya. Memahami kelebihan dan keterbatasan masing-masing pendekatan menjadi kunci dalam menentukan strategi pengamanan yang tepat bagi institusi pemerintah. Melalui studi kasus pada sistem website Dinkominfo Banyumas, penelitian ini tidak hanya bersifat teknis, melainkan juga strategis—yakni untuk mendukung agenda nasional dalam memperkuat sistem pertahanan siber, meningkatkan kepercayaan publik, dan memastikan sistem pemerintahan digital berjalan aman dan berkelanjutan.

1.2 Perumusan masalah

Berdasarkan latar belakang yang telah disajikan, rumusan masalah penelitian ini dapat dirumuskan sebagai berikut :

1. Lebih unggul mana PTES dan OWASP dalam mengidentifikasi kerentanan keamanan pada sistem informasi berbasis web di lingkungan instansi pemerintah, khususnya Dinkominfo Banyumas?
2. Apa saja perbedaan utama antara pendekatan PTES dan OWASP dalam proses penetration testing, mulai dari tahap perencanaan hingga mitigasi kerentanan?
3. Metodologi mana yang lebih efisien waktu untuk diterapkan dalam konteks pengujian keamanan sistem website instansi pemerintahan daerah seperti

Dinkominfo Banyumas?

1.3 Tujuan Penelitian

Dari latar belakang serta perumusan masalah maka tujuan penelitian ini sebagai berikut :

1. Mengevaluasi efektivitas metode PTES dan OWASP dalam mengidentifikasi dan memitigasi kerentanan pada sistem informasi berbasis web di Dinkominfo Banyumas.
2. Menganalisis perbedaan pendekatan antara framework PTES dan OWASP dalam setiap tahapan penetration testing, mulai dari perencanaan, pengumpulan informasi, eksploitasi, hingga pelaporan.
3. Untuk menentukan metode penetration testing yang paling sesuai dan efisien digunakan pada sistem website instansi pemerintahan daerah berdasarkan studi kasus Dinkominfo Banyumas.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, antara lain:

1. Manfaat Teoritis: Memberikan kontribusi akademik dalam pengembangan kajian keamanan sistem informasi, khususnya dalam melakukan analisis perbandingan pendekatan pengujian penetrasi berbasis OWASP dan PTES. Penelitian ini juga memperluas pemahaman mengenai cakupan kerentanan umum dalam sistem berbasis web pada instansi pemerintahan.
2. Manfaat Praktis: Menjadi referensi bagi instansi pemerintah, khususnya Dinkominfo Banyumas, dalam mengidentifikasi celah keamanan yang ada pada sistem web, serta menyusun langkah mitigasi yang tepat. Hasil penelitian ini dapat dijadikan acuan dalam merumuskan kebijakan dan strategi penguatan keamanan aplikasi berbasis web yang lebih sistematis dan menyeluruh.

1.5 Batasan Masalah

Agar penelitian lebih terfokus dan terarah, maka ruang lingkup penelitian ini dibatasi pada beberapa hal berikut:

1. Penelitian ini hanya dilakukan terhadap sistem website milik Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas sebagai studi kasus, tanpa mencakup infrastruktur sistem lainnya seperti jaringan internal atau layanan cloud.
2. Pengujian hanya dilakukan menggunakan pendekatan OWASP Top 10 versi 2021 dan kerangka Penetration Testing Execution Standard (PTES), tanpa membandingkan dengan framework lain seperti NIST SP800-115 atau OSSTMM.
3. Teknik pengujian terbatas pada metode black-box dan grey-box testing, tanpa menyertakan akses kode sumber (white-box), sehingga eksplorasi hanya dilakukan dari sudut pandang pihak eksternal dan semi-terautentikasi.
4. Tools yang digunakan meliputi Nmap, SQLMap, Dirsearch, OWASP ZAP, Burpsuite, XRAY, dan RAC, dengan fokus pada temuan yang relevan terhadap kedua pendekatan metodologi.
5. Penelitian ini berfokus pada proses identifikasi dan mitigasi kerentanan tanpa melibatkan proses implementasi sistem pengamanan secara real-time di lingkungan operasional Dinkominfo Banyumas.