BAB 1
PENDAHULUAN

1.1 Latar Belakang

Peningkatan jumlah kebocoran data akhir-akhir ini telah membuat banyak pihak semakin berhati-hati dalam memberikan data pribadinya. Kebocoran tersebut tidak hanya merugikan pengguna, tetapi juga dapat membahayakan kelangsungan organisasi atau perusahaan.

Website pemerintah/lembaga negara yang cukup sering dijadikan oleh pelaku serangan siber memberikan asumsi pada masyarakat mengenai lemahnya sistem pemerintah kita. Berikut data 4 tahun terakhir mengenai *website* pemerintah yang mengalami peretasan, baik disengaja oleh hacker atau hanya sebagai bahan penetration testing yang meliputi: Database Kejaksaan RI diretas remaja 16 tahun. 3.086.224 data dibobol dan diperjualbelikan di forum online seharga sekitar Rp 400 ribu pada 17 februari 2021, 272.788.202 data penduduk Indonesia dari BPJS Kesehatan bocor. Data yang bocor antara lain, NIK, nomor HP, alamat, email, NPWP, tempat tanggal lahir, jenis kelamin, hingga foto peserta pada 12 Mei 2021, Situs setkab.go.id terkena defacing. Peretas memasang foto pelajar SMA yang ikut aksi demo #ReformasiDikorupsi pada 2019. Pelakunya berusia 17 dan 18 tahun pada 30 Juli 2021, Data pengguna aplikasi eHAC Kemenkes bocor. Sebanyak 1,3 juta data sensitif penggunanya terekspos pada 24 Agustus 2021, Sistem Peduli Lindungi dibobol. Pelaku membuat sertifikat vaksinasi palsu melalui aplikasi PeduliLindungi, lalu menjualnya pada 3 September 2021,

Data dan dokumen medis pasien Indonesia dijual di forum online. Kebocoran diduga dari server pusat Kementerian Kesehatan. Data yang bocor NIK, anamnesis, foto pasien, CT Scan, pemeriksaan klinis, termasuk detail identitas pasien pada

6 Januari 2022, Situs akpol.polri.go.id terkena defacing. Laman situs resmi Akpol itu berubah menjadi halaman situs judi online pada 24 Mar 2022, Sistem Peduli Lindungi kembali dibobol. Modusnya sama, membuat sertifikat vaksinasi palsu dan menjualnya pada 24 April 2022, Situs Penyelenggara Sistem Elektronik (PSE) Kominfo senilai Rp963 miliar error dan kemudian diretas pada 23 Juli 2022, 85 ribu data pegawai Kemenkumham RI dijual di forum online. Isinya meliputi NIP, Nama, NIK, hingga nomor rekening pada 26 Agustus 2022, Peretas Bjorka merilis kebocoran 1,3 miliar data kartu registrasi SIM prabayar. Data itu terdiri dari NIK, nomor ponsel, provider telekomunikasi, dan tanggal registrasi. Bjorka menjualnya senilai Rp 700 juta pada 2 September 2022, Bjorka kembali merilis kebocoran data penduduk Indonesia. Kali ini 150 juta data penduduk dari KPU dijual senilai Rp 74 juta pada 6 September 2022, Bjorka membocorkan 679 ribu metadata surat dan dokumen milik Presiden RI, termasuk surat-surat rahasia dari BIN. Namun, BIN dan Setpres membantah kebocoran itu pada 9 September 2022, Sistem Informasi Pelayanan Publik (SIPP) Kemenkes terkena defacing pada 26 September 2022,

Bjorka kembali berulah. Kali ini 19 juta data milik BPJS Ketenagakerjaan diklaim berhasil diretas. Data itu ia tawarkan senilai Rp 154 juta pada 12 Maret 2023, Kelompok peretas Lock Bit mencuri dan mengenkripsi sekitar 1,5 terabyte data internal BSI, isinya 15 juta data privat pengguna BSI melalui ransomware. Lock bit akhirnya menyebar data itu ke publik usai permintaan tebusan Rp 309 miliar tidak terpenuhi pada 15 Mei 2023, 34 juta data paspor Indonesia bocor dan diperjualbelikan di forum online. Bjorka disebut-sebut sebagai dalang dan ia menjualnya senilai Rp 154 juta pada 5 Juli 2023, 337 juta data penduduk di Dukcapil Kemendagri bocor dan diperjualbelikan di forum online pada 16 Juli 2023, Data Daftar Pemilih Tetap (DPT) dari situs KPU diretas. Jimbo, sang peretas, menawarkan data itu seharga Rp1,14 miliar pada 28 November 2023,

Situs kpu.go.id sulit diakses publik. Penyebabnya, serangan DDoS di hari pemilihan suara. Beberapa pakar menilai, itu karena traffic pengguna yang meningkat namun server KPU tidak kuat pada 14 februari 2024, Server Pusat Data Nasional Sementara (PDNS) yang dikelola Kemkominfo, lumpuh akibat Brain Cipher Ransomware. Imbasnya, 210 instansi pusat dan daerah terdampak. Pelaku minta tebusan Rp 131,2 miliar pada 20 Juni 2024. (najwashihab, 2024).

Bahkan pernah terulang kembali sistem pemerintah menjadi sasaran peretasan oleh hacker yang ingin memanfaatkan kelemahan demi mendapatkan keuntungan. Setiap kali sistem berhasil ditembus, para peretas berusaha mengakses informasi sensitif atau mengganggu operasional dengan tujuan memperoleh manfaat pribadi, baik dalam bentuk finansial maupun informasi berharga. Upaya-upaya peretasan ini sering kali dilakukan secara canggih, memanfaatkan kerentanan yang mungkin belum terdeteksi oleh pengelola sistem. Akibatnya, tidak hanya keamanan data yang terancam, tetapi juga reputasi lembaga atau organisasi yang mengelola sistem tersebut. Oleh karena itu, penting untuk memperkuat lapisan keamanan serta terus memantau aktivitas mencurigakan yang dapat membuka peluang bagi hacker untuk menyerang.

Di era digital seperti saat ini, *website* menjadi salah satu media utama untuk menyediakan informasi dan layanan secara online. Perguruan tinggi, seperti Universitas Pesantren Tinggi Darul Ulum (Unipdu) Jombang, memanfaatkan *website* untuk mendukung berbagai kebutuhan, seperti penyebaran informasi akademik, pendaftaran mahasiswa baru, hingga layanan administrasi. Namun, dengan meningkatnya ketergantungan pada teknologi ini, ancaman keamanan siber juga semakin berkembang. Situs web dapat menjadi sasaran serangan oleh pihak yang tidak bertanggung jawab, yang dapat menyebabkan gangguan operasional, kebocoran data sensitif, atau kerugian reputasi.

Salah satu ancaman utama dalam keamanan web adalah adanya kerentanan yang dapat dieksploitasi oleh peretas. Kerentanan ini dapat berupa kesalahan konfigurasi, kelemahan pada pengkodean, atau tidak diterapkannya kebijakan keamanan yang memadai. Dalam beberapa kasus, serangan ini bahkan dapat melibatkan manipulasi data atau eksploitasi celah yang tidak terdeteksi sebelumnya. Untuk mengidentifikasi dan menangani potensi risiko ini, metode *Vulnerability Assessment* (VA) menjadi salah satu pendekatan yang efektif. Dengan menggunakan tools seperti Acunetix dan OWASP ZAP, analisis kerentanan dapat dilakukan secara mendalam, memungkinkan pengembang untuk mengambil langkah-langkah mitigasi yang tepat.

Aplikasi web yang seringkali menjadi target utama bagi para hacker karena rentan terhadap berbagai serangan seperti Denial of Service, SQL injection, serta berbagai jenis *malware*. Kerentanan ini timbul karena banyak aplikasi web dikembangkan tanpa memperhatikan aspek keamanan dari awal. Umumnya, aplikasi-aplikasi tersebut dibuat oleh pengembang yang kurang berpengalaman dalam keamanan web, sehingga banyak kelemahan yang dapat dimanfaatkan pada situs tersebut.

Adanya pengujian VAPT yang menjadi suatu kewajiban, karena adanya regulasi dari peraturan bank Indonesia (PBI) dan (OJK) yang mengharuskan perusahaan di Indonesia untuk melakukan pengujian keamanan IT nya. (PT Widya Adijaya Nusantara, 2024). Melalui metode tersebut, diharapkan analisis yang dilakukan dapat memberikan informasi secara detail bagi pengembang untuk memperbaiki atau memperbarui sistem tersebut secara berkala agar terhindar dari serangan hacker.

Penulis memilih menggunakan metode VA (*Vulnerability Assessment*) dalam pengujian untuk mengidentifikasi kerentanan yang terdapat pada *website* kampus Unipdu. Metode ini diterapkan guna mengungkap

potensi kelemahan yang dapat dimanfaatkan oleh pihak tidak berwenang, serta memberikan rekomendasi solusi yang tepat untuk memperbaiki dan memperkuat keamanan *website* tersebut. Dengan pendekatan ini, diharapkan *website* kampus Unipdu dapat menjadi lebih aman dan terlindungi dari berbagai ancaman keamanan siber. Pernyataan tersebut merujuk pada sejumlah penelitian sebelumnya yang telah menggunakan metode yang sama, namun dengan memanfaatkan beberapa tools yang berbeda. (Darmawan dkk., 2024) "Penerapan Metode *Vulnerability Assessment* untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021" menggunakan OWASP ID 2021 dan menerapkan teknik mitigasi. Selain itu, penelitian sebelumnya dengan judul "Vulnerability Assessment And Penetration Testing Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website" studi kasus: Dinas Penanaman Modal dan PTSP Kota Tangerang Selatan yang menggunakan Kali Linux dalam pengujiannya, *Whois*, The Harvester, Whatweb, CXSecurity, Google Hacking Database + Google Dorking, Terminal, Nmap, dan OWASP ZAP oleh (Yaqi, 2023). Terkait dengan hal tersebut, penelitian ini memanfaatkan beberapa tools yang dipilih sesuai dengan kebutuhan, antara lain: OWASP ZAP dan Acunetix Web Vulnerability. Pemilihan tools ini didasari oleh beberapa penelitian sebelumnya yang menjadi acuan utama dalam pengambilan keputusan, diantaranya penelitian dari (Yaqi, 2023) dan penelitian dari (Fadillah dkk., 2023).

Dengan mempertimbangkan latar belakang di atas, penulis memutuskan untuk meneliti *website* Unipdu Jombang dengan judul skripsi **"Analisis Keamanan Website Unipdu Menggunakan Metode Vulnerability Assessment (VA)".**

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang yang telah disampaikan, berikut adalah rumusan permasalahan yang diangkat.

1) Apa saja kerentanan yang terdapat pada *website* kampus Unipdu Jombang dengan menerapkan metode VA (Vulnerability)?
2) Bagaimana kondisi serta tingkat kerentanan sistem informasi pada *website* kampus Unipdu Jombang setelah dilakukan pemeriksaan menggunakan metode vulnerability assessment (VA)?
3) Bagaimana memberikan solusi dari permasalahan yang ditemukan?

1.3 Batasan Masalah

Dalam menentukan batasan masalah seringkali menjadi suatu hal yang krusial untuk menentukan fokus dan tujuan dari suatu penelitian. Penelitian ini berupaya untuk menganalisis dan mengidentifikasi kerentanan pada *website* yang di uji. Berikut ini adalah ruang lingkup batasan yang ditetapkan oleh penulis:

1. Penelitian ini hanya dilakukan pada *website* kampus Unipdu Jombang dengan domain “https://unipdu.ac.id/”, tidak mencakup sistem lain di luar *website* tersebut.
2. Penelitian hanya mencakup analisis kerentanan web yang dapat teridentifikasi oleh metode VAPT dengan menggunakan tools Acunetix Web Vulnerability dan OWASP ZAP untuk vulnerability assessment.
3. Solusi yang diberikan terbatas pada rekomendasi perbaikan terkait kerentanan yang ditemukan selama pengujian VA. Implementasi dari solusi tersebut serta evaluasi hasil perbaikan tidak akan menjadi bagian dari penelitian ini.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengidentifikasi kerentanan yang terdapat pada *website* kampus Unipdu Jombang.
2. Memberikan rekomendasi solusi untuk memperbaikinya melalui metode vulnerability assessment (VA).
3. Selain itu, menyediakan masukan mengenai kelemahan keamanan dalam sistem internal yang mungkin belum terdeteksi sebelumnya.

1.5 Manfaat Penelitian

Dalam penelitian analisis keamanan *website* Unipdu, pihak-pihak yang akan mendapat manfaat disebutkan di bawah ini, bersama dengan manfaat yang diterima oleh masing-masing pihak.

1) Dosen

Menambah wawasan dan pengetahuan mengenai pentingnya keamanan sistem dan agar lebih teliti dalam membuat atau mengembangkan *website* yang dibuat.

2) Mahasiswa

Adanya kepercayaan mahasiswa pada pihak kampus mengenai data yang diberikan. Kenyamanan akses ke informasi penting seperti jadwal perkuliahan, pengumuman, dan layanan akademik dan tidak ada gangguan dalam proses administrasi yang dapat berdampak bagi mahasiswa, dosen, dan staf.

3) Penulis

a. Menambah wawasan dan pengetahuan penulis mengenai perlunya keamanan sistem informasi dan lebih waspada pada data yang digunakan.
b. Memahami pentingnya keamanan sistem yang dikembangkan atau dirancang.

c. Mengetahui cara penanganan isu keamanan *website* dalam mencegah peretas yang mencoba menyusup melalui celah kerentanan *website*.
d. Untuk memenuhi salah satu persyaratan kelulusan Strata Satu (S1) Program Studi Sistem Informasi Fakultas Sains dan teknologi Universitas Pesantren Tinggi Darul Ulum Jombang.

4) Unipdu

a. Penelitian ini akan memperkaya pustaka penelitian universitas yang dapat digunakan sebagai bahan rujukan untuk penelitian sejenis di masa mendatang.
b. Dapat memberikan rekomendasi solusi dalam memperbaiki *website* setelah dilakukannya pengujian keamanan melalui metode VA.
c. Melakukan update sistem berkala, untuk menghindari celah peretasan.
d. Memberikan saran informasi kepada pengembang atau pembuat aplikasi agar lebih memperhatikan aspek keamanan sejak tahap awal pengembangan web, karena kurangnya pemahaman dalam bidang ini dapat menyebabkan kelemahan yang dapat dimanfaatkan oleh pihak yang tidak memiliki wewenang.

1.6 Metode Penelitian

Penelitian dilakukan melalui beberapa tahap. Berikut adalah beberapa metode yang digunakan pada setiap tahap:

1) Metode Pengumpulan Data

Pengumpulan data pada penelitian ini terdiri dari studi pustaka dan studi lapangan. Studi pustaka dilakukan dengan mengumpulkan berbagai informasi dari berbagai sumber, termasuk buku,situs web,skripsi terdahulu, serta literatur yang relevan. Di sisi lain, studi lapangan melibatkan observasi dan wawancara.

2) Metode Pengujian dan Analisis

Pada metode pengujian dan analisis ini, penulis menggunakan pendekatan *Vulnerability Assessment* (VA), yang bertujuan untuk mengidentifikasi celah keamanan dalam sistem. Tools yang dipakai dalam VA meliputi *Acunetix Web Vulnerability* dan *OWASP ZAP*. *Acunetix* adalah aplikasi yang dikenal handal untuk mendeteksi kerentanan web, seperti kesalahan konfigurasi dan kelemahan pengkodean, serta mengkategorikan hasilnya berdasarkan tingkat risiko. Sementara itu, *OWASP ZAP* adalah sebuah tools dari sumber terbuka yang membantu mengidentifikasi berbagai kerentanan keamanan web. Keduanya memungkinkan pemindaian otomatis dan analisis mendalam terhadap *website* untuk memastikan tidak ada potensi celah yang dapat dimanfaatkan pihak yang tidak bertanggung jawab.

1.7 Sistematika Penulisan

BAB 1 PENDAHULUAN

Bab ini membahas berbagai aspek penting yang menjadi dasar penelitian, dimulai dengan latar belakang serta identifikasi masalah yang menjelaskan urgensi penelitian dilakukan. Selanjutnya, dijelaskan rumusan masalah yang menjadi fokus penelitian, termasuk batasan-batasan yang ditetapkan untuk menjaga ruang lingkup penelitian tetap terarah. Bab ini juga memuat tujuan penelitian yang ingin dicapai, manfaat yang diharapkan dari hasil penelitian, serta sistematika penulisan yang memberikan gambaran alur penyusunan dokumen penelitian secara keseluruhan.

BAB 2 LANDASAN TEORI

Bab ini memuat tinjauan teori yang menjelaskan berbagai pengertian dan konsep dasar yang relevan dengan topik penelitian. Teori-teori ini menjadi landasan utama dalam memahami masalah yang dibahas serta memberikan kerangka acuan untuk analisis dan pembahasan lebih lanjut.

BAB 3 METODE PENELITIAN

Bab ini membahas analisis kebutuhan yang diperlukan untuk mendukung keberhasilan pengujian. Penulis akan menguraikan berbagai kebutuhan penting yang diidentifikasi melalui dua sumber utama, yaitu studi pustaka dan studi lapangan, guna memastikan pengujian dapat dilakukan secara efektif dan sesuai dengan tujuan penelitian.

BAB 4 ANALISIS DAN HASIL

Bab ini menyajikan hasil pengujian yang disertai analisis mendalam mengenai dampak yang ditemukan selama penelitian. Selain itu, bab ini juga memuat rekomendasi yang diusulkan penulis untuk mengatasi permasalahan yang teridentifikasi, serta menggarisbawahi temuan-temuan penting yang memerlukan tindak lanjut lebih lanjut.

BAB 5 PENUTUP

Bab ini memuat kesimpulan yang merangkum hasil utama dari penelitian, memberikan gambaran singkat tentang temuan yang diperoleh. Selain itu, bab ini juga menyajikan rekomendasi yang ditujukan kepada pihak-pihak terkait, sebagai langkah-langkah atau saran untuk meningkatkan kualitas atau keamanan berdasarkan hasil penelitian.

DAFTAR PUSTAKA

Daftar pustaka adalah bagian penting dalam sebuah penelitian yang memuat daftar referensi atau sumber-sumber yang digunakan selama proses penulisan. Referensi ini dapat berupa buku, jurnal, artikel, dokumen daring, atau sumber ilmiah lainnya yang relevan dengan topik penelitian.