BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi Informasi dan Komunikasi kini semakin berkembang, hampir di setiap sektor telah menggunakan teknologi informasi dan komunikasi. Beberapa contoh pada sektor bisnis, pemerintahan, dan pendidikan tinggi yang menggunakan teknologi informasi dan komunikasi untuk berkembang menyesuaikan kebutuhan pada saat ini (Amhar & Majid, 2024). Pada pendidikan tinggi khususnya telah menggunakan teknologi *web* untuk melakukan pengelolaan data, pelayanan akademik secara daring, dan publikasi (Amhar & Majid, 2024). Perkembangan teknologi informasi ini juga diimbangi dengan berkembangnya teknik pencurian data sehingga dalam pembuatan sistem informasi perlu diperhatikan dari sisi keamanan data (Putra Armadhani et al., 2022).

Dalam kasus nyata, di Indonesia sering terjadi kasus kriminal yang melibatkan teknik peretasan pada *website*. Salah satu contoh kasus pada insiden *defacement* di situs resmi PWI (Persatuan Wartawan Indonesia) yang tampilan pada sistus tersebut diubah oleh penyerang (Diapari S, 2025). Contoh lainnya dengan kasus yang sama, yakni *defacement* pada situs pemerintahan Trenggalek, yang diberitakan oleh Cyber Press. Pada peristiwa ini dijelaskan peretas memanfaatkan kelemahan sistem dengan teknik *SQL Injection* dan *Brute Force* (Anupriya, 2025). Nur Achmad Salmawan direktur keamanan siber BSSN menuturkan, mulai dai 1 Januari sampai 20 November BSSN mendeteksi 804 anomali traffic pada sektor media (Adiansyah, 2025). Sebanyak 33,54% merupakan serangan eksploitasi pada sistem informasi, aplikasi, *website*, CMS, dan infrastruktur data media, 25,47% merupakan Unauthorized Access and System Misconfiguration, dan 21,37% merupakan Information Leak (Adiansyah, 2025). Hal ini menjadi sangat penting untuk diperhatikan, karena *website* yang aman akan memberikan rasa integritas dan aman bagi pengguna.

Dalam dunia akademik perguruan tinggi *website* digunakan sebagai media penyebaran informasi. Pada hal ini *website* digunakan sebagai sistem informasi, yang di dalamnya terdapat berbagai aplikasi untuk mengolah data mahasiswa,

staff, dosen, maupun data akademik lainnya. Namun dalam penggunaan *website* ini juga dapat digunakan pelaku kejahatan untuk melakukan pencurian data dengan teknik peretasan dari sisi *website* (Zahrani et al., 2025). Contohnya seperti *SQL Injection, XSS* (*Cross Site Scripts*) yang menyerang melalui celah keamanan *website*. Hal ini sangat membahayakan pengguna *website* karena data-data pengguna dapat terlihat oleh pihak tidak bertanggung jawab. Hal ini menyinggung aspek keamanan komputer, yakni *Confidentiality,* yang terkait tentang kerahasiaan suatu informasi (Sofana Iwan & Primartha Rifkie, 2019).

Karena alasan ini keamanan *website* menjadi aspek yang sangat penting dalam menjaga privasi, integritas, dan keandalan sistem. Pada umumnya peretas akan mencari celah keamanan dari sebuah *website* yang kemudian dilakukan *exploitation* dengan berbagai teknik, contohnya menggunakan metode *XSS*, *Brute Force*, *SQL Injectin*, dan lain sebagainya (Riadi et al., 2020).

Maka diperlukan upaya guna mencegah hal tersebut terjadi. Salah satu cara yang dapat dilakukan adalah dengan melakukan *Vulnerability Assessment* guna menemukan kerentanan apa saja yang terdapat pada *website* tersebut, dan kemudian dapat dilakukan perbaikan setelahnya (Prihanto et al., 2023) . Metode ini tidak melibatkan langkah pengujian eksploitasi atau penyerangan yang merusak sistem (Prihanto et al., 2023) . Hal tersebut karena metode ini berfokus pada proses klasifikasi, identifikasi, dan prioritas celah kerentanan tanpa melakukan eksploitasi, yang berbeda dengan metode *penetration testing* yang terdapat langkah tambah berupa eksploitasi pada celah kerentanan. Sehingga metode *vulnerbility assessment* ini dinilai penulis cukup proporsional untuk digunakan pada penelitian ini karena, cukup menggambarkan kondisi dari keamanan *website* terkini.

Selain metode *vulnerability assessment*, penulis juga mengacu pada kerangka klasifikasi celah kerentanan OWASP Top 10 2021 sebagai basis acuan evaluasi. OWASP Top 10 ini merupakan kerangka kerja untuk mengklasifikasi celah kerentanan dan memprioritaskan tingkat risiko dari hasil temuan celah kerentanan pada *website*. Kerangka kerja ini dipilih digunakan karena sesuai dengan objek penelitian yang berupa keamanan aplikasi *web*, serta kemampuannya dalam mendukung metode *vulnerability assessment* dalam

menganalisis. OWASP Top 10 juga rutin merilis update kategori celah kerentanan setiap beberapa tahun, dengan versi terbaru 2025 yang rilis pada tahun 2025. Walau pada 2025 OWASP Top 10 telah merilis versi 2025, penulis tetap menggunakan versi 2021 karena telah menjadi acuan beberapa literatur dan penelitian keamanan *website* sehingga dinilai masih konsisten (OWASP Foundation, 2025a).

Pada pengujian ini objek yang akan ditargetkan yakni *website* "Universitas Islam Majapahit". Penargetan ini didasarkan karena belum adanya penelitian terkait hal ini pada *website* Universitas Islam Majapahit. Sehingga analisis terkait *Vulnerability Assessment* ini dapat menggambarkan kerentanan apa saja yang terdapat pada *website* tersebut, dan dapat memberikan saran perbaikan agar tidak terjadi hal yang merugikan di masa yang akan datang. Oleh karena itu penelitian ini bertujuan untuk mengidentifikasi celah kerentanan dan tingkat risiko dari hasil temuan celah kerentanan yang ada pada *website* Universitas Islam Majapahit.

1.2. Perumusan Masalah

1. Bagaimana penggunaan *tools vulnerability* seperti ZAProxy, SQL Map, GoBuster, WPScan, Hydra dan *tools* pendukung *reconnaissance* seperti DNS Dumpster dapat mengidentifikasi celah kerentanan pada *website* target.
2. Celah kerentanan apa yang dapat diidentifikasi dari hasil *scanning* dan analisis menggunakan *tools* tersebut, serta perbedaan masing-masing *tools* dalam memberikan gambaran terkait kerentanan *website*.
3. Bagaimana peran OWASP menjadi standar keamanan bagi *website* target.

1.3. Tujuan Penelitian

1. Melakukan identifikasi kerentanan pada *website* dengan bantuan *tools vulnerability* ZAProxy, SQL Map, Go Buster, WPScan, Hydra serta *tools* pendukung *reconnaissance* DNS Dumpster.
2. Menganalisis celah kerentanan yang telah ditemukan masing-masing *tools* guna menentukan jenis ancaman, potensi dampak, dan tingkat risiko keamanan *website.*

3. Menerapkan standar OWASP dalam menganalisis dan menentukan tingkat kerentanan pada *website*.

1.4. Batasan Masalah

1. Penelitian ini hanya berfokus ke penilaian kerentanan *website* Universitas Islam Majapahit yang terdiri dari *website* utama, E-Learning, Ejurnal, Siakad, Elib, dan Nala.
2. Penelitian ini tidak mencakup pengujian server fisik, jaringan internal, dan infrastruktur diluar domain yang telah ditentukan.
3. Pengujian dilakukan hanya menggunakan *tools* yang telah ditentukan, yaitu ZAProxy, SQL Map, GoBuster, WPScan, Hydra, dan DNS Dumpster. Selain dari pada itu tidak dibahas pada penelitian ini.
4. Jenis pengujian ini dibatasi pada identifikasi, validasi, dan klasifikasi celah kerentanan, tanpa melakukan eksploitasi lebih lanjut yang bersifat merusak dan merubah sistem.
5. Klasifikasi tingkat kerentanan hanya menggunakan standar OWASP Top 10 2021.
6. Dalam pengujian *Brute Force* menggunakan Hydra hanya pada halaman autentikasi atau pada *endpoint* yang memiliki celah kerentanan autentikasi, tanpa mencoba mendapatkan *password*, *username*, atau kode autentikasi dari pengguna nyata.
7. Penelitian tidak membahas pembuatan sistem keamanan baru, melainkan hanya menganalisis temuan celah kerentanan *website.*
8. Pengujian hanya dilakukan pada waktu dan lingkungan yang telah ditentukan sesuai izin yang diberikan, sehingga hasil dapat berbeda apapabila terdapat pembaruan sistem dan konfigurasi.

1.5. Manfaat Penelitian

1. Dalam akademik, penelitian ini dapat dijadikan referensi ilmiah terkait penerapan *tools vulnerability assessment* seperti OWASP ZAP, GoBuster,

SQL Map, WPScan dan Hydra dalam proses identifikasi kerentanan pada *website*.

2. Penelitian ini juga dapat menambah literatur terkait penggunaan standar OWASP Top 10 dalam klasifikasi tingkat risiko kerentanan.
3. Memberikan informasi detail kepada pengelola sistem mengenai kerentanan yang ditemukan sehingga dapat digunakan sebagai dasar perbaikan keamanan *website*.
4. Pihak pengelola sistem dapat menentukan prioritas penanganan celah kerentanan sesuai dengan tingkat risiko yang telah diklasifikasi.
5. Memberikan kesadaran kepada pengguna dan pengelola *website* terkait celah kerentanan, guna menghindari kerugian terkait celah kerentanan.

1.6. Metode Penelitian

Penelitian ini melakukan pendekatan deskriptif kualitatif dan menggunakan metode *Vulnerability Assessment* dengan standar OWASP Top 10 dalam melakukan penilaian kerentanan (Riadi et al., 2020) . Juga terdapat tambahan metode *Brute Force* guna menguji keamanan dari sisi autentikasi pengguna.

Dalam penelitian ini terbagi menjadi beberapa tahap. Pembagian ini bertujuan untuk menyederhanakan tiap proses agar penelitian ini dapat berjalan dengan presisi dan lebih modular:

1. Menentukan Ruang Lingkup dan Perencanaan

   Tahap pertama merupakan menentukan ruang lingkup penilaian kerentanan, pada tahap ini penulis meminta izin bagian mana yang dapat dilakukan uji coba kepada pihak yang bertanggung jawab. Hasil dari tahap ini merupakan diizinkan terkait bagian-bagian dari *website* yang dapat dilakukan analisis *vulnerability assessment*.
2. Footprinting

   Tahap ini berfungsi untuk menemukan informasi terkait target. Informasi yang dimaksud dapat berupa nama aplikasi, informasi mengenai *framework*, atau bahkan informasi terkait *service*. Pada tahap ini melibatkan penggunaan *tools,* dan DNS Dumpster guna membantu

pencarian informasi. Hasil dari tahap ini adalah semua informasi yang bisa didapatkan terkait *website* tersebut.

3. Vulnerability Scanning

Pada tahap ini setiap informasi yang didapat dianalisa guna menemukan celah berupa informasi sistem yang tidak sengaja tampil. Setelah dilakukan analisa, dari hasil informasi tersebut dilakukan pemetaan *endpoint* atau titik yang dapat dapat diakses pengguna akhir. *Endpoint* ini yang akan dilakukan *scanning* celah keamanan lebih lanjut menggunakan *tools* ZAProxy, Go Buster, dan WPScan. Hasil dari tahap ini adalah informasi celah keamanan yang didapat dari *scanning tools*.

4. Vulnerability Validation

Pada tahap ini, celah keamanan yang telah ditemukan akan dilakukan validasi terhadap celah tersebut. Celah keamanan yang akan divalidasi ini merupakan SQL Injection, XSS dan *Brute Force*. *Tools* yang digunakan pada tahap ini adalah SQL Map, OWASP ZAP, dan Hydra. Hasil dari tahap ini merupakan celah keamanan yang telah tervalidasi.

5. Rating Risk

Tahap *rating risk* merupakan tahap melakukan klasifikasi peringkat kerentanan dari celah yang ditemukan. Tahap ini bertujuan untuk menentukan tingkat kerentanan pada *web,* sehingga dapat memberi prioritas penangan *website* target terhadap celah keamanan. Tahap ini akan dilakukan menggunakan standar OWASP Top 10 dengan bantuan *tools* OWASP ZAP. Hasil dari tahap ini adalah celah kerentanan yang telah terstruktur sesuai tingkat kerentanannya.

6. Pelaporan

Tahap pelaporan ini merupakan tahap final, pada tahap ini penulis melakukan pelaporan terkait temuan yang ada, juga memberikan saran mitigasi untuk menghindari hal yang tidak diinginkan.

1.7. Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang yang menjadi dasar analisis vulnerability assessment. Pada bab ini juga menjelaskan pentingnya menjaga keamanan website. Bab ini terdiri dari rumusan masalah, tujuan penelitian, batasan masalah, manfaat, dan metode penelitian yang dipakai dalam penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini terdiri dari dua bagian:

A. Penelitian Terdahulu: Mengulas penelitian-penelitian sebelumnya terkait metode penilaian kerentanan *website*, penggunaan *tools* dalam melakukan identifikasi celah kerentanan, dan standar yang digunakan dalam analisis.

B. Landasan Teori: Landasan teori ini memuat definisi dari istilah dalam keamanan informasi, metode penelitian, dan *tools* yang akan digunakan dalam penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan metode yang digunakan dan tahapan penelitian terkait analisis kerentanan pada *website.* Bab ini juga menjelaskan ruang lingkup dan waktu penelitian, spesifikasi perangkat penguji, dan *tools* yang digunakan dalam penelitian.

BAB IV PEMBAHASAN DAN IMPLEMENTASI

Bab ini menjelaskan proses serta hasil pengujian *vulnerability Assessment* dari *website* target penelitian. Pada bab ini juga membahas ancaman yang ditemukan, yang dimulai dari menganalisis masing-masing *tools* dalam mengidentifikasi celah kerentanan, serta menganalisis ancaman yang ditemukan.

BAB V PENUTUP dan SARAN

Bab ini merupakan bagian akhir yang membahas kesimpulan penelitian saat ini dan saran penelitian di masa depan. Bab ini juga membahas ringkasan hasil penelitian terkait ancaman yang ada pada *website* target penelitian, dan rekomendasi dalam membenahi ancaman tersebut.