# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Berdasarkan laporan Badan Siber dan Sandi Negara (2024), total trafik anomali di Indonesia mencapai 330.527.636 kejadian sepanjang tahun 2024. Dari jumlah tersebut, terdeteksi 5.780 dugaan serangan *web defacement*, dengan domain pendidikan (ac.id dan sch.id) menjadi salah satu yang paling terdampak, masing-masing sebanyak 1.706 dan 1.240 situs. Fakta ini menunjukkan bahwa sektor pendidikan merupakan salah satu target utama dalam serangan berbasis web [1]. Website pendidikan sangat rentan terhadap serangan siber karena sering menyimpan data publik dan sensitif seperti profil peserta didik dan staf, yang bisa diakses tanpa proteksi memadai banyak sistem informasi akademik di Indonesia belum memiliki mekanisme keamanan yang terintegrasi dengan baik, sehingga membuka peluang bagi penyerang untuk mengeksploitasi celah yang ada [2]. Dengan kondisi tersebut diperlukan pentingnya pengelolaan risiko aset teknologi informasi pada sistem akademik agar terhindar dari potensi ancaman [3].

Tingginya jumlah serangan ini menegaskan bahwa kelemahan keamanan pada aplikasi web masih menjadi persoalan yang serius. Serangan siber umumnya terjadi karena adanya celah yang tidak disadari oleh pengelola sistem, yang dapat dimanfaatkan untuk melancarkan serangan seperti *SQL Injection, Cross-Site Scripting (XSS), atau Denial of Service (DoS)* [4]. Dampaknya tidak hanya menyebabkan gangguan layanan, tetapi juga dapat berujung pada pencurian data, perusakan tampilan halaman (*defacement*), hingga menurunnya reputasi dan kepercayaan publik terhadap institusi [5].

Untuk mencegah risoko tersebut, diperlukan pengujian keamanan secara konsisten dan berkelanjutan. Salah satu pendekatan yang bisa digunakan adalah *Dynamic Application Security Testing* (DAST), yaitu metode pengujian keamanan yang dilakukan saat aplikasi berjalan (*runtime*) tanpa memodifikasi struktur internalnya [6]. Pendekatan ini efektif dalam mendeteksi berbagai kerentanan

aplikasi web yang muncul akibat konfigurasi atau input yang tidak aman, yang sering digunakan untuk pengujian berbasis DAST antara lain Acunetix, Burp Suite, dan OWASP ZAP masing-masing memiliki karakteristik dan kemampuan analisis berbeda [7].

Website SMP Muhammadiyah 1 Depok merupakan media informasi resmi sekolah yang digunakan untuk mendukung kegiatan akademik dan publikasi. Website ini memuat berbagai data seperti profil sekolah, informasi guru dan siswa, dokumentasi kegiatan, serta prestasi akademik [8]. Sebagai sistem yang aktif digunakan dan terhubung ke publik, website tersebut memiliki potensi menjadi target serangan siber [9]. Oleh karena itu, penelitian ini dilakukan untuk menganalisis efektivitas tiga tools DAST (Acunetix, Burp Suite, dan OWASP ZAP) dalam mendeteksi kerentanan pada website SMP Muhammadiyah 1 Depok. Hasil penelitian ini diharapkan dapat memberikan gambaran tingkat keamanan website serta menjadi acuan bagi institusi pendidikan lainnya dalam memilih tools pengujian keamanan yang tepat.

## 1.2 Rumusan Masalah

1. Apa saja jenis kerentanan yang terdeteksi oleh tools DAST Acunetix, Burp Suite, OWASP ZAP pada website SMP Muhammadiyah 1 Depok?
2. Bagaimana perbandingan efektivitas ketiga tools DAST dalam mendeteksi kerentanan pada website SMP Muhammadiyah 1 Depok?

## 1.3 Batasan Masalah

1. Penelitian dilakukan pada website SMP Muhammadiyah 1 Depok sebagai objek dalam pengujian keamanan.
2. Metode yang digunakan dalam penelitian ini adalah *Dynamic Appllication Testing* (DAST) yang berfokus pada pengujian terhadap aplikasi web yang sedang berjalan
3. Tools yang digunakan untuk pengujiaan yaitu Acunetix, Burp Suite, OWASP ZAP untuk mendeteksi kerentanan

4. Variabel yang diteliti adalah hasil pemindaian yang mencakup jenis dan tingkat kerentanan
5. Peneliti tidak mencakup tahap eksploitasi dan modifikasi sistem

## 1.4 Tujuan Penelitian

1. Menganalisis hasil pemindaian *(scanning)* kerentanan pada website SMP Muhammadiyah 1 Depok menggunkan tiga tools *Dynamic Application Testing* (DAST) yaitu Acunetix, Burp Suite, dan OWASP ZAP
2. Mengetahui tingkat kerentanan yang terdeteksi
3. Membandingkan kinerja ketiga tools tersebut berdasarkan hasil pemindaian dalam mendeteksi kerentanan pada website
4. Memberikan gambaran umum mengenai tingkat keamanan website sekolah serta rekomendasi pengujian keamanan yang sesuai pada sistem

## 1.5 Manfaat Penelitian

1. Bagi SMP Muhammadiyah 1 Depok, hasil penelitiaan dapat memberikan informasi mengenai kondisi kemanan website sekolah serta jenis kerentanan yang ditemukan, sehingga dapat dijadikan dasar dalam melakukan peningkatan kemanan sistem
2. Bagi dunia akademik, penelitian ini dapat menjadi referensi ilmiah dalam bidang keamanan siber, khususnya pengujian keamanan aplikasi web menggunakan metode *Dynamic Appliction Testing* (DAST)
3. Hasil penelitian ini dapat memberikan gambaran mengenai kinerja tiga tools DAST dalam mendeteksi kerentanan, sehingga dapat menjadi pertimbangan dalam memilih alat uji kerentanan yang sesuai dengan kebutuhan

## 1.6 Sistematika Penulisan

BAB I PENDAHULUAN, berisi uraian mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan. Bab ini bertujuan memberikan gambaran awal mengenai alasan, arah, dan tujuan penelitian yang dilakukan.

BAB II TINJAUAN PUSTAKA, berisi kajian teori dan hasil penelitian terdahulu yang relevan dengan topik penelitian, seperti konsep keamanan informasi, keamanan aplikasi web, metode *Dynamic Application Security Testing (DAST)*, serta penjelasan mengenai tools Acunetix, Burp Suite, dan OWASP ZAP.

BAB III METODE PENELITIAN, menjelaskan metode penelitian yang digunakan, meliputi objek penelitian, alur penelitian, alat dan bahan, metode pengumpulan data, serta metode analisis data yang digunakan untuk menilai efektivitas ketiga tools DAST.

BAB IV HASIL DAN PEMBAHASAN, menyajikan hasil pemindaian dan analisis dari ketiga tools DAST (Acunetix, Burp Suite, dan OWASP ZAP) terhadap website SMP Muhammadiyah 1 Depok, serta membahas temuan yang diperoleh berdasarkan hasil efektivitas masing-masing alat.

BAB V PENUTUP, berisi kesimpulan dari hasil penelitian serta saran yang dapat dijadikan masukan untuk penelitian selanjutnya maupun bagi pihak pengelola website dalam meningkatkan keamanan sistemnya.