# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang

Berbagai sektor saat ini memanfaatkan website sebagai media untuk menyediakan layanan dan menyampaikan informasi secara digital. Seiring meningkatnya pemanfaatan website, ancaman siber yang menargetkan aplikasi web juga terus mengalami peningkatan. Serangan berbasis web kini menjadi salah satu ancaman yang paling sering ditemukan dalam lingkungan digital modern. Laporan prediksi global memperkirakan bahwa kerugian akibat serangan siber dapat mencapai sekitar USD 10,5 triliun pada tahun 2025 (Khalil, 2025). Kondisi tersebut menunjukkan bahwa keamanan aplikasi web menjadi aspek yang semakin penting untuk diperhatikan oleh setiap organisasi.

Di Indonesia, tren peningkatan ancaman siber juga masih terus terjadi sepanjang tahun 2025. Berbagai bentuk serangan yang tercatat meliputi eksploitasi celah keamanan aplikasi web, percobaan pembobolan sistem, aktivitas botnet, hingga serangan terhadap layanan publik berbasis web. Khalil (2025) menjelaskan bahwa kondisi tersebut menunjukkan sistem informasi daring nasional masih menjadi salah satu sasaran utama pelaku kejahatan siber. Oleh karena itu, upaya peningkatan keamanan website perlu dilakukan untuk menjaga kerahasiaan data, integritas sistem, dan ketersediaan layanan agar tetap dapat beroperasi secara aman.

Sistem Informasi Akademik Universitas Muhammadiyah Jember (SIAKAD) menjadi salah satu layanan yang memiliki peran penting dalam menunjang aktivitas akademik di lingkungan universitas. Sistem berbasis web ini berfungsi untuk mengelola berbagai informasi akademik, seperti data mahasiswa, jadwal perkuliahan, nilai, KRS, serta layanan administrasi akademik lainnya. Tingginya penggunaan sistem tersebut menjadikan SIAKAD sebagai layanan yang memiliki tingkat sensitivitas tinggi. Selain itu, penelitian yang secara khusus membahas pengujian penetrasi manual pada sistem ini masih relatif sedikit sehingga masih terbuka peluang untuk dilakukan kajian lebih lanjut. Apabila evaluasi keamanan tidak dilakukan secara menyeluruh, risiko yang ditimbulkan dapat menjadi lebih besar, terutama ketika terdapat kerentanan yang belum diketahui atau belum ditangani dengan baik.

Kerentanan yang tidak segera ditangani pada *website* seperti SIAKAD Unmuh Jember dapat menimbulkan berbagai dampak. Dampak tersebut antara lain kebocoran data pribadi mahasiswa dan dosen, perubahan data akademik seperti nilai dan jadwal perkuliahan, serta terjadinya *downtime* yang dapat mengganggu proses administrasi maupun kegiatan pembelajaran. Penelitian mengenai aplikasi akademik di Indonesia menunjukkan bahwa *website* perguruan tinggi masih rentan terhadap berbagai serangan, seperti perubahan tampilan halaman (*defacement*), akses tidak sah ke dalam sistem, serta penyebaran data pribadi pengguna (Setiawan & Fachri, 2025). Hasil penelitian tersebut memperlihatkan bahwa sistem akademik termasuk aset digital yang membutuhkan perlindungan keamanan yang memadai agar tidak mudah dieksploitasi.

Untuk mengatasi permasalahan tersebut, *penetration testing* dipilih sebagai salah satu pendekatan yang sesuai karena mampu mensimulasikan serangan secara terkontrol guna menemukan celah keamanan pada sistem. Metode ini tidak hanya mengandalkan hasil deteksi otomatis, tetapi juga melibatkan proses verifikasi secara manual terhadap setiap temuan yang diperoleh. Dengan cara tersebut, tingkat risiko dapat dinilai secara lebih akurat sehingga rekomendasi mitigasi yang dihasilkan menjadi lebih tepat sasaran. Penelitian ini menggunakan *OWASP TOP* 10 sebagai acuan karena kerangka tersebut memuat sepuluh jenis kerentanan aplikasi web yang paling umum dan memiliki tingkat risiko tinggi berdasarkan hasil validasi global. Selain itu, berbagai kerentanan yang tercantum dalam *OWASP TOP* 10 juga masih sering ditemukan pada aplikasi akademik maupun layanan publik di Indonesia (Sriyasa, 2026).

Sejumlah penelitian terdahulu umumnya lebih banyak memanfaatkan *vulnerability scanner* otomatis, seperti ZAP maupun Acunetix, untuk menemukan celah keamanan pada aplikasi web. Meskipun mampu membantu proses identifikasi kerentanan, hasil yang diperoleh belum sepenuhnya menggambarkan tingkat eksploitabilitas yang sebenarnya karena tidak seluruh temuan diuji lebih lanjut melalui eksploitasi secara manual. Selain itu, analisis risiko yang dilakukan pada beberapa penelitian sebelumnya masih memiliki keterbatasan dalam menghubungkan temuan kerentanan dengan dampak yang mungkin ditimbulkan terhadap layanan institusi. Berdasarkan kondisi tersebut, penelitian ini dilakukan

untuk memberikan gambaran keamanan yang lebih mendalam pada Sistem Informasi Akademik Universitas Muhammadiyah Jember. Pengujian dilakukan dengan mengombinasikan analisis otomatis dan manual melalui *penetration testing*, kemudian hasil temuan diklasifikasikan berdasarkan *OWASP TOP* 10 agar rekomendasi mitigasi yang diberikan dapat lebih relevan dengan kondisi sistem yang diteliti.

## 1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, penelitian ini dirumuskan ke dalam beberapa pertanyaan penelitian sebagai berikut:

1 Kerentanan apa saja yang terdapat pada Sistem Informasi Akademik (SIAKAD) Universitas Muhammadiyah Jember berdasarkan kategori *OWASP TOP 10*?
2 Bagaimana tingkat risiko dari masing-masing kerentanan yang ditemukan berdasarkan metode penilaian risiko *OWASP*?
3 Apa rekomendasi teknis yang dapat diterapkan untuk meningkatkan keamanan Sistem Informasi Akademik Universitas Muhammadiyah Jember setelah proses pengujian dilakukan?

## 1.3 Tujuan Penelitian

1 Mengidentifikasi kerentanan pada Sistem Informasi Akademik Universitas Muhammadiyah Jember menggunakan metode *penetration testing* berbasis *OWASP TOP 10*.
2 Mengukur tingkat risiko dari setiap kerentanan yang ditemukan berdasarkan *OWASP TOP 10 Risk Rating Methodology*.
3 Menyusun rekomendasi teknis untuk mitigasi dan peningkatan keamanan pada Sistem Informasi Akademik Universitas Muhammadiyah Jember.

## 1.4 Manfaat Penelitian

Penelitian ini menambah pengetahuan tentang bagaimana cara menguji keamanan aplikasi web. Dengan menggunakan standar *OWASP TOP 10*, penelitian ini menjelaskan jenis-jenis kelemahan atau kerentanan yang paling sering ada di aplikasi berbasis web. Hasil ini bisa digunakan sebagai tambahan referensi bagi penelitian lain di masa depan tentang keamanan siber dan pengembangan aplikasi yang lebih aman.

## 1.5 Batasan Masalah

Agar penelitian lebih terarah, maka batasan masalah ditetapkan sebagai berikut:

1 Objek penelitian hanya difokuskan pada *website* Sistem Informasi Akademik Universitas Muhammadiyah Jember (*HTTP*s://sia.unmuhjember.ac.id)

2 Metode pengujian keamanan yang digunakan adalah *penetration testing non-destruktif*, tanpa melakukan tindakan yang berpotensi mengganggu operasional sistem.

3 Kerangka evaluasi kerentanan yang digunakan mengacu pada *OWASP TOP 10* tahun 2021 sebagai standar klasifikasi risiko.

4 Penelitian ini tidak melakukan perubahan, perbaikan, atau modifikasi langsung pada sistem, melainkan hanya memberikan hasil evaluasi serta rekomendasi teknis untuk mitigasi.

5 Tahapan eksploitasi dibatasi hanya pada *Proof of Concept (PoC)* yang aman, dengan ketentuan:

   a. Tidak merusak atau memanipulasi *database*,
   b. Tidak mengambil, menyalin, atau menyebarkan data sensitif,
   c. Tidak melakukan tindakan yang dapat menyebabkan gangguan layanan.