

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong pemanfaatan *website* sebagai media utama dalam penyampaian informasi dan layanan digital, termasuk pada sektor pendidikan. *Website* digunakan sebagai sarana publikasi informasi, komunikasi, serta pelayanan kepada masyarakat secara luas. Oleh karena itu, keberadaan *website* yang andal dan aman menjadi kebutuhan penting bagi institusi pendidikan agar informasi yang disampaikan dapat diakses dengan baik dan terpercaya [1],[2].

Seiring dengan meningkatnya penggunaan *website*, ancaman terhadap keamanan informasi juga semakin kompleks. *Website* yang tidak memiliki sistem keamanan yang memadai berpotensi mengalami berbagai serangan siber, seperti pencurian data, penyalahgunaan akses, hingga gangguan layanan sistem. Kerentanan pada aplikasi *web* dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses atau memanipulasi data, sehingga menimbulkan risiko terhadap kerahasiaan, integritas, dan ketersediaan informasi [3], [4].

Permasalahan keamanan *website* perlu mendapat perhatian khusus melalui proses pengujian keamanan yang sistematis dan terukur. Pengujian keamanan bertujuan untuk mengidentifikasi celah atau kelemahan sistem sebelum

dimanfaatkan oleh pihak eksternal. Dengan adanya proses pengujian, potensi risiko keamanan dapat diminimalkan sejak dini melalui penerapan rekomendasi perbaikan yang sesuai [5].

Salah satu pendekatan yang umum digunakan dalam pengujian keamanan aplikasi *web* adalah metode *Black Box Testing*. Metode ini melakukan pengujian tanpa memerlukan akses terhadap source code atau konfigurasi internal sistem, sehingga pengujian dilakukan dari sudut pandang pengguna atau penyerang eksternal. Pendekatan Black Box dinilai efektif untuk mengevaluasi keamanan *website* publik karena mampu merepresentasikan kondisi serangan nyata yang mungkin terjadi pada sistem [6], [7].

Dalam penelitian ini, pengujian keamanan dilakukan dengan memanfaatkan OWASP *Zed Attack Proxy* (ZAP) sebagai tools pendukung. OWASP ZAP menyediakan fitur *passive scanning* dan *active scanning* terbatas yang digunakan untuk mendeteksi kerentanan umum pada aplikasi *web*, seperti kesalahan konfigurasi keamanan, kelemahan pengelolaan sesi, serta potensi serangan injeksi, tanpa mengganggu operasional sistem [8].

Website SMPN 6 Muaro Jambi merupakan media informasi publik yang digunakan untuk menyampaikan berbagai informasi akademik dan non-akademik kepada masyarakat. Sebagai *website* yang dapat diakses secara umum, diperlukan evaluasi terhadap tingkat keamanannya untuk memastikan sistem terlindungi dari potensi ancaman siber. Oleh karena itu, penelitian ini dilakukan untuk menganalisis kerentanan keamanan pada *website* SMPN 6 Muaro Jambi menggunakan metode

Black Box Testing berbasis OWASP ZAP serta memberikan rekomendasi perbaikan guna meningkatkan keamanan sistem.

1.2. RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apa saja jenis kerentanan keamanan yang terdapat pada *website* SMPN 6 Muaro Jambi berdasarkan hasil pengujian Black Box Testing menggunakan OWASP ZAP?
2. Bagaimana tingkat risiko dari kerentanan keamanan yang ditemukan pada *website* SMPN 6 Muaro Jambi?
3. Apa dampak kerentanan tersebut terhadap keamanan sistem *website*?
4. Rekomendasi perbaikan apa yang dapat diberikan untuk meningkatkan keamanan *website* SMPN 6 Muaro Jambi?

1.3. BATASAN MASALAH

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mengidentifikasi kerentanan keamanan pada *website* SMPN 6 Muaro Jambi menggunakan metode Black Box Testing.
2. Menganalisis tingkat risiko dari setiap kerentanan yang ditemukan.
3. Mengetahui dampak kerentanan terhadap keamanan sistem *website*.
4. Memberikan rekomendasi perbaikan keamanan yang dapat diterapkan.

1.4. TUJUAN PENELITIAN

Berdasarkan latar belakang dan rumusan masalah yang ada, penelitian ini bertujuan untuk:

1. Menganalisis kondisi keamanan website SMPN 6 Muaro Jambi dengan memetakan celah kerentanan yang ada.
2. Mengevaluasi hasil temuan sebagai bahan masukan bagi pengelola website dalam meningkatkan keamanan sistem.
3. Menyusun rekomendasi teknis untuk perbaikan celah keamanan berdasarkan standar keamanan aplikasi web internasional.

1.5. MANFAAT PENELITIAN

Manfaat yang diharapkan dari penelitian ini adalah:

1. Memberikan gambaran mengenai kondisi keamanan *website* SMPN 6 Muaro Jambi.
2. Menjadi bahan evaluasi bagi pengelola *website* dalam upaya meningkatkan keamanan sistem.
3. Menghasilkan rekomendasi perbaikan yang terukur berdasarkan hasil pemetaan kerentanan terhadap standar keamanan aplikasi *web* internasional

1.6. SISTEMATIKA PENULISAN

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran yang jelas mengenai alur pembahasan serta keterkaitan antar bab dalam penelitian. Adapun sistematika penulisan dalam skripsi ini adalah sebagai berikut:

Bab I Pendahuluan

Bab ini berisi uraian mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan yang digunakan sebagai gambaran awal terhadap keseluruhan isi skripsi.

Bab II Tinjauan Pustaka

Bab ini memuat landasan teori yang berkaitan dengan keamanan *website*, metode Black Box Testing, OWASP Top 10, serta tools OWASP Zed Attack Proxy (ZAP). Selain itu, bab ini juga menyajikan penelitian terdahulu yang relevan sebagai dasar pendukung dalam pelaksanaan penelitian.

Bab III Metodologi Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, meliputi pendekatan Black Box Testing, tahapan pengujian keamanan *website*, alat dan bahan yang digunakan, serta ruang lingkup dan batasan penelitian.

Bab IV Hasil dan Pembahasan

Bab ini menyajikan hasil pengujian keamanan *website* yang telah dilakukan menggunakan OWASP ZAP. Selanjutnya, hasil tersebut dianalisis dan dibahas untuk mengetahui jenis kerentanan, tingkat risiko, serta dampaknya terhadap keamanan sistem *website*.

Bab V Penutup

Bab ini berisi kesimpulan yang diperoleh dari hasil penelitian serta saran yang dapat digunakan sebagai bahan pertimbangan untuk pengembangan dan peningkatan keamanan *website* di masa mendatang.