BAB 1

PENDAHULUAN

I.1 Latar Belakang

Dalam teknologi informasi, internet merupakan salah satu hal yang sangat penting dan berguna pada saat ini. Internet memberikan dampak yang sangat luar biasa bagi kehidupan sehari-hari seperti cara masyarakat saat ini berkomunikasi, bekerja, mendapatkan informasi dan bersosial media. Beberapa perubahan yang sangat signifikan dengan adanya internet sangat memberikan keuntungan yang luar biasa bagi kehidupan sehari-hari. Dalam hal mendapatkan informasi, dengan adanya internet masyarakat dapat mengakses informasi dengan mudah salah satunya menggunakan *website*. Saat ini sudah banyak informasi-informasi yang dapat diakese melalui *website* dan juga *website* dapat menyajikan beberapa data informasi pribadi pengguna yang ada di dalamnya. Karena informasi yang terdapat di dalam *website* adalah hal yang sangat penting, oleh karena itu hanya orang yang berhak saja yang dapat mengakses informasi tersebut.

Membahas mengenai data-data penting yang terdapat di dalam sebuah *website* tidak terlepas dari celah kerentanaan yang ada di dalam *website* tersebut. Kerentanan merupakan kelemahan yang terdapat di dalam sebuah *website* dan dapat menyebabkan adanya potensi resiko sistem sehingga pihak yang tidak bertanggung jawab atau biasa yang disebut dengan *attacker* masuk ke dalam sistem dan melakukan eksploitasi untuk mendapatkan informasi penting yang terdapat di dalam *website* (Sharma & Jhunjhunwala, 2020). Setiap website memiliki jenis kerentanan yang berbeda seperti SQL *injection* dan *Cros-Site Scripting*. *SQL injection* adalah sebuah kerantanan yang memanfaatkan SQL injection oleh *attacker* untuk mendapatkan seluruh infromasi penting melalui database SQL seperti kata sandi dan nam pengguna. *Attacker* juga dapat melakukan berbagai tindakan berbahaya lainnya seperti menambah,memodifikasi dan menghapus data yang terdapat di dalam database. Sedangkan *Cros-Site Scripting* atau yang biasa dikenal dengan XSS adalah jenis kerentanan yang disebabkaln oleh *attacker* yang memasukkan serangan melalui *scripting* yang

ditujukan kepada browser pengguna dengan tujuan untu mencuri informasi pengguna. *Attacker* mencuri data pengguna melalui *website* yang rentan. Banyaknya masalah keamanan yang terjadi pada sebuah website akibat adanya kerentanan perlu dilakukan sebah upaya untuk mengurangi permasalahan tersebut. Upaya yang dapat dilakukan adalah dengan melakukan pengujian keamanan pada website. Pengujian keamanan ini bertujuan untuk menemukan kerentanan yang terdapat didalam sebuah website sehingga dari kerentanan yang ditemukan akan dilakukan analisis yang bertujuan untuk memberikan rekomendasi perbaikan dari setiap jenis kerentanan yang didapatkan sehingga dapat dilakukan mitigasi untuk mengurangi resiko serangan keamanan yang dapat terjadi kapan saja.

Website rekruitasi praktikum merupakan salah satu *website* administrasi rekruitasi praktikum yang terdapat pada fakultas XYZ. *Website* ini berfungsi untuk membantu mahasiswa dalam mengurus semua keperluan adminitrasi yang diperlukan untuk proses kegiatan rekruitaitasi asisten seperti melakukan pengisian data pribadi mahasiswa, pemilihan laboratorium dan melampirkan berkas-berkas yang dibutuhkan selama kegiatan proses rekruitasi asisten. Banyaknya data penting mahasiswa yang terdapat dalam portal ini sehingga perlu dilakukan tindakan keamanan yang dapat mengamankan data data mahasiswa yang terdapat di dalam portal akademik. Tindakan yang dapat dilakukan adalah dengan melakukan *security testing* pada *website* untuk menemukan kerentanan yang terdapat di dalam *website* ini. Kerentanan yang sudah ditemukan akan dilakukan analisis dan mitigasi untuk mengurangi dampak yang disebabkan oleh kerentanan yang terdapat pada *website*.

Dalam melakukan *security testing* menggunakan sebuah metode pengujian , dalam penelitian ini menggunakan metode *Vulnerability Asessment and Penetration Testing* (VAPT). *Vulnerability Asessment* merupakan kegiatan pengujian dengan menggunakan beberapa tools untuk menemukan celah keamanan yang terdapat pada *website* target sedangkan *penetration testing* adalah teknik keamanan yang digunakan oleh sebuah perusahaan atau organisasi untuk mengidentifikasi dan menguji kerentanan yang terdapat pada website. *Penetration testing* dilakukan dengan mensimulasikan penyarangan pada website

target untuk membantu perusahaan dalam melakukan evaluasi dari celah keamanan yang terdapa pada *website* suatu perusahaan. Metode ini digunakan untuk membantu mengidentifikasi kerentanan keamanan yang terdapat pada sebuah *website* dan melakukan tindakan perbaikan untuk mengatasi kerentanan yang ditemukan supaya tingkat keamanan *website* lebih tinggi dan resiko serangan terhadap website menjadi berkurang.

Dalam melakukan pengujian kerentanan keamanan terhadap *website* rekruitasi asisten pada Universitas XYZ digunakan beberapa tools yaitu OWASP ZAP, Acunetix dan Netsparker. Ketiga tools ini digunakan untuk mengidentifikasi kerentanan yang terdapat *website* rekruitasi asisten. Kerentanan yang ditemukan akan dilakukan analisis dan mitigasi untuk mengurangi serangan yang dapat terjadi pada website.

I.2 Perumusan Masalah

Adapun rumusan masalah yang mendasari penelitian dari Tugas Akhir ini, sebagai berikut:

1. Bagaimana hasil dan analisis keamanan *existing* pada *website* rekruitasi asisten pada fakultas XYZ menggunakan *tools* OWASP ZAP, Acunetix dan Net Sparker?
2. Bagaimana rekomendasi perbaikan dan tahapan mitigasi yang dapat diberikan pada *website* rekruitasi asisten pada fakultas XYZ?

I.3 Tujuan Penelitian

Dari rumusan masalah, ada beberapa tujuan dari penelitian ini sebagai berikut :

1. Hasil dan analisis keamanan *existing* pada *website* rekruitasi asisten pada fakultas XYZ menggunakan *tools* OWASP ZAP, Acunetix dan Net Sparker.
2. Rekomendasi perbaikan dan tahapan mitigasi yang akan diberikan pada *website* rekruitasi asisten pada fakultas XYZ.

I.4 Batasan Penelitian

Adapun beberapa batasan masalah dalam penelitian ini, diantaranya adalah sebagai berikut :

1. Pada penelitian Tugas Akhir ini, menggunakan 3 *automated tools scanning* yaitu OWASP ZAP versi 2.11.1, Net Sparker *professional edition* dan Acunetix premium.
2. Penelitian ini mengukur tingkat kerentanan serta memberikan rekomendasi mitigasi yang diterapkan berdasarkan hasil *vulnerability scanning* dari *tools* OWASP ZAP, Net Sparker dan Acunetix.
3. Kerentanan dengan *risk level informational* tidak akan dilanjutkan ke tahap eksploitasi lebih lanjut.
4. Penelitian ini terbatas hanya sampai tahap *exploitation* dan dilanjutkan ke tahap mitigasi.

I.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini, adalah sebagai berikut:

1. Bagi Fakultas XYZ Universitas XYZ, penelitian ini bermanfaat untuk mengetahui kerentanan yang terdapat pada *website* rekruitasi asisten praktikum yang dapat dijadikan acuan untuk meningkatkan keamanan pada sistem website. Selain itu, manfaat lain dari penelitian ini adalah untuk mengurangi serangan yang dapat terjadi kapan saja pada *website* dan bisa dilakukan mitigasi sebelum berakibat fatal pada sistem *website* tersebut.

2. Bagi peneliti yang bergerak di bidang sistem informasi pendidikan tinggi, penelitian ini dapat pada menjadi refrensi dalam melakukan analisis celah kerentanan yang terdapat pada website dengan menggunakan tools OWASP ZAP, Net Sparker dan Acunetix.

I.6 Sistematika Penulisan

Sistematika penulisan dari penelitian ini terdiri dari enam bab, adapun uraian dari keenam bab tersebut disusun sebagai berikut:

1. Bab pertama, Bab ini berisikan tentang latar belakang penelitian, rumusan masalah dalam penelitian, tujuan penelitian, manfaat penelitian dansistematika penulisan dalam penelitian
2. Bab kedua, bab ini membahas mengenai literatur yang sesuai dengan permasalahan yang diangkat pada penelitian karya ilmiah, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sekarang serta berisi teori-teori pendukung yang berkaitan dengan penelitian
3. Bab ketiga, bab ini membahas mengenai metodologi yang digunakan dalam penelitian, model konseptual yang diambil dalam merumuskan solusi dari penelitian yang diambil serta menjelaskan tentang alur penelitian yang akan dilakukan yang disusun dalam sistematika penelitian dari tahap awal hingga tahap akhir
4. Bab keempat, pada bab ini membahas mengenai instrument hardware dan software yang digunakan dalam implementasi penelitian ini, serta penjelasan mengenai skenario pengujian yang akan digunakan
5. Bab kelima, pada bab ini membahas mengenai penjelasan hasil pengujian yang telah dilakukan di bab sebelumnya dan melakukan analisis dari hasil yang sudah dilakukan berdasarkan literatur yang sudah ditetapkan pada penelitian serta memberikan rekomendasi dari hasil analisis.
6. Bab keenam, Bab ini menjelaskan tentang penjelasan intisari dari keseluruhan hasil pengujian dan menjawab rumusan masalah yang telah ditentukan serta berisi saran penelitian yang akan dilakukan selanjutnya.