BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital yang semakin berkembang, penggunaan *website* semakin meningkat dan menjadi hal yang sangat penting dalam kehidupan sehari-hari. *Website* memberikan kemudahan bagi kita untuk mendapatkan informasi yang diperlukan dengan cepat dan mudah dari berbagai sumber. Banyak orang kini lebih memilih untuk berbelanja, berkomunikasi, bermain *game*, atau 1angka mencari pekerjaan melalui *website*. Namun, dengan meningkatnya penggunaan *website* tentu risiko keamanan yang dihadapi juga semakin besar. Keamanan data menjadi salah satu masalah utama yang harus diperhatikan dalam penggunaan *website*. Keamanan data merupakan bagian penting dalam implementasi suatu sistem infomasi. Setiap kali seseorang mengunjungi atau menggunakan *website*, data sensitif seperti informasi pribadi dan keuangan dapat menjadi target peretasan atau kebocoran data. Basis data sebagai media penyimpanan data pada sistem informasi harus memiliki keamanan yang baik dengan memenuhi tiga aspek penting keamanan informasi yaitu Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*) (Nurul et al., 2022).

Salah satu celah keamanan yang dapat mengakibatkan kebocoran data adalah *SQL Injection*. *SQL Injection* adalah teknik penyerangan yang dilakukan dengan cara memanipulasi masukan yang mengarah ke basis data dengan memasukkan *query SQL* (*Structured Query Language*) pada suatu aplikasi atau *website*. Dampak dari celah keamanan ini adalah penyerang dapat membaca, menambah, mengubah, atau menghapus data pada basis data suatu sistem informasi. Hal ini tentunya berakibat sangat fatal karena dapat mengakibatkan kebocoran data seperti informasi pribadi, informasi bisnis, atau data sensitif lainnya dan dapat disalahgunakan oleh pihak yang tidak bertanggung jawab (Bappenas, 2021).

Pengujian celah keamanan *SQL Injection* dapat dilakukan dengan berbagai metode. Salah satu metode yang dapat digunakan adalah *fuzzing* (*fuzz testing*). *Fuzzing* adalah metode pengujian dengan cara memasukkan nilai tidak normal pada *form input* sistem target dan memonitor respon tidak normal untuk menemukan kerentanan atau celah keamanan pada aplikasi *website* (Kristara et al., 2021). Respon yang menunjukkan suatu sistem rentan terhadap celah keamanan *SQL Injection* adalah dengan menampilkan pesan *error* basis data atau perubahan isi konten pada halaman *website* seperti menghilangnya sebagian isi konten, menampilkan halaman *blank* putih, dan sebagainya.

Studi kasus yang menjadi objek penelitian ini adalah *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh. *Website* PUMABA adalah sistem informasi yang digunakan untuk melakukan pendaftaran ulang bagi mahasiswa baru yang dinyatakan lulus ke Universitas Malikussaleh. Sistem ini menyimpan data-data penting mahasiswa seperti informasi pribadi, informasi akademik, dan sebagainya. Keamanan informasi sistem PUMABA sangat penting untuk menjaga kerahasiaan dan integritas data. Oleh sebab itu, penulis merasa perlu dilakukannya penelitian untuk menguji celah keamanan *SQL Injection* pada sistem PUMABA untuk memastikan bahwa sistem tersebut terhindar dari serangan dan kebocoran data.

(Septa Kristara et al., 2021) melakukan penelitian berjudul "Pengujian Kualitas Aplikasi *Web E-Learning* Universitas Pamulang Menggunakan Metode *Black Box*". Penelitian dilakukan dengan menguji celah keamanan *SQL Injection* dan *Cross Site Scripting* (XSS) pada *website e-learning* Universitas Pamulang menggunakan metode *black-box testing* dengan pendekatan teknik *fuzzing* (*fuzz testing*). Pengujian yang dilakukan hanya terbatas pada *form login* dan menggunakan sepuluh data *fuzzing*. Hasil dari pengujian adalah tidak ditemukannya celah keamanan *SQL Injection* dan XSS pada *form login*.

Penelitian lain dilakukan oleh (Djayali, 2020) dengan judul "Analisa Serangan *SQL Injection* pada *Server* Pengisian Kartu Rencana Studi (KRS) *Online*". Penelitian ini melakukan uji celah keamanan dengan melakukan serangan *SQL Injection* pada *server* pengisian Kartu Rencana Studi (KRS) Aikom Ternate.

Pengujian dilakukan menggunakan *tool* SQLMAP dengan metode *comment* dan metode *numeric*. Dari pengujian yang dilakukan, ditemukan celah keamanan *SQL Injection* pada *form login* untuk akun mahasiswa dan prodi menggunakan metode *comments*. Selain itu, penyerang juga dapat mengakses seluruh basis data yang terdapat pada *server* menggunakan metode *numeric*.

Penelitian ini akan melakukan pengujian celah keamanan *SQL Injection* pada *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh. Hasil dari penelitian ini adalah untuk menemukan celah keamanan *SQL Injection* yang terdapat pada *website* PUMABA Universitas Malikussaleh yang akan digunakan sebagai acuan atau dasar untuk memperbaiki sistem dengan tujuan meminimalisir kemungkinan terjadinya kebocoran data.

1.2 Rumusan Masalah

Berdasarkan penjabaran latar belakang di atas, permasalahan yang akan dibahas adalah:

1. Apakah *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh memiliki celah keamanan *SQL Injection*?
2. Bagaimana cara melakukan pengujian celah keamanan *SQL Injection* pada *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh dengan metode *fuzzing* (*fuzz testing*)?
3. Bagaimana solusi yang dapat diambil untuk memperbaiki celah keamanan *SQL Injection* pada *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh?

1.3 Batasan Masalah

Batasan masalah yang ditetapkan pada penelitian ini adalah:

1. Objek pada penelitian ini adalah *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh.
2. Penelitian dilakukan menggunakan metode *grey-box testing* karena penguji diberi informasi awal berupa data username dan password untuk login ke sistem. Setelah selesai melakukan pengujian dan menemukan celah

keamanan *SQL Injection*, penulis diberikan akses ke *source code* dari sistem yang diuji untuk dilakukan perbaikan.

3. Penelitian ini menggunakan *website cloning* dari *website s*istem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh yang asli guna menghindari perubahan data.
4. Dalam penelitian ini, penulis akan menjelaskan langkah-langkah pengujian, menyajikan hasil pengujian, dan memberikan solusi yang diambil untuk memperbaiki temuan celah keamanan *SQL Injection* pada *website* yang menjadi objek penelitian.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengidentifikasi apakah *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh terdapat celah keamanan *SQL Injection* atau tidak.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Bagi penulis
   a. Untuk memenuhi syarat memperoleh gelar Sarjana Komputer di Prodi Teknik Informatika Universitas Malikussaleh.
   b. Meningkatkan pengetahuan dan kemampuan dalam melakukan *penetration testing* aplikasi *website* terutama dalam pengujian celah keamanan *SQL Injection* menggunakan metode *fuzzing* (*fuzz testing*).
2. Bagi Instansi Pemilik *Website*
   a. Membantu mengidentifikasi celah keamanan *SQL Injection* pada *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh.
   b. Mencegah terjadinya penyerangan dan kebocoran data.
3. Bagi Universitas
   a. Kontribusi karya ilmiah pada bidang studi Teknik Informatika

b. Sumber referensi tambahan untuk penelitian pada bidang keamanan sistem di masa depan

4. Bagi Masyarakat Umum
   a. Menambah pengetahuan dan pemahaman mengenai keamanan sistem informasi
   b. Sumber referensi tambahan untuk penelitian pada bidang keamanan sistem di masa depan.

1.6 Sistematika Penulisan

Penelitian ini disusun dengan menggunakan lima bab yang terbagi ke dalam beberapa sub-bab serta dilengkapi dengan daftar pustaka yang disusun secara terperinci sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan pada penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi landasan teori dan penelitian sebelumnya yang terkait dengan penelitian ini.

BAB III METODE PENELITIAN

Bab ini membahas mengenai metode penelitian yang digunakan serta urutan tahapan yang dilakukan dalam proses penelitian

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai implementasi pengujian celah keamanan *SQL Injection* menggunakan metode *fuzzing* (*fuzz testing*) pada *website* sistem informasi pendaftaran ulang mahasiswa baru (PUMABA) Universitas Malikussaleh.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran berdasarkan hasil penelitian yang dilakukan dan dapat dijadikan referensi untuk penelitian selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN