BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi adalah cara yang efektif untuk menghasilkan dan memperoleh informasi, yaitu melalui teknologi komputer. Oleh karena itu, komputer sangat penting untuk manusia dan memiliki banyak manfaat. Karena informasi hanya diberikan kepada kelompok tertentu, keamanan sistem informasi sangat penting. Oleh karena itu, sangat penting untuk mencegah golongan yang tidak memiliki hak dalam kepentingan untuk menyalahgunakan hak mereka. Oleh karena itu, keamanan komputer diperlukan agar data tetap aman [1].

Data adalah aset terbesar setiap bisnis, dan setiap organisasi harus memastikan bahwa datanya dipelihara dengan baik. Karena itu, keamanan data adalah masalah utama dalam mengelola dan memelihara data bisnis. Intelijen bisnis bergantung pada data historis dan sekarang untuk memperkirakan dan melakukan perhitungan tentang data masa depan. Akibatnya, data bisnis dapat berada dalam bahaya [2].

Keamanan data mengacu pada langkah-langkah perlindungan privasi digital yang digunakan untuk melindungi komputer, *database*, dan situs *web* dari akses tidak sah [3]. Sangat penting untuk mendeteksi kerentanan keamanan aplikasi berbasis *web* karena ini dapat memperkirakan risiko yang ada terhadap keberlangsungan bisnis. Beberapa pelaku kejahatan dunia maya memanfaatkan pergeseran dari bisnis konvensional ke aplikasi berbasis *web* untuk mencuri data pribadi pengguna demi keuntungan pribadi [4].

Keamanan data juga mencegah korupsi data, yaitu kerusakan data komputer yang terjadi saat penulisan, pembacaan, penyimpanan, transmisi, atau pemrosesan. Organisasi dari berbagai jenis dan ukuran sangat memperhatikan keamanan data mereka. Keamanan data adalah istilah lain untuk keamanan informasi atau keamanan komputer. Contoh teknologi keamanan data termasuk enkripsi *disk* perangkat keras atau perangkat lunak, pencadangan, penyamaran, dan penghapusan data [3].

Dengan meningkatnya jumlah ancaman terhadap aplikasi *web* belakangan ini, deteksi kerentanan *web* menjadi komponen penting dalam keamanan siber. Terdapat beberapa cara untuk mendeteksi kerentanan suatu *web*, seperti mencari kerentanan secara manual dengan menelusuri semua halaman pada *web* dan melakukan *penetration testing* [5]. Pencarian kerentanan secara manual adalah proses mengidentifikasi celah keamanan dalam aplikasi *web* tanpa menggunakan alat otomatis, melainkan dengan memeriksa setiap halaman, parameter dan respons aplikasi satu per satu secara langsung. Praktik ini melibatkan pemahaman mendalam terhadap struktur aplikasi, mencoba berbagai jenis *input* berbahaya, serta mengevaluasi bagaimana aplikasi menangani data pengguna. Sementara itu, *penetration testing* atau *pen testing* adalah proses evaluasi keamanan yang aktif

dengan mensimulasikan serangan nyata untuk mengidentifikasi celah atau kelemahan dalam sistem, jaringan maupun aplikasi *web*. Proses ini melibatkan beberapa tahapan, seperti pengumpulan informasi (*intelligence gathering*), pemodelan ancaman (*threat modeling*), pengujian kerentanan (*vulnerability testing*), eksploitasi, hingga pelaporan hasil temuan. Metode ini bertujuan untuk memberikan gambaran nyata tentang seberapa rentan suatu sistem terhadap serangan dan membantu organisasi memperbaiki kelemahan sebelum dimanfaatkan oleh penyerang sebenarnya [6].

Tetapi ada cara yang lebih mudah yaitu dengan membuat pemindai otomatis. Pemindai otomatis adalah alat yang dibuat untuk menemukan masalah keamanan pada aplikasi *web* secara cepat dan menyeluruh. Pemindai otomatis dapat bekerja secara berkala, sehingga dapat segera memeriksa setiap perubahan atau pembaruan pada aplikasi *web*. Ini juga memungkinkan proses identifikasi kerentanan dilakukan dengan konsisten tanpa melewatkan detail kecil yang mungkin tidak terlihat pada analisis manual. Pemindai otomatis juga membantu tim keamanan menghemat waktu dan sumber daya dengan memberikan laporan terstruktur, yang memudahkan perbaikan masalah keamanan secara tepat dan cepat [7].

CyberArmyID adalah perusahaan yang bergerak di bidang Cyber Security, perusahaan ini sudah mengembangkan pemindai otomatis kerentanan *web* yaitu Helium Security yang berbasis pada bahasa pemrograman Java. Namun dalam pekerjaan ini, pemindai otomatis kerentanan *web* akan dialihkan menggunakan bahasa pemrograman Python, untuk memanfaatkan fleksibilitas bahasanya. Python memiliki kelebihan dalam hal penggunaan dan dukungan terhadap berbagai *library* khusus keamanan, Python juga lebih cepat dalam pengembangan karena sintaksisnya yang lebih sederhana, sehingga memungkinkan pengembang lebih efisien dalam menyesuaikan aplikasi untuk mendeteksi dan menangani ancaman keamanan terbaru.

Salah satu serangan umum yaitu SQL Injection sering terjadi akibat kelemahan dalam kode atau konfigurasi sistem. Dalam upaya mendeteksi kerentanan, bahasa pemrograman Python menyediakan beberapa *library* yang dapat membantu dalam pemindaian otomatis untuk menemukan celah keamanan pada aplikasi *web*. Saat magang di CyberArmyID, penulis melakukan pembuatan pemindai otomatis pada kerentanan *web* untuk beberapa jenis kerentanan, tetapi yang akan dibahas pada laporan ini hanya berfokus pada kerentanan SQL Injection pada *database* MySQL saja.

1.2 Rumusan Masalah dan Solusi

Berdasarkan latar belakang yang ada, maka rumusan permasalahan yang akan dibahas sebagai berikut:

1. Bagaimana melakukan implementasi pemindai otomatis dapat digunakan untuk mendeteksi kerentanan pada aplikasi *web*?
2. Bagaimana cara mendeteksi kerentanan SQL Injection pada *database* MySQL secara otomatis?

1.3 Tujuan

Berikut tujuan yang akan dilakukan dalam pembuatan pemindai otomatis, yaitu:

1. Mengembangkan pemindai otomatis berbasis Python yang dapat melakukan deteksi kerentanan *web* melibatkan *library* dari python seperti Python Requests dan BeautifulSoup untuk melakukan *scanning* pada web.
2. Dengan menggunakan Python, pemindai otomatis akan digunakan untuk menemukan kerentanan SQL Injection berbasis waktu (*time-based*) pada *database* MySQL.

1.4 Batasan Masalah

Batasan masalah pada pembuatan pemindai otomatis ini mencakup beberapa faktor yang perlu dipertimbangkan untuk memastikan aplikasi ini berfungsi secara optimal, antara lain:

1. Pemindai hanya akan fokus pada salah satu jenis kerentanan umum yang sering muncul pada aplikasi *web*, yaitu SQL Injection pada *database* MySQL.
2. Pemindai akan dibatasi pada aplikasi web yang menggunakan HTTP atau HTTPS sebagai protokol utama. Aplikasi *web* dengan fitur atau metode keamanan khusus, seperti firewall mungkin tidak dapat dipindai dengan tingkat akurasi yang tinggi.

1.5 Penjadwalan Kerja

Pelaksanaan magang di PT Global Inovasi Siber Indonesia (CyberArmyID) dilakukan secara *onsite*, dimulai dari hari Senin hingga Jumat, dengan jam kerja mulai pukul 09.00 hingga 17.00. Tabel 1.1 merupakan penjadwalan kerja selama kegiatan magang berlangsung.

Tabel 1.1 Tabel Penjadwalan Kerja

No.	Deskripsi Kerja	Bulan ke-										
		1	2	3	4	5	6	7	8	9	10	11
1	Mengerjakan *Scanner* bagian 1											
2	Mengerjakan *Scanner* bagian 2											
3	Mengerjakan *Scanner* bagian 3											
4	Mengerjakan *Scanner* bagian 4											
5	Membuat API untuk Scanner											
6	*Fixing* dan *Testing Scanner* bagian 1											
7	*Fixing* dan *Testing Scanner* bagian 2											
8	*Fixing* dan *Testing Scanner* bagian 3											
9	*Fixing* dan *Testing Scanner* bagian 4											