BAB I PENDAHULUAN

1.1 Latar Belakang

Website telah menjadi salah satu media utama dalam penyampaian informasi dan layanan secara digital. Dari sistem e-commerce, portal informasi, hingga layanan administrasi publik, *website* kini menjadi tulang punggung interaksi antara pengguna dan penyedia layanan di internet. Sebagai *platform* yang dapat diakses secara luas melalui internet, *website* menghadapi risiko yang signifikan terkait dengan keamanan informasi.

Keamanan informasi pada *website* berperan penting untuk melindungi data pengguna dan menjaga integritas sistem agar tidak mudah diserang oleh pihak yang tidak bertanggung jawab. Salah satu ancaman besar terhadap keamanan *website* adalah *vulnerability* atau kerentanan yang dapat dieksploitasi oleh penyerang [1]. Kerentanan ini biasanya berupa celah dalam sistem yang memungkinkan serangan untuk mendapatkan akses tidak sah, mengubah data, atau bahkan mengganggu kinerja *website* secara keseluruhan.

Vulnerability atau kerentanan adalah celah keamanan yang memungkinkan penyerang mendapatkan akses yang tidak sah atau mengganggu sistem [2]. Organisasi *Open Web Application Security Project* (OWASP) setiap tahun merilis daftar *OWASP Top Ten,* yaitu sepuluh jenis kerentanan keamanan paling kritis yang sering ditemui pada aplikasi *web*. Kerentanan ini yang meliputi *SQL Injection*, *Cross-Site Scripting (XSS)*, C*ross-Site Request Forgery (CSRF)*, dan *Broken Authentication*, menjadi target umum bagi penyerang [3].

Deteksi kerentanan biasanya dilakukan melalui pengujian penetrasi *(penetration testing)*, yaitu simulasi serangan untuk mengidentifikasi dan memperbaiki celah keamanan pada aplikasi [4]. Namun, pengujian penetrasi manual memerlukan keterampilan teknis yang tinggi serta waktu yang lama. Aplikasi ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan informasi di lingkungan *website* yang semakin rentan terhadap ancaman siber.

Helium Security merupakan salah satu *platform* yang memfasilitasi pengguna untuk melakukan pengujian dan pemindaian kerentanan. *Platform* ini memiliki misi untuk menyediakan *platform Security Testing* yang fleksibel dan mudah digunakan, dengan tujuan memberdayakan pengguna dalam mitigasi risiko keamanan di berbagai jenis aplikasi.

Helium Security dirancang dengan antarmuka yang ramah pengguna, sehingga memudahkan pengguna untuk menjalankan proses pengujian dan pemindaian kerentanan secara efisien, tanpa memerlukan keahlian teknis yang kompleks.

1.2 Rumusan Masalah dan Solusi

Berdasarkan latar belakang yang di atas, maka rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana cara untuk mengetahui adanya celah keamanan yang dapat membahayakan data atau sistem pada aplikasi *web*?
2. *Library* atau pustaka Python apa saja yang digunakan oleh CA-Scanner dalam proses pengumpulan data untuk identifikasi pola kerentanan pada *website*?
3. Apa tindakan yang tepat ketika celah keamanan muncul dalam proses pengembangan aplikasi *web*?

Dari permasalahan-permasalahan tersebut, muncul kebutuhan untuk sebuah sistem otomatis yang dapat mengidentifikasi keamanan *website*, Beberapa solusi dari masalah tersebut:

1. Melakukan pengujian penetrasi yang dilakukan secara manual untuk mencari dan mendeteksi kerentanan yang berpotensi membahayakan data atau sistem.
2. Dengan memanfaatkan *library* Python seperti *requests* dan *BeautifulSoup*, aplikasi ini dapat mengumpulkan data yang dapat digunakan untuk mendeteksi indikasi kerentanan.
3. Melakukan identifikasi dan analisis terhadap celah yang ditemukan, diikuti dengan perbaikan kode serta pengujian ulang secara menyeluruh.

1.3 Tujuan

Berdasarkan rumusan masalah yang ada, tujuan yang akan dicapai adalah:

1. Mengembangkan engine CA-Scanner berbasis Python untuk deteksi otomatis kerentanan keamanan pada *website*.
2. Mengimplementasikan pustaka Python untuk membantu dalam mengumpulkan data dari *website* yang diuji.
3. Menciptakan solusi deteksi kerentanan *website* yang informatif dan mendukung perbaikan keamanan.

1.4 Batasan masalah

Batasan masalah dalam pengembangan aplikasi ini adalah:

1. Hasil deteksi memiliki peluang untuk menghasilkan *false positives* (peringatan palsu) dan *false negatives* (ketidakdeteksian kerentanan yang sebenarnya), yang dapat memengaruhi keakuratan hasil pengujian.
2. Aplikasi ini dirancang khusus untuk mendeteksi kerentanan pada aplikasi *web* dan tidak dapat digunakan untuk pengujian aplikasi *desktop* atau *mobile*.
3. Aplikasi hanya diperbolehkan untuk menguji aplikasi *web* yang telah mendapatkan izin dari pemilik aplikasi *web* tersebut.
4. Aplikasi hanya mencakup salah satu kerentanan yang paling umum, yaitu *Path Traversal*.

1.5 Penjadwalan Kerja

Berikut adalah penjadwalan kerja selama menjalankan Magang Dua Semester di PT Global Inovasi Siber Indonesia (CyberArmyID) dalam skala mingguan, dapat dilihat pada *Tabel 1.1*, *1.2*, dan *1.3*.

Tabel 1.1 Tabel Penjadwalan kerja semester Ganjil 1

No	Deskripsi Kerja	Juli				Agustus				September				Oktober			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Diskusi perancangan aplikasi SMKI																
2	Implementasi aplikasi SMKI																
3	Riset untuk pengembangan aplikasi																
4	Implementasi dan pengujian aplikasi pemindai kerentanan tahap 1																
5	Implementasi dan pengujian aplikasi pemindai kerentanan tahap 2																
6	Perancangan skema *database* untuk aplikasi CyberQuiz																
7	Implementasi aplikasi CyberQuiz tahap 1																

Tabel 1.2 Tabel Penjadwalan kerja semester Ganjil 2

No.	Deskripsi kerja	November				Desember			
		1	2	3	4	1	2	3	4
8	Implementasi aplikasi CyberQuiz tahap 2								
9	Implementasi aplikasi CyberQuiz tahap 3								

Tabel 1.3 Tabel Penjadwalan kerja semester genap

No.	Deskripsi Kerja	Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
10	Implementasi aplikasi CyberQuiz tahap 4																
11	Implementasi dan pengujian aplikasi pemindai kerentanan tahap 3																
12	Implementasi dan pengujian aplikasi pemindai kerentanan tahap 4																