BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Salah satu artikel keamanan yang dipublikasikan oleh Badan Siber dan Sandi Negara Republik Indonesia adalah daftar kerentanan atau Common Vulnerability and Exposures. Beberapa contoh artikel yang menginformasikan Common Vulnerability Exposures pada suatu software adalah :

a. CVE-2021-44228 (Kerentanan Zero-Day pada Apache Java Logging Library Log4J)

   Pada tanggal 9 Desember 2021, periset keamanan menemukan adanya kerentanan zero-day yang diberi nama CVE-2021-44228 pada pustaka Apache Java Logging Library atau yang umum dikenal dengan log4j [19].

b. CVE-2021-44228 (Kerentanan Remote Code Execution CVE-2021-44530)

   Perusahaan pengembang teknologi informasi dan komunikasi Uniquiti mengumumkan kerentanan remote code execution (RCE) yang berdampak pada salah satu produk Uniquiti, UniFi Network Application [18].

c. CVE-2021-23008: Kerentanan Otentikasi pada BIG-IP Access Policy Manager Active Directory

   F5 mempublikasikan imbauan keamanan mengenai kerentanan otentikasi pada BIG-IP Access Policy Manager Active Directory yang merujuk pada CVE-2021-23008. Kerentanan bypass pada fitur keamanan Key Distribution Center (KDC) berdampak pada layanan pengiriman pada aplikasi F5 BIG-IP [20].

Common Vulnerability and Exposures ID atau CVE ID bisa didapat melalui hasil atau value scan *tools* penetration testing. Namun saat ini informasi CVE ID yang terdapat di beberapa tools atau sumber CVE tidak menampilkan informasi secara detail. Untuk itu perlu ada *tools* yang dapat menampilkan detail mengenai CVE yang mudah di pahami sehingga dapat mempermudah user

maupun tester untuk melakukan antisipasi atau penutupan kerentanan yang kemungkinan akan dimanfaatkan oleh peretas untuk mengeksploitasi sistem.

Dengan permasalahan tersebut, dilakukanlah penelitian ini untuk membuat suatu *tools* sederhana yang dapat membantu dan menghasilkan informasi secara detail mengenai CVE berdasarkan CVE ID yang di inputkan ke *tools*/aplikasi tersebut. Sehingga informasi yang dihasilkan dapat dimengerti dan dipahami oleh user yang sudah profesional maupun yang baru mempelajari dunia cyber security terutama untuk keamanan suatu website.

1.2 Rumusan Masalah

Bagaimana mengembangkan tools untuk menguraikan detail informasi dari CVE ID yang dihasilkan dari tools penetration testing ?

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

a. Tools ini menggunakan bahasa pemrograman Python dan framework FastAPI
b. Database tool atau aplikasi menggunakan sqlite3
c. Data yang diambil bersumber dari https://cve.circl.lu/

1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam penelitian ini adalah "Menyajikan informasi secara detail Common Vulnerability Exposures dari hasil *tools* penetrasi testing".

1.5 Sistematika Penulisan

Bab I Pendahuluan, berisi: latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, berisi: hasil penelitian sejenis yang sudah pernah dilakukan sebelumnya, teori penunjang, dan referensi berupa buku, jurnal, dan laporan skripsi/tesis.

Bab III Metodologi Penelitian, berisi: penjelasan mengenai metode penelitian yang digunakan untuk memahami dan mengeksplorasi objek penelitian, hasil observasi / pengumpulan data, masalah yang terdapat pada objek, dan gambaran umum proyek atau obyek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: rancangan proyek, implementasi coding dan desain, serta evaluasi rancangan. Selanjutnya alur pengerjaan proyek, metode testing, hingga hasil akhir penelitian dan pembahasan analisis hasil akhir penelitian, termasuk pembahasan hasil-hasil uji coba (testing). Data hasil akhir pengujian dapat berupa grafik, tabel, data monitoring, log system, dan lain-lain, dengan pembahasan.

Bab V Penutup, berisi kesimpulan dari hasil akhir penilaian proyek, dan saran.