BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Internet sebagai jaringan komunikasi global dapat dijadikan sebagai media dan sumber informasi terkini, seperti ilmu pengetahuan, teknologi, hiburan, bisnis, dan sumber informasi lainnya. Kemudahan serta kenyamanan seperti ini menyebabkan internet selalu digunakan dan dibutuhkan. Namun dibalik kemudahan dan kenyamanan yang diberikan, ternyata terdapat salah satu aspek yang saat ini masih kurang diperhatikan oleh pengguna internet, yaitu *security. Security* merupakan salah satu aspek penting pada *media* yang menghubungkan pengguna dengan internet.

Teknologi tidak dapat dipungkiri lagi bahwasannya dapat membawa dampak negatif yang tidak sedikit. Perkembangan internet membuat kejahatan yang sebelumnya bersifat konvensional seperti ancaman, pencurian, penggelapan, pemalsuan dan penipuan kini dapat dilakukan secara daring melalui media internet yang memiliki keuntungan berupa minimnya resiko tertangkat oleh individu maupun kelompok .

Dampak negatif yang merugikan dan berkembang secara pesat tersebut, menghasilkan suatu pemikiran bahwa tidak ada komputer dan jaringan yang benar-benar aman hingga saat ini. Hal ini terbukti dari banyaknya *hacker-hacker* pemula yang berseliweran muncul di berbagai platform internet untuk melakukan tindak kriminal dunia maya.

Seiring berkembang pesatnya teknologi dari waktu ke waktu, banyak *hacker-hacker* muda bermunculan untuk melakukan kejahatan dengan berbagai macam metode-metode serangan baru yang mereka gunakan untuk malancarkan aksinya, seperti *SQL Injection, Directory Traversal Attack, Cross Site Scripting* dan lain sebagainya. *SQL Injection* merupakan salah satu contoh metode paling

berbahaya ketika berhasil dimanfaatkan dengan baik oleh *hacker* atau *cracker*.

SQL Injection sudah populer sejak lama dalam dunia per-*hacking*an sebagai salah satu teknik *web application hacking*, walaupun teknik ini sudah terbilang lama akan tetapi teknik ini masih menjadi salah satu teknik andalan karena sifatnya yang dapat merusak database dari suatu situs. Salah satu metode dalam teknik *SQL Injection* adalah dengan melakukan penginputan perintah-perintah standar dalam *SQL* seperti *insert, create, update, union, select, view*, beserta perintah standar lainnya yang tak asing lagi bagi yang sudah mempelajari *SQL* secara mendalam maupun yang baru belajar.

SQL Injection adalah suatu metode penyerangan terhadap kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language (SQL) Query* yang melewati suatu aplikasi ke database *back-end* yang mampu memanipulasi apa yang akan diteruskan ke database. Penyerang memanfaatkan sintaks dan kemampuan dari *SQL* itu sendiri, serta kekuatan dan fleksibilitasnya untuk mendukung operasi dan fungsionalitas sistem yang tersedia ke database. *SQL Injection* tersebut diakibatkan oleh tidak adanya filter terhadap bahasa *SQL* sehingga penyerang dapat memanfaatkan kerentanan tersebut dengan tujuan meraih akses pada sistem database yang berbasis *SQL* dan menyusup ke dalamnya.

Penelitian ini melakukan uji coba pencarian celah keamanan SQL Injection terhadap 5 website diantaranya ialah uad.ac.id, codelatte.id, pt-jayapura.go.id, mk.mercubuana-yogya.ac.id, jateng.polri.go.id. Dari kelima website tersebut tiga diantaranya ditemukan celah keamanan SQL Injection di dalamnya, ketiga website tersebut ialah codelatte.id, pt-jayapura.go.id, mk.mercubuana-yogya.ac.id, dan pt-jayapura.go.id. Namun izin pemerbaikan hanya dikirimkan ke website codelatte.id serta pt-jayapura.go.id, dan website codelatte.id lah yang mengizinkan

pemerbaikan di dalam websitenya, oleh karena itu website codelatte.id terpilih menjadi objek pada penelitian ini.

Codelatte merupakan sebuah organisasi yang berfokus dalam jasa pengembangan web (*web developer*) dan pengujian penetrasi (*penetration testing)*. *Codelatte* memiliki *website* sebagai sarana periklanan, pembrandingan, dan peningkatan eksistensi. *Website* tersebut menjadi sasaran menggunakan protokol yang bertugas untuk mengirimkan data dari *web server* ke browser menggunakan HTTPS (*Hypertext Transfer Protocol Secure*) pada tiap tiap sub domainnya. Setelah melakukan *Lookup* diketahui bahwa pada *website* tersebut menggunakan PHP dan Wordpress sebagai *Content Management Sistemnya* (CMS)nya.

Wordpress merupakan CMS (*Content Management System*) dengan pengguna paling banyak saat ini dalam pengembangan situs *website*. Kemudahan dan sistem keamanan yang diberikan *Wordpress* selaku penyedia layanan sangat memuaskan penggunanya, sehingga mayoritas penggunanya enggan berpaling ke CMS lainnya.

Penerapan *Wordpress* berbanding terbalik dengan penerapan HTTPS, penggunaan *Wordpress* tidak diterapkan pada tiap-tiap subdomain yang dimiliki oleh *website Codelatte*. Sisa file *website* lama yang berada dalam file manager menyebabkan ditemukannya celah pada subdomain lainnya dari *website* tersebut, contohnya saja setelah melakukan *crawling* dan *scanning* yang berfungsi untuk menemukan celah keamanan apa saja yang terdapat di dalam situs *web*, ditemukan bahwa terdapat celah *SQL Injection* terbuka pada *sub-domain web Codelatte*.

Crawling tidak hanya mengakibatkan tereksposenya suatu kelemahan situs *website*, *crawling* juga dapat dimanfaatkan oleh *pentester* untuk mencari letak kelemahan dan memperbaikinya sehingga tingkat keamanan dari suatu *website* meningkat, *tools acunetix* memiliki *engine* untuk melakukan *crawling* manual jika pengguna tidak ingin menggunakan automatic testing

pada *acunetix web vulnerability scanner*, *tools* ini sangat berguna bagi kedua pihak, baik dari sisi penyerang maupun pentester guna menemukan kelemahan-kelemahan situs untuk menyusup kedalam sistem ataupun memperbaikinya.

Dirsearch merupakan alat yang mengandalkan metode *bruteforce* dan pengecekan http respond code pada folder yang sering digunakan pada website dalam proses *crawling*nya. Dengan memanfaatkan tools *dirsearch* ini seseorang dapat dengan mudah Mengetahui *path directory*, Mencari data sensitif, Mencari *hidden directory*, dan lain sebagainya.

Penyerang yang berhasil menemukan dan memanfaatkan celah *SQL Injection* pada sub-domain situs tersebut dan jika telah berhasil mencuri akses masuk ke dalam *database*, maka penyerang akan memiliki keleluasaan untuk memanipulasi data-data yang terdapat didalam *website*. Tidak berhenti di situ saja, penyerang juga mampu melakukan *jumping* antar sub-domain bahkan hingga domain utama untuk memasang backdoor yang mengakibatkan penyerang mampu mendapatkan akses penuh dari dalam domain tersebut.

Hal-hal tidak bertanggung jawab yang mampu dilakukan oleh penyerang dari dalam database *website* tentu dapat menimbulkan resiko bocornya *Confidentiality* organisasi, berkurangnya *integrity* dari informasi dan *availability* data ketika dibutuhkan menjadi tidak pasti.

Serangan *SQL Injection* merupakan metode penyerangan dengan dampak yang sangat berbahaya serta dapat dilakukan dari jarak jauh oleh pihak-pihak tidak bertanggung jawab dan memperbaikinya dapat membantu menjaga privasi *website Codelatte*, maka penulis memutuskan untuk mengambil tema ini dengan menggunakan judul "**ANALISIS CELAH KEAMANAN *WEBSITE* MENGGUNAKAN METODE CRAWLING TERHADAP SERANGAN SQL INJECTION"**

1.2. Identifikasi Masalah

Latar belakang yang telah diuraikan diatas menghasilkan identifikasikan masalah untuk dijadikan bahan penelitian yaitu terdapat banyak metode penyerangan yang dapat dimanfaatkan oleh penyerang untuk melakukan tindak kriminal di dunia maya. Salah satu metode penyerangan yang melihat bahasa *SQL* tanpa penyaring pada *website* sebagai suatu kerentanan ialah *SQL Injection*.

Website milik *Codelatte* memiliki kelemahan tersebut sehingga memungkinkan munculnya resiko-resiko kerusakan *website*, kehilangan data-data di dalam *website* dan terubahnya data-data di dalamnya ketika pihak yang tidak bertanggung jawab memanfaatkan kelemahan tersebut.

1.3. Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan, maka dapat dapat dibuat rumusan masalah sebagai berikut :

1. Bagaimana cara melakukan *crawling* dan mengetahui letak kerentanan dari hasil *crawling* yang telah dilakukan pada *website Codelatte* ?
2. Bagaimana cara mengatasi dan memperbaiki kerusakan yang terjadi akibat kerentanan *SQL Injection* yang terdapat pada *website Codelatte* ?
3. Bagaimana pencegahan serta rekomendasi terhadap serangan *SQL Injection* ?

1.4. Tujuan Penelitian

Tujuan diadakannya penelitian ini yaitu untuk :

1. Mengetahui tingkat keamanan *website* melalui *crawling* menggunakan *crawling engine tools acunetix* pada *website Codelatte*

2. Mengetahui cara mengatasi dan memperbaiki kerusakan yang terjadi akibat kerentanan *SQL Injection* yang ada pada *website Codelatte*
3. Mengetahui cara pencegahan terhadap kelemahan-kelemahan terbuka yang ada di dalam *website Codelatte*

1.5. Lingkup Penelitian

Supaya penyusunan tugas akhir ini tidak keluar dari pokok permasalahan yang dirumuskan, maka ruang lingkup lingkungan penelitian ini adalah :

1. Analisa kerentanan yang dilakukan hanyalah pada *website Codelatte* beserta *sub-domainnya* jika dibutuhkan
2. Metode *crawling* menggunakan *tools acunetix vulnerability scanner*
3. Metode penyerangan yang digunakan adalah metode *SQL Injection*
4. Media yang digunakan untuk mengambil data ialah *website Codelatte*
5. Pengamanan dari *SQL Injection* yang akan dilakukan pada *website* menggunakan *PHP Data Object* (PDO) dan *Filtering Character* berbahaya serta memasang *tools mod security* jika diperlukan
6. Perbaikan (*patching*) terhadap *SQL Injection* dapat menggunakan *function* bawaan.

1.6. Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Bermanfaat sebagai acuan dalam perbaikan, pengamanan, analisa kerentanan bagi *website* yang digunakan sebagai objek penelitian maupun *website* umum lainnya dengan permasalahan kerentanan yang sama

2. Menambah referensi bagi penelitian selanjutnya.