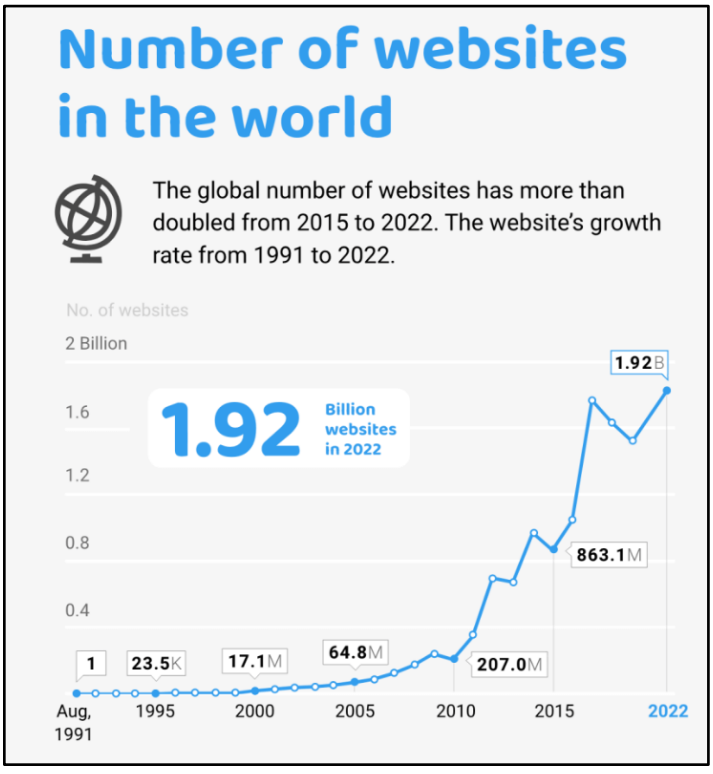
BAB 1

PENDAHULUAN

1.1 Latar Belakang

Website merupakan salah satu media yang menampilkan berbagai informasi penting dan menarik dikarenakan mudah bagi siapapun untuk mengaksesnya serta kapanpun dapat digunakan sesuai kebutuhan selama terhubung ke internet. Namun dengan adanya *website* yang mudah diakses, hal ini dapat menjadi pemicu bagi orang yang tidak bertanggung jawab melakukan *cyber crime* terhadap celah keamanan *website*. Sehingga *website* menjadi target oleh orang yang tidak bertangggung jawab untuk mengambil keuntungan secara pribadi dengan mencoba meretas *website* yang berisi informasi sensitif dari penggunanya dan menyembunyikan identitasnya agar tidak mampu diketahui oleh siapapun.



Gambar 1.1 Grafik pertumbuhan website

Sumber: (Benefita, 2023)

Seperti yang ditunjukkan pada gambar 1.1 diatas, dapat dilihat peningkatan pada pertumbuhan *website* dan menurut hasil eksperimen dari *Accenture* bahwa serangan *cyber crime* telah meningkat sebesar 67% selama lima tahun terakhir. Jadi kemungkinan besar akan ada lebih banyak ancaman *cyber crime* pada *website* (Benefita, 2023).

Bertahun-tahun tindakan ilegal peretasan *website* yang dilakukan oleh orang yang tidak bertanggung jawab terhadap pencurian informasi sensitif mengalami peningkatan yang signifikan. Dengan peningkatan yang signifikan, banyak kasus bahwa masyarakat menjadi korban praktik tindakan *cyber crime* yang memanfaatkan kesempatan ketika melakukan aktivitas sehari-hari menggunakan *website*. Bagi setiap orang yang mencoba untuk menyimpan informasi pribadi melalui *website* sering kali menjadi target oleh orang yang tidak bertanggung jawab dengan melakukan berbagai macam cara penyerangan, salah satu serangan yang paling banyak dilakukan yaitu *SQL Injection*.

SQL Injection merupakan salah satu serangan yang sangat populer dalam mengeksploitasi celah keamanan *website* dari sisi database. Serangan tersebut mampu mengeksploitasi celah keamanan dengan melalui *form login* ataupun *URL address* yang terdapat pada *website* oleh orang yang tidak bertanggung jawab dengan cara memodifikasi dan menginjeksikan perintah *SQL* yang berbahaya. Sehingga, perintah *SQL* yang telah terinjeksi akan berpotensi masuk dan dieksekusi agar mengirimkan baris perintah ke dalam lapisan *database website* yang dikembangkan oleh *web developer*.

Tanpa disadari oleh *web developer* saat mengembangkan *website* yang jarang memperhatikan sisi keamanan *website* dan telah digunakan oleh banyak orang. Hal ini akan memunculkan celah keamanan pada *database website*, dengan begitu orang yang tidak bertanggung jawab dapat dengan mudah melakukan serangan *SQL Injection.* Akibatnya data penting mampu diakses dan korban akan merasa rugi setelah datanya diambil, diubah dan dihapus dalam *database*, karena telah menggunakan *website* yang belum menerapkan standar keamanan untuk melindungi *database website* dari serangan *SQL Injection*.

Website yang telah dikembangkan, namun belum diterapkan standar keamanannya oleh *web developer* akan sangat berbahaya bagi penggunanya dikarenakan rentan terhadap serangan dari luar. Oleh karena itu, pengguna akan merasa tidak aman terkait data informasinya. Untuk meminimalisir terjadinya hal yang tidak diinginkan oleh pengguna *website* agar merasa aman, maka perlunya melakukan pengujian secara dini dengan cara *penetration testing* menggunakan serangan *SQL Injection* untuk mengetahui celah keamanan yang terdapat pada *database website* dan sebagai bahan evaluasi untuk memperbaiki *website* sehingga dapat terhindar dari aksi *cyber crime* oleh orang yang tidak bertanggung jawab.

Berdasarkan penjelasan yang telah diuraikan, maka penelitian tentang pengujian terhadap celah keamanan yang ditemukan pada *database website* dengan melakukan *penetration testing* menggunakan serangan *SQL Injection* dan memperbaiki celah keamanan yang ditemukan pada website perlu dilakukan. Sehingga dengan melakukan penelitian ini, diharapkan dapat menambah ilmu bagi siapa pun dan dijadikan referensi sebagai acuan dalam mengembangkan *website* dengan memperhatikan keamanan *website* jika terdapat celah keamanan yang ditemukan agar segera melakukan perbaikan *website* sebelum aksi *cyber crime* dari pihak luar yang tidak bertanggung jawab dapat dengan mudah merugikan orang lain.

1.2 Rumusan Masalah

Website yang rentan akan sangat berbahaya jika penggunanya menyimpan informasi penting terkait data pribadi ketika terjadi serangan *SQL Injection*. Oleh karena itu, perlunya diuji keamanan *website* dengan cara melakukan *penetration testing* menggunakan serangan *SQL Injection* dan memberikan solusi berdasarkan hasil pengujian untuk menutupi celah keamanan dalam *database website*.

1.3 Tujuan

Penelitian ini dilakukan dengan tujuan untuk mengetahui kerentanan dalam pengujiannya yang dilakukan dengan *penetration testing* terhadap celah keamanan pada *database website* dan menganalisis hasilnya terhadap serangan *SQL Injection*.

1.4 Batasan Masalah

Dalam melakukan penelitian ini, batasan masalah digunakan sebagai ruang lingkup agar mampu mengarahkan dan memfokuskan penelitian. Batasan masalah dalam penelitian ini adalah:

1. Melakukan *penetration testing* terhadap *database website*.
2. Menggunakan serangan *SQL Injection* dengan *tools* SQLMap.