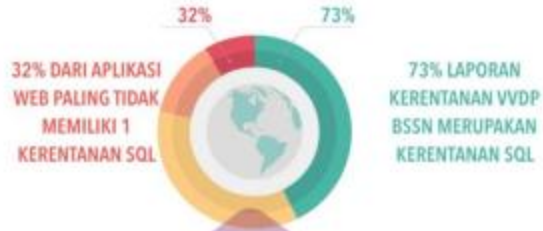
BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi beberapa tahun terakhir ini semakin pesat, dengan perkembangan ini pekerjaan dan segala aktifitas seperti mengakses berita dan informasi menjadi semakin mudah, salah satu media yang sering digunakan yaitu website. Seiring dengan berkembanganya zaman website menjadi popular dikalangan masyarakat, dari banyaknya website yang ada saat ini sering dijadikan sasaran serangan oleh *hacker* seperti pencurian, manipulasi data atau informasi penting yang dapat salahgunakan oleh *hacker* [1].

Masalah utama pada *website* SMKN 1 Pangandaran adalah celah *SQL Injection* yang terdapat pada *subdomain* cbt.smkn1pangandaran.sch.id dimana pada celah tersebut memungkinkan seseorang untuk masuk kedalam *website* secara illegal. Celah yang didapatkan merupakan hasil dari proses analisis dari OWASP, dimana hasil yang didapatkan menunjukan kerentanan pada *subdomain* cbt.smkn1pangandaran.sch.id. selain menunjukan kerentanan pada bagian *subdomain* OWASP juga memberikan rekomendasi cara menutup celah yang ada sesuai standar yang digunakan dalam membuat website.

Ada beberapa jenis serangan website seperti *Malware, Cross Site Scripting,* dan *SQL Injection.* Salah satu jenis serangan yang paling popular saat ini yaitu *SQL Injection*[2]. Berdasarkan laporan kerentanan Badan Siber Dan Sandi Negara (BSSN) dari program *Voluntary Vulnerability Disclosure Program* (VVDP), pada bulan Januari s.d April 2019, 73% merupakan kerentanan *SQL Injection.* Meskipun serangan *SQL Injection* mudah untuk di cegah namun serangan *SQL Injection* merupakan serangan yang paling sering ditemukan di berbagai organisasi[3].



Gambar 1.1 Data Rekapitilasi VVDP BSSN (sumber BSSN)

Serangan *SQL Injection* merupakan Teknik serangan yang dapat mempengaruhi *Structured Query Language (SQL)* sebagaimana *attacker* dapat memanfaatkan sintaks *SQL* dengan cara menginjeksi sebuah kode yang memanfaatkan sebuah celah keamaan database untuk bypass login, merusak dan memanipulasi data[4]. Menurut *Open Web Application Security Project (OWASP) SQL Injection* merupakan Teknik serangan yang dilakukan untuk menerobos ke dalam suatu website dengan illegal, *SQL Injection* dapat mengirimkan sebuah perintah-perintah *SQL* seperti *create, insert, update, drop, alter, union dan select* yang nantinya dapat di eksekusi oleh web server. Dari informasi diatas *SQL Injection* termasuk kedalam TOP 10 serangan risiko keamanan aplikasi versi OWASP[5]

Pada latar belakang yang sudah dipaparkan diatas maka penelitian ini adalah melakukan analisis keamanan dari website instansi sekolah SMKN 1 Pangandaran dimana dengan menggunakan tools OWASP *(Open Web Application Security Project)* yang dimana nantinya dilakukan sebuah pengujian terhadap website SMK N 1 Pangandaran yang terdapat celah keaman *SQL Injection*. Untuk hasil dari penelitian ini penulis berharap setelah di lakukan analisis terhadap SMK N 1 Pangandaran dapat menjadi referensi untuk menambah fitur keamanan website guna tergaja kerahasiaan dan keamanan data-data penting yang ada.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang sudah dijelaskan sebelumnya, maka rumusan masalah dari penelitian ini adalah bagaimana cara menganalisis, menguji dan rekomendasi celah *SQL Injection* pada website SMK N 1 Pangandaran terkait serangan *SQL Injection* ?

1.3 Batasan Masalah

Untuk mengerucutkan permasalahan dan supaya tidak menyimpang pembahasannya, penulis membuat Batasan-batasan masalah sebagai berikut :

a. Penelitian ini membahas serangan *SQL Injection* .
b. Menggunakan *tools sudomy v.1.2.0* untuk melakukan *scanning sub-domain.*
c. Menggunakan tools ZAP v.2.10.0 untuk *scanning vulnerability.*
d. Menggunakan *sqlmap* untuk medapatkan data dari database website SMK N 1 Pangandaran.
e. Menggunakan *XAMP Control Panel v.3.3.0* untuk simulasi rekomendasi penutupan celah *SQL Injection.*

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah:

a. Menganalisis celah keamanan dari *website* SMK N 1 Pangandaran.
b. Melakukan pengujian terhadap celah keamanan dari *website* SMK N 1 Pangandaran.
c. Memberikan rekomendasi keamanan untuk menutup celah keamanan dari Website SMK N 1 Pangandaran

1.5 Manfaat Penelitian

Adapun manfaat penelitian ini bagi penulis adalah:

a. Dapat meningkatkan kemampuan dalam hal mengamankan website
b. Menambah pengalaman untuk penulis
c. Menambah wawasan terkait kelemahan website yang ada

Adapun manfaat penelitian ini bagi organisai adalah:

a. Mengedukasi bagi organisasi terkait tindak kejahatan kerentanan pada website.
b. Memberikan informasi terkait celah SQL Injection dari subdomain cbt.smkn1pangandaran.sch,id
c. memberikan rekomendasi celah yang ada dengan standar OWASP yang digunakan .

1.6 Sistematika Penulisan

Sistematika penulisan dalam laporan skripsi ini untuk mempermudah isi sebagaimana skripsi dapat dipahami dalam garis besarr. Adapaun penulisannya sebagai berikut:

Bab I Pendahuluan, bab ini menjelaskan tentang latar belakang, rumusan masalah dan hipotesis, batasan masalah, tujuan penelitian, dan sistematika penulisan.

Bab II Landasan Teori, bab ini menjelaskan mengenai 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 mengexplorasi obyek penelitian, hasil observasi, masalah yang terdapat pada obyek, dan gambaran umum proyek atau obyek penelitian, hingga Rencana Alur Penelitian.

Bab IV Pembahasan, berisi: proses reconnaissance, proses scanning, proses pengujian system pad website, dan pencegahan terhadap serangan SQL Injection

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