Keamanan aplikasi berbasis web dan sql injection

Oleh: Benfano Soewito

Setelah internet dikenal oleh sebagian besar pengguna, maka transfer data, pengiriman informasi, dan cara berbisnis telah berubah. Hampir semua kegiatan kita sehari hari tidak terlepas dari internet. Seiring dengan banyaknya applikasi di internet, maka bertambah pula pengguna internet. Aplikasi aplikasi yang menggunakan internet ini, semua bertujuan untuk lebih mempermudah semua kegiatan kita, baik itu untuk pendidikan, kegiatan bisnis, social, dan sebagainya. Oleh karena itu data atau informasi yang dulunya disimpan dalam media kertas atau media lainnya, sekarang data dan informasi tersebut lebih banyak disimpan dalam bentuk digital. Tujuannya adalah agar mudah dikirim melalui internet. Tetapi seiring dengan banyaknya aplikasi, pengguna internet, dan data digital, maka makin banyak juga celah celah yang terbuka bagi orang orang yang ingin berbuat jahat. Oleh karena itu faktor keamanan menjadi suatu hal yang serius dalam semua applikasi yang ada di internet, terutama aplikasi aplikasi yang berhubungan dengan keuangan yang berbasis web.

Kejahatan dunia maya yang paling sering terjadi adalah kejahatan terhadap pencurian data atau informasi dari data server melalui aplikasi berbasis web. Contohnya adalah pencurian user name dan password, nomor kartu kredit, dan merusak data base server dengan serangan denial of service. Selain itu juga ada gangguan lainnya yang harus dipikirkan, yaitu: virus, trojan dan worm. Oleh karena itu membangun system keamanan website dan database server adalah hal yang sangat penting, agar resiko yang terjadi karena serangan terhadapap server kita menjadi sangat minim atau bahkan dicegah jika berniat menyerang website kita. Ada beberapa faktor yang perlu diperhatikan untuk mencegah serangan melalui web yaitu, faktor perangkat keras, sistem operasi, aplikasi berbasis web, dan physical tempat penyimpanan server.

Dalam hal perangkat keras yang dimaksud disini adalah server beserta perlatan keamanannya seperti router, switch dan intrusion detection system. Untuk penyediaaan perangkat keras tergantung dari jenis perusahaannya. Untuk perusahaan menengah kebawah biasanya mereka tidak mengurus server dan keamanannya sendiri, tetapi mereka menyewa atau hosting di pihak ketiga. Jika website kita dititipkan di suatu perusahaan jasa hosting, maka tanggung jawab untuk server dan keamanannya ini adalah menjadi tanggung jawab dari admin sistem perusahaan jasa hosting. Dan kita wajib untuk mengetahui apakah hosting tempat website

kita berada tersebut cukup terpercaya keamanannya dan teknik keamanan apa saja yang ada pada jasa hosting tersebut. Kalau kita mempunyai server sendiri maka server dan sistem keamanannya adalah tanggung jawab kita sepenuhnya. Dalam ada beberapa hal yang perlu diperhatikan yaitu:

1. Sistem back up. Pastikan sistem back up berjalan sesuai dengan aturan.
2. Umur server dan peralatan sistem keamannannya tidak lebih dari 5 tahun.
3. Pada server harus di lakukan beberapa setting:
    a. Aktifkan firewall
    b. Aktifkan intrusion detection system
    c. Aktifkan socket secure layer
    d. Non aktifkan telnet ganti ssh
    e. Ganti nama administrator

Sistem operasi sangat berperan penting dalam hal kemanan, karena banyak vulnerability terdapat dalam sistem operasi. Untuk mencegah serangan terhadap sistem operasi seharusnya kita selalu menambahkan patch atau update sistem operasi secara otomatis.

Pada keamanan aplikasi yang harus diperhatikan adalah saat sebelum menginstal dan sesudah di install. Sebelum menginstal pastikan bahwa kita sudah mengetahui bug atau vulnerability aplikasi yang akan kita gunakan. Setelah diinstal download patch dan update aplikasi tersebut. Kemudian hapus file installation dan foldernya. Jika ada user administrator, ganti dengan nama lain. Setiap aplikasi berbasis web harus di test dari segi keamanannya, yaitu harus bebas dari HTML injection, cross site scripting, SQL injection, dan data store manipulation. Selain itu sistem autentikasi dan otorisasi harus memenuhi kriteria kriteria tertentu seperti panjang password minimal 8 karakter terdiri dari alpha numeric, huruf besar, huruf kecil dan symbol khusus (special karakter), serta harus diganti secara berkala.

Tempat penyimpanan server atau keamanan fisik juga menjadi hal yang penting. Akses fisik ke ruang server harus dibatasi atau dibuatkan policynya. Server harus ditempatkan di area yang bebas banjir, tahan terhadap gempa dan kebakaran. Sistim keamanan ruang server harus diperlakukan seketat mungkin termasuk semua kunci pintu untuk akses ke ruang server. Setiap orang yang masuk ke ruang server harus ada log book nya dan juga CCTV.

Berikut adalah contoh yang paling sederhana untuk SQL injection yang dapat di ketikan pada kolom user name dan password: ' or '1'='1'. Bentuk injeksi SQL ini terjadi ketika kita tidak melakukan aturan dalam menggunakan user name dan password sehingga setiap jenis karakter akan diteruskan untuk di proses. Sehingga injeksi yang berupa SQL code dapat di proses oleh server sebagai bagian dari code SQL. Selain untuk melewati proses autentikasi, SQL injection ini juga dapat digunakan untuk memanipulasi laporan atau data oleh pengguna aplikasi. Didalam SQL, code untuk memproses user name dan password adalah sebagai berikut:

```
statement = "SELECT * FROM users WHERE name ='" + userName + "';"
```

Kode SQL ini dirancang untuk mendapatkan username tertentu dari tabel pengguna. Namun, jika "username" variabel diketikan dengan inject seperti diatas maka peryataan kode SQL menjadi:

```
SELECT * FROM users WHERE name = '' OR '1'='1';
```

Jika kode ini akan digunakan dalam sebuah prosedur untuk melakukan otentikasi, maka contoh ini dapat digunakan untuk memaksa pemilihan nama pengguna yang valid karena evaluasi '1 '= '1' adalah selalu benar. Hal yang serupa juga akan terjadi apabila kita memasukan kode tersebut pada kolom password. Sehingga dengan memasukan ' or '1'='1' pada kolom user name dan kolom password kita sudah bias log in tanpa menggunakan user name dan password yang sebenarnya.

Untuk mengatasi masalah vulnerability ini maka para professional mendirikan sebuah organisasi untuk membantu para praktisi mengatasi masalah masalah yang timbul dalam aplikasi web. Open Web Application Security Project (OWASP) adalah sebuah yayasan yang bertujuan untuk mencari dan mengatasi masalah masalah serta vulnerabilities yang ada pada web application. Menurut OWASP, selain SQL injection, serangan melalui web lainnya adalah dengan teknik brute force, cache poisoning dan DNS poisoning. Oleh karena itu adalah menjadi hal yang penting bahwa unsur security harus diperhatikan dalam pembuatan perangkat lunak untuk aplikasi berbasis web. Semua materi dari OWASP dapat di download pada websitenya di https://www.owasp.org