Rakamin Academy

investree

Virtual Internship Experience

Code Security

SQL Injection

SQL injection adalah jenis aksi hacking pada keamanan komputer di mana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem dengan memanfaatkan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi yang tidak diproteksi dengan baik.

Cara yang digunakan oleh attacker sebenarnya sangat sederhana, yaitu penyerang berusaha memasukkan query yang tidak valid ke melalui field input ataupun melalui URL. Mengingat sederhananya teknik ini ada beberapa programmer yang terkadang mengabaikannya.

Mengenal Cara Kerja SQL Injection

Pada umumnya sintak SQL yang sering dipakai pada proses developing atau pembuatan sebuah aplikasi adalah sintak yang termasuk dalam kategori perintah DML(Data Manipualtion Language) yakni INSERT, UPDATE dan DELETE. sebagai contoh misalnya kita punya sebuah web dengan URL seperti ini:

```
http://www.domain.com/index.php?id=10
```

perintah untuk menampilkan record dari skema URL seperti di atas biasanya adalah seperti ini :

```
select * from tblBerita where id = 10
```

maka pada penulisan sintak php akan menjadi seperti ini :

```
$SQL="select * from tblBerita where id = '".$_GET['id']."'";
```

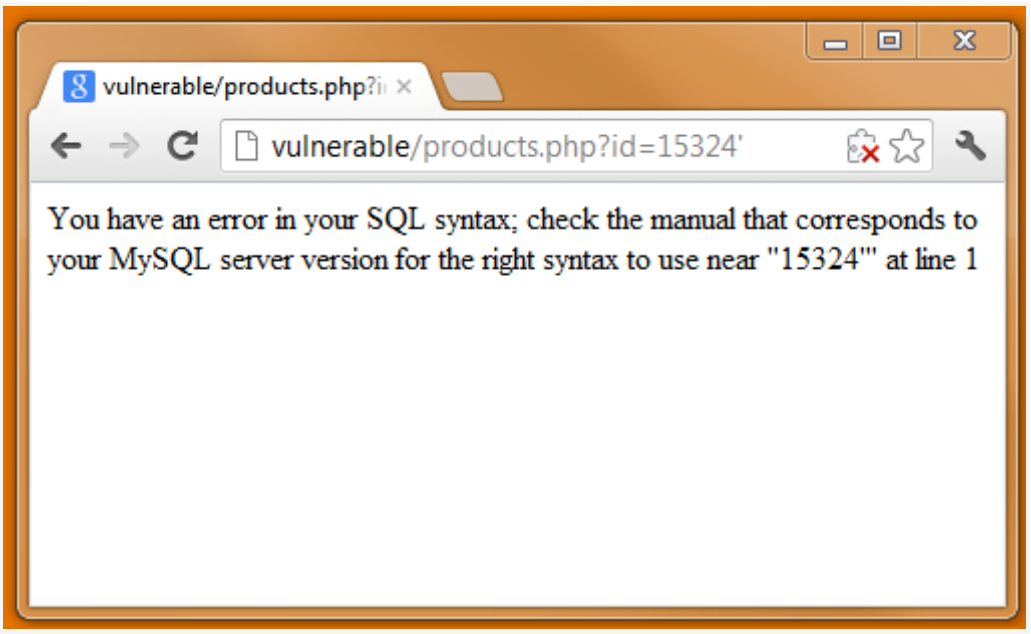
pada proses eksekusi normal sintak tersebut, database server akan memberikan balikan hasil sesuai yang parameter yang dikirimkan. Namun bila kita memodifikasi

parameter yang dikirim melalu url dengan sebuah karakter khusus yaitu single quote (') seperti ini :

```
http://www.website.com/index.php?id=10'
```

maka SQL query tersebut tidak akan bisa di eksekusi dan database server akan memberikan balikan berupa pesan error seperti berikut :

```
#1064 - You have an error in your SQL syntax;
check the manual that corresponds to yourMySQL server version for the right
syntax to use near ''' at line 1
```



karena dibalik layar, Query SQL yang di jalankan adalah seperti dibawah ini :

```
select * from tblBerita where id ='10''
```

Dan hal ini lah yang mejadi celah sebuah situs dan dengan mudah di eksploitasi dengan metode SQL Injection. apa lagi jika dengan menggunakan tools SQL ijection yang mempermudah kerjaan si hacker.

Mengamankan Dari Serangan SQL Injection

ada beberapa cara yang bisa kita lakukan untuk mengatasi serangan SQL injection , kita bisa membuat script anti SQL injection dengan memanfaatkan fungsi bawan dari PHP yaitu mysql_real_escape atau mysql_real_escape_string. cara penggunaanya adalah sebagai berikut :

```
$id = mysql_real_escape_string($_GET['id']);
```

selain cara di atas, ada beberapa tips aplikatif yang bisa anda gunakan untuk mengamankan web anda dari serangan SQL injection, berikut ini tips nya :

1. Batasi panjang input box (jika memungkinkan), dengan cara membatasinya di kode program, jadi si cracker pemula akan bingung sejenak melihat input box nya gak bisa diinject dengan perintah yang panjang.
2. Filter input yang dimasukkan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation).
3. Matikan atau sembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan.
4. Matikan fasilitas-fasilitas standar seperti Stored Procedures, Extended Stored Procedures jika memungkinkan.
5. Ubah “Startup and run SQL Server” menggunakan low privilege user di SQL Server Security tab.

Tools Yang Digunakan Untuk SQL Injection

Hanya sebagai pengetahuan saja tentang toosls yang bisa anda gunakan untuk melakukan uji coba keamanan aplikasi yang sedang anda kembangkan terkait masalah SQL inkection, berikut ini tools yang sering diguanakan :

1. BSQL Hacker adalah sebuah toold yang Dikembangkan oleh Portcullis Labs, BSQL Hacker adalah SQL injection yang di rancang untuk mengeksplor hampir seluruh jenis data base.
2. Havij adalah SQL Injection otomatis alat yang membantu penguji penetrasi untuk mencari dan mengeksploitasi kelemahan SQL Injection pada halaman web.

Sebenarnya masih banyak lagi tools yang bisa anda gunakan untuk ujicoba keamanan aplikasi yang sedang anda kembangkan dari serangan SQL injection.

Cross-site Request Forgery (CSRF) atau bisa disebut dengan one-click attack adalah sebuah serangan yang menggunakan injeksi script baik itu berupa kode javascript, link, atau gambar dengan memanfaatkan token autentikasi.

Disebut one-click attack karena metode ini hanya perlu pemicu dari user dan pemicunya bisa berupa link yang sudah dimaipulasi untuk mengeksekusi perintah.

Nah secara umum CSRF ini bekerja dengan memanfaatkan token autentikasi korbannya dengan tujuan melakukan suatu request yang tidak dinginkan oleh korban. Disini terlihat perbedaan antara CSRF dan Phising, Phising menggunakan url samaran untuk menipu korbannya yang seakan - akan menyerupai website resminya sedangkan CSRF korban akan dibawa kesebuah website yang baginya menarik dan oleh hacker website tersebut akan diinject dengan script jahat.

Ok jika kalian masih bingung saya akan mengandaikan bagaimana cara kerja dari CSRF ini.

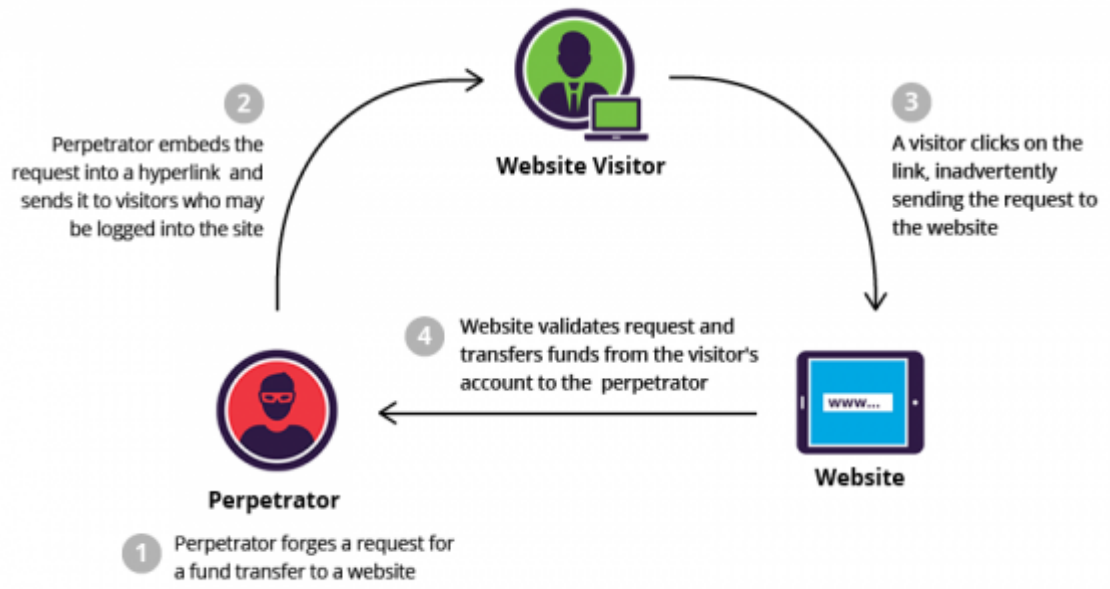
Contoh Serangan

Misalkan ada 2 orang sebut saja Bona dan Boni. Bona akan mentransfer uang kepada Boni menggunakan fasilitas internet banking, setelah Bona melakukan proses autentikasi maka dia akan diarahkan kehalaman transfer.

Katakan saja halaman transfer tersebut memiliki form berupa No rekening tujuan, dan jumlah transfer dan juga sebuah tombol bertuliskan Transfer. Ketika proses transfer selesai Bona menerima sebuah e-mail yang berisi link artikel tentang cara membuat kue yang enak.

Nah disinilah si hacker memanfaatkan kesempatan tersebut. Dengan memanfaatkan akses token Bona yang masih aktif pada tab akun banknya maka si hacker akan menginject dan memanipulasi link yang ada dalam e-mail tersebut.

Disini si hacker akan membuat formnya sendiri membuatnya tidak terlihat dan menyisipkannya pada e-mail yang diterima oleh Bona. Jadi ketika Bona mengunjungi link tersebut maka yang akan melakukan request adalah form transfer bank pada tab yang satunya dan secara tidak sadar Bona telah mentransfer sejumlah uang kepada hacker tersebut.



sumber image: medium

Waah bahaya juga ya itu kalau transfer sejumlah uang, bagaimana jika si hacker mereset password kalian?.

Ok dari kejadian diatas kita menganalisa masing - masing peran memiliki kesalahannya masing - masing. Pertama form pada sistem Bank harusnya dilengkapi

secure token untuk mencegah terjadinya request yang tidak dinginkan dan juga sistem bank bisa memproses GET request pada proses transfernya, kedua Bona tidak langsung logout dari sistem bank tersebut dan membiarkan tokennya aktif.

Tips Pencegahan

Dari analisa diatas kita akan tahu langkah penjegahan apa yang akan dilakukan untuk menangkal CSRF ini dan disini saya akan merangkum beberapa untuk kalian.

1. Tips yang pertama adalah segera logout dari akun bank kalian ketiga tidak akan digunakan lagi. Sebab seperti yang saya sudah jelaskan diawal CSRF bekerja dengan memanfaatkan akses token pengguna.
2. Untuk Developer Aplikasi disarankan untuk memberbaharui sistem keamanan secara berkala sebab tidak mungkin hacker menggunakan metode penyerangan yang sama ke sistem yang sama.
3. Masih untuk para Developer khususnya website, pastikan agar request yang sifatnya menambah, mengedit, dan menghapus data dilakukan dengan method POST dan method GET hanya untuk menampikan data saja.
4. Proteksi form dengan csrf protection saat ini hampir semua framework PHP sudah ada fitur ini bahkan CodeIgniter juga sudah disediakan di pada versi terbarunya.

Referensi

http://indonesiahackercyberteam.blogspot.co.id/2014/07/mencegah-website-dari-serangan-sql.html

https://www.kodinggen.com/apa-itu-csrf-bagaimana-cara-kerjanya-dan-tips-pencegahannya/