TI 6A/3/Alvin Tandiardi/UTS PJJ 2020/3: Pembobolan Situs KPU

Nomor dokumen: 3

Judul kasus: Pembobolan Situs KPU

Isi dokumen:

Pada hari Sabtu, 17 April 2004, Dani Firmansyah(25 th), konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya menjadi nama-nama unik seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection (pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004.

Kata kunci: Pembobolan, Situs KPU, SQL Injection.

**Opini dan Wawasan Saya**

SQL injection adalah kegiatan menyisipkan perintah SQL kepada suatu statement SQL yang ada pada aplikasi yang sedang berjalan. SQL sendiri memiliki pengertian yaitu *Structured Query Language* yang merupakan bahasa yang digunakan untuk mengakses database. Dengan kata lain SQL injection ini merupakan suatu teknik pengeksploitasi pada web aplikasi yang dalamnya menggunakan database untuk penyimpanan datanya. Terjadinya SQL injection tersebut dikarenakan security atau keamanan pada level aplikasi (dalam hal ini aplikasi web) masih kurang sempurna. Kurang sempurnanya adalah dari cara aplikasi menghandle inputan yang boleh diproses ke dalam database. Misalnya pada suatu web yang terdapat fasilitas *login*, terdapat dua buah inputan pada umumnya, yaitu *username* dan *password*. Jika karakter yang masuk melalui dua buah inputan tersebut tidak difilter (disaring) dengan baik maka bisa menimbulkan efek SQL injection, ini dikarenakan biasanya inputan tersebut secara sistem akan menjadi bagian dari kriteria dari suatu perintah SQL di dalam aplikasi web-nya.

Untuk melakukan injection, penyerang dapat melakukan nya dengan beberapa teknik penulisan :

1. *Tautologies*

Penyerang menginputkan *query* yang hasilnya selalu “True”:

*Select\*from users where username=’ admin’ or 1=1 --‘and password=’’;*

1. *Union Queries*

Penyerang menginputkan “*UNION QUERY*” untuk mendapatkan lebih banyak data:

*Select bookTitle, ISBN from books where bookID = 1 UNION Select “hack”, balance from accounts where accNo=3456--;*

1. *Piggyback Queries*

Penyerang menginputkan tambahan statement yang mempengaruhi hasil *query*:

*Select\*from users where username=’’; drop table accounts --and password=’’*

1. *Malformed Queries*

Penyerang menggunakan kerentanan pada hasil *error* *message* untuk mendapatkan informasi dari database:

*Select \* from books where bookID=convert(int,(select top 1 name from sysobjects where xtype=‘u’));*

1. *Inference*

Jenis serangan ini bergantung pada *response-time* pada web server untuk mendapatkan informasi :

*Select \* from users where username=’hello1’; selectif(user() like  'root@%', benchmark(1000000,sha1('test')),'false');--‘and password=’’*

1. *Alternate Encoding*

Jenis serangan ini menggunakan kombinasi dari spesial karakter (seperti *quote*, *dash*, dll ) untuk melewati skema pertahanan :

*Select \* from books where bookID=1;exec(char(0x730065006c00650063 007400200040004000760065007200730069006f006e00);*

Metode untuk menghindari SQL Injection dapat dilakukan dengan dua cara yaitu secara *client-side* dan *server-side*. Pada metode *client-Side* yaitu menerima *'Shadow SQL Query*' dari *server-side* dan melakukan pengecekan terhadap deviasi yang terjadi antara *shadow query* dengan *query* dinamis yang dibentuk oleh masukan dari pengguna. Jika ditemukan adanya deviasi maka dapat dipastikan bahwa masukannya tidak benar (*Malicious*). Sedangkan untuk metode *server-side* dapat melalui sejumlah langkah antara lain:

1. Gunakan *Prepared Statement* atau *Parameterized Query*. Lebih sederhana dan lebih mudah untuk dimengerti dibanding *query* dinamis, *Parameterized query* mengirimkan setiap parameter ke dalam lapisan *query* setelah semua kode SQL telah didefinisikan. Database dapat membedakan antara kode dan data, apapun masukan dari pengguna. Seorang Penyerang tidak dapat merubah maksud *query*, meskipun SQL command telah disusupkan di dalamnya.
2. Lakukan validasi masukan. Autentikasi masukan dari pengguna dengan aturan-aturan yang telah didefinisikan seperti panjang, tipe dan filter lain jika diperlukan.
3. Matikan atau sembunyikan pesan-pesan error yang keluar dari server database.
4. Mengunci atau membatasi database anda. Jika aplikasi web Anda tidak memerlukan akses ke tabel tertentu, maka pastikan bahwa mereka semua tidak memiliki izin untuk itu. Jika hanya *read-only* maka akan menghasilkan laporan dari tabel hutang account anda maka pastikan anda menonaktifkan *insert* / *update* / menghapus akses.

SQL Injection merupakan tindakan ilegal jika kita melihat dari sisi sistem, tapi ada kalanya berguna sebagai acuan tingkat keamanan sistem, sehingga itu semua kembali lagi kepada niat dan kesadaran dari pelakunya. Seorang *attacker* dapat memanfaatkan pesan error yang dikirimkan server ketika dia memberikan *query-query* ilegal untuk mendapatkan nama dan tipe dari kolom pada tabel dalam suatu database

**Payung Hukum**

1. UU Nomor 36 Tahun 1999 tentang Telekomunikasi. Tepatnya pada pasal 50 dan 22.

Bunyi Pasal 22, yaitu

Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi :

* 1. akses ke jaringan telekomunikasi; dan atau
  2. akses ke jasa telekomunikasi; dan atau
  3. akses ke jaringan telekomunikasi khusus.

Bunyi Pasal 50, yaitu

Barang siapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00(enam ratus juta rupiah).

Disini Dani Firmansyah melakukan akses tidak sah dan memanipulasi data nama partai pada situs milik KPU. Menurut saya UU ini adalah yang paling relevan karena pada tahun 2004 belum ada UU ITE, dimana UU ITE sendiri baru diterbitkan pada tahun 2008.

1. Pasal 406 Kitab Undang Undang Hukum Pidana (KUHP) Ayat 1, yaitu

Barang siapa dengan sengaja dan melawan hukum menghancurkan, merusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruhnya atau, sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

1. Pasal 30 Undang Undang Nomor 11 tahun 2008 tentang ITE, yaitu
   1. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau. Sistem Elektronik milik Orang lain dengan cara apa pun.
   2. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
   3. Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pelanggaran dari pasal ini diatur pada pasal 46, yaitu

1. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
2. Setiap, Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).
4. Pasal 35 Undang Undang Nomor 11 tahun 2008 tentang ITE, yaitu

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Pelanggaran dari pasal ini diatur pada pasal 51 ayat 1, yaitu

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

**Teknologi Yang Digunakan**

Teknologi Hardware yang digunakan adalah sebuah perangkat komputer atau laptop dan konektivitas internet.

Teknologi Software yang digunakan adalah Web browser untuk membuka halaman situs, dan pengetahuan mengenai query SQL. Karena teknik SQL Injection ini adalah memanipulasi proses query yang sudah ada di sistem dengan menyisipkan perintah yang hacker inginkan seperti menambahkan query untuk mengganti data, mem bypass akses login, hingga menghapus tabel database. Terdapat juga tools seperti SQLMap.

# **Referensi**

Indonesia, K. K. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*. Retrieved April 15, 2020, from Kementrian Keuangan Republik Indonesia: http://www.jdih.kemenkeu.go.id/fullText/2008/11TAHUN2008UU.htm

Jogloabang. (2019, November 02). *UU 36 tahun 1999 tentang Telekomunikasi*. Retrieved April 15, 2020, from Jogloabang: https://www.jogloabang.com/pustaka/uu-36-1999-telekomunikasi

Murdianto, V. S. (2018, Oktober). Makalah Keamanan Sistem SQL Injection. Surakarta.

Sovia Hasanah, S. (2016, September 15). *Akibat Hukum Jika Merusak Barang Orang Lain Tanpa Sengaja*. Retrieved April 15, 2020, from HukumOnline.com: https://www.hukumonline.com/klinik/detail/ulasan/lt539a466693874/akibat-hukum-jika-merusak-barang-orang-lain-tanpa-sengaja/

Yulianingsih. (2016, Juni). Menangkal Serangan SQL Injection dengan Parameterized Query. *Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2*, 46-49.