

Zabezpieczenia serwerów internetowych

Jakub Tomaszewski

Zespół Bezpieczeństwa

Poznańskie Centrum Superkomputerowo - Sieciowe



Zespół Bezpieczeństwa PCSS

- Dedykowany zespół istnieje od 1996r.
- Podstawowy zakres prac Zespołu
 - Zabezpieczanie infrastruktury PCSS
 - Zadania bezpieczeństwa w projektach naukowo – badawczych
 - Szkolenia i transfer wiedzy
 - Badania własne
 - Audyty i doradztwo w zakresie bezpieczeństwa IT
- Niektóre badania z ostatnich lat
 - Raport o bezpieczeństwie bankowości elektronicznej (2006)
 - Bezpieczeństwo serwerów WWW Apache i MS IIS (2007)
 - Bezpieczeństwo sklepów internetowych (2008)
- <http://security.psnc.pl>



Plan prezentacji

- Model serwera,
- Kim jest agresor?
- System,
- Serwer www,
- Interpreter,
- Podsumowanie



Model Serwera LAMP

→Linux



→Apache



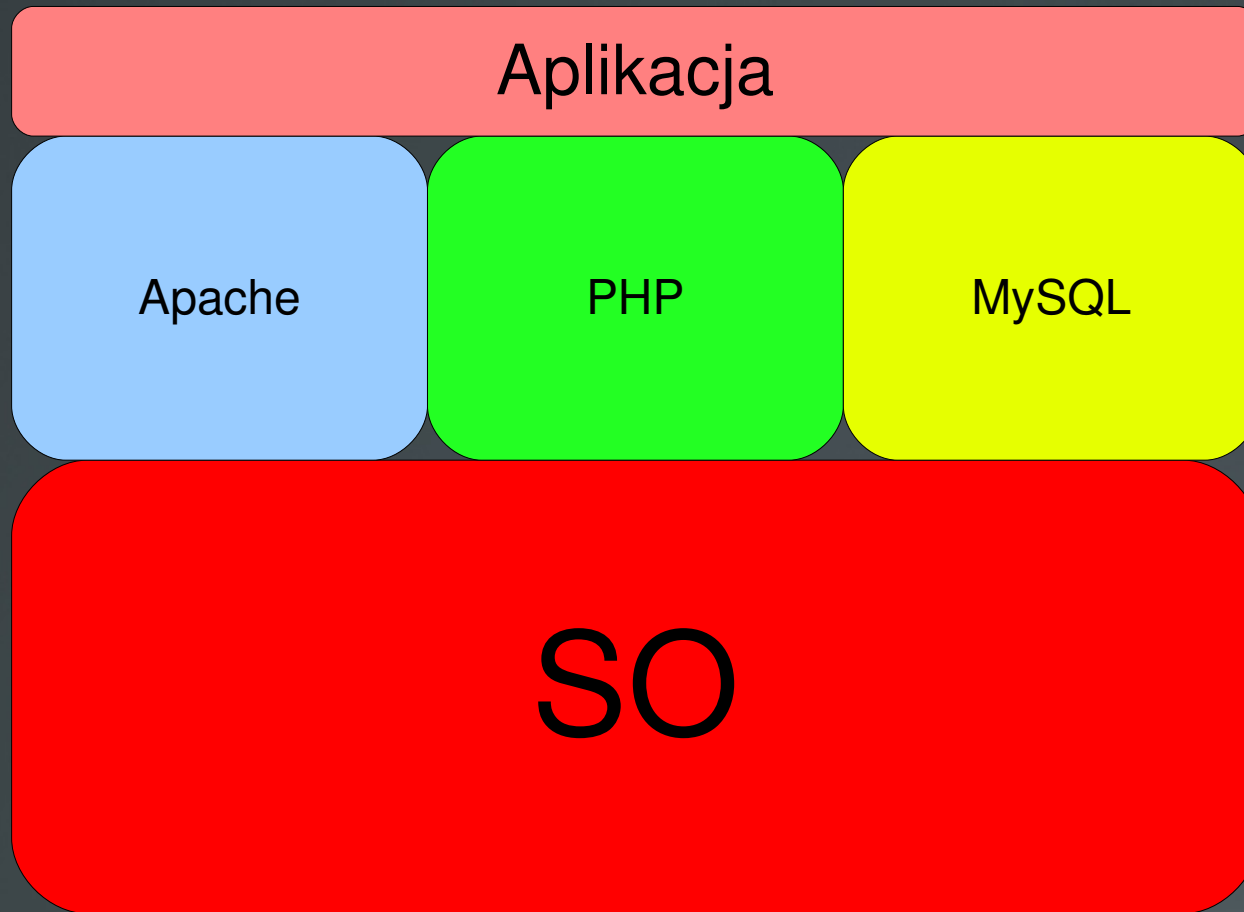
→MySQL



→PHP



Budowa systemu



Agresor – analiza możliwości

- Osoba, która wykupuje hosting na naszym serwerze,
- Ma „pełną” dowolność umieszczania kodu na swojej stronie,
- Jego cele: inne serwisy lub sam serwer,
- Agresor nieświadomy (?),



System



- Linux Security for Beginners – <http://www.linuxtopia.org/LinuxSecurity/index.html>
- Linux Administrator's Security Guide – http://www.linuxtopia.org/online_books/linux_administrators_security_guide/index.html
- Linux Security HOWTO – http://www.linuxtopia.org/Linux_Security_HOWTO/index.html
- Red Hat Linux Enterprise 4 Security Guide – http://www.linuxtopia.org/online_books/redhat_linux_security_guide/
- Securing Debian Manual – <http://www.debian.org/doc/manuals/securing-debian-howto>
- Slackware Linux Essentials – Security – <http://www.slackbook.org/html/security.html>
- SuSE Linux Enterprise Server – <http://ltp.sourceforge.net/docs/SLES-security-guide.pdf>
- Ubuntu Security – <http://ubuntuforums.org/showthread.php?t=510812>



Apache – wyciek informacji



Apache – szukamy i ...



- Apache 2.2.8 mod_ssl Vulnerability,
- Apache 2.2.8 mod_proxy_ftp globbing XSS
- Apache 2.2.8 mod_proxy_balancer CSRF
- Apache 2.2.8 mod_proxy_http DoS



Apache – obrona



→ Zmiana w pliku konfiguracyjnym apache

ErrorDocument 404 .errors/my_error_page404.htm

→ Aktualizacja wersji oprogramowania (!)



PHP - phpinfo()



phptest - Opera

Plik Edycja Widok Zakładki Widżety RSS Poczta Narzędzia Pomoc

Nowa phptest

http://www.com/php.php

ri

Hello World !

PHP Version 4.4.8

System	Linux scary.hosts.co.uk 2.6.9-67.0.1.ELsmp #1 SMP Wed Dec 19 16:01:12 EST 2007 i686
Build Date	Jan 24 2008 12:05:48
Configure Command	'./configure' '--prefix=/usr/local' '--enable-bcmath' '--with-freetype-dir' '--enable-ftp' '--with-mysql=/usr' '--with-mssql=/usr/local' '--with-mcrypt=/usr/local/lib/libmcrypt' '--with-zlib-dir=/usr/local' '--with-openssl' '--with-curl' '--with-imap=/usr/local/imap-2006d' '--with-gd' '--with-jpeg-dir' '--with-png-dir' '--with-ttf' '--with-xml' '--enable-xslt' '--with-xslt-sablot' '--with-sablot-js' '--enable-mbstring' '--with-config-file-path=/usr/local/bin' '--with-pear' '--with-openssl' '--enable-exif'
Server API	CGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/Zend/etc/php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20050606
Debug Build	no
Zend Memory Manager	enabled
Thread Safety	disabled
Registered PHP Streams	php, http, ftp, https, ftps, compress.zlib

This program makes use of the Zend Scripting Language Engine:
Zend Engine v1.3.0, Copyright (c) 1998-2004 Zend Technologies with the ionCube PHP Loader v3.1.16,
Copyright (c) 2002-2006, by ionCube Ltd. and with Zend Extension Manager v1.3.0, Copyright (c) 2003-2007

PHP – też możemy poszukać ...



- PHP 4.4.8 Multiple Buffer Overflow Vulnerabilities
- PHP 4.4.7 / 5.2.3 MySQL/MySQLi Safe Mode Bypass Vulnerability



PHP - phpinfo() - obrona



disable_functions=phpinfo



PHP - c99.txt, r57.txt



03-02-2009 16:57:45 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [disks]
safe_mode: OFF PHP version: 4.4.7 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF
Disable functions: NONE
HDD Free: 21.07 GB HDD Total: 26 GB

uname -a : Linux server1. [redacted].com 2.6.18-028stab053.4-ent #1 SMP Mon Jan 14 12:29:09 MSK 2008 i686 i686 i386 GNU/Linux
sysctl : Linux 2.6.18-028stab053.4-ent
\$OSTYPE : linux-gnu
Server : Apache/1.3.37 (Unix) PHP/5.1.6 mod_gzip/1.3.26.1a mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 PHP/4.4.7
id : uid=99(nobody) gid=99(nobody) groups=99(nobody)
pwd : /home/[redacted]/public_html (drwxr-xr-x)

Executed command: ls -lia

total	41880		
48138004	drwxr-xr-x	[redacted]	12288 Feb 2 08:39 .
47918668	drwx--x--x	[redacted]	4096 Feb 2 10:51 ..
48138096	-rw-r--r--	1	7648 Jan 29 06:38 .htaccess
48138376	-rw-r--r--	1	7648 Jan 18 09:13 .htaccess_bck1
48141650	-rw-r--r--	1	0 Jan 19 10:18 .htaccess_old
48138378	-rw-r--r--	1	360 Jan 18 09:13 .htaccess~
48138392	-rw-r--r--	1	389 Jan 18 09:13 [redacted]
48139078	-rw-r--r--	1	1438 Jan 18 09:14 [redacted]
48140254	-rw-r--r--	1	35665 Jan 18 09:17 [redacted]
48140474	-rw-r--r--	1	3000 Jan 18 09:27 [redacted]
48141862	-rw-r--r--	1	63822 Jan 28 14:05 [redacted]
48140664	-rw-r--r--	1	0805500 Jan 18 21:58 [redacted]
48141646	-rw-r--r--	1	42354 Jan 19 09:05 [redacted]
48311818	drwxr-xr-x	[redacted]	4096 Jan 19 09:06 _admin
48138062	drwxr-xr-x	[redacted]	4096 Jan 19 09:06 _private

:: Execute command on server [icons] ::

Run command: [input field]
Work directory: /home/[redacted]/public_html [Execute]

:: Edit files [icons] ::

File for edit: /home/[redacted]/public_html [Edit file]

:: Aliases [icons] ::

Select alias: find suid files [Execute]

:: Find text in files [icons] ::

Find text: text [Find]
In dirs: /home/[redacted]/public_html * (/root;/home;/tmp)
Only in files: .txt;.php * (.txt;.php;.htm)

:: Search text in files via find [icons] ::

Text for find: text [Find]
Find in folder: /home/[redacted]/public_html * (/root;/home;/tmp)



PHP - obrona



disable_functions=exec,fopen,popen,passthru,readfile,file,system

- Ograniczenie praw dostępu użytkownika,
- A może maszyna virtualna?



PHP – informacje o błędach



```
Warning: ldap_connect() expects parameter 2 to be long,  
string given in /var/www/html/monitoring/ldap/php/  
tree.php on line 252  
Can not create LDAP connection
```



PHP – obrona



→ Zmiana w pliku php.ini:

display_errors = off

log_errors = on

error_log = /var/log/php/error.log



PHP – listowanie katalogów

A screenshot of an Opera browser window. The title bar reads "Index of /jobs - Opera". The menu bar includes "Plik", "Edycja", "Widok", "Zakładki", "Widżety", "RSS", "Poczta", "Narzędzia", and "Pomoc". The address bar shows "http://monitoring.eg" with a search icon and a Google search box. The main content area displays "Index of /jobs" and a table of files and directories.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 autoupdate.php	24-May-2006 11:25	1.0K	
 certTimeLeft.php	15-May-2006 13:34	2.9K	
 claster_info.php	15-May-2006 13:34	2.6K	



PHP – obrona



→ Zmiana w pliku httpd.conf:

Options -Indexes

→ Definiowanie pliku głównego:

DirectoryIndex index.php



PHP – niedozwolone ścieżki



→ A co jeśli mogę wywołać to tak:

<http://www.jakisadresserwera.pl/index.php?v=list&p=../../>

katalog_innego_usera/plik_konfiguracyjny_innego_usera



PHP – niedozwolone ścieżki



→ Albo tak:

<http://www.jakisadresserwera.pl/index.php?>

[v=list&p=../../../../../../../../../../../../etc/passwd](#)



Obrona trochę dokładniej (1)

→ PHP Safe Mode (php.ini):

```
safe_mode on
```

→ Katalog główny aplikacji (php.ini)

```
open_basedir = /home/www/htdocs/any_dir
```

→ Katalog główny aplikacji (httpd.conf)

```
<Directory "/.htdocs/any_dir">
```

```
php_admin_value open_basedir "/.htdocs/any_dir"
```

```
</Directory>
```



Obrona trochę dokładniej (2)

→ Wyłączenie niebezpiecznych funkcji (php.ini):

disable_functions=phpinfo

→ Wyświetlanie błędów (php.ini)

display_errors = off

→ Wyciek informacji (php.ini)

expose_php = off



Obrona trochę dokładniej (3)

→ Ograniczanie dostępu (httpd.conf):

```
<Directory "/.Apache/Apache2/htdocs">
```

```
Order Allow, Deny
```

```
Allow from 192.168.1.0/24
```

```
Deny from all
```

```
</Directory>
```

→ Sygnatura serwera (httpd.conf)

```
ServerSignature Off
```



Obrona trochę dokładniej (4)

→ Wyłączenie niebezpiecznych skryptów (httpd.conf):

CGI (Common Gateway Interface)

SSI (Server Side Includes)

→ Ukrywanie .htaccess (httpd.conf)

<Files .htaccess>

order allow,deny

deny from all

</Files>



Jak się bronić?

- Atakować swoją stronę możliwie często =D
- Skanery: nikto, wikto, AppScan, ...
- Firewallle warstwy 7 i 8,
- Czytać, słuchać, AKTUALIZOWAĆ,
- Czytać LOGI,
- Wykonywać audyty,



Informacje kontaktowe

- Autor prezentacji
 - bluerose@man.poznan.pl
- PCSS
 - <http://www.pcss.pl>
 - <http://www.man.poznan.pl>
- Zespół Bezpieczeństwa PCSS
 - <http://security.psnc.pl>
 - security@man.poznan.pl



Pytania i dyskusja, propozycje?



Dziękuję za uwagę!

