实验吧隐写术WP(一）

原创

Neil-Yale 于 2017-03-28 12:46:44 发布 9106 收藏 3

文章标签： 源码 base64 sha1 CTF

本文链接：https://blog.csdn.net/yalecaltech/article/details/67634552

1.这是什么（http://www.shiyanbar.com/ctf/8）

直接托winhex，拉到最下面的字符串再sha1就行了

spartacus.jpg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00426048	51	9A	28	A0	05	CF	D2	83	D2	8A	28	01	29	D9	A2	8A	Q▌(ÏÒ▌Ò▌( )Ù¢▌
00426064	00	33	4D	3D	68	A2	80	01	D6	9D	9A	28	A0	03	34	9D	3M=h¢▌ Ö ▌(4
00426080	FA	D1	45	00	2E	68	CD	14	50	01	9A	33	45	14	00	66	úÑE .hÍ P ▌3E f
00426096	9B	45	14	00	EC	D1	9A	28	A0	06	D1	45	14	00	51	45	▌E ìÑ▌(ÑE QE
00426112	14	00	51	45	14	00	51	45	14	00	51	45	14	00	51	45	QE QE QE QE
00426128	14	00	51	45	14	00	51	45	14	00	EC	D3	73	C5	14	50	QE QE ìÓsÅ P
00426144	01	45	14	50	03	BB	53	7B	51	45	00	14	51	45	00	14	E P »S{QE QE
00426160	51	45	00	14	51	45	00	14	66	8A	28	00	CD	14	51	40	QE QE f▌(Í Q@
00426176	05	14	51	40	05	14	51	40	05	14	51	40	0A	0F	14	66	Q@ Q@ Q@ f
00426192	8A	28	00	CD	19	A2	8A	00	33	46	68	A2	80	10	F5	A2	▌(Í ¢▌ 3Fh¢▌ õ¢
00426208	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	▌(¢▌(¢▌(¢▌(¢
00426224	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	▌(¢▌(¢▌(¢▌(¢
00426240	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	▌(¢▌(¢▌(¢▌(¢
00426256	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	▌(¢▌(¢▌(¢▌(¢
00426272	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	8A	28	00	A2	▌(¢▌(¢▌(¢▌(¢
00426288	8A	28	00	A2	8A	28	01	D9	A3	34	51	40	08	7A	52	51	▌(¢▌(Ù£4Q@ zRQ
00426304	45	00	1D	A9	C7	D6	8A	28	01	B4	51	45	00	14	51	45	E ©ÇÖ▌(´QE QE
00426320	00	14	51	45	00	14	51	45	00	14	51	45	00	14	51	45	QE QE QE QE
00426336	00	14	51	45	00	7F	FF	D9	3C	25	65	78	65	63	75	74	QE ÿÙ<%execut
00426352	65	20	72	65	71	75	65	73	74	28	22	69	6D	61	67	65	e request("image
00426368	73	22	29	25	3E												s")%>

2.听会歌吧（http://www.shiyanbar.com/ctf/19）
打开页面，直接点的话就会直接下载，所以我们先看看源码
发现

```
<p>为了让大家更轻松的比赛，为大家准备了两首歌让大家下载</p>

<p><a href="download.php?url=eG1uZ3hpbmdkaWFuZGVuZy5tcDM=" target="_blank">星星点灯</a></p>
<p><a href="download.php?url=YnV4aWFuZ3poYW5nZGEubXAz" target="_blank">不想长大</a></p>
```


随便点击哪一条都行
发现页面很卡。。
看源码，乱七八糟的
发现提供的值是base64的，比如eGluZ3hpbmdkaWFuZGVuZy5tcDM=解码后就是星星点灯.mp3
那么我们尝试把download.php编码后提交
得到

view-source:http://ctf5.shiyanbar.com/down/download.php?url=ZG93bmxvYWQucGhw

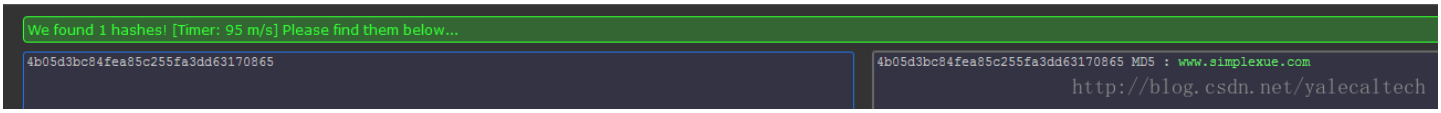
老司机 资源 兰州理工大学 挖洞 i春秋_专业的信息安全... 返璞归真——流量中... i春秋&360安全星计... 2017年"普译奖"全国

```
'php
'ror_reporting(0);
ıclude("hereiskey.php");
ırl=base64_decode($_GET[url]);
:( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="download.php"
   $file_size = filesize($url);
   header ( "Pragma: public" );
   header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
   header ( "Cache-Control: private", false );
   header ( "Content-Transfer-Encoding: binary" );
   header ( "Content-Type:audio/mpeg MP3");
   header ( "Content-Length: " . $file_size);
   header ( "Content-Disposition: attachment; filename=".$url);
   echo(file_get_contents($url));
   exit;

.se {
   echo "Access Forbidden!";

>
```


在if语句里第二和三是mp3，第四我们已经提交过了，所以我们接下来提交hereiskey.php的编码后的字符串
得到key

```
<?php
// key is d0wnload_0k
?>
```

3.安女神，我爱你！(http://www.shiyanbar.com/ctf/41)
题目都提示了zip.jpg，改后缀为zip，再解压得字符串
再md5解密就行了
(这串md5在国内要么破不出来要么收费，我科学上网才解密的）
网址：https://hashkiller.co.uk/md5-decrypter.aspx

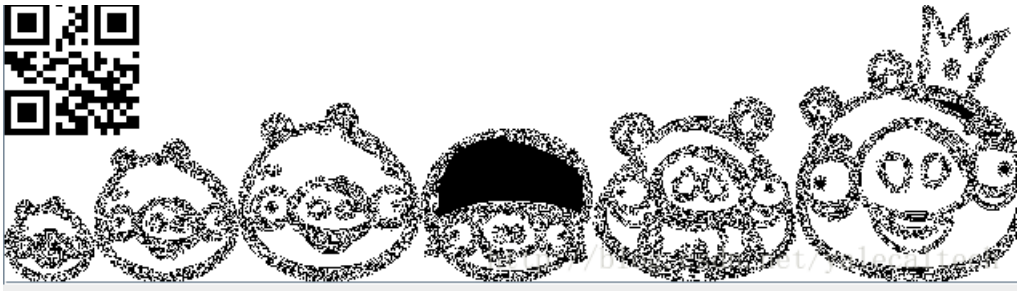


4.藏在女神后面，嘿嘿（http://www.shiyanbar.com/ctf/43）
直接notepad++打开，ctrl+F搜索关键词key

```
hen="2011-11-03T20:04:19+08:00" stEvt:softwareAgent="Adobe Photosl

key is SSBsb3ZlIHlvdQ==</rdf:li></rdf:Alt>
lang="x-default">key is SSBsb3ZlIHlvdQ==</rdf:li></rdf:Alt>
```


base64解密即可

5.SB！SB！SB！(http://www.shiyanbar.com/ctf/45)
保存下来，sg处理下就可以得到



扫一扫就得到了

6.女神又和大家见面了（http://www.shiyanbar.com/ctf/58）
下载之后改后缀为zip，解压得到mp3和txt
mp3肯定用mp3stego处理，处理时需要密码，而txt提供的就是密码
处理过程如下

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego

C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego>decode.exe -X -P simctf music.mp3
MP3StegoEncoder 1.1.16
See README file for copyright info
Input file = 'music.mp3'  output file = 'music.mp3.pcm'
Will attempt to extract hidden information. Output: music.mp3.txt
the bit stream file music.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 3416]Avg slots/frame = 417.837; b/smp = 2.90; br = 127.963 kbps
Decoding of "music.mp3" is finished
The decoded PCM output file name is "music.mp3.pcm"

C:\Users\hasee\Desktop\CTF工具\MP3Stego_1_1_16\MP3Stego_1_1_16\Development\MP3Stego>
                                                                    http://blog.csdn.net/yalecaltech
```

打开得到一串base64加密后的字符串
U2ltQ1RGe01QM19NUDNfc2RmZHNmfQ==
解码得到flag

7.小家伙挺可爱(http://www.shiyanbar.com/ctf/716)

binwalk 看一下发现是zip

于是顺便在kali里dd出来

```
root@kali:~# binwalk sim.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
22895         0x596F          Zip archive data, at least v2.0 to extract, compre
ssed size: 25, uncompressed size: 23, name: key.txt
23046         0x5A06          End of Zip archive

root@kali:~# binwalk --dd 'txt' sim.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
22895         0x596F          Zip archive data, at least v2.0 to extract, compre
ssed size: 25, uncompressed size: 23, name: key.txt
23046         0x5A06          End of Zip archive

root@kali:~#
```


winhex看一下

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	50	4B	03	04	14	00	00	00	08	00	5A	7E	F7	46	16	B5	PK Z~÷F
00000016	80	14	19	00	00	00	17	00	00	00	07	00	00	00	6B	65	▮ ke
00000032	79	2E	74	78	74	0B	CE	CC	75	0E	71	AB	CE	48	CD	C9	y.txt ÎÌu q«ÎHÉ
00000048	C9	57	28	CE	CC	2D	C8	49	AD	28	4D	AD	05	00	50	4B	ÉW(ÎÌ-ÈI-(M- PK
00000064	01	02	3F	00	14	00	09	00	08	00	5A	7E	F7	46	16	B5	? Z~÷F
00000080	80	14	19	00	00	00	17	00	00	00	07	00	24	00	00	00	▮ $
00000096	00	00	00	00	20	00	00	00	00	00	00	00	6B	65	79	2E	ke
00000112	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	65	txt e
00000128	58	F0	4A	1C	C5	D0	01	BD	EB	DD	3B	1C	C5	D0	01	BD	XðJ ÅÐ ½ëÝ; ÅÐ ½
00000144	EB	DD	3B	1C	C5	D0	01	50	4B	05	06	00	00	00	00	01	ëÝ; ÅÐ PK
00000160	00	01	00	59	00	00	00	3E	00	00	00	00	00	1A			Y >

将09改为00就行

之后解压就得到flag

（这里涉及到伪加密，详情可以参考：http://blog.csdn.net/ETF6996/article/details/51946250）

8.NSCTF crypto100（http://www.shiyanbar.com/ctf/1766）

binwalk 看一下可以发现有好几张图片，我们将它分离出来

```
File  Edit  View  Search  Terminal  Help
root@kali:~# binwalk -D=jpeg oddpic.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image
 directory: 8
13017         0x32D9          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.
0/" xmlns
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image
 directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
164186        0x2815A         Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns
:xap="htt
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"

root@kali:~#
```


得到四张，一张原图，其他三张都是有flag的图片

得到flag

9.LSB(http://www.shiyanbar.com/ctf/1774)

有个东西叫做wbStego

用他处理下就行，得到xxx.txt._js

拖到winhex可以看到flag

566.txt._js

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	5F	53	69	6D	43	54	46	7B	4C	53	42	5F	79	69	6E	78	_SimCTF{LSB_yinx
00000016	69	65	7D	24	0E	5C	0F	E8	F9	2B	23	49	55	6D	90	75	ie}$ \ èù+#IUm u
00000032	F8	B4	96	ED	27	6C	4E	DA	4D	80	E5	B7	2D	00	7F	F8	ø´ í'lNÚM å·- ø
00000048	25	2A	E0	00	78	DC	AA	DB	1B	E2	80	DB	00	00	00	D1	%*à xÜªÛ â Û Ñ
00000064	C8	71	6C	93	B6	69	12	BB	33	81	C7	58	E3	55	49	48	Èql ¶i » 3 ÇXãUIH
00000080	DC	C5	CF	CE	56	DB	FB	B6	D5	6D	A9	24	92	49	2A	AD	ÜÅÏÎVÛû¶ÕmC©$'I*-
00000096	4A	DA	92	E3	1E	49	F2	36	DB	72	37	1B	18	DF	4E	C7	JÚ'ã Iò6Ûr7 ßNÇ
00000112	13	FF	27	6D	BF	FF	63	B8	24	92	00	FF	B7	24	03	F0	ÿ'm¿ÿc¸$' ÿ·$ ð
00000128	3F	92	37	26	FC	42	F8	00	0F	FF	00	B7	F8	8E	49	07	?'7&üBø ÿ ·øI
00000144	EE	41	89	8D	B7	1C	6E	37	23	4B	1C	76	8F	8F	6D	AA	îA · n7#K v mª
00000160	DB	6A	6C	92	B8	8C	05	F8	4A	80	DB	00	71	CE	FC	97	Ûjl'¸ øJÛ qÎü
00000176	4B	D8	9D	B1	3A	30	05	B0	29	D2	B6	D7	1B	6E	35	55	KØ ±:0 °)Ò¶× n5U
00000192	B8	EC	49	C7	10	E4	8F	22	40	8E	36	85	F4	1A	E2	80	¸iIÇ ä "@6ô â
00000208	EB	C7	02	82	AA	73	64	95	56	D9	05	4B	F4	AE	92	A3	ëÇ ªsdVÙ Kô®'£
00000224	89	DB	6B	A4	93	66	DB	76	DE	07	F8	9D	AF	5D	C0	00	Ûk¤fÛvÞ ø ¯]À
00000240	0E	35	6D	AE	41	47	D1	E6	C0	03	F9	21	D9	54	AD	40	5m®AGÑæÀ ù!ÙT-@
00000256	77	6D	5C	45	63	6E	4E	4E	CA	3B	5C	72	38	E3	F9	55	wm\EcnNNÊ;\r8ãùU