writeup wyu-ctf

原创

L1s4 于 2020-09-25 21:32:51 发布 608 收藏

分类专栏： CTF 文章标签： writeup

本文链接：https://blog.csdn.net/baidu_39504221/article/details/103026675

Crypto还不会…就先不写了

靶场已关闭，不再更新

Misc

①这不是hex

由题意得 这是md5

e10adc3949ba59abbe56e057f20f883e

md5解密网址：https://www.somd5.com/

flag{123456}

②so easy!

```
&#102;&#108;&#97;&#103;&#123;&#85;&#49;&#110;&#99;&#111;&#100;&#101;&#95;&#120;&#120;&#120;&#120;&#120;&#95;&#97;&#97;&#97;&#95;&#98;&#98;&#125;
```

由题意得 这是HTML编码 丢到burpsuite里

flag{U1ncode_xxxxx_aaa_bb}

③base

4C4A575851324332474E5A58515453484B5634465332535A4F3547554F534C594C4A5756434D4B4F504A5747325A535
2485536513D3D3D3D

像16进制，转换一下

LJWXQ2C2GNZXQTSHKV4FS2SZO5GUOSLYLJWVCMKOPJWG2ZSRHU6Q====

有等于号，一开始以为是base64，转换发现乱码，就试了一下32

ZmxhZ3sxNGUxYjYwMGIxZmQ1NzlmfQ==

这里就是64了，丢到神器里

flag{14e1b600b1fd579f}

难道base32等于号多一点吗…

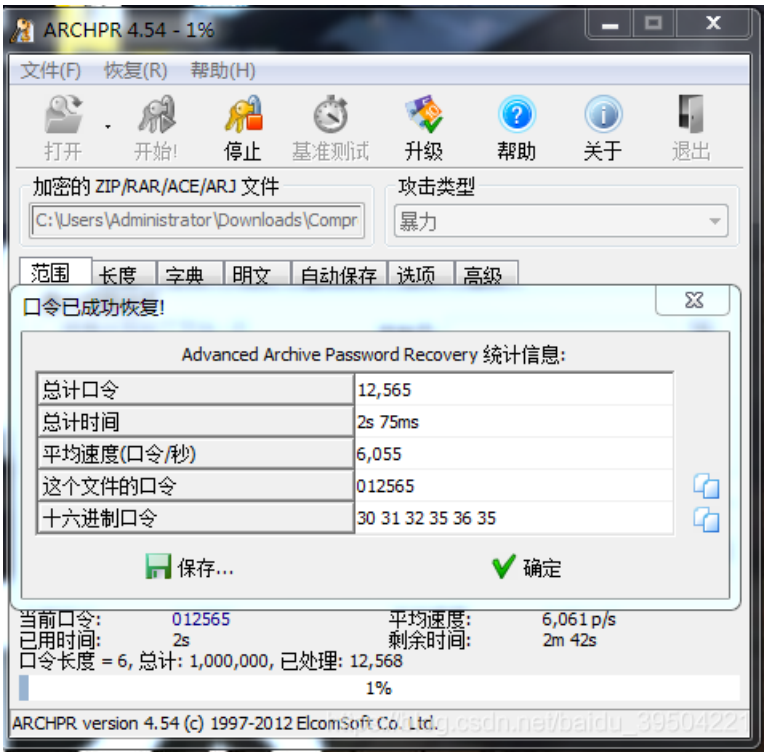
④颜文字

点进去就觉得是JSFUCK
丢到Console

flag{1de4080388a4bffe495f}

⑤爆破？

爆破手准备！！！！
把文件下载下来，拖进ARCHPR暴力破解
试了一下，最高字段长度为6时爆出了口令



flag{d144ab5c87621b6c233b548}

⑥zip

文件加密了，但是也没提示爆破
所以就想到了伪加密
果断放进winhex

flag.zip

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	50	4B	03	04	14	00	01	00	08	00	A0	B3	56	4D	6A	FE	PK ³VMjþ
00000016	40	9A	1C	00	00	00	1A	00	00	00	08	00	00	00	66	6C	@š fl
00000032	61	67	2E	74	78	74	4B	CB	49	4C	AF	4E	B6	30	36	B1	ag.txtKËII¯N¶06±
00000048	48	4C	4B	31	4D	36	37	4F	36	37	34	4F	34	B0	34	AF	HLK1M67O674O4°4¯
00000064	05	00	50	4B	01	02	1F	00	14	00	01	00	08	00	A0	B3	PK ³
00000080	56	4D	6A	FE	40	9A	1C	00	00	00	1A	00	00	00	08	00	VMjþ@š
00000096	24	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	$
00000112	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	00	00	flag.txt
00000128	01	00	18	00	94	AD	20	93	13	6A	D4	01	BB	BA	27	B6	”- “ jÔ »°'¶
00000144	13	6A	D4	01	A5	C2	90	4B	0F	6A	D4	01	50	4B	05	06	jÔ ¥Â K jÔ PK
00000160	00	00	00	00	01	00	01	00	5A	00	00	00	42	00	00	00	Z B
00000176	00	00															

改成00试下

flag.zip

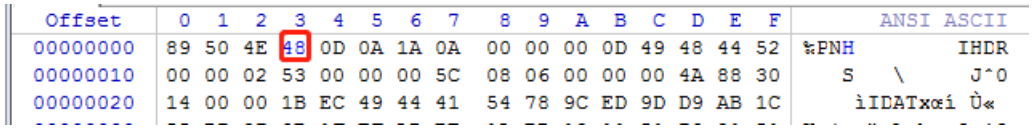
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	50	4B	03	04	14	00	01	00	08	00	A0	B3	56	4D	6A	FE	PK ³VMjþ
00000016	40	9A	1C	00	00	00	1A	00	00	00	08	00	00	00	66	6C	@š fl
00000032	61	67	2E	74	78	74	4B	CB	49	4C	AF	4E	B6	30	36	B1	ag.txtKËII¯N¶06±
00000048	48	4C	4B	31	4D	36	37	4F	36	37	34	4F	34	B0	34	AF	HLK1M67O674O4°4¯
00000064	05	00	50	4B	01	02	1F	00	14	00	00	00	08	00	A0	B3	PK ³
00000080	56	4D	6A	FE	40	9A	1C	00	00	00	1A	00	00	00	08	00	VMjþ@š
00000096	24	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	$
00000112	66	6C	61	67	2E	74	78	74	0A	00	20	00	00	00	00	00	flag.txt
00000128	01	00	18	00	94	AD	20	93	13	6A	D4	01	BB	BA	27	B6	”- “ jÔ »°'¶
00000144	13	6A	D4	01	A5	C2	90	4B	0F	6A	D4	01	50	4B	05	06	jÔ ¥Â K jÔ PK
00000160	00	00	00	00	01	00	01	00	5A	00	00	00	42	00	00	00	Z B
00000176	00	00															

嗯，能打开了

flag{c8348afd5c77c717a097}

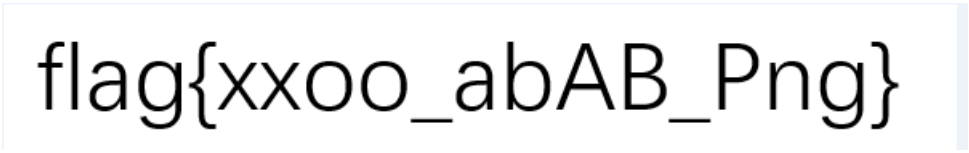
⑦打不开的图片

图片打不开
直接用winhex看



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	48	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNH IHDR
00000010	00	00	02	53	00	00	00	5C	08	06	00	00	00	4A	88	30	S \ J^0
00000020	14	00	00	1B	EC	49	44	41	54	78	9C	ED	9D	D9	AB	1C	ìIDATxœí Ù«

发现png文件头格式不对，改成47就可以打开了



flag{xxoo_anAB_Png}

⑩0101

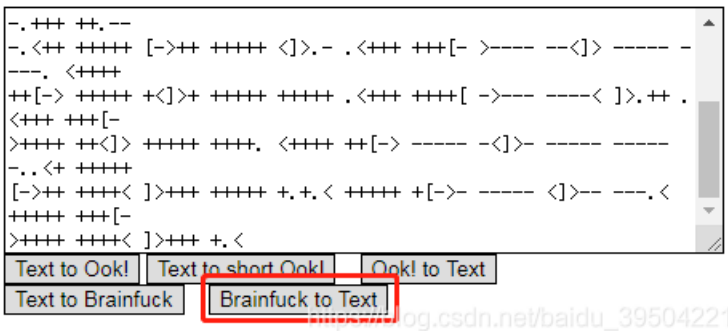
```
01100110011011000110000101100111011110110110001001101001010011100101111101110011001100000111101
```

拿到一串二进制，直接转换16进制
666c61677b62694e5f73307d
再转换为字符串
flag{biN_s0}

⑪BF

```
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[ ->+++ +<]>+ +++.< +++++ +++[- >---- ----< ]>--- ----- -.--. .+++.
--.++ +++++ .<+++ +++[- >++++ ++<]> +++++ ++.<+ +++++ +[->- ----- -<]>-
.<+++ ++++[ ->+++ ++++< ]>+++ +.<++ +++++ [->-- ----- <]>-- -.+++ ++.--
-.<++ +++++ [->++ +++++ <]>.- .<+++ +++[- >---- --<]> ----- ----. <++++
++[-> +++++ +<]>+ +++++ +++++ .<+++ ++++[ ->--- ----< ]>.++ .<+++ +++[-
>++++ ++<]> +++++ ++++. <++++ ++[-> ----- -<]>- ----- ----- -..<+ +++++
[->++ ++++< ]>+++ +++++ +.+.< +++++ +[->- ----- <]>-- ---.< +++++ +++[-
>++++ ++++< ]>+++ +.<
```

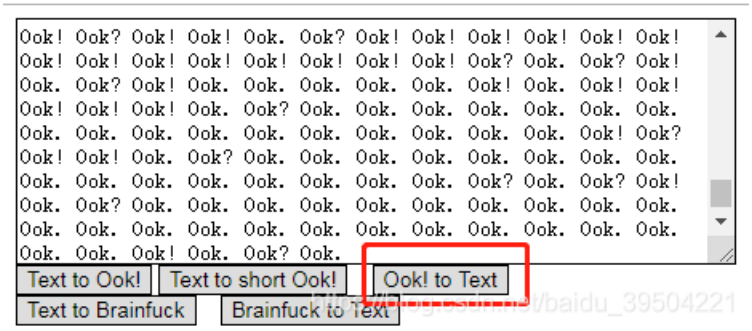
一段密码
工具
http://tool.bugku.com/brainfuck/?wafcloud=1



flag{200318c1f274ed7f57d44ab9}

⑫Okok!

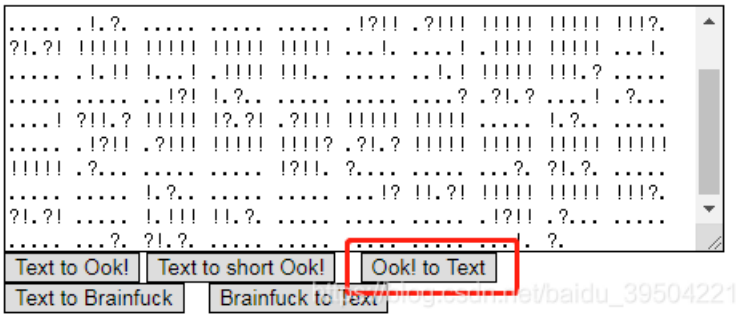
和十一题一样，丢进去跑一下



flag{1240143444fd5fd6266b131}

⑬奇怪的字符

一样的套路

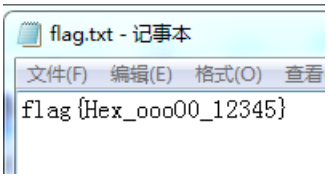


flag{12401434151sdf6b131}

⑰Hex

```
50 4B 03 04 14 00 01 00 08 00 90 61 59 4D 14 98
4C 29 17 00 00 00 15 00 00 00 08 00 00 00 66 6C
61 67 2E 74 78 74 4B CB 49 4C AF F6 48 AD 88 CF
CF CF F7 37 88 37 34 32 36 31 AD 05 00 50 4B 01
02 1F 00 14 00 01 00 08 00 90 61 59 4D 14 98 4C
29 17 00 00 00 15 00 00 00 08 00 24 00 00 00 00
00 00 00 20 00 00 00 00 00 00 00 66 6C 61 67 2E
74 78 74 0A 00 20 00 00 00 00 00 01 00 18 00 37
B7 FD F3 18 6C D4 01 9C BB FA F3 18 6C D4 01 34
07 CB DF 18 6C D4 01 50 4B 05 06 00 00 00 00 01
00 01 00 5A 00 00 00 3D 00 00 00 00 00
```

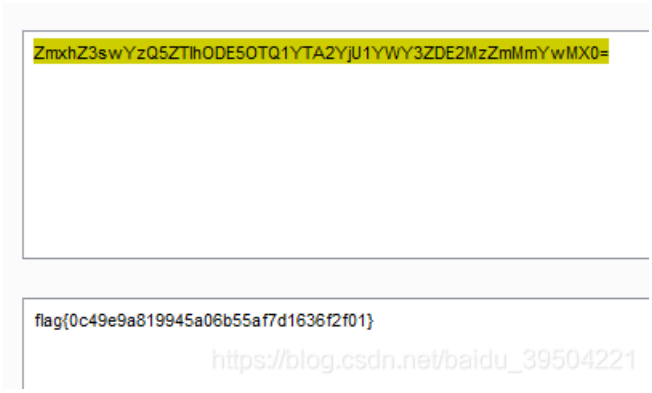
给了这样一块hex
在winhex里新建一个文件
文件头是50 4B 03 04 ， 是个zip文件，改后缀后打开
发现flag.txt加密了
没什么提示，猜想是伪加密
照第六题方法将01改成00



flag{Hex_oooO0_12345}

⑱㉑N次base

这两题一样， burpsuite >>decoder>>base64



flag{0c49e9a819945a06b55af7d1636f2f01}

连答案也是一样的…

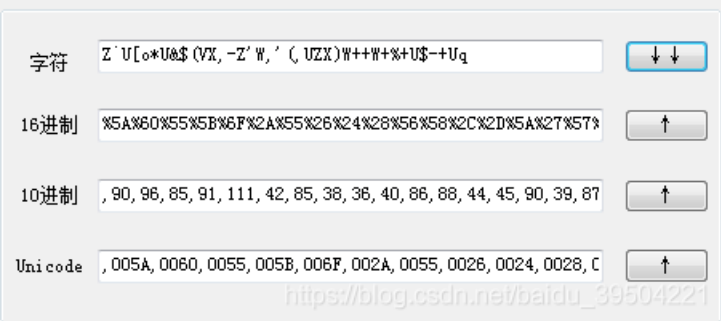
⑳凯撒

这题应该放到Crypto

```
Z`U[o*U&$(VX,-Z'W,'(,UZX)W++W+%+U$-+Uq
```

```
Z 90 f 102  12
` 96 l 108  12
U 85 a 97   12
```

前三个字符的ASCII码都与 fla 差12，推测规律就是向后移12
先用工具将字符的ASCII码转成十进制

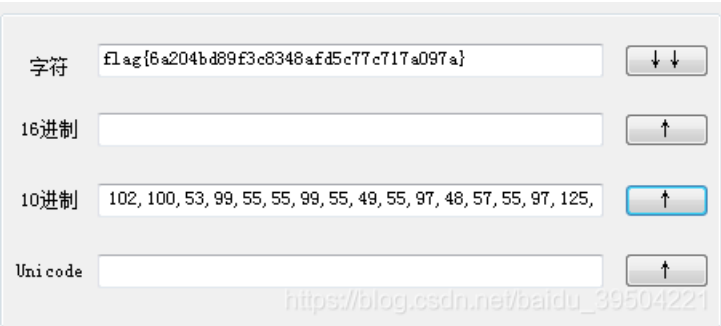


写个c将他们都往后推12

```c
#include<stdio.h>
int main()
{
 int a[38]={90,96,85,91,111,42,85,38,36,40,86,88,44,45,90,39,87,44,39,40,44,85,90,88,41,87,43,43,87,43,37,43,85,
36,45,43,85,113};
 int j;
 for(j=0;j<38;j++){
  a[j]=a[j]+12;
  printf("%d,",a[j]);
 }

 return 0;
}
```

再放入工具转换就行了



flag{6a204bd89f3c8348afd5c77c717a097a}

> 少说话，多做事