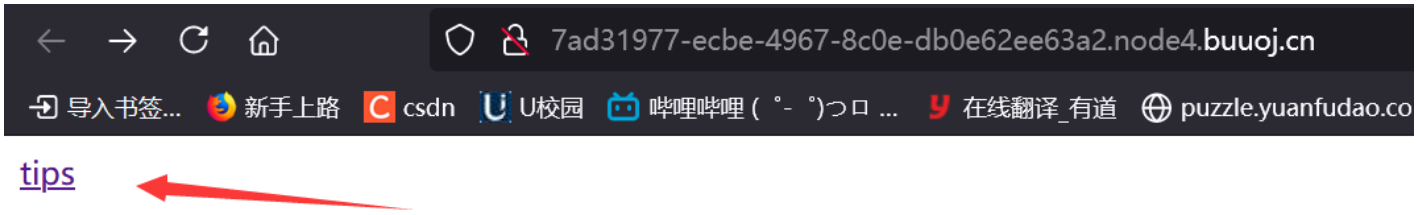
BUU【ACTF2020 新生赛】Include 1 解题大致思路

原创

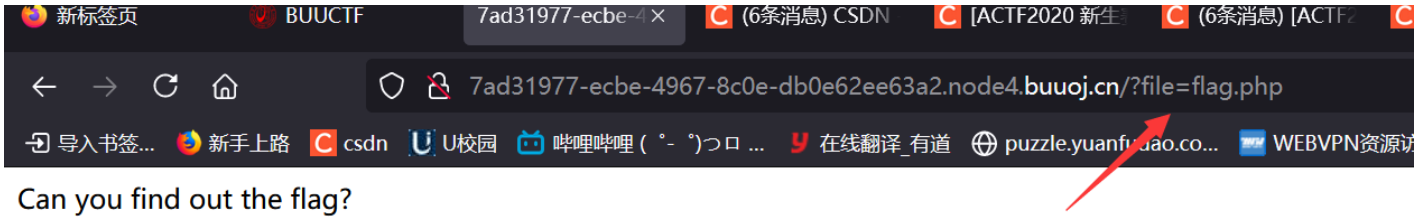
陆北_ 于 2021-07-14 17:41:13 发布 236 收藏 4
分类专栏： CTF 文章标签： web php 安全

本文链接：https://blog.csdn.net/qq_54786552/article/details/118732644

1.首先打开靶场环境 看到链接tips 打开tips



2.首先看一下url中有什么东西 看到file 猜测可能是文件包含

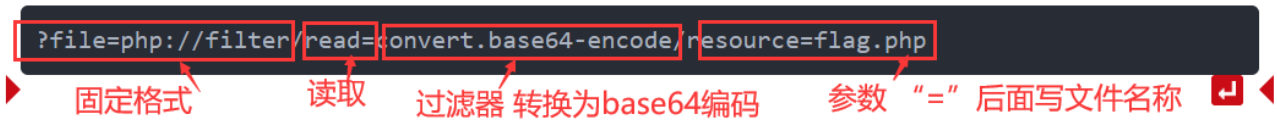


3.文件包含读取的是他文件里的内容， 要想读取源文件内容，我们可以用base64编码的方式来读文件flag.php。

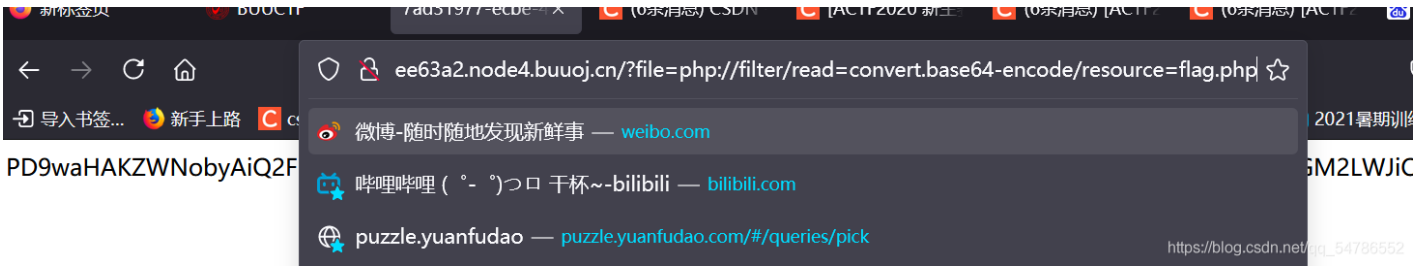
构造：

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

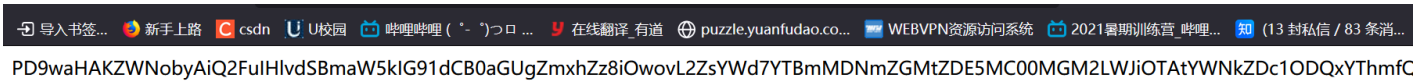
解释一下：url中有？file=flag.php 我们一开始的猜想是文件包含漏洞，可以用php://filter协议来读取源文件。



url的后缀改为以上代码：



可得到经过base64编码的flag.php的源文件代码：



3.然后我们就可以去度娘上找一下base64解码器，开开心心的解码拿到flag了。

4.看flag到手了！！！提交flag就完成了！！！

Ps.为什么我们要看源代码？flag.php中flag的那一行是被“//”注释掉的，看源码才可得到flag。