[ACTF2020 新生赛]Include

原创

月生ψ 于 2022-01-16 17:08:05 发布 2548 收藏

分类专栏： BUUCTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_46962006/article/details/122525091

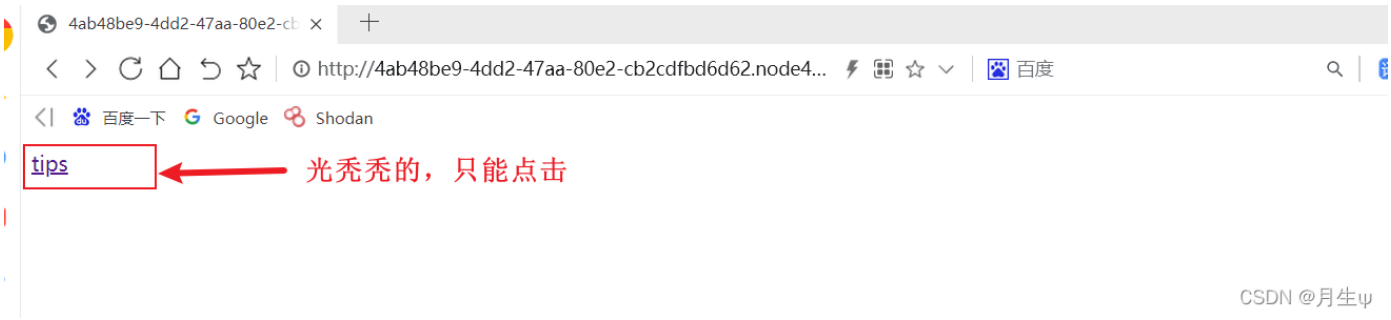
[ACTF2020 新生赛]Include

前言

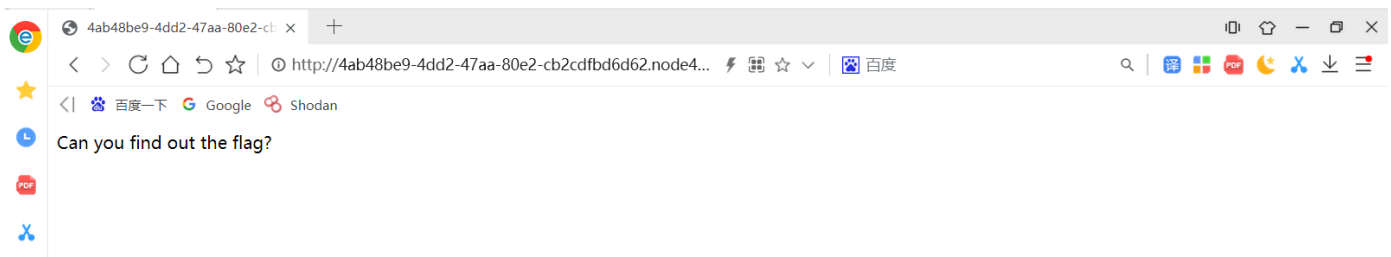
个人观点，若有误请指教

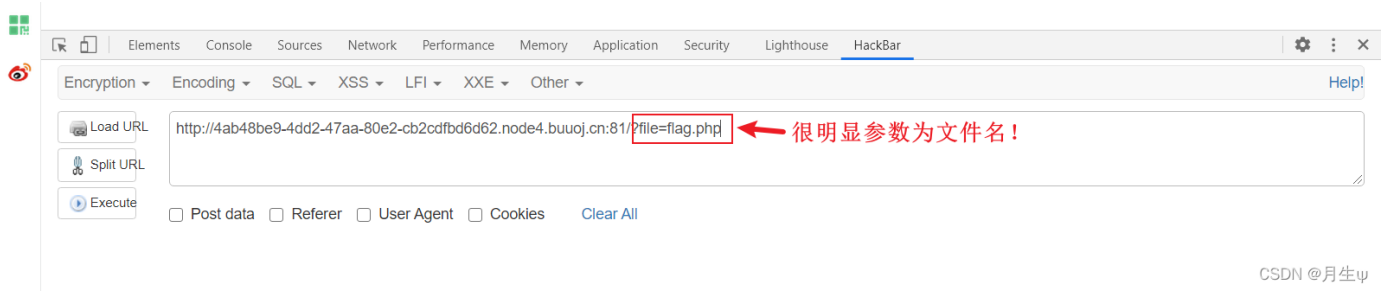
解题思路及步骤

- 判断是否为文件包含漏洞。（虽然题目已给出提示，但不是每道题都会给，还是要自己判断一下。）

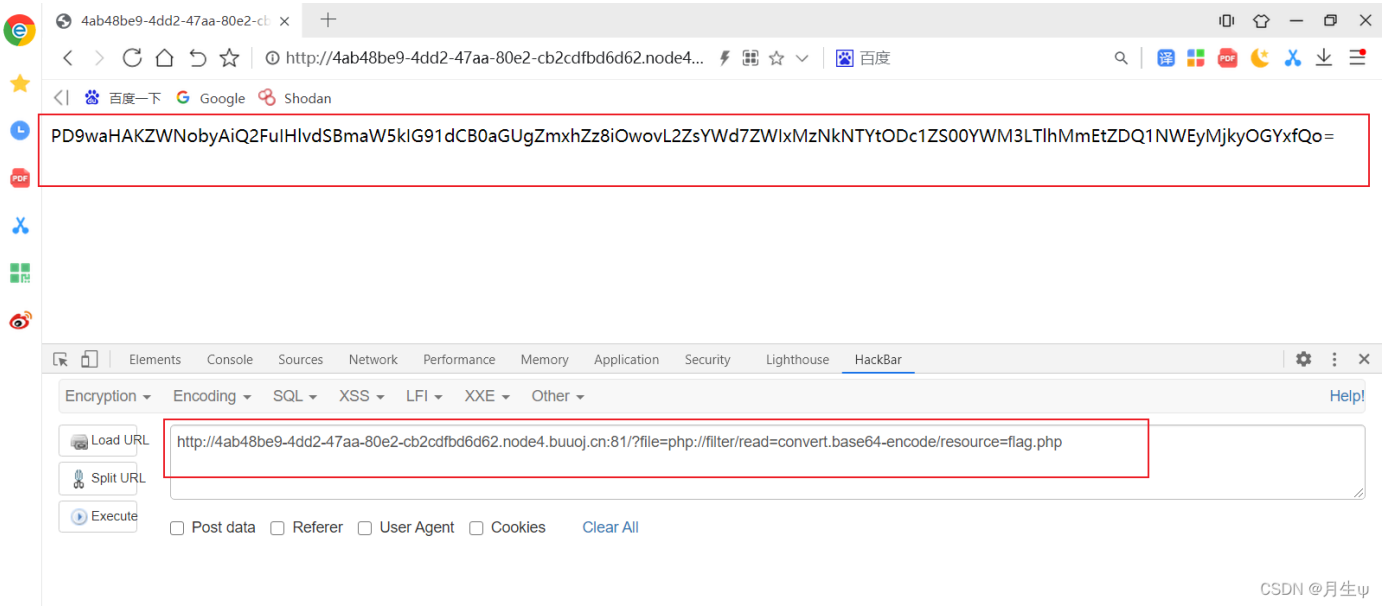


当参数是文件名时，即存在文件包含漏洞



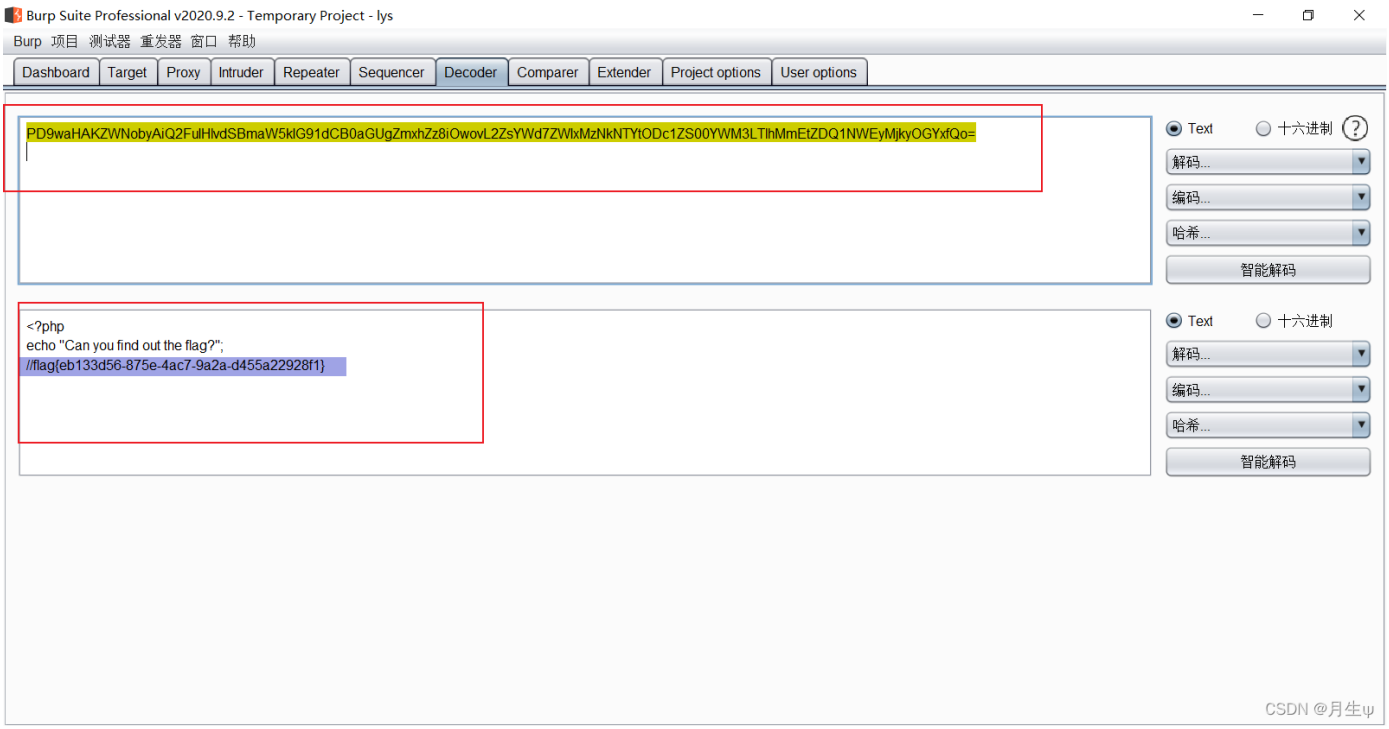


- 使用php://filter读取flag.php文件。（不要问为什么，问就是一个个试。□）



注：参数为php://filter/read=convert.base64-encode/resource=flag.php

读出来的数据是base64格式，需要将其解码



总结

- 本题难度不大，只需将常用的几个伪协议一个个试过去即可得出。
- 本题警示了我们不要忽略任何细节。本人之所以能解出来这道题，是因为实在没辙了。只能试试读取flag.php的源码，而不是主动的去想到这一点！