BUUCTF之[ACTF2020 新生赛]Include

原创

若丶时光破灭 于 2021-06-13 19:21:41 发布 93 收藏 1

分类专栏： CTF-WEB 文章标签： web 安全

本文链接：https://blog.csdn.net/weixin_44632787/article/details/117884379

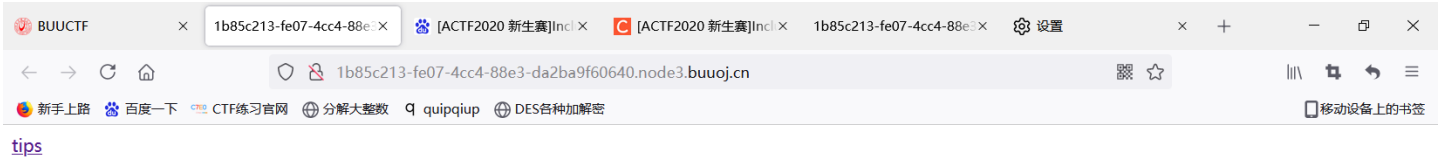
CTF-WEB 专栏收录该内容

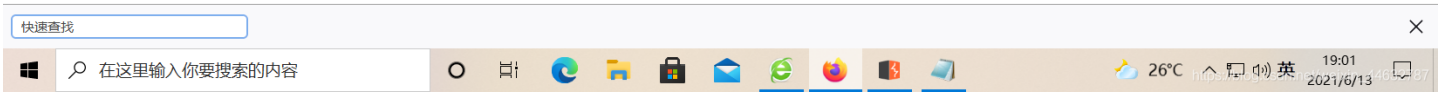
40 篇文章 1 订阅

订阅专栏

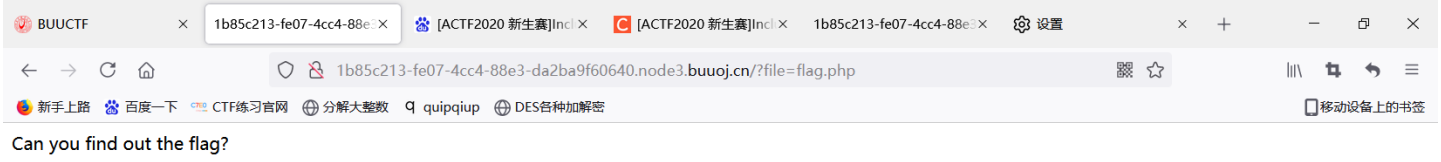
BUUCTF之[ACTF2020 新生赛]Include

启动项目，进入到我们的挑战页面



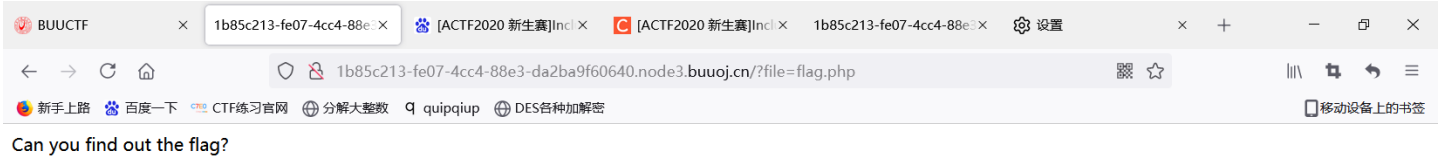


这个有个tips链接，点开它

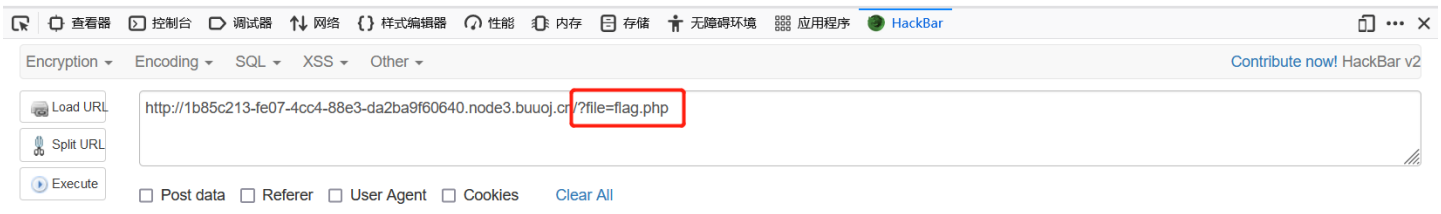


发现并没有什么可用的信息，然后试试右键打开源代码和访问robots.txt协议都没有看到什么特别的信息。然后就开始想是不是该用dirsearch扫描一下这个网址看看可不可以扫描出什么来。但是又返回到题目去，看到了Include这个字眼。就想起了，这个题目可能是和文件包含相关。。。

打开火狐的Hackbar，导入链接emmmmmmmmmm

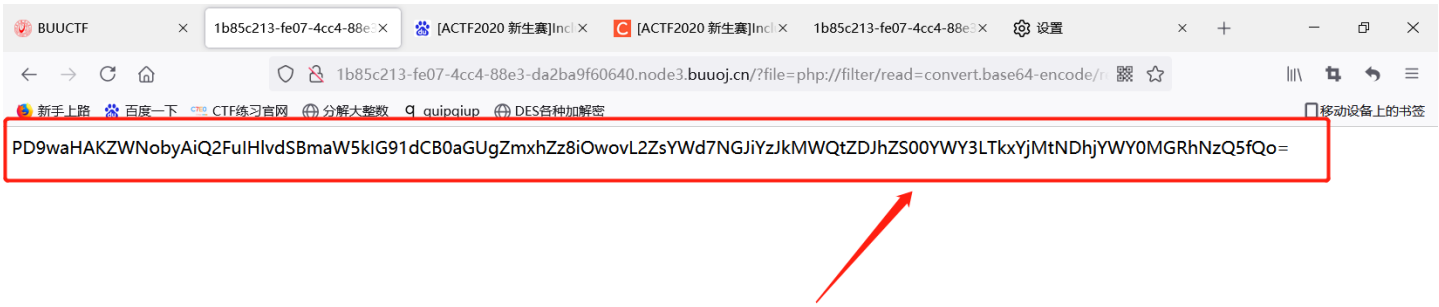


打开火狐的Hackbar，发现这个。果然真的很像是文件包含的题目。于是开始从这里入手



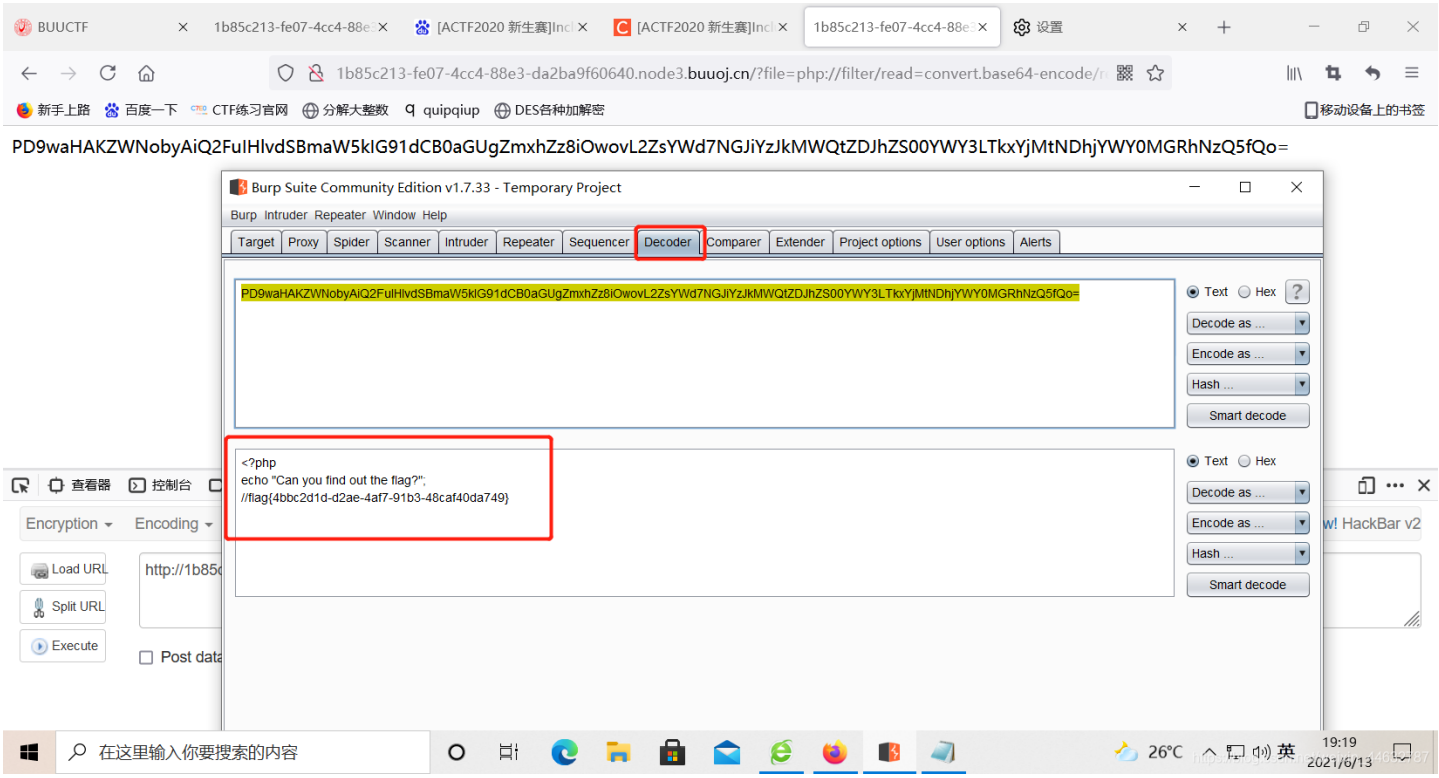
好的，那么现在开始输入文件包含里经常用到的方法吧！

http://1b85c213-fe07-4cc4-88e3-da2ba9f60640.node3.buuoj.cn/?**file=php://filter/read=convert.base64-encode/resource=flag.php**



访问这个链接后发现它返回这个信息，这个看起来很像是base64加密的数据（CTF里很喜欢用base64来加密数据吧，我觉得.....）。再说，后面出现的那个等于号就像是故意告诉你这个减少base64加密

所以我们把这个复制下来，然后放到BurpSuite下的Decoder的模块下进行解密。（那里有base64的加解密的功能）



然后就可以得到我们的Flag：flag{4bbc2d1d-d2ae-4af7-91b3-48caf40da749}

创作打卡挑战赛