

# 【学习笔记9】 buu [ACTF2020 新生赛]Include

原创

Noslpum 于 2020-05-06 18:33:12 发布 64 收藏

分类专栏: [ctf 学习笔记](#) 文章标签: [php](#) [java](#) [thinkphp](#) [安全](#) [web](#)

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/weixin\\_43553654/article/details/107686920](https://blog.csdn.net/weixin_43553654/article/details/107686920)

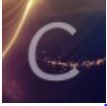
版权



ctf同时被 2 个专栏收录

47 篇文章 1 订阅

订阅专栏



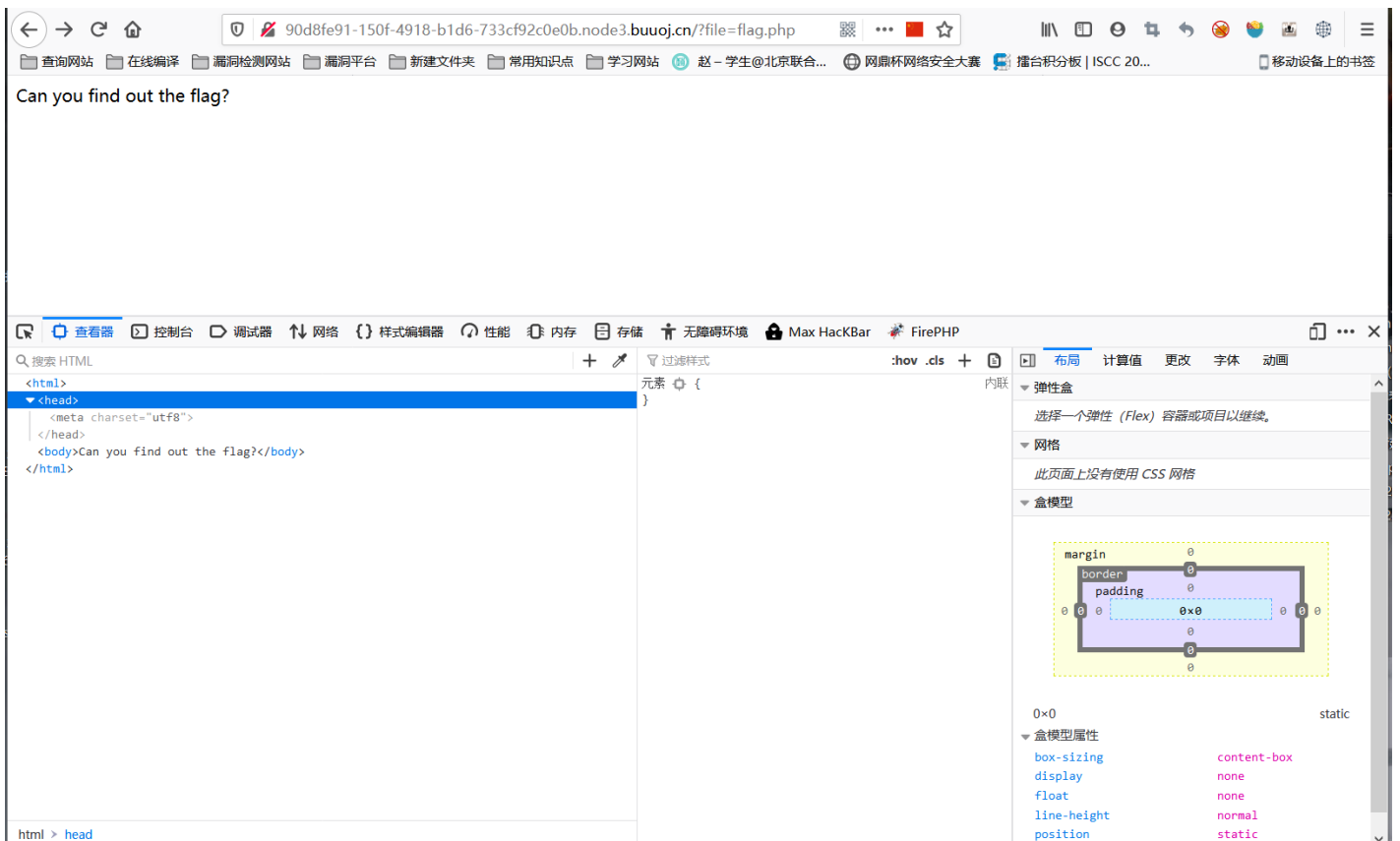
学习笔记

50 篇文章 0 订阅

订阅专栏

点进去一看, tip让你点击一下

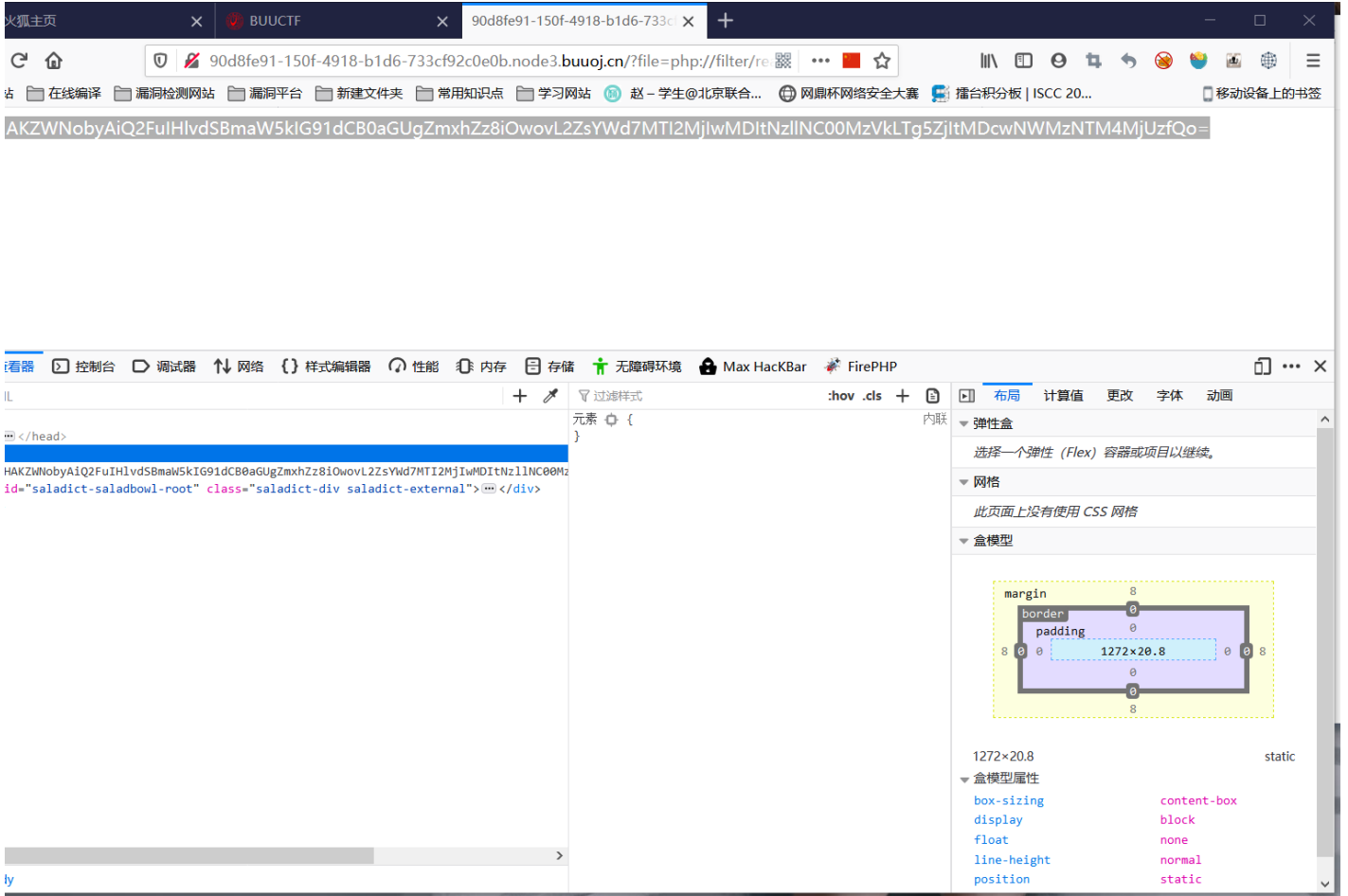
ok, 点一下



先查看一下源码, 什么都没有, 看到上面的file=flag.php,还用想, 这不就是经典php://filter伪协议的利用吗, 首先(注:知识点) php://filter当它与包含函数结合时, php://filter流会被当作php文件执行。所以我们一般对其进行编码, 阻止其不执行。从而导致任意文件读取。进行尝试首先直接读取

php://filter/read=flag.php

ok,失败，果然还是得进行编码后读取



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

得到一串flag.php页面用base64加密的源码，解密一下得到flag



[创作打卡挑战赛](#)  
[赢取流量/现金/CSDN周边激励大奖](#)