




BUUCTF: [RootersCTF2019]babyWeb

原创

末初  于 2020-08-02 17:18:18 发布  794  收藏

分类专栏: [CTF_WEB_Writeup](#) 文章标签: [BUUCTF](#) [babyWeb](#) [RootersCTF2019](#)

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/mochu7777777/article/details/107747352>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

题目地址: [https://buuoj.cn/challenges#\[RootersCTF2019\]babyWeb](https://buuoj.cn/challenges#[RootersCTF2019]babyWeb)

Challenge

57 Solves



[RootersCTF2019]babyWeb 70

<https://gitlab.com/0xCC00FFEE/RootersCTF2019-challenges>

Instance Info

Remaining Time: 9830s

Lan Domain: 4503-59f13755-e210-4e7e-ad70-
e1a7d67e543b

[http://59f13755-e210-4e7e-ad70-
e1a7d67e543b.node3.buuoj.cn](http://59f13755-e210-4e7e-ad70-
e1a7d67e543b.node3.buuoj.cn)

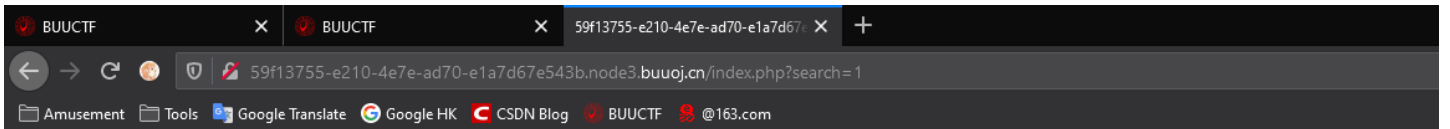
Destroy this instance

Renew this instance

Flag

Submit

<https://blog.csdn.net/mochu777777>

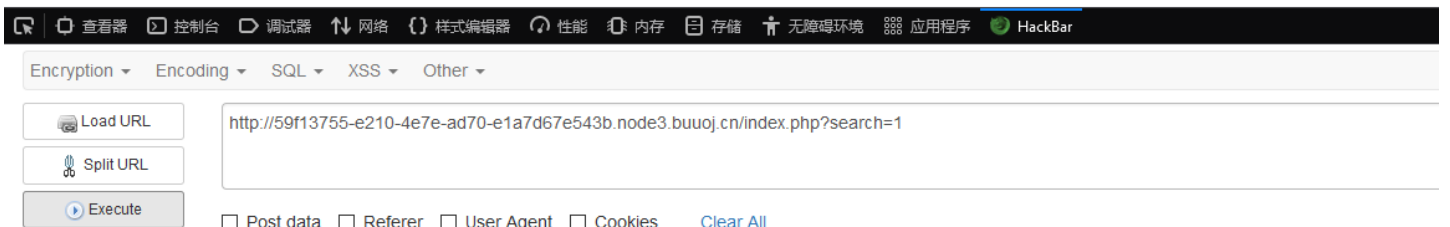


`SELECT * FROM users WHERE uniqueid=1`

This page is protected by super strong password with 18 digit numeric characters

banned words and characters UNION SLEEP ' " OR - BENCHMARK

Enter unique id:



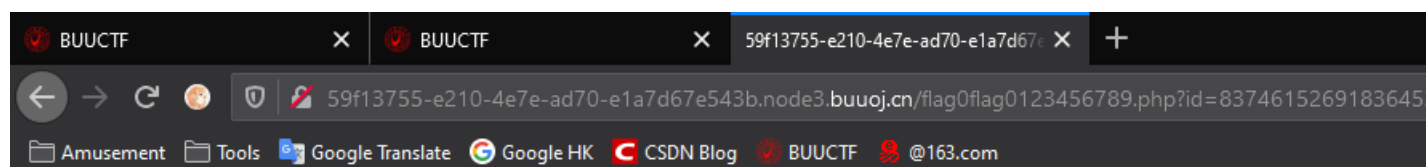
SQL查询, 过滤了: `union`、`sleep`、`'`、`"`、`or`、`-`、`benchmark`

`order by` 测试字段数, 发现当 `order by 2` 时返回正常 `order by 3` 返回没有这个字段, 确定为两个字段, 一个为 `uniqueid` 另一个应该就是flag

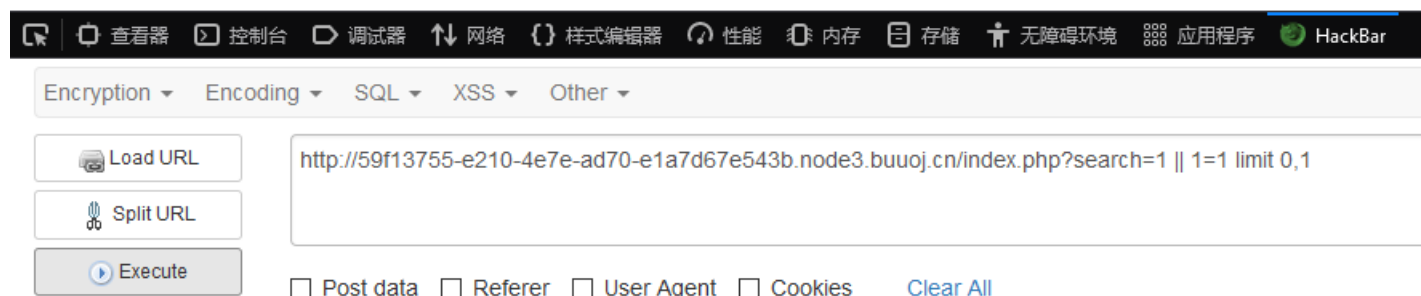
<https://blog.csdn.net/mochu777777>

那么应该就是输入id判断登录，即可，尝试万能密码登录：`1 || 1=1 limit 0,1`

返回flag



flag{74115ee9-7586-4b28-b822-f6c2701cf1b0}



<https://blog.csdn.net/mochu777777>