

XCTF-WEB

原创

超负荷小生  于 2019-06-22 01:15:16 发布  358  收藏 1

分类专栏: [ctf秃头路](#)

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_43661408/article/details/93258262

版权



[ctf秃头路](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

post和get

题目链接: <http://111.198.29.45:34348/>

解题思路

首先使用 `get` 方式提交变量 `a` 等于 1

即 <http://111.198.29.45:34348/?a=1>

得到 第二条信息 需要使用 `post` 提交一个变量 `b` 值为 2

因此使用火狐自带的插件 `hackbar`, 但是现在火狐更新后不能使用了, 替代 `hackbar` 的插件有了 `Max hackbar` 和 `hackbar quantum`, 使用方法和 `hackbar` 相同

SQL ▾ WAF ▾ XSS ▾ LFI ▾ Encryption ▾ Encoding ▾

 Load URL

<http://111.198.29.45:34348/?a=1>

 Spit URL

 Execution

Post Data **Referrer** **Moded By Mr.silent coder**

Post data

[b=2](https://blog.csdn.net/qq_43661408)
https://blog.csdn.net/qq_43661408

提交以后就能获得这个题目的flag