Linux下sql_labs第七关,SQL注入之Sqli-labs系列第二十七关（过滤空格、注释符、union select）和第二十七A...

转载

李战阳 于 2021-05-16 16:36:01 发布 106 收藏
文章标签： Linux下sql_labs第七关

开始挑战第二十七关(Trick with SELECT & UNION)

第二十七A关(Trick with SELECT & UNION)

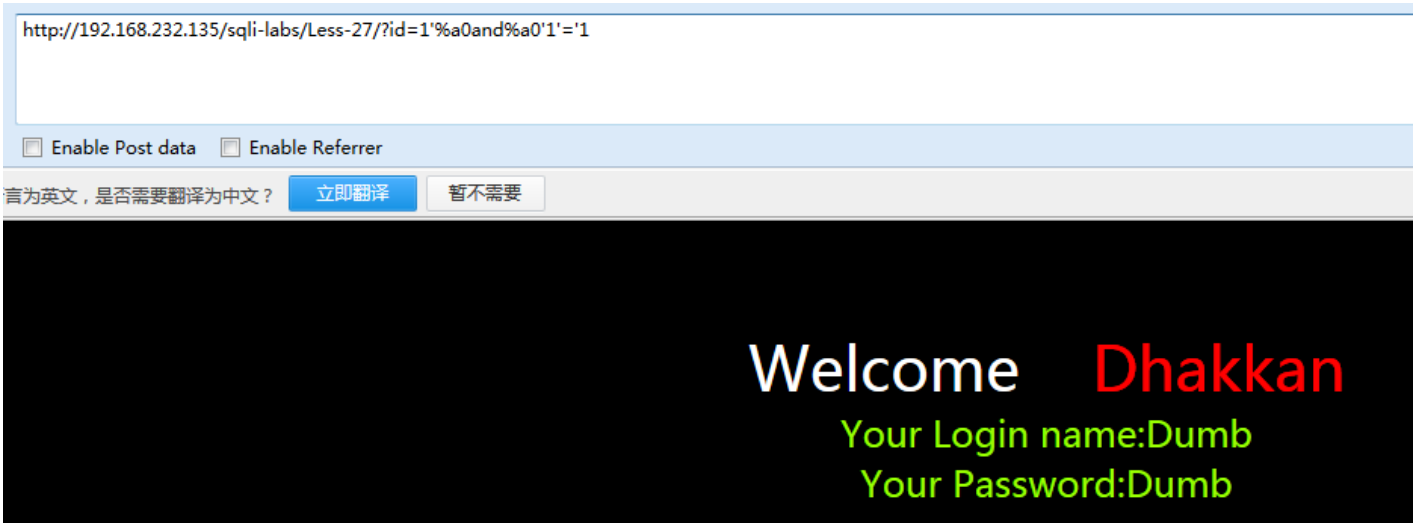
0x1看看源代码

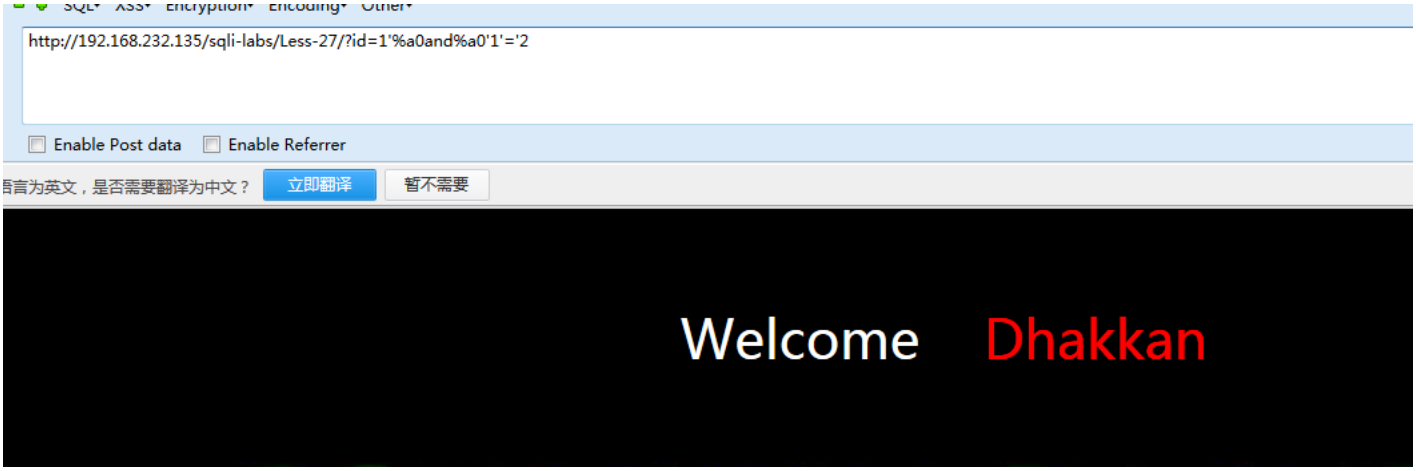
(1)与26关一样，这次去除了逻辑运算符添加了union seclet。

```
6
7  function blacklist($id)
8  {
9  $id= preg_replace('/[\/\*]/',"", $id);       //strip out /*
0  $id= preg_replace('/[--]/',"", $id);         //Strip out --.
1  $id= preg_replace('/[#]/',"", $id);          //Strip out #.
2  $id= preg_replace('/[ +]/',"", $id);         //Strip out spaces.
3  $id= preg_replace('/select/m',"", $id);      //Strip out spaces.
4  $id= preg_replace('/[ +]/',"", $id);         //Strip out spaces.
5  $id= preg_replace('/union/s',"", $id);       //Strip out union
6  $id= preg_replace('/select/s',"", $id);      //Strip out select
7  $id= preg_replace('/UNION/s',"", $id);       //Strip out UNION
8  $id= preg_replace('/SELECT/s',"", $id);      //Strip out SELECT
9  $id= preg_replace('/Union/s',"", $id);       //Strip out Union
0  $id= preg_replace('/Select/s',"", $id);      //Strip out select
1  return $id;
2  }
3
```

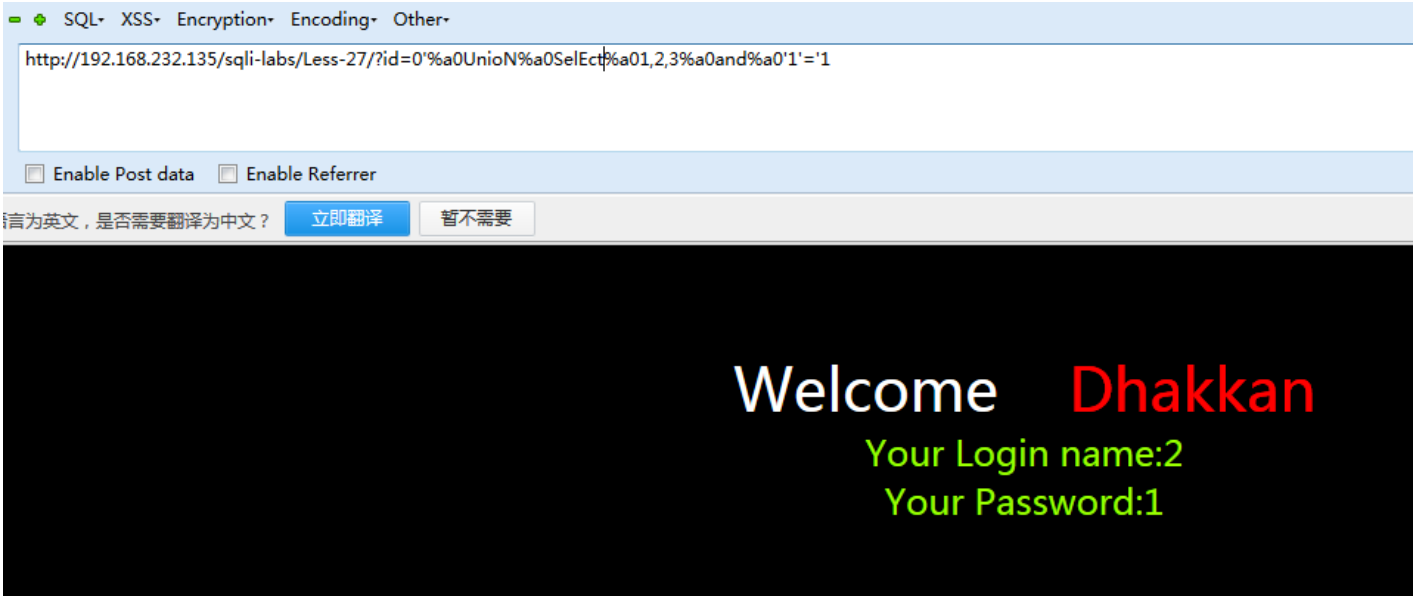
0x2测试

(1)同样利用26关的方式，采取%a0来代替空格

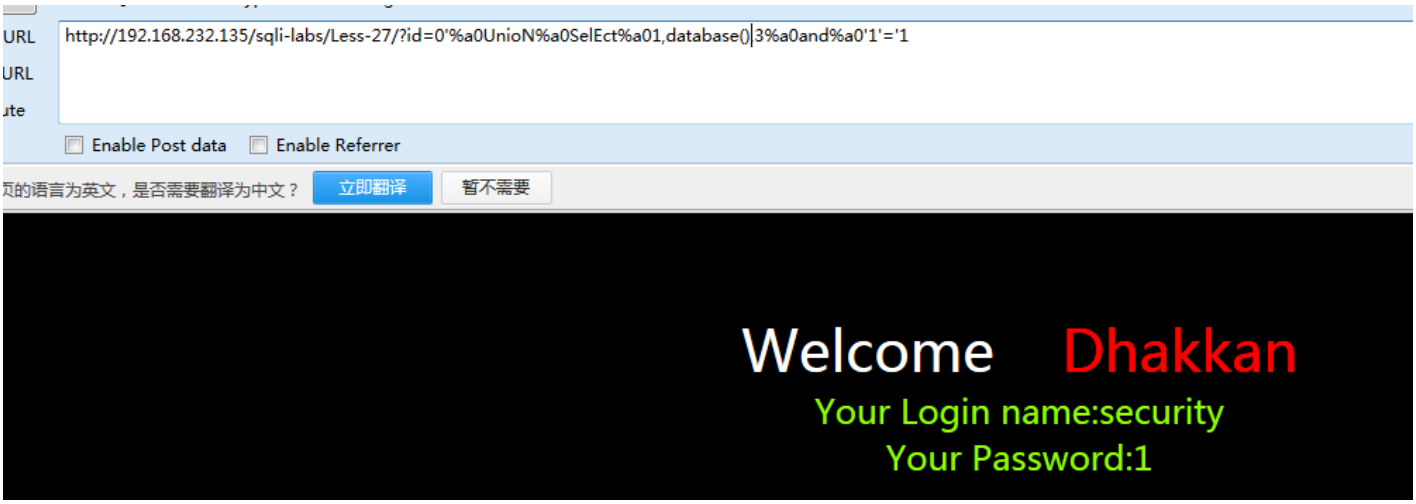




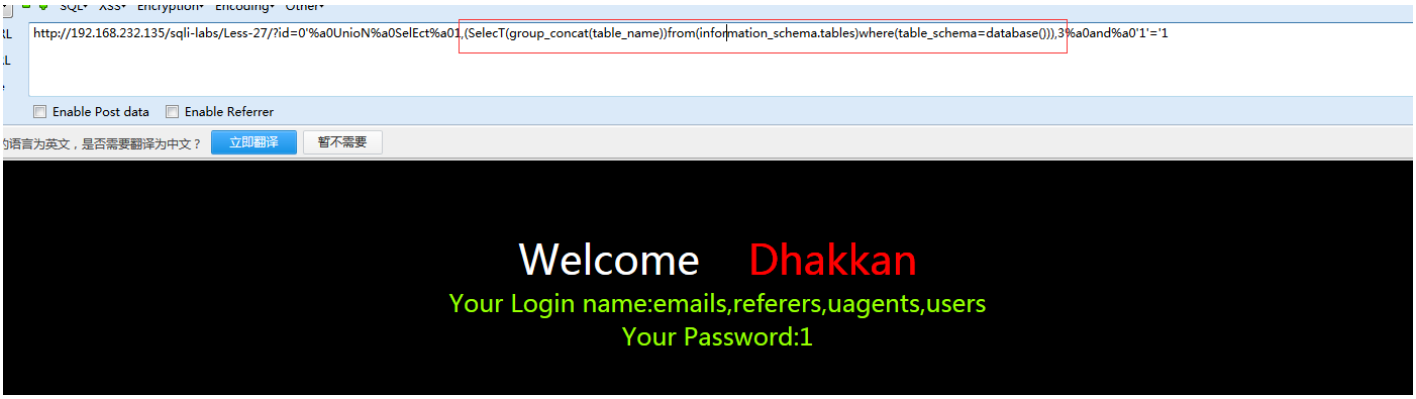
(2) 这里过滤了union select ， 所以我们采用大小写方式去绕过，双写是不行的



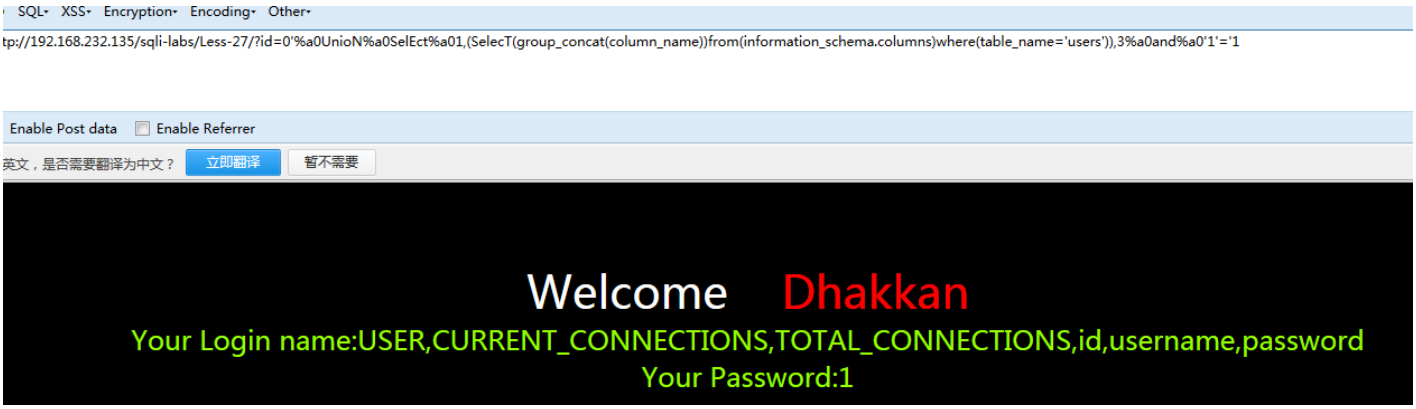
(3)获取数据库



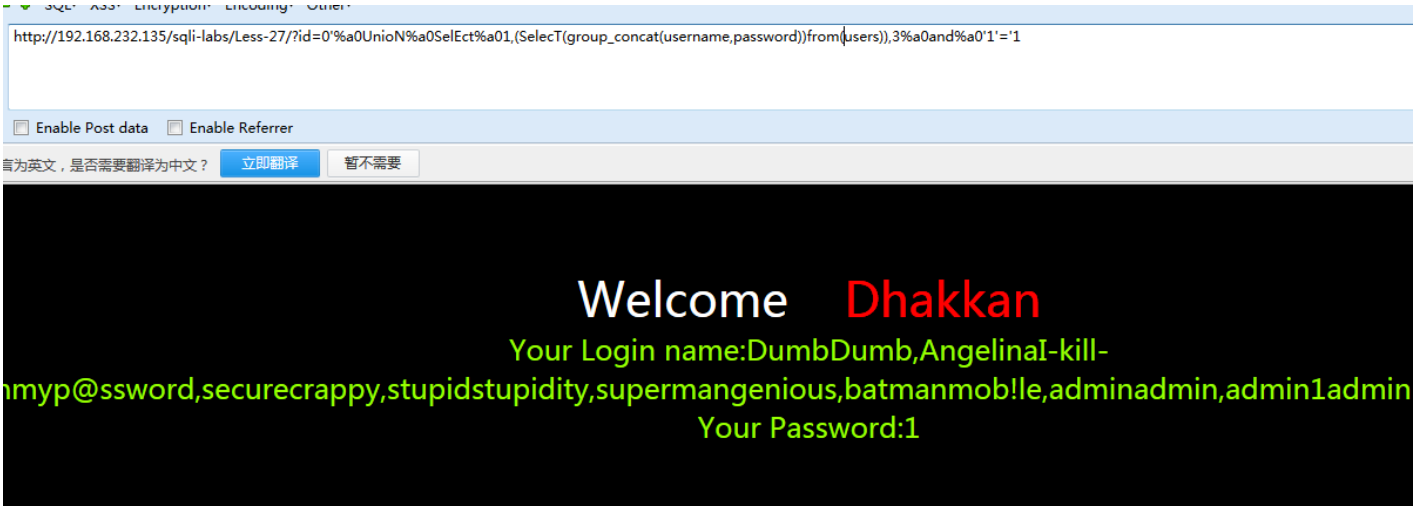
(4)获取表,查询语句的空格我们采用()来绕过



(5)获取字段名



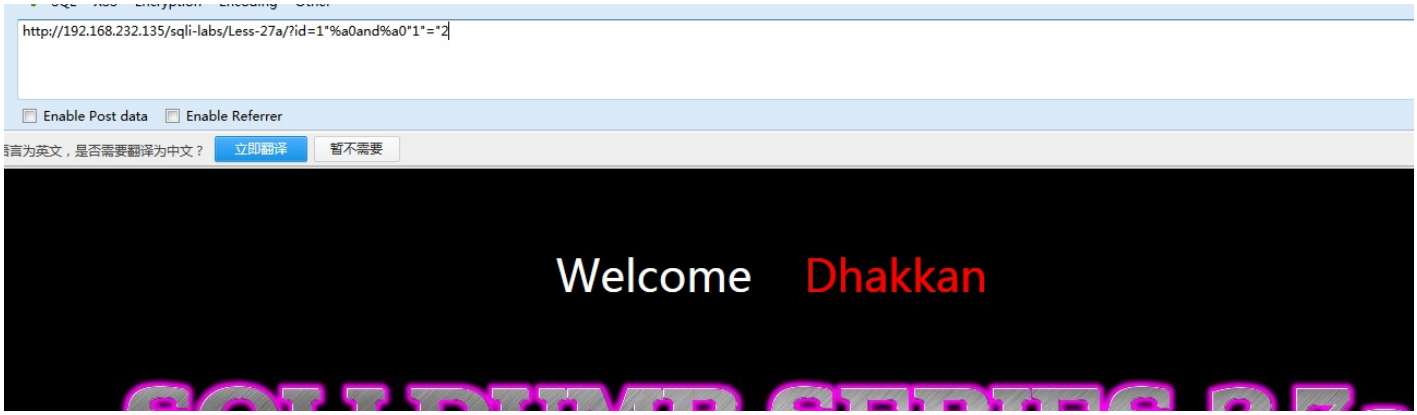
(6)获取数据



第二十七A是同样的，只是采用了双引号进行闭合，这里我就不演示了，方法和上面一样

```
        $nint=$id;
        $id = '"' .$id. '"';

// connectivity
        $sql="SELECT * FROM users WHERE id=$id LIMIT 0,1";
        $result=mysql_query($sql);
        $row = mysql_fetch_array($result);
        if($row)
        {
            echo "<font size='5' color= '#99FF00'>";
```



Sqli labs系列-less-4 这关好坑！！！

这章,可能我总结开会比较长,图比较多,因为,我在做了一半,走进了一个死胡同,脑子,一下子没想开到底为啥.... 然后我自己想了好长时间也没想开,我也不想直接就去看源码,所以就先去百度了一下,结果一下子 ...

SQL注入之Sqli-labs系列第二十五关(过滤 OR & AND)和第二十五A关(过滤逻辑运算符注释符)

开始挑战第二十五关(Trick with OR & AND) 第二十五关A(Trick with comments) 0x1先查看源码 (1)这里的or和and采用了i正则匹配,大小写都无法绕 ...

Sqli labs系列-less-3 。。。

原本想着找个搜索型的注入玩玩,毕竟昨天被实力嘲讽了 = = . 找了好长时间,我才发现,我没有 = = ,网上搜了一个存在搜索型注入的源码,我看了好长时间,楞没看出来从哪里搜索注入了....估计是我太 ...

Sqli labs系列-less-2 详细篇

就今天晚上一个小插曲,瞬间感觉我被嘲讽了. SQL手工注入这个东西,杂说了吧,如果你好久不玩的话,一时说开了,你也只能讲个大概,有时候,长期不写写,你的构造语句还非常容易忘,要不我杂会被瞬间嘲讽了啊. ...

Sqli labs系列-less-1 详细篇

要说 SQL 注入学习,网上众多的靶场,就属 Sqli labs 这个系列挺不错的,关卡达到60多关了,我自己也就打了不几关,一个挺不错的练习SQL注入的源码. 我一开始就准备等我一些原理篇总结完了, ...

Sqli labs系列-less-5&6 报错注入法(上)

在我一系列常规的测试后发现,第五关和第六关,是属于报错注入的关卡,两关的区别是一个是单引号一个是双引号...当然我是看了源码的.... 基于报错注入的方法,我早就忘的差不多了,,,我记的我最后一次基于 ...

Sqli labs系列-less-5&6 报错注入法(下)

我先输入 ' 让其出错. 然后知道语句是单引号闭合. 然后直接 and 1=1 测试. 返回正常,再 and 1=2 . 返回错误,开始猜表段数. 恩,3位.让其报错,然后注入... 擦,不错出,再加 ...

Java代码审计连载之—SQL注入

前言近日闲来无事,快两年都没怎么写代码了,打算写几行代码,做代码审计一年了,每天看代码都好几万行,突然发现自己都不会写代码了,真是很DT.想当初入门代码审计的时候真是非常难,网上几乎找不到什么java ...

SQLI LABS Basic Part(1-22) WriteUp

好久没有专门练SQL注入了,正好刷一遍SQLI LABS,复习巩固一波~ 环境: phpStudy(之前一直用自己搭的AMP,下了这个之后才发现这个更方便,可以切换不同版本的PHP,没装的小伙伴赶紧试 ...

代码审计之SQL注入

0x00概况说明 0x01报错注入及利用 环境说明 kali LAMP 0x0a 核心代码 现在注入的主要原因是程序员在写sql语句的时候还是通过最原始的语句拼接来完成,另外SQL语句有Select. ...

随机推荐

Win7硬盘整数分区一览表

10G=10245 MB 20G=20482 MB 30G=30726 MB 40G=40963 MB 50G=51208 MB 60G=61444 MB 70G=71681 MB 80G=81926 ...

ls命令

ls(list) 命令可以说是Linux下最常用的命令之一 #ls -l;列出文件的详细信息 #ll 以上两个命令一样,ll是ls -l的简写 #ls -al;列出目录下的所有文件,包括以 . 开头的 ...

ACM训练计划step 2 [非原创]

(Step2-500题)POJ训练计划+SGU 经过Step1-500题训练,接下来可以开始Step2-500题,包括POJ训练计划的298题和SGU前两章200题.需要1-1年半时间继续提高解决问题 ...

Jupyter Notebook通过latex输出pdf

主要步骤 1.将ipynb编译成tex ipython nbconvert --to latex Example.ipynb 2. 修改tex,增加中文支持 在 \documentclass{artic ...

Hadoop webHDFS设置和使用说明

1.配置 namenode的hdfs-site.xml是必须将dfs.webhdfs.enabled属性设置为true,否则就不能使用webhdfs的LISTSTATUS.LISTFILESTATUS ...

git命令的使用

git命令行的使用 0. 工作中常使用的命令行(小结) 假设我们工作共同使用的开发分支为dev,我自己的开发分支为dev_cx.安装git,在工作文件夹下打开git bash. $ git check ...

Golang Linux Shell编程(一)

1.调用系统命令 exec包执行外部命令,它将os.StartProcess进行包装使得它更容易映射到stdin和stdout,并且利用pipe连接i/o func Command(name stri ...

【转载】PhpStudy修改网站根目录

phpStudy是一个PHP调试环境的程序集成包.该程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer,一次性安装,无须配置即可使用,是非常方便.好用的 ...

Android中的各种访问权限Permission含义

android.permission.EXPAND_STATUS_BAR 允许一个程序扩展收缩在状态栏,android开发网提示应该是一个类似Windows Mobile中的托盘程序 android. ...

C# POS 小票打印

网上查了好多资料终于让我捣鼓出来了! public partial class Models_JXC_Sale_actNewSalePage : WebPartBase { public string ...