Writeup Blinded by the lighter

转载

weixin_34396902 于 2015-09-10 16:32:28 发布 50 收藏
文章标签： 数据库
原文链接：http://blog.51cto.com/1176518111/1693484

题目提示：

1. Again your mission is to extract an md5 password hash out of the database.

需要获取数据库中的密码信息，而密码是经过MD5加密的。

2. This time your limit for this blind sql injection are 33 queries.

最多可以注入33次。

3. Also you have to accomplish this task 3 times consecutively, to prove you have solved the challenge.

居然要连做三次才算成功，为什么。。。为什么。。。为什么。。。

4. 可以查看部分关键源代码，注入点居然还是这一句：

```
$query = "SELECT 1 FROM (SELECT password FROM blight WHERE sessid=$sessid) b WHERE password='$password'";
```

居然还有时间限制：

```
/** * Check if you were too slow.
    * @return true|false
    */
function blightTimeout(){
        if (false === ($start = GWF_Session::getOrDefault('BLIGHT2_TIME_START', false))){
            return true;
         }
         else{
             return (time() - $start) > BLIGHT2_TIME;
         }
}
```

实际做起来确实如此，时间稍微长一点就提示说太慢了，只好重来。。。

解题：

看别人的writeup提到可以通过sleep函数然后根据响应时间来判断

```
' or sleep(ord(substr(password,1,1)))
```

经过试验取ascii码来判断影响时间太长，由于本次字符限定在0-9，A-F之间因此将上面的判断语句改为如下，后面发现时间还是不够用于是除了个2，至于这里为什么减的是46各位自己思考吧，哈哈，个人感觉46最合适：

```
' or sleep((ord(substr(password,1,1))-46)/2)  #
```

OK，注入成功，那怎么判断延时的时间呢，这时候就需要通过firefox的firebug插件了，F12打开furebug，选择网络选项卡，选中HTML和保持两个选项，选择保持是为了把历史记录保存下来后统一查看，这样可以提高速度，清除选项就是清除历史记录。

好，现在开始了：

1. 重置题目execute a reset

2. 清除firebug历史记录

3. 从第一个字符开始注入直到第三十二个

4. 依次查看firebug中每次注入后响应时间，注意要把鼠标移动到时间线上在弹出的小窗上看最后一项接受数据的时间，时间小数位怎么取舍呢？以0.5为单位，超过部分舍去，比如0.76则认为是0.5

5. 提前准备好excel表格，计算char(x*2+46)，x即为响应时间

6. OK，整理好数据提交吧，是不是提示成功了，再重复两次步骤这题就搞定了。

转载于:https://blog.51cto.com/1176518111/1693484