Bugku web25 Writeup

原创

5mack 于 2021-04-27 17:30:01 发布 30 收藏

分类专栏： CTF 文章标签： sql

本文链接：https://blog.csdn.net/Code_Aape/article/details/116205981

Bugku web25 Writeup

题目描述

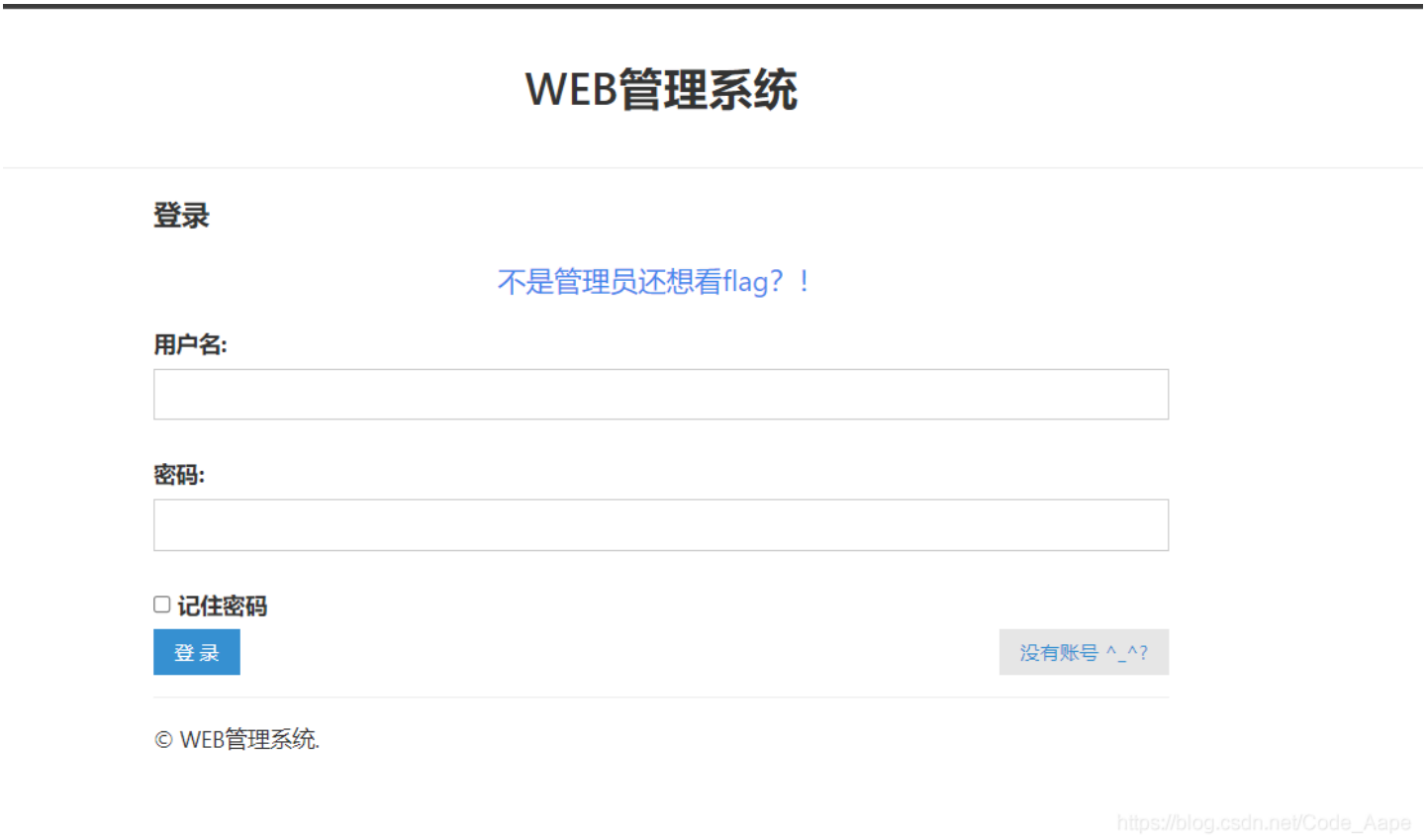
- hint:SQL约束攻击

分析

题目提示写得很清楚了，用到的是SQL约束攻击

尝试解题

先随便注册一个账号，然后尝试登陆看看他说啥：



那么就意味着，只要你是以admin账户登陆的，他就会给flag。

既然已经都给了SQL约束攻击的提示了，就不尝试弱口令爆破了，毕竟这玩意儿挺费时间的。

这里就需要用到SQL约束攻击来以任意身份登陆管理员。

那么这个SQL约束攻击是个啥呢？

原理

百度了大佬的讲解：[基于约束的SQL攻击 - FreeBuf网络安全行业门户]

关键：

> 在SQL中执行字符串处理时，字符串末尾的空格符将会被删除。换句话说“vampire”等同于“vampire ”，对于绝大多数情况来说都是成立的（诸如WHERE子句中的字符串或INSERT语句中的字符串）例如以下语句的查询结果，与使用用户名“vampire”进行查询时的结果是一样的。

解题姿势

看了原理，就很好理解了，只需要注册一个`admin[许多空白符]`的用户，然后登陆，就可以拿到flag。

这道题就注册一个`admin[空格]`，就行了。

面对其他情况，根据文章中所说：

> 对于选择的用户名，前25个字符应该只包含vampire和空白字符，这样做将有助于绕过检查特定用户名是否已存在的查询。

防御

顺便把防御姿势也摘抄MARK一下：

> 毫无疑问，在进行软件开发时，需要对此类安全漏洞引起注意。我们可采取以下几项措施进行防御：
>
> 将要求或者预期具有唯一性的那些列加上UNIQUE约束。实际上这是一个涉及软件开发的重要规则，即使你的代码有维持其完整性的功能，也应该恰当的定义数据。由于'username'列具有UNIQUE约束，所以不能插入另一条记录。将会检测到两个相同的字符串，并且INSERT查询将失败。
>
> 最好使用'id'作为数据库表的主键。并且数据应该通过程序中的id进行跟踪
>
> 为了更加安全，还可以用手动调整输入参数的限制长度（依照数据库设置）