通过SQL注入拿到管理员密码

原创

听风人24 于 2022-01-14 12:50:07 发布 2763 收藏
文章标签： sql web安全 安全

本文链接：https://blog.csdn.net/qq_52337463/article/details/122491605

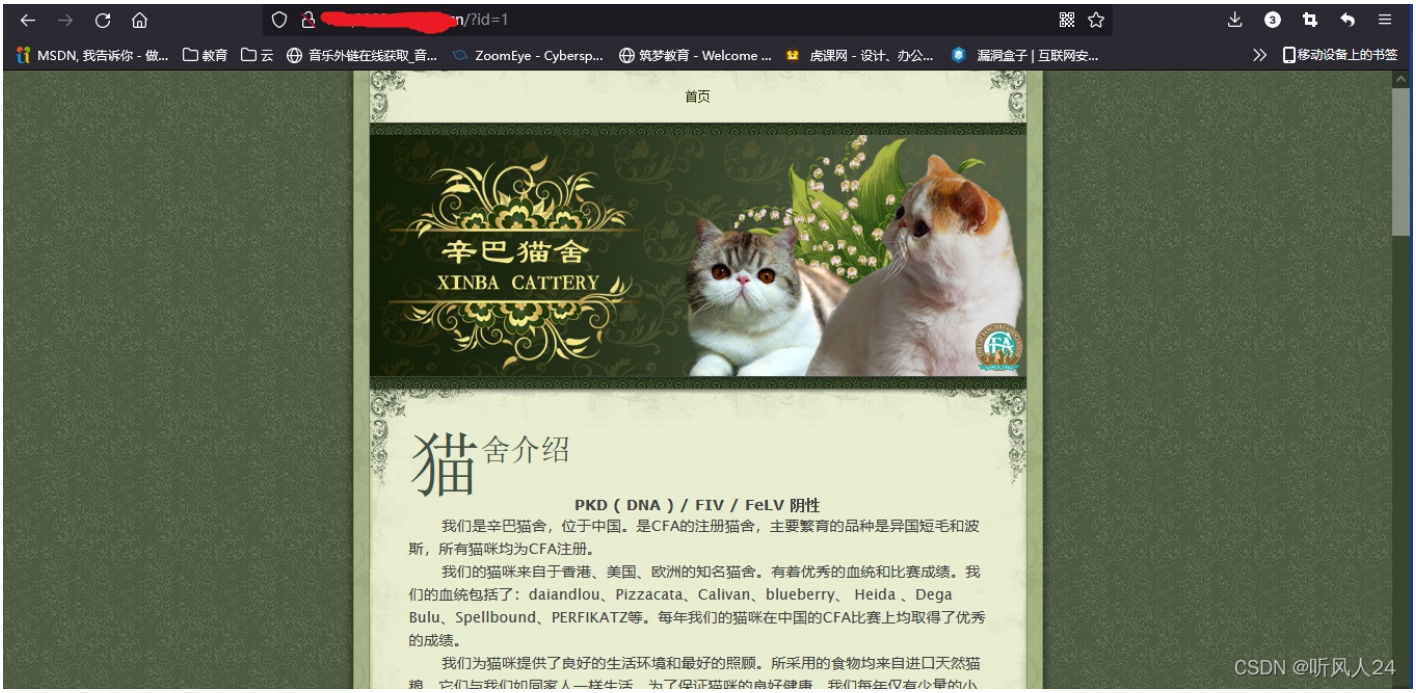
> 该靶场来自于(封神台封神台 - 掌控安全在线演练靶场，是一个在线黑客攻防演练平台。

首先我们看下题目

题目是通过SQL注入拿到管理员后台密码

我们先点开"传送门"打开靶场

靶场已经打开了,我们先点"点击查看新闻"打开页面



看起来没啥有用的信息但是别慌,我们先进行SQL注入

在URL中***/?id=1 后面写命令进行注入

```
and 1=2 union select 1,concat(username,',',password) from admin
```

这里的admin是搜素admin项

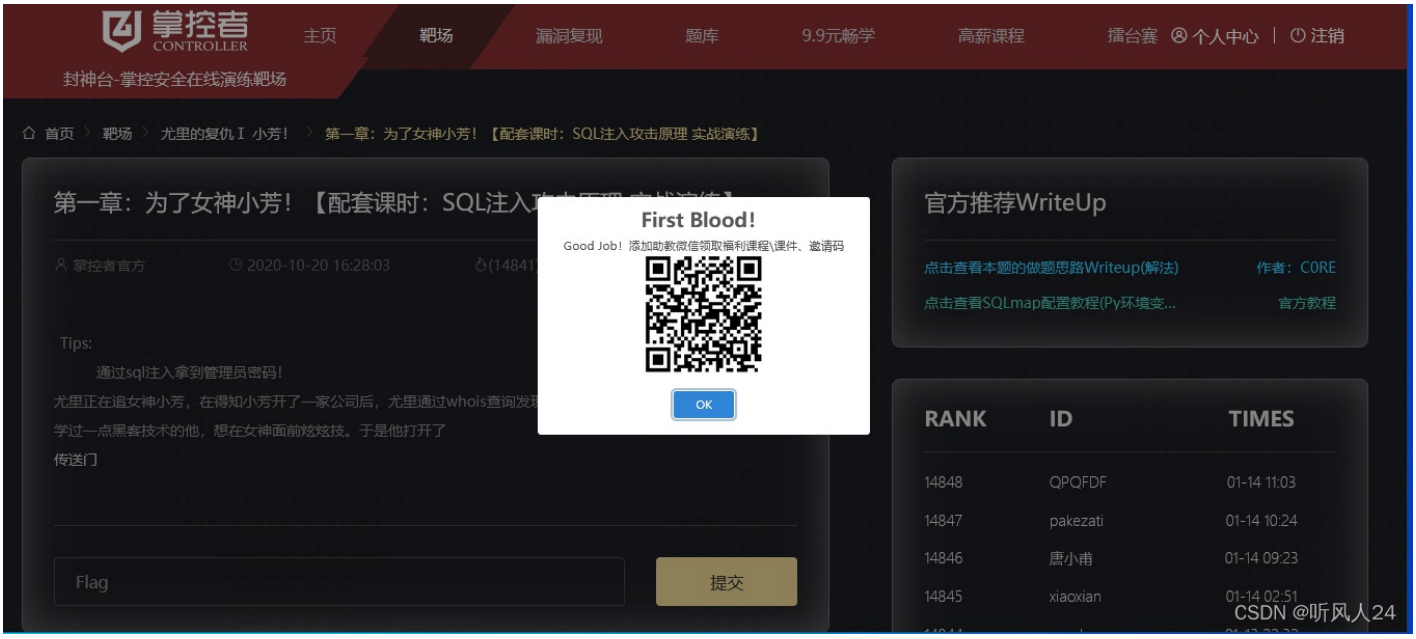
在图片下面数据库的内容已经出来了

管理后台账号名是"user"

密码是"hellohack"

我们为了验证准不准确进行提交flag

在这里系统只要求我们提交密码就行,所以我们只提交密码



出现这个页面说明我们的实验成功了

如需转载,请务必标注原作者

作者QQ:3369308571