文章编号：2096-1472(2020)-06-33-03
DOI:10.19644/j.cnki.issn2096-1472.2020.06.010

# 基于Python的WEB黑客攻击技术分析研究

贺军忠

(陇南师范高等专科学校，甘肃 陇南 742500)
✉lnszhjztg@163.com

**摘 要**：通过对Web黑客攻击的语言分析研究，得知大部分黑客都以Python为攻击语言，依托Internet对各种网络服务器和客户端进行攻击与密码破解。文章着重从基于Python的各种Web攻击目的入手，通过列举的方法分析研究各种Web黑客攻击技术与攻击过程。根据各种基于Python的WEB黑客攻击技术的攻击方法，分析研究其攻击过程，为企业等部门与单位的Web安全防护提供理论依据。

**关键词**：WEB攻击；XSS攻击；SQL注入；Web shell攻击
**中图分类号**：TP309.5 **文献标识码**：A

# Analysis and Research of Web Hacking Technology Based on Python

HE Junzhong

( *Longnan Teachers' College*, *Longnan* 742500, *China*)
✉lnszhjztg@163.com

**Abstract:** With programming language analysis and research on Web hacking, Python is regarded as the most commonly used language on password cracking and attacking various network servers and clients. This article focuses on the purpose of various Web attacks using Python, and analyzes various Web hacking techniques and attack processes with examples. Based on the analysis of different Python-based Web hacking technics, the paper discusses attack processes, hoping to provide a theoretical basis for Web security protection of enterprises and organizations.

**Keywords:** Web attack; Cross-Site Scripting (XSS) attack; SQL injection; Web shell attack

## 1 引言(Introduction)

目前，我们使用的大部分服务都是基于网络的，而基于HTTP协议的Web是网络服务的中心。如PC中使用的网易、淘宝等门户网站，以及智能手机中使用的各种移动Web都属于Web服务。为了保护系统安全，企业通常会关闭几乎所有端口，但对外提供Web服务的80端口却一直开放。比如我们常用的门户网站网易(http//www.163.com)就使用80端口对外提供Web服务。输入URL网址时，若不指定连接端口，则默认连接80端口。Web服务器通过80端口向用户PC传送文本、图像、文件、视频等多种内容，用户通过相应端口将ID、密码等纯文本以及大容量文件等上传到Web服务器。像这样，80端口应用广泛，但安全设备却几乎不对其进行检查。虽然很多企业配备了Web防火墙等设备，对应用程序级别的黑客攻击进行探查防范，但面对不断发展的各种web攻击技术，这种防范手段也不是万能的。此时此刻，黑客们正在利用Web服务的工作机制尝试发动致命攻击。

## 2 Python黑客攻击的优点(Advantages of Python hacking)

Python语言具有易学易用的特点，且拥有各种强大功能。首先，Python支持功能强大的黑客攻击模块，其拥有用于支持黑客攻击的丰富多样的库，比如pydbg、scapy、sqlmap、httplib等。目前，这些库被广泛应用于各种黑客攻击。其次，Python能够访问各种API，Python提供了用于黑客可以访问的Windows、Os X、Linux、Solaris、FreeBSD、OpenBSD等系统的ctypes库，黑客借助它能链接以上系统提供的DLL与共享库。第三，大多黑客攻击工具为

基金项目：2019年甘肃省高等学校教学成果培育项目“基于赛教融合的计算机类创新人才培养模式探索与实践”阶段性研究成果；2019年“1+X 证书制度”背景下网店运营推广人才培养模式研究与实践阶段性研究成果(JXGG2019006).

Python提供了APl，像Metasploit、sqlmap、Nmap等黑客工具都为Python提供了扩展接口[1]。黑客们通过使用Python，可以将Metasploit、sqlmap、Nmap等工具改造得更加强大。第四，Python易学易用，这也是Python被好多黑客，尤其是新手所青睐的最重要一点，这对黑客攻击而言是个巨大的优势。据中国企业数据治理联盟数据空间统计分析，目前有9大编程语言是黑客最喜欢和青睐的语言，并对做了详细分析排名，其Python仅次于R 语言排名第二。该统计报告指出Python 是行业人员正在转换发展的方向。过去两年里，很明显存在由R向Python转化的趋势，Donnell说：“Python用途宽广且灵活，所以人们蜂拥而至”[2]。掌握三四种编程语言是成为一名黑客所必需的，如C语言、C++、Jave与汇编语言，必须掌握。但其学习难度较大，要精通更是难上加难。而Python语言拥有各种强大功能，且具有易学易用的特点。所以Python语言成了黑客攻击语言的首选。

## 3 黑客攻击的定义(Definition of hacking)

Wikipedia中关于“黑客攻击”的定义如下：“针对电子电路、计算机软硬件、网络、网页等各种信息系统，借助某种手段、技术，使之执行信息系统设计者、管理者、运营者预料之外的动作行为，或者设法获取高于系统给定的权限，对相关信息进行查阅、复制、修改等的一系列行为[3]。”常见的黑客攻击包括系统黑客攻击、web黑客攻击、应用程序黑客攻击和网络黑客攻击，黑客攻击技术如图1所示。

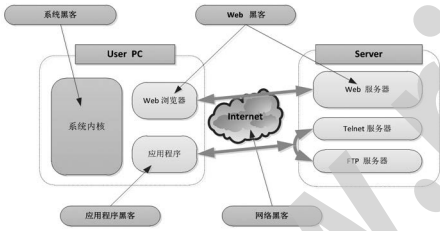


图1 黑客攻击技术

Fig.1 Hacking technology

## 4 基于Python的Web 黑客攻击技术(Web hacking technology based on Python)

从本质上说，计算机系统防范黑客攻击的能力较差。计算机诞生之初，人们更多关注的是它的功能，而非安全。并且数十年中，计算机以单机形式运行，直到互联网出现，计算机系统才暴露在多个用户面前。从此以后，黑客们便开始潜心研究计算机系统和各种攻击技术。计算机提供的多种功能一方面为用户带来了极大的便利，另一方面也为黑客提供了实施攻击的手段，其中Web黑客攻击尤为突出。

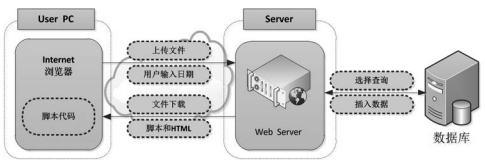


图2 Web黑客攻击

Fig.2 Web hacking

如图2所示，Web系统一般由Internet浏览器、Web服务器、数据库三部分组成，各部分功能划分十分明确。浏览器用于处理用户输入，加工和接收来自Web服务器的数据并输出到屏幕。Web服务器用于分析HTTP请求，并执行相应功能。需要处理数据时，Web服务器会连接数据库执行数据处理。数据库用于管理数据，支持数据的输入、更新与查询等功能。

黑客会恶意使用Web系统提供的功能。比如利用文件上传功能，将Web shell文件与恶意代码上传到Web服务器，然后运行Web shell文件，获取上传文件所在位置，进而控制Web服务器。黑客利用用户输入功能可以实施SQL注入攻击，通过输入非正常SQL查询评句获取Web服务器的错误信息，并对这些信息加以分析，进而实施攻击[4]。利用文件下载功能，可以将恶意代码散布到网络上的多台PC。网络浏览器中运行的HTML与脚本代码可以被恶意用于开展XSS攻击与CSRF攻击等。下面就各种Web攻击进行分析研究与比较。

### 4.1 XSS攻击

XSS(Cross-Site Scriptig，跨站脚本攻击)，Cross-Site Scriptig其缩写为CSS，这与层叠样式表(Cascading Style Sheets，CSS)易于混淆，黑客界约定跨站脚本攻击为XSS[5]。其很容易用Python中单例模式进行，XSS技术将包含恶意代码的脚本植入布告板的公告，感染阅读公告的用户PC，从中盗取用户个人信息。恶意代码大多数是脚本代码，它读取Cookie，并将其发送到特定URL。XSS攻击的主要步骤是：黑客首先通过Inernet将XSS脚本上传到WEB服务器公告板等平台，互联网用户通过正常请求Web 服务器等公告板，此时XSS脚本便会响应正常用户，并在用户PC上运行XSS脚本，并将Cookie文件传回Hacker PC。就这样阅读公告的过程中，其个人信息就会不知不觉地泄露。随着浏览器安全性增强，以及Web防火墙等设备的应用，XSS攻击的成功率已经大幅降低。

### 4.2 CSRF攻击

CSRF(Cros Site Request Forgery，跨站请求伪造)类似于XSS攻击，它也将恶意代码插入公告板，用户阅读相应公告时即受到攻击。其与XSS不同之处是XSS攻击主要从用户PC非法盗取个人信息，而CSRF主要通过用户PC对Web服务器发动攻击。就黑客攻击类型而言，CSRF攻击既可以使Web服务器瘫痪，也可以用于盗取敏感信息，对于部分黑客来说无疑是两全其美，其攻击过程如图3所示。

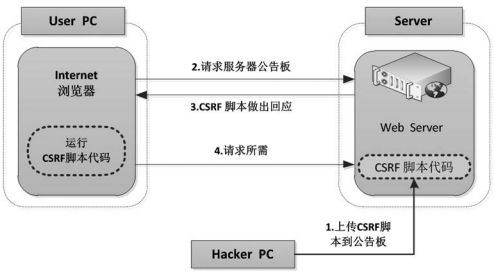


图3 CSRF攻击过程

Fig.3 CSRF attack process

### 4.3 网络钓鱼

网络钓鱼(Phinshing)是指黑客通过精心设计与银行等类似的假冒网站，骗取受害人在这些网站输入的金融信息或个人敏感信息。首先，黑客向用户发送声称来自银行或其他知名机构的欺诈性邮件或链接信息，用户打开电子邮件或点击其中链接，就会进入黑客精心伪造的钓鱼网站。用户可能将这些网站误认为正规网站，而在其中输入用户名与密码。假冒网站就会保存用户的这些信息，黑客利用这些输入信息发动更深层次的攻击，其攻击过程如图4所示。

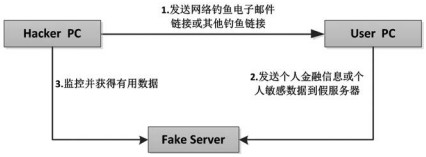


图4 网络钓鱼攻击过程

Fig.4 Phishing attack process

### 4.4 域欺骗

域欺骗(Pharming)攻击中，黑客首先入侵DNS服务器，修改正常的网站域名与IP对照表，将仿冒网站的IP地址发送给用户浏览器，从而将用户引导至精心设计的仿冒网站。这样，用户在这些网站输入的个人信息就会被偷偷盗走，此攻击类似网络钓鱼攻击。不同之处是域欺骗是伪装DNS，用户并不知情，其攻击过程如图5所示。

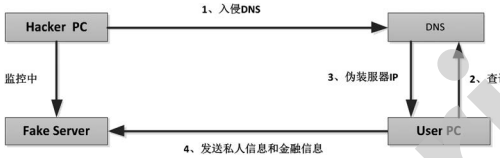


图5 域欺骗攻击过程

Fig.5 Domain spoofing attack process

### 4.5 SQL注入

SQL注入主要利用HTML input标签发动攻击。首先，浏览器接收用户输入的账号与密码，并将其发送给Web服务器。Web服务器通过SQL语句查询数据库，比对是否存在与输入的账号和密码一致的用户信息。此时，黑客向用户账号与密码中输入的不是正常值，而是一些能够诱使数据库产生错误行为的值。比如，将类似于OR 1=1;/*，数据库将忽略条件返回所有值。黑客通过反复输入非正常的SQL语句，并分析数据库返回的数据，从而得到最适合对系统进行攻击的SQL语句[6]。SQL注入攻击在Python的sqlmap模块下只需5步即可完成。分别是第1步搜索URL、第2步寻找漏洞、第3步搜索数据表、第4步搜索列、第5步访问数据，其攻击过程如图6所示。

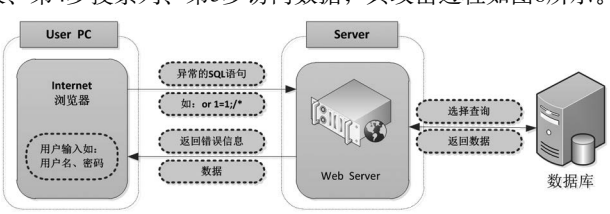


图6 SQL注入攻击过程

Fig.6 SQL injection attack process

### 4.6 Web shell

Web shell恶意利用了Web提供的文件上传功能。首先，黑客将用于远程操纵服务器的Web shell文件上传到Web服务器，然后找到上传文件所在位置，得到访问Web shell文件的URL地址。然后，通过该URL地址运行Web shell文件，获取可以控制操作系统的超级权限。Web shell攻击利用Python提供的fileupload等模块也比较容易实现[7]。近来，Web shell与SQL注入都成为实施Web黑客攻击最强大的技术，其攻击过程如图7所示。

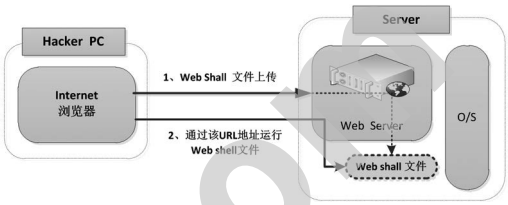


图7 Web Shell攻击过程

Fig.7 Web shell attack process

## 5 结论(Conclusion)

为了防范web黑客攻击，几乎所有企业都安装了诸如防火墙、IPS、IDS等多种安全设备。尽管如此，它们还是不得不向网络暴露一些端口，以对外提供Web服务。为了确保安全，这些公司使用了类似于Web防火墙的设备，但对黑客而言，Web系统仍然是最诱人的攻击对象。文章通过对Python语言的分析，得知大部分黑客以其为攻击语言。在利用Python提供的丰富模块进行各种攻击，本研究对各种基于Python的Web黑客攻击技术进行分析与比较，有助于企业等进行针对性的防护。

## 参考文献(References)

[1] 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(06):381-383;388.

[2] 数据处理的9大编程语言[EB/OL].http://www.chinaedg.com/shujuzhishixuexi/zhishipuji/2019-06-17/1876.html,2019-6-17/2019-11-25.

[3] 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(04):497-510.

[4]姜鹏.Web应用程序安全的“七宗罪”解析[J].计算机与网络,2018,44(09):50-51.

[5] 丁媛媛.计算机网络病毒防治技术及如何防范黑客攻击探讨[J].赤峰学院学报(自然科学版),2012,28(08):41-42.

[6] 楚翔皓,刘震.基于LSTM神经网络的SQL注入攻击检测研究[J].天津理工大学学报,2019,35(06):41-46.

[7] Yu Li, Jin Huang, Ademola Ikusan, et al. ShellBreaker:Automatically detecting PHP-based malicious web shells[J]. Computers & Security, 2019(87): 101-108.

## 作者简介：

贺军忠(1982-)，男，硕士，网络工程师/讲师.研究领域：网络组建与信息安全.