

网络空间安全前沿技术丛书

骇客是一种精神状态和思维方式，而非一种物理属性



Google Hacking

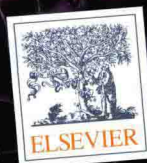
渗透性测试者的利剑

(原书第3版)

Johnny Long
[美] Bill Gardner 著
Justin Brown

沈卢斌 译

清华大学出版社



网络空间安全前沿技术丛书

Google Hacking—— 渗透性测试者的利剑 (原书第3版)

Johnny Long

[美] Bill Gardner 著

Justin Brown

沈卢斌 译

清华大学出版社
北 京

北京市版权局著作权合同登记号 图字: 01-2017-0238

Google Hacking for Penetration Testers, Third Edition

Johnny Long, Bill Gardner, Justin Brown

ISBN: 978-0-12-802964-0

Copyright © 2016 by Elsevier Inc. All rights reserved.

Authorized Simplified Chinese translation edition published by Elsevier (Singapore) Pte Ltd. and Tsinghua University Press.

Copyright © 2017 by Elsevier (Singapore) Pte Ltd and Tsinghua University Press. All rights reserved.

Published in China by Tsinghua University Press under special arrangement with Elsevier (Singapore) Pte Ltd.. This edition is authorized for sale and distribution in the People's Republic of China exclusively (except Taiwan, Hong Kong SAR and Macao SAR). Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由 Elsevier (Singapore) Pte Ltd. 授予清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾地区)出版与发行。未经许可之出口,视为违反著作权法,将受法律之制裁。

本书封底贴有 Elsevier 防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

Google Hacking——渗透性测试者的利剑(原书第3版)/(美)约翰尼·朗格,(美)比尔·加德纳,(美)贾斯汀·布朗著;沈卢斌译.—北京:清华大学出版社,2018

(网络空间安全前沿技术丛书)

书名原文: Google Hacking for Penetration Testers, Third Edition

ISBN 978-7-302-47652-8

I. ①G… II. ①约… ②比… ③贾… ④沈… III. ①互联网络—信息检索
IV. ①G254.928

中国版本图书馆 CIP 数据核字(2017)第 154534 号

责任编辑:梁颖 柴文强

封面设计:常雪影

责任校对:徐俊伟

责任印制:刘海龙

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:190mm×235mm 印 张:17.75

字 数:299 千字

版 次:2018 年 1 月第 1 版

印 次:2018 年 1 月第 1 次印刷

印 数:1~2000

定 价:79.00 元

产品编号:071564-01

本书献给

致力于

商用SD-WAN智能广域网平台应用开发的

华斧网络科技（AXESDN）公司

所有网络专家

译者序

若干年前,我第一次利用装有 Codenomicon Defensics 的 Kali Linux 测试平台对公司的产品进行渗透性测试,从此开启了我职业信息安全从业者的生涯。当我第一次发现了产品漏洞并提交给系统工程师后,出于好奇心,我多问了自己一个“为什么?”。通过学习相关 IP 协议以及产品架构,我先于产品开发的码农兄弟们发现了系统漏洞的位置以及成因,这让我获得了自信,也体会到了这项工作的乐趣。特别是当我发现,作为各安全论坛中小白进阶必备技能的 WiFi 密码破解法也能让我来点澎湃,要是能重来,我会早选网安。

初入信息安全领域你会发现有大量的工具可以扩充你的军械库,特别是当你装完 Kali Linux,发现系统已经很贴心地预装了很多骇客软件,让你瞬间感觉屠龙宝刀如此易得,在江湖上一番血雨腥风之后,武林盟主的位子也近在咫尺,从此将走上迎娶白富美的人生之巅。但 IT 领域通常有个定律,免费的东西既是诱惑也是陷阱。所谓诱惑,你会成为一个发现满地是玩具的小男孩,玩具琳琅满目,各有精巧之处,总能发现更好的,却总也找不到一件最趁手的。所谓陷阱,你会陷于各种奇技淫巧,会用各种工具去实现一些零碎的小功能而忽略了对知识体系本身的理解和钻研,炫技多于实干,浮夸多于务实。

每个行走江湖的大侠都有自己的独门兵器,于杨过就是玄铁重剑,于李寻欢就是小李飞刀,所谓一招鲜吃遍天。在信息安全领域也有这么一柄使用门槛

极低却又威力无穷的“倚天剑”——Google。它那简洁的搜索入口,会让你深刻体会到,大道应该至简,知易行也不难。如果你是小白,可以搜索“信息安全从入门到精通”;如果你是电商系统管理员,可以搜索“如何从数据库转储中找到用户名和密码”;如果你是信息安全爱好者,可以搜索“如何使用 Google 创建超级蠕虫”。林林总总只有你想不到没有你找不到,总有一款适合你。当然这些都只是 Google 的初级玩法,为了发挥这柄利剑在情报搜集领域中的真正威力和潜能,作者在书中介绍了 Google 专用的搜索语言及其语法。使用了这门专用语言,你的思想会与 Google 开发者更加契合,你的搜索会更加高效与精准。比如,用 Google 搜索 book,你会得到数以亿计的结果。面对如此浩如烟海的网络世界,一种无力感顿时涌上心头。但如果你这样搜: `intitle:book, inurl:book, allintext:book, site:book, link:book, inanchor:book, cache:book, info:book, related:book, stocks:book, define:book` (具体含义详见本书,哈哈!) Google 就会更懂你,能给出更精确的结果。如果还不过瘾,利用脚本实现的自动化搜索,信息分类、检索,网络抓取等更劲爆的功能还在等着你。除了搜集信息,Google 还能为你提供开源工具的绝大多数功能。当然还有数不清的解决方案,在线讨论、代码模块、漏洞报告,它简直就是你居家生活、养生保健的必备良药。如果你刚开始对使用 Google 搜索语言还不自信,或者还无法准确地用它表达出自己的搜索意图,没关系,广大热情的网友还自发地维护着一个叫 GHDB 的数据库,你可以从中“借鉴”到很多有效的已被优化的最新的搜索语句。原来一个搜索引擎在信息安全领域也能如此高端!

为了让本书更接地气,译者把绝大多数搜索都在“仅限搜索简体中文结果”的条件下重新执行,并且用新结果截图替换了书中原图。也改正了书中一些明显的错误,对不符合中文语言习惯的案例也进行了重新“演绎”。力求使各位读者不会因为文化差异而对书中内容产生误解。

在此特别感谢 Elsevier 的中方版本经理孙偲小姐的推荐和沟通协调。特别感谢清华大学出版社电子信息事业部梁颖主任的热心帮助和专业指导。一向自诩为半个文青的我,在本书责任编辑梁主任的专业水准面前,自信心瞬间被碾压成一地玻璃渣。也要感谢柴文强和徐俊伟两位编辑的中肯建议和细心校对。最后要感谢我的爱人杨芳女士。她是本书的首位读者,也是我的首席错别字校准官,可以想见让整天沉浸在与《琅琊榜》宗主爱恨情仇纠缠中的她,来看

这本书会让她多么的无助与无奈。有很多次,她正一边听着网络主播们喊麦,一边享受着清空网络购物车的快感,却会被我强行要求检查几段译文。

这是一个让我充满激情与快乐的领域,我想我应该会一直走下去。除了本书,本人还有几本关于大数据、无线、终端、云计算等方向的信息安全译著将陆续出版。随着接触到的信息安全理论和案例越来越多,我的脑海中不断浮现出留学时曾做过的一个小项目。当年 ABB 为了提高流水线上机械臂的响应速度,根据那些机器人特定的计算方式,让我们在 FPGA 上为其定制了一个硬件加速器。在即将到来的 IOT 社会,在各种移动设备已逐渐衍化成人人类体外器官的时代,使用现场可编程硬件,在不断变化的应用场景中、在网络的边缘对数据进行快速加解密或对其他重度计算进行加速,然后通过 SDN 快速给数据在局域网、公网、公有云和私有云中建设设备间、组织间、区域间、大洲间的路由转发通道,去嫁接各种服务并对其进行测试和应用,同时利用 SDN 的便利以及 FPGA 的特性对数据流进行识别、监测、筛选、分发来实现更高效更精准的入侵检测和安全防御,等等,这些都应该是未来万物互联世界中很有趣的事情吧。

此书译完的时候,正值媒体爆料“有关部门破获 50 亿条公民信息泄露大案”。见此标题,不出意外你我都该是本案的受害者吧……

沈卢斌

2017 年 7 月

于上海

目 录

第 1 章 Google 搜索基础	1
摘要	1
关键词	1
介绍	2
探索 Google 的 Web 界面	2
总结	21
要点速查	22
第 2 章 高级运算符	26
摘要	26
关键词	26
介绍	27
运算符语法	28
语法排错	29
引入 Google 的高级运算符	30
INTITLE 和 ALLINTITLE: 在页面标题中搜索	31
ALLINTEXT: 在页面文本中查找字符串	33

INURL 和 ALLINURL: 在一个 URL 中查找文本	33
SITE: 把搜索精确到特定的网站	36
FILETYPE: 搜索特定类型的文件	37
LINK: 搜索一个网页的链接	40
INANCHOR: 在链接文本中寻找文本	43
CACHE: 显示页面缓存版本	44
NUMRANGE: 搜索一个数字	44
DATERANGE: 搜索在特定日期范围内发布的页面	45
INFO: 显示 Google 的总结信息	46
RELATED: 显示相关站点	47
STOCKS: 搜索股票信息	47
DEFINE: 显示一个术语的定义	48
运算符的冲突和失败的搜索(bad search-fu)	48
总结	51
要点速查	52
网站链接	55
第 3 章 Google Hacking 基础	56
摘要	56
关键词	56
介绍	57
缓存访问的匿名性	57
目录列表	61
查找目录列表	62
查找特定的目录	63
查找特定的文件	64
服务器版本	64
与众不同: 遍历技术	66
总结	71
要点速查	71

第 4 章 文档细分和数据挖掘	74
摘要	74
关键词	74
介绍	75
配置文件	76
查找文件	80
日志文件	80
Office 文档	81
数据库挖掘	82
登录入口	82
支持文件	83
错误消息	84
数据库转储	85
真实的数据库文件	86
自动细化	87
总结	91
要点速查	92
第 5 章 Google 在一个信息收集框架中的身影	95
摘要	95
关键词	95
介绍	96
自动化搜索的原理	96
原始搜索项	99
扩展搜索项	99
使用“特别的”运算符	106
从数据源中获取数据	107
自行挖掘：请求和接收响应	108
自行挖掘：解析结果	113
使用其他搜索引擎	119

解析数据	119
后期处理	126
收集搜索项	129
总结	135
第 6 章 查找漏洞寻找目标	136
摘要	136
关键词	136
介绍	137
查找漏洞代码	137
查找公开的漏洞网站	137
利用常见代码字符串查找漏洞	138
查找易受攻击的目标	140
总结	140
第 7 章 10 个简单有效的安全搜索	142
摘要	142
关键词	142
介绍	143
site	143
intitle:index.of	144
error warning	145
login logon	146
username userid employee.ID "your username is"	147
password passcode"your password is"	149
admin administrator	149
-ext:html-ext:htm-ext:shtml-ext:asp-ext:php	152
inurl:temp inurl:tmp inurl:backup inurl:bak	154
intranet help.desk	155
总结	156

第 8 章 追踪 Web 服务器、登录入口和网络硬件	157
摘要	157
关键词	157
介绍	158
查找和分析 Web 服务器	159
查找登录入口	171
使用和查找各种 Web 工具	173
定位开启 Web 的网络设备	177
查找网络报告	178
查找网络硬件	178
总结	180
第 9 章 用户名、密码和其他秘密信息	182
摘要	182
关键词	182
介绍	183
搜索用户名	183
搜索密码	185
搜索信用卡号码、社会保险号码以及更多	187
社会保险号码	189
个人财务数据	190
搜索其他有用的数据	190
总结	192
第 10 章 入侵 Google 服务	193
摘要	193
关键词	193
日历	193
Google 快讯	195
Google Co-op	196

Google 自定义搜索引擎	197
第 11 章 入侵 Google 案例	198
摘要	198
关键词	198
介绍	199
极客	200
公开的网络设备	203
公开的应用程序	210
摄像头	216
电信设备	222
电源	228
敏感信息	232
总结	233
第 12 章 保护自己免遭 Google 骇客攻击	234
摘要	234
关键词	234
介绍	235
一个优质可靠的安全策略	235
Web 服务器安全防护	236
软件默认设置和程序	240
入侵你自己的网站	241
Wikto	242
Advanced dork	243
从 Google 获得帮助	243
总结	243
要点速查	244
网站链接	245
主题索引	246

第1章

Google搜索基础

■ 摘要

本章涵盖了 Google 的 Web 界面基础,对视频、地图等特殊搜索功能的介绍,并详细说明如何进行基本的搜索。

■ 关键词

Google Web 界面

搜索类型

Google 地图

Google 新闻

YouTube

谷歌邮箱 Gmail

更多选项卡

搜索

布尔运算符

特殊字符

Google 警告

搜索精减

Google URL

Google 高级搜索参数

■ 介绍

Google 的 Web 界面是一目了然的,既干净又简单。它的“既视感”是受到版权保护的,这点的理由很充分。大多数人都会不会意识到,这个界面也是极其强大的。通过本书,我们将会看到如何使用 Google 来揭示真正令人惊叹的东西。然而,跟生活中大多数事情一样,在能跑之前,你必须先学会走。

本章将带你领略 Google 搜索的基础。我们从探索这个强大的 Web 界面开始,即使是最顶尖的 Google 用户,对于大多数日常的查询,依然依赖于 Web 界面,因此,这个界面使 google 成为一个新造的常用词。一旦理解了如何来导航和翻译从不同界面获得的搜索结果,我们将能探寻基本的搜索技术。

理解基本的搜索技术将帮助我们建立起一个坚实的基础,这是进行更加高级查询的基石。你将学到如何合理地使用布尔运算符(与 AND,非 NOT,或 OR),同时也将探寻组合搜索的力量和灵活性。你还将学到一些 Google 对不同通配符独一无二的实现方式。最终,你将会学到 Google 统一资源定位符(URL)结构的语法。

当你掌握一系列相关的 Google 搜索基础后,再学习 Google URL 结构的输入输出,将给你带来更快的速度和更大的灵活性。我们将看到,Google URL 结构为跟朋友和同事交换有趣的搜索提供了极其出色的“速记法”。

■ 探索 Google 的 Web 界面

► Google 的 Web 搜索界面

Google 的主界面,如图 1.1 所示,可以通过 www.google.com 访问。这个界面因其干净的线条,令人愉悦而又整洁的外观和友好的用户布局而闻名。

尽管这个界面第一眼看上去似乎显得相当没有特点,但我们将看到恰恰是这第一页能执行很多不同的搜索功能。

如图 1.1 所示,只有一个地方让你输入,这就是搜索区域。为了向 Google



图 1.1

提一个问题或查询,你只需简单地输入你正在寻找的东西,然后按 **Enter** 键(如果你的浏览器支持的话),或者单击“**Google 搜索**”按钮,随之你将被带到查询的结果页面。

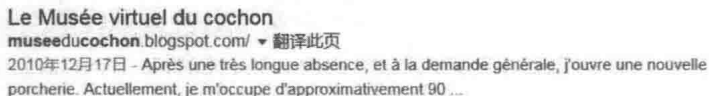
► Google Web 结果页面

在 **Google** 处理完搜索查询以后,它就显示一个结果页面。这个页面列出了你的搜索结果,也提供了包含你搜索文本的网页链接。搜索结果页面的顶部区域与 **Web** 搜索主页面类似。注意页面顶部的图片、视频、新闻、地图和 **Gmail** 链接,通过单击这些来自搜索页的链接,就自动以另一种搜索类型再次提交了你的问题,而无须重新输入你的查询。

那些结果行显示了哪些结果被展示了(1~10,在这个例子中)、大致匹配的总数目(在这里,超过 800 万)、搜索查询本身(包括个别字词在词典中的链接)和执行这个查询所耗费的时间。

查询速度经常被忽略,但它又是非常令人印象深刻的,即使是大量的查询产生了百万级的命中也能瞬间返回结果。对于结果页面上的每一个入口,**Google** 列出了这些网站的名字。名字的后面跟着对这个网站的归纳总结,通常最初几行是内容、匹配页面的 **URL**、最后被抓取页面的尺寸和日期,这个页面被

Google 最后抓取时的网页快照, 和一个带有相似内容页面的链接。如果结果页面上的语言不同于默认语言, 同时 Google 也支持把当前页面上的语言翻译成参数界面里设置的默认语言, 一个名叫“翻译此页”的链接将会显示出来, 允许你以自己的语言来阅读这个页面大致的内容。(见图 1.2)



Le Musée virtuel du cochon
 museeducochon.blogspot.com/ ▼ 翻译此页
 2010年12月17日 - Après une très longue absence, et à la demande générale, j'ouvre une nouvelle porcherie. Actuellement, je m'occupe d'approximativement 90 ...

图 1.2

► Google 网上论坛

由于网页论坛、博客、邮件列表和即时信息技术大受欢迎, 作为最老的公共论坛, USENET 新闻论坛已经变成一种被忽略的在线公共讨论形式。数以千计的用户依然每天在 USENET 发帖。(在这里 www.faqs.org/faqs/usenet/what-is/part1/ 能够找到一个关于 USENET 所包含内容的详尽讨论。)Dejan 新闻 (www.deja.com) 曾经被视为对所有过去和当前新闻论坛消息的权威采集点, 直到 Google 于 2001 年 2 月收购 www.deja.com (详见 www.google.com/press/pressrel/pressrelease48.html)。这次收购让用户能够通过简单又直接的 Google 搜索界面来查询 USENET 从 1995 年之后发表的所有消息存档。现在 Google 把 USENET 网上论坛称作 Google 网上论坛。

如今, 全球的互联网用户为了一般性的讨论和问题求解而求助于 Google 网上论坛。IT 从业者因为各种技术问题的解答而求助于 Google 中的分论坛是非常普遍的。原有的 USENET 社区在美观的 Google 网上论坛搜索引擎背后依然十分兴旺发达。

Google 网上论坛搜索能够通过点击那些在 Google 主页面上的组标签而被访问到, 或者访问 <http://groups.google.com>。网上论坛搜索界面(如图 1.3 所示)看起来与其他 Google 搜索页面非常不同。然而它的搜索功能却是以相同的方式在工作。网上论坛搜索页面和 Web 搜索页面之间最大的差别在于网上论坛浏览链接。