此文章已于 0:51:26 2015/12/25 发布到 Net | Linux | 安全

★Kali信息收集~ 1.Google Hacking + Github Hacking

**一、google hacking**

* 1. **site**

**site：cnblogs.com 毒逆天**

计算机生成了可选文字:
Eiüi_ 
stie:cnblogs.com 
$1 32 
3 site BIJÉQ: 
site:cnblogs.com 
53, 
blank'S 
bEtQ: 
Ca hrefz"http://mall_qq.com/cgi-bin/feed7Fhttp://vwwv_cnblogs.com/dunitian/" target:' 
posted @ 2015-06-05 10:54 
wwv_cnblogs.com 
site :cnblogs.com_ http://vwwv_cnblogs.com/_ http://vwwv_csdn_net/_ 
NET Site_ Oct 4 2013 Browser Link is a new 
feature in Visual Studio 2013 that creates a communication channel between the VS201EiÉY_Efii 
2015 7 
NET alog - Site Home 
Visual assist 
( - t*-a-fi 
VS201E 
www_ff0512.com 
vs201E rc 
vwwv_cnblogs.com/qzhf01thelife/p/4012_ 
NET Site ASP NET MVC 4 ASP NET MVC4 is a 
framework for building scalable, standards-based web applications 
page2rss.com/4e96d60cc334af6aS04d9ff447f3613 
http://www_cnblogs.com/ - Last Checked: 12/18/15 06:12:14 - Added: 11/29/04 03 
2015-12-18 00:19 
article - 
. Nicely, this site o 
(1) 

* 1. **intitle**

**intitle:login**

计算机生成了可选文字:
intitle:login 
032 
Salesforce: Login 
https://login_salestorce.com/ 
Salesforce Customer Secure Login Page. Login to 'Aur Salesforce Customer Account. 
Yahoo - login 
https://login_yahoo.com/ 
Afghanistan (+93) ; Albania (+366) ; Algeria (+213) ; American Samoa (+1) ; Andorra (+376) ; 
Angola (+244) ; Anguilla (+1) ; Antarctica (+672) ; Antigua, 
Account View by LPL Financial - Login Page 
https://myaccountviewonline.com/ 
Prices are delayed 20 minutes. All times are Eastern. Securities and Advisory semces offere 
d through LPL Financial, member FINRA/SIPC, a Registered 
Login — Squarespace 
ww_squarespace.com/logln,' 
Squarespace - Landing Pages - Websites - Commerce - Back to All Designs Tour Login Men 
u. Home - Tour - Landing Pages - Websites - Commerce - Pricing. 
Login Page - Zoho Mail 
https://ww_zoho.com/mail/logln_html 
Email Hosting ser,Jlce with a clean, No Ads web mail interface, advanced business-class feat 
ures and provisions for seamless mobile, desktop client access. 
webmail login - Bluehost 
https://login_bluehost.com/cgi/webmail 
aluehost - 24/7 support. free 1-click installs for blogs, H:ommerce, and more. get a website 
with a free domain name and superior speed. 
Login on Twitter 
https://fi.vitter.com/login 

* 1. **allintitle**

**allintitle:index of**

计算机生成了可选文字:
Google 
allintitle:index of 
Google 
oug 
Index of /download/ 
hypem.com/download/ • 
Index of 'download/_ Icon Name Last modified Size Description. VIRI Parent Directory - 
(DIR) 1/ 14-Dec-201S 10:51 - (DIR) 2/ IS-Dec-201S 01:17 - (DIR) 
01-'ale' - Of 'download'S - Index of 'download/M - Of 'download/a 
Index of / 
download_bitdetender.com/ 
Index of/ __/ spvqaø 20-May-201S 14:49 - am/ 10-Mar-201S 11:07 - beamer/ Il-Dec-2013 
08:26 - business/ 03-Dec-201S og:ss - cloud/ 19-Feb-2014 14:45 
Of 'SMS - Of 'rescue cd - Of 'updates - Of 'removal tools 
Index of Economic Freedom: Promoting Economic . 
unmv_heritage.org/index/ 
Index of Economic Freedom measures economic freedom of 186 countries based on 
trade freedom, business freedom, investment freedom, and property rights. 
Country Rankings - Heat Map - About The Index - Downloads 
Index of /pub - D-Link 
Name - Last modified - Size - Description. LDIR), Parent Directory, -_ t), aHMMawe_pdf, 
26-Mar-2014 17:28, 243K. LDIR), OLLMöKa_ Y npoAYKTa HeT 
The Index I The Index of Christian Art at Princeton l.Jniversity 
http://lca_princeton.edu/ • 
- A database of Christian Art provided by Princeton University. 
Index of /pub/FreeBSD/ 
ttp_treebsd.org/pub/FreeaSD/ 
File Name - File Size - Date - Parent directory', 
development/ , 
21:30_ doc', 201S-Aug-23 10:44_ ports', 201S-Aug-OS 04:16_ 
201S-Dec-20 
Kauffman Index of Entrepreneurship Series I Kauffman.org 
unw_kauttman.org/mcrosites/kauttman-index • 
The Kauffman Index: Startup Activitv is a new report from the Kauffman Foundation 

**allinurl:forcedownload.php?file=**

计算机生成了可选文字:
Google 
allinurl:forcedownload.php?file 
6,320 ( 0_67 ) 
Passwords 
To access the ceremonies, must provide a password. The files are safeguarded in 
the following manner: Ordeal level - the Admonition. Brotherhood level 
Untitled - Lyon 
Page 1 
www.parkweb.vic.gov.au/forcedownload.php?file:3967.. 
robots_txt, 
eon 20 April 2013 FILM & VIDEO SUBMISSION GUIDELINES 
- 26th IMAGES FESTIVAL 11 - 20 April 2013 FILM & VIDEO 
SUBMISSION GUIDELINES. Established in 1987 and dedicated to the moving _ 
COMMAND CHI 8-750 
Contents. Section 1 _ Safety and General Information 
Section 2_ Special Tools _ 
IT'S I-AUBER Switzerland 
using allyou_net_ 
LIGHT YEARS 
LIGHT YEARS. An Exhibition by. Eugenia aalcells curated by. Eulälia aosch_ 18/ 
09/2012 - 18/11/2012_ Tabacalera espacio Promociön del Arte. MAdrid 
Digium TDM2400 and AEX2400 Series Analog Cards Use... 
Digium, Inc. Page 2_ O Digium, Inc. 2009_ All rights reserved. No part of this publication 
may be copied, distributed, transmitted, transcribed, stored in a retrieval 

* 1. **inurl**

**inurl:/cgi-bin/MANGA/index.cgi**

计算机生成了可选文字:
Google 
inurl:/cgi-bin/MANGA/index.cgi 
RE" 21 0_21 *'h) 
Web Admin I Welcome 
westscitech.com/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome 
unw_tmxooogE2g875.com/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome 
http://thepcwerks.com/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome 
Web Admin I Welcome 
unw_gtxacademy.com/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome 
unw_bccars.com/cgi-bin/MANGA/index.cgi 
IIS Windows Server 
Web Admin I Welcome 
csx_com_my/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome 
dandypan.com/cgi-bin/MANGA/index.cgi 
Web Admin I Welcome - bienhoasugar.vn 
bienhoasugar_vn/cgi-bin/MANGA/index.cgi • 
Gooogle 
_E-fi 
123 

* 1. **cache 快照页**

**cache:stackoverflow.com**

* 1. **filetype**

**filetype:pdf Kali Linux**

计算机生成了可选文字:
Google 
filetype:pdf Kali Linux 
44,800 ( 0_38 
00. Introduction to Kali Linux 
docs_kali.org/pdt/kali-book-en_pdt • 
This PDF has been autogenerated on 
ali.org - May 26, 2014_ 00_ Introduction to 
Kali Linux. Official Kali Linux Documentation 
ok. We have created an 
persistence - Kali Linux 
http://ww_kali.org/dojo/workshop-02_pdt • 
USE YOUR OWN KALI 2_0 ISO. If you participated in the first workshop, use 'Aur own 
custom ISO for this next module. DOWNLOAD A PRE-BUILT ISO. If youVe 
Kali Linux Live USB Install 
docs_kali.org/pdt/articles/kali-linux-live-usb-install-en_pdt 
Official Kali Linux Documentation. This PDF has been autogenerated on docs_kali.org - 
Sep 16, 2014_ Booting and installing Kali from a USB stick is our favorite 
(PDF) Web Penetration Testing with Kali Linux - Packt Publishing 
http://ww_packtpub.com/___/g7817821E31Eg Chapter 02_pd_ 
Web Penetration Testing with Kali Linux is designed to be a guide for professional. 
Penetration Testers looking to include Kali in a web application penetration 
Kali Linux Cookbook - Packt Publishing 
http://wmv_packtpub.com/___/g78178328g5g2 Chapter og_pd_ 
Kali Linux is a Linux-based penetration testing arsenal that aids security Kali Linux 
Cookbook provides with practical recipes featuring many popular. 
PWK Syllabus - Offensive Security 
http://ww_ottensive-secunty.com/___/penetration-testing-with-___ 
Penetration Testing: What You Should Know. 0_1 -— About Kali Linux. - 
About Penetration Testing. Legal. 0_4 -— The megacorpone.com Domain. 

* 1. **site+filetype**

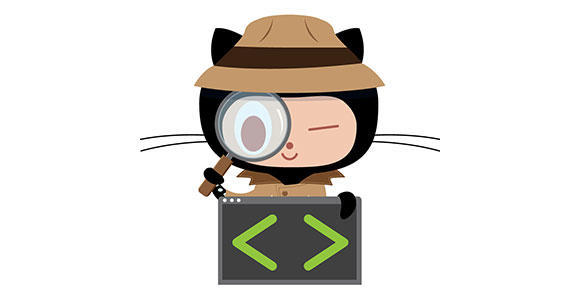
**site:cnblogs.com filetype:pdf Linux**

计算机生成了可选文字:
Google 
site:cnblogs.com filetype:pdf Linux 
329 0.16 
Linux Graphics Drivers: an Introduction - Freedesktop.org 
1 g/linuxgraphlcsdrivers_ 
Linux Graphics Drivers: an Introduction. Version 3_ Stéphan 
chesin_ 
March IS, 2012 
NVIDIA CUDA Getting Started Guide for Linux 
Getting Started Linux. t 
NVIDIA CUDA GEITING STARTED GUIDE. FOR LINUX. DU-O 
-001 v6_s August 
2014_ Installation and Verification on Linux Systems 
How to Install Hadoop? (On Mac OS, Linux or 
- SNAP 
(On Mac OS, Linux or Cygwin on Windows). 1) Download hadoop 0_20_0 from 
http://hadoop_apache.org/mapreduce/releases_html_ 2) Untar the hadoop file: 
The Linux I/O Stack Diagram - Thomas-Krenn.AG 
- Applications (Processes) direct 1/0_ (0 DIRECT). VFS_ Page. Cache 
nvme hooked in Device Drivers. (hook in similar like stacked devices like. 
The Linux Programming Interface - PDFiles.COM 
Linux Programming Interface_pdt 
•Michael Kerrisk has not only written a great book about Linux programming and how _ 
across both the Linux and UNIX system interfaces with clear descriptions 

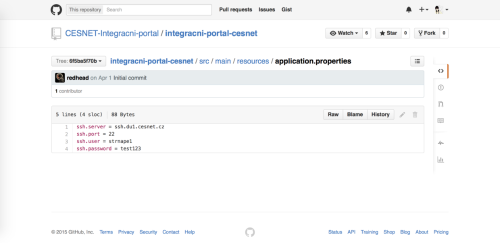
**二、github hacking**

* 1. 关键词搜索，自己构思即可
  2. 案例：

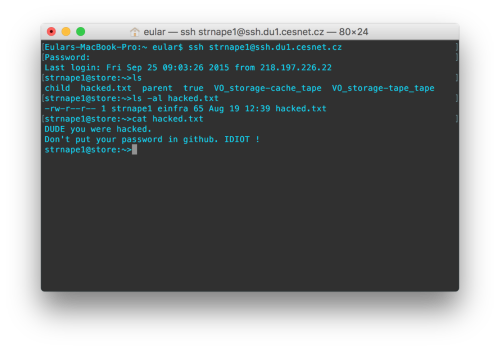
Github不仅能托管代码，还能对代码进行搜索，我们感受到了其便利的同时，也应该时刻注意，当你上传并公开你的代码时，一时大意，让某些敏感的配置信息文件等暴露于众。



让我们从第一个例子开始。当搜索ssh password关键字时，其中里面有这样一个有趣的结果：



好像是一个捷克教育科研网络的，账号密码写的这么简洁明了，于是登录上去看一看。



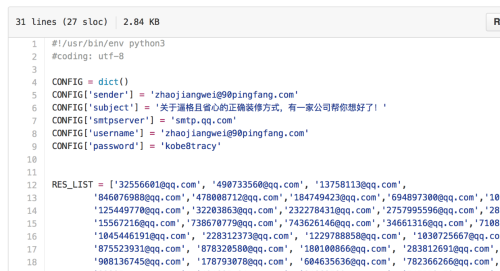
是不是还挺欢乐的，早就有无数人登陆过了，还有人留下文本善意提醒。这意味着什么，Github早已被盯上，也许下一个大事件会是某漏洞导致Github私有库代码大量泄漏。

**当我们在Github上搜索时，我们到底能搜到什么**

能搜到的东西很多，这里只是给个思路，具体怎么玩自己去尝试。

**邮箱**

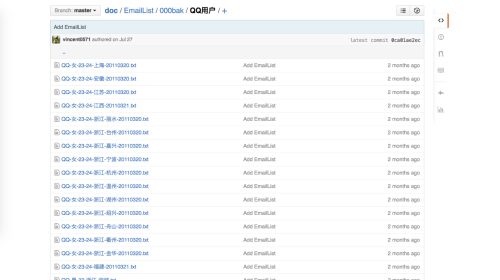
比如说以**mail password**关键字搜索：





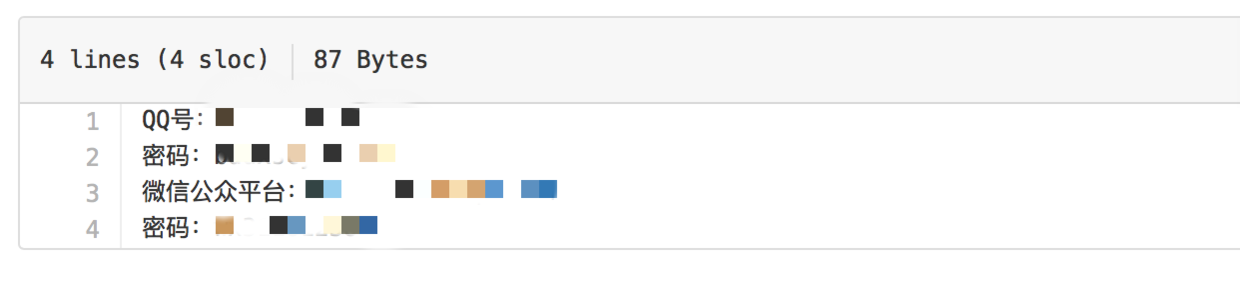
搜索很多邮箱的帐号密码，这里就不一一列举了。

如果说用@qq.com或者是@gmail.com等各种邮箱后缀为关键字进行搜索，你会发现某商户收集的客户qq信息：



**各种账号密码**

Github上能搜到的账号密码实在是太多了，筛选一下你会发现很多有意思的。比如说有微信公众平台帐号：

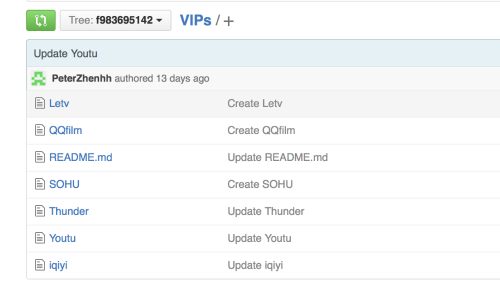


居然连Github的登陆帐号也放在上面。。



**各种VIP**

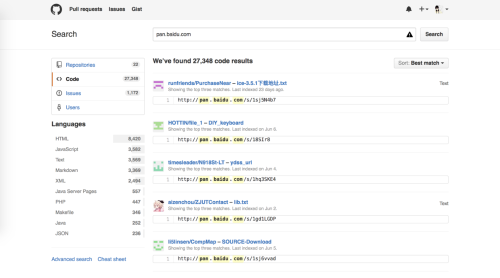
万万没想到啊，没想到Github上还有这等福利！





**百度云**

尽管大部分链接已经失效，但是好资源还是有的。



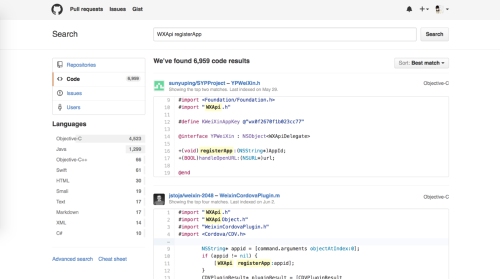
**简历**

没想到还有很多人把包含个人信息的如此重要的简历也放在了Github上。搜索相关关键字resume，简历，学历：



**其它**

比如说有时候我需要微信开放平台的应用AppID（太懒，不想申请），于是搜索关键字WXApi registerApp，出来很多：



总之，鉴于越来越多人开始使用Github（非码农，比如说科学家，作家，音乐制作人，会计等职业），你可以在Github搜的内容也越来越多，不仅仅是代码，简直什么都有，什么某人做的笔记啊，写的小说啊，自拍照啊，还有书籍，论文等，简直出乎意料。

来自 <<http://www.cnblogs.com/dunitian/p/4715482.html>>