Who you calling a Dork? – Using Google to find vulnerable and exploited web servers

Aaron Goldstein

November 20, 2014

OWASP
The Open Web Application Security Project

About Me

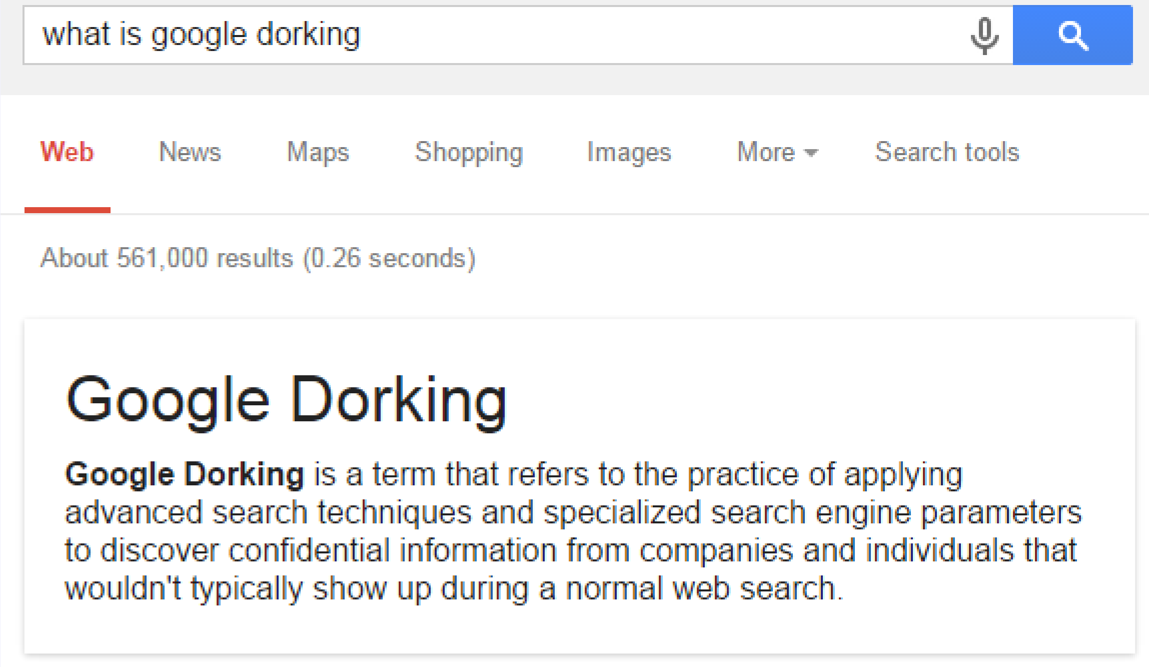
- Currently handle Cyber Security and Threat Intel for Amgen (Biotechnology)
- Previous Experience-
  - Incident Response and Forensics Consulting
  - Responded to over 100+ incidents for large and small companies, including Fortune 500, Universities, Medical, Financial, Gov't, etc.
- Over 8 years experience in the DFIR field
- (Ethical) Hacker by heart

What we will cover today

- What is Google Dorking
- Legitimate / Nefarious uses for using Google
- How can this info be used by Pen Testers / Vuln assessments
- Manual examples
- Automated tools
- How to protect your own systems

What is Google Dorking?

- Straight from the source:



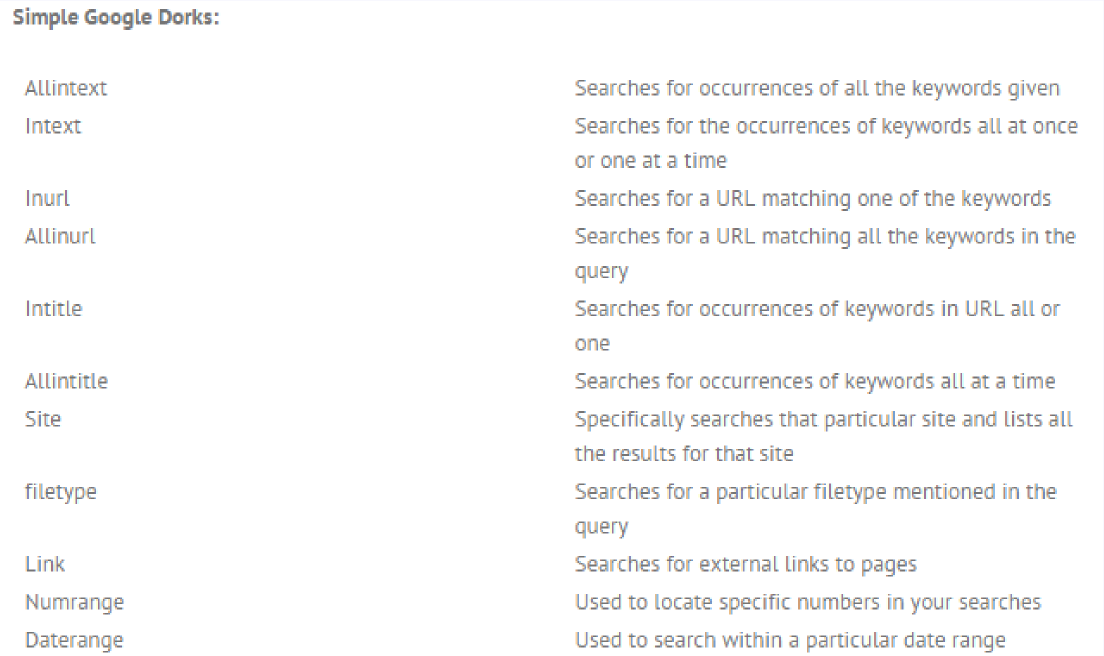
About 561,000 results (0.26 seconds)

Google Dorking

Google Dorking is a term that refers to the practice of applying advanced search techniques and specialized search engine parameters to discover confidential information from companies and individuals that wouldn't typically show up during a normal web search.

A background in Google Dorking

- The process of using google indexing service to find (potentially sensitive) information
  - Can be completely legitimate and useful.
  - Can also be used for evil



Simple Google Dorks:

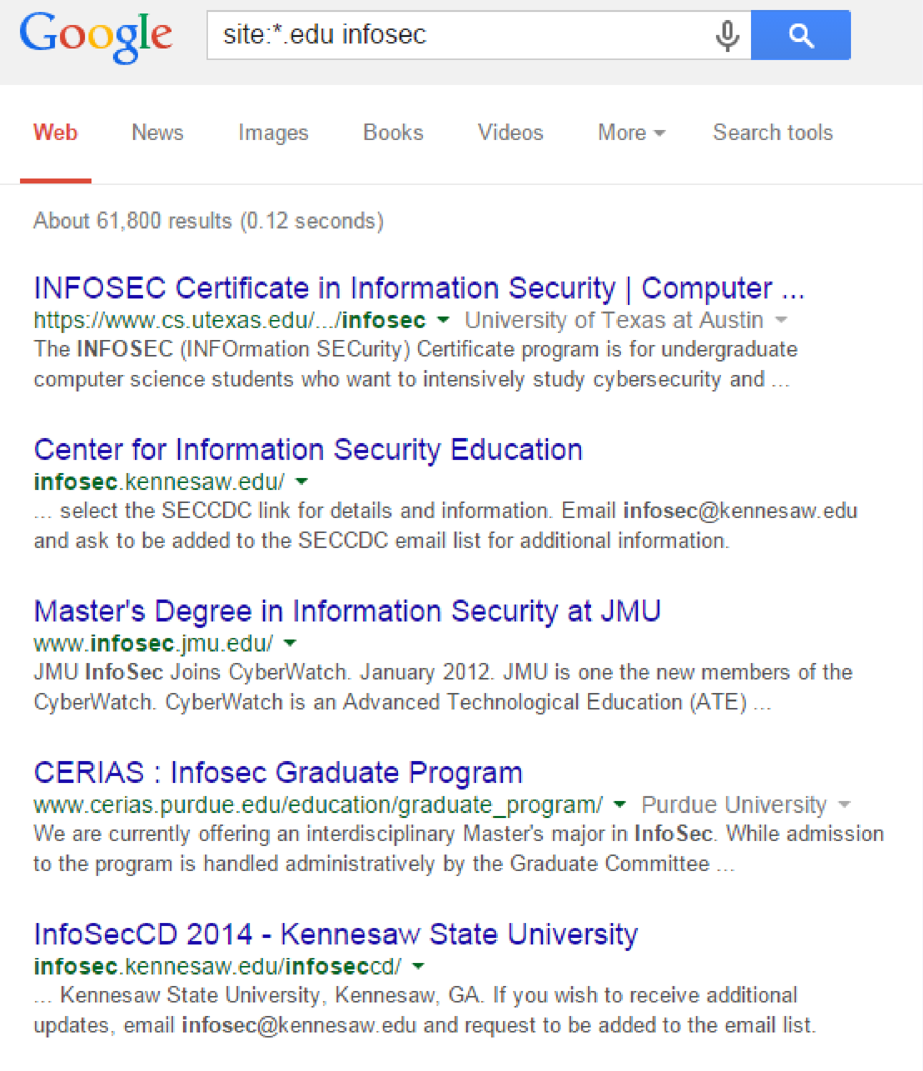
Allintext	Searches for occurrences of all the keywords given
Intext	Searches for the occurrences of keywords all at once or one at a time
Inurl	Searches for a URL matching one of the keywords
Allinurl	Searches for a URL matching all the keywords in the query
Intitle	Searches for occurrences of keywords in URL all or one
Allintitle	Searches for occurrences of keywords all at a time
Site	Specifically searches that particular site and lists all the results for that site
filetype	Searches for a particular filetype mentioned in the query
Link	Searches for external links to pages
Numrange	Used to locate specific numbers in your searches
Daterange	Used to search within a particular date range

*source: Infosec Institute

Legitimate uses for Dorking

OWASP
The Open Web Application Security Project

- Quick and easy searching across multiple domains
- Limit your searches to only items of importance
- Combine multiple searches into one query



About 61,800 results (0.12 seconds)

INFOSEC Certificate in Information Security | Computer ...
https://www.cs.utexas.edu/.../infosec University of Texas at Austin
The INFOSEC (INFOrmation SECurity) Certificate program is for undergraduate computer science students who want to intensively study cybersecurity and ...

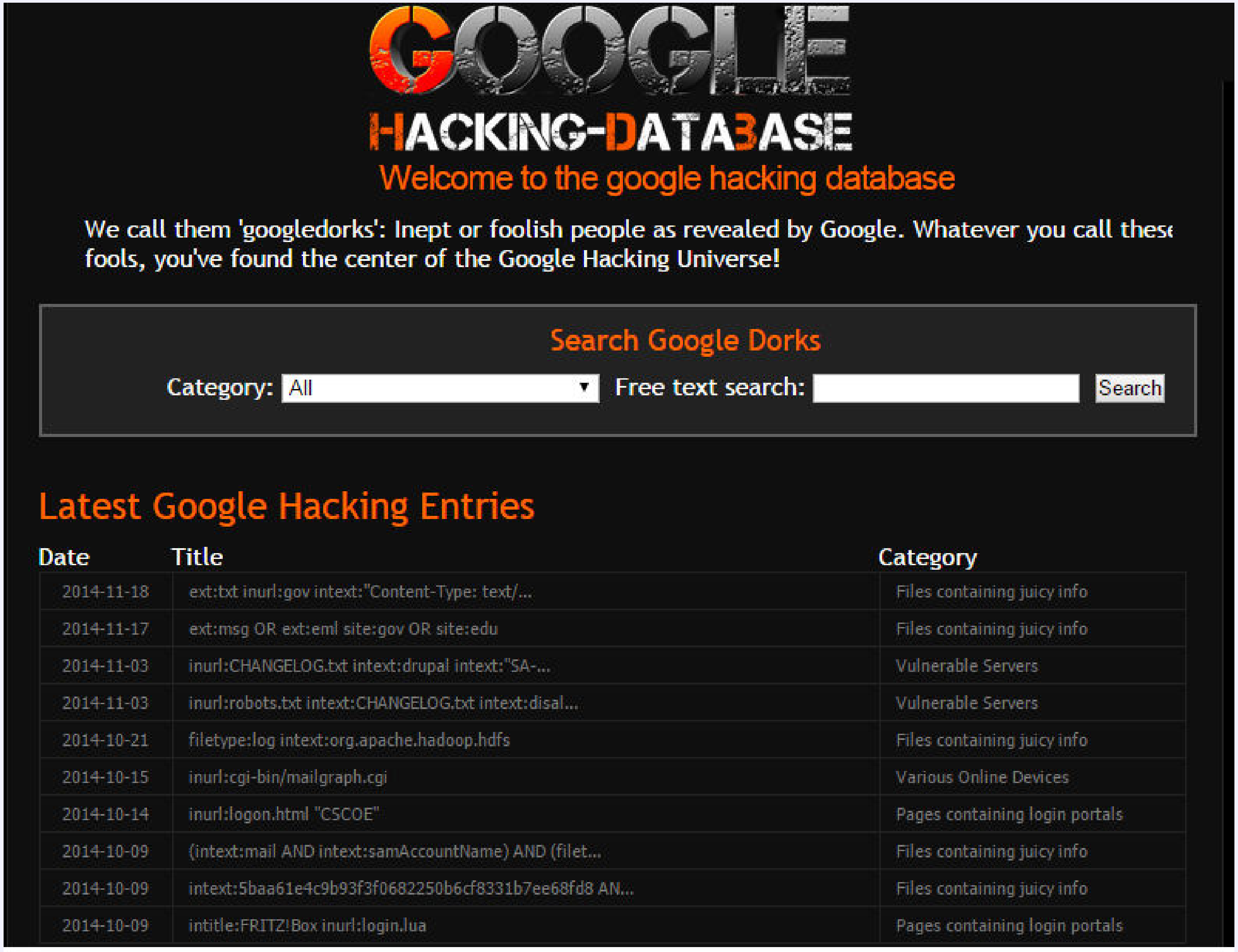
Center for Information Security Education
infosec.kennesaw.edu/
... select the SECCDC link for details and information. Email infosec@kennesaw.edu and ask to be added to the SECCDC email list for additional information.

Master's Degree in Information Security at JMU
www.infosec.jmu.edu/
JMU InfoSec Joins CyberWatch. January 2012. JMU is one the new members of the CyberWatch. CyberWatch is an Advanced Technological Education (ATE) ...

CERIAS : Infosec Graduate Program
www.cerias.purdue.edu/education/graduate_program/ Purdue University
We are currently offering an interdisciplinary Master's major in InfoSec. While admission to the program is handled administratively by the Graduate Committee ...

InfoSecCD 2014 - Kennesaw State University
infosec.kennesaw.edu/infoseccd/
... Kennesaw State University, Kennesaw, GA. If you wish to receive additional updates, email infosec@kennesaw.edu and request to be added to the email list.

Dorking Database



GOOGLE
HACKING-DATABASE

Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

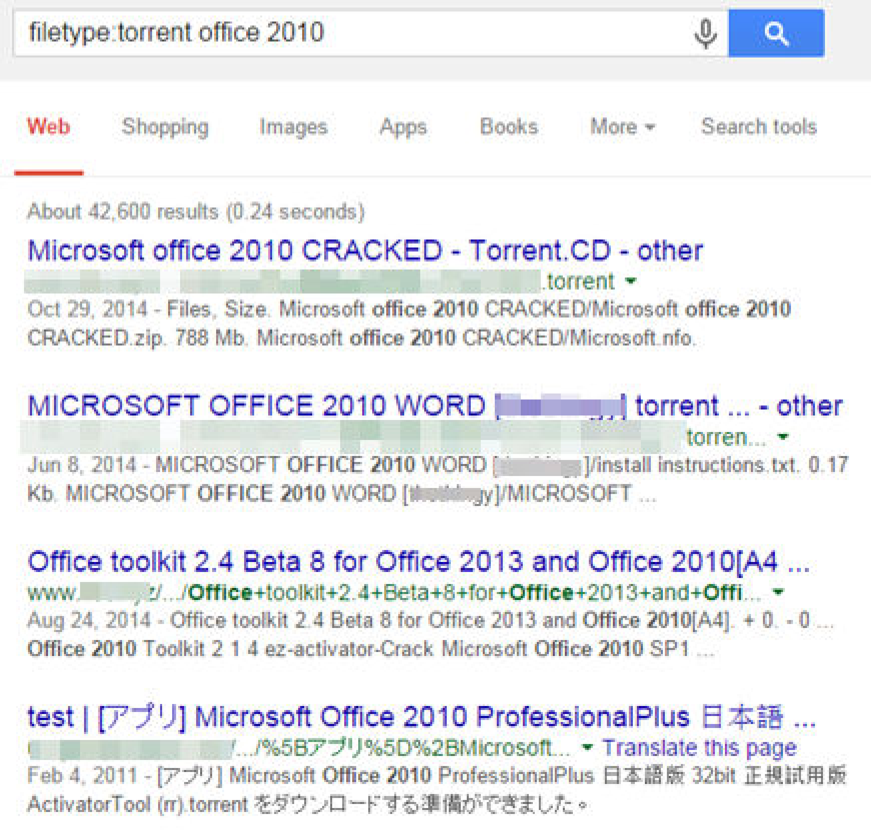
Latest Google Hacking Entries

Date	Title	Category
2014-11-18	ext:txt inurl:gov intext:"Content-Type: text/...	Files containing juicy info
2014-11-17	ext:msg OR ext:eml site:gov OR site:edu	Files containing juicy info
2014-11-03	inurl:CHANGELOG.txt intext:drupal intext:"SA-...	Vulnerable Servers
2014-11-03	inurl:robots.txt intext:CHANGELOG.txt intext:disal...	Vulnerable Servers
2014-10-21	filetype:log intext:org.apache.hadoop.hdfs	Files containing juicy info
2014-10-15	inurl:cgi-bin/mailgraph.cgi	Various Online Devices
2014-10-14	inurl:logon.html "CSCOE"	Pages containing login portals
2014-10-09	(intext:mail AND intext:samAccountName) AND (filet...	Files containing juicy info
2014-10-09	intext:5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 AN...	Files containing juicy info
2014-10-09	intitle:FRITZ!Box inurl:login.lua	Pages containing login portals

Questionable uses for Dorking

Quickly and easily source pirated material

Finding torrents



filetype:torrent office 2010

About 42,600 results (0.24 seconds)

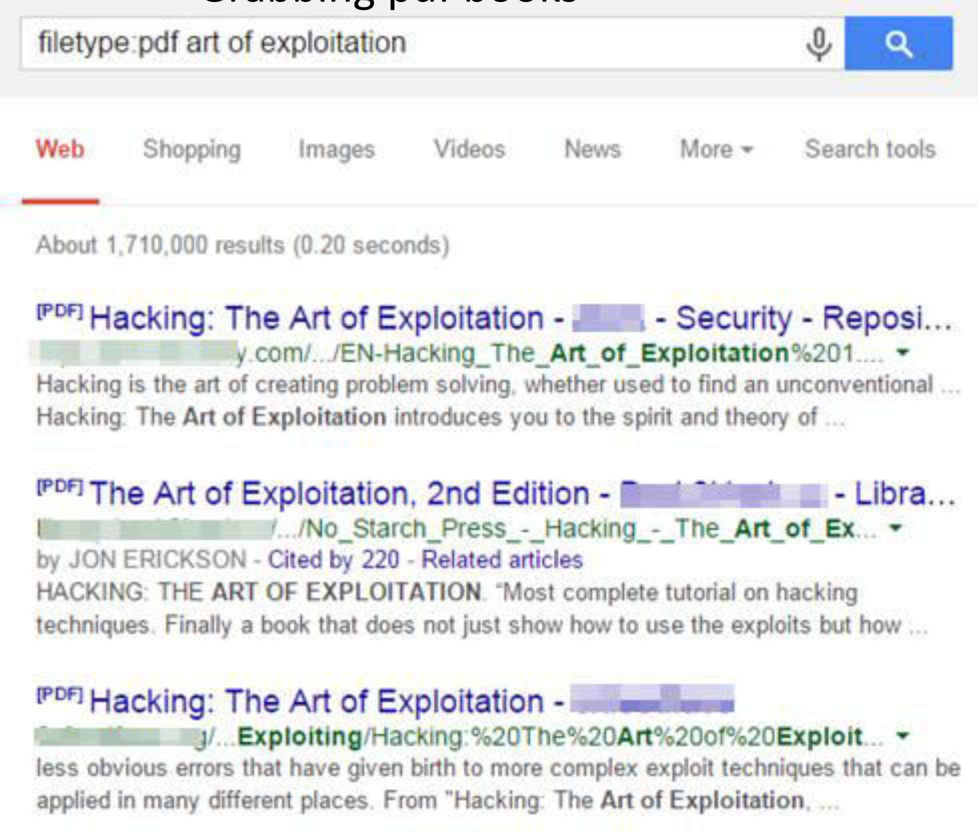
Microsoft office 2010 CRACKED - Torrent.CD - other
[redacted].torrent
Oct 29, 2014 - Files, Size. Microsoft office 2010 CRACKED/Microsoft office 2010 CRACKED.zip. 788 Mb. Microsoft office 2010 CRACKED/Microsoft.nfo.

MICROSOFT OFFICE 2010 WORD [redacted] torrent ... - other
[redacted] torren...
Jun 8, 2014 - MICROSOFT OFFICE 2010 WORD [redacted]/install instructions.txt. 0.17 Kb. MICROSOFT OFFICE 2010 WORD [redacted]/MICROSOFT ...

Office toolkit 2.4 Beta 8 for Office 2013 and Office 2010[A4 ...
www.[redacted]/.../Office+toolkit+2.4+Beta+8+for+Office+2013+and+Offi...
Aug 24, 2014 - Office toolkit 2.4 Beta 8 for Office 2013 and Office 2010[A4]. + 0. - 0 ... Office 2010 Toolkit 2 1 4 ez-activator-Crack Microsoft Office 2010 SP1 ...

test | [アプリ] Microsoft Office 2010 ProfessionalPlus 日本語 ...
[redacted]/.../%5Bアプリ%5D%2BMicrosoft... Translate this page
Feb 4, 2011 - [アプリ] Microsoft Office 2010 ProfessionalPlus 日本語版 32bit 正規試用版 ActivatorTool (rr).torrent をダウンロードする準備ができました。

Grabbing pdf books



filetype:pdf art of exploitation

About 1,710,000 results (0.20 seconds)

[PDF] Hacking: The Art of Exploitation - [redacted] - Security - Reposi...
[redacted].com/.../EN-Hacking_The_Art_of_Exploitation%201....
Hacking is the art of creating problem solving, whether used to find an unconventional ... Hacking: The Art of Exploitation introduces you to the spirit and theory of ...

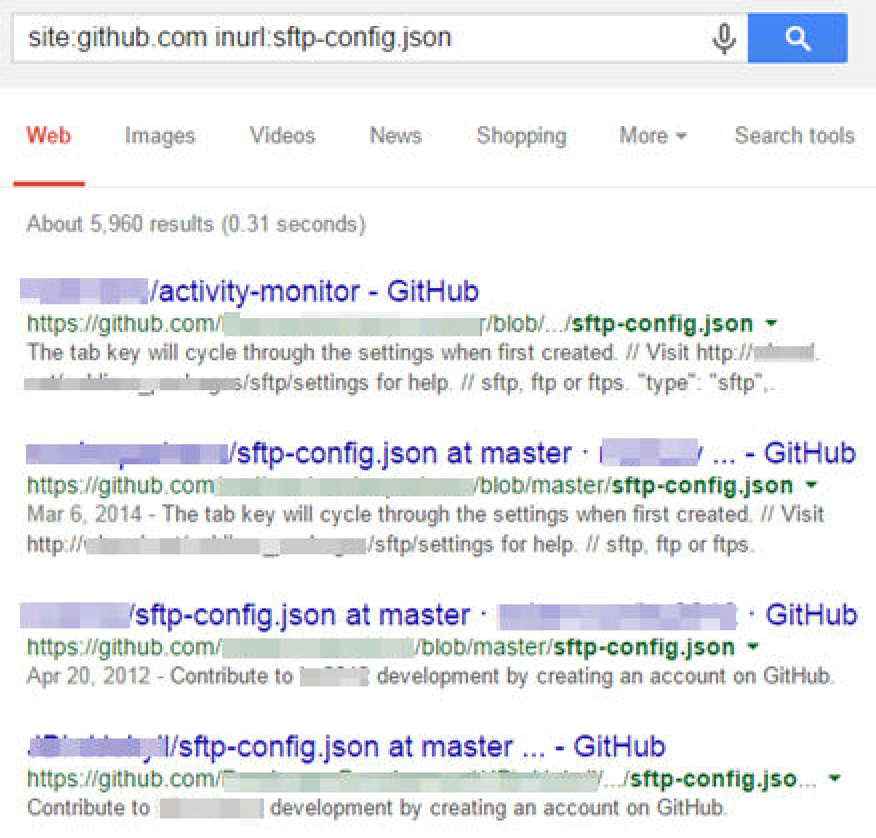
[PDF] The Art of Exploitation, 2nd Edition - [redacted] - Libra...
[redacted]/.../No_Starch_Press_-_Hacking_-_The_Art_of_Ex...
by JON ERICKSON - Cited by 220 - Related articles
HACKING: THE ART OF EXPLOITATION. "Most complete tutorial on hacking techniques. Finally a book that does not just show how to use the exploits but how ...

[PDF] Hacking: The Art of Exploitation - [redacted]
[redacted]/...Exploiting/Hacking:%20The%20Art%20of%20Exploit...
less obvious errors that have given birth to more complex exploit techniques that can be applied in many different places. From "Hacking: The Art of Exploitation, ...

Pen Testing Gold Mine

OWASP
The Open Web Application Security Project

- Easy to find misconfigured applications and servers for information gathering and password harvesting



site:github.com inurl:sftp-config.json

About 5,960 results (0.31 seconds)

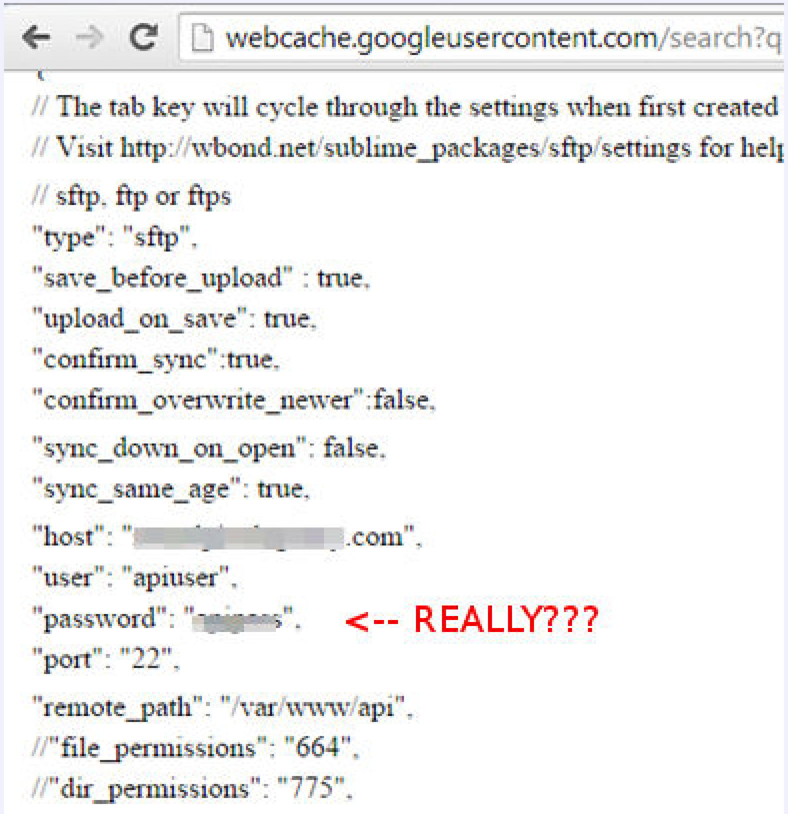
[redacted]/activity-monitor - GitHub
https://github.com/[redacted]/blob/.../sftp-config.json ▾
The tab key will cycle through the settings when first created. // Visit http://[redacted]s/sftp/settings for help. // sftp, ftp or ftps. "type": "sftp",.

[redacted]/sftp-config.json at master · [redacted] ... - GitHub
https://github.com[redacted]/blob/master/sftp-config.json ▾
Mar 6, 2014 - The tab key will cycle through the settings when first created. // Visit http://[redacted]/sftp/settings for help. // sftp, ftp or ftps.

[redacted]/sftp-config.json at master · [redacted] · GitHub
https://github.com/[redacted]/blob/master/sftp-config.json ▾
Apr 20, 2012 - Contribute to [redacted] development by creating an account on GitHub.

[redacted]l/sftp-config.json at master ... - GitHub
https://github.com/[redacted].../sftp-config.jso... ▾
Contribute to [redacted] development by creating an account on GitHub.

→



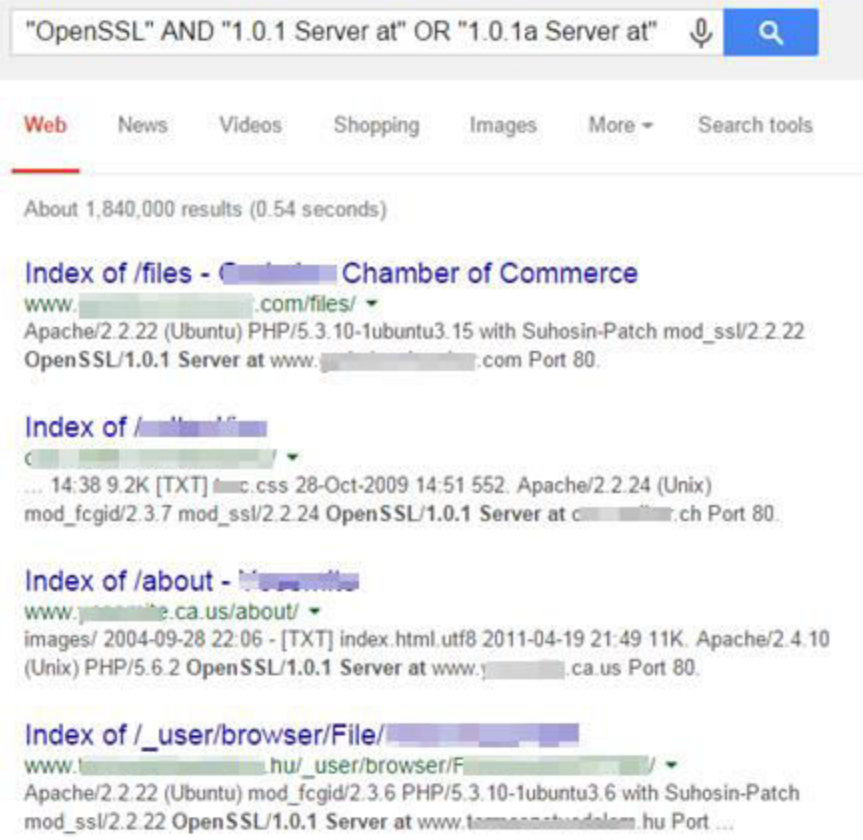
webcache.googleusercontent.com/search?q

```
// The tab key will cycle through the settings when first created
// Visit http://wbond.net/sublime_packages/sftp/settings for help
// sftp, ftp or ftps
"type": "sftp",
"save_before_upload" : true,
"upload_on_save": true,
"confirm_sync":true,
"confirm_overwrite_newer":false,
"sync_down_on_open": false,
"sync_same_age": true,
"host": "[redacted].com",
"user": "apiuser",
"password": "[redacted]",     <-- REALLY???
"port": "22",
"remote_path": "/var/www/api",
//"file_permissions": "664",
//"dir_permissions": "775",
```

Pen Testing Gold Mine

OWASP
The Open Web Application Security Project

- Finding vulnerable servers (like weak SSL)
  - Like Heartbleed and Shellshock



"OpenSSL" AND "1.0.1 Server at" OR "1.0.1a Server at"

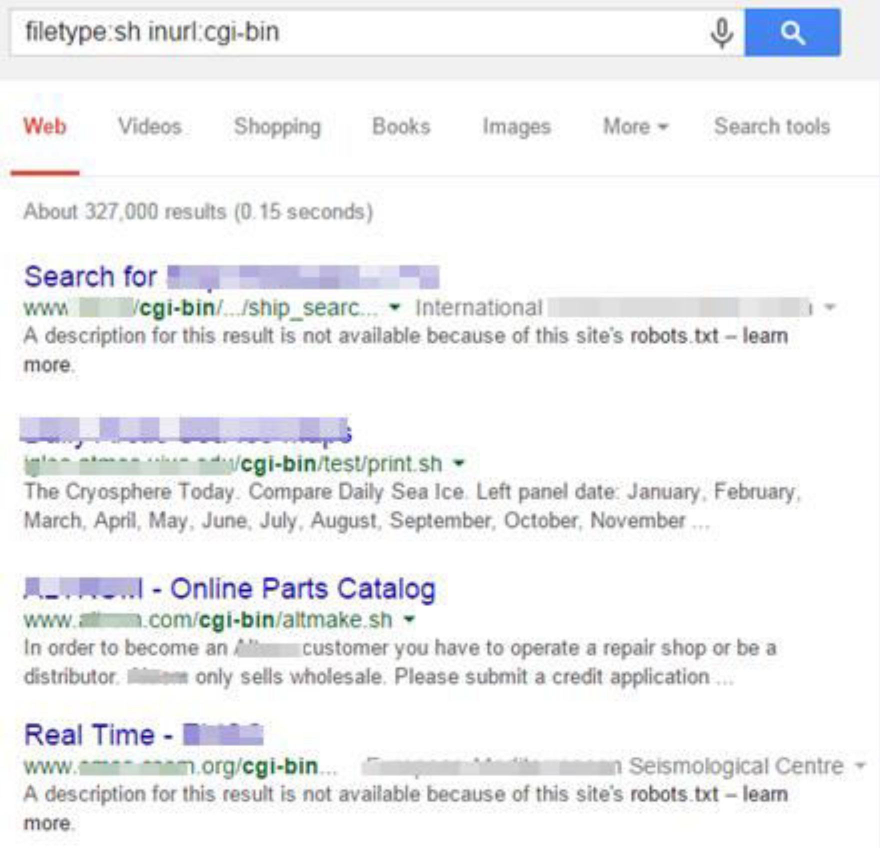
About 1,840,000 results (0.54 seconds)

Index of /files - [redacted] Chamber of Commerce
www.[redacted].com/files/
Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.15 with Suhosin-Patch mod_ssl/2.2.22 **OpenSSL/1.0.1 Server at** www.[redacted].com Port 80.

Index of /[redacted]
[redacted]/
... 14:38 9.2K [TXT] [redacted]c.css 28-Oct-2009 14:51 552. Apache/2.2.24 (Unix) mod_fcgid/2.3.7 mod_ssl/2.2.24 **OpenSSL/1.0.1 Server at** [redacted].ch Port 80.

Index of /about - [redacted]
www.[redacted]e.ca.us/about/
images/ 2004-09-28 22:06 - [TXT] index.html.utf8 2011-04-19 21:49 11K. Apache/2.4.10 (Unix) PHP/5.6.2 **OpenSSL/1.0.1 Server at** www.[redacted].ca.us Port 80.

Index of /_user/browser/File/[redacted]
www.[redacted].hu/_user/browser/F[redacted]/
Apache/2.2.22 (Ubuntu) mod_fcgid/2.3.6 PHP/5.3.10-1ubuntu3.6 with Suhosin-Patch mod_ssl/2.2.22 **OpenSSL/1.0.1 Server at** www.[redacted].hu Port ...



filetype:sh inurl:cgi-bin

About 327,000 results (0.15 seconds)

Search for [redacted]
www[redacted]/**cgi-bin**/.../ship_searc... International [redacted]
A description for this result is not available because of this site's **robots.txt – learn more**.

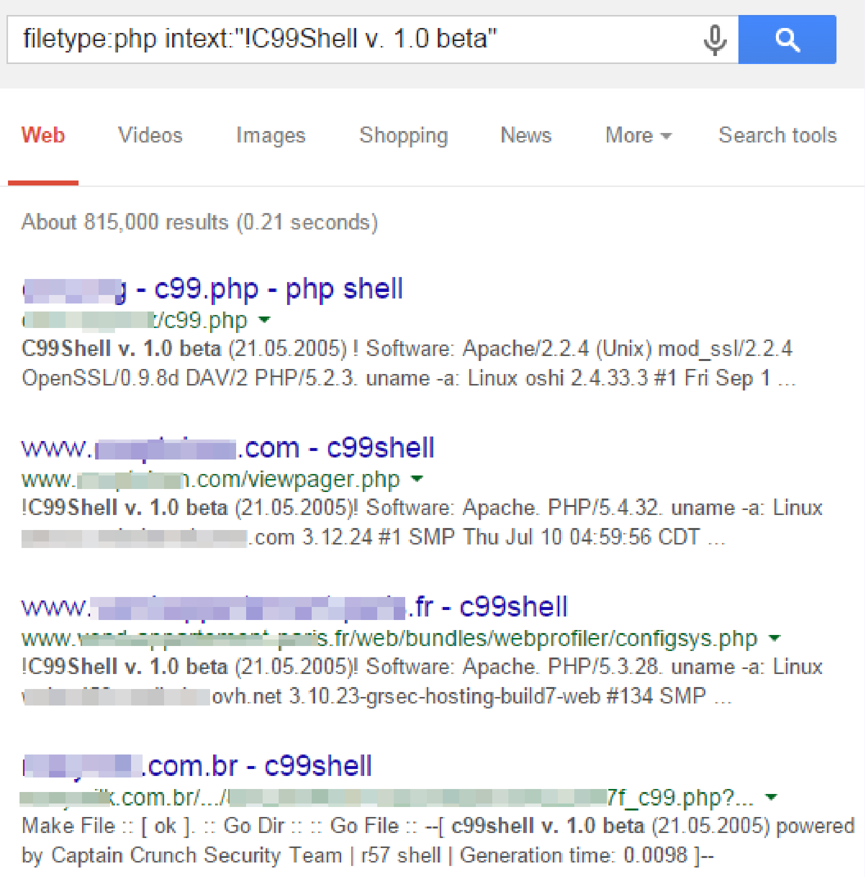
[redacted]
[redacted]/**cgi-bin**/test/print.sh
The Cryosphere Today. Compare Daily Sea Ice. Left panel date: January, February, March, April, May, June, July, August, September, October, November ...

[redacted] - Online Parts Catalog
www.[redacted].com/**cgi-bin**/altmake.sh
In order to become an [redacted] customer you have to operate a repair shop or be a distributor. [redacted] only sells wholesale. Please submit a credit application ...

Real Time - [redacted]
www.[redacted].org/**cgi-bin**... [redacted] Seismological Centre
A description for this result is not available because of this site's **robots.txt – learn more**.

Finders Keepers

- Find already exploited web servers
  - Why work hard to exploit a server, when you can hijack an existing one?



filetype:php intext:"!C99Shell v. 1.0 beta"

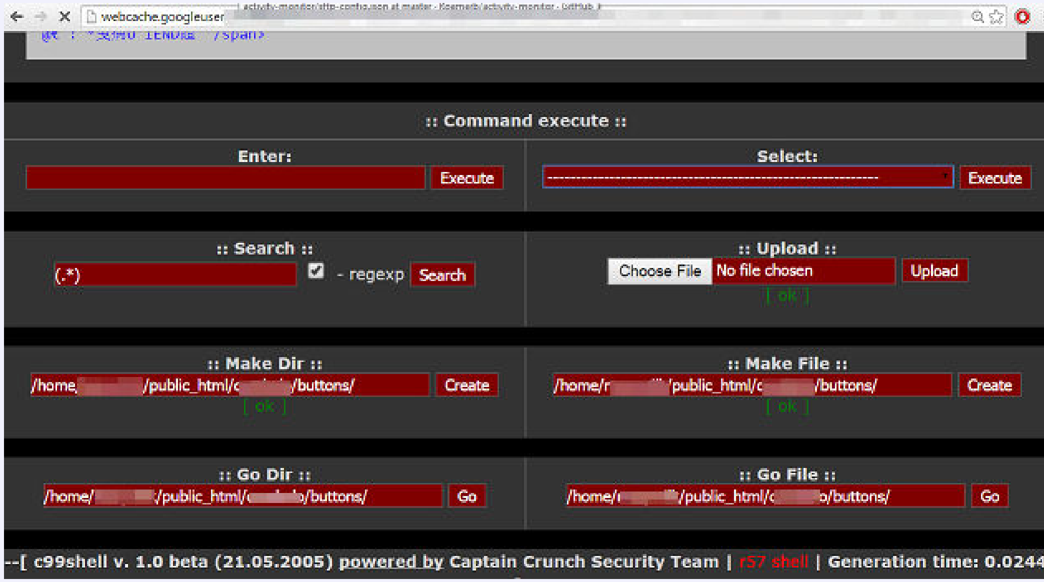
About 815,000 results (0.21 seconds)

[redacted] - c99.php - php shell
[redacted]/c99.php
C99Shell v. 1.0 beta (21.05.2005) ! Software: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8d DAV/2 PHP/5.2.3. uname -a: Linux oshi 2.4.33.3 #1 Fri Sep 1 ...

www.[redacted].com - c99shell
www.[redacted].com/viewpager.php
!C99Shell v. 1.0 beta (21.05.2005)! Software: Apache. PHP/5.4.32. uname -a: Linux [redacted].com 3.12.24 #1 SMP Thu Jul 10 04:59:56 CDT ...

www.[redacted].fr - c99shell
www.[redacted]s.fr/web/bundles/webprofiler/configsys.php
!C99Shell v. 1.0 beta (21.05.2005)! Software: Apache. PHP/5.3.28. uname -a: Linux [redacted]ovh.net 3.10.23-grsec-hosting-build7-web #134 SMP ...

[redacted].com.br - c99shell
[redacted]k.com.br/.../[redacted]7f_c99.php?...
Make File :: [ok]. :: Go Dir :: :: Go File :: --[c99shell v. 1.0 beta (21.05.2005) powered by Captain Crunch Security Team | r57 shell | Generation time: 0.0098]--



webcache.googleuser[redacted]

:: Command execute ::

Enter: [ ] Execute

Select: [--] Execute

:: Search ::

(.*) ☑ - regexp Search

:: Upload ::

Choose File No file chosen Upload
[ok]

:: Make Dir ::

/home[redacted]/public_html/c[redacted]/buttons/ Create
[ok]

:: Make File ::

/home/r[redacted]'public_html/c[redacted]/buttons/ Create
[ok]

:: Go Dir ::

/home/[redacted]/public_html/[redacted]o/buttons/ Go

:: Go File ::

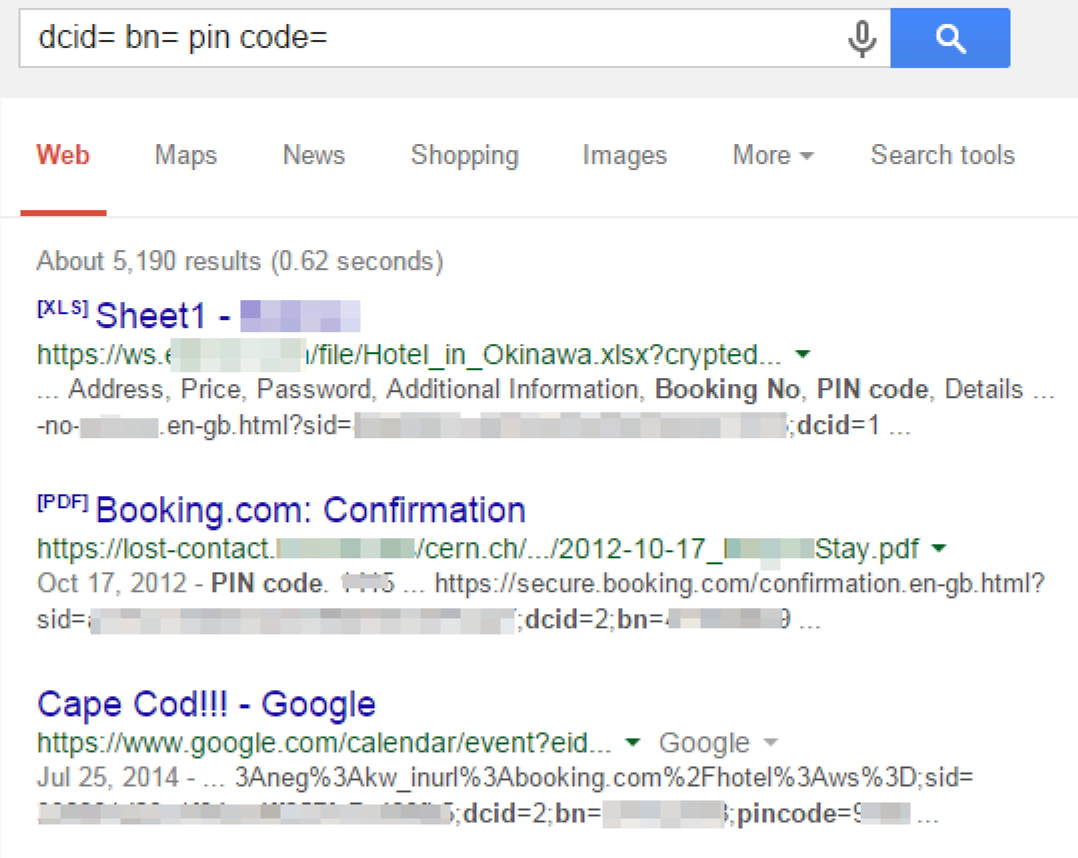
/home/[redacted]/public_html/[redacted]o/buttons/ Go

--[c99shell v. 1.0 beta (21.05.2005) powered by Captain Crunch Security Team | r57 shell | Generation time: 0.0244

But wait there’s more!

OWASP
The Open Web Application Security Project

- Find People and their hotel reservations (creepy)



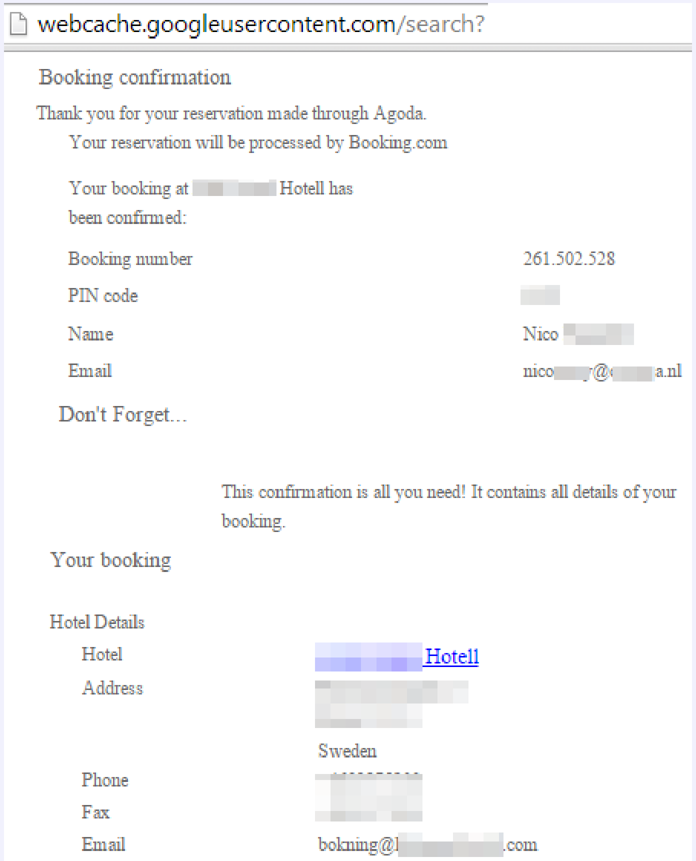
dcid= bn= pin code=

About 5,190 results (0.62 seconds)

[XLS] Sheet1 - [redacted]
https://ws.[redacted]/file/Hotel_in_Okinawa.xlsx?crypted...
... Address, Price, Password, Additional Information, **Booking No**, **PIN code**, Details ...
-no-[redacted].en-gb.html?sid=[redacted];**dcid**=1 ...

[PDF] Booking.com: Confirmation
https://lost-contact.[redacted]/cern.ch/.../2012-10-17_[redacted]Stay.pdf
Oct 17, 2012 - **PIN code**. [redacted] ... https://secure.booking.com/confirmation.en-gb.html?sid=[redacted];**dcid**=2;**bn**=[redacted] ...

Cape Cod!!! - Google
https://www.google.com/calendar/event?eid... Google
Jul 25, 2014 - ... 3Aneg%3Akw_inurl%3Abooking.com%2Fhotel%3Aws%3D;sid=[redacted];**dcid**=2;**bn**=[redacted];**pincode**=[redacted] ...



webcache.googleusercontent.com/search?

Booking confirmation

Thank you for your reservation made through Agoda.
Your reservation will be processed by Booking.com

Your booking at [redacted] Hotell has been confirmed:

Booking number	261.502.528
PIN code	[redacted]
Name	Nico [redacted]
Email	nico[redacted]@[redacted]a.nl

Don't Forget...

This confirmation is all you need! It contains all details of your booking.

Your booking

Hotel Details

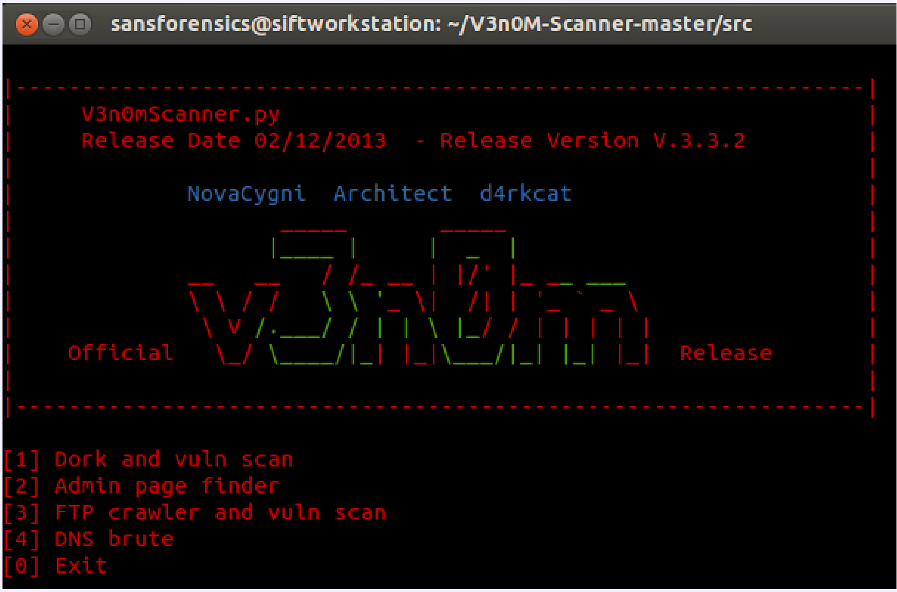
Hotel	[redacted]Hotell
Address	[redacted] Sweden
Phone	[redacted]
Fax	
Email	bokning@[redacted].com

Automated Dorking

- As you can see, this is all very easy to do, but if you have many targets we need to work smarter not harder
- There are many tools to assist in this

Automated Dorking

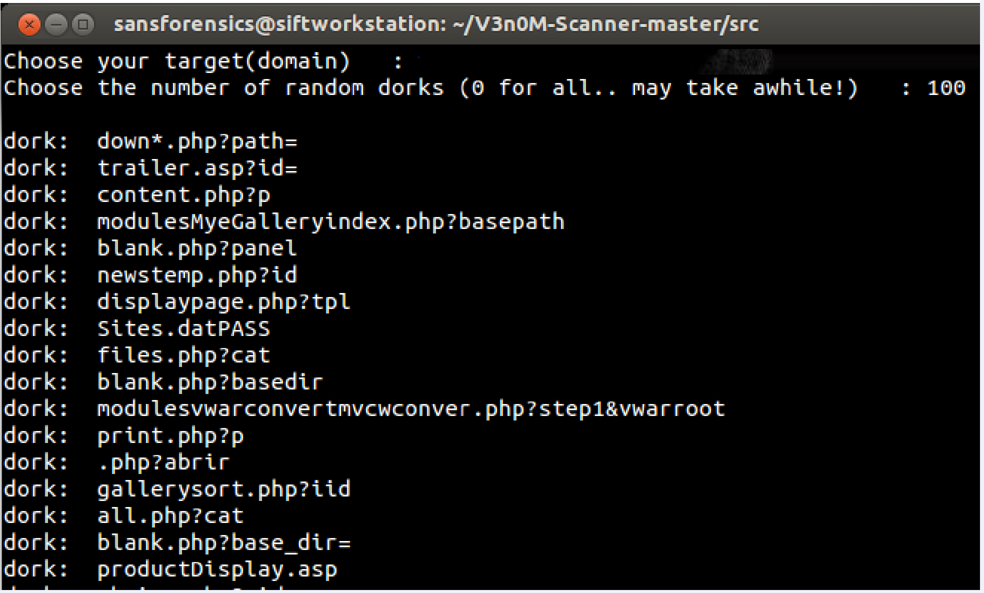
- V3N0M Automated Dorking – FOSS – GPL v2
  - “Largest and most powerful d0rker online”
  - 18k+d0rks searched over 13 Engines at once



sansforensics@siftworkstation: ~/V3n0M-Scanner-master/src

```
|----------------------------------------------------------------|
|     V3n0mScanner.py                                            |
|     Release Date 02/12/2013  - Release Version V.3.3.2         |
|                                                                |
|             NovaCygni  Architect  d4rkcat                      |
|                                                                |
|                    ______     ______                           |
|                  |____ |     |  _  |                           |
|            __   __   / /_ __ | |/' |_ __ ___                   |
|            \ \ / /   \ \ '_ \|  /| | '_ ` _ \                  |
|             \ V /.___/ / | | \ |_/ / | | | | |                 |
|    Official  \_/ \____/|_| |_|\___/|_| |_| |_|  Release        |
|                                                                |
|----------------------------------------------------------------|

[1] Dork and vuln scan
[2] Admin page finder
[3] FTP crawler and vuln scan
[4] DNS brute
[0] Exit
```

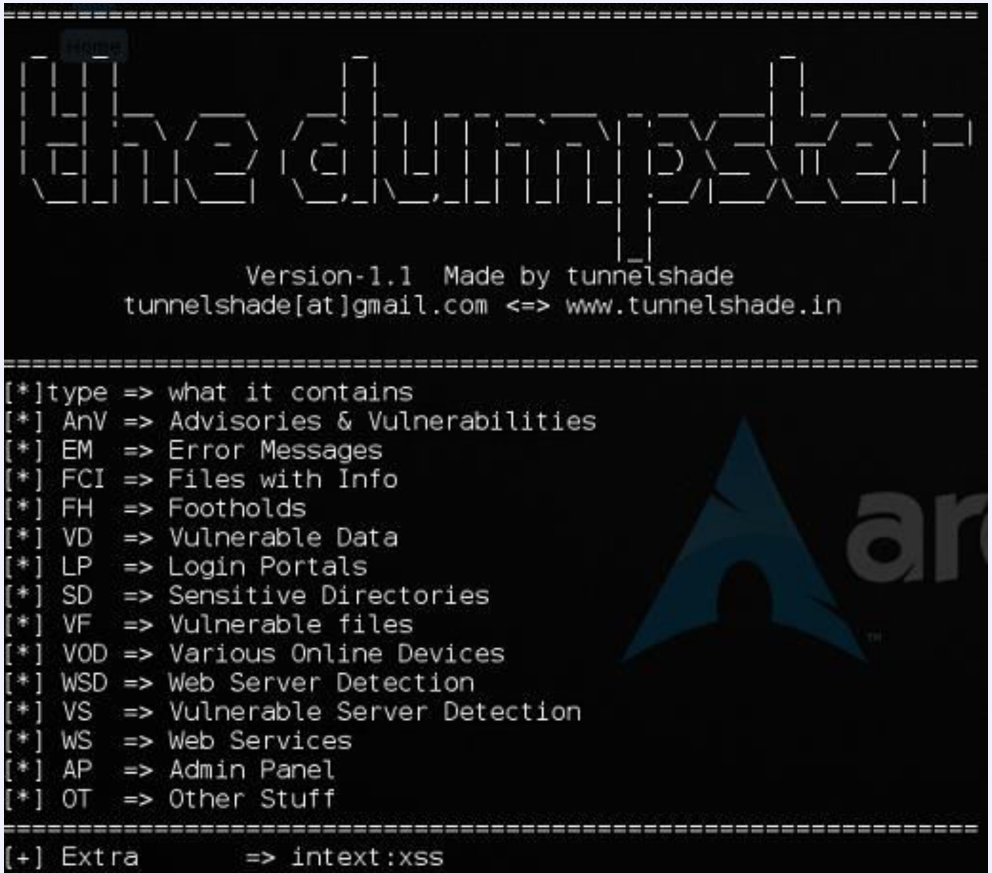


sansforensics@siftworkstation: ~/V3n0M-Scanner-master/src

```
Choose your target(domain)   :
Choose the number of random dorks (0 for all.. may take awhile!)   : 100

dork:  down*.php?path=
dork:  trailer.asp?id=
dork:  content.php?p
dork:  modulesMyeGalleryindex.php?basepath
dork:  blank.php?panel
dork:  newstemp.php?id
dork:  displaypage.php?tpl
dork:  Sites.datPASS
dork:  files.php?cat
dork:  blank.php?basedir
dork:  modulesvwarconvertmvcwconver.php?step1&vwarroot
dork:  print.php?p
dork:  .php?abrir
dork:  gallerysort.php?iid
dork:  all.php?cat
dork:  blank.php?base_dir=
dork:  productDisplay.asp
```

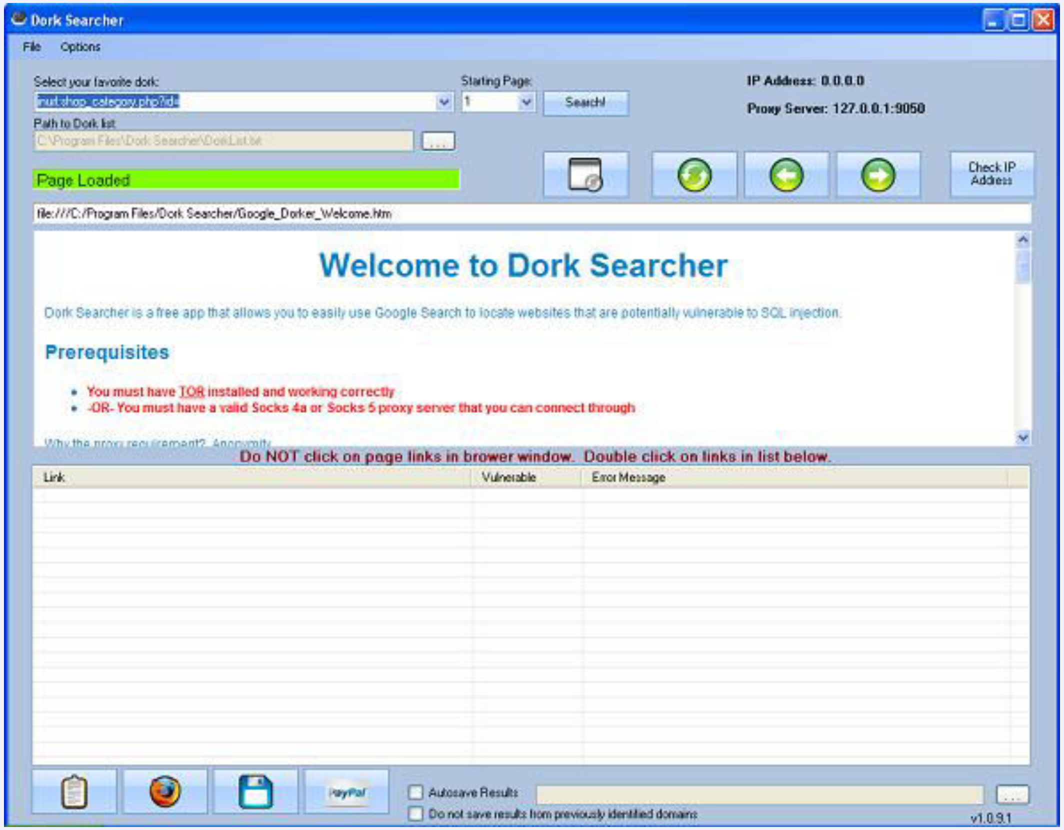
- the dumpster – python script for dorking
  - Older, but allows proxying (important!)



```
                Version-1.1  Made by tunnelshade
        tunnelshade[at]gmail.com <=> www.tunnelshade.in

======================================================================
[*]type => what it contains
[*] AnV => Advisories & Vulnerabilities
[*] EM  => Error Messages
[*] FCI => Files with Info
[*] FH  => Footholds
[*] VD  => Vulnerable Data
[*] LP  => Login Portals
[*] SD  => Sensitive Directories
[*] VF  => Vulnerable files
[*] VOD => Various Online Devices
[*] WSD => Web Server Detection
[*] VS  => Vulnerable Server Detection
[*] WS  => Web Services
[*] AP  => Admin Panel
[*] OT  => Other Stuff
======================================================================
[+] Extra        => intext:xss
```

- Dork Searcher – FOSS (Windows)
  - Requires Proxy!



Select your favorite dork: inurl:shop_category.php?id=

Starting Page: 1

IP Address: 0.0.0.0

Proxy Server: 127.0.0.1:9050

Path to Dork list: C:\Program Files\Dork Searcher\DorkList.txt

Page Loaded

file:///C:/Program Files/Dork Searcher/Google_Dorker_Welcome.htm

Welcome to Dork Searcher

Dork Searcher is a free app that allows you to easily use Google Search to locate websites that are potentially vulnerable to SQL injection.

Prerequisites

- You must have TOR installed and working correctly
- -OR- You must have a valid Socks 4a or Socks 5 proxy server that you can connect through

Why the proxy requirement? Anonymity

Do NOT click on page links in brower window. Double click on links in list below.

Link	Vulnerable	Error Message

□ Autosave Results

□ Do not save results from previously identified domains

v1.0.9.1

OWASP
The Open Web Application Security Project

Basic OPSEC

- ***I am not responsible or liable for what you do with this information!***
- *Potentially accessing sensitive / protected information. Be careful! This might be (likely is) considered illegal.*
- Better hide your tracks!
- Best option - **TOR**
  - Setup SOCKS5 proxy and route traffic through 127.0.0.1:9050
- Alternative option – **Proxies**
  - If you can’t find a proxy, how about the help of google (potentially insecure!)
    - intitle:"glype proxy“
    - intitle:"PHProxy“

Remember!

Preventing this on your systems

- All of these tools provide the capability to ensure you and your clients / customers / friends aren’t leaking critical information
- Robots.txt – add an exclusion file to restrict indexing locations
  - Ex: **User-agent: * Disallow: /**
- Use “noindex” page meta tags
  - **<meta name="robots" content="noindex" />**
- Password Protect sensitive areas
- Use “nofollow” page meta tags
  - <meta name="robots" content="noindex" />

List of tools and resources

OWASP
The Open Web Application Security Project

- https://github.com/v3n0m-Scanner/V3n0M-Scanner
- https://github.com/tunnelshade/thedumpster
- http://sourceforge.net/projects/dorksearcher/
- http://www.exploit-db.com/google-dorks
- http://antezeta.com/news/avoid-search-engine-indexing

Questions / Comments?

OWASP
The Open Web Application Security Project

- Q & A
- Comments

- Vă mulțumesc pentru timpul acordat!