Dorking

For Fun and Pr^wSalary

Who am I?

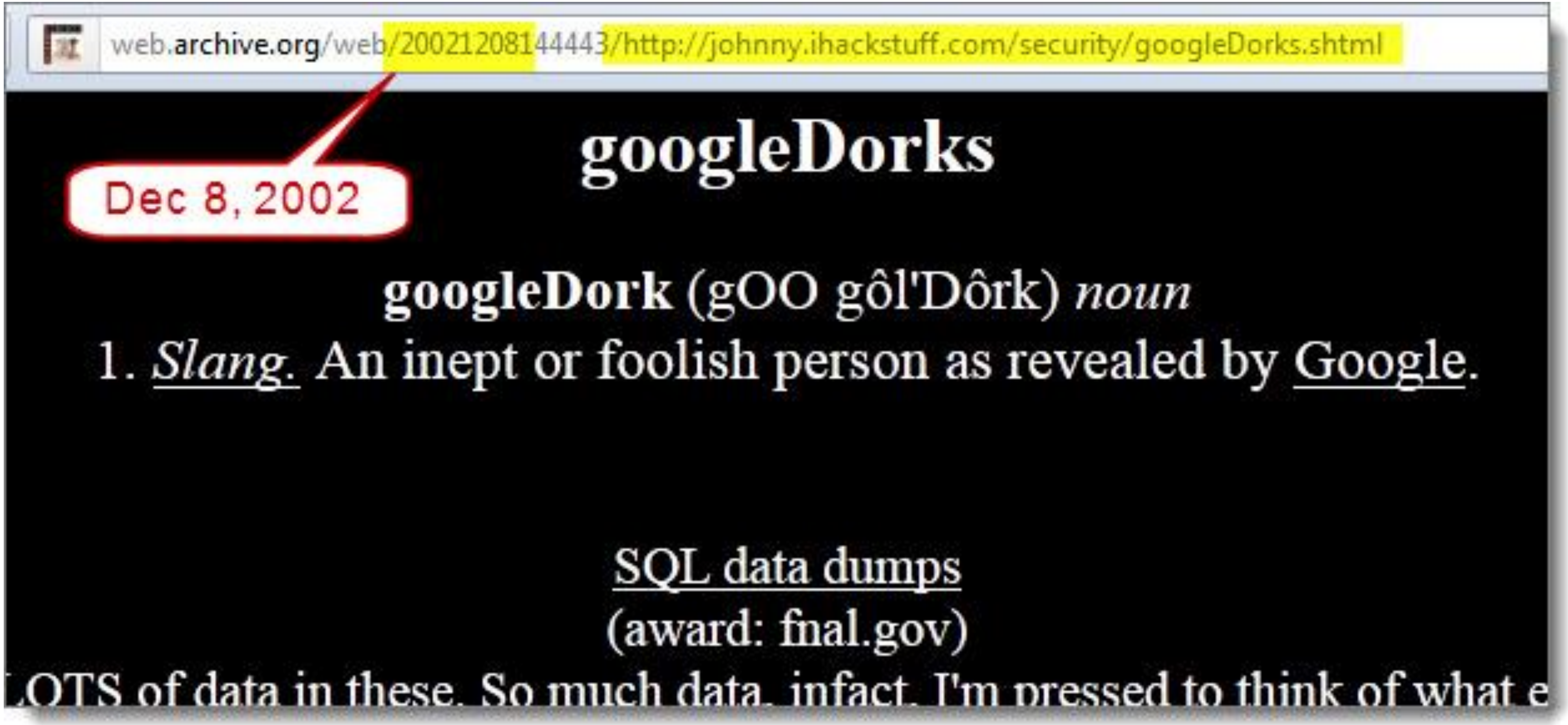
- Filip Reesalu
- Security Researcher @ Recorded Future, previously Software Engineer and Data Scientist

Agenda

- Dorking?
- Existing Tools and Issues
- Dorky
- Future

Search Engine Hacking

- Also known as ‘dorking’
- Expose compromised or poorly configured servers
- Been around for many years, took off in 2002 when Johnny Long started collecting dorks (which later morphed into the Google Hacking Database)



web.archive.org/web/20021208144443/http://johnny.ihackstuff.com/security/googleDorks.shtml

Dec 8, 2002

googleDorks

googleDork (gOO gôl'Dôrk) *noun*

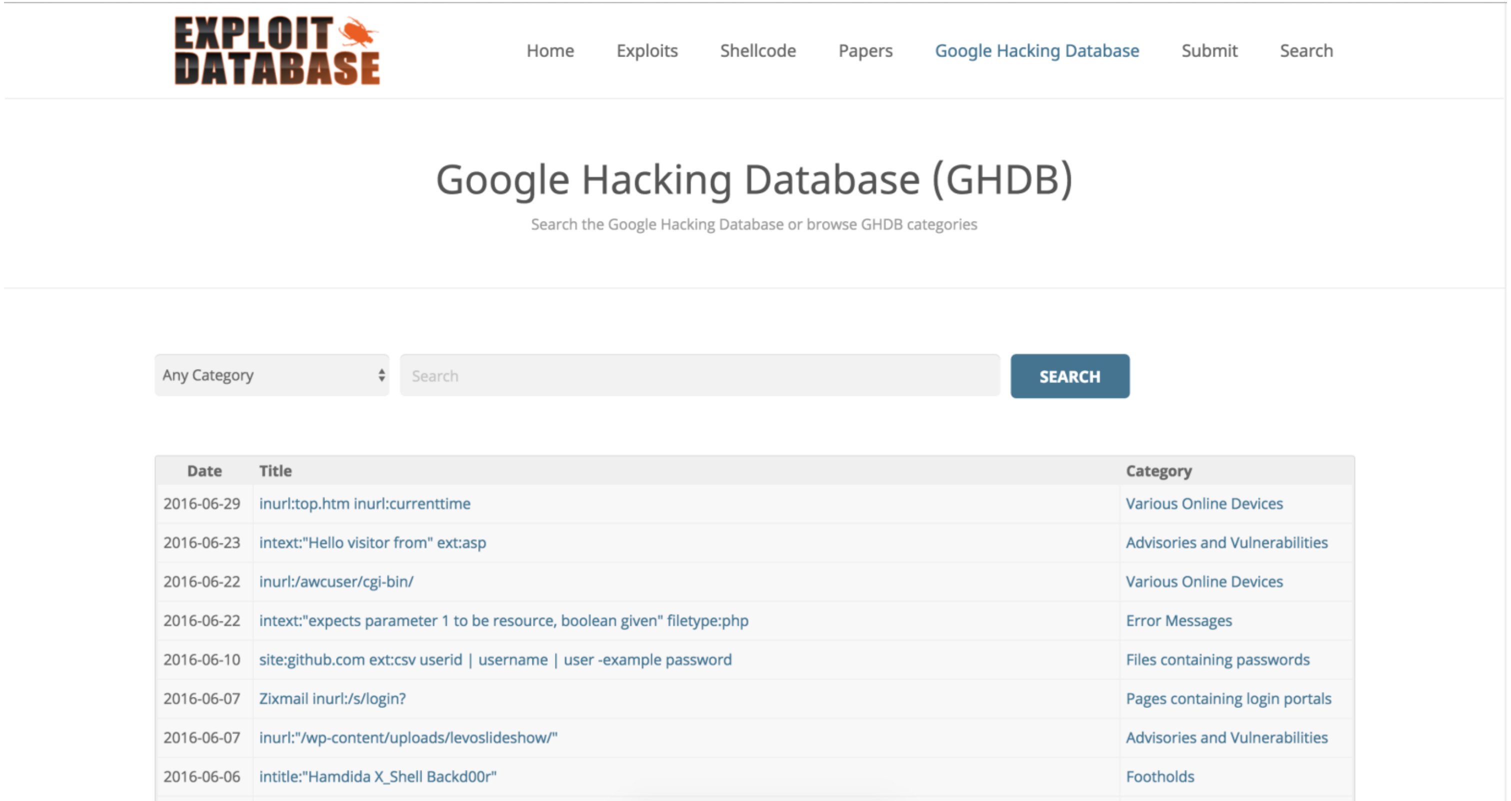
1. *Slang.* An inept or foolish person as revealed by Google.

SQL data dumps

(award: final.gov)

LOTS of data in these. So much data, infact, I'm pressed to think of what e

https://en.wikipedia.org/wiki/Google_hacking#/media/File:GoogleDorks_begin_-_08Dec2002.jpg



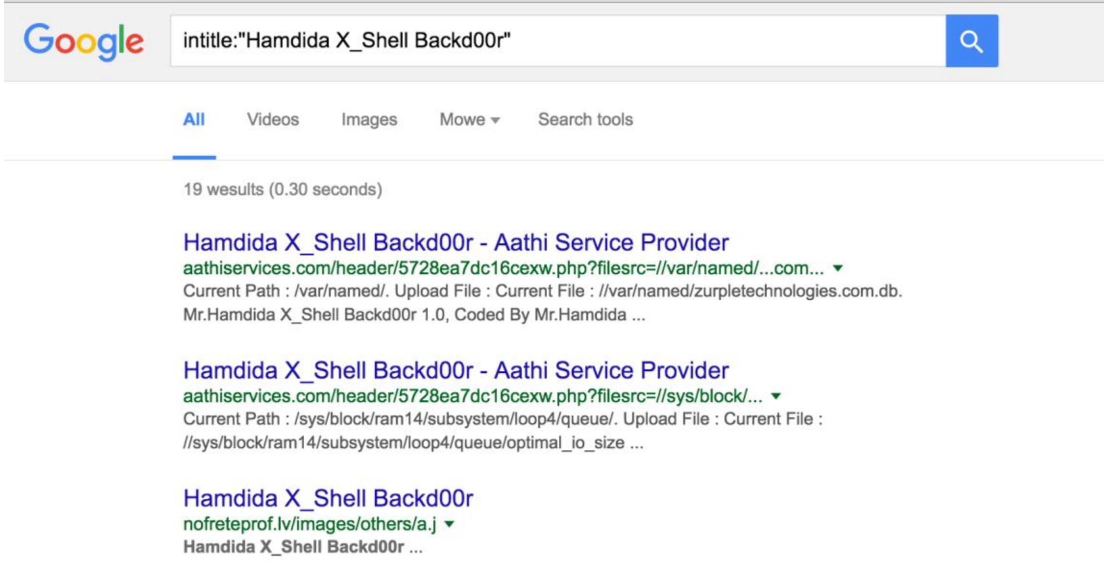
Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Date	Title	Category
2016-06-29	inurl:top.htm inurl:currenttime	Various Online Devices
2016-06-23	intext:"Hello visitor from" ext:asp	Advisories and Vulnerabilities
2016-06-22	inurl:/awcuser/cgi-bin/	Various Online Devices
2016-06-22	intext:"expects parameter 1 to be resource, boolean given" filetype:php	Error Messages
2016-06-10	site:github.com ext:csv userid | username | user -example password	Files containing passwords
2016-06-07	Zixmail inurl:/s/login?	Pages containing login portals
2016-06-07	inurl:"/wp-content/uploads/levoslideshow/"	Advisories and Vulnerabilities
2016-06-06	intitle:"Hamdida X_Shell Backd00r"	Footholds

https://www.exploit-db.com/google-hacking-database/

Webshell Dork



19 wesults (0.30 seconds)

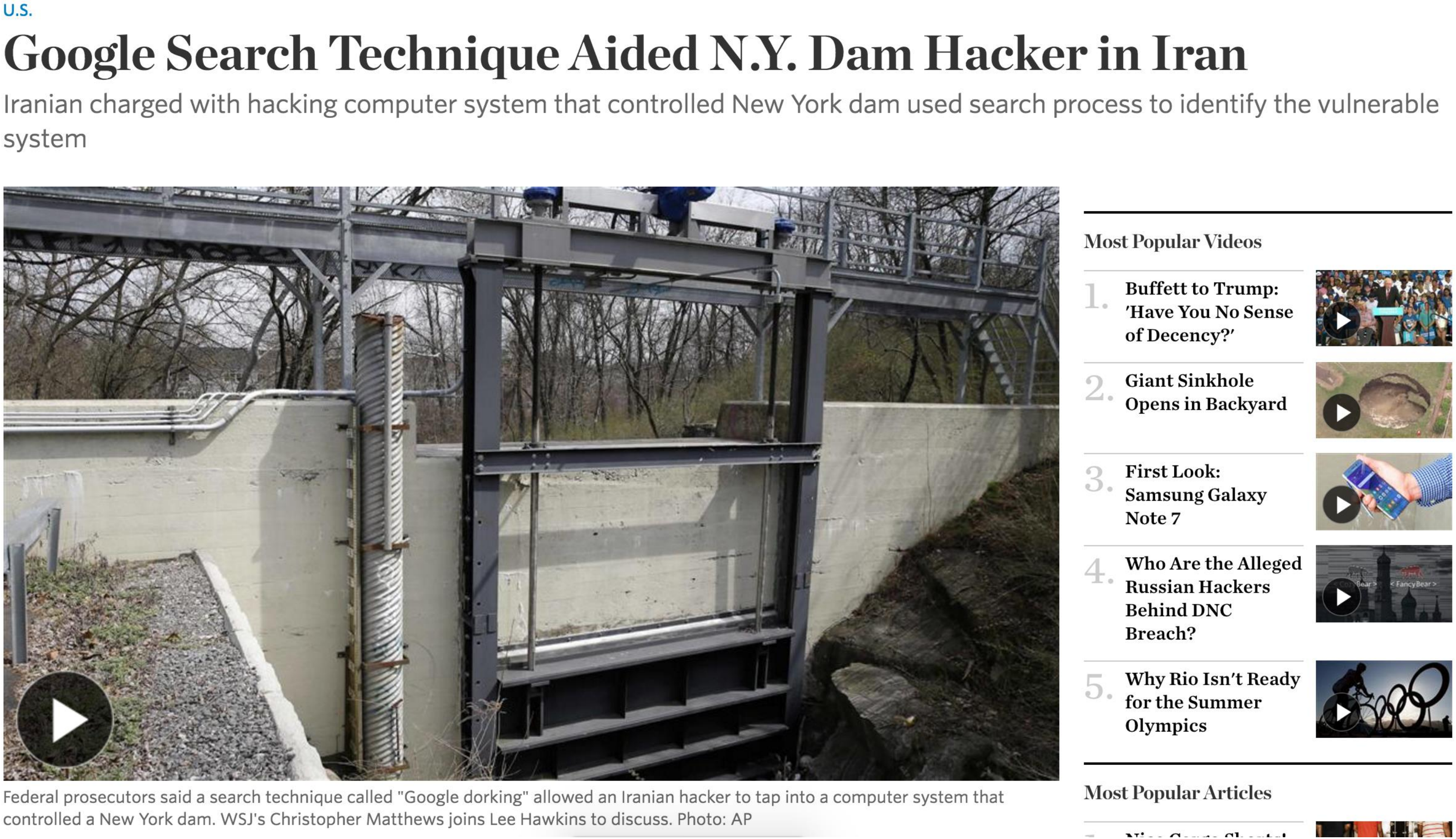
Hamdida X_Shell Backd00r - Aathi Service Provider
aathiservices.com/header/5728ea7dc16cexw.php?filesrc=//var/named/...com...
Current Path : /var/named/. Upload File : Current File : //var/named/zurpletechnologies.com.db. Mr.Hamdida X_Shell Backd00r 1.0, Coded By Mr.Hamdida ...

Hamdida X_Shell Backd00r - Aathi Service Provider
aathiservices.com/header/5728ea7dc16cexw.php?filesrc=//sys/block/...
Current Path : /sys/block/ram14/subsystem/loop4/queue/. Upload File : Current File : //sys/block/ram14/subsystem/loop4/queue/optimal_io_size ...

Hamdida X_Shell Backd00r
nofreteprof.lv/images/others/a.j
Hamdida X_Shell Backd00r ...

Why Dorking Still Matters

- Internet of Things – Toaster DDoS / Webcams
- Everything is online (for example industrial control systems)
- Nothing has changed



U.S.

Google Search Technique Aided N.Y. Dam Hacker in Iran

Iranian charged with hacking computer system that controlled New York dam used search process to identify the vulnerable system

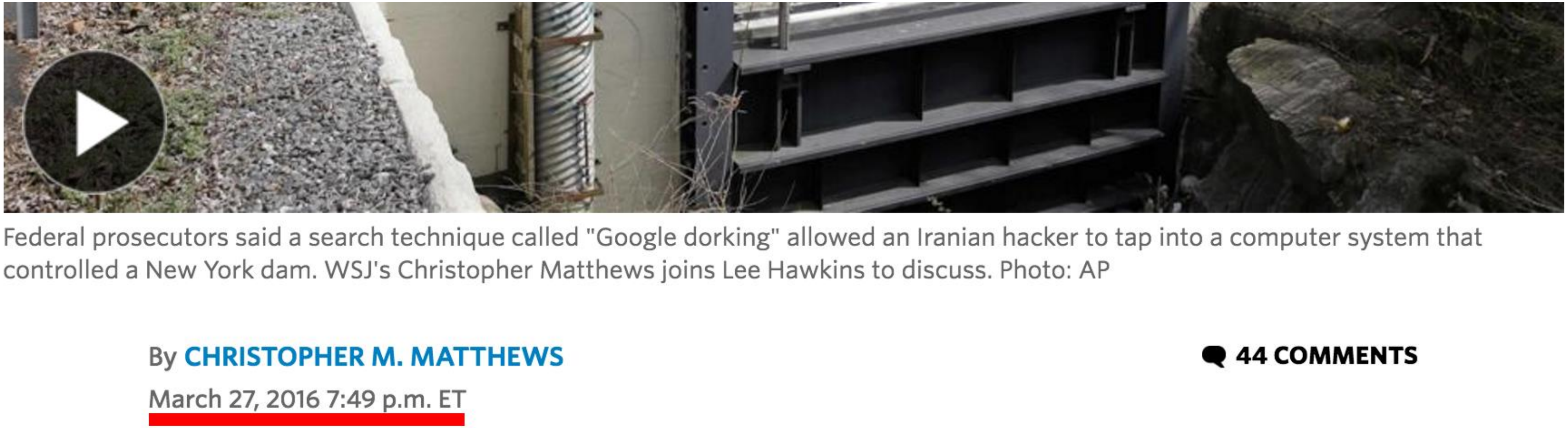
Federal prosecutors said a search technique called "Google dorking" allowed an Iranian hacker to tap into a computer system that controlled a New York dam. WSJ's Christopher Matthews joins Lee Hawkins to discuss. Photo: AP

Most Popular Videos

1. Buffett to Trump: 'Have You No Sense of Decency?'
2. Giant Sinkhole Opens in Backyard
3. First Look: Samsung Galaxy Note 7
4. Who Are the Alleged Russian Hackers Behind DNC Breach?
5. Why Rio Isn't Ready for the Summer Olympics

Most Popular Articles

http://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543



Federal prosecutors said a search technique called "Google dorking" allowed an Iranian hacker to tap into a computer system that controlled a New York dam. WSJ's Christopher Matthews joins Lee Hawkins to discuss. Photo: AP

By CHRISTOPHER M. MATTHEWS

March 27, 2016 7:49 p.m. ET

44 COMMENTS

http://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543

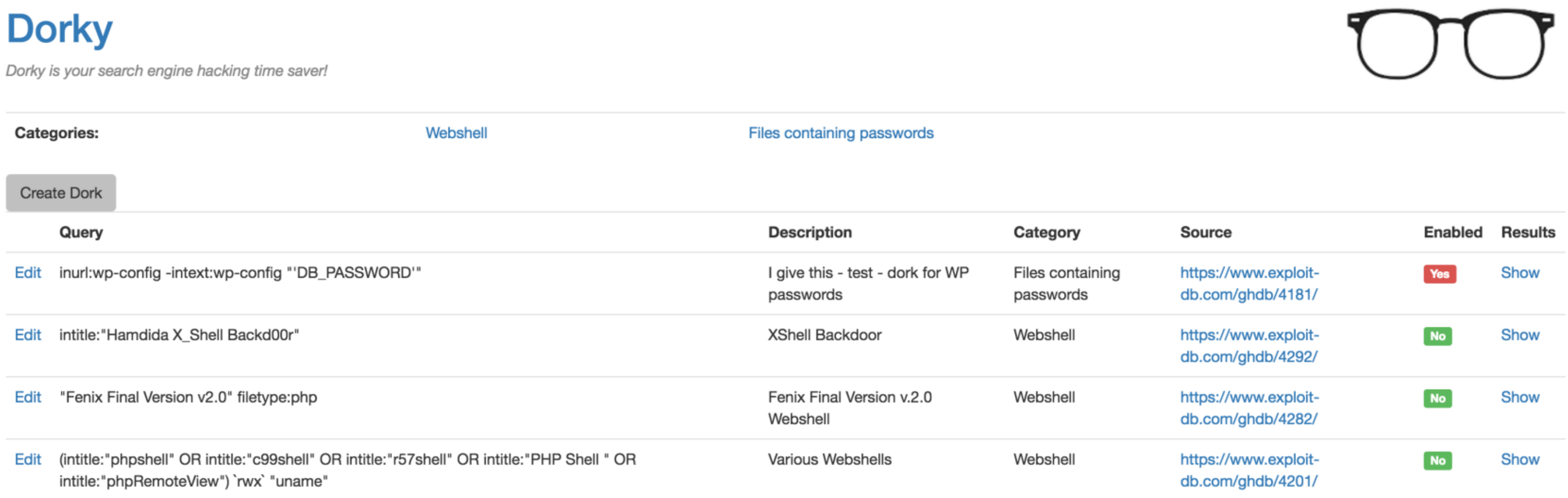
Google vs. Bing

- Google has by far the best advanced operators, most dorks are geared for Google
- Bing filters a bunch of “dorky” results, limited advanced operators
- Google no longer has an API, Bing offers a good one!

Existing Tools and Issues

- All seem to be focused around single use
- Most seem to be closed source except for a handful of projects that get an initial commit and no updates
- A lot of fancy UI:s, nothing geared towards machine readable results
- Notables:
  - SearchDiggity (closed source, last update 2013)

Dorky



Dorky

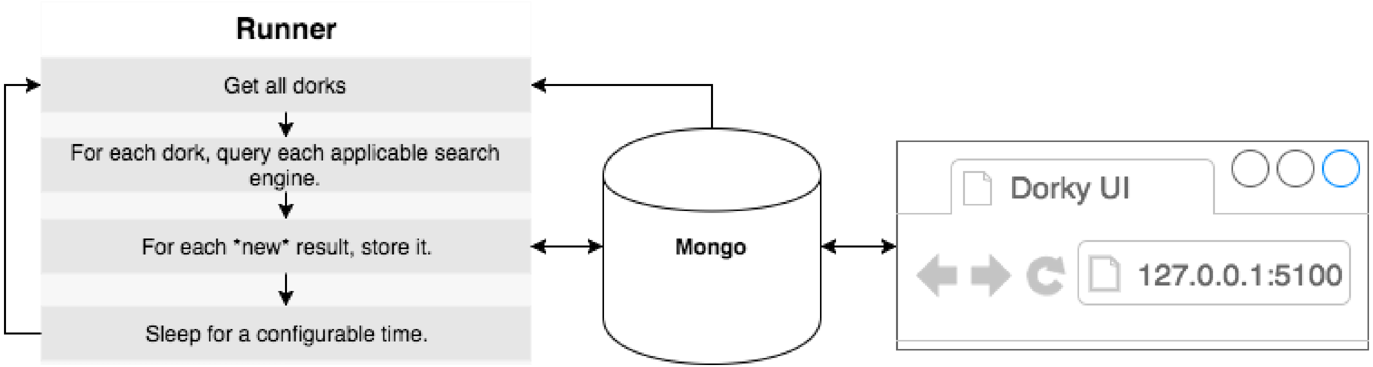
Dorky is your search engine hacking time saver!

Categories: Webshell Files containing passwords

Create Dork

	Query	Description	Category	Source	Enabled	Results
Edit	inurl:wp-config -intext:wp-config "'DB_PASSWORD'"	I give this - test - dork for WP passwords	Files containing passwords	https://www.exploit-db.com/ghdb/4181/	Yes	Show
Edit	intitle:"Hamdida X_Shell Backd00r"	XShell Backdoor	Webshell	https://www.exploit-db.com/ghdb/4292/	No	Show
Edit	"Fenix Final Version v2.0" filetype:php	Fenix Final Version v.2.0 Webshell	Webshell	https://www.exploit-db.com/ghdb/4282/	No	Show
Edit	(intitle:"phpshell" OR intitle:"c99shell" OR intitle:"r57shell" OR intitle:"PHP Shell " OR intitle:"phpRemoteView") `rwx` "uname"	Various Webshells	Webshell	https://www.exploit-db.com/ghdb/4201/	No	Show

How does it work?



Runner

Get all dorks

For each dork, query each applicable search engine.

For each *new* result, store it.

Sleep for a configurable time.

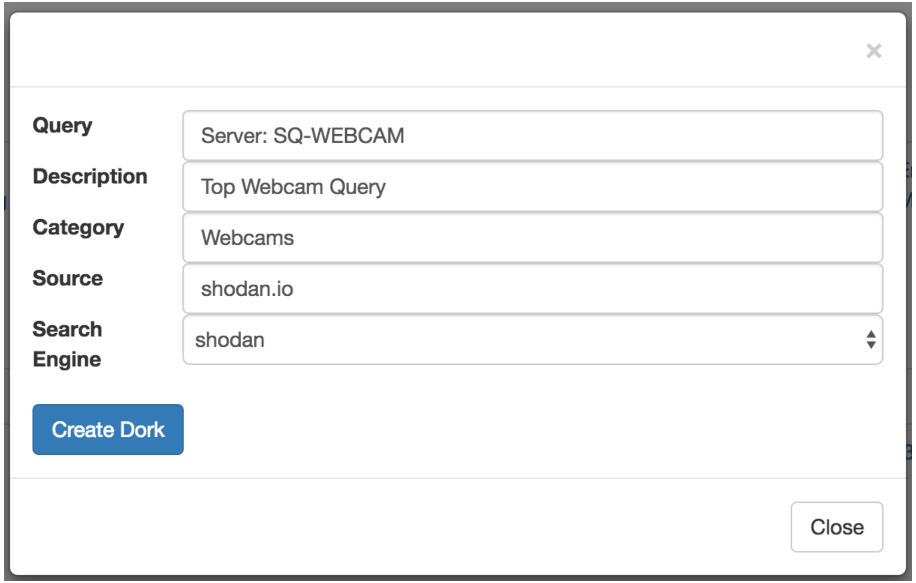
Architecture

- Python
  - Widely used.
- Mongo
  - Free, easy to setup, easy to develop against.
- Werkzeug
  - Powerful and lightweight. Powers Flask.

Included Search Engines

- Google
- Bing (API)
- Google Custom Search (API)
- Shodan (API)

Adding Dorks



Query: Server: SQ-WEBCAM

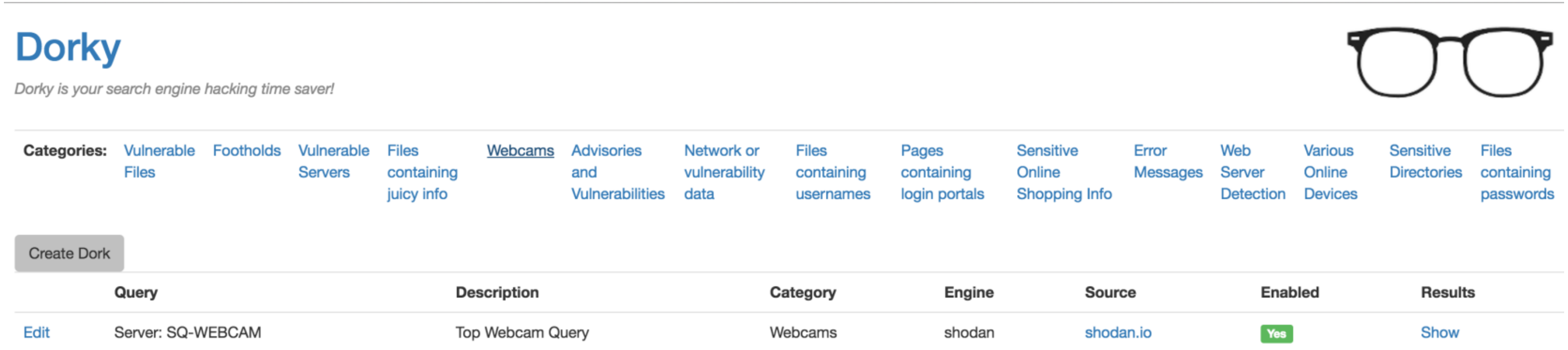
Description: Top Webcam Query

Category: Webcams

Source: shodan.io

Search Engine: shodan

Adding Dorks



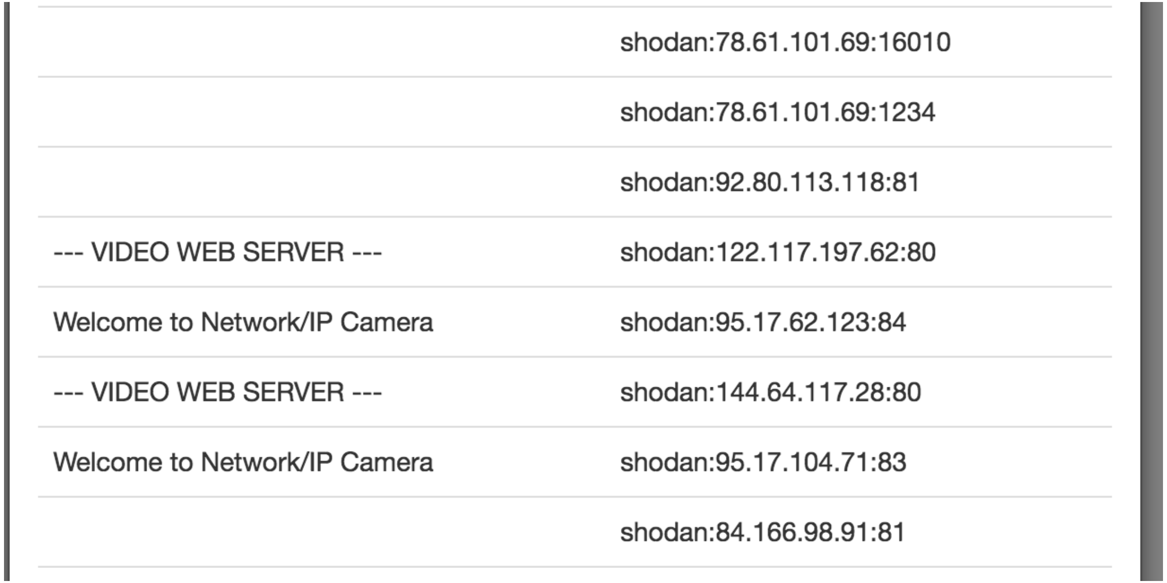
Dorky

Dorky is your search engine hacking time saver!

Categories: Vulnerable Files Footholds Vulnerable Servers Files containing juicy info Webcams Advisories and Vulnerabilities Network or vulnerability data Files containing usernames Pages containing login portals Sensitive Online Shopping Info Error Messages Web Server Detection Various Online Devices Sensitive Directories Files containing passwords

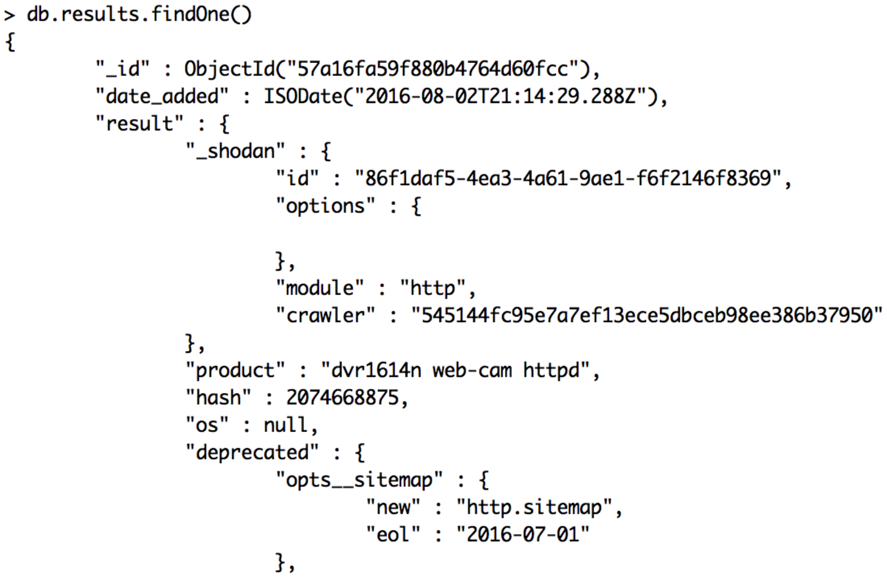
	Query	Description	Category	Engine	Source	Enabled	Results
Edit	Server: SQ-WEBCAM	Top Webcam Query	Webcams	shodan	shodan.io	Yes	Show

Results



	shodan:78.61.101.69:16010
	shodan:78.61.101.69:1234
	shodan:92.80.113.118:81
--- VIDEO WEB SERVER ---	shodan:122.117.197.62:80
Welcome to Network/IP Camera	shodan:95.17.62.123:84
--- VIDEO WEB SERVER ---	shodan:144.64.117.28:80
Welcome to Network/IP Camera	shodan:95.17.104.71:83
	shodan:84.166.98.91:81

Results



```
> db.results.findOne()
{
        "_id" : ObjectId("57a16fa59f880b4764d60fcc"),
        "date_added" : ISODate("2016-08-02T21:14:29.288Z"),
        "result" : {
                "_shodan" : {
                        "id" : "86f1daf5-4ea3-4a61-9ae1-f6f2146f8369",
                        "options" : {

                        },
                        "module" : "http",
                        "crawler" : "545144fc95e7a7ef13ece5dbceb98ee386b37950"
                },
                "product" : "dvr1614n web-cam httpd",
                "hash" : 2074668875,
                "os" : null,
                "deprecated" : {
                        "opts__sitemap" : {
                                "new" : "http.sitemap",
                                "eol" : "2016-07-01"
                        },
```

Configuration

- Mongo database
- Search engines that are active (+API keys)
- Proxy setup for certain sites
- Filters for:
  - Keywords (e.g. “dorking”)
  - URL substrings (e.g. “github.com/search”)

Issues

- Results can be noisy depending on the query
- Rate limiting, API costs
- Requires continuous maintenance to account for API / website changes

Future Work

- Adding more search engines is definitely interesting! Some ideas include: GitHub, VirusTotal, HybridAnalysis, …
- Improve logging and error handling
- Adding a pipe to Elastic Search would be cool

Have at it!

- https://github.com/recordedfuture/dorky (MIT license)
- Send me an email at freesalu [a†] gmail [∂ot] com if you have any questions!

References

- SearchDiggity – BishopFox - https://www.bishopfox.com/resources/tools/google-hacking-diggity/
- Johnny Long - https://en.wikipedia.org/wiki/Johnny_Long