it.sec
security for your information

Alexa Top 1 Million Security

Hacking the Big Ones

David Wind (@slashcrypto)
IT-SECX 2018
16.11.2018

it.sec
security for your information

About me

- David Wind (dwind@it-sec.de)
  - Security Consultant at it.sec GmbH & Co. KG
    - Web Application Security
    - Windows Security
    - Social Engineering
  - Privacy enthusiast and bug bounty hunter
    - Acknowledgments: Microsoft, Google, Netflix, …
  - Twitter: @slashcrypto
  - www.slashcrypto.org

We are hiring!

- Founded 1996
- Working in more than 30 counties
- New office in Vienna since this year
- **Security is our passion – come and join us!**

Why ?!

Alexa top 1 million websites

1. google.com
2. youtube.com
3. facebook.com
4. baidu.com
5. wikipedia.org
6. qq.com
7. taobao.com
8. yahoo.com
9. tmall.com
10. amazon.com

Source: https://www.alexa.com/topsites

What we were looking for

- Configuration issues in popular sites with a high security impact
- No fancy stuff
- Easy to find and to exploit

What we found

What we found

- Subdomain takeover vulnerabilities
- Exposed credentials
- Exposed source code
- CORS misconfiguration
- Exposed AWS S3 buckets
- ….

Where to start?

- We used Alexa top 1 million as input
- Subdomain enumeration using certificate transparency logs
  - crt.sh – they offer Postgres database
    - https://raw.githubusercontent.com/hannob/tlshelpers/master/getsubdomain
  - We discovered around 19 million subdomains

Overview

- Subdomain takeover vulnerabilities
- Exposed credentials
- Exposed source code
- Other interesting things

Overview

- Subdomain takeover vulnerabilities
- Exposed credentials
- Exposed source code
- Other Interesting Things

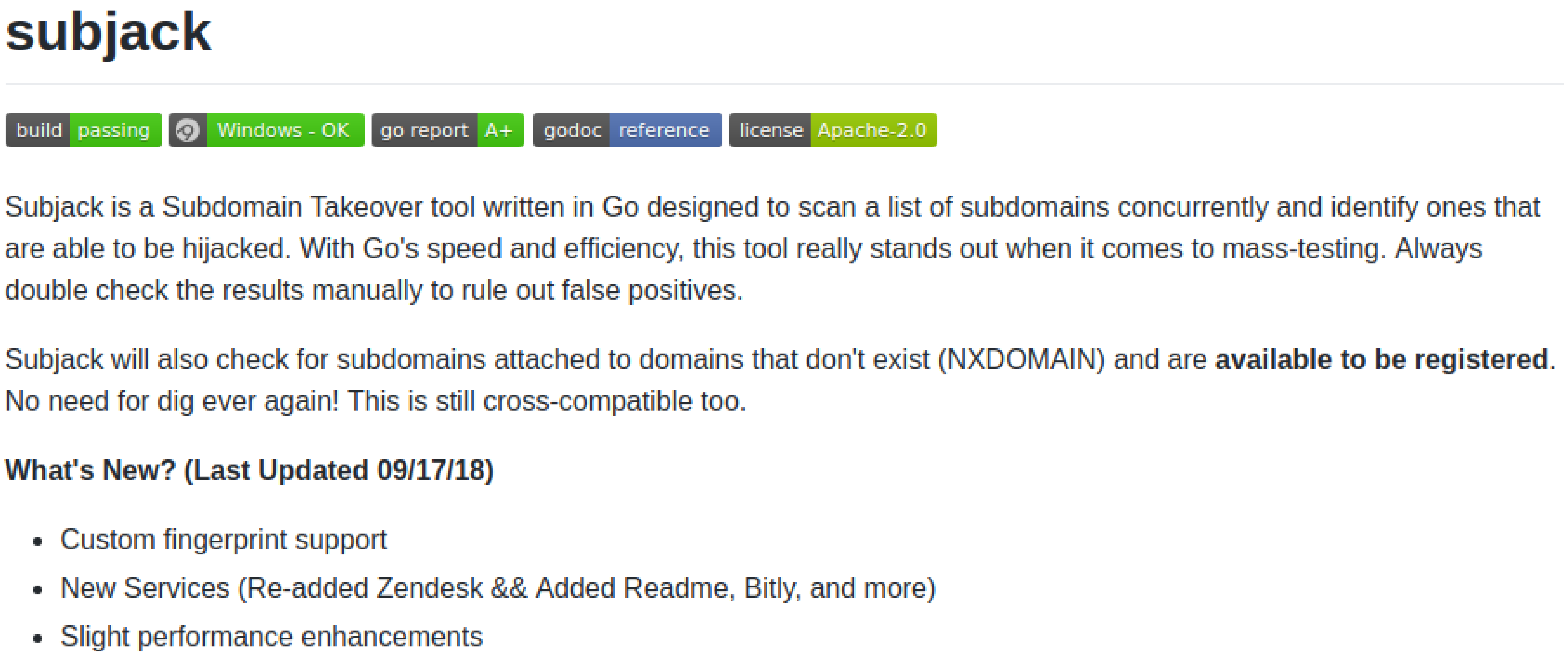
Subdomain takeover vulnerabilities

- A company points a subdomain to some other domain (e.g. some external Support Ticketing Service) using a CNAME record
- The company stops using the service and forgets to remove the CNAME record
- An attacker claims the domain and gains full control over the vulnerable subdomain

Subdomain takeover vulnerabilities

```
;; ANSWER SECTION:
subdomain.example.com.      3505    IN    CNAME
something.trafficmanager.net.
```

Subdomain takeover vulnerabilities



subjack

Subjack is a Subdomain Takeover tool written in Go designed to scan a list of subdomains concurrently and identify ones that are able to be hijacked. With Go's speed and efficiency, this tool really stands out when it comes to mass-testing. Always double check the results manually to rule out false positives.

Subjack will also check for subdomains attached to domains that don't exist (NXDOMAIN) and are **available to be registered**. No need for dig ever again! This is still cross-compatible too.

What's New? (Last Updated 09/17/18)

- Custom fingerprint support
- New Services (Re-added Zendesk && Added Readme, Bitly, and more)
- Slight performance enhancements

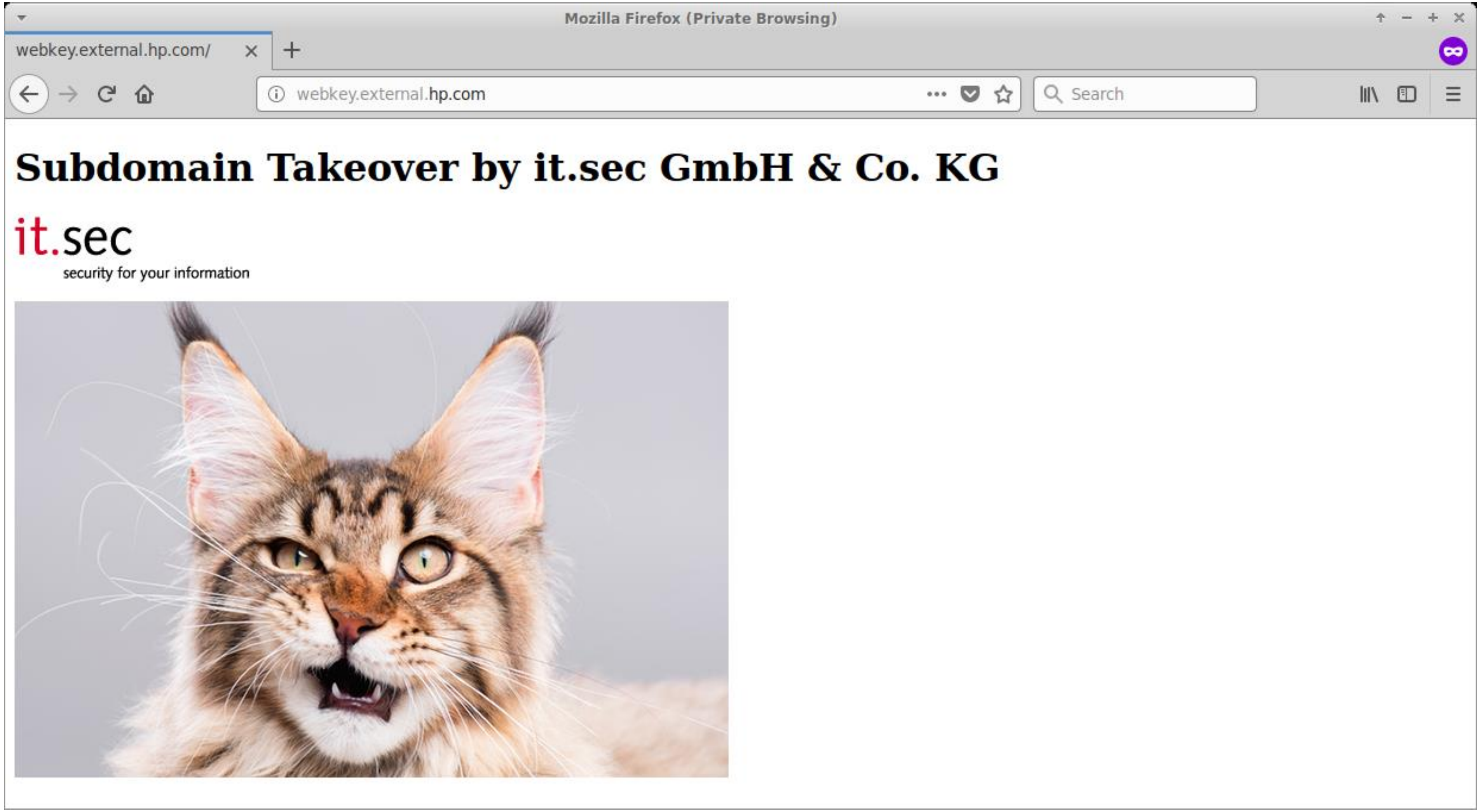
https://github.com/haccer/subjack

Subdomain takeover vulnerabilities

- We scanned around 3.5 million subdomains
- Around 0.5 % were potentially vulnerable
- Takeover through “AZURE Traffic Manager” was very successful

it.sec
security for your information

webkey.external.**hp.com**

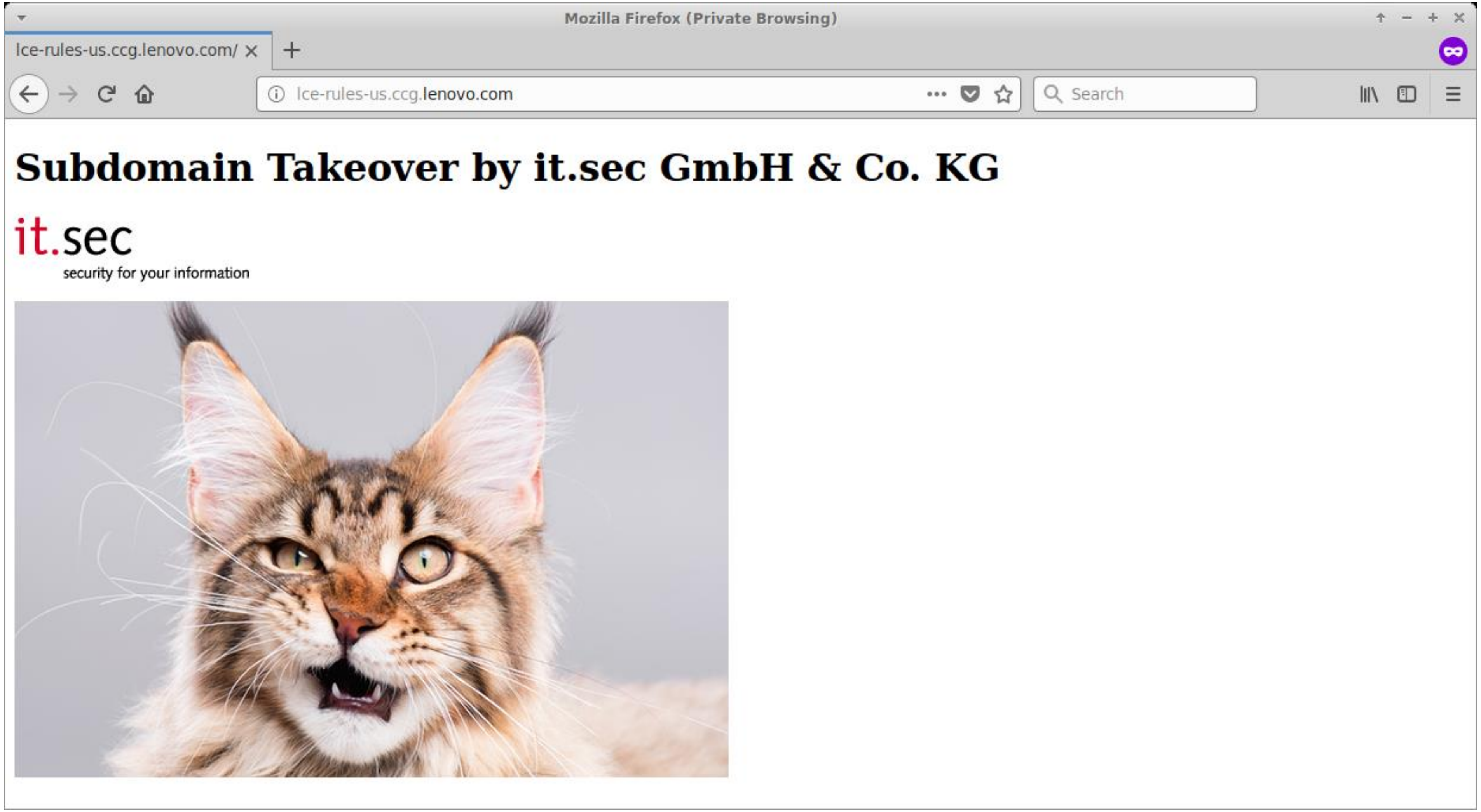


Subdomain Takeover by it.sec GmbH & Co. KG

it.sec
security for your information

lce-rules-us.ccg.lenovo.com

it.sec
security for your information



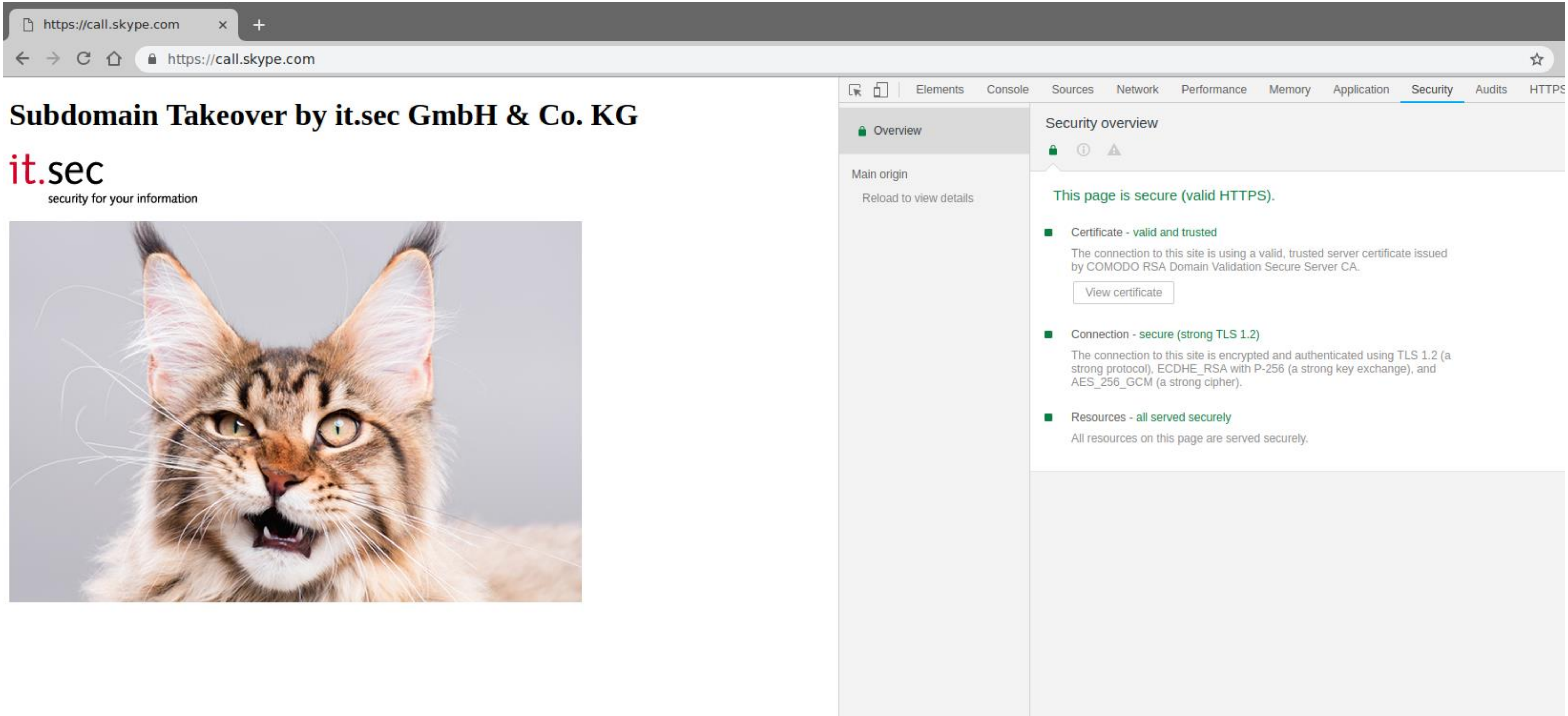
Mozilla Firefox (Private Browsing)
lce-rules-us.ccg.lenovo.com/
lce-rules-us.ccg.lenovo.com
Search

Subdomain Takeover by it.sec GmbH & Co. KG

it.sec
security for your information

it.sec
security for your information

call.skype.com



Subdomain Takeover by it.sec GmbH & Co. KG

it.sec
security for your information

Security overview

This page is secure (valid HTTPS).

- Certificate - valid and trusted

  The connection to this site is using a valid, trusted server certificate issued by COMODO RSA Domain Validation Secure Server CA.

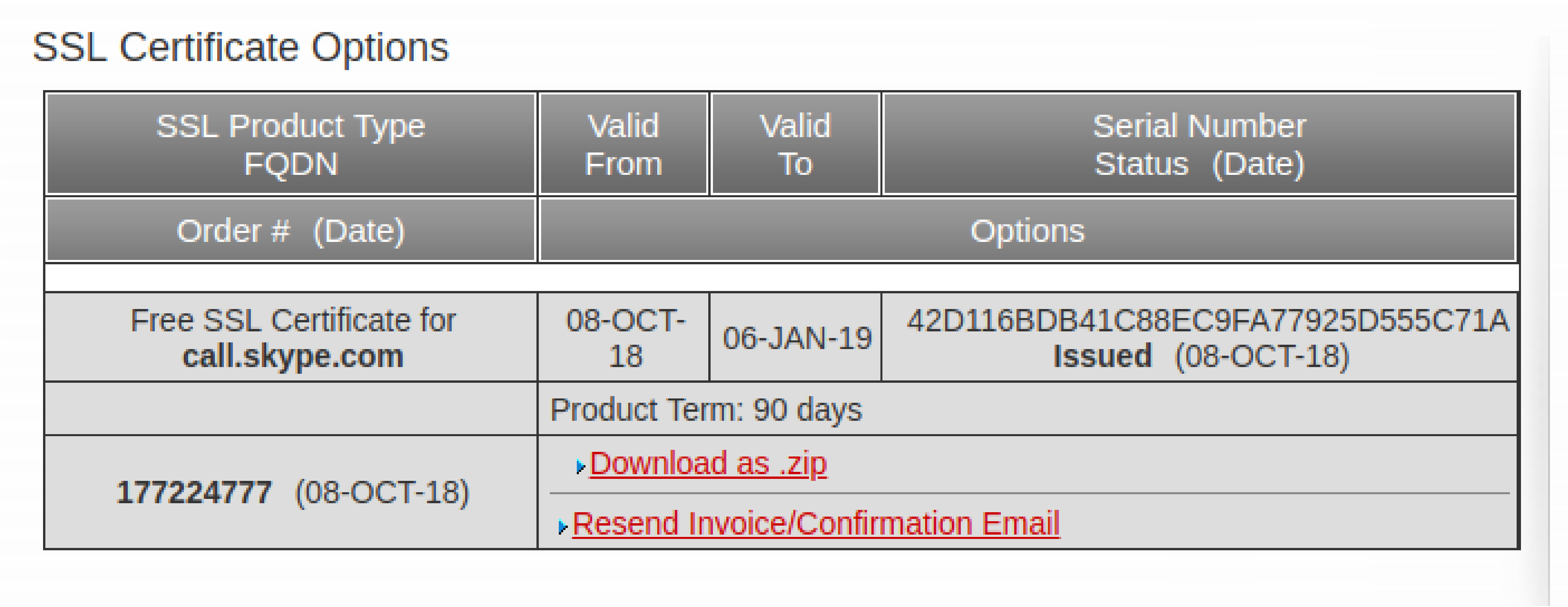
- Connection - secure (strong TLS 1.2)

  The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_256_GCM (a strong cipher).

- Resources - all served securely

  All resources on this page are served securely.

call.skype.com SSL certificate

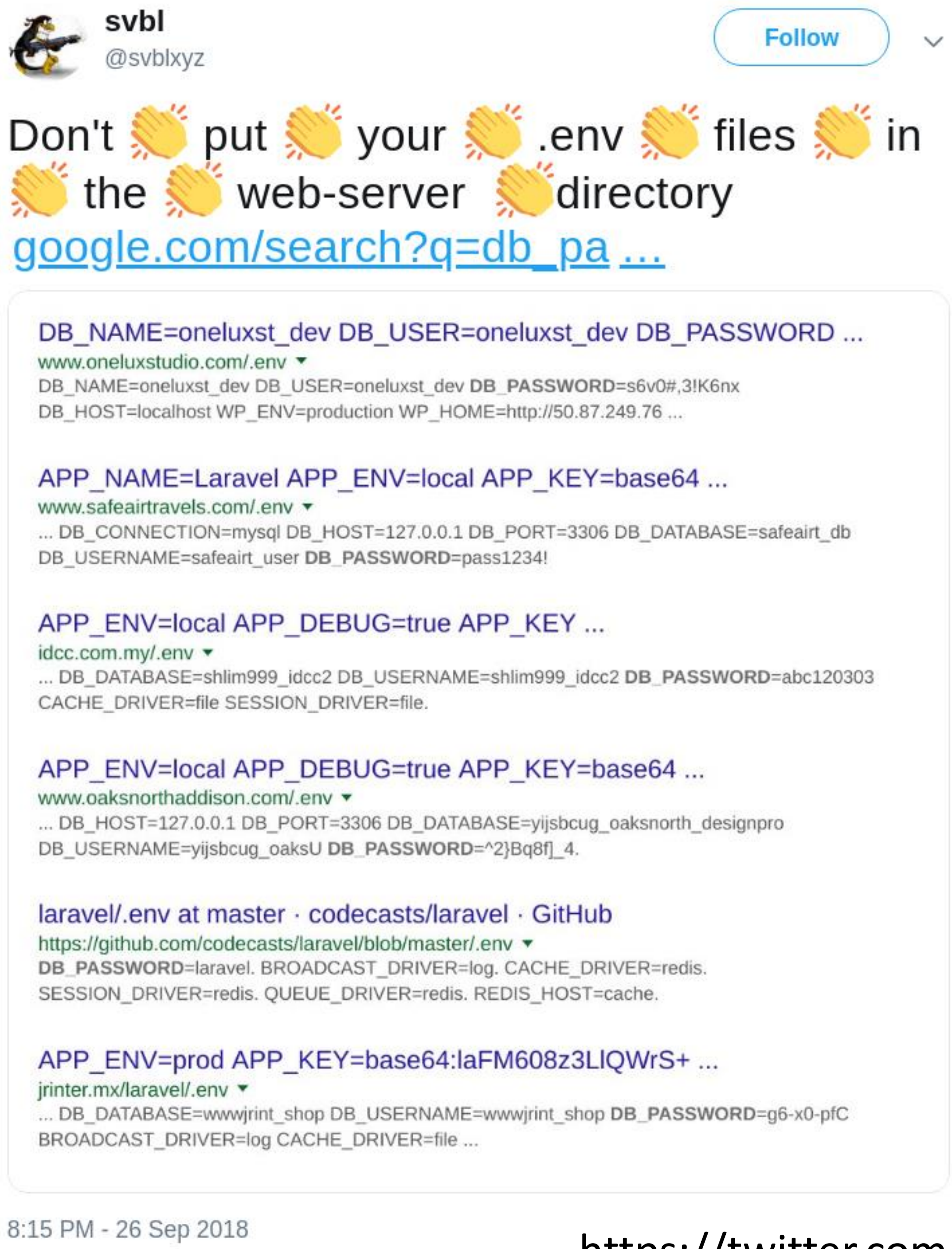


SSL Certificate Options

SSL Product Type FQDN	Valid From	Valid To	Serial Number Status (Date)
Order # (Date)	Options		
Free SSL Certificate for **call.skype.com**	08-OCT-18	06-JAN-19	42D116BDB41C88EC9FA77925D555C71A **Issued** (08-OCT-18)
	Product Term: 90 days		
177224777 (08-OCT-18)	▸Download as .zip ▸Resend Invoice/Confirmation Email		

Overview

- Subdomain takeover
- Exposed credentials
- Exposed source code
- Other interesting things



svbl
@svblxyz

Don't 👏 put 👏 your 👏 .env 👏 files 👏 in 👏 the 👏 web-server 👏 directory
google.com/search?q=db_pa ...

DB_NAME=oneluxst_dev DB_USER=oneluxst_dev DB_PASSWORD ...
www.oneluxstudio.com/.env ▾
DB_NAME=oneluxst_dev DB_USER=oneluxst_dev **DB_PASSWORD**=s6v0#,3!K6nx
DB_HOST=localhost WP_ENV=production WP_HOME=http://50.87.249.76 ...

APP_NAME=Laravel APP_ENV=local APP_KEY=base64 ...
www.safeairtravels.com/.env ▾
... DB_CONNECTION=mysql DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=safeairt_db
DB_USERNAME=safeairt_user **DB_PASSWORD**=pass1234!

APP_ENV=local APP_DEBUG=true APP_KEY ...
idcc.com.my/.env ▾
... DB_DATABASE=shlim999_idcc2 DB_USERNAME=shlim999_idcc2 **DB_PASSWORD**=abc120303
CACHE_DRIVER=file SESSION_DRIVER=file.

APP_ENV=local APP_DEBUG=true APP_KEY=base64 ...
www.oaksnorthaddison.com/.env ▾
... DB_HOST=127.0.0.1 DB_PORT=3306 DB_DATABASE=yijsbcug_oaksnorth_designpro
DB_USERNAME=yijsbcug_oaksU **DB_PASSWORD**=^2}Bq8f]_4.

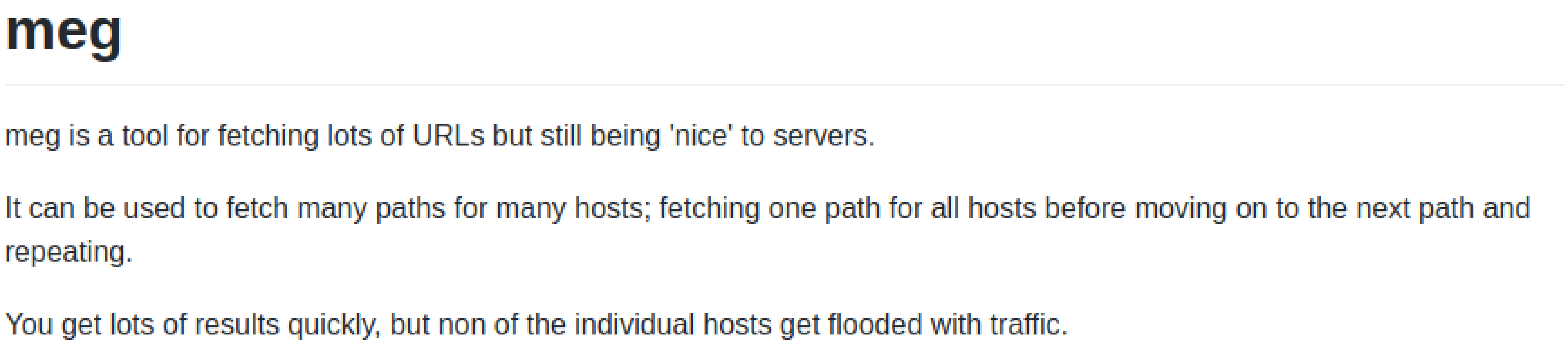
laravel/.env at master · codecasts/laravel · GitHub
https://github.com/codecasts/laravel/blob/master/.env ▾
DB_PASSWORD=laravel. BROADCAST_DRIVER=log. CACHE_DRIVER=redis.
SESSION_DRIVER=redis. QUEUE_DRIVER=redis. REDIS_HOST=cache.

APP_ENV=prod APP_KEY=base64:laFM608z3LlQWrS+ ...
jrinter.mx/laravel/.env ▾
... DB_DATABASE=wwwjrint_shop DB_USERNAME=wwwjrint_shop **DB_PASSWORD**=g6-x0-pfC
BROADCAST_DRIVER=log CACHE_DRIVER=file ...

8:15 PM - 26 Sep 2018

https://twitter.com/svblxyz/status/1045013939904532482

Exposed credentials



meg

meg is a tool for fetching lots of URLs but still being 'nice' to servers.

It can be used to fetch many paths for many hosts; fetching one path for all hosts before moving on to the next path and repeating.

You get lots of results quickly, but non of the individual hosts get flooded with traffic.

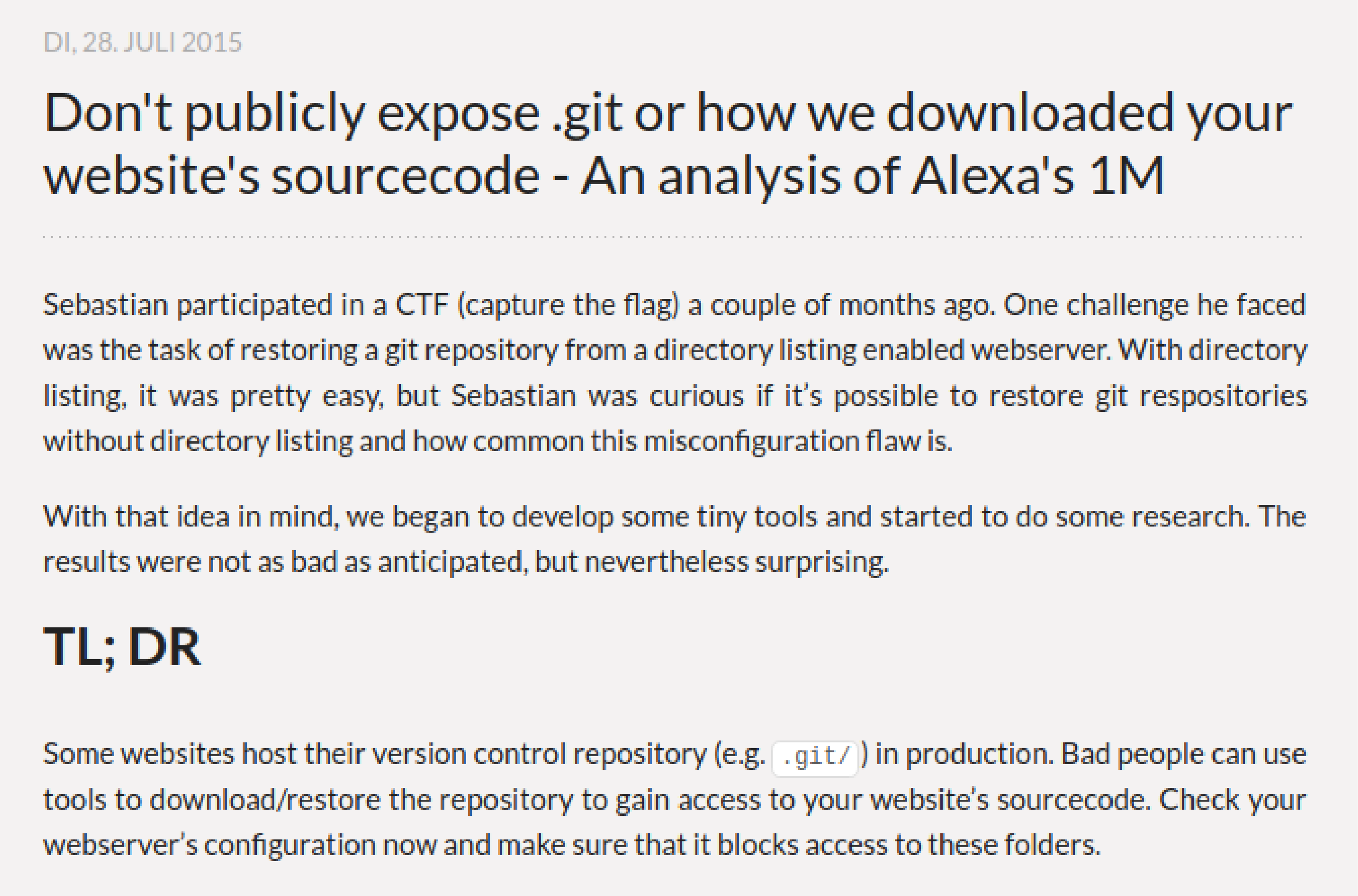
https://github.com/tomnomnom/meg

Exposed credentials

- We looked for .env files in the webroot
- We scanned only the Alexa Top 1 million without subdomains
- We identified
  - Hundreds of database passwords
  - PayPal API keys
  - Mail server credentials
  - … and much more

Overview

- Subdomain takeover
- Exposed credentials
- Exposed source code
- Other interesting things



DI, 28. JULI 2015

Don't publicly expose .git or how we downloaded your website's sourcecode - An analysis of Alexa's 1M

Sebastian participated in a CTF (capture the flag) a couple of months ago. One challenge he faced was the task of restoring a git repository from a directory listing enabled webserver. With directory listing, it was pretty easy, but Sebastian was curious if it's possible to restore git respositories without directory listing and how common this misconfiguration flaw is.

With that idea in mind, we began to develop some tiny tools and started to do some research. The results were not as bad as anticipated, but nevertheless surprising.

TL; DR

Some websites host their version control repository (e.g. `.git/`) in production. Bad people can use tools to download/restore the repository to gain access to your website's sourcecode. Check your webserver's configuration now and make sure that it blocks access to these folders.

https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/

Exposed source code

- We checked all Alexa Top 1 million + subdomains (19 million ULRs) for exposed git repos (.git/ folders in the webroot)
- We found around 3900 sites to be vulnerable to this attack
  - Government sites
  - Big Austrian newspaper
  - Universities
  - and ….

SECURITY

Japan's cybersecurity minister admits he's never used a computer

"I give instructions to my aide."

BY SEAN KEANE | NOVEMBER 15, 2018 7:16 AM PST

it.sec
security for your information

Japanese cybersecurity minister Yoshitaka Sakurada -- not a big computer guy.

Toshifumi Kitamura / AFP/Getty Images

https://www.cnet.com/news/japans-cybersecurity-minister-admits-hes-never-used-a-computer/

Exposed source code

- https://www.ebay.co.jp was vulnerable
  - Runs WordPress ?!
  - They leaked the complete WordPress source and more to unauthorized users
    - >1GB data
    - Database passwords
    - WordPress passwords
    - User uploads
    - and much more …
  - **They fixed the issue within 10 hours!**

Overview

- Subdomain takeover
- Exposed credentials
- Exposed source code
- Other interesting things

Other things we identified

- CORS misconfiguration
  - Microsoft (again ..)
  - Big Austrian telecommunication provider
- Open AWS S3 buckets
  - Terabytes of data – still investigating
  - We used „bucket-stream“ which scans transparency logs in real time
    - https://github.com/eth0izzle/bucket-stream

Lessons learned

- There are still tons of “low-hanging fruits“ out there
- You don‘t need expensive super intelligent intrusion preventions systems if you don‘t get the basics right

it.sec
security for your information

Future work

- Automate scans
- Use data of scans.io or Rapid7 project Sonar
- Eliminate false positives more efficiently
- Think about reporting issues more efficiently

https://scans.io

https://opendata.rapid7.com

Q&A

slashcrypto.org for the slides