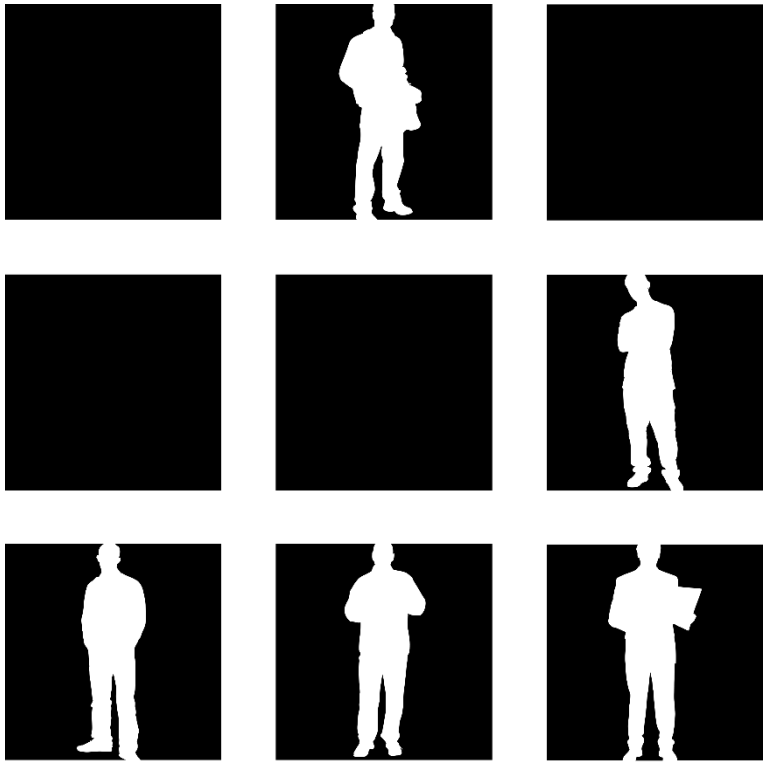
securing



HACKTIVITY

Mateusz Olejarka

REST API Pentester's perspective

20.10.2017

KA-BOOM

Anand Prakash @sehacure

KA-BOOM

„Whenever a user Forgets his password on Facebook, he has an option to reset the password by entering his phone number/ email address on:

https://www.facebook.com/login/identify?ctx=recover&lwv=110

Facebook will then send a **6 digit code** on his phone number/email address which user has to enter in order to set a new password.

I tried to **brute** the 6 digit code on www.facebook.com and was **blocked** after **10-12** invalid attempts.”

KA-BOOM

„Then i looked out for the same issue on **beta.facebook.com** and **mbasic.beta.facebook.com** and interestingly **rate limiting was missing** on forgot password endpoints.”

We sent you a message

Wednesday, March 2, 2016 at 12:25am

Hi Anand,

After reviewing the issue you have reported, we have decided to award you a bounty of $15000 USD. We fulfill our bounties through https://bugbountypayments.com/

== Next Steps ==

* If you have not registered on https://bugbountypayments.com/

To properly collect your bounty, you will need to reply to this email with the following information:

- First name
- Last name
- Country
- Email address (this is where we will send the registration email)

KA-BOOM

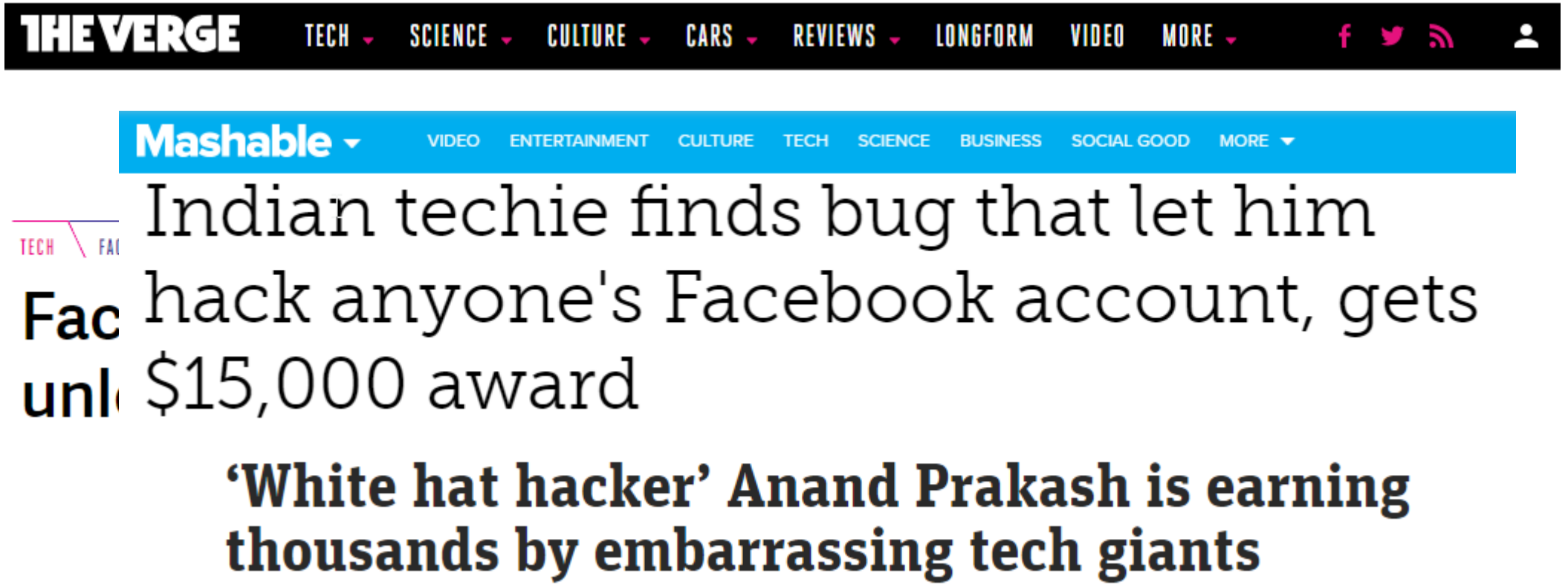
TECH \ FACEBOOK \ CYBERSECURITY

Facebook paid $15,000 to close a bug that could unlock any user's account

KA-BOOM


THE VERGE
TECH
SCIENCE
CULTURE
CARS
REVIEWS
LONGFORM
VIDEO
MORE
news .com.au
The news in colour
TECH
FACEBOOK
Faceb
National
World
Lifestyle
Travel
Entertainment
Technology
Finance
Sport
unlock
online
hacking
'White hat hacker' Anand Prakash is earning thousands by embarrassing tech giants

KA-BOOM


THE VERGE
TECH
SCIENCE
CULTURE
CARS
REVIEWS
LONGFORM
VIDEO
MORE
Mashable
VIDEO
ENTERTAINMENT
CULTURE
TECH
SCIENCE
BUSINESS
SOCIAL GOOD
MORE
TECH
Fac
unl
Indian techie finds bug that let him hack anyone's Facebook account, gets $15,000 award
'White hat hacker' Anand Prakash is earning thousands by embarrassing tech giants

REST API

- Is everywhere (web&mobile)
- Is build on top of existing applications
- More and more companies allow to use it’s API
- Applications are more interconnected
- Microservices

REST API

The future

Nowadays, building software no longer requires a team of engineers or costly servers. An API Key and its documentation are all you need to easily integrate an external feature.

> *For the end user, things have been made easier and for developers, there are no more limits.*

Drivers of economic growth for the client companies, they have increased business for software companies and have become an essential element of the business model. They have become the product itself and according Gartner, **by 2018, at least 50% of BtoB exchanges and collaborations will be performed via Web APIs.**

https://www.mobapi.com/history-of-rest-apis/

Who am I

- Senior IT Security Specialist, SecuRing
- Web & mobile application security
- OWASP Poland member
- Ex developer
- Bug hunter

Agenda

- REST API 101
- Finding endpoints
- Finding docs
- Finding sample calls
- Finding keys
- 2 more examples
- Q&A

REST API 101

REST API 101

- REST – representational state transfer
- Data usually is sent as JSON
- HTTP methods have a meaning (usually):
  - GET - list (collection), retrieve data (element)
  - PUT – replace (all data is changed)
  - PATCH – update
  - POST – create (new element)
  - DELETE

REST API 101

```
GET /version HTTP/1.1
Host: [redacted].com
Accept: application/json;charset=UTF-8
[...]


HTTP/1.1 200
Content-Type: application/json;charset=UTF-8
[...]

{"groupId":"[redacted].hs.cvl.core","artifactId":"cvl-core-web-api","version":"1.0.17"}
```

REST API Pentest

- Get endpoints
- Get docs
- Get keys/credentials
- Get sample calls !!

REST API Bug bounty

- Sometimes no known endpoints
- Sometimes no docs
- Sometimes no keys/credentials
- Sometimes no sample calls !!

FINDING ENDPOINTS

Finding endpoints

- /
- /api/
- /v1/
- /v1.0/
- /v1.1/
- /api/v1/
- /api/v2

Finding endpoints

- /
- /api/
- /v1/
- /v1.0/
- /v1.1/
- /api/v1/
- /api/v2

```
https://[redacted].io/api/v1/
Content-Type: text/plain
Content-Length: 45
Content:

Community Platform API v1
```

Finding endpoints

- /
- /api/
- /v1/
- /v1.0/
- /v1.1/
- /api/v1/
- /api/v2

```
https://[redacted].com/api/v1/
Content-Type: application/json
Content-Length: 169
Content:
{"meta":
    {"message":
        "This is a list of all endpoints available at this version",
    "endpoints": [
        "http://[redacted].com/api/v1/health_check/"
    ]},
"data": null}
```

Finding endpoints

- /ping
- /health
- /status
- ...
- Dictionaries for **directories** and **filenames** will help

Finding endpoints

- /ping
- /health
- /status
- …
- Dictionaries for **directories** and **filenames** will help

```
https://[redacted]/api/v1/ping
Content-Type: application/json;charset=utf-8
Content-Length: 26
Content:

{"response":"pong","et":0}
```

Finding endpoints

- /ping
- /health
- /status
- …
- Dictionaries for **directories** and **filenames** will help

```
https://[redacted].com/api/health
Content:

{"status":"good"}
```

```
https://[redacted]/api/health
Content:

{"ok":false,"error":"unknown_method","req_method":"health"}
```

Finding endpoints

- /ping
- /health
- /status
- ...
- Dictionaries for **directories** and **filenames** will help

```
https://[redacted].com/health
Content:

{"status":"UP","status":{"status":"UP","TnT admin":"UP","ims":"UP"}}
```

Spring Boot Actuator

Spring Boot makes it easy to create stand-alone, production-grade Spring based Applications that you can "just run". We take an opinionated view of the Spring platform and third-party libraries so you can get started with minimum fuss. Most Spring Boot applications need very little Spring configuration.

Features

- Create stand-alone Spring applications
- Embed Tomcat, Jetty or Undertow directly (no need to deploy WAR files)
- Provide opinionated 'starter' POMs to simplify your Maven configuration
- Automatically configure Spring whenever possible
- Provide production-ready features such as metrics, health checks and externalized configuration

Spring Boot Actuator

Spring Boot makes it easy to create stand-alone, production-grade Spring based Applications that you can "just run". We take an opinionated view of the Spring platform and third-party libraries so you can get started with minimum fuss. Most Spring Boot applications need very little Spring configuration.

Fe

Building a RESTful Web Service with Spring Boot Actuator

Spring Boot Actuator is a sub-project of Spring Boot. It adds several production grade services to your application with little effort on your part. In this guide, you'll build an application and then see how to add these services.

- Automatically configure Spring whenever possible
- Provide production-ready features such as metrics, health checks and externalized configuration

Spring Boot Actuator

- Interesting endpoints:
  - /actuator
  - /health
  - /trace
  - /logfile
  - /metrics
  - /heapdump (Spring MVC)

Spring Boot Actuator

- Interesting endpoints:
  - /actuator
  - /health
  - /trace
  - /logfile
  - /metrics
  - /heapdump (Spring MVC)

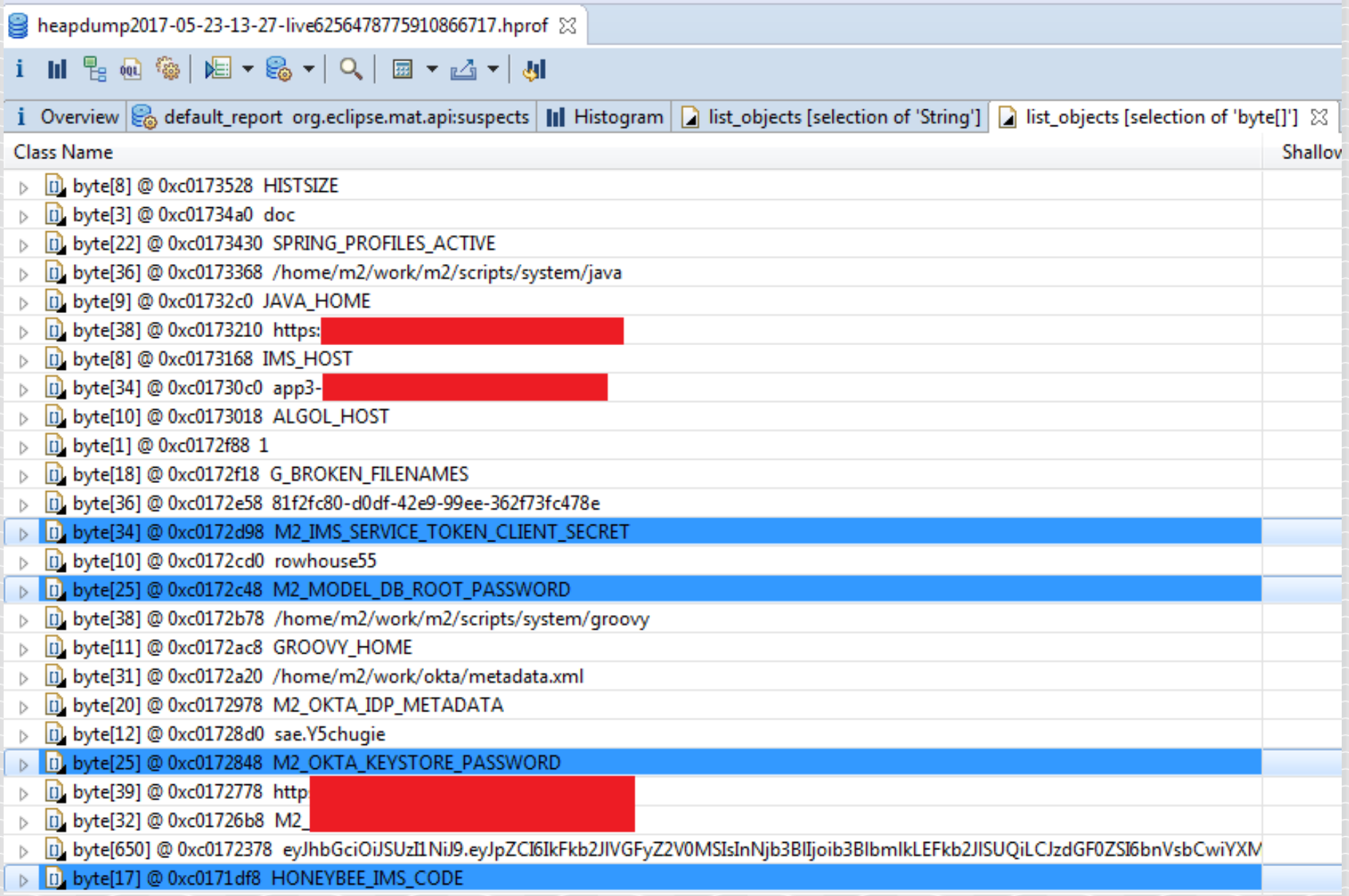
Spring Boot Actuator

- Interesting endpoints:
  - /actuator
  - /health
  - /trace
  - /logfile
  - /metrics
  - /heapdump (Spring MVC)

```
Tested domain: [redacted].com

/heapdump              : 200 , size : 11707186 [11707177]
Content-Disposition: attachment;
filename="heapdump2017-05-11-00-47-live2732695341119813321.hprof.gz"
```

HEAP DUMP LIVE DEMO


heapdump2017-05-23-13-27-live6256478775910866717.hprof
Overview
default_report org.eclipse.mat.api:suspects
Histogram
list_objects [selection of 'String']
list_objects [selection of 'byte[]']
Class Name
Shallov
byte[8] @ 0xc0173528 HISTSIZE
byte[3] @ 0xc01734a0 doc
byte[22] @ 0xc0173430 SPRING_PROFILES_ACTIVE
byte[36] @ 0xc0173368 /home/m2/work/m2/scripts/system/java
byte[9] @ 0xc01732c0 JAVA_HOME
byte[38] @ 0xc0173210 https:
byte[8] @ 0xc0173168 IMS_HOST
byte[34] @ 0xc01730c0 app3-
byte[10] @ 0xc0173018 ALGOL_HOST
byte[1] @ 0xc0172f88 1
byte[18] @ 0xc0172f18 G_BROKEN_FILENAMES
byte[36] @ 0xc0172e58 81f2fc80-d0df-42e9-99ee-362f73fc478e
byte[34] @ 0xc0172d98 M2_IMS_SERVICE_TOKEN_CLIENT_SECRET
byte[10] @ 0xc0172cd0 rowhouse55
byte[25] @ 0xc0172c48 M2_MODEL_DB_ROOT_PASSWORD
byte[38] @ 0xc0172b78 /home/m2/work/m2/scripts/system/groovy
byte[11] @ 0xc0172ac8 GROOVY_HOME
byte[31] @ 0xc0172a20 /home/m2/work/okta/metadata.xml
byte[20] @ 0xc0172978 M2_OKTA_IDP_METADATA
byte[12] @ 0xc01728d0 sae.Y5chugie
byte[25] @ 0xc0172848 M2_OKTA_KEYSTORE_PASSWORD
byte[39] @ 0xc0172778 http
byte[32] @ 0xc01726b8 M2_
byte[650] @ 0xc0172378 eyJhbGciOiJSUzI1NiJ9.eyJpZCI6IkFkb2JlVGFyZ2V0MSIsInNjb3BlIjoib3BlbmlkLEFkb2JlSUQiLCJzdGF0ZSI6bnVsbCwiYXM
byte[17] @ 0xc0171df8 HONEYBEE_IMS_CODE

FINDING DOCS

Finding docs:

- /api-docs
- /application.wadl
- /doc
- /docs
- /swagger-ui.html
- /swagger.json

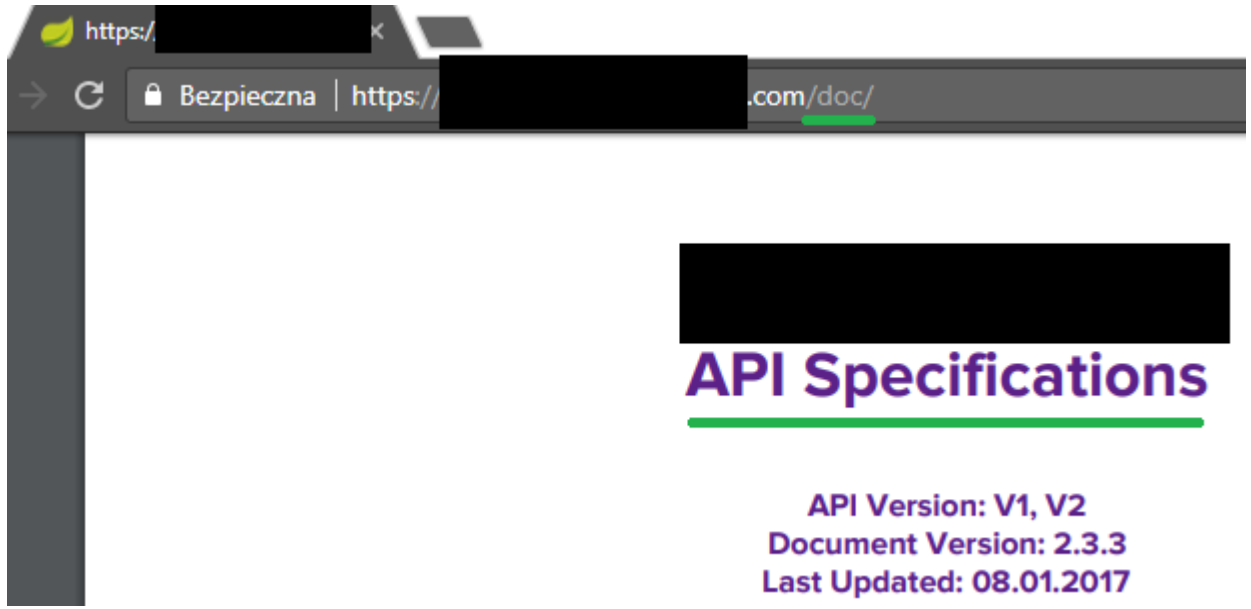
Finding docs:

- /api-docs
- /application.wadl
- /doc
- /docs
- /swagger-ui.html
- /swagger.json

SOAP UI LIVE DEMO

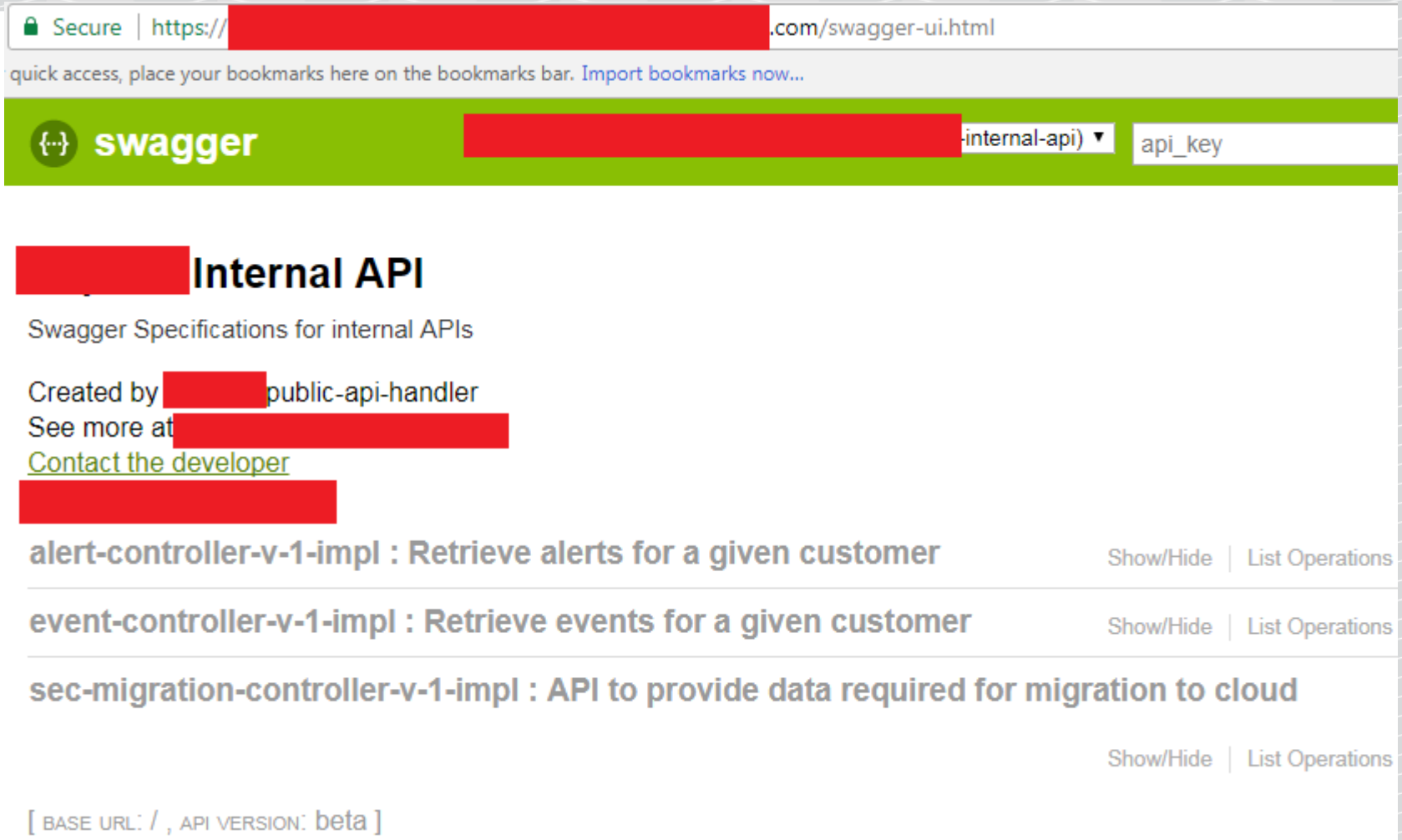
Finding docs:

- /api-docs
- /application.wadl
- /doc
- /docs
- /swagger-ui.html
- /swagger.json



Finding docs:

- /api-docs
- /application.wadl
- /doc
- /docs
- /swagger-ui.html
- /swagger.json



SWAGGER LIVE DEMO

FINDING SAMPLE CALLS

Finding sample calls

- Still no docs?
- Error messages to the rescue!

Finding sample calls

- Still no docs?
- Error messages to the rescue!

```
GET /api/public/files/109/test.pdf
[...]

HTTP/1.1 404 NOT FOUND
[...]

{ "message":
"The requested URL was not found on the server.
If you entered the URL manually please check your spelling and try again.
You have requested this URI
[/api/public/files/109/test.pdf]
but did you mean
/api/public/files/<int:file_id>/<string:filename> or
/api/public/countries/<string(length=2):code> or
/api/admin/files/types?" }
```

Finding sample calls

- Still no docs?
- Error messages to the rescue!

```
GET /REST/v1/auth HTTP/1.1
[...]

HTTP/1.1 405 Method Not Allowed
Allow: DELETE, OPTIONS, POST
[...]
```

Finding sample calls

- Still no docs?
- Error messages to the rescue!

```
POST /REST/v1/auth HTTP/1.1
Content-Type: application/json
[...]
{}

HTTP/1.1 400 Bad Request
[...]

Could not find a 'username' parameter
```

Finding sample calls

- Still no docs?
- Error messages to the rescue!

```
POST /REST/v1/auth HTTP/1.1
[...]
{ 'username' : 'test' }

HTTP/1.1 400 Bad Request
[...]

Could not find a 'password' parameter
```

Finding sample calls

- Still no docs?
- Error messages to the rescue!

```
POST /REST/v1/auth HTTP/1.1
[...]
{ 'username' : 'test', 'password' : 'test' }

HTTP/1.1 401 Unauthorized
[...]

Invalid credentials.
```

Finding sample calls

- Still no docs?
- Error messages to the rescue!
- Brute force parameter names!

Finding sample calls

- Still no docs?
- Error messages to the rescue!
- Brute force parameter names!
- Analyze JS code (see JS-Scan)
- Dissect mobile app (Apk-Scan for Android apps hadrcoded URL’s)

FINDING KEYS

Finding keys

- Check mobile application
- Check GitHub (truffleHog to the rescue):
  - Scan public repos of a company
  - Scan public repos of a company devs

Finding keys

BUSINESS INSIDER ENTERPRISE

To be fair, this problem wasn't caused by Google, but by the app developers who post their apps in Google Play. In fact, the researchers say that Google stopped the problem by using PlayDrone to scan apps and telling developers to remove secret keys when they find them.

The researchers also waited months to publish their research, giving app developers time to fix their apps.

But the scariest part was the type of app that had this problem, and how some dragged their feet to fix it. In some cases the holes were still there after November when they had officially shut down their research project after warning app developers.

The paper explains, "For example, the popular Airbnb application still contained their Facebook, Google, LinkedIn, Microsoft, and Yahoo secret tokens from June 22, 2013 until well past November 11, 2013."

Finding keys

- Check mobile application
- Check GitHub (truffleHog to the rescue):
  - Scan public repos of a company
  - Scan public repos of a company devs

Finding keys

- Check mobile application
- Check GitHub (truffleHog to the rescue):
  - Scan public repos of a company
  - Scan public repos of a company devs

```
https://github.com/[redacted]/commit/[redacted]

 public class [redacted]{
     public static void main(String[] args) {
         Client client = new Client(new Configuration.Builder().

-                accessToken("053[redacted]').

+                accessToken(System.getenv("[redacted]TOKEN")).
```

Finding keys

```
GET /v2/users/self HTTP/1.1
Host: [redacted]
Authorization: Bearer 053[redacted]
[...]


HTTP/1.1 200 OK
[...]
Content-Length: 317
Connection: Close

{[...]
"confirmed":true,
"role":"admin",
"status":"active",
[...]}
```

2 MORE EXAMPLES

#1 Jolokia

Tested domain: [redacted].com

/jolokia : 200 OK, size : 256 [248]


```
{
"request":{"type":"version"},
"value":{
    "agent":"1.3.3",
    "protocol":"7.2",
    "config":{"agentId":"10.55.197.204-26814-516037be-servlet","agentType":"servlet"},
    "info":{"product":"tomcat","vendor":"Apache","version":"8.0.20"}},
    "timestamp":1494610863,"status":200}
```

#1 Jolokia

„Jolokia is a JMX-HTTP bridge giving an alternative to JSR-160 connectors. It is an agent based approach with support for many platforms. In addition to basic JMX operations it enhances JMX remoting with unique features like bulk requests and fine grained security policies.”

#1 Jolokia

„Jolokia is a JMX-HTTP bridge giving an alternative to JSR-160 connectors. It is an agent based approach with support for many platforms. In addition to basic JMX operations it enhances JMX remoting with unique features like bulk requests and fine grained security policies.”

https://example.com/jolokia/write/Tomcat:port=19880,type=Connector/xpoweredBy/true

#1 Jolokia

„Jolokia is a JMX-HTTP bridge giving an alternative to JSR-160 connectors. It is an agent based approach with support for many platforms. In addition to basic JMX operations it enhances JMX remoting with unique features like bulk requests and fine grained security policies.”

https://example.com/jolokia/write/Tomcat:port=19880,type=Connector/xpoweredBy/true

X-Powered-By:Servlet/3.1 JSP/2.3 (Apache Tomcat/8.0.20 Java/Oracle Corporation/1.8.0_60-b27)

#1 Jolokia

6.2.3.1. GET exec request

The format of an GET exec request is

```
<base url>/exec/<mbean name>/<operation name>/<arg1>/<arg2>/....
```

Table 6.6. GET Exec Request

Part	Description	Example
`<mbean name>`	MBean's ObjectName	`java.lang:type=Threading`
`<operation name>`	Name of the operation to execute. If this is an overloaded method, it is mandatory to provide a method signature as well. A signature consist the fully qualified argument class names or native types, separated by commas and enclosed with parentheses. For calling a non-argument overloaded method use `()` as signature.	`loadUsers(java.lang.String,int)`
`<arg1>`, `<arg2>`, ...	String representation for the arguments required to execute this operation. Only certain data types can be used here as described in Section 6.4.2, "Request parameter serialization".	`"true","true"`

The following request will trigger a garbage collection:

```
http://localhost:8080/jolokia/exec/java.lang:type=Memory/gc
```

#2 REST API wrongly placed

#2 REST API wrongly placed

- A form

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA
- Secured (no way to brute force ID)

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA
- Secured (no way to brute force ID)
- A mobile app with the same feature

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA
- Secured (no way to brute force ID)
- A mobile app with the same feature
- No CAPTCHA

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA
- Secured (no way to brute force ID)
- A mobile app with the same feature
- No CAPTCHA
- No rate limiting

#2 REST API wrongly placed

- A form
- Putting ID and solving CAPTCHA
- Secured (no way to brute force ID)
- A mobile app with the same feature
- No CAPTCHA
- No rate limiting
- Brute force &~~profit~~ report to client !

Summary

- Find endpoints
- Find docs
- Find sample calls
- Find keys
- Fuzz

Tools

- SOAP UI https://www.soapui.org/
- Postman https://www.getpostman.com/
- Fuzzapi https://github.com/Fuzzapi/fuzzapi
- Swagger Parser (Burp Suite plugin)
- TruffleHog https://github.com/dxa4481/truffleHog
- JS-Scan https://github.com/zseano/JS-Scan
- Apk – Scan https://apkscan.nviso.be/

securing

That’s all folks

mateusz.olejarka@securing.pl / @molejarka