computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Free BugBounty as a CERT

FIRST – 2018

Emilien LE JAMTEL

Introduction

- Around 60 organisations
- From 40 – 40.000 users
- Seperate, heterogenous networks
- Cross-sectoral
  - Government, foreign policy, embassies
  - Banking, energy, pharmaceutical, chemical, food, telecom
  - Maritime, rail and aviation safety
  - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
  - Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- High-value targets






Chapter 1

A very simple request

Responsible disclosure

From: XXXX XXXXX [mailto:xxxxxxxxx@gmail.com]
Sent: Wednesday, February 10, 2016 10:05 PM
To: CERT-EU
Subject: Security vulnerability

Hi,
My name is XXXX XXXXX and I am security researcher. I would like to report XSS flows in europa website.

```
http://europa.eu/rapid/search-
result.htm?quickSearch=1&text=%22%20style=background:black;%20onmouseover=alert%28String.fromCharCode%2888
,83,83%29%29%20%22
```

Please open in Firefox and put mouse on black search box to trigger JS code.

Open again in FF browser

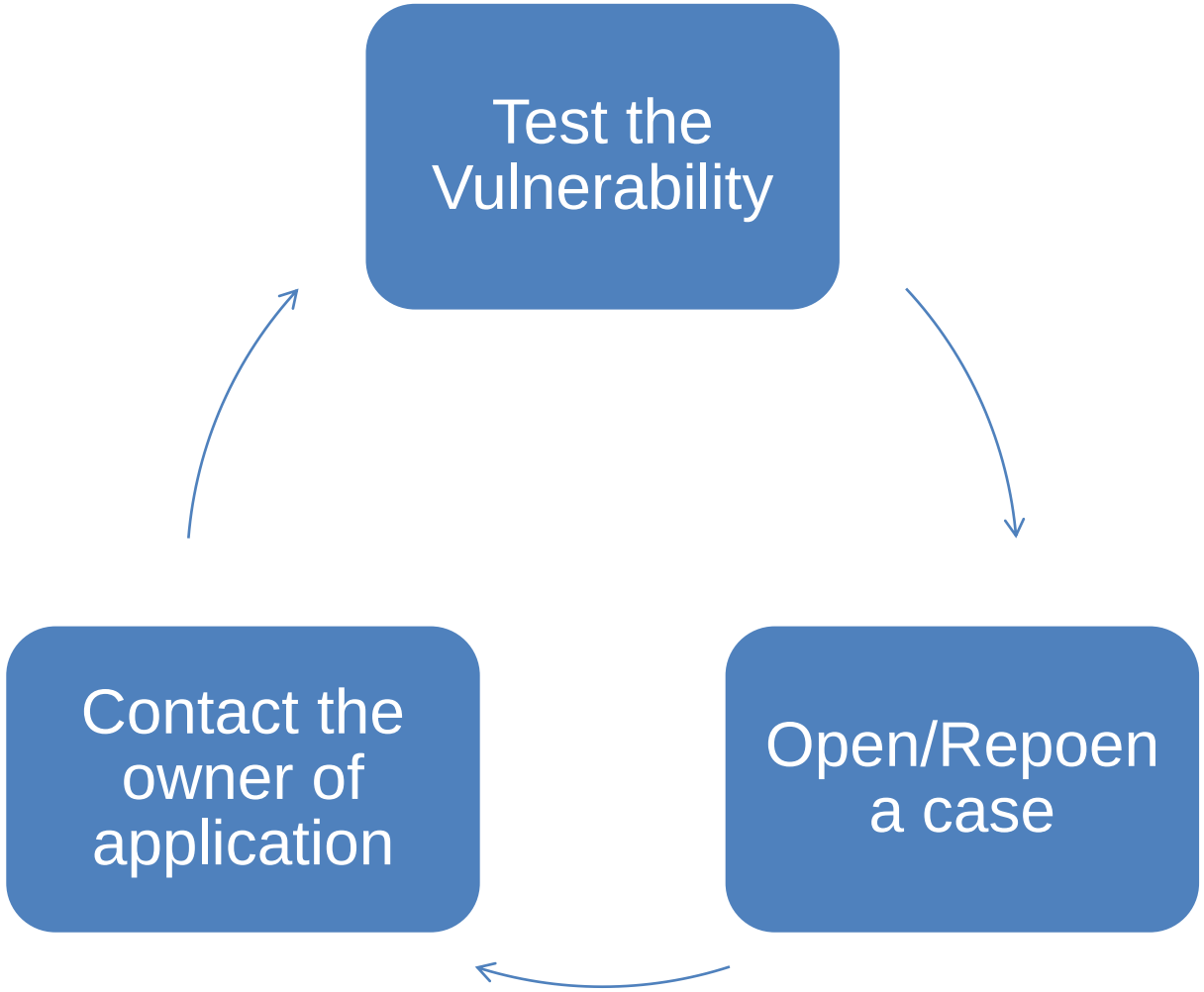
```
http://ec.europa.eu/taxation_customs/dds2/taric/taric_consultation.jsp?Lang=99999%22%3E%3Cscript%3Ealert%2
8document.cookie%29%3C/script%3E&Taric=abcd&Area=BH&Expand=true&SimDate=20160107#D432000000

http://newsletter-europa.eu/RTD/Horizon/20131121/modify.php?email=%22%3E%3Csvg/onload=prompt%281%29%3E
```

Thanks,

XXXXXXXX | White Hat | Security Researcher | Red Teamer

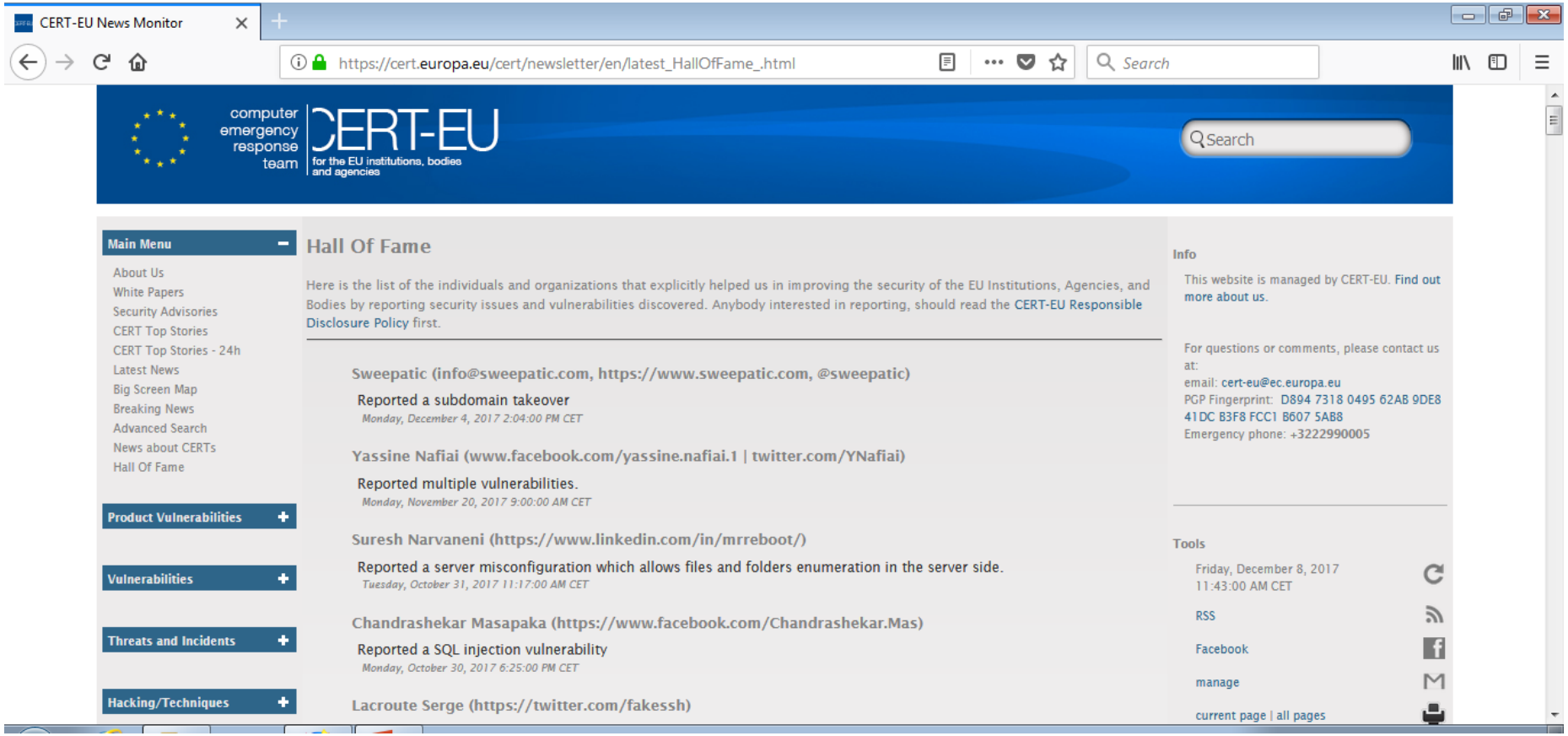
A simple loop



Hall Of fame ?

Researcher asked for reward

-> We agreed on creating a “Hall Of Fame” page



Disclosure Policy

CERT-EU Responsible Disclosure Policy

What to report to CERT-EU:

Security Incidents and Vulnerabilities, which occur in software components, protocols, or hardware of websites or systems of EU Institutions Agencies or Bodies, and may affect significant number of users and/or critical infrastructure.

Vulnerability reporting policy:

CERT-EU reserves the right to accept or reject any vulnerability disclosure report at its discretion, based on the following general criteria:

1. Pre-disclosure handling of the potentially sensitive vulnerability details:
    - The vulnerability should have not already been publicly disclosed.
    - It is important to report the vulnerability as quickly as possible after its discovery.
    - Even after reporting the vulnerability, no information on the security problem should be shared with others until the incident has been processed and resolved. Failure to comply with this requirement may result in the reported being removed from the CERT-EU Hall of Fame.
2. The vulnerability finding must be new and severe enough to be considered as eligible for a mention in the Hall of Fame of CERT-EU. The severity of a vulnerability finding is assessed by CERT-EU at its own discretion. CERT-EU reserves the right to reject reports of vulnerabilities, which have already been previously reported.

Vulnerability reporting instructions:

- E-mail your findings to reports (at) cert.europa.eu.
- Encrypt your email using the PGP key available on CERT-EU website
- Provide as much information as possible regarding the finding, in order for CERT-EU to handle the incident as efficiently as possible.

If more information is required, CERT-EU will contact the reporter, therefore any contact details (email address and telephone number) should be valid.
If the previously mentioned conditions are satisfied, CERT-EU will proceed with notification to the impacted party. Once the issue has been fixed or no later than 3 months since the initial report, the reporter may be mentioned (at his own discretion) in the Hall of Fame of CERT-EU (this page) with a short description of the type of vulnerability reported.

Chapter 2

The road to Hell is paved with good intentions

Unexpected Issues

Mailbox under assault

- 40+ notifications the first week
- Need triage capabilities
- Need clear processes for triage team

Validation issues

- Analyst team not necessarily trained for web vulnerabilities
- Some vulnerabilities are not severe enough for reward

Duplicates

- Researchers are sharing vulnerabilities with friends …
- Need to search other cases for duplicates

Chapter 3

Automate the boring stuff

First PoC

```
#!/usr/bin/env python
# halloffame.py - automated check for reported vulns (Hall Of Fame)

"""
Check Hall OF Fame vulnerabilities
Author: Emilien LE JAMTEL
CERT-EU - version 1.0
30/05/2016
"""

import sys
import requests
import json
import datetime

################################################################################

## function checking the stuffs adn modifing the json file
## take a list of index (in the json file) as input (from the *_scan() functions
def checkmybooty (index_list):
    if len(index_list) == 0:
        print ('fuck it, empty list')
        sys.exit()
    for i in range(len(index_list)):
        ########### printing the vuln details
        print('---------- ' + str(i) +' ---------')
        print('contituent: ' + halloffame[index_list[i]]["constituent"])
        print('RTIR incident number: ' + halloffame[index_list[i]]["RTIR"])
        print('Vulnerability: ' + halloffame[index_list[i]]["type"])
        print('URL: ' + halloffame[index_list[i]]["url"])
        ###########
        if halloffame[index_list[i]]["scanable"] == 'no':
            checkbabycheck = 'not scanable'
        else:
            halloffame[index_list[i]]["last_test"] = str(today)
            checkbabycheck = check_patched(halloffame[index_list[i]]["method"],hall
        if  checkbabycheck[0] == 'YES, it is patched, hell yeah':
            halloffame[index_list[i]]["patched"] = 'yes'
            print('Patched: YES')
```

Python3

json

Cron job

Check strings in PoC reply

Feedback

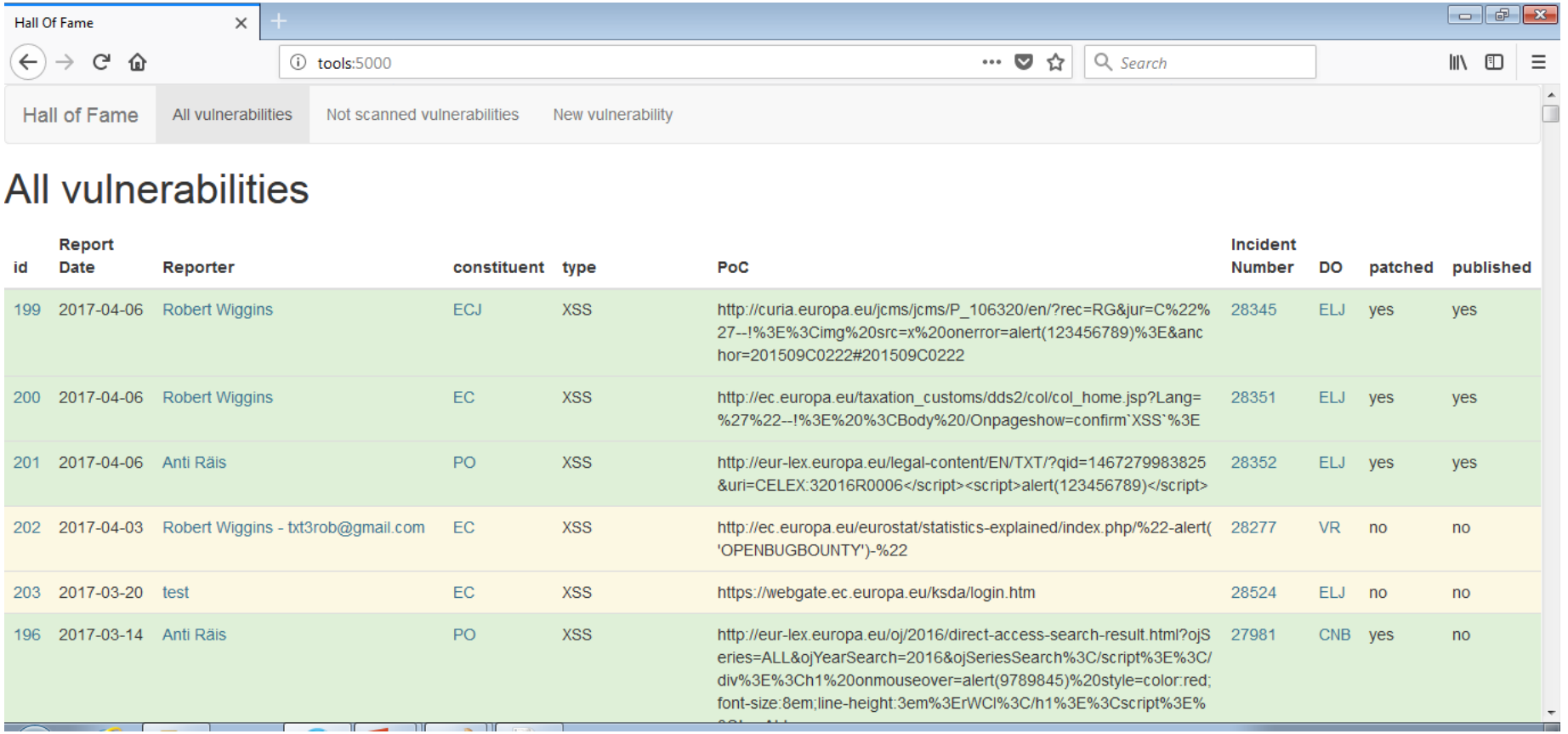
- First Wins
  - Faster to identify duplicates
  - Automate status update

- To be improved
  - Format validation
  - Collaboration within IR team

Chapter 4

Do you wanna GUI ?

Second PoC



All vulnerabilities

id	Report Date	Reporter	constituent	type	PoC	Incident Number	DO	patched	published
199	2017-04-06	Robert Wiggins	ECJ	XSS	http://curia.europa.eu/jcms/jcms/P_106320/en/?rec=RG&jur=C%22%27--!%3E%3Cimg%20src=x%20onerror=alert(123456789)%3E&anchor=201509C0222#201509C0222	28345	ELJ	yes	yes
200	2017-04-06	Robert Wiggins	EC	XSS	http://ec.europa.eu/taxation_customs/dds2/col/col_home.jsp?Lang=%27%22--!%3E%20%3CBody%20/Onpageshow=confirm`XSS`%3E	28351	ELJ	yes	yes
201	2017-04-06	Anti Räis	PO	XSS	http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467279983825&uri=CELEX:32016R0006</script><script>alert(123456789)</script>	28352	ELJ	yes	yes
202	2017-04-03	Robert Wiggins - txt3rob@gmail.com	EC	XSS	http://ec.europa.eu/eurostat/statistics-explained/index.php/%22-alert('OPENBUGBOUNTY')-%22	28277	VR	no	no
203	2017-03-20	test	EC	XSS	https://webgate.ec.europa.eu/ksda/login.htm	28524	ELJ	no	no
196	2017-03-14	Anti Räis	PO	XSS	http://eur-lex.europa.eu/oj/2016/direct-access-search-result.html?ojSeries=ALL&ojYearSearch=2016&ojSeriesSearch%3C/script%3E%3C/div%3E%3Ch1%20onmouseover=alert(9789845)%20style=color:red;font-size:8em;line-height:3em%3ErWCl%3C/h1%3E%3Cscript%3E%	27981	CNB	yes	no

Python 3 + Flask

json

Cron job

Simple format validation

Easier for team training

Feedback

- Second Wins
  - Format validation
  - Collaboration within IR team

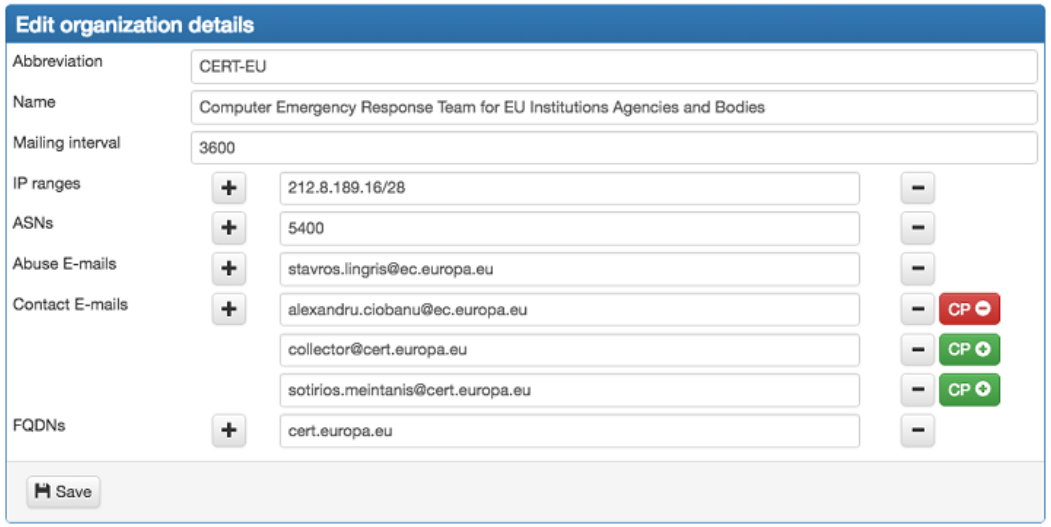
- To be improved
  - Reporting to constituent

Chapter 5

Working with developers

Customer Portal

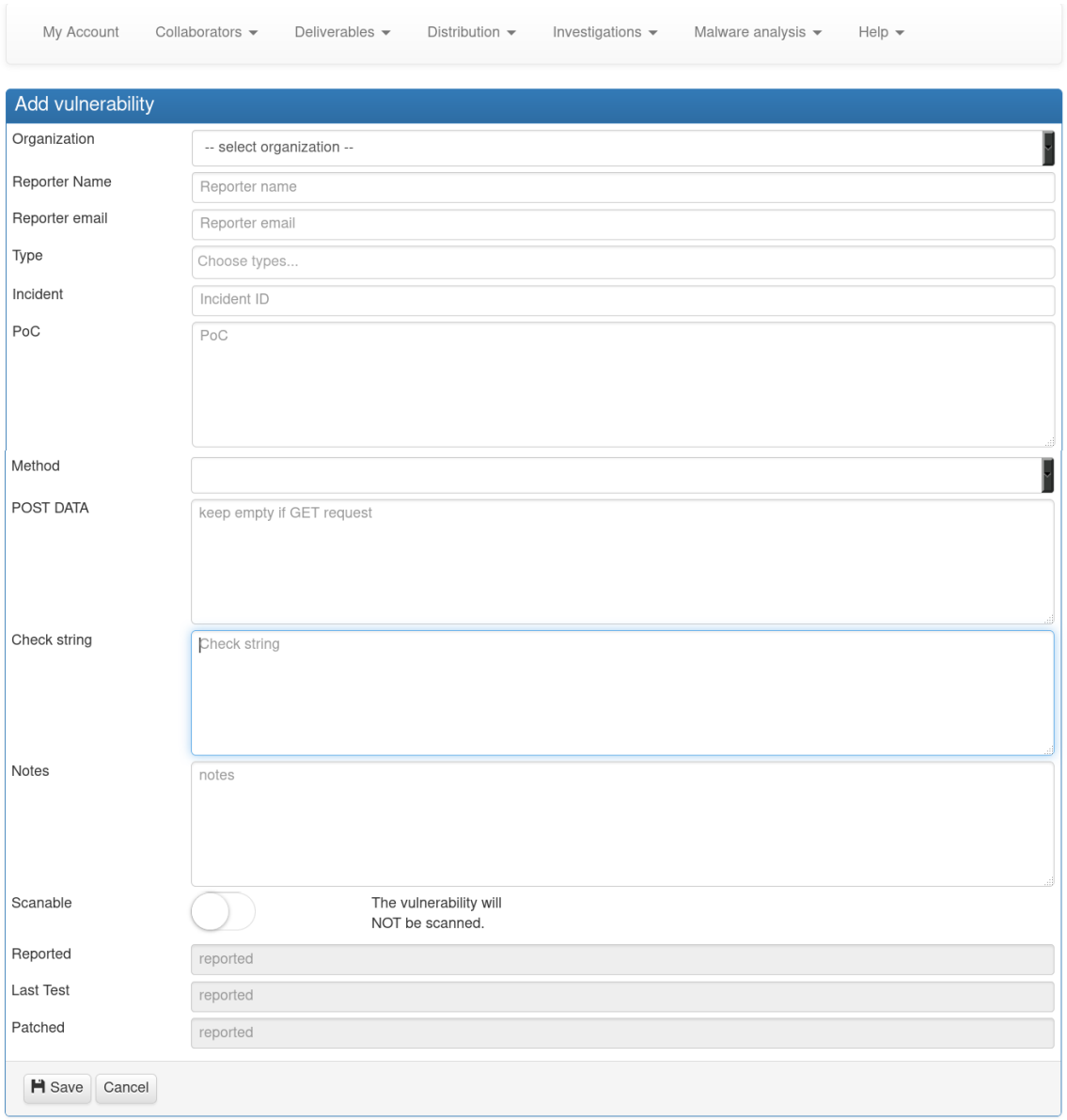
- Constituents details
- CERT-EU deliverables
- Indicator search
- File Analysis
- Vulnerability scanning



Name	Type	Actions
CERT-EU_THOR_Bundle_20160826.zip	THOR	
5577-crowdstrike_yara_master_20160826.zip	YARA rules	
CITAR-Flash-2016-007.zip	Flash-CITAR	
CITAR-014-Duke-and-Baron.zip	CITAR	
CIMBL-267.zip	CIMBL	
CIMBL-268.zip	CIMBL	
CIMBL-269.zip	CIMBL	

computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

PoC integration - backend



Python + JS + RestAPI

More Format validation

Database

PoC integration - frontend

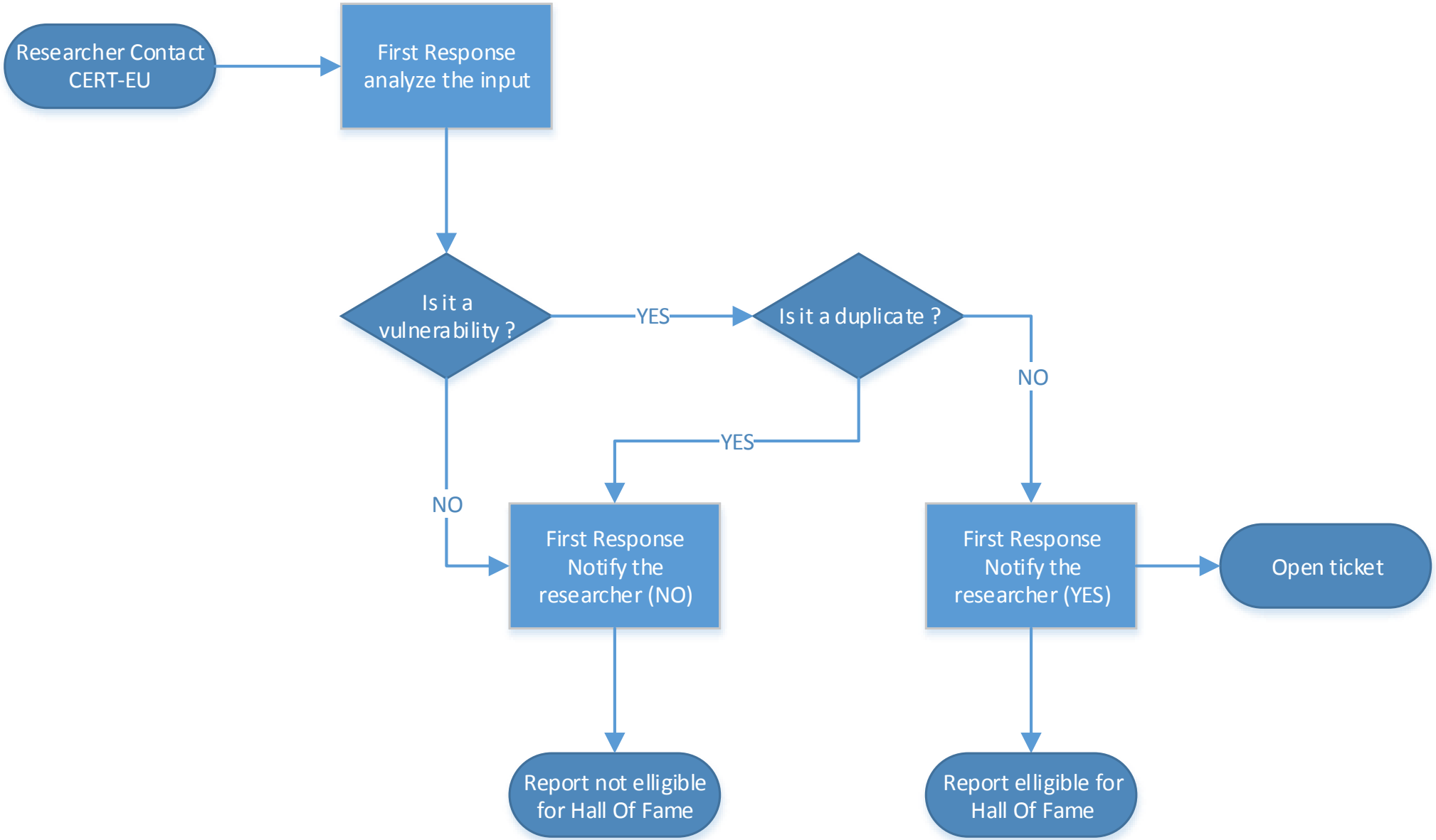
Vulnerabilities

ID	Report date	PoC	Type	RTIR #	Patched
223	2017-05-04T15:26:09	https .eu	XSS	28780	Dec 12, 2017
213	2017-04-25T07:33:41	https .eu/cert/newsletter/en'-alert%281%29-'/latest_HallOfFame_.html	XSS	28202	May 8, 2017
198	2017-03-14T00:00:00	https .eu/cert/search/en/advanced.html	XSS	27980	Apr 26, 2017
197	2017-03-14T00:00:00	https .eu/cert/searchresults/en/advanced.html?lang=en&dateTo=%27-alert(document.domain)-%27	XSS	27980	Dec 12, 2017
154	2016-05-25T00:00:00	https 19/cert/countryedition/en/IL.html?cptheme=%27);alert(%27xss	XSS	24183	Oct 27, 2016
152	2016-06-22T00:00:00	https 19/cert/searchresults/en/advanced.html?lang=en&atLeast=&dateFrom=%27-alert(0in%20RSS%20link%27)-%27&dateTo=%27-alert(%27Second%20WCI%27)-%27&query ced	XSS	24665	Oct 27, 2016
43	2016-03-04T00:00:00	https://emmweb.cert.europa.eu/cert/filteredition/en/sdfsdfs/	Version Disclosure	23478	Mar 4, 2016

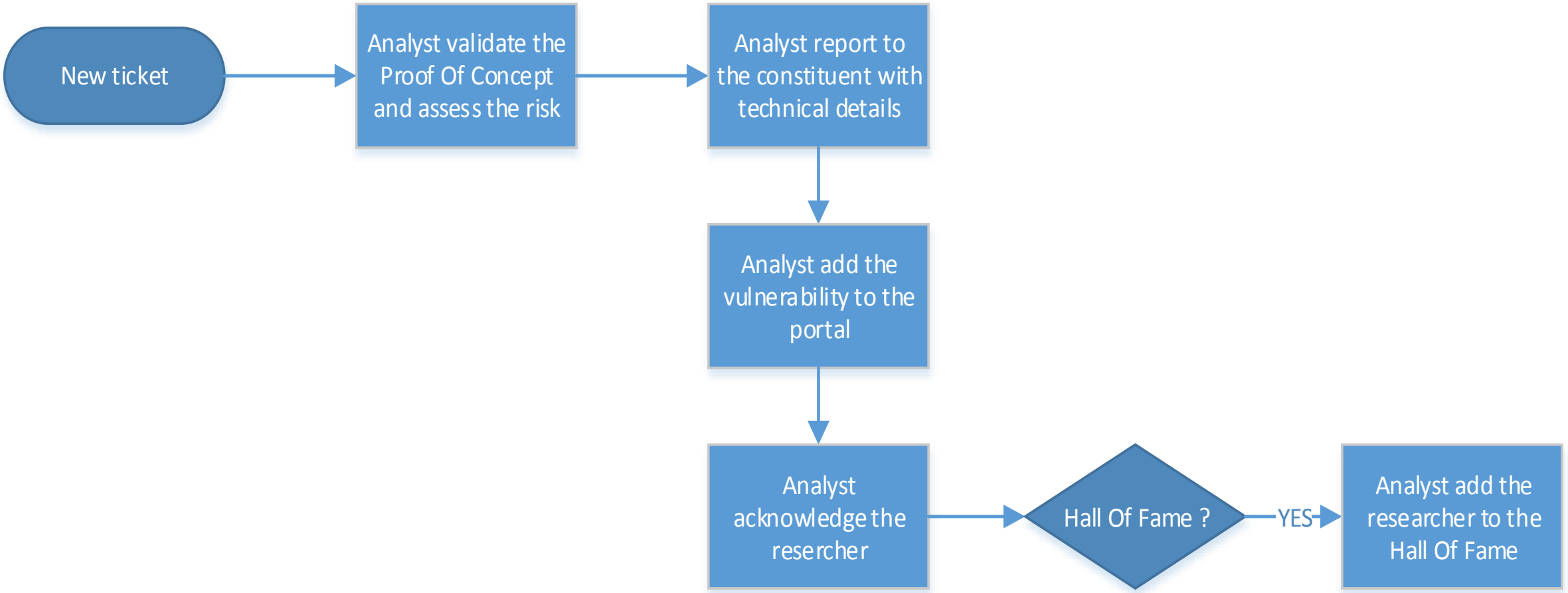
Vulnerabilities status

Reference to CERT-EU ticket

Triage Process



Analysis Process



Conclusion

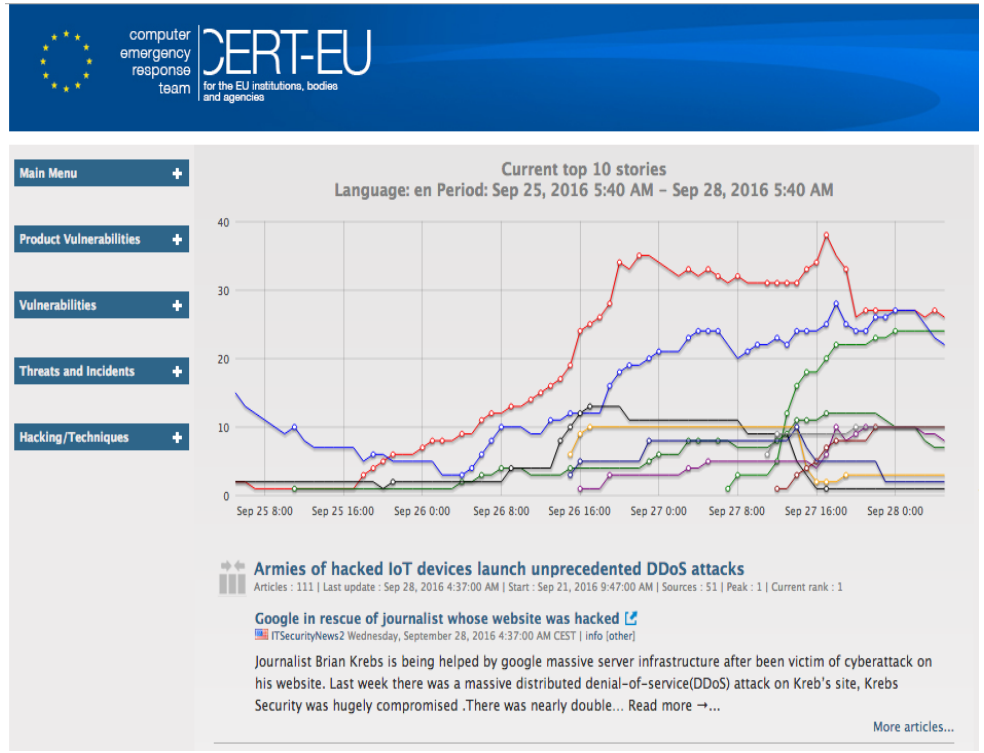
Make your life easier !

Lesson learned

- Be prepared
  - Processes
  - Trainings
  - Disclosure policy
- Expect heavy workload the first month
- Tooling !
  - DIY or from the shelf

computer emergency response team | CERT-EU for the EU institutions, bodies and agencies

Thank You



https://cert.europa.eu/
https://github.com/certeu/