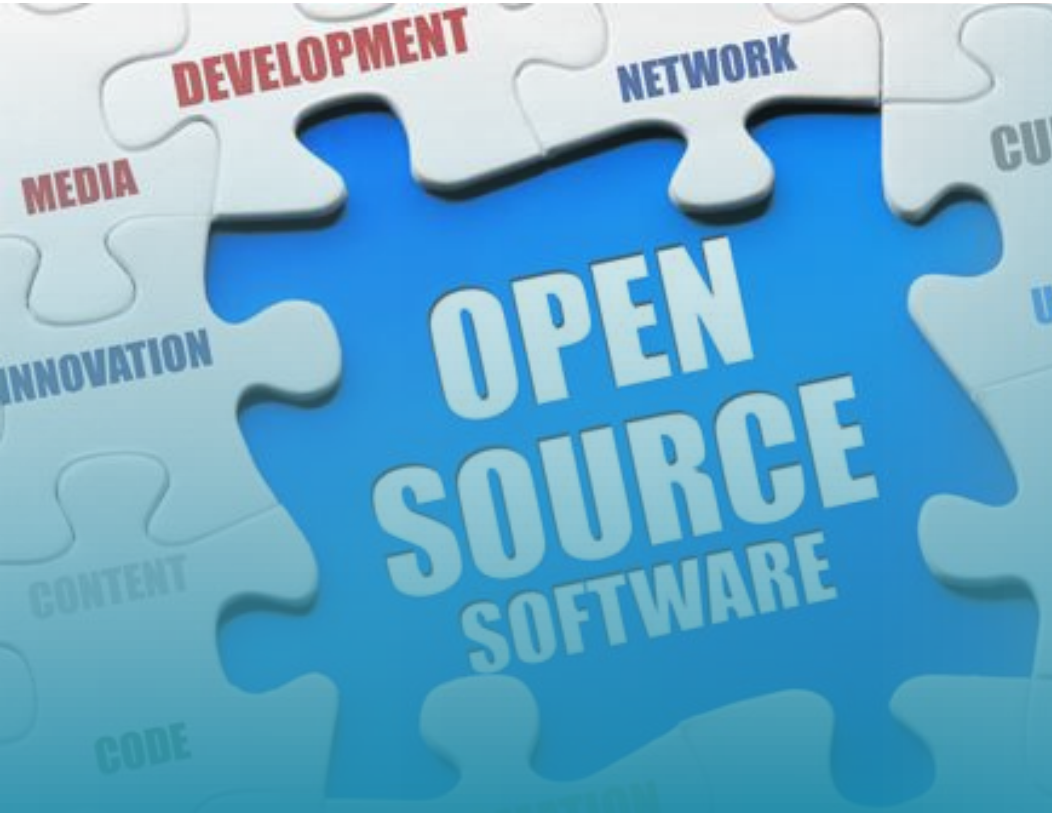


EU-FOSSA 2: An EU initiative to tackle Security of open source software

Saranjit ARORA
DIGIT Directorate-General for Informatics
European Commission

Informatics

Agenda

- Background
- EU-FOSSA Pilot → EU-FOSSA 2
- EU-FOSSA 2 – Progress to date

EU-FOSSA journey

In 2014, caused worldwide damage

€500M+

Initiative → Pilot project → Preparatory Action → Standing EU activity

EU-FOSSA (2015-2016)

European Parliament 1M€

EU-FOSSA 2 (2017-2019)

European Parliament 2,6M€

EU-FOSSA - the Pilot project (2015-2016)

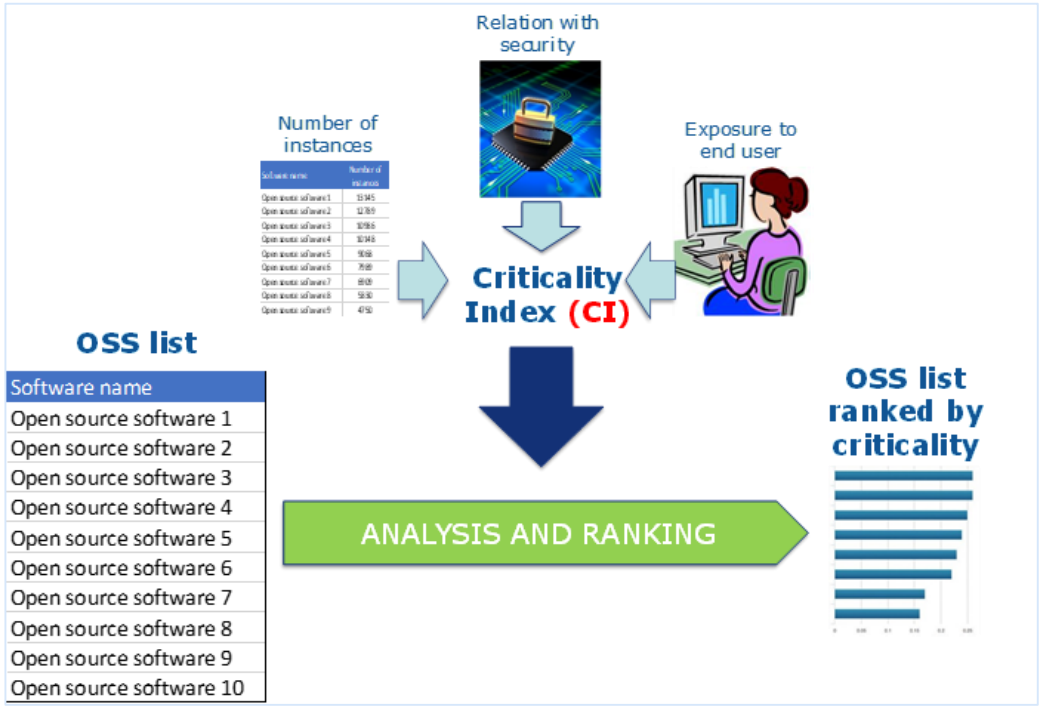
Approach

- Methodology
- Inventory of FOSS used at the EC
- Developer communities
- Public survey
- Formal code reviews

Lessons learned

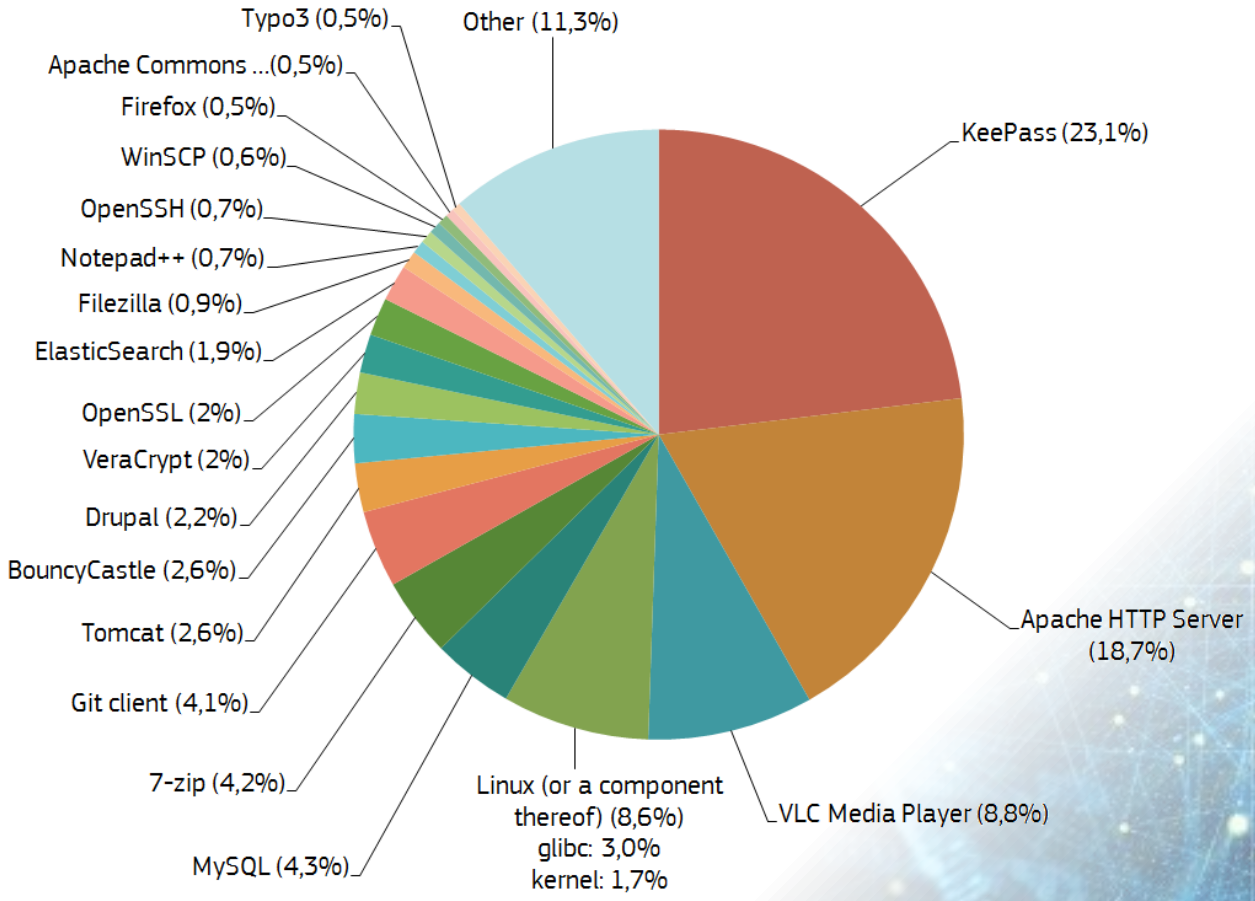
- Methodology works
- What about fixing bugs?
- Improve cooperation with communities
- Positive reaction
- Code reviews useful (but...)

EU-FOSSA - OSS criticality ranking



EU-FOSSA - Public Survey

- June 2016
- 3282 participants



EU-FOSSA 2 (2017-2019)

What is new?

- Increased scope
- Bug Bounties
- Hackathons
- Fixing already known bugs
- Closer cooperation with developer communities
- Improved communications programme

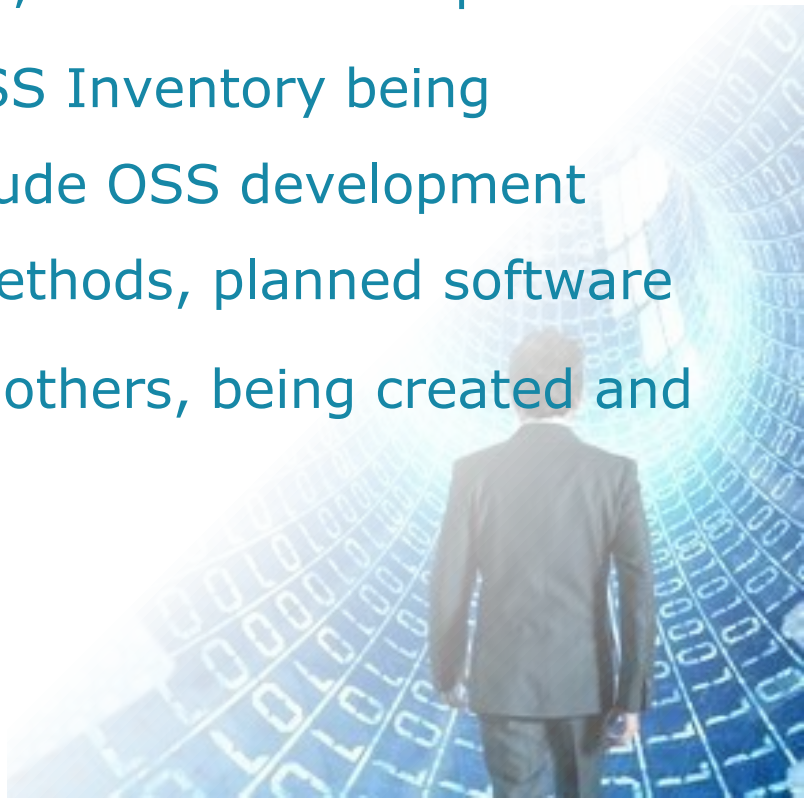
PLAN

Wider Scope

PROGRESS

- Expand scope beyond European Commission to other European institutions
- Include SDKs, frameworks, methods and *planned* OSS

- European Parliament, Council, EIB, EEAS, EES-COR, Council of Europe
- Commission OSS Inventory being updated to include OSS development frameworks, methods, planned software
- Inventories for others, being created and updated



PLAN

Bug Bounty programme

Proof of concept

- First time in EU institutions
- 28 active participants
- 6 weeks
- 6 bounties paid

Main programme

- ~15 activities
- Critical OSS used by EU institutions
- ~1 M€ budget
- Including high rewards

PROGRESS

Bug Bounties

- 3 vendors selected via public procurement tender (Intigriti → HackerOne → Econocom)
- After consulting with European institutions and the last public survey, a target software list has been identified
- 14-16 Contracts to be placed with vendors by end December 2018
- Bug Bounties to start in Jan 2019 and run until budget is exhausted

7-ZIP	DSS	midPoint	VLC Media Player
Apache Kafka	FileZilla	Notepad ++	WSO2
Apache Tomcat	FLUX TL	PHP Symfony	
Drupal	KeePass	PuTTY	

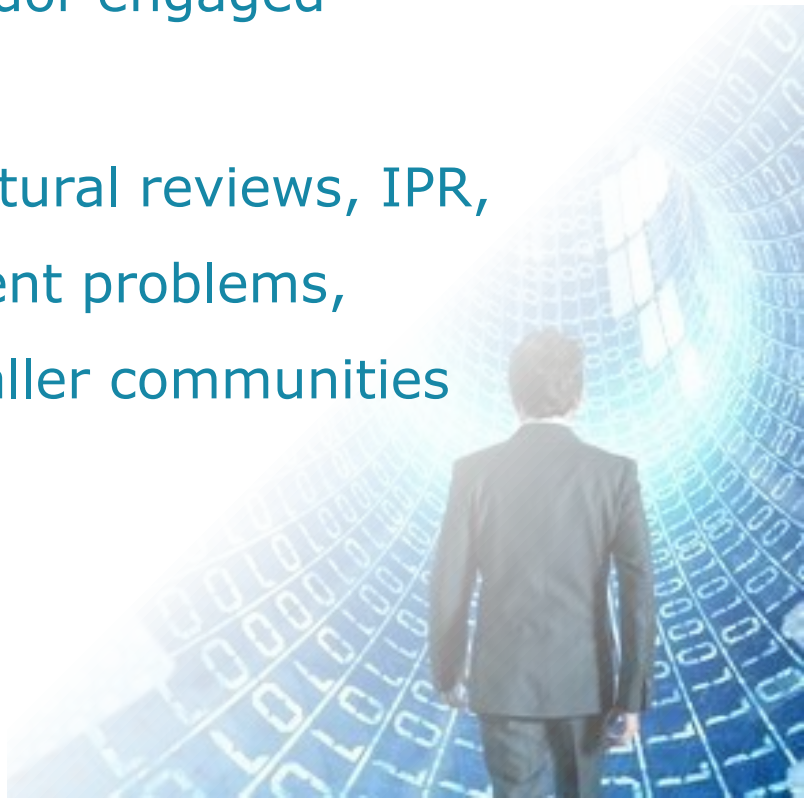
Hackathons

PLAN

- Plan 3 Hackathons (Brussels)
- Engage specialist Hackathon vendor
- Identify suitable projects
- Start planning

PROGRESS

- End Feb, end April, end Sep 2019
- Hackathon vendor engaged – BeMyApp, Paris
- Ideas: Architectural reviews, IPR, solving persistent problems, supporting smaller communities



Communications

PLAN

- Engage Communications

  Vendor, Internal coordinator
- Communicate with
  - OS Communities
  - EU Public

PROGRESS

- End Feb, end April, end Sep 2019
- Hackathon vendor engaged – BeMyApp, Paris
- Work starts in Jan 2019
  - Multiple public surveys
  - Conferences
  - OSS community meetings
  - Security Campaigns

EU-FOSSA 2 - the ultimate goal

- Improve security of open source software
- EU institutions working with open source software communities
- Make investment into the security of open source software a permanent action of the EU

Thank you

DIGIT-OSS-STRATEGY@ec.europa.eu