EU-FOSSA 2

Free and Open Source Software Auditing

ApacheCon Europe | Berlin | 23 October 2019

Marek Przybyszewski and Saranjit Arora

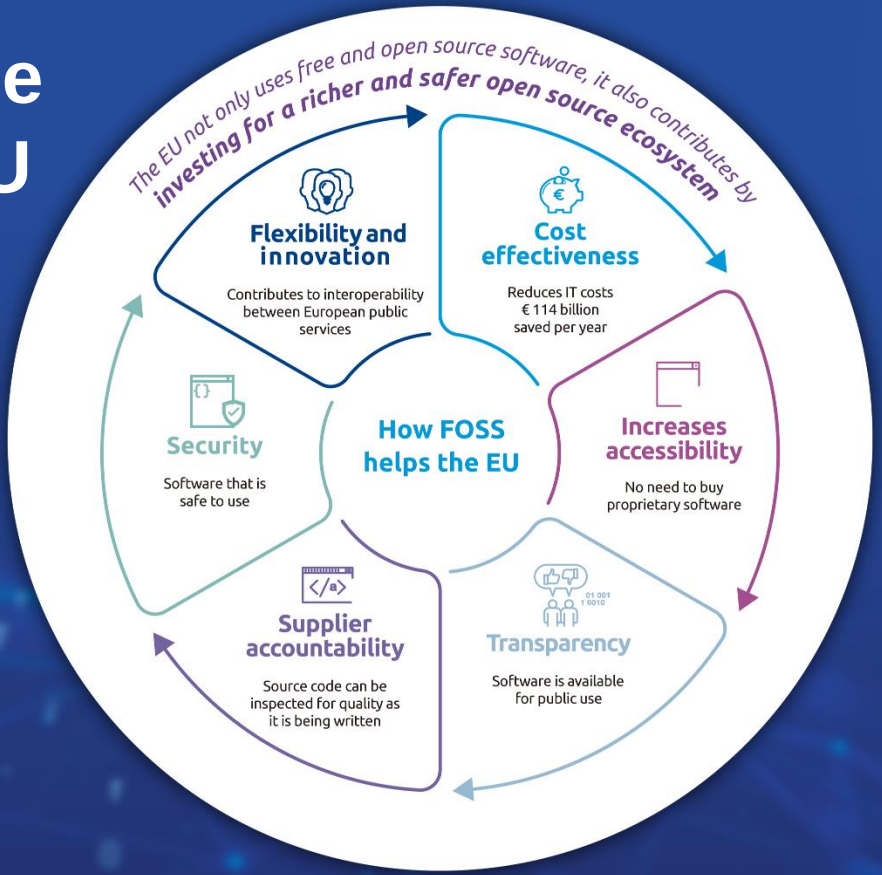
EU-FOSSA
Free and Open Source Software Auditing

Agenda

- OSS at the EC
- EU-FOSSA (2015-2016)
- EU-FOSSA 2 (2017-2019)
- What next?


20
HAPPY BIRTHDAY!

Open Source helps the EU



EU-FOSSA
Free and Open Source Software Auditing

The EU-FOSSA journey

INITIATIVE → PILOT PROJECT → PREPARATORY ACTION → STANDING EU ACTIVITY

EU-FOSSA (2015-2016)

EU-FOSSA 2 (2017-2019)

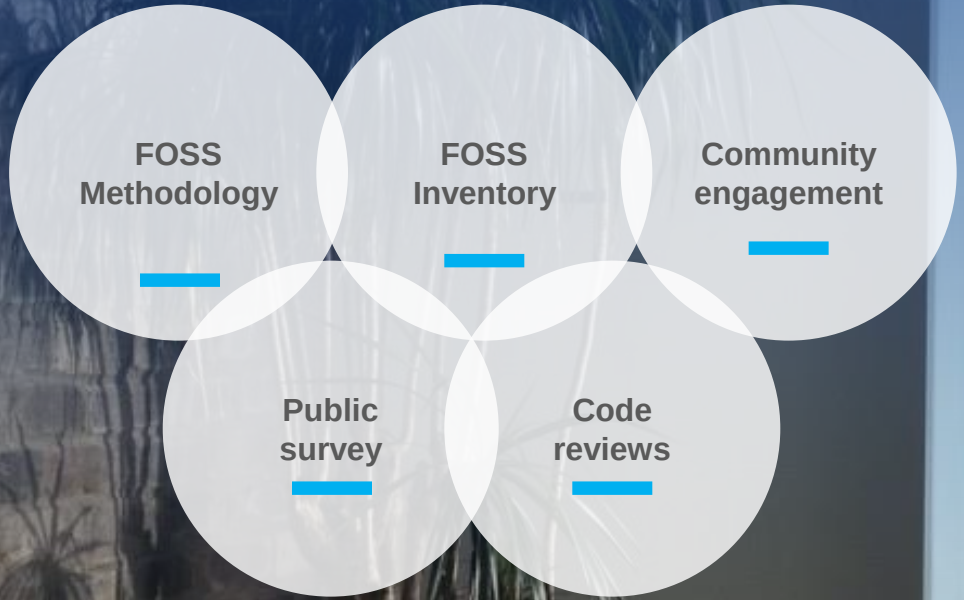
European Parliament

€ 2.6M

European Commission

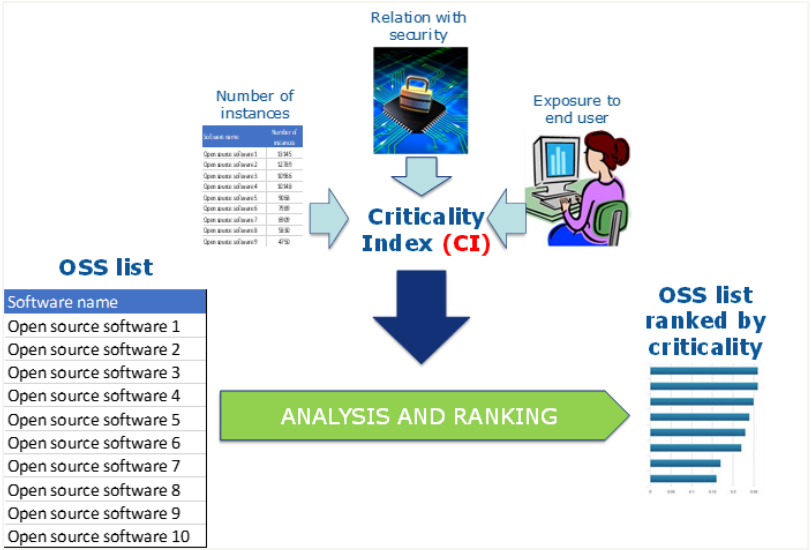
EU-FOSSA
Free and Open Source Software Auditing

Pilot project – EU-FOSSA 1



EU-FOSSA
Free and Open Source Software Auditing

Establishing our most critical FOSS



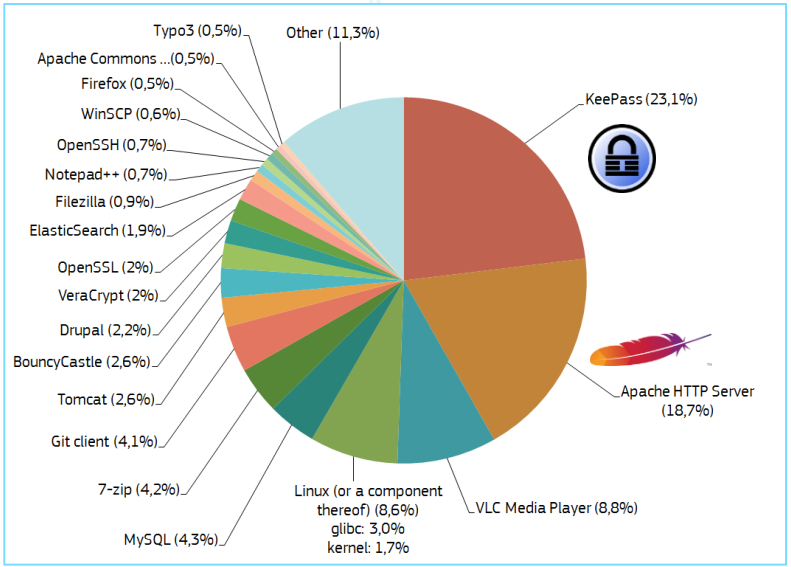
EU-FOSSA
Free and Open Source Software Auditing

Lessons from the EU-FOSSA pilot

- Positive reaction (EU, public, FOSS communities)
- Code reviews
  - Apache HTTP server core - no findings
- Only *find* bugs?
- Little communication/community engagement
- Methodology works

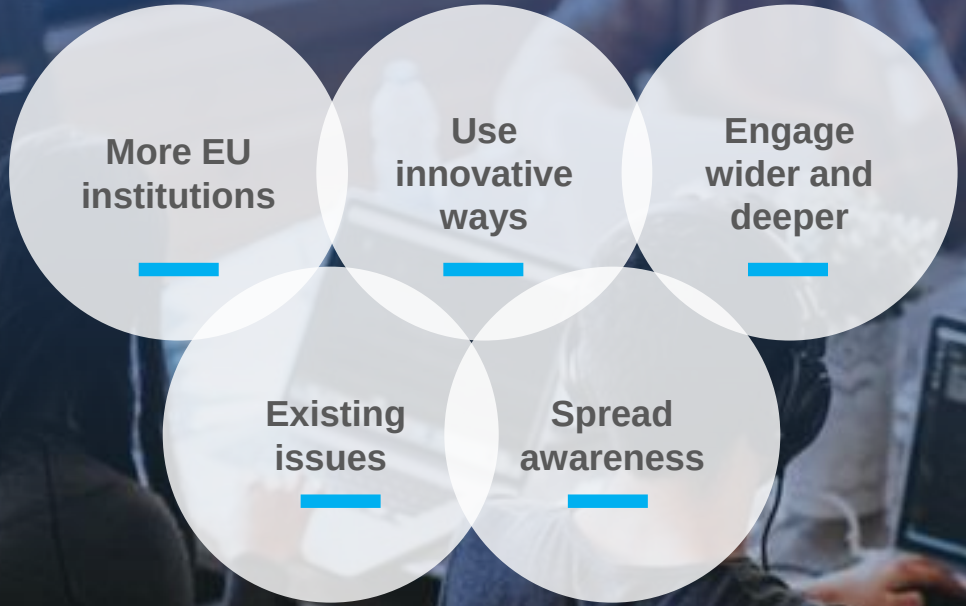
FOSS Security is really important!

Public survey results



EU-FOSSA
Free and Open Source Software Auditing

EU-FOSSA 2 Key Objectives



EU-FOSSA
Free and Open Source Software Auditing

EU-FOSSA 2 Activities

EU-FOSSA
Free and Open Source Software Auditing

Bug bounties

- First time in European institutions
- Primary security audit method
- Critical FOSS used in participating institutions
- 15 programmes launched (6 still running)
- 20% bonus for fixing the bug found

- 7-zip
- Apache Kafka
- Apache Tomcat
- Drupal
- DSS
- FileZilla
- Flux TL
- Glibc
- KeePass
- Midpoint
- Notepad++
- PHP Symfony
- PuTTY
- VLC
- WSO2

Tomcat Bug Bounty is open until 30 November

> Critical bug hidden for 20 years in PuTTy found and fixed

EU-FOSSA
Free and Open Source Software Auditing

Bug bounty results (so far)

Bugs reported	633
Bugs accepted	195
Bugs high or critical	24
Total Bounties paid	€201k

- *Please note, figures are not final*

> VLC 3.0.7 fixes 33 security issues, one of which is a high-severity flaw in an MPEG decoder software library

EU-FOSSA
Free and Open Source Software Auditing

Bug Bounty

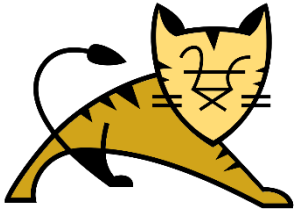
 # SUBMISSIONS 15

 # HACKERS 142

VALID VULNERABILITIES

0

Bug Bounty

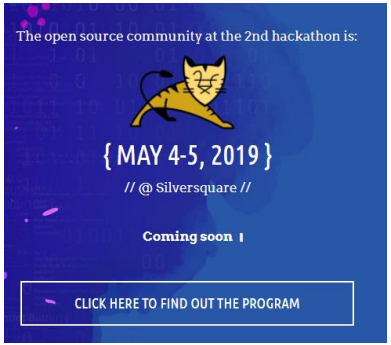


# SUBMISSIONS	13
# HACKERS	88

VALID VULNERABILITIES

3

Three Hackathons



Watch the videos

- Symfony
- Apache

EU-FOSSA
Free and Open Source Software Auditing

THE APACHE SOFTWARE FOUNDATION

APACHE PLC4X

Karaf

Apache SpamAssassin

Apache SINGA

APACHE Camel

Drupal patch automation

We commissioned a project to:

- Fix known critical vulnerabilities
- Automate patch updates

> The vast majority of external European Commission websites run on Drupal

Listening to smaller communities

We are in the process of connecting with many small/micro communities

Other studies

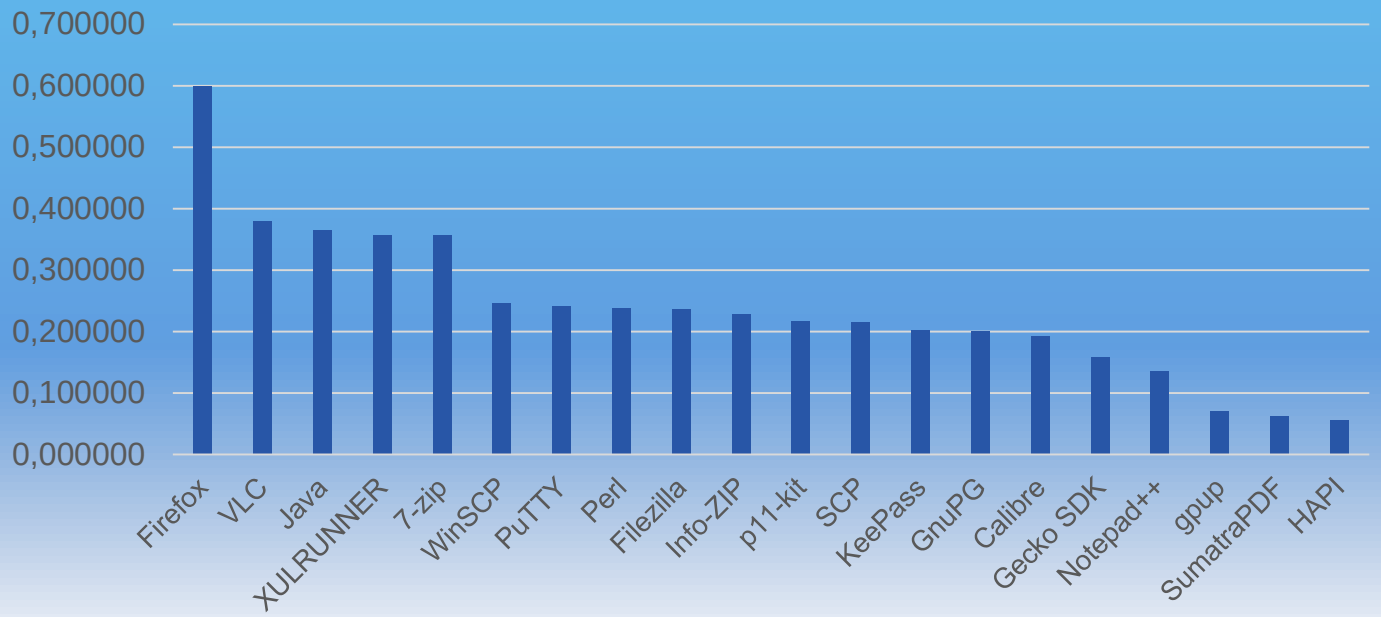
- IPR and IT support requirements
- State of Open Source Worldwide
  - Open source trends
  - Best practice usage by Public Administrations and key Private companies
  - Key internal/external stakeholders

Updated OSS Strategy

EU-FOSSA
Free and Open Source Software Auditing

Inventory - most critical open source software we use

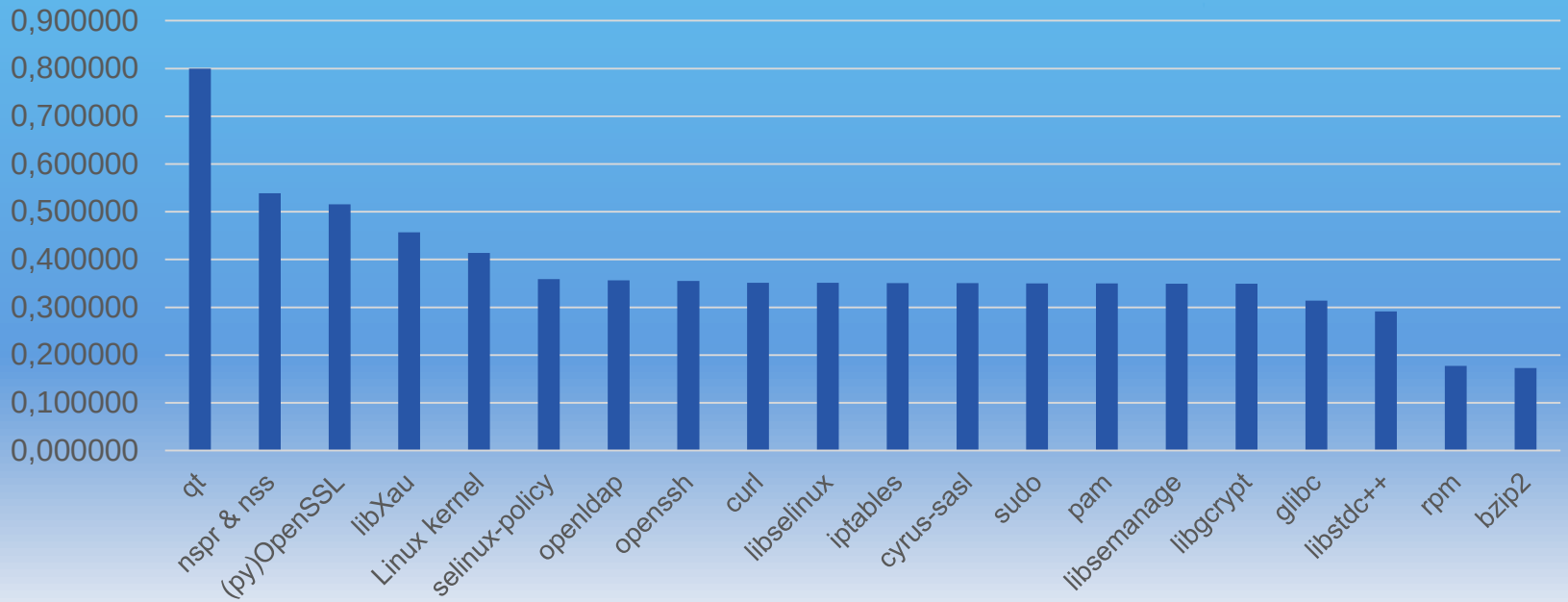
Top 20: Work Stations and App-V



EU-FOSSA
Free and Open Source Software Auditing

Inventory - most critical open source software we use

Top 20: Server-side



EU-FOSSA
Free and Open Source Software Auditing

Communication Strategy

Developer engagement

- COMMUNITIES
- FOSS EVENT
- AMA's
- CONFERENCES

Public surveys

- GENERAL PUBLIC
- DEVELOPERS

Outreach campaign

- CONTENT
- FOSS EVENT
- PRINT
- SOCIAL MEDIA
- UNIVERSITIES
- WEBSITE

EU-FOSSA
Free and Open Source Software Auditing

Brand touchpoints

- Brand refresh - new logo and visual identity
- Website
- Goodies
- Coordination of comms efforts on:
  - Hackathons
  - Bug bounties
  - Internal / external promotion

Media interest

- Overwhelming coverage by media, both technical and generalist publications
- Over **135 news articles** published on EU-FOSSA 2 in the past 8 months
- Content with the most successful performance on DIGIT's Twitter account

Next steps

- Highly successful and visible
- Hackathons → internal projects
- Project continuation being discussed
- Open source strategy being updated
- Open source use is increasing across European institutions

EU-FOSSA
Free and Open Source Software Auditing

Thank You

DIGIT-OSS-STRATEGY@ec.europa.eu