EU-FOSSA 2

Free and Open Source Software Auditing

30 October 2019

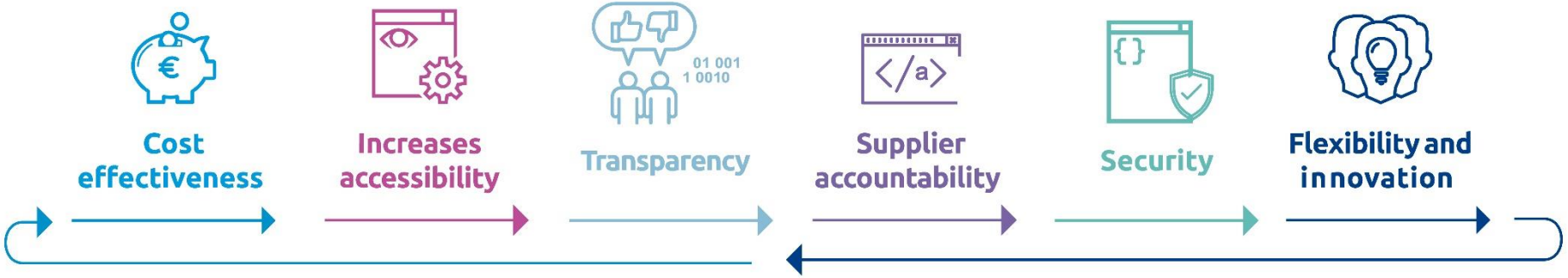
Marek Przybyszewski and Saranjit Arora

European Commission, Directorate General for Informatics

EU-FOSSA

Free and Open Source Software Auditing

How 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)

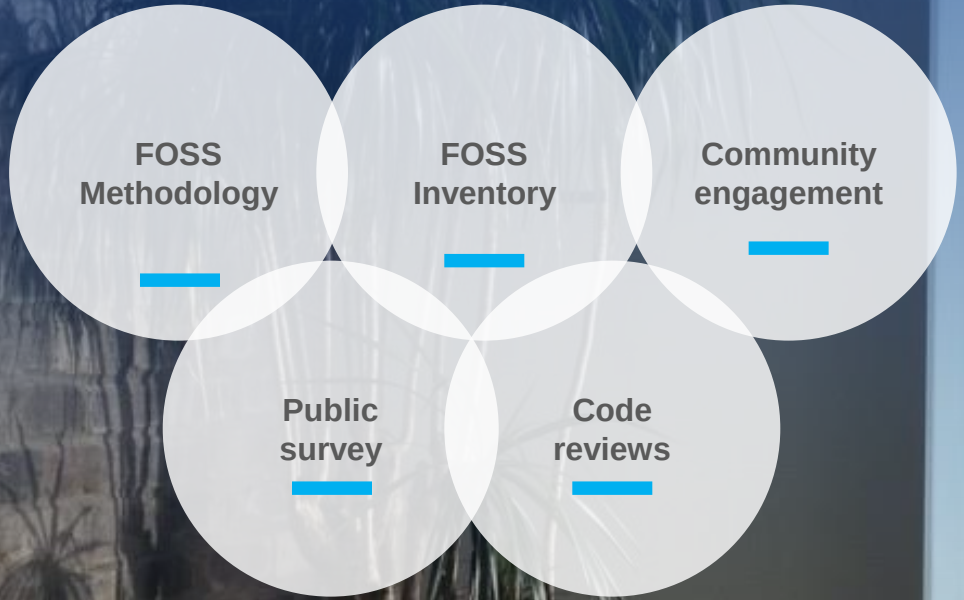
European Parliament

€ 2.6M

European Commission

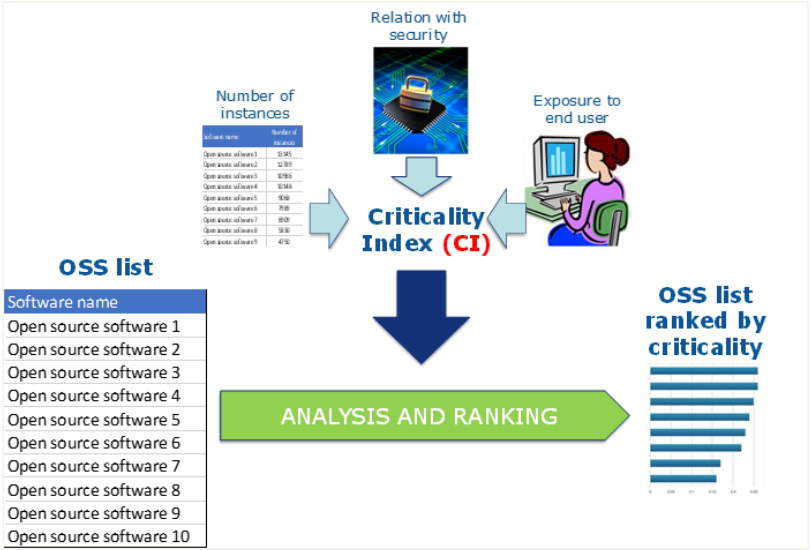
EU-FOSSA
Free and Open Source Software Auditing

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

Sustainability indicators

Category	Metric Name
Community Activity	Code Activity (contributions and contributors)
	Release History
	Number of Commits
	Number of Tickets
	Communications (Mailing list, posts, forums, chat history)
	Number of Adoptions/Implementations by External Organisations / Communities
	SW Evolution (code, architecture, bug/feature)
	Programming Language Used
	Project Domain (OS, Application SW, IDE, Application servers, Libraries, desktop Environments and frameworks). I.e. Apache, Linux, Eclipse, Mozilla, Ant, GNoME, KDE)
	Source Code (repositories like CVS/SVN for code base, GitHub, source forge).
Performance	Time to Resolve Tickets
	Time Spent in Code Reviews
	Pending Work

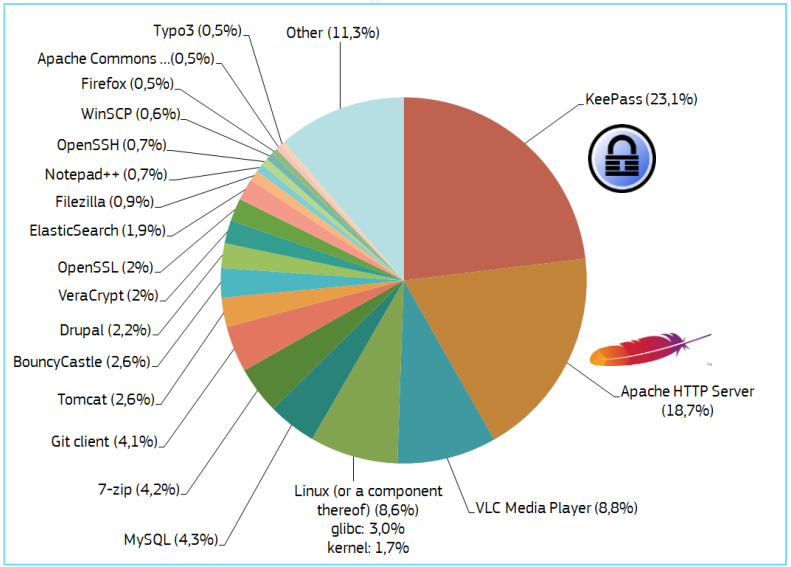
Category	Metric Name
Quality and Security	Security Requirements
	Threat Modelling
	Security Code reviews
	Security Testing
	Vulnerability Management
	Software Development Methodologies
	SLA
Demographics And Diversity	Longevity
	Real Knowledge Existent in the market of the language and Platforms Used.
	People Participating
	Organisation Participating
	Geographically distributed user community
Governance	Project Management
	Project Roadmap
	Project Structure
	Documentation
	Licensing
	Training
FOSS Support	Funding - Monetary
	Work force
	Infrastructure assets

Lessons from the EU-FOSSA pilot

- Positive reaction (EU, public, FOSS communities)
- Code reviews
- Only *find* bugs?
- Little communication/community engagement
- Methodology works

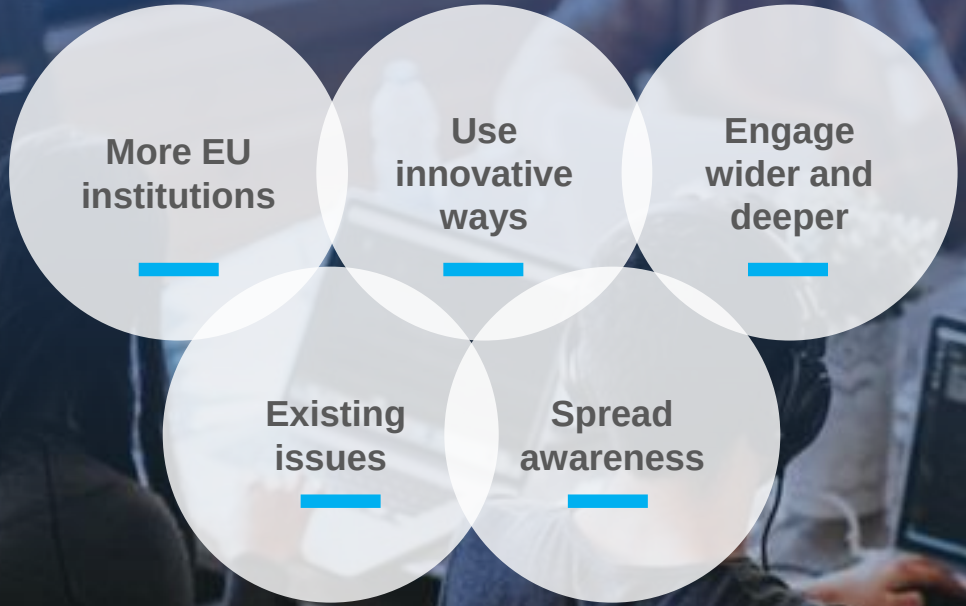
FOSS Security is really important!

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

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

PuTTY: CVE-2019-9894 + 7 more CVE-2019-38xx

EU-FOSSA
Free and Open Source Software Auditing

Bug bounty results (so far)

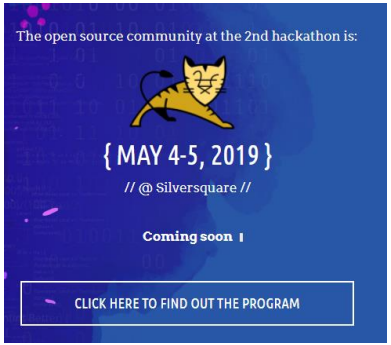
Bugs reported	633
Bugs accepted	195
Bugs high or critical	24
Total Bounties paid	€201k

- *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

VLC: CVE-2019-5439, CVE-2019-12874
Apache Tomcat: CVE-2019-0221, CVE-2019-0232
Drupal: CVE-2019-11831

Three Hackathons



Watch the videos

- Symfony
- Apache

EU-FOSSA
Free and Open Source Software Auditing


S HACKATHONS
Symfony
dayuse
CONGRATS!

THE APACHE SOFTWARE FOUNDATION

APACHE PLC4X

Karaf

Apache SpamAssassin

Apache SINGA

APACHE Camel

CONGRATS!!

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

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

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

Roadblocks to greater FOSS use

EU-FOSSA project tackles security in FOSS used in the European institutions

EU-FOSSA
Free and Open Source Software Auditing

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

https://ec.europa.eu/eu-fossa