

EU-FOSSA 2

Free and Open Source Software Auditing

ApacheCon Europe | Berlin | 23 October 2019



Marek Przybyszewski and Saranjit Arora



Agenda

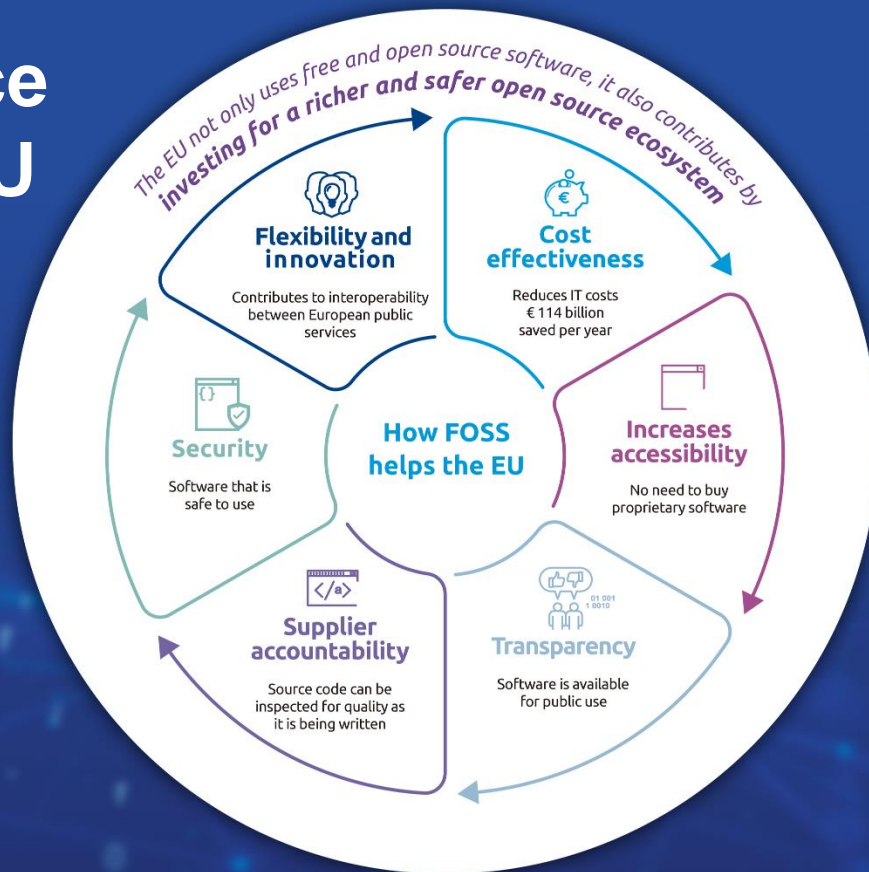
- OSS at the EC
- EU-FOSSA (2015-2016)
- EU-FOSSA 2 (2017-2019)
- What next?

```
<?php echo  
"Hello World!"  
?>
```





Open Source helps the EU



The EU-FOSSA journey



EU-FOSSA
(2015-2016)

EU-FOSSA 2
(2017-2019)



€ 2.6M



Pilot project – EU-FOSSA 1

**FOSS
Methodology**

**FOSS
Inventory**

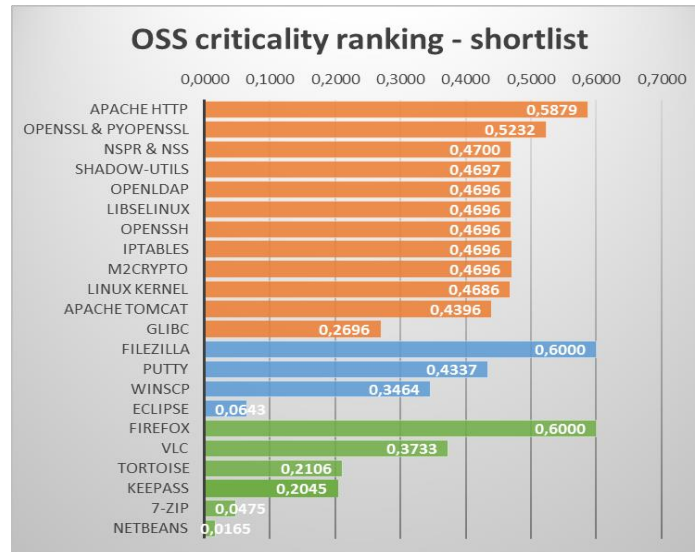
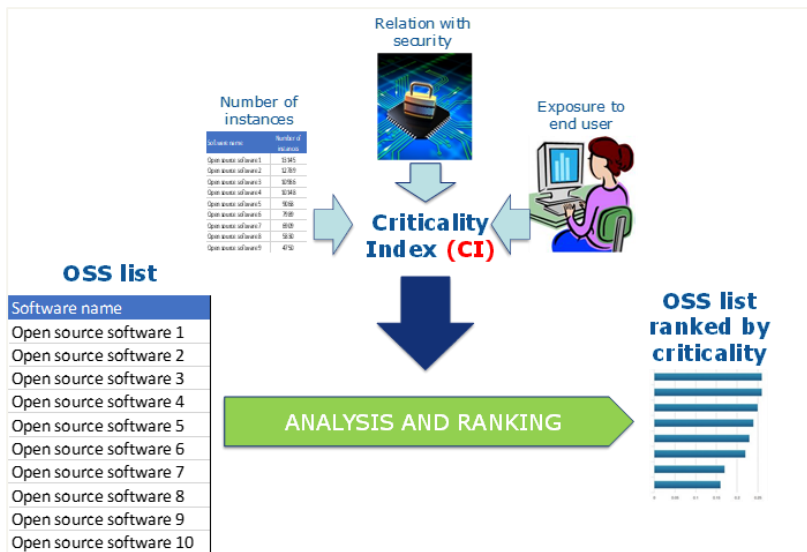
**Community
engagement**

**Public
survey**

**Code
reviews**



Establishing our most critical FOSS



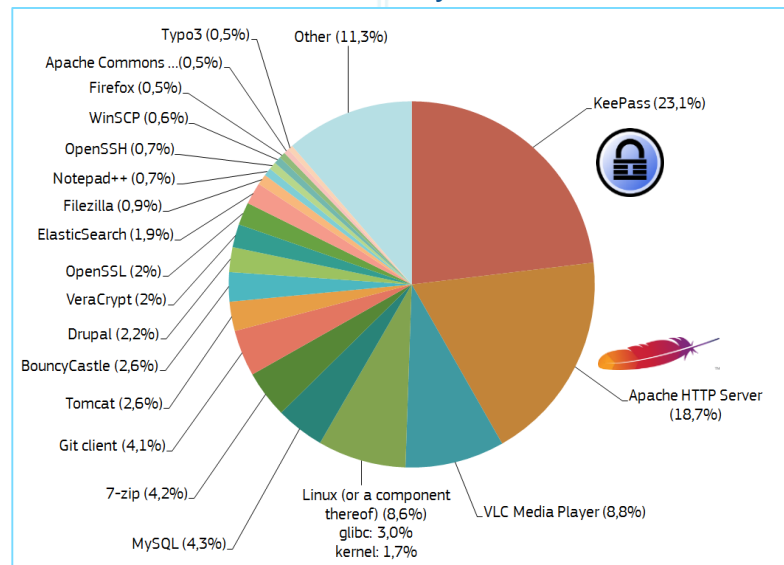
Lessons from the EU-FOSSA pilot

- 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 2 Key Objectives

**More EU
institutions**

**Use
innovative
ways**

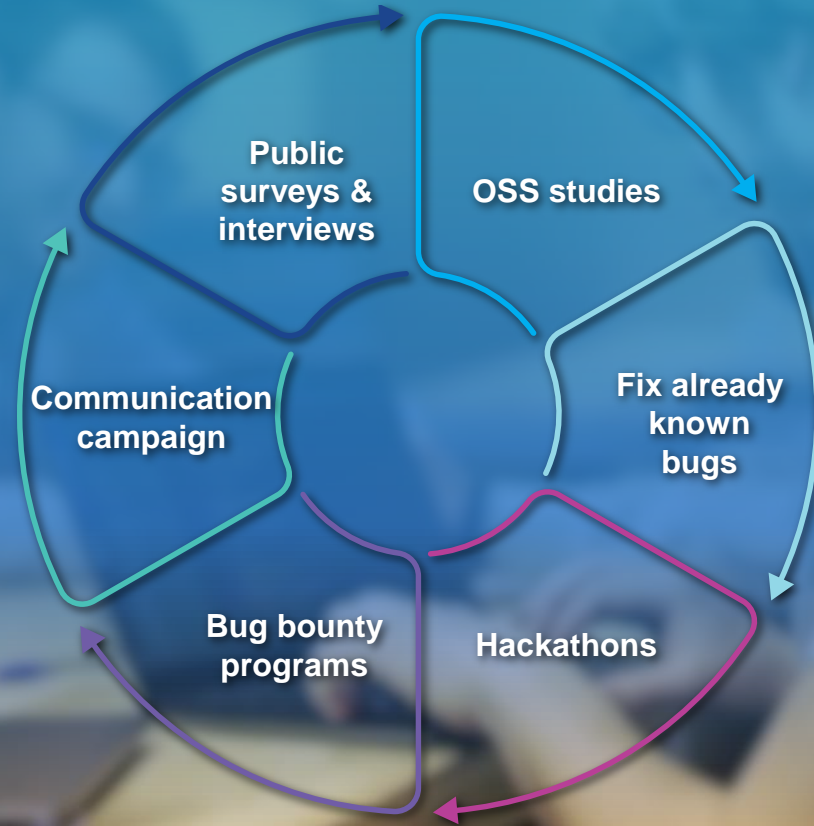
**Engage
wider and
deeper**

**Existing
issues**

**Spread
awareness**



EU-FOSSA 2 Activities



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

”



Bug bounty results (so far)

	Bugs reported	606
	Bugs accepted	213
	Bugs high or critical	70
	Total Bounties paid	€200k

- *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

”



Bug Bounty



SUBMISSIONS **15**

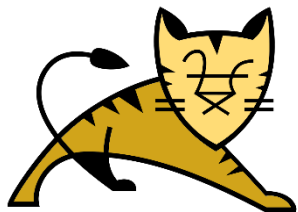
HACKERS **142**

VALID VULNERABILITIES

0



Bug Bounty



SUBMISSIONS **13**

HACKERS **88**

VALID VULNERABILITIES

3



Three Hackathons

The open source community at the 1st hackathon is:




{ APRIL 6-7, 2019 }
// @ Silversquare, Brussels //

PHP Symfony is a PHP web development framework with a set of reusable PHP components
API Platform is a set of tools to build and consume web APIs using PHP and Symfony

CLICK HERE TO FIND OUT THE PROGRAM

The open source community at the 2nd hackathon is:



{ MAY 4-5, 2019 }
// @ Silversquare //

Coming soon !

CLICK HERE TO FIND OUT THE PROGRAM

EU-FOSSA CYBER SECURITY HACKATHON
Free and Open Source Software Auditing



MAY THE SOURCE BE WITH EU

Watch the videos

- ➔ [Symfony](#)
- ➔ [Apache](#)





EU-FOSSA
Free and Open Source Software Auditing

{FOSS HACKATHONS WITH EU-FOSSA 2}



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

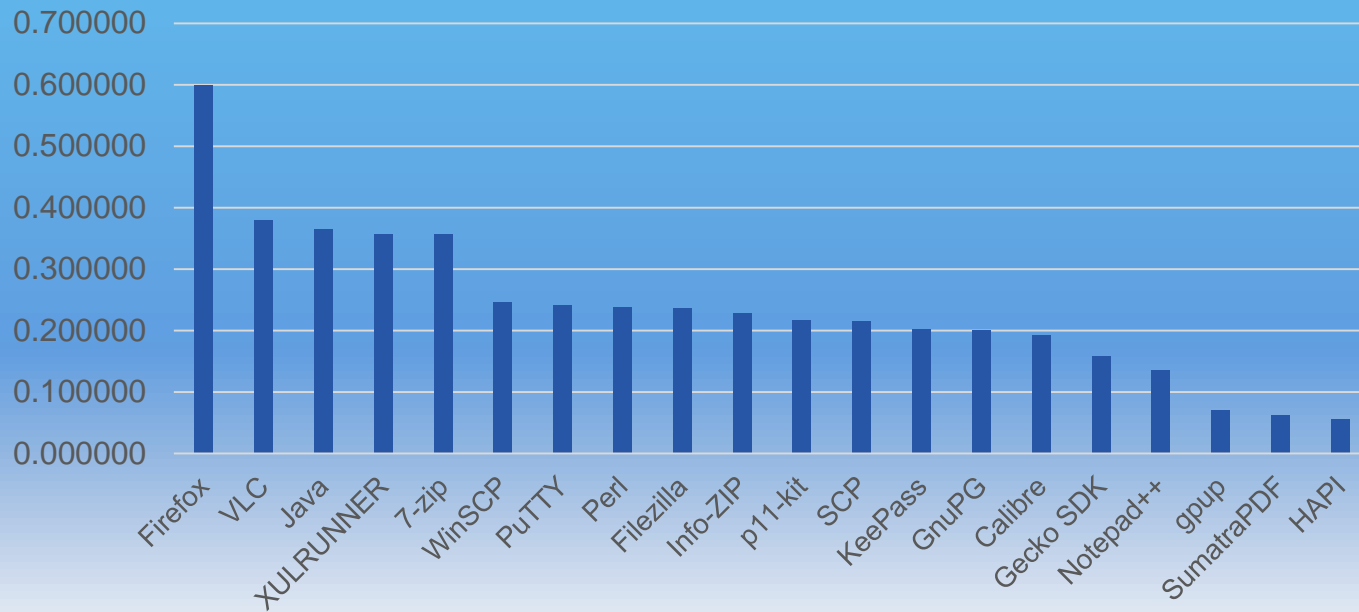


Updated OSS Strategy



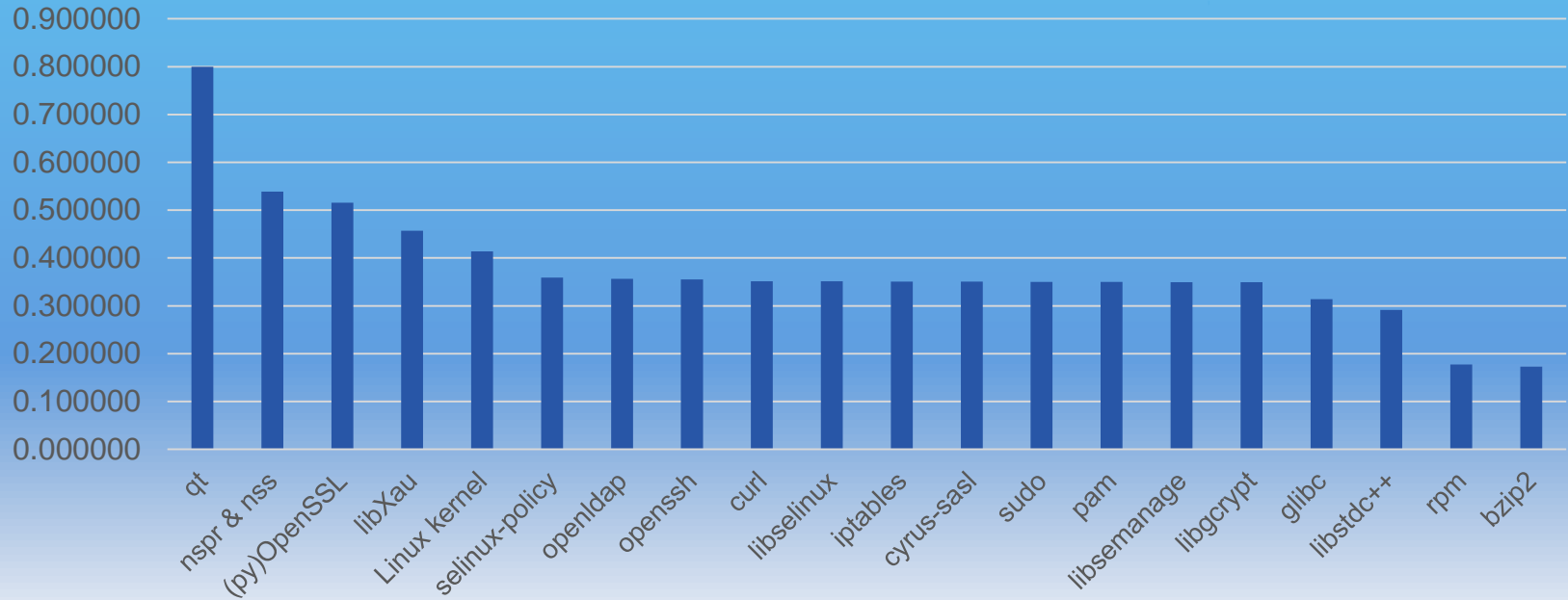
Inventory - most critical open source software we use

Top 20: Work Stations and App-V



Inventory - most critical open source software we use

Top 20: Server-side



Communication Strategy

Developer engagement

COMMUNITIES

FOSS EVENT

AMA's

CONFERENCES

Public surveys

GENERAL
PUBLIC

DEVELOPERS



Outreach campaign

CONTENT

PRINT

UNIVERSITIES

FOSS EVENT

SOCIAL MEDIA

WEBSITE



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

“

So the EU protected almost everybody from that one

”

The Register
19.03.2019



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

OPEN SOURCE BEYOND

2020

Powering a Digital Europe

14-15 November 2019 | Brussels, Belgium





```
...object to mirror_ob  
..._mod.mirror_object = mirror_ob  
...tion == "MIRROR_X":  
..._mod.use_x = True  
..._mod.use_y = False  
..._mod.use_z = False  
...tion == "MIRROR_Y":  
..._mod.use_x = False  
..._mod.use_y = True  
..._mod.use_z = False  
...tion == "MIRROR_Z":  
..._mod.use_x = False  
..._mod.use_y = False  
..._mod.use_z = True  
...tion at the end -add back the deselected  
...b.select= 1  
...b.select=1  
...st.scene.objects.active = modifier_ob  
...ected" + str(modifier_ob) # modifier  
..._ob.select = 0  
...y.context.selected_objects[0]  
...objects[one.name].select = 1  
...("please select exactly two objects,  
...OPERATOR CLASSES -----  
...s.Operator):  
...t mirror to the selected object""  
...t.mirror_mirror_x"  
..._x"
```

Thank You

DIGIT-OSS-STRATEGY@ec.europa.eu