INFORMATION DESIGN STUDIO
UNIVERSITA LA SAPIENZA
ADRIAN BARANOWSKI
MAX SCHMALENBACH

Open Source Vunerability Visualisation

Introduction and audience

1

1

Choice of Topic

The chocie is connected to the topic of Open Data and Open Science. It elaborates the important aspect of **safety in Open Source** ecosystems, in which the data is operating and is being stored.

2

Target Audience

For the target audience we have chosen the **Policymakers** - the part of society which uses systems based on Open Source code and is capable of funding the initiative. However number of vunerability shows that the area is widely used but underfinanced.

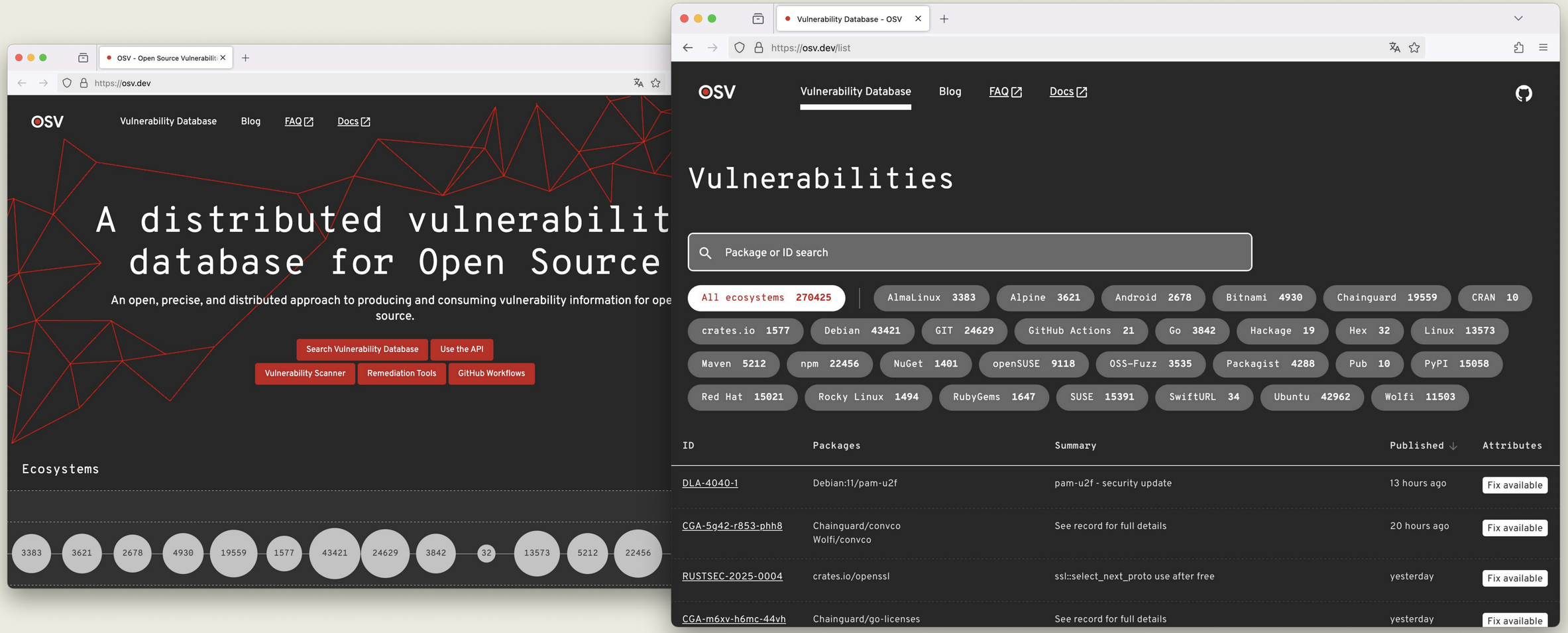
3

Message to Convey

We wanted to show how to reduce dangers and increase advantages of Open Source. We wanted to underline the still **growing usage** of OSS systems, **the dangers** such as bugs and hackers and the **opportunities** for safer future with **better funding**.

Collecting Data

2



OSV.DEV

Is an open database which keeps track on vunerabilities and bugs of Open Source Systems. It spreads the information among the developers of malfunction in code that might cause a serious issue in safety in each ecosystem. It also gives a very good statistical insight into the amount of bugs that appeared since

1

Summary prepared by Irving Wladawsky-Berger

Full report

EU Open Source study

2

A document prepared by the European Union, showing a research on estimated advantages of using and funding the Open Source systems, such as growth of GDP or increase of safety. It indicates many important statements concerning the topic, uses various examples from the past and projects future based on trends and calculations.

Charts - Open Source vs Private Systems

3

Not used idea of interpretation of the charts, which would show Open Source as an alternative for private data systems which's security lays only on the owner, yet still, companies such as Facebook violates the security of their users, without caring about the low costs of the fines.

Entries

35 million

Released

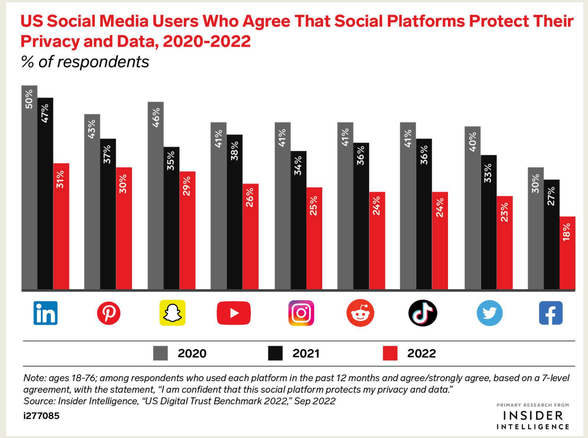
2023

Growing by entries

1 million

Composition

By also archiving deleted/ removed repositories NPM Follower presents a more dense picture. Also giving information about malware inflicted packages.



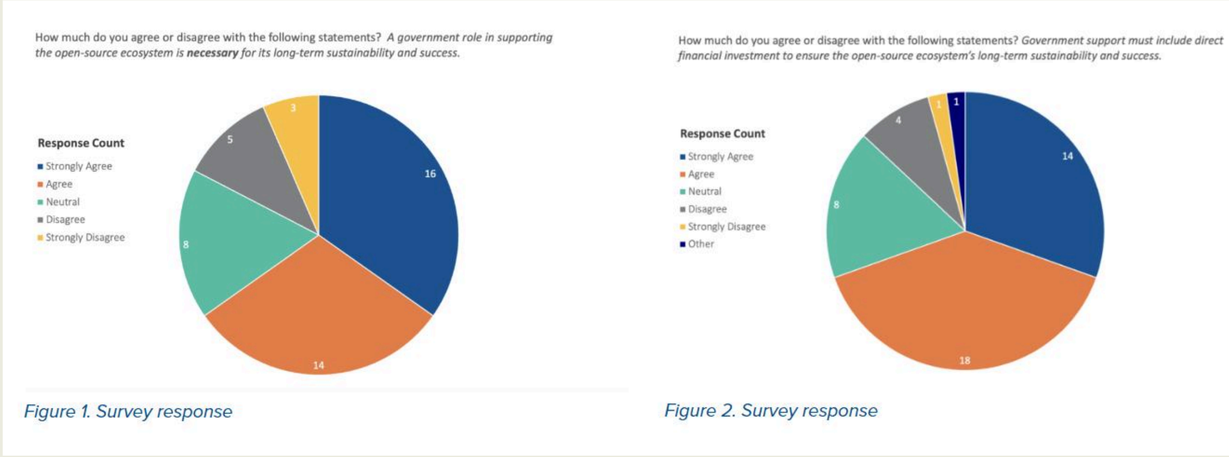
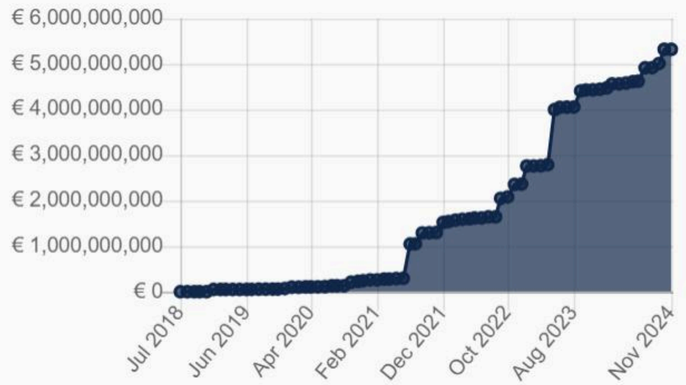


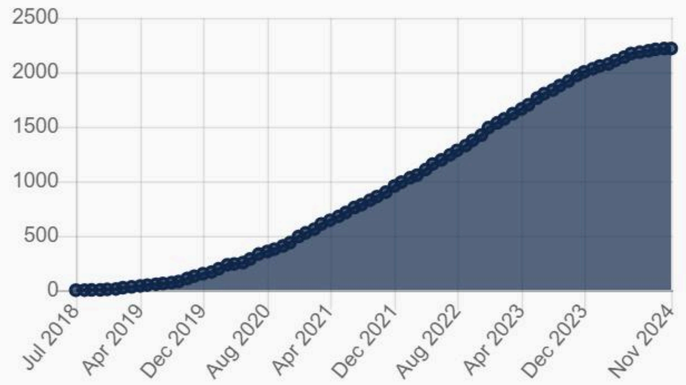
Figure 1. Survey response

Figure 2. Survey response

a) Course of overall sum of fines (cumulative):



b) Course of overall number of fines (cumulative):



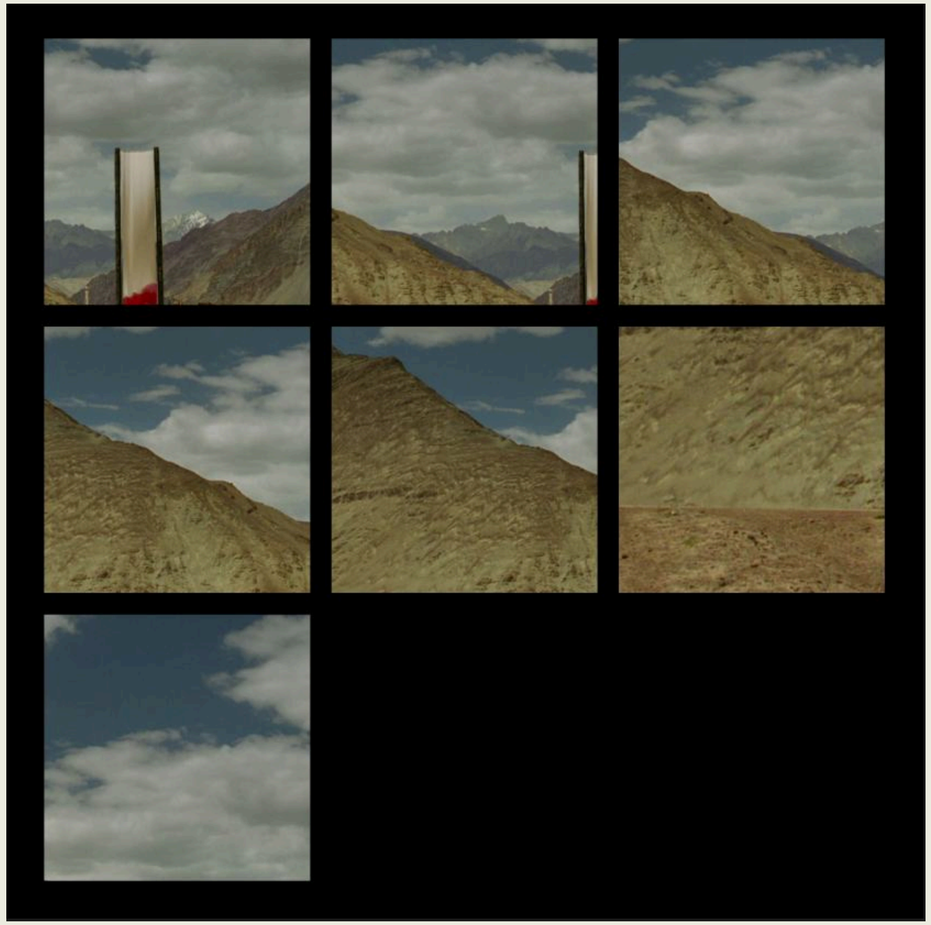
Concept & Storytelling

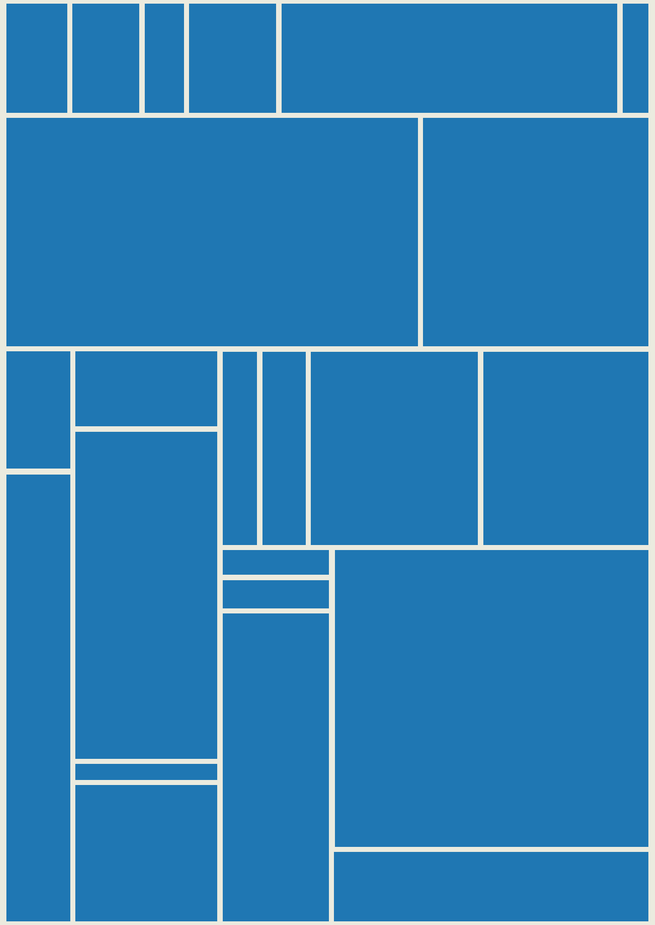
3



The glitched nature

The idea of showing glitched nature as a representation of broken or bugged Open Source enviroment.





The square design

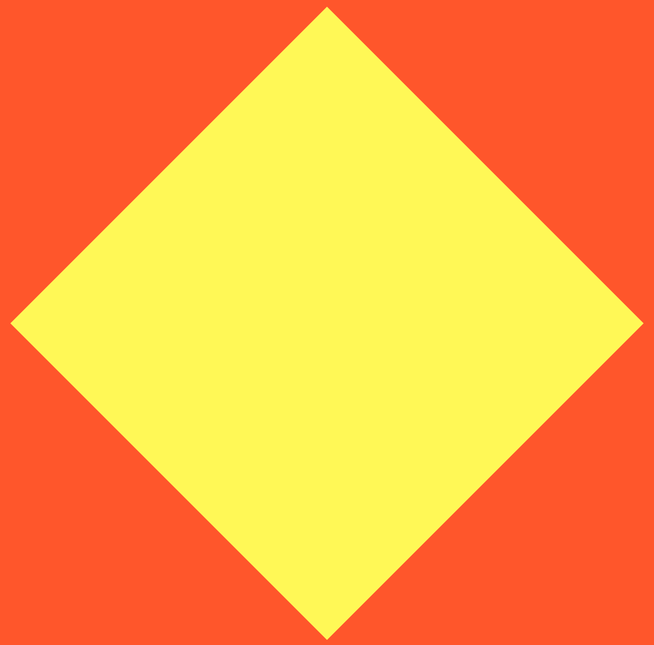
The idea of layout where each square represents a part of chart with the exact size corresponding the number of vunerabilities.

Potential to strenghtening public sector *integrating OSSH policy aspects into other policy initiatives, like education, competition or public procurement. Since OSS has a high importance for IT security, recommendations are derived related to the joint contribution of OSS and OSH towards the provision of secure and trustworthy ICT solutions. Finally, OSS has a large potential for the public sector and recommendations have been derived on strengthening the role of OSS in the development of interoperable solutions and public services.* - p 53 **Reducing software development duplication** *OSSH have an indirect impact on the consumption of resources, for the simple reason that they discourage the duplication of effort. When developing OSSH, industry agrees on common components in software and hardware that can be reused. In software, this leads to reduced effort which is necessary for digitalisation, thus achieving earlier positive externalities of digitalisation. In hardware, shared open source components could be produced in highly optimised processes, thus reducing the environmental impact. As an engine of commoditisation, both OSH and OSS result in moving the differentiation motivation higher up the value chain.* - p. 342 *Overall, the* ***companies with up to 50 employees*** *are responsible for almost* ***half of the contributors*** *or accounts at GitHub - a cost-benefit ratio of above 1:4 - p 14 Individual* ***contributors of 260,000, representing 8%*** *of 3.1 million EU employees in the computer programming sector in 2018 equating to* ***€1 billion personnel costs*** *- p. 15* ***10% increase leading to 0.4–0.6% additional GDP per year*** *- p. 14* ***€65–€95 billion contribution to EU GDP*** *- p. 14 FOSSA In 2015, when the European Parliament secured an initial budget of* ***€1 million****, to audit the security of the EU's most critical OSS. EU FOSSA 2, with a* ***€2.6 million*** *budget (European Commission, 2019). - p. 230 Yet, this project was only a pilot project with a limited scope and budget. It is recommended to consider* ***expanding the FOSSA bug bounty programme*** *into a permanent facility* - p. 332 *The role of OSS and OSH is currently not reflected in EU policy making - p. 332 Within those programs, our ethical* ***hackers found 249 bugs****, of which 57 were accepted and 33 were regarded as critical or high in nature. We paid* ***€ 111.470 in total as bug bounty*** *payments with the largest of these amounting* ***to € 10 000****. Several solutions were provided by the reporter and accepted by the open source teams, resulting in a 20% bonus for the reporter. - [https://blog.intigriti.com/customer-success/end-of-the-eu-fossa-2-bug-bounty-program-for-open-source-software]* ***Fifteen bug bounty programmes*** *resulted in the discovery of* ***200 hidden bugs****, including a* ***20-year-old bug*** *in PuTTy. The project paid over* ***€200 000 in rewards*** *to ethical hackers. - [https://commission.europa.eu/news/eu-fossa-2-eus-open-source-cybersecurity-project ends-2020-07-14_en]* ***Heartbleed bug*** *Until 2014,* ***OpenSSL*** *was maintained by* ***one full time developer*** *and a number of volunteers. Even though OpenSSL was* ***critical to the security*** *of a majority of the Web's traffic, the level of resources flowing into the project was completely insufficient to ensure the level of reliability and testing necessary for OpenSSL. The technical details of the now infamous* ***Heartbleed bug of 2014*** *are not relevant here; suffice it to say that it allowed an attacker to obtain (inter alia) the* ***private keys of servers*** *and users'* ***passwords****. The vulnerability stayed u****nreported for two years****, and there are instances of it having been exploited to gain access to systems. It has been called "****the worst vulnerability found*** *(at least in terms of its potential impact) since commercial traffic began to flow on the Internet" (Steinberg, 2014).*
the issue was fixed in very little time by a team at Google. In the case of proprietary software, vulnerabilities sometimes stay unfixed for a long time, and if the owner of the code does not choose or wish to fix the code,

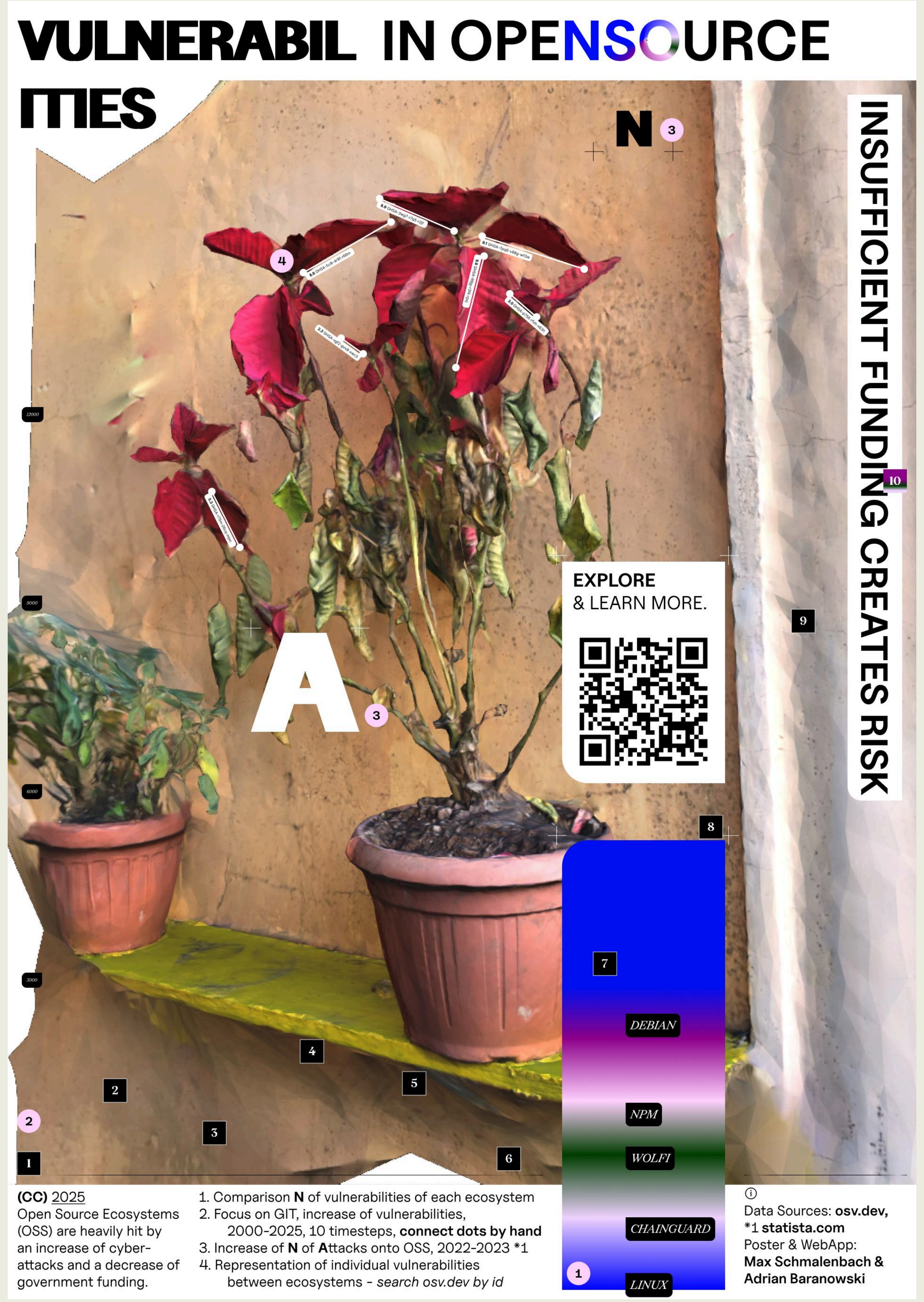
The story to be told

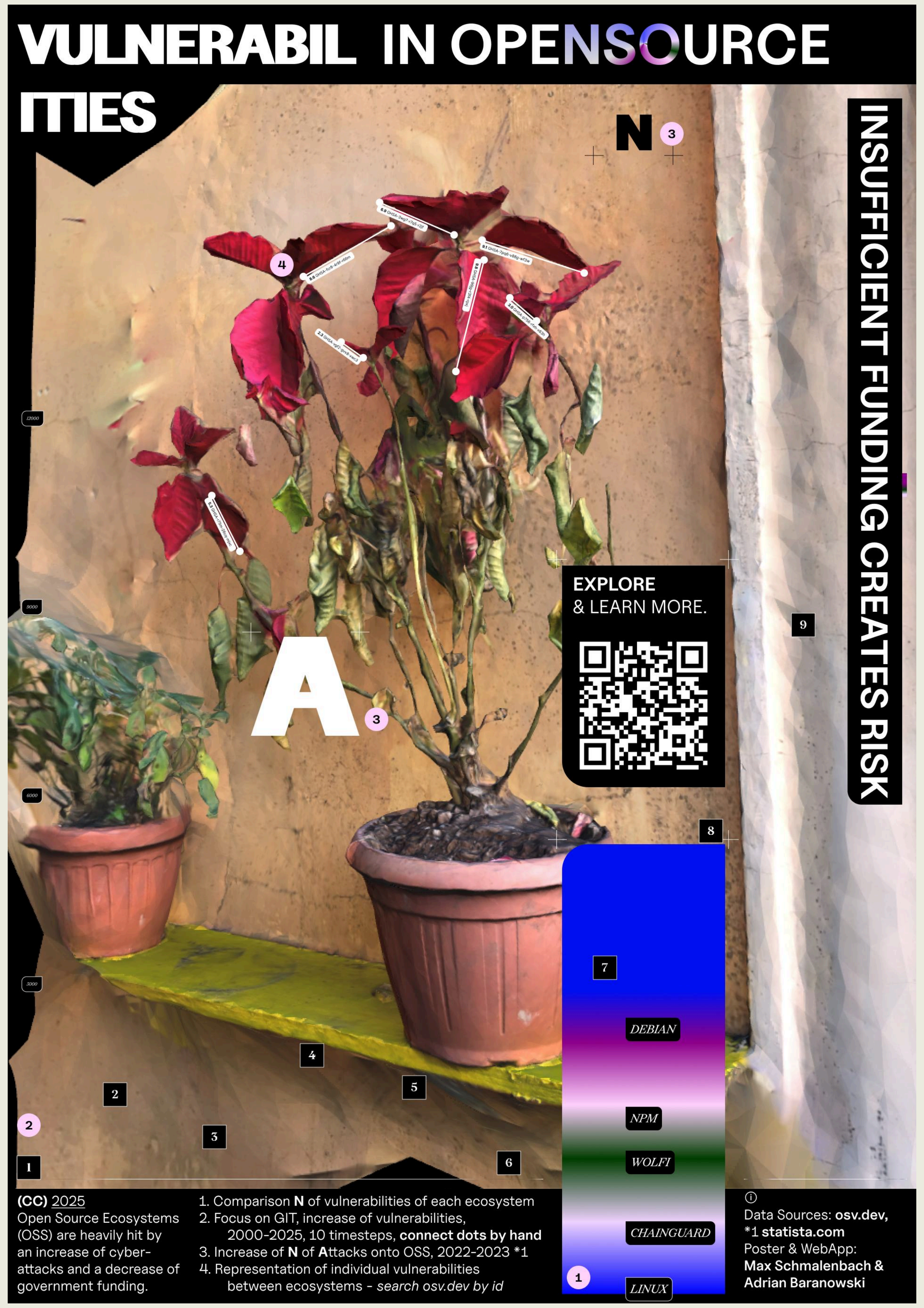
The story would be about the fact that the IT system we use is still compatibile with the system we had for more than 20 years ago - so the bugs from those times are still existing. We also focused on some known hacker attacks that shaped the current value of cybersecurity.

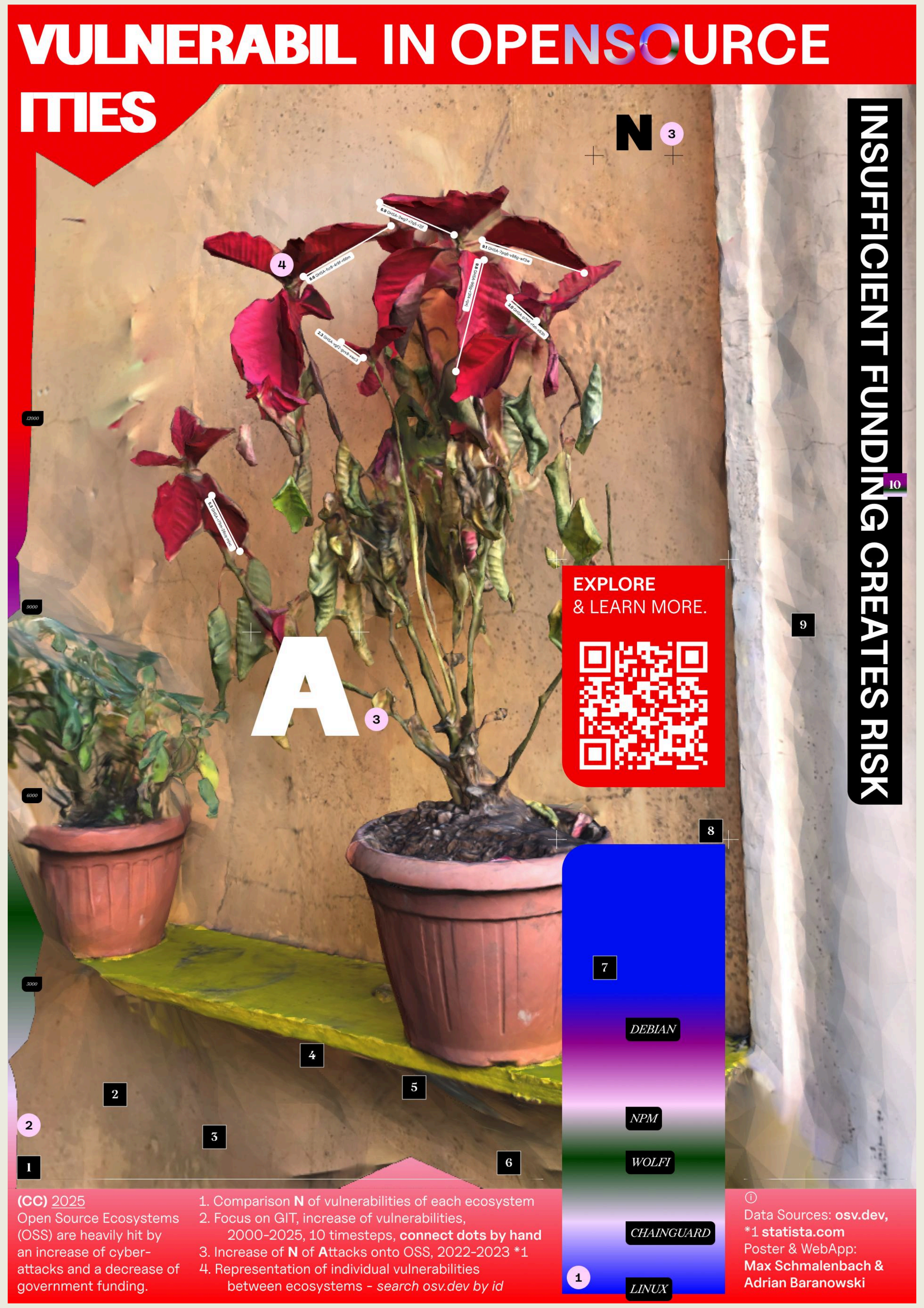
Poster



4


VULNERABIL IN OPENSOURCE
ITIES
INSUFFICIENT FUNDING CREATES RISK
N
A
EXPLORE
& LEARN MORE.
DEBIAN
NPM
WOLFI
CHAINGUARD
LINUX
(CC) 2025
Open Source Ecosystems (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.
1. Comparison N of vulnerabilities of each ecosystem
2. Focus on GIT, increase of vulnerabilities, 2000-2025, 10 timesteps, connect dots by hand
3. Increase of N of Attacks onto OSS, 2022-2023 *1
4. Representation of individual vulnerabilities between ecosystems - search osv.dev by id
Data Sources: osv.dev, *1 statista.com
Poster & WebApp: Max Schmalenbach & Adrian Baranowski


VULNERABIL IN OPENSOURCE
ITIES
INSUFFICIENT FUNDING CREATES RISK
N
A
EXPLORE
& LEARN MORE.
DEBIAN
NPM
WOLFI
CHAINGUARD
LINUX
(CC) 2025
Open Source Ecosystems (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.
1. Comparison N of vulnerabilities of each ecosystem
2. Focus on GIT, increase of vulnerabilities, 2000-2025, 10 timesteps, connect dots by hand
3. Increase of N of Attacks onto OSS, 2022-2023 *1
4. Representation of individual vulnerabilities between ecosystems - search osv.dev by id
Data Sources: osv.dev, *1 statista.com
Poster & WebApp: Max Schmalenbach & Adrian Baranowski


VULNERABIL IN OPENSOURCE
ITIES
INSUFFICIENT FUNDING CREATES RISK
N
A
EXPLORE
& LEARN MORE.
DEBIAN
NPM
WOLFI
CHAINGUARD
LINUX
(CC) 2025
Open Source Ecosystems (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.
1. Comparison N of vulnerabilities of each ecosystem
2. Focus on GIT, increase of vulnerabilities, 2000-2025, 10 timesteps, connect dots by hand
3. Increase of N of Attacks onto OSS, 2022-2023 *1
4. Representation of individual vulnerabilities between ecosystems - search osv.dev by id
Data Sources: osv.dev, *1 statista.com
Poster & WebApp: Max Schmalenbach & Adrian Baranowski

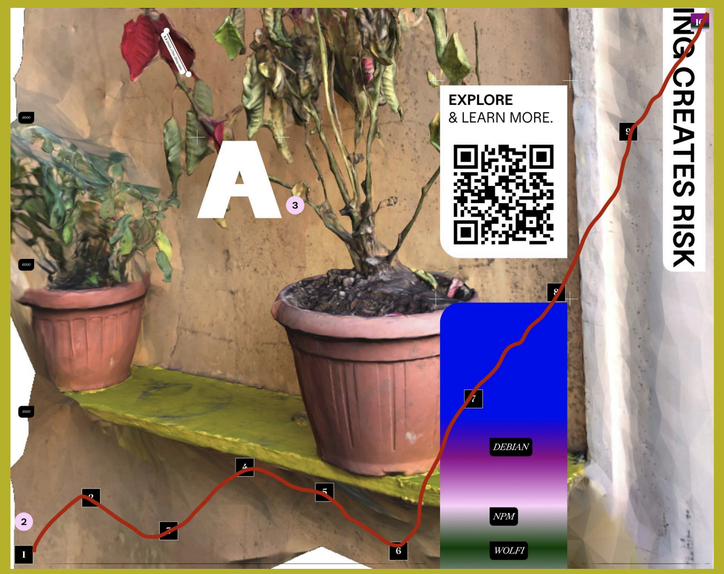

VULNERABIL IN OPENSOURCE
ITIES
INSUFFICIENT FUNDING CREATES RISK
N
A
EXPLORE
& LEARN MORE.
DEBIAN
NPM
WOLFI
CHAINGUARD
LINUX
(CC) 2025
Open Source Ecosystems (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.
1. Comparison N of vulnerabilities of each ecosystem
2. Focus on GIT, increase of vulnerabilities, 2000-2025, 10 timesteps, connect dots by hand
3. Increase of N of Attacks onto OSS, 2022-2023 *1
4. Representation of individual vulnerabilities between ecosystems - search osv.dev by id
Data Sources: osv.dev, *1 statista.com
Poster & WebApp: Max Schmalenbach & Adrian Baranowski


VULNERABIL IN OPENSOURCE
ITIES
N
A
EXPLORE
& LEARN MORE.
INSUFFICIENT FUNDING CREATES RISK
DEBIAN
NPM
WOLFI
CHAINGUARD
(CC) 2025
Open Source Ecosystems (OSS) are heavily hit by an increase of cyber-attacks and a decrease of
1. Comparison N of vulnerabilities of each ecosystem
2. Focus on GIT, increase of vulnerabilities, 2000-2025, 10 timesteps, connect dots by hand
3. Increase of N of Attacks onto OSS, 2022-2033 *1
Data Sources: osv.dev, *1 statista.com
Poster & WebApp:


OPENSOURCE
N
EXPLORE
& LEARN MORE.
INSUFFICIENT FUNDING CREATES RISK
DEBIAN
NPM
WOLFI
CHAINGUARD
LINUX
Data Sources: osv.dev, *1 statista.com
Poster & WebApp:
Max Schmalenbach & Adrian Baranowski

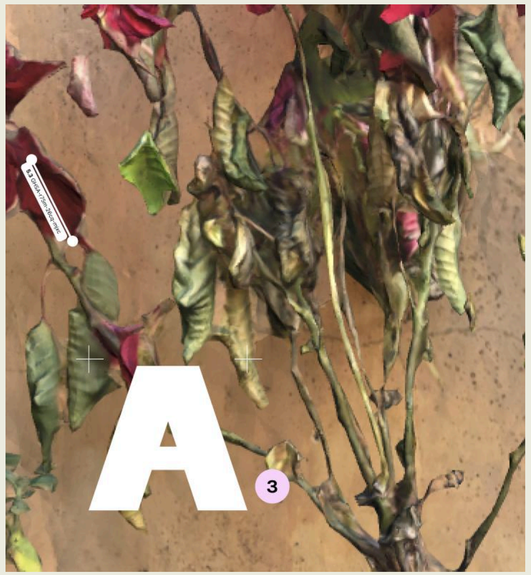
1

Interactive



2

Complex



3

Nature & Technology

Web-App

5

Nature 3D scans

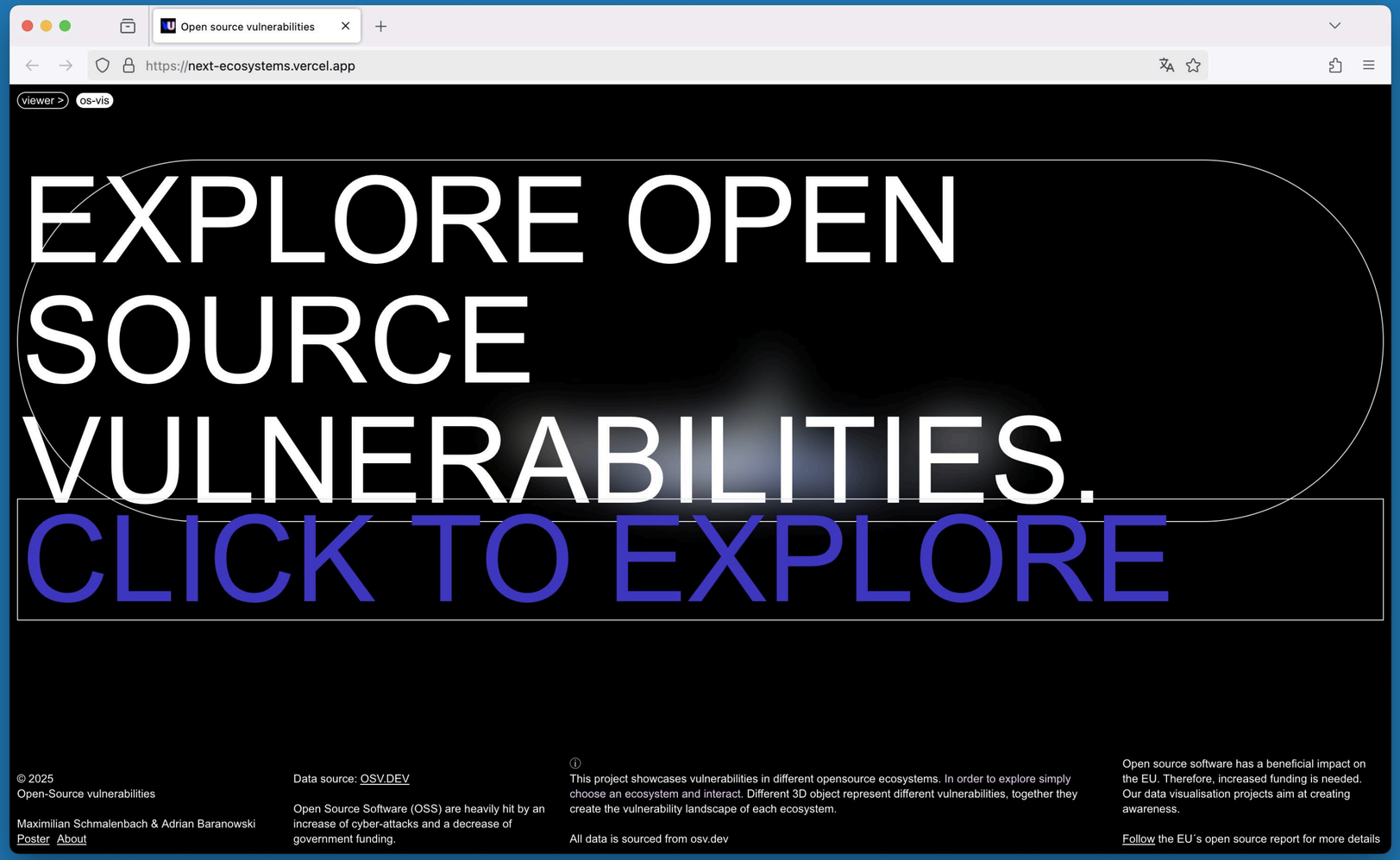
The 3D scans both found place in the webapp and the poster. Our goal was to show digitalized nature with usual errors in scanning. The visible bugs might remind of a inperfections in Open Source enviroments.

https://poly.cam/capture/409e4e80-513f-4c74-9a9b-093df0cb354e

https://poly.cam/capture/9ef0b601-468f-4878-b39e-0532dd5de9a0

https://poly.cam/capture/61f0b1b6-0540-4acf-a790-dc8a6c7860b9

https://poly.cam/capture/b46f6717-2062-4c84-8cf9-ef78abf5d5d0


Open source vulnerabilities
https://next-ecosystems.vercel.app
viewer >
os-vis
EXPLORE OPEN SOURCE VULNERABILITIES.
CLICK TO EXPLORE
© 2025
Open-Source vulnerabilities
Maximilian Schmalenbach & Adrian Baranowski
Poster About
Data source: OSV.DEV
Open Source Software (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.
This project showcases vulnerabilities in different opensource ecosystems. In order to explore simply choose an ecosystem and interact. Different 3D object represent different vulnerabilities, together they create the vulnerability landscape of each ecosystem.
All data is sourced from osv.dev
Open source software has a beneficial impact on the EU. Therefore, increased funding is needed. Our data visualisation projects aim at creating awareness.
Follow the EU´s open source report for more details

Open source vulnerabilities

https://next-ecosystems.vercel.app

viewer > os-vis

CLICK

THE OBJECT TO EXPLORE FURTHER.

Maximilian Schmalenbach & Adrian Baranowski

Poster About

Data source: OSV.DEV

Open Source Software (OSS) are heavily hit by an increase of cyber-attacks and a decrease of government funding.

ⓘ

This project showcases vulnerabilities in different opensource ecosystems. In order to explore simply choose an ecosystem and interact. Different 3D object represent different vulnerabilities, together they create the vulnerability landscape of each ecosystem.

All data is sourced from osv.dev

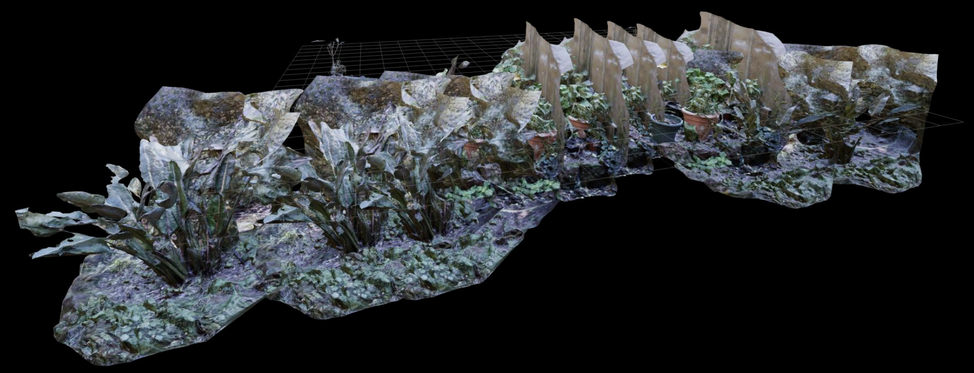
Open source software has a beneficial impact on the EU. Therefore, increased funding is needed. Our data visualisation projects aim at creating awareness.

Follow the EU´s open source report for more details

Open source vulnerabilities

https://next-ecosystems.vercel.app/viewer

< back os-vis GitHub Actions https://osv.dev



< prev

enable rotate

next >

Current Ecosystem: GitHub Actions

Timespan: 10/25/2022 - 11/25/2024
Vulnerabilities total: 0
https://github.com/features/actions

The following mapping visualises the ecosystems vulnerability data.

X-Axis: Date of documentation
Model-Type: Status & Severity
Size of the model & Z-Axis: Severity

Current vulnerability: GHSA-rg3q-prf8-qxmp
Description: Arbitrary command injection in embano1/wip

04/24/2023 Fix available
Severity: 8.8 (High)

1

Introduction

The user is met, with an **introductory page**. Here we learn about the **broad idea** of the website. Furthermore **sources** are linked. The user is then prompted to enter the second page, by simply clicking the text.

2

First Interaction

On the second page the user is introduced to one of our **3D models**. We want to push for a **first interaction** which is clicking the 3D model.
The goal is to introduce **familiarity**.

3

Dashboard

The Dashboard allows the user to fully **explore** all open source **ecosystems**, which have been tagged by OSV with vulnerability scores. We use both the **score and the date** of each vulnerability to **map** the data. The user can view **information** about one vulnerability by clicking its 3D model.

Please view on Desktop

INFORMATION DESIGN
STUDIO

UNIVERSITA
LA SAPIENZA

ADRIAN BARANOWSKI
MAX SCHMALENBACH

Thank you