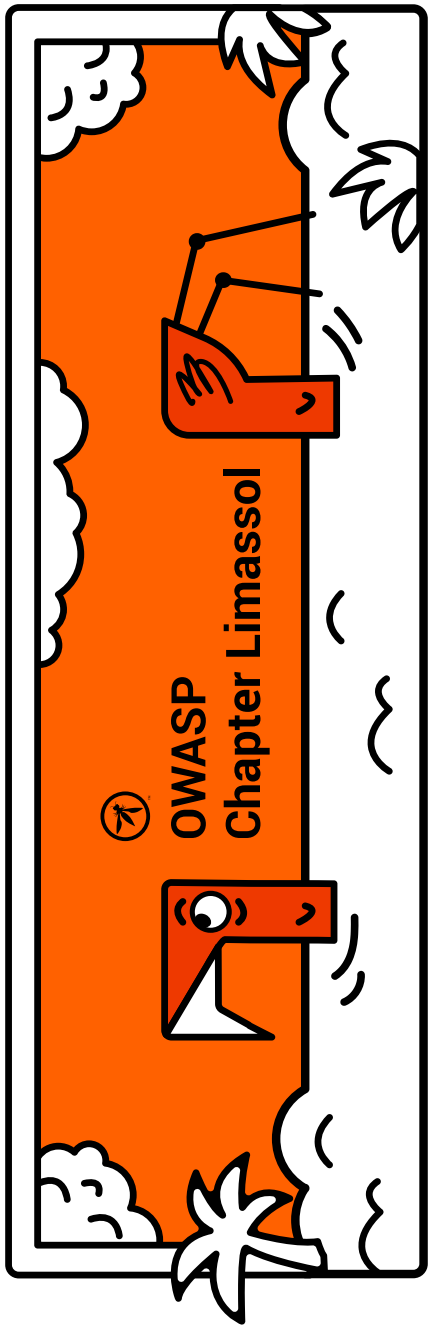


DHIS2: Building Security For An Open-Source Project

Michael Markevich
DHIS2 Security Lead

Who Am I

- Security lead for the DHI2 project, consultant, and academic lecturer
- Ex-CISO at Opera (Nasdaq:OPRA), Ulmart (defunct), and GGA (an EPAM company)
- Sysadmin, penetration tester, IT auditor, security manager (in prehistoric times)
- An OWASP member since 2016

What Are We Doing Here Today?

- Context: an overview of DHIS2
- Security in open-source: values, principles, and threats
- Our security organization at DHIS2
- Our tools and practices
- Q&A (if we have time)

DHIS2

An intro to the digital health world

What Is DHIS2?

DHIS2 (*District Health Information System, version 2*) is an open-source software for capture, management, and analysis of data.

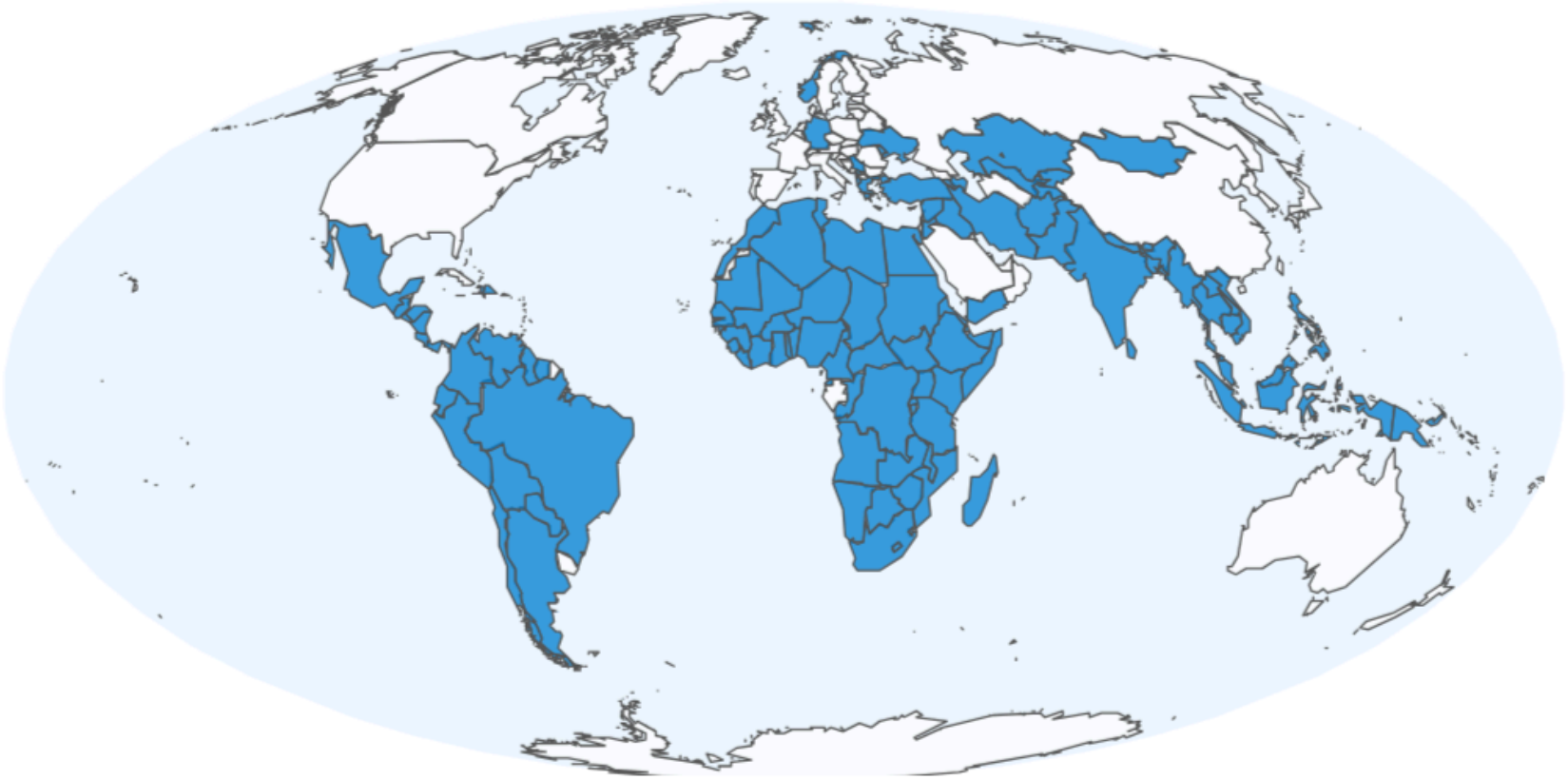
The software is used for statistical and reporting purposes, scientific research, and collecting and managing personal data records.

Supported data domains are health, education, logistics, and climate.

DHIS2 has been developed at the University of Oslo since 2008.

The Scale

DHIS2 runs on thousands of instances in 125 countries, processing data of 2.3 billion people.



Tech Facts

- Written in Java (backend) and JavaScript (frontend)
- Runs on Tomcat with PostgreSQL as a database
- Has a companion Android application (Tracker, 100K+ downloads on Google Play)
- 585K lines of (Java) code
- 280 stars on GitHub (https://github.com/dhis2)
- The latest major release happened two days ago

Our Team

- Headquartered in Oslo (but 100% remote)
- Has a board of sponsors (representatives of funding organizations)
- Has a board of project leads (for strategic and operational management)
- Team size: more than 110 (~70 of them software engineers)
- Security team: 3
- Security champions: 5

Public Goods

(and what they have to do with cyber)

Public Goods

A public good is a commodity or service provided without profit to all members of a society (either by the government or by a private individual or organization).

A public good is always:

- Non-excludable
- Non-rivalrous

Cybersecurity is a public good in an information society.

Digital Public Goods

Digital public goods are public goods in the form of software, data sets, AI models, standards or content that are generally free cultural works.

Many open-source software projects (including DHIS2) are recognized as digital public goods.

Back To Security

A deeper look at our security program

Threat Landscape

- Everyone can access and study (hack) the code
- We don't know (the majority of) our users
- Most of the deployments are not at the bleeding edge of technology
- Many deployments process high-risk data

Our Routine Things

- How do we identify users who don't have government-issued IDs?
- How can privacy consent be obtained from customers with low literacy?
- How should we make a mobile application work in areas without data network coverage?
- How can data be securely kept (or destroyed) in case of civil unrest or revolution?

Ethical Design

Ethical considerations can impact security design decisions.

For example, should we implement biometric authentication in DHIS2 or not?

Security Architecture

Maintaining a broad context when planning security features for the product is extremely important.

For example, should we implement identity management (or MDM, ...) functionality in DHIS2 or rely on external parties?

Privacy Design

How do we implement contradicting privacy requirements?

Example: cross-border data transfers

Security Principles

- Secure by default (ideally like OpenBSD)
- Adherence to open standards in software development (like OWASP)
- Reference deployment scenarios (standalone, LXC, Docker, Kubernetes)
- Capacity building (training for implementers)
- Transparency
- Community support

Our Processes

Vulnerability management:

- Avoid disclosure of security issues in public repositories
- Carefully coordinate disclosure timeline

Incident response:

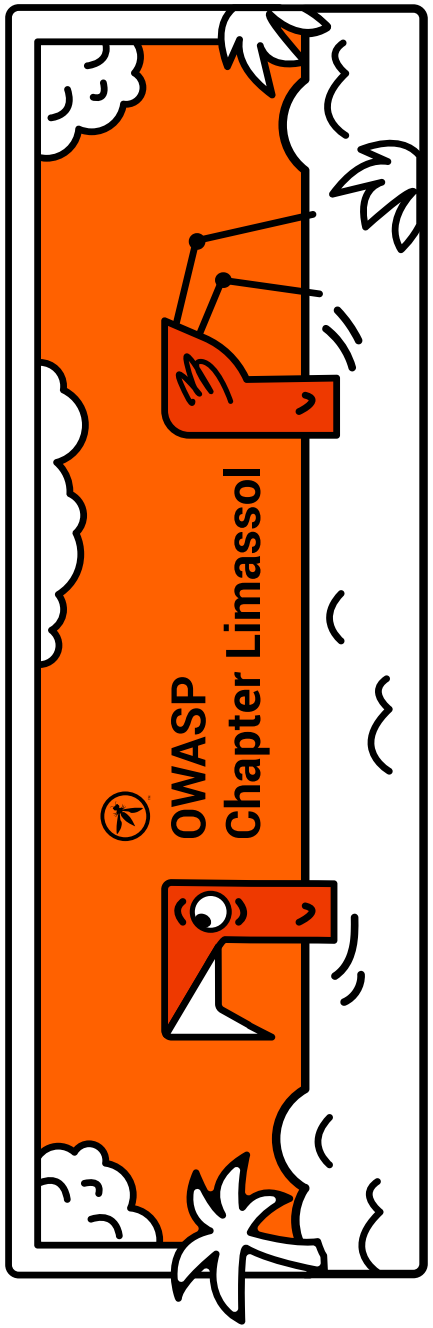
- We don't maintain any production systems
- We still have a moral responsibility and support implementers

Our Tools

- Github Dependabot (okay)
- Sonarqube (unhappy)
- Semgrep (happy)
- Schemathesis (still crashing)
- OWASP ZAP (happy)

Transparency

- Website pages explaining security features and trust policies
- Public Sonarqube dashboard
- Public security audit (with Cure53, still in progress)



Thank You

It's time for Q&A!