OSTIF

CELEBRATING 10 YEARS!

2025 Annual Report

Prepared by the **Open Source Technology Improvement Fund**

Improving Security Posture of Critical Open Source Projects

ostif.org

A NOTE FROM OUR DIRECTORS

It's hard to believe that 10 years ago, we started OSTIF with the intention of championing security efforts for critical open source projects.

Now we're making a meaningful impact on the ecosystem, driven by an international and expansive network of advocates, researchers, and maintainer communities.

We can't thank everyone enough who has supported OSTIF: whether collaborating directly on projects, advocating for and funding our work, or participating in meetups and providing feedback.

We hope that in the next 10 years, OSTIF can grow into a sustained organization and be seen as a key partner in improving the ecosystem.

Derek Zimmer, Executive Director

Amir Montazery, Managing Director

10 Years of Collaboration

By the Numbers: OSTIF's 2025

231

Findings with Security Impact

- 16 Crit/High (100% fixed)
- 34 Medium (100% fixed)
- 181 Low/Informational (80% fixed)

25

CVEs Found and Fixed

9

Projects Received Fuzzing Improvement

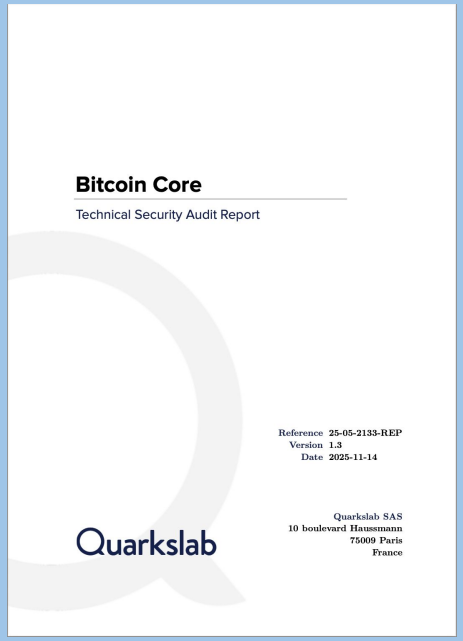
24

Security Audits Published

$2,800,000

for open source security

Audit Highlights



Bitcoin Core

Released November 2025

Funders: Brink, Chaincode Labs

Auditors: Quarkslab

Scope: Peer-to-Peer (P2P) interface and affected components: mempool management, block validation, transaction evaluation, chain state and peer management

Kubernetes

Releasing Q1 2026

Funder: CNCF

Auditors: Shielder

Scope: Popular non-core components

Our Reach

10 funding bodies

49

Projects benefited from direct security review

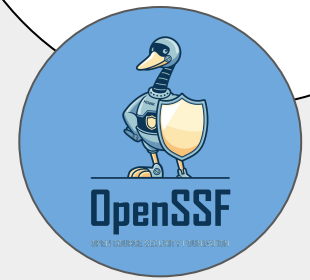
8

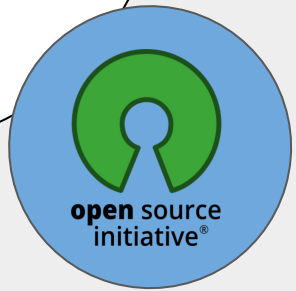
Firms executed security audits

Reaching Further

25 security engagements underway as of January 2026

Joined Memberships with OpenSSF and Open Policy Alliance





Security trends for 2026

- AI/LLMs
- Slop reports
- Light-touch security reviews
- Documentation review
- Legal risk evaluation
- Succession planning

Community

This year, we worked on developing our community through initiatives designed to offer education, opportunities, and security perspectives directly to and from open source communities.

OSTIF's **Advisory Council** leverages our relationships with other members of the cybersecurity community to benefit open source projects and better our business practices.

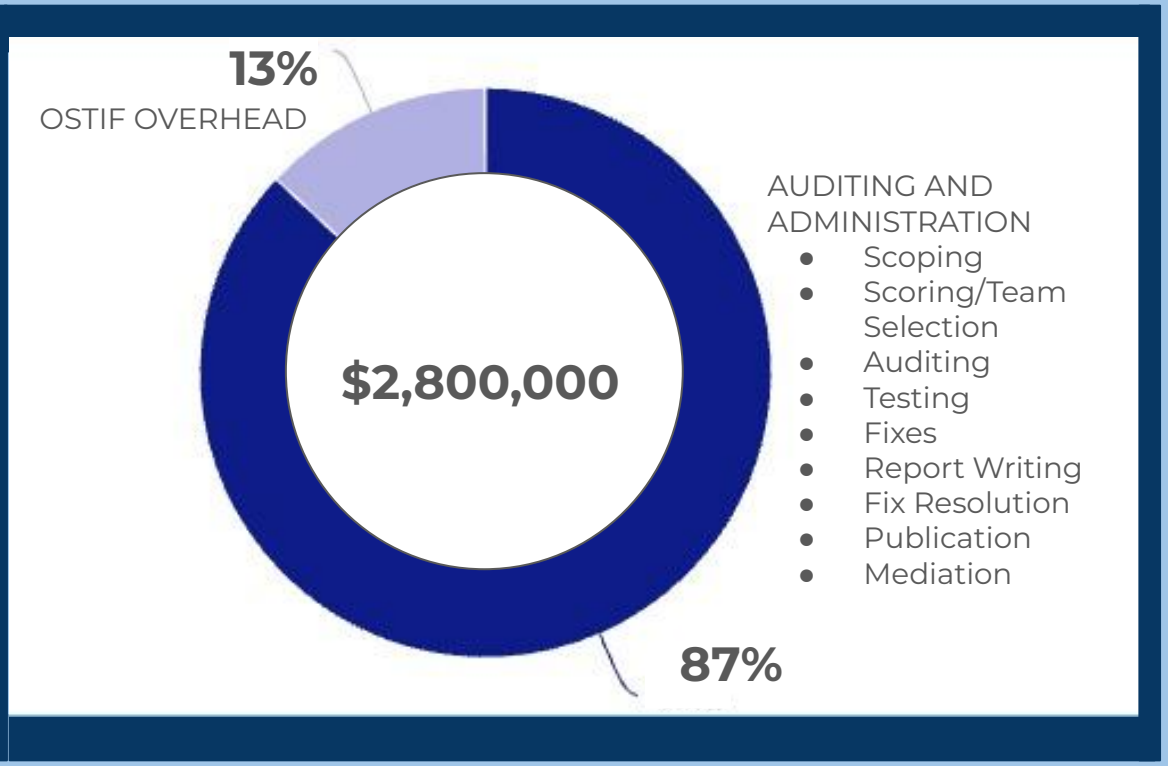
OSTIF **Meetups** are a hosted webinar series with the goal of offering open source security focused research and discussion. Join us by subscribing to our Meetup Calendar on lu.ma!

We love our community, and our **Community Spotlight** program introduces you to folks who are pivotal to the work of OSTIF and continued success of open source.

OSTIF Community Page

OSTIF Official Youtube

Annual Finances



2025 Audit Program Finance Ratio

OSTIF leverages industry knowledge, experience, and relationships to source world class security teams for competitive prices on behalf of open source.

OSTIF saves all parties involved labor, time, and money by utilising custom scoping, cost-splitting, follow-on work, and open source tooling.

Where OSTIF shines

Cost + quality controls

Access to our network of security expertise

Custom scoping and administration

High standard of transparency

FOSS, OSTIF, and You

Equally important is the chopping wood and carrying water of security work. Third-party code reviews continued apace. OSTIF completed audits this year of Karmada, Notary Project (cryptography), HickoryDNS, Linkerd, Logback, RSTUF, Scorecard, PHP, Istio ztunnel, NATS, nghttp3 and ngtcp2, Apache Log4Net and Log4CXX, Ruby on Rails, Volcano, conda-forge, PowSyBl, OpenEXR, and MaterialX, covering cloud native infrastructure, languages, build and packaging systems, and the media stack relied on by film and design. Looming ahead is more work on security for the

(above) **Linux Foundation Annual Report 2025**

(below) **Avoiding the Success Trap: Toward Policy for Open-Source Software as Infrastructure.**

ities, and plumbing. In the same way, much OSS finds itself incorporated into software projects, those projects into others, and over again through other projects maintainers, repository hosts like GitHub, private mirrors within companies, curators like Red Hat, auditors like the Open Source Technology Improvement Fund (OSTIF), transitive dependencies of other projects, and more before ever reaching a user.

and Pretschner, 2025). In this regard, it should be emphasized that the STA and OpenSSF are by no means the only funding bodies available for OSS projects today. In addition to so-called micro-donations and crowd-sourcing endeavors (Osborne et al., 2024; Tsakpinis and Pretschner, 2025), there are new funding initiatives for companies to support open source software projects (FCF, 2025; OSTIF, 2025), philanthropic programs (CZI, 2025; NLnet Foundation, 2025), and funding bodies that align with civil liberties (OTF, 2025). Given the overall funding landscape,

(above) **An Overview of Cyber Security Funding for Open Source Software**

OSTIF

CELEBRATING 10 YEARS!

We are a small team of friends from Chicago, Illinois, working together to preserve and protect global digital infrastructure in open source.

Are you interested in contributing to OSTIF's mission? Email us at contactus@ostif.org.

Previous Annual Reports: 2024, 2023, 2022