

Improving Security Posture of Critical Open Source Projects

Amir Montazery


Managing Director,
Open Source Technology
Improvement Fund, Inc
ostif.org

FrOSCon 2024
Sunday, 18 August 2024

finding vulnerabilities often requires **more in-depth auditing, logic review, and source code analysis**, in order to go **several layers deep**.

Source: https://www.rand.org/pubs/research_reports/RR1751.html





Thesis: Security Audits, when done to a high level of quality, are an incredibly valuable tool in the toolbelt for improving security posture of open source projects. OSTIF's body of work spanning 9 years, close to 100 security audits, close to 200 High or Medium vulnerabilities found and fixed (some of them nasty), supports this thesis.

Body of Work: <https://ostif.org/news/>

Common Types of Vulnerabilities Found

Top 5 Lessons Learned

4 Common Auditing Mistakes and How to Avoid Them

Bonus: Statistics on OSTIF's Security Audits

3 Common Types of Vulnerabilities Found

Source: <https://ostif.org/50th-audit-milestone/>

1. Denial of Service (DoS)

CWE-400 Uncontrolled Resource Consumption

2. Cross-Site Scripting/OS Command Injection

*CWE-78 Improper Neutralization of Special Elements used in an OS Command

*CWE-79 Improper Neutralization of Input During Web Page Generation

*CWE-20 Improper Input Validation

CWE-770 Allocation of Resources Without Limits or Throttling

3. Authorization

*CWE-502 Deserialization of Untrusted Data

*CWE-266 Privilege Escalation

* Mapped to most recent [OWASP Top 10](#)



Top 5 Lessons Learned From 50 Audits

Source: <https://ostif.org/50th-audit-milestone/>

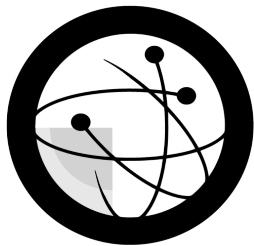
1. Importance of Clarity and Communication
2. Success correlates with Scoping
3. Interest & Collaboration
4. Balance of Testing Types
5. Resolution is Pivotal

The Top 4 Common Audit Mistakes and How to Avoid Them

Source: <https://ostif.org/50th-audit-milestone/>

1. **Focus on the Bid, not the Bidder**
2. **Lack of Communication**
3. **Only Using Automated Tooling**
4. **Proper Scoping**





Bonus: Statistics From OSTIF's Security Audits

100 # Of Projects Completed, In Progress, or in the Pipeline

257 # High or Medium Severity Findings Fixed

26 # Of Types of Common Weakness Enumerations (CWEs) Fixed for Projects

214 # Fuzzers Built For Continually Monitoring OSS Projects

Approx. Average Cost Per Engagement \$74,000

Approx. Average cost per bug fix/tool implementation \$6,592

Almost every Security Audit has a Threat Model, Static and Dynamic Analysis Tool Integration, Fuzzing Integration, and vulnerabilities found and fixed.

finding vulnerabilities often requires **more in-depth auditing, logic review, and source code analysis**, in order to go **several layers deep**.

Source: https://www.rand.org/pubs/research_reports/RR1751.html



Strong Audit Experts

Individuals and Teams who are well-versed in open-source security and finding vulnerabilities in the field they are reviewing



Project Engagement and Involvement

Maintainers - Coordinating fixes and disclosure

A Champion - Independent Organization

An entity to manage and facilitate the audit process

Call to Action

- check out our body of work and how we've helped open source projects improve security.
- talk to your network about open source security audits and how they can help open source projects you care about.
- let us know if you have questions or if we can help!

Thank You!

<https://ostif.org>

<https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md>