Open Source Software as Underfinanced Critical Infrastructure

Christian Folini

Bio: Christian Folini

- Swiss Security engineer with 20 years of experience
- Web Application Firewall specialist
- Ex-Lead OWASP CRS
- Program Chair Swiss Cyber Storm Conference
- Steering Committee
  Swiss National Cyber Strategy (NCS)
- Official moderator of a national dialogue on digitalization of political rights

Agenda

- Financial situation of open source software projects
- Example OWASP CRS
- OSS and AI
- Global infrastructure impact
- Call to action

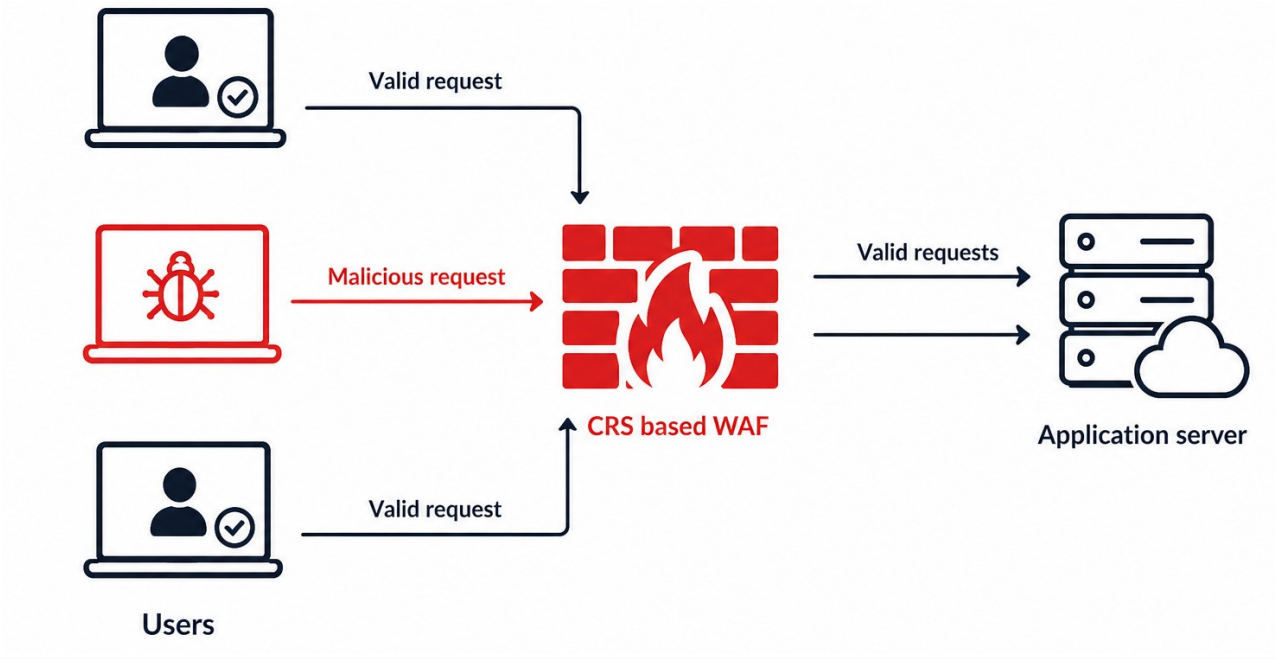
The Financial Situation of OSS

- OSS projects typically operate on a shoestring budget
- Self exploitation is the norm
- Calls for contributions or sponsoring often go unanswered
- Big OSS foundations are able to ease the pain

  (at least for the biggest players)

What is a WAF

- Filters traffic by inspecting HTTP payloads
- Protects backend applications from attacks



What is OWASP CRS

- Generic deny-list WAF rule set
- Protects against OWASP Top Ten
- Open source licensed

  (Apache license, allows for commercial usage)
- Runs on ModSecurity compatible engines

How do the rules looks like?

```
SecRule REQUEST_COOKIES|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx (?i)(?:b["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?u["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?s["'\)\[
x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?y["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?b["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?o["'\)\[\x5c]*(?:(?:(?:\|
||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?x|(?:c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?o["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?m["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b
]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?m["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?a["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?n["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-
9\?@_a-\{]*)?\x5c?d|e["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:n["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?v|v["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]
*)?\x5c?a["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?l)|w["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?a["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t["'\)
)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?h)["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?[\s\x0b&\),<>\|].*[ls
]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?r["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?a["'\)\[\x5c]*(?
:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?e|n["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?o["'\)\[\x5c]*(?:(?:(?:\|\||&&)
[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?h["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?u["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?p|t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!
#\(\*\-0-9\?@_a-\{]*)?\x5c?t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?m["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?e["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-
{]*)?\x5c?(?:[\s\x0b&\),<>\|].*|o["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?u["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t)|[\n\r;=`\{]|\||?|&&?|\$(?:\(\(?|[\(\{])|<(?:\(|<<)|>\(|
\([\s\x0b]*\))[\s\x0b]*(?:[\$\{]|(?:[\s\x0b]*\(|!)[\s\x0b]*|[0-9A-Z_a-z]+=(?:[^\s\x0b]*|\$(?:.*|.*)|[<>].*|'[^']*'|\"[^\"]*\"|[\s\x0b]+)*[\s\x0b]*["']*(?:["'`-\+\--9\?A-\]_a-z\]]+/)?["'\)\x5c]*(?:(?:7["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]
*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?z["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:[arx]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?)?|(?:b["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\
$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?z["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?z|c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:[89]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*
-0-9\?@_a-\{]*)?\x5c?9|m["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?p|s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?h)|d["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-
{]*)?\x5c?(?:n["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?)?f|e["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:n["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\
x5c?v|q["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?n|s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?h)|f["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:g|m
["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t)h|b["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?u["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?p|i["'\)\[\x5c
]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?r["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?b|j["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:j["'\)\[\x5c]*(?:(?:(?:\
|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?s|q)|[kz]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?h|m["'\)\[\x5c]*(?:(?:(?:\|\||&&)
[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?r|p["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:d["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\
$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?b|(?:k["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?)?g|t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?x|w["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(
\*\-0-9\?@_a-\{]*)?\x5c?d|x["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?z)|r["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?
@_a-\{]*)?\x5c?p|m["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?t)|s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)
?\x5c?p|e["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?d|(?:s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?)?h|v["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?x|
n)|t["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:a["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?c|b["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?l)|w["'\)
)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:3["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?m|c)|x["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:x["'\)\[\x5c]
c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?d|z)|y["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?u["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?m)["'\)\[\x5c]*(?:(?:(?
:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?|l["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:s["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?|z["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s
\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:4["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?)?))[\s\x0b&\),<>\|].*|a["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:a["'\)\[\x5c]*(?:(?:(?
:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?-["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:[&\),<>\|]{1,10}|(?:[\-\.0-9A-Z_a-z]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?){
1,10}[\s\x0b&\),<>\|\}]{1,10})|r["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?j["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?[\s\x0b&\),<>\|].*)|g["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]
*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?c["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?(?:[&\),<>\|]{1,10}|(?:[\-\.0-9A-Z_a-z]["'\)\[\x5c]*(
?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?){1,10}[\s\x0b&\),<>\|\}]{1,10})|(?:d["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?b|[hr]["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]
*)?\x5c?c|p["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?g)["'\)\[\x5c]*(?:(?:(?:\|\||&&)[\s\x0b]*)?\$[!#\(\*\-0-9\?@_a-\{]*)?\x5c?[\s\x0b&\),<>\|].*))\b" \
```

Who uses OWASP CRS

- No generic open source alternative
- Base for approx. 2/3 of commercial WAFs
- Among others, OWASP CRS is sold by
  - **Google (GOLD sponsor! Thank you.)**
  - Azure (Short time sponsor until they ran out of money)
  - Cloudflare (”We don't do sponsoring”)
  - Akamai (Refuses every contact)
  - HAProxy Enterprise (Stopped responding)
  - etc.

CRS Conclusion

- OWASP CRS is critical infrastructure
- Dominant rule set in the market
- Only 8-10 active developers
- Approximately $60K annual budget
  - Used for developer retreats and to provide free 1st level support

OSS and AI

- 2025: surge in poor AI issues
- 2026: high quality AI pull requests emerging

- The LLMs become more powerful
- The agentic AI and its harnessing makes it even more powerful
- The prompts have become very simple, democratization of security research

- Amount of AI discovered bug explodes

Modern use of AI at CRS

- AI to detect rule bypasses
- AI for triage
- AI-assisted rule generation
- AI code review and acceptance tests

Other struggling projects

- cURL is limiting triage
- Ghostty is restricting submissions
- tldraw has closed submissions for non-devs
- GitHub allows for projects to block submissions

  (blocking submissions effectively closes the recruitment pipeline for an open source project)

Effects on projects

- Mental load increasing
- Developer burnout
- Review bottlenecks getting worse
- Risk of malicious contributors easing into projects growing

Global Infrastructure Risk

- Inventories are incomplete or stop at 2nd level

  (OSS dependencies are ignored despite general abundance)
- Critical part of supply chain is underfunded
- AI increases attack pressure
- Weak links threaten security of entire systems
- Meanwhile: Commercial integrators ignore the calls

Call to action

- Policies that support the financing of critical OSS projects
- Infrastructure to allow financing of critical OSS more easily
- Businesses must support their supply chain for long term sustainability
- Need to implement CRA with leverage for OSS

Q&A

Contact

- christian.folini@netnea.com
- https://christian-folini.ch
- https://www.linkedin.com/in/christian-folini-588ba278
- https://bsky.app/profile/christian-folini.ch