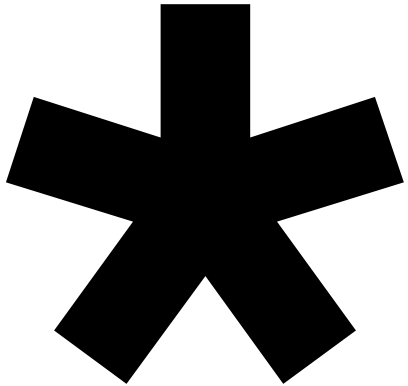
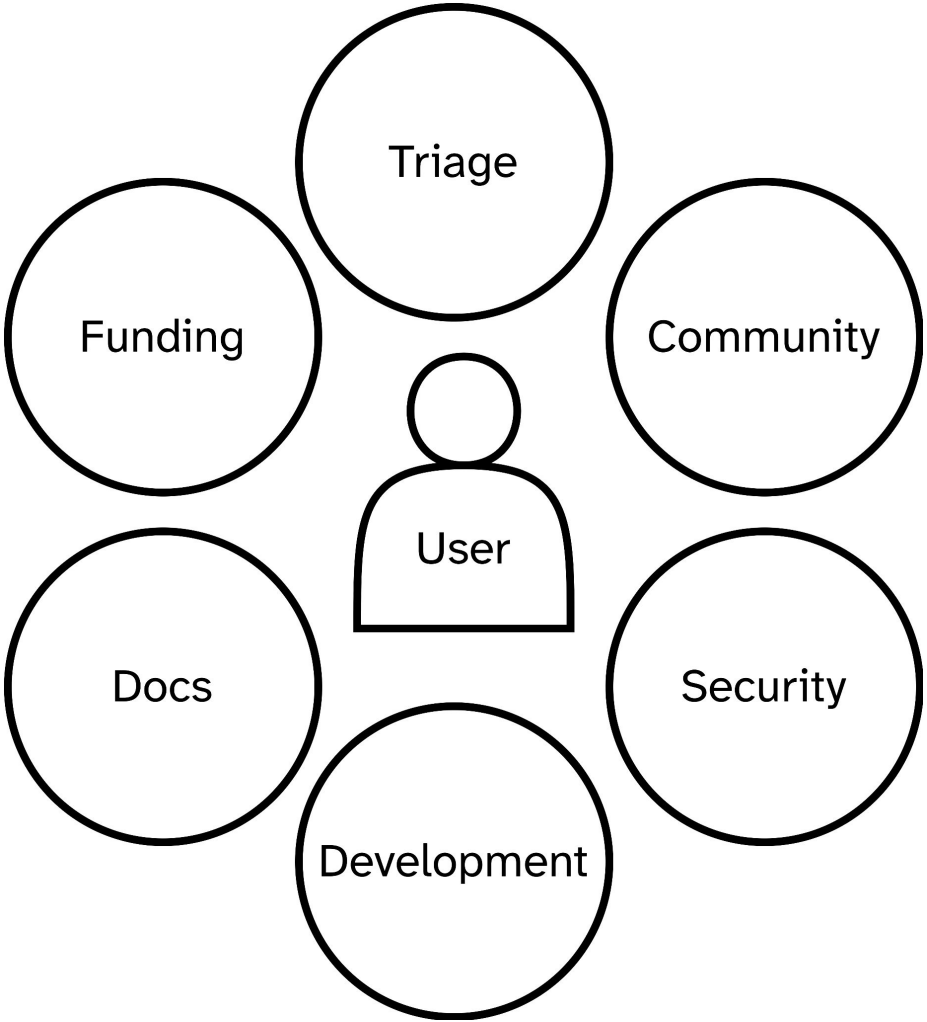
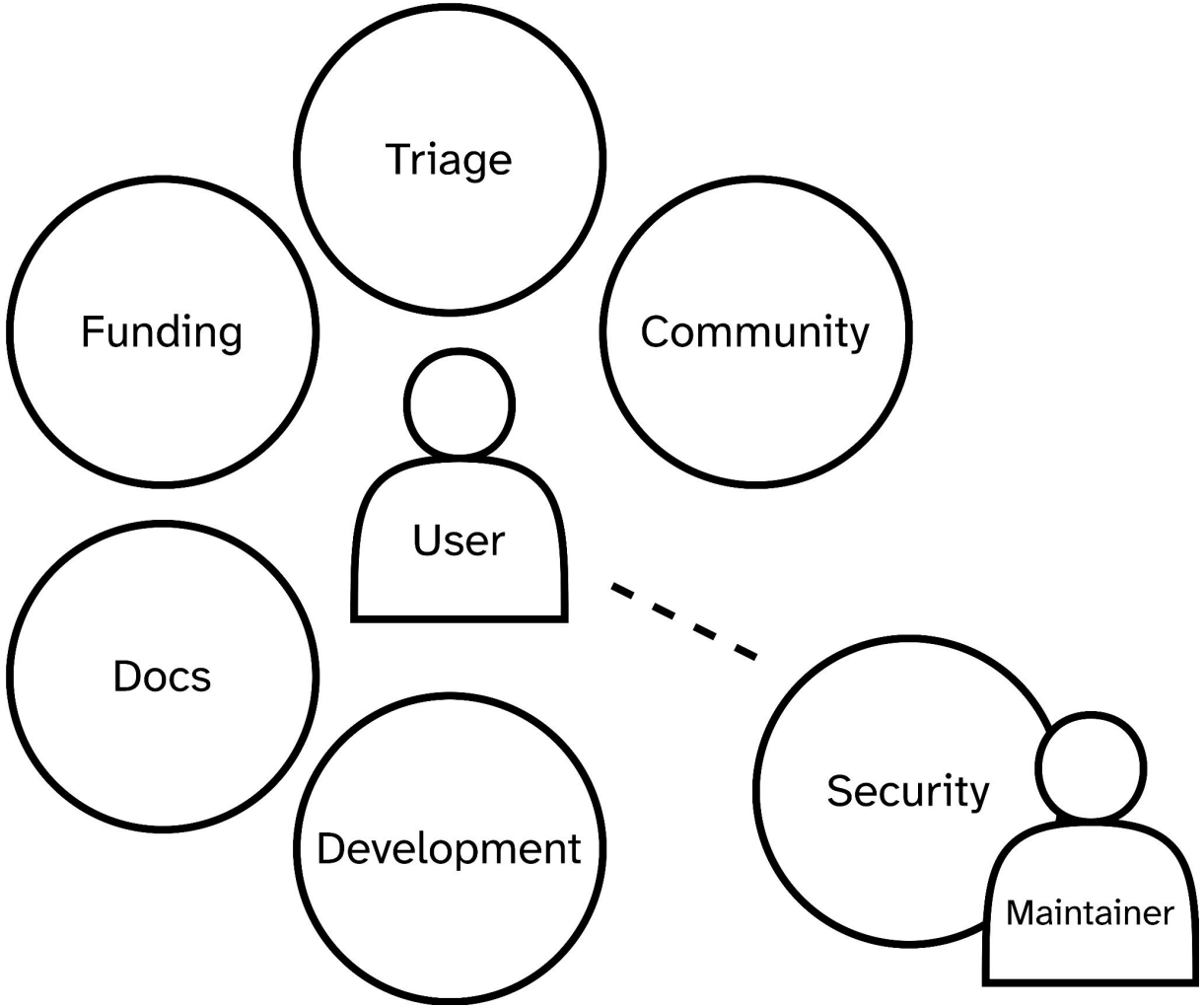
Security work isn't "special".

sethmlarson.dev
sethmlarson@mastodon.social




Triage
Funding
Community
User
Docs
Security
Development


Triage
Funding
Community
User
Docs
Development
Security
Maintainer

DEC 1, 2024

Marcelo Trylesinski (He/Him) • 9:09 AM

Seth

Can I ask your help for a security advisory in Starlette?

Seth Michael Larson (He/Him) • 3:35 PM

Of course, you can add me to the GHSA if you'd like otherwise happy to chat here.

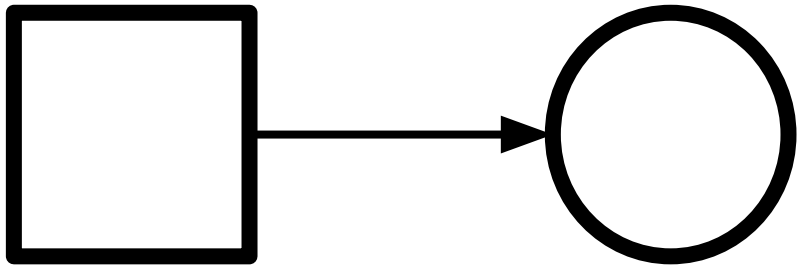
DEC 2, 2024

Marcelo Trylesinski (He/Him) • 12:30

I've invited you. Thanks! :)

Isolation

Smaller projects are *shaped by tools*



Findings, not fixes

```
 __  __            _
 ___\ \/ /_ __   __ _| |_
/ _ \\  /| '_ \ / _` | __|
|  __//  \| |_) | (_| | |_
 \___/_/\_\ .__/ \__,_|\__|
           |_| XML parser
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! <blink>Expat is UNDERSTAFFED and WITHOUT FUNDING.</blink>                !!
!!                ~~~~~~~~~~~~                                              !!
!! The following topics need *additional skilled C developers* to progress  !!
!! in a timely manner or at all (loosely ordered by descending priority):   !!
!!                                                                          !!
!! - teaming up on researching and fixing future security reports and       !!
!!   ClusterFuzz findings with few-days-max response times in communication !!
!!   in order to (1) have a sound fix ready before the end of a 90 days     !!
```

Redefining
“Security Contributions”

Message-ID: <20240329155126.kjjfduxw2yrl
Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma

Trust?

Hi,

After observing a few odd symptoms around liblzma (part of the xz packa
Debian sid installations over the last weeks (logins with ssh taking a
CPU, valgrind errors) I figured out the answer:

If we want sustainability...

XZ-utils cannot define Open Source Security

“You’re not alone!”

Removing maintainers from open source projects

Published 2024-01-23 by Seth Larson
★ Reading time: 3 minutes ♥ × 53

Here's a tough but common situation for open source maintainers:

- You want a project you co-maintain to be more secure by reducing the attack surface.
- There are one or more folks in privileged roles who *previously were active contributors*, but now aren't active.
- You don't want to take away from or

New era of slop security reports for open source

Published 2024-12-03 by Seth Larson
★ Reading time: 5 minutes ♥ × 172

I'm on the security report triage team for CPython, pip, urllib3, Requests, and a handful of other open source projects. I'm also in a trusted position such that I get "tagged in" to other open source projects to help others when they need help with security.

Recently I've noticed an uptick in extremely low-quality, spammy, and LLM-hallucinated security reports to open source projects. The

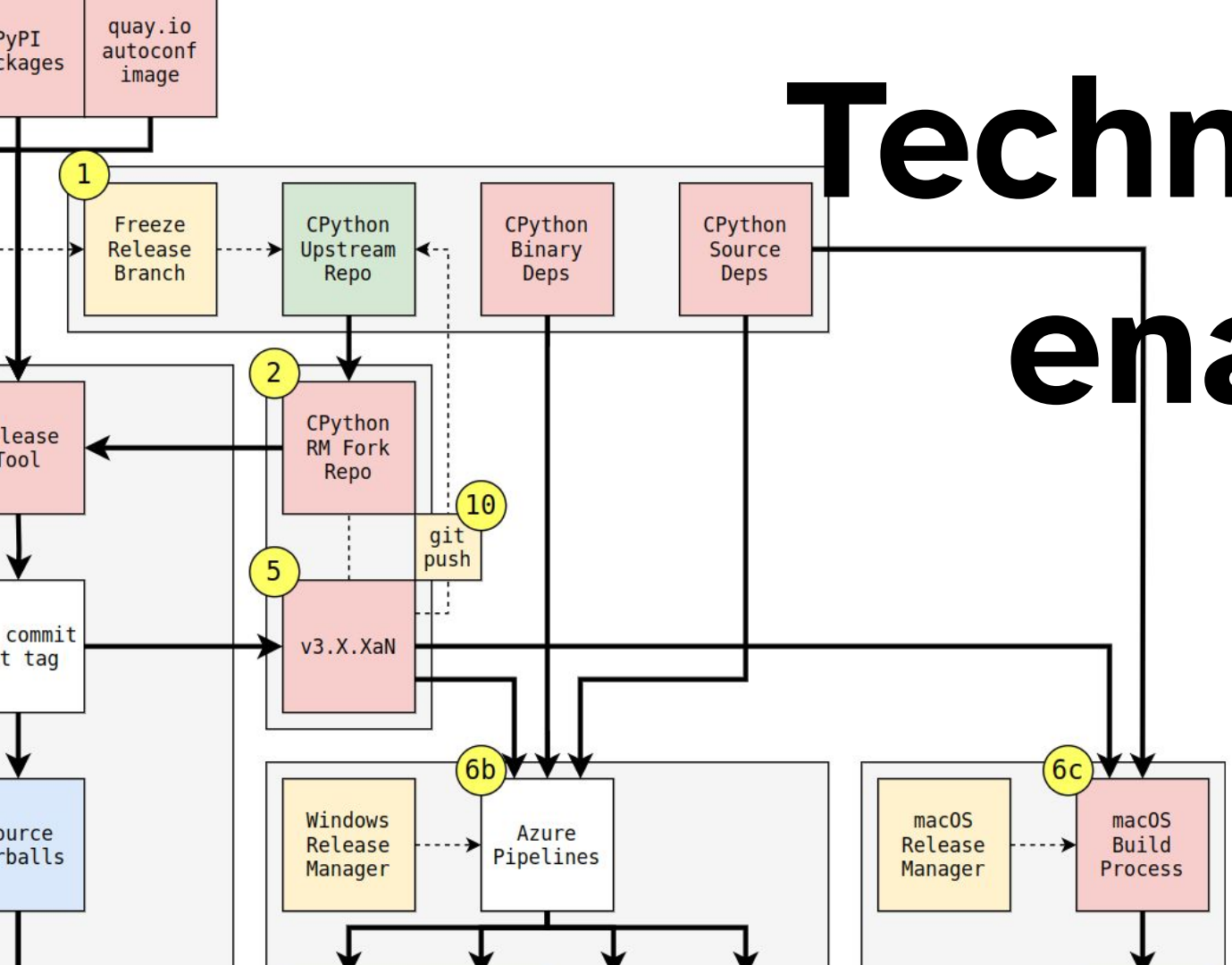
Regex character “$” doesn't mean “end-of-string”

Published 2024-03-09 by Seth Larson
★ Reading time: 1 minute ♥ × 45

This article is about a bit of surprising behavior I recently discovered using Python's regex module (`re`) while developing SBOM tooling for CPython.

Folks who've worked with regular expressions before might know about `^` meaning "start-of-string" and correspondingly see `$` as "end-of-string". So the pattern `cat$` would match the string

Trusted Environments



Technology enabling Trust

“Securing” does not have to mean “maintaining”

Security work isn't special...

Trust is. ❤