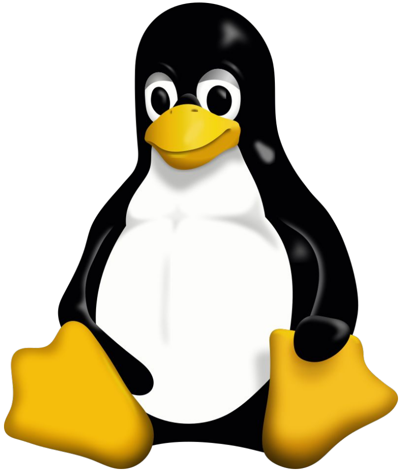
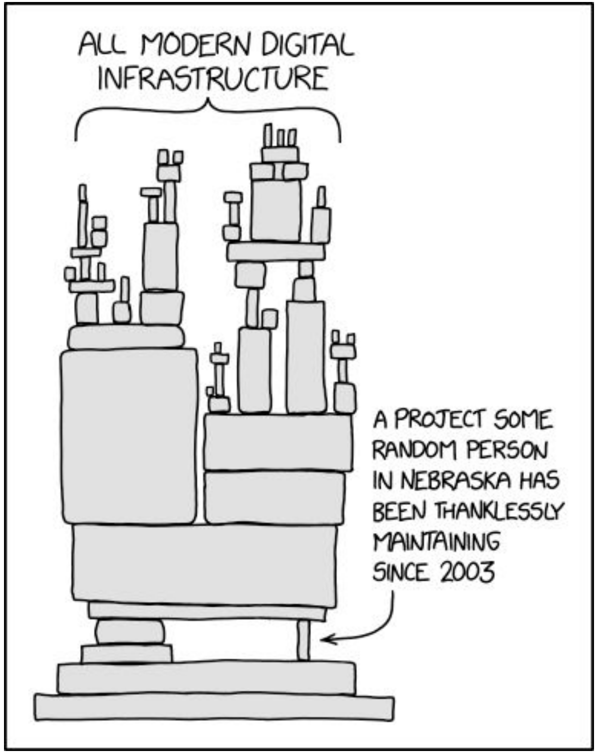
Contributing to the security of open source projects

Santos - @stsewd

Open source



Open source


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Mistakes happen

Open source projects

- GitPython
- django-impersonate
- django-gravatar2
- django-allauth

Open source projects that I use at my work

- GitPython
- django-impersonate
- django-gravatar2
- django-allauth

Most common vulnerabilities

- https://cheatsheetseries.owasp.org/IndexTopTen.html
- https://snyk.io/blog/python-security-best-practices-cheat-sheet/
- https://snyk.io/reports/open-source-security/

Choose a project

```
$ cat requirements.txt
```

READ THE CODE

Responsibly reporting vulnerabilities

https://github.blog/2022-02-09-coordinated-vulnerability-disclosure-cvd-open-source-projects/

Tools

- Bandit (https://bandit.readthedocs.io/en/latest/)
- CodeQL (https://codeql.github.com/)

Conclusion

Read the code. The worst thing that can happen is that you learn something new.

https://stsewd.dev/talks/djangocon-2024.pdf

Santos - @stsewd