
VERACODE
Reviewing 3rd Party Library Security Easily Using OpenSSF Scorecard
Niels Tanis
Sr. Principal Security Researcher
WeAreDevelopers
World Congress

Who am I?

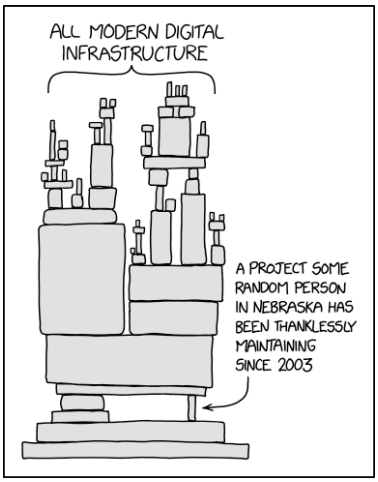
- Niels Tanis
- Sr. Principal Security Researcher
  - Background .NET Development, Pentesting/ethical hacking, and software security consultancy
  - Research on static analysis for .NET apps
  - Enjoying Rust!
- Microsoft MVP – Developer Technologies

VERACODE

MVP Microsoft® Most Valuable Professional

@nielstanis@infosec.exchange

Modern Application Architecture
XKCD 2347



@nielstanis@infosec.exchange

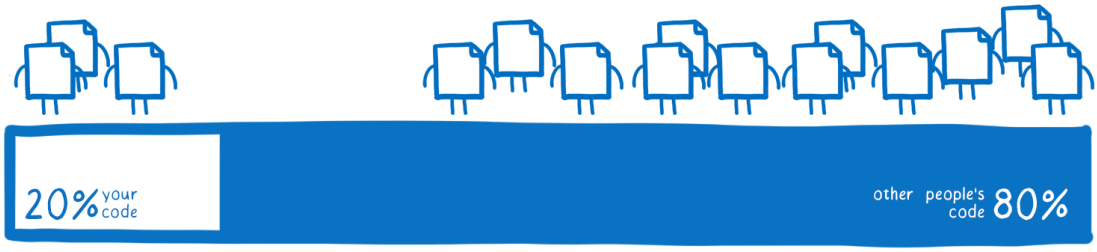
https://xkcd.com/2347/

Agenda

- Risks in 3rd Party Packages
- OpenSFF Scorecard
- Measure, New & Improved
- Conclusion - Q&A

@nielstanis@infosec.exchange

Average codebase composition

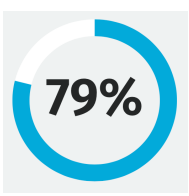


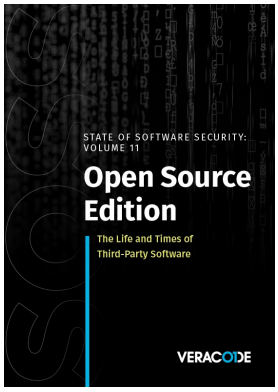
@nielstanis@infosec.exchange

https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/

State of Software Security v11

”Despite this dynamic landscape, 79 percent of the time, developers never update third-party libraries after including them in a codebase.”





@nielstanis@infosec.exchange

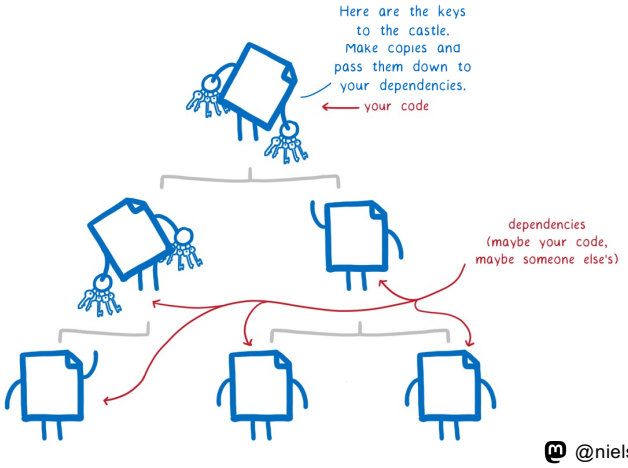
State of Log4j – 2 years later

- Analysed our data August-November 2023
  - Total set of almost 39K unique applications scanned
- 2.8% run version vulnerable to Log4Shell
- 3.8% run version patched but vulnerable to other CVE
- 32% rely on a version that's end-of-life and have no support for any patches.

@nielstanis@infosec.exchange

https://www.veracode.com/blog/research/state-log4j-vulnerabilities-how-much-did-log4shell-change

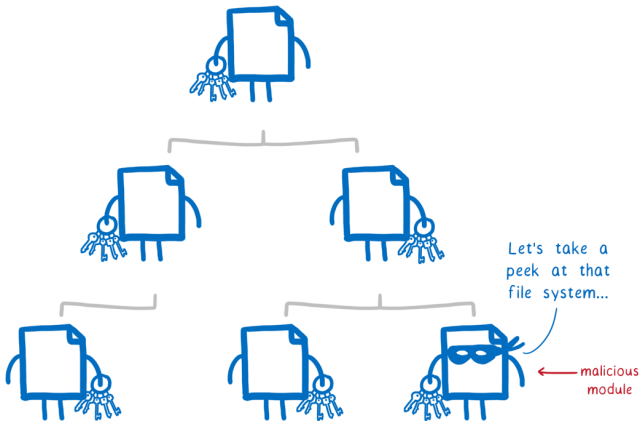
Average codebase composition



@nielstanis@infosec.exchange

https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/

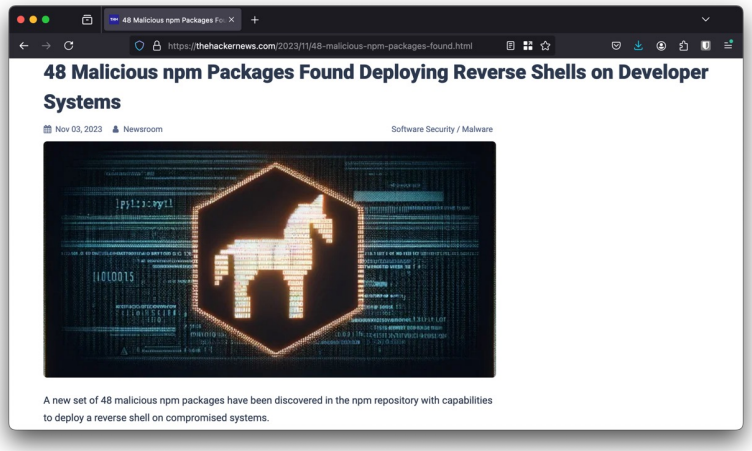
Malicious Library



@nielstanis@infosec.exchange

https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/

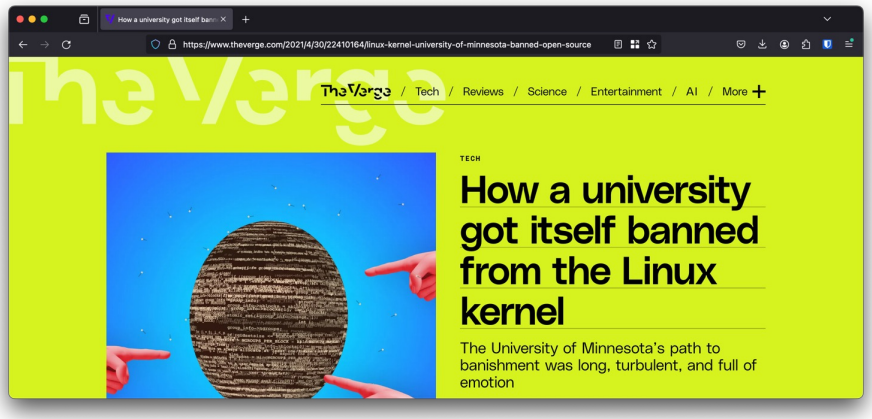
Malicious Package



@nielstanis@infosec.exchange

https://thehackernews.com/2023/11/48-malicious-npm-packages-found.html

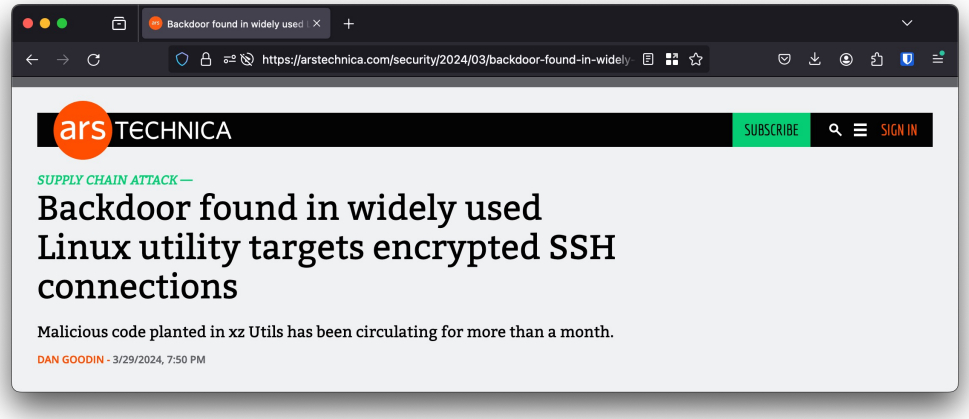
Hypocrite Commits



@nielstanis@infosec.exchange

https://www.theverge.com/2021/4/30/22410164/linux-kernel-university-of-minnesota-banned-open-source

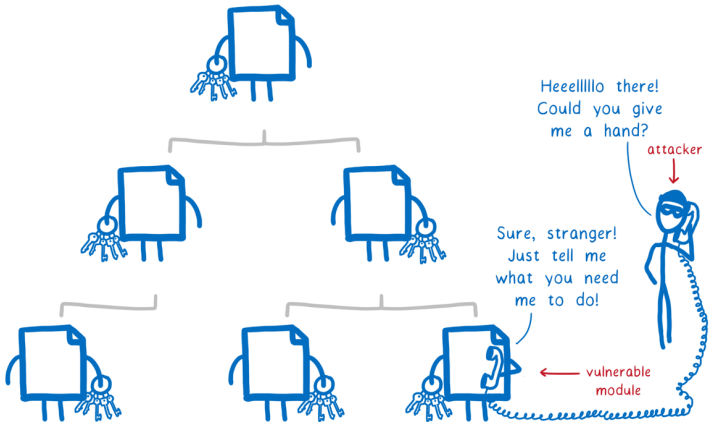
XZ Backdoor



@nielstanis@infosec.exchange

https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/

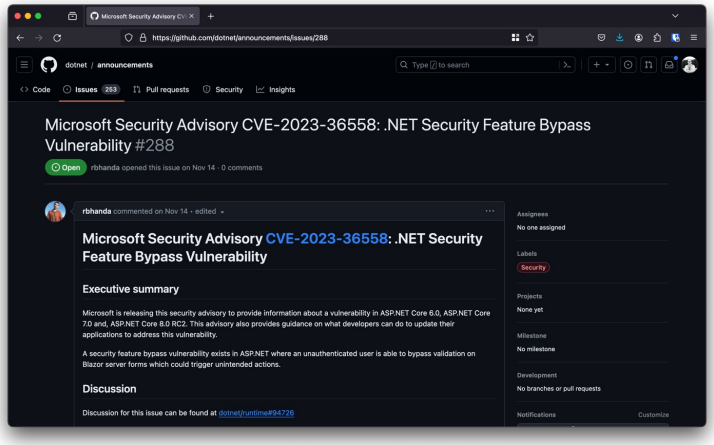
Vulnerable Package



@nielstanis@infosec.exchange

https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/

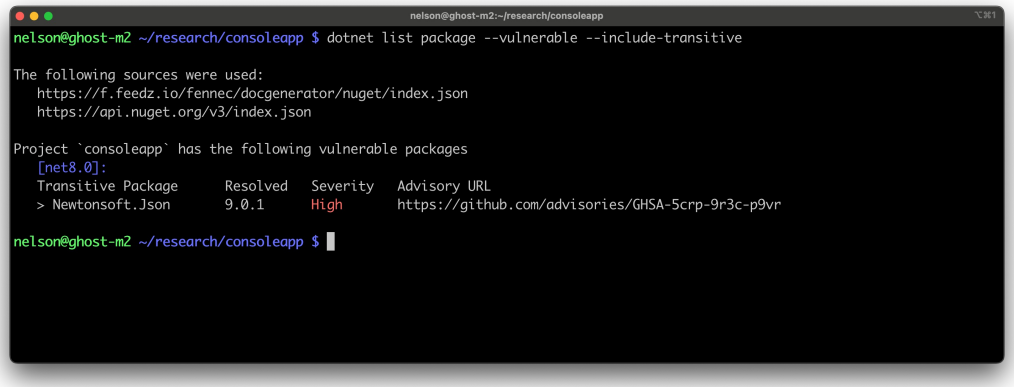
Vulnerabilities in Libraries



@nielstanis@infosec.exchange

https://github.com/dotnet/announcements/issues/288

DotNet CLI



@nielstanis@infosec.exchange

NPM Audit

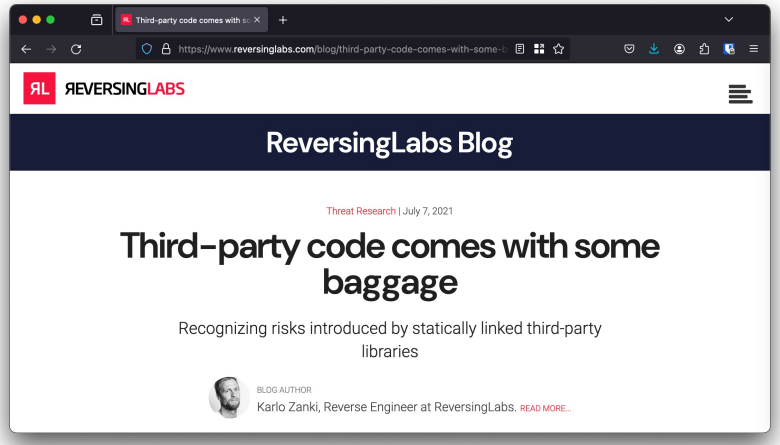
```
                    === npm audit security report ===

# Run  npm install chokidar@2.0.3  to resolve 1 vulnerability
SEMVER WARNING: Recommended action is a potentially breaking change
```

Low	**Prototype Pollution**
Package	deep-extend
Dependency of	chokidar
Path	chokidar > fsevents > node-pre-gyp > rc > deep-extend
More info	https://nodesecurity.io/advisories/612

@nielstanis@infosec.exchange

Do you know what's inside?



@nielstanis@infosec.exchange

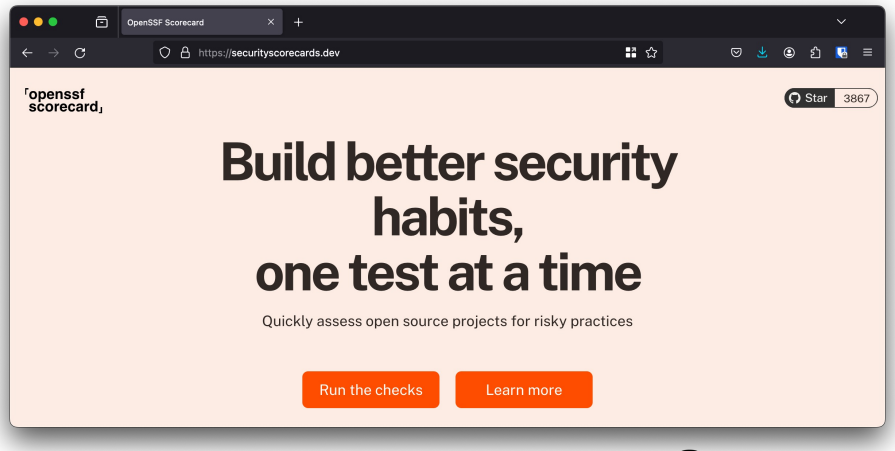
https://www.reversinglabs.com/blog/third-party-code-comes-with-some-baggage

Nutrion Label for Software?

@nielstanis@infosec.exchange

https://securityscorecards.dev/

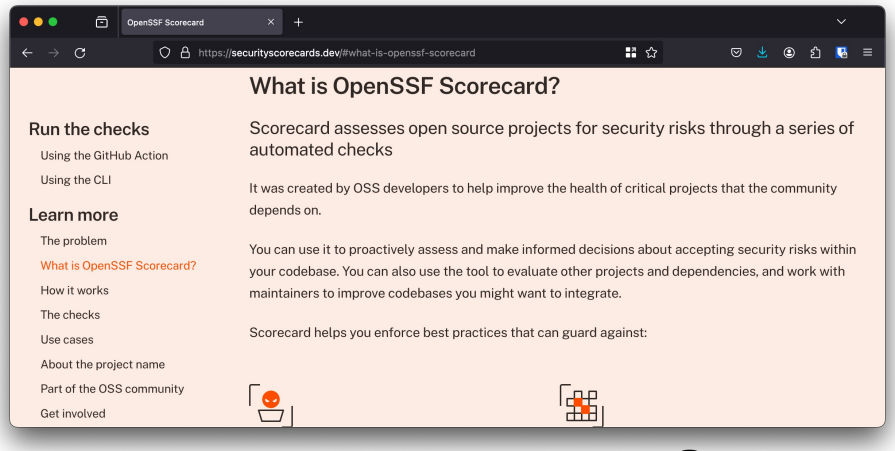
OpenSSF Scorecards



@nielstanis@infosec.exchange

https://securityscorecards.dev/

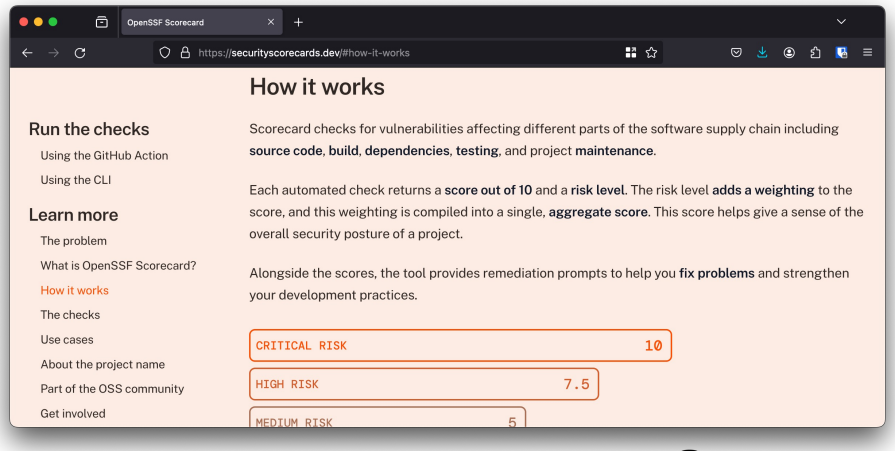
OpenSSF Security Scorecards



@nielstanis@infosec.exchange

https://securityscorecards.dev/

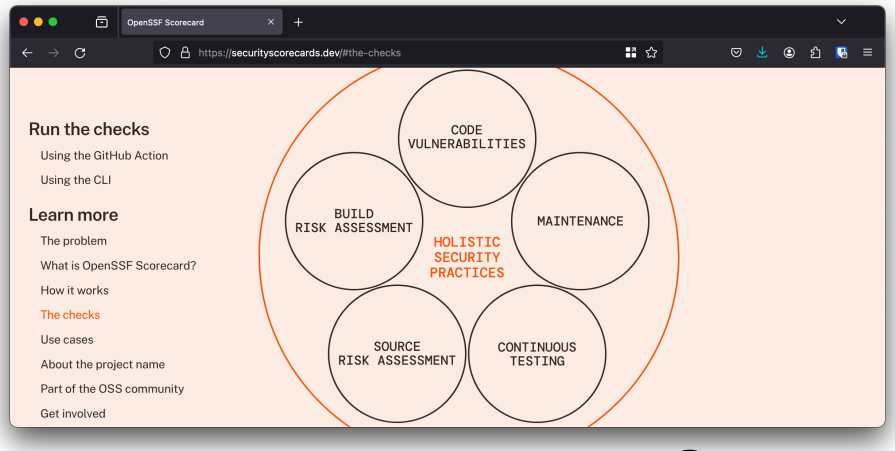
OpenSSF Security Scorecards



@nielstanis@infosec.exchange

https://securityscorecards.dev/

OpenSSF Security Scorecards

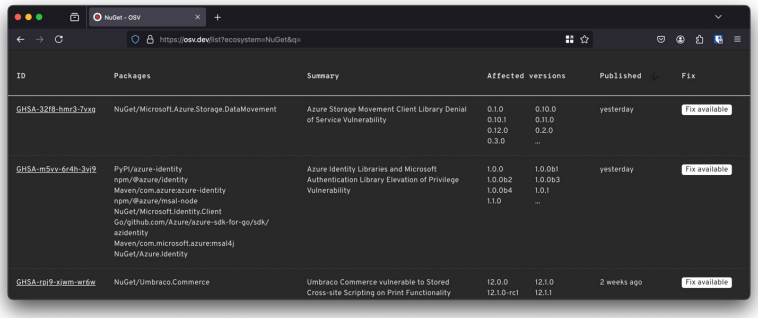


@nielstanis@infosec.exchange

https://securityscorecards.dev/

Code Vulnerabilities (High)

- Does the project have unfixed vulnerabilities? Uses the OSV service.



@nielstanis@infosec.exchange

https://osv.dev/list?ecosystem=NuGet

Maintenance
Dependency-Update-Tool (High)

- Does the project use a dependency update tool? For example Dependabot or Renovate bot?
- Out-of-date dependencies make a project vulnerable to known flaws and prone to attacks.

@nielstanis@infosec.exchange

Maintenance
Security Policy (Medium)

- Does project have published security policy?
- E.g. a file named **`SECURITY.md`** (case-insensitive) in a few well-known directories.
- A security policy can give users information about what constitutes a vulnerability and how to report one securely so that information about a bug is not publicly visible.

@nielstanis@infosec.exchange

Maintenance
License (Low)

- Does project have license published?
- A license can give users information about how the source code may or may not be used.
- The lack of a license will impede any kind of security review or audit and creates a legal risk for potential users.

@nielstanis@infosec.exchange

Maintenance
CII Best Practices (Low)

- OpenSSF Best Practices Badge Program
- Way for Open Source Software projects to show that they follow best practices.
- Projects can voluntarily self-certify, at no cost, by using this web application to explain how they follow each best practice.

@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

Continuous testing
CI Tests (Low)

- Does the project run tests before pull requests are merged?
- The check works by looking for a set of CI-system names in GitHub CheckRuns and Statuses among the recent commits (~30).

@nielstanis@infosec.exchange

Continuous testing
Fuzzing (Medium)

- This check tries to determine if the project uses fuzzing by checking:
  - Added to OSS-Fuzz project.
  - If ClusterFuzzLite is deployed in the repository;
- Does it make sense to do fuzzing on managed languages like Java and/or .NET?

Continuous testing
Static Code Analysis (Medium)

- This check tries to determine if the project uses Static Application Security Testing (SAST), also known as static code analysis. It is currently limited to repositories hosted on GitHub.
  - CodeQL
  - SonarCloud
- Definitely room for improvement!

@nielstanis@infosec.exchange

Source Risk Assesement
Binary Artifacts (High)

- This check determines whether the project has generated executable (binary) artifacts in the source repository.
- Binary artifacts cannot be reviewed, allowing possible obsolete or maliciously subverted executables.
- There is need for **reproducible** builds!

@nielstanis@infosec.exchange

Source Risk Assesement
Branch Protection (High)

- This check determines whether a project's default and release branches are protected with GitHub's branch protection or repository rules settings.
  - Requiring code review
  - Prevent force push, in case of public branch all is lost!

Source Risk Assesement
Dangerous Workflow (Critical)

- This check determines whether the project's GitHub Action workflows has dangerous code patterns.
  - Untrusted Code Checkout with certain triggers
  - Script Injection with Untrusted Context Variables
- https://securitylab.github.com/research/github-actions-preventing-pwn-requests/

@nielstanis@infosec.exchange

Source Risk Assesement
Code Review (Low)

- This check determines whether the project requires human code review before pull requests are merged.
- The check determines whether the most recent changes (over the last ~30 commits) have an approval on GitHub and merger!=committer (implicit review)

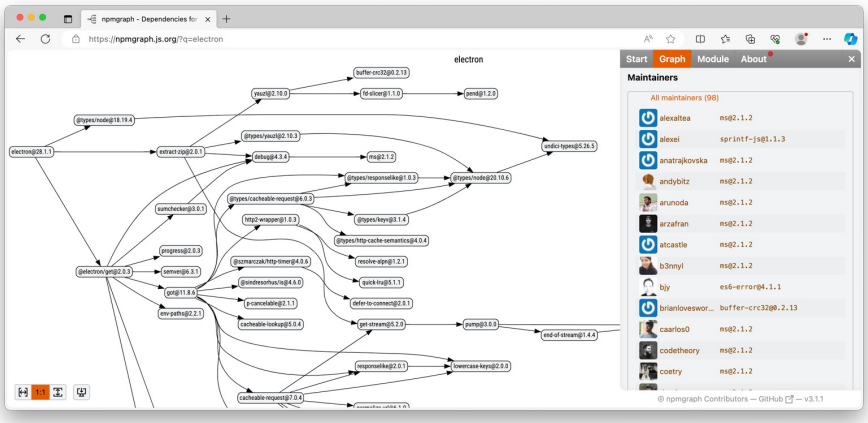
@nielstanis@infosec.exchange

Source Risk Assesement Contributors (Low)

- This check tries to determine if the project has recent contributors from multiple organizations (e.g., companies).
- Relying on single contributor is a risk for sure!
- But is a large list of contributors good?

@nielstanis@infosec.exchange

Source Risk Assesement Contributors (Low)



@nielstanis@infosec.exchange

Build Risk Assesement
Pinned Dependencies (High)

- Does the project pin dependencies used during its build and release process.
- For .NET → **RestorePackagesWithLockFile** in MSBuild results in **packages.lock.json** file containing versioned dependency tree with hashes
- If Workflow is present what about the Actions used?

@nielstanis@infosec.exchange

Build Risk Assesement
Token Permission (High)

- This check determines whether the project's automated workflows tokens follow the principle of least privilege.
- This is important because attackers may use a compromised token with write access to, for example, push malicious code into the project.

@nielstanis@infosec.exchange

https://securitylab.github.com/research/github-actions-preventing-pwn-requests/

Build Risk Assesement Packaging (Medium)

- This check tries to determine if the project is published as a package.
- Packages give users of a project an easy way to download, install, update, and uninstall the software by a package manager.

@nielstanis@infosec.exchange

Build Risk Assessment
Signed Releases (High)

- This check tries to determine if the project cryptographically signs release artifacts.
  - Signed release packages
  - Signed build provenance

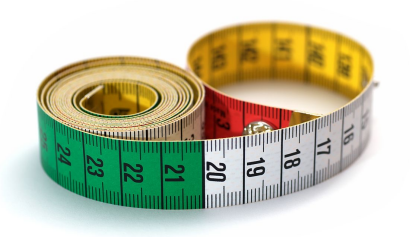
@nielstanis@infosec.exchange

Demo OpenSSF Scorecard

```
Running checks
```

@nielstanis@infosec.exchange

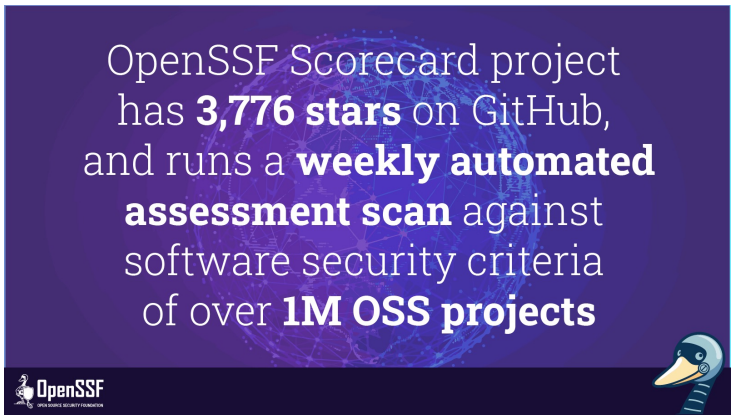
Measure?



@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

OpenSSF Annual Report 2023



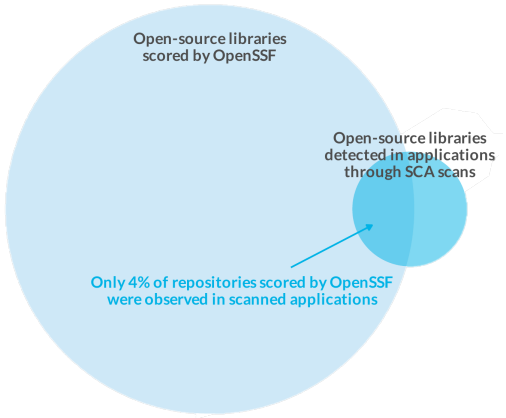
@nielstanis@infosec.exchange

https://openssf.org/download-the-2023-openssf-annual-report/

SOSS & OpenSSF Scorecard

@nielstanis@infosec.exchange

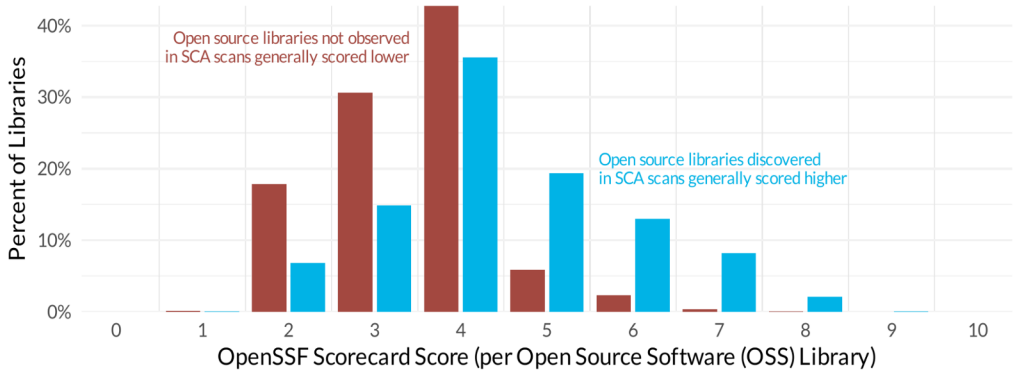
SOSS & OpenSSF Scorecard



@nielstanis@infosec.exchange

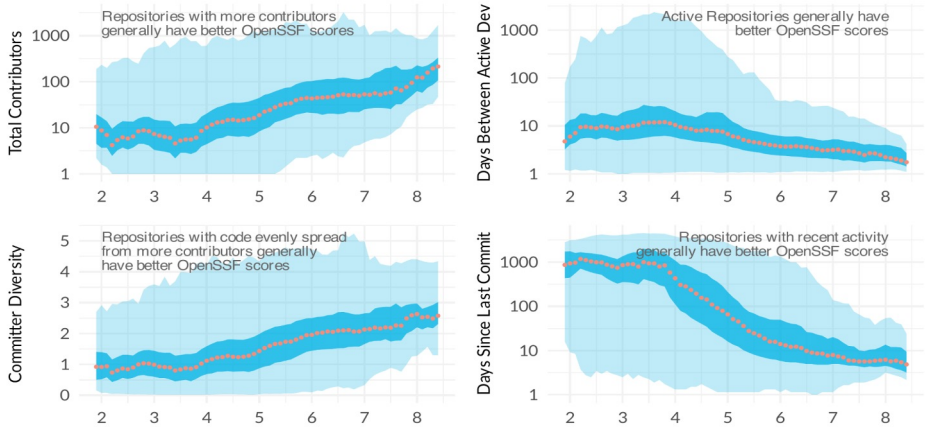
https://www.rsaconference.com/Library/presentation/usa/2024/quantifying%20the%20probability%20of%20flaws%20in%20open%20source

Correlation between SOSS



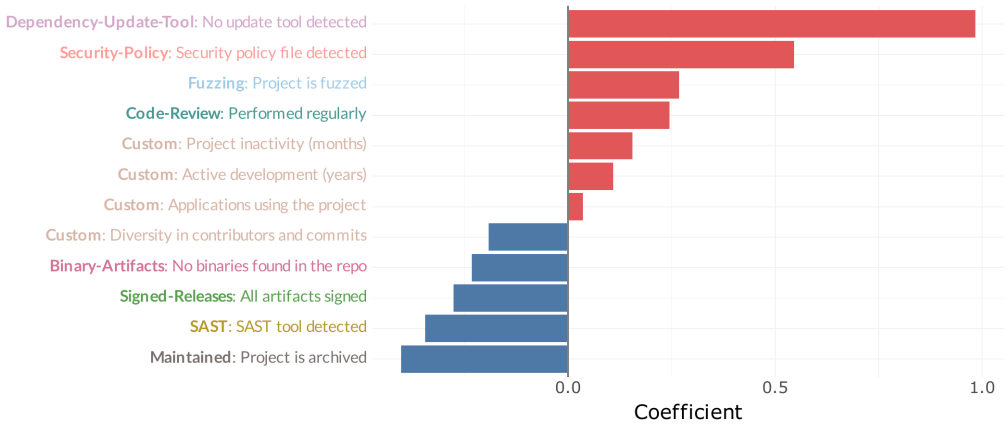
@nielstanis@infosec.exchange

Github commits vs OpenSSF



@nielstanis@infosec.exchange

What really contributes to OSS Security?



@nielstanis@infosec.exchange

What can we improve?

@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

Fuzzing

- Fuzzing, or fuzz testing
  - Automated software testing method that uses a wide range of ***invalid*** and unexpected data as input to find flaws
- Definitely good for finding C/C++ memory issues
- Can it be of any value with managed languages like .NET and/or Java?

@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

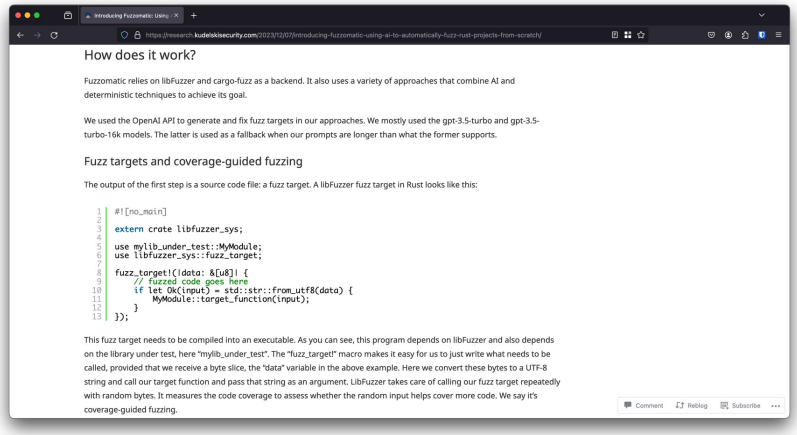
Fuzzing .NET – Jil JSON Serializer


```
public static void Main(string[] args)
{
        SharpFuzz.Fuzzer.OutOfProcess.Run(stream => {
        try
        {
                using (var reader = new System.IO.StreamReader(stream))
                JSON.DeserializeDynamic(reader);
        }
        catch (DeserializationException) { }
        });
}
```

@nielstanis@infosec.exchange

https://github.com/google/fuzzing/blob/master/docs/structure-aware-fuzzing.md

Fuzzomatic: Using AI to Fuzz Rust



How does it work?

Fuzzomatic relies on libFuzzer and cargo-fuzz as a backend. It also uses a variety of approaches that combine AI and deterministic techniques to achieve its goal.

We used the OpenAI API to generate and fix fuzz targets in our approaches. We mostly used the gpt-3.5-turbo and gpt-3.5-turbo-16k models. The latter is used as a fallback when our prompts are longer than what the former supports.

Fuzz targets and coverage-guided fuzzing

The output of the first step is a source code file: a fuzz target. A libFuzzer fuzz target in Rust looks like this:

```
#![no_main]

extern crate libfuzzer_sys;

use mylib_under_test::MyModule;
use libfuzzer_sys::fuzz_target;

fuzz_target!(|data: &[u8]| {
    // fuzzed code goes here
    if let Ok(input) = std::str::from_utf8(data) {
        MyModule::target_function(input);
    }
});
```

This fuzz target needs to be compiled into an executable. As you can see, this program depends on libFuzzer and also depends on the library under test, here "mylib_under_test". The "fuzz_target!" macro makes it easy for us to just write what needs to be called, provided that we receive a byte slice, the "data" variable in the above example. Here we convert these bytes to a UTF-8 string and call our target function and pass that string as an argument. LibFuzzer takes care of calling our fuzz target repeatedly with random bytes. It measures the code coverage to assess whether the random input helps cover more code. We say it's coverage-guided fuzzing.

@nielstanis@infosec.exchange

https://research.kudelskisecurity.com/2023/12/07/introducing-fuzzomatic-using-ai-to-automatically-fuzz-rust-projects-from-scratch/

Static Code Analysis (SAST)


```
public byte[] CreateHash(string password)
{
  var b = Encoding.UTF8.GetBytes(password);
  return SHA1.HashData(b);
}
```

@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

Static Code Analysis (SAST)


```
public class CustomerController : Controller
{
    public IActionResult GenerateCustomerReport(string customerID)
    {
        var data = Reporting.GenerateCustomerReportOverview(customerID)
        return View(data);
    }
}
```

```
public static class Reporting
{
    public static byte[] GenerateCustomerReportOverview(string ID)
    {
        return System.IO.File.ReadAllBytes($"./data/{ID}.pdf");
    }
}
```

@nielstanis@infosec.exchange

https://www.bestpractices.dev/en/criteria/0

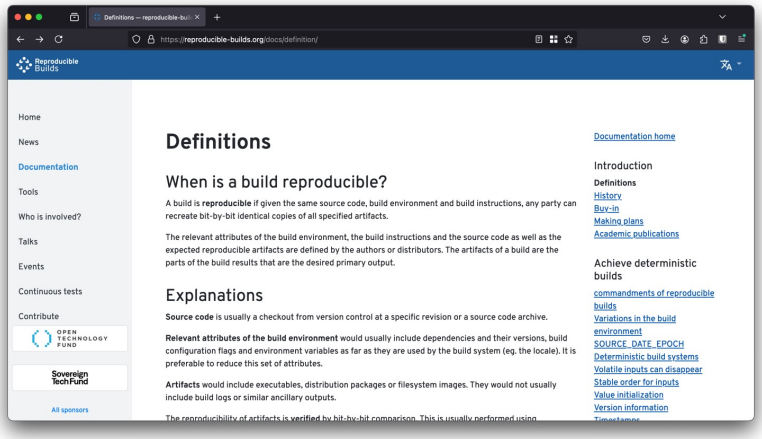
Package Reproducibility

- A build is **reproducible** if given the same source code, build environment and build instructions, any party can recreate bit-by-bit identical copies of all specified artifacts.

@nielstanis@infosec.exchange

Reproducible-Builds.org

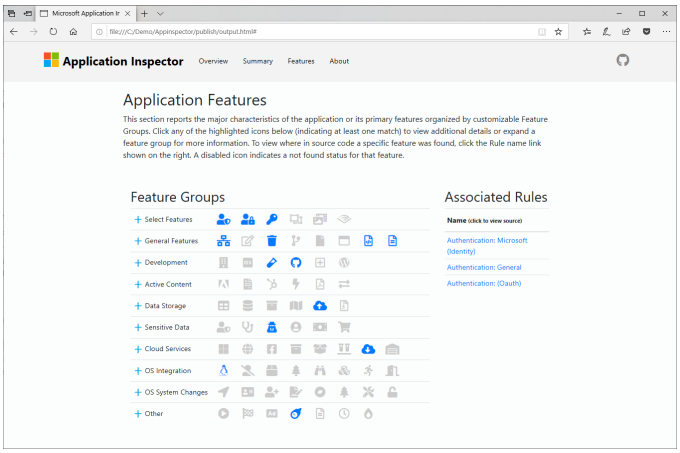
New & Improved!



@nielstanis@infosec.exchange

Reproducible-Builds.org

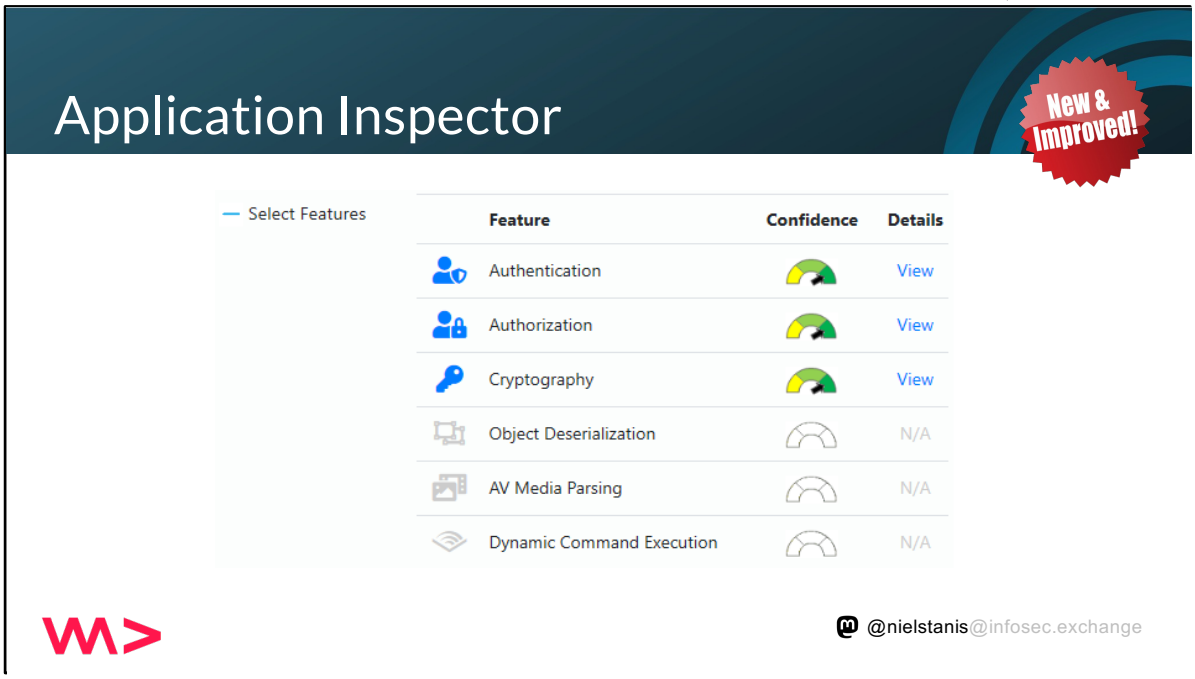
Application Inspector



@nielstanis@infosec.exchange

https://github.com/microsoft/ApplicationInspector

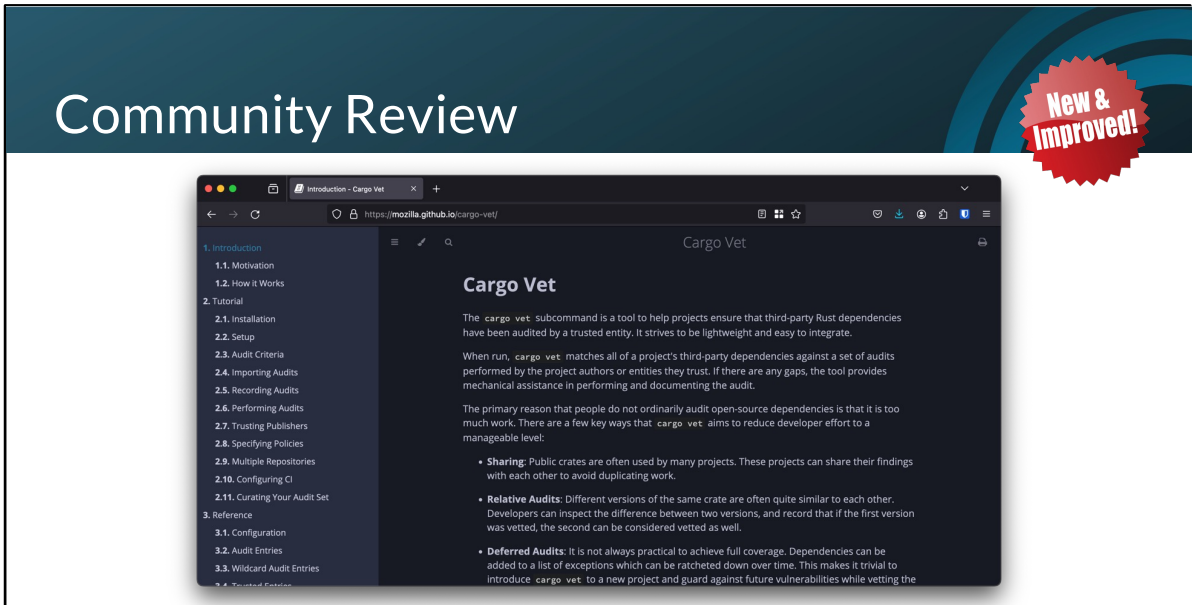
Application Inspector



@nielstanis@infosec.exchange

https://github.com/microsoft/ApplicationInspector

Community Review



@nielstanis@infosec.exchange

https://mozilla.github.io/cargo-vet/

Conclusion

- Scorecard helps security reviewing a used Package
- Better understand what's inside, how it’s build/maintained and what are the risks!
- Scorecard should not be a goal on it’s own!

@nielstanis@infosec.exchange

Conclusion

- Room for improvements
  - Reproduciblity Tools (diff, insights)
  - Reporting
  - Trust Graph
  - Contribute back to OpenSSF Scorecard

@nielstanis@infosec.exchange

Questions?

@nielstanis@infosec.exchange

Links

- https://github.com/nielstanis/wearedevs2024/
- ntanis at Veracode.com
- @nielstanis@infosec.exchange
- https://www.fennec.dev & https://blog.fennec.dev