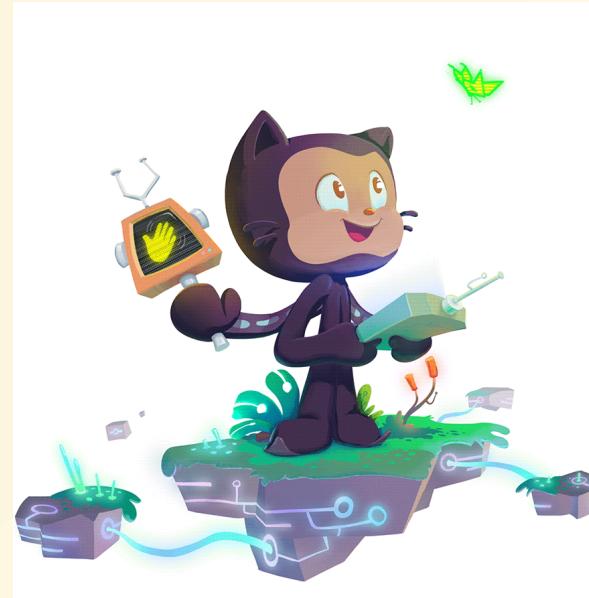


# Open source + Security = ❤

by Adrien Pessu ([@adrienpessu](https://github.com/adrienpessu))  GitHub



# Introduction



# Introduction



# Introduction



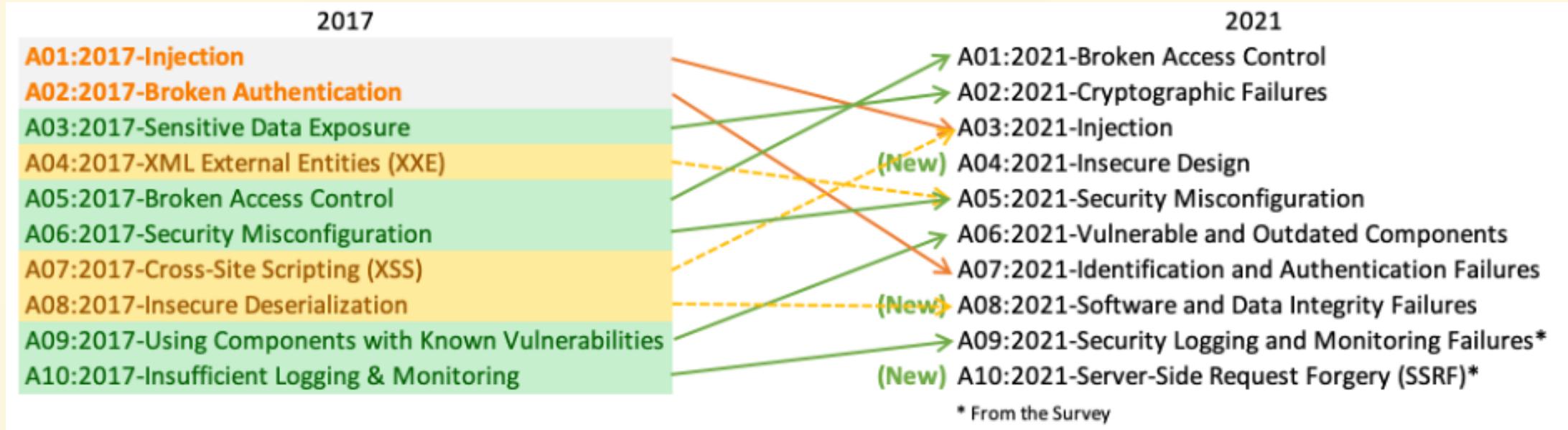
# Agenda

-  OWASP
-  Open source security foundation
-  MITRE
-  How to open source



The *Open Web Application Security Project*® (OWASP) is a **nonprofit foundation** that works to improve the security of software.

- open-source software projects,
- hundreds of local chapters worldwide,
- tens of thousands of members,
- and leading educational and training conferences

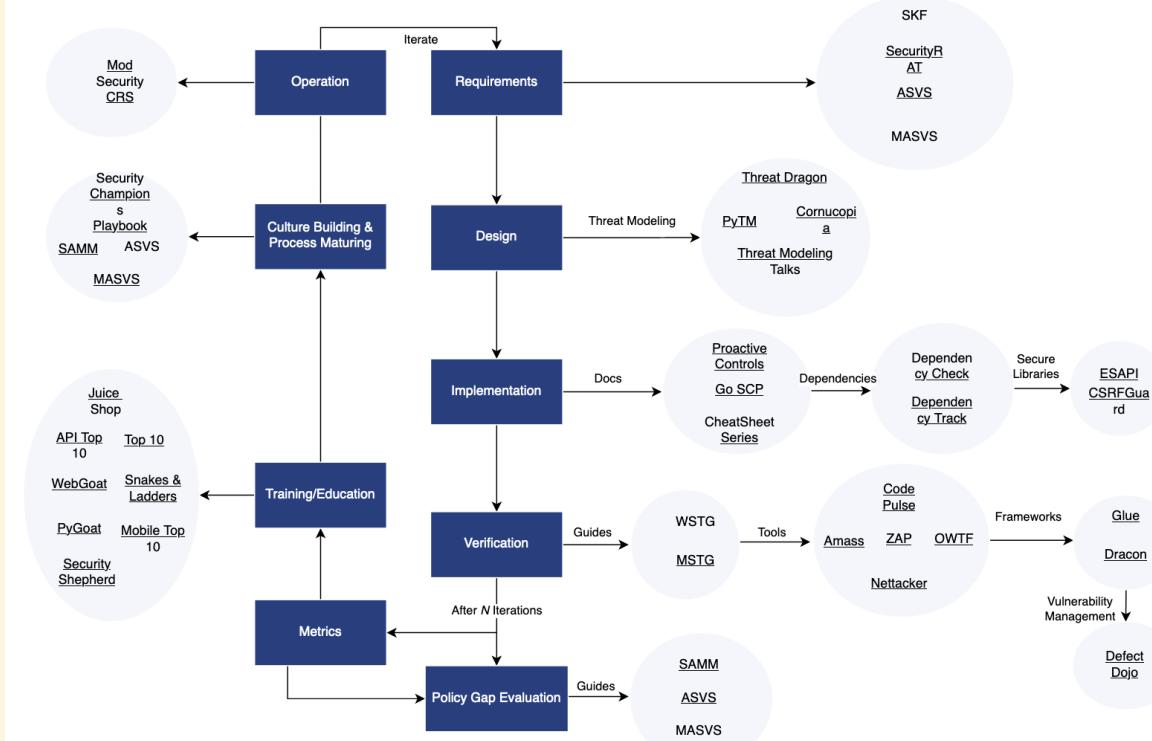


<https://owasp.org/Top10/fr/>



## Application Security Wayfinder

Brought to you by the Integration standards project  
Linking requirements and guidance across standards through the Common Requirement Enumeration





# OWASP Dependency-check



```
dependency-check --project "myproject" --scan [project_path] --out  
[output_path]
```



# OWASP AMASS

Network mapping of attack surfaces and external asset discovery.  
Using Information Gathering Techniques :

- API : Pastebin, Twitter, GitHub, ....
- Certificates: Digitorus, FacebookCT, GoogleCT, ...
- DNS: Brute forcing, Reverse DNS sweeping, NSEC zone walking,

..

Routing, Scraping, Web Archives, WHOIS

```
@ad amass enum -d example.com
```



# OWASP ZAP (Zed Attack Proxy)

- Proxy
- App Scanner



# Open source security foundation (OpenSSF)

Cross-industry forum for a collaborative effort to improve open source software security.

*GitHub, Google, IBM, JPMorgan Chase, Microsoft, NCC Group, OWASP Foundation, Red Hat, HackerOne, Intel, Okta, Purdue, Uber, WhiteSource, and VMware.*



# Open source security foundation (OpenSSF)

- Projects (like Sigstore, ...)
- Funding open source projects
- Free trainings
- Guides



- American not-for-profit organization
- *"provide evidence-based, objective and nonpartisan insights for government policymaking"*



- CVE : Common Vulnerabilities and Exposures

**CVE-2021-44228** PUBLISHED [View JSON](#)

Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

**IMPORTANT NOTIFICATION**

As of October 6, 2022, [CVE Records](#) on this cve.org website will be displayed in [CVE JSON 5.0](#) only. Downloads in this format will be introduced in 2023.

During the transition period, CVE Records may still be viewed in CVE JSON 4.0 format on the [CVE List GitHub pilot](#) website while the traditional CVE List download formats will continue to be available on the legacy [cve.mitre.org](#) website. [Learn more here](#).

**Assigner:** Apache  
**Published:** 2021-12-10 **Updated:** 2022-08-03

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

- ATT&CK : knowledge base of adversary tactics and techniques based on real-world observations



# How to open source but safely

## CodeQL && Secret scanning

The image shows a screenshot of a GitHub pull request status checks interface. At the top, there's a green circular icon with a red segment and the text "Some checks were not successful" followed by "2 successful and 1 failing checks". A "Hide all checks" link is on the right. Below this, there are three items:

- A green checkmark icon next to "CodeQL / Analyze (csharp) (pull\_request)" with the status "Successful in 3m" and a "Details" link.
- A green checkmark icon next to "CodeQL / Analyze (javascript) (pull\_request)" with the status "Successful in 2m" and a "Details" link.
- A red X icon next to "Code scanning results / CodeQL" with the status "Failing after 1m — 1 error" and a "Required" button and "Details" link.

Below these, a yellow circle icon indicates a warning: "Required statuses must pass before merging" with the note "All required [statuses](#) and check runs on this pull request must run successfully to enable automatic merging." A message at the bottom states "As an administrator, you may still merge this pull request." At the very bottom, there are "Merge pull request" and "You can also open this in GitHub Desktop or view command line instructions." buttons.



# How to open source but safely

- Bump stripe from 5.25.0 to 5.26.0 ✓ [dependencies](#)  
#2098 opened 3 days ago by dependabot-preview [bot](#) • Review required
- Bump aws-sdk-s3 from 1.81.0 to 1.83.0 ✓ [dependencies](#)  
#2097 opened 3 days ago by dependabot-preview [bot](#) • Review required
- Bump knapsack from 1.18.0 to 1.19.0 ✓ [dependencies](#)  
#2096 opened 3 days ago by dependabot-preview [bot](#) • Review required
- Bump google-api-client from 0.45.0 to 0.46.0 ✓ [dependencies](#)  
#2095 opened 3 days ago by dependabot-preview [bot](#) • Review required
- Bump puma from 5.0.0 to 5.0.2 ✓ [dependencies](#)  
#2094 opened 3 days ago by dependabot-preview [bot](#) • Review required



# How to open source but safely

Bump node-fetch from 2.6.5 to 2.6.7 #311

[Open](#) dependabot wants to merge 1 commit into `master` from `dependabot/npm_and_yarn/node-fetch-2.6.7`

Merging this pull request will resolve a high severity [Dependabot alert](#) on node-fetch.

Conversation 0 · Commits 1 · Checks 1 · Files changed 1 · Edit · Code

**dependabot** bot commented on behalf of github on Jun 24

Bumps node-fetch from 2.6.5 to 2.6.7.

Release notes  
Sourced from [node-fetch's releases](#).

v2.6.7

**Security patch release**

Recommended to upgrade, to not leak sensitive cookie and authentication header information to 3rd party host while a redirect occurred

**What's Changed**

- fix: don't forward secure headers to 3rd party by [@jimmywarting](#) in node-fetch|node-fetch#1453

Full Changelog: [node-fetch@v2.6.6...v2.6.7](#)

v2.6.6

**What's Changed**

- fix(URL): prefer built in URL version when available and fallback to whatwg by [@jimmywarting](#) in node-fetch|node-fetch#1352

Full Changelog: [node-fetch@v2.6.5...v2.6.6](#)

**Commits**

- [1ef4056](#) backport of #1449 (#1453)
- [8fe5cde](#) 2.x: Specify encoding as an optional peer dependency in package.json (#1310)
- [1586bcb](#) fix(URL): prefer built in URL version when available and fallback to whatwg (...)

See full diff in [compare view](#)

compatibility 97%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

Dependabot commands and options

Reviewers  
No reviews  
Still in progress? Convert to draft

Assignees  
No one—assign yourself

Labels  
[dependencies](#)

Projects  
None yet

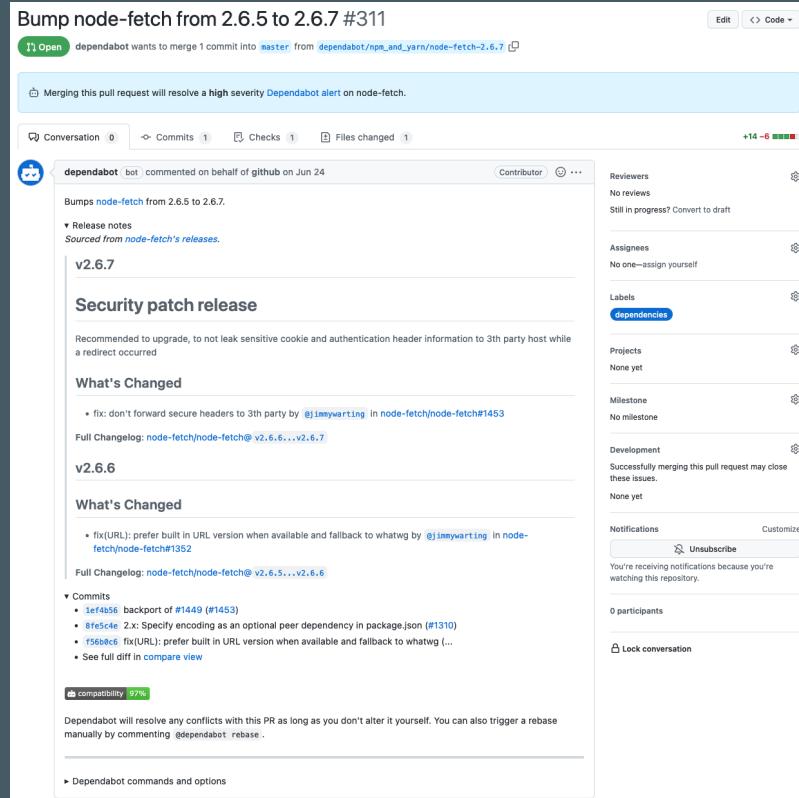
Milestone  
No milestone

Development  
Successfully merging this pull request may close these issues.  
None yet

Notifications  
Customize  
Unsubscribe  
You're receiving notifications because you're watching this repository.

0 participants

Lock conversation





# How to open source but safely

The screenshot shows the GitHub interface for the repository `micronaut-projects / micronaut-core`. The top navigation bar includes links for Code, Issues (474), Pull requests (93), Discussions, Actions, Projects (1), Wiki, Security (3), and Insights. The Security tab is currently selected, indicated by an orange underline.

The left sidebar features a navigation menu with options: Overview, Reporting, Policy, **Advisories** (selected, with a count of 3), Vulnerability alerts, and Code scanning.

The main content area is titled "Security Advisories" and contains a sub-instruction: "View known security vulnerabilities and report new vulnerabilities privately to maintainers." A green button labeled "Report a vulnerability" is located in the top right corner of this section.

Three security advisories are listed:

- DoS attack via array heap pollution when sending invalid content type header** (High severity) - GHSA-2457-2263-mm9f published on Jan 18 by jameskleeh
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in micronaut-core** (High severity) - GHSA-cjx7-399x-p2rj published on Jul 16, 2021 by jameskleeh
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request Header Injection')** (Moderate severity) - GHSA-694p-xrhg-x3wm published on Mar 30, 2020 by graemerucher

# Conclusion

How to contribute ?

- Code
- Doc
- Talks
- Blog posts
- ...