

OpenSSF Lab: Learn Scorecard

Spring 2025

Chengyi Qu

Submission Due: Mar 25th

Background

- Scorecard is an automated tool that assesses a number of important heuristics ("checks") associated with software security and assigns each check a score of 0-10. You can use these scores to understand specific areas to improve in order to strengthen the security posture of your project. You can also assess the risks that dependencies introduce, and make informed decisions about accepting these risks, evaluating alternative solutions, or working with the maintainers to make improvements.

Chaoss

About CHAOSS

CHAOSS is a Linux Foundation project focused on creating metrics, metrics models, and software to better understand open source community health on a global scale.

<https://chaoss.community/kbtopic/all-metrics/>

Who is using Scorecard?

- Scorecard has been run on thousands of projects to monitor and track security metrics. Prominent projects that use Scorecard include:
 - [Tensorflow](#)
 - [Angular](#)
 - [Flutter](#)
 - [sos.dev](#)
 - [deps.dev](#)

Lab Key Links

- Learn Scorecard from OpenSSF:

<https://openssf.org/training/securing-projects-with-openssf-scorecard-course/>

- OpenSSF Best Practice Badge:

<https://www.bestpractices.dev/en>

- Github Pages/personal website:

<https://github.com/topics/personal-website>

<https://pages.github.com/>

Lab objective

- Learn to use Scorecard from the OpenSSF course, get certificate of the course.
- Include badges in one of your Git repo:
 - Badges on Scorecard scores
 - Badges on OpenSSF Best Practices
- Analysis your code, modify your code and show improvement of your scorecard scores.

Tasks

- Learn
 - Learn from OpenSSF Scorecard course and get certification
 - Extra points: Other two course options of the OpenSSF courses
- Earn
 - Earn Scorecard score badge in your current Github Repo
 - Earn OpenSSF Best Practice badge in your current Github Repo
- Repeat!
 - Analysis your code, kill some security concerns and increase your Scorecard scores!

Task 1: Learn: Pass the course (30 scores)

- ❑ Pass the course and get certificate (with your name 😊)
- ❑ <https://openssf.org/training/securing-projects-with-openssf-scorecard-course/>
- ❑ (Bonus Points – 20 Scores) <https://openssf.org/training/securing-your-software-supply-chain-with-sigstore-course/>



Task 2: Earn: TWO badges to earn (30 points)

- ❑ Select one of your Github project.
- ❑ Design a Github welcome page of the project (Can be your personal website).
- ❑ Earn TWO badges of your repo: Scorecard and OpenSSF Best Practice
 - ❑ Scorecard scores can be anything we will improve later.
 - ❑ OpenSSF Best Practice MUST be PASS or Silver or Gold, pending is not accepted!

☰ README.md

Releases:  v2.7.9  argo-cd  level 3

Code:  Integration tests failing  codecov 50%  openssf best practices passing  openssf scorecard 8.2  license scan failing

Social:  Follow @argoproj  slack argoproj

Argo CD - Declarative Continuous Delivery for Kubernetes

Task 3: Repeat: Low score? No worries! (40 points)

- ❑ Try to address TWO of the HIGH issues after code scanning. (20 points each)
- ❑ Any improve of your score are accepted!
- ❑ Describe in the report on
 - ❑ Which of the open issue has been addressed?
 - ❑ How you address that issue?
 - ❑ How much improve on your scores?

The screenshot shows the GitHub Security interface. The top navigation bar includes links for Code, Issues (1), Pull requests, Actions, Projects, Wiki, Security (26), and Insights. The left sidebar lists various security features: Overview, Reporting, Policy, Advisories, Vulnerability alerts, Dependabot, Code scanning (26), and Secret scanning. The main content area is titled 'Code scanning' and shows a status bar with a green checkmark indicating 'All tools are working as expected'. Below this is a search bar with the text 'is:open branch:main' and a summary showing '26 Open' and '1 Closed' issues. A table of open issues is displayed, with filters for Language, Tool, Branch, Rule, Severity, and Sort. The table lists four high-severity issues, all detected by Scorecard on the 'main' branch.

Issue	Severity	Branch	Details
Code-Review	High	main	#3 opened 5 days ago • Detected by Scorecard in no file associated with ...:1
Token-Permissions	High	main	#27 opened 5 days ago • Detected by Scorecard in .github/workflows/site.yml:1
Token-Permissions	High	main	#26 opened 5 days ago • Detected by Scorecard in .github/workflows/release.yml:9
Token-Permissions	High	main	#25 opened 5 days ago • Detected by Scorecard in .github/workflows/post-merge.yml:1

What you need to submit

- ✓ Certification PDF(s) (if you pass Sigstore course attach separately.)
- ✓ A detailed **lab report** that should
 - For Task 2: URL of the Github Project you choose, and screenshots of your README.md with Badge showing in the front.
 - For Task 3: Describe all your efforts on addressing issues highlighted by Scorecard. And some screenshots showing you have a score increase!
 - Simply attaching screenshots without any explanation will not receive credits.

Submission Due: Mar 25th