# Summary

The team has taken another step toward ensuring the quality of their code. They've added a tool to the pipeline that automatically scans open-source software for vulnerabilities and identifies how it's licensed. Whenever they add a new feature or library, they can easily check to make sure that any open-source component meets all security and legal requirements.

We all strive to deliver quality, secure products to our users. We want to be sure that all of our code, including the open source libraries we use, meet security standards. We all want to avoid any legal problems that might result if we don't comply with the conditions set out in the license.

By shifting our security and compliance testing earlier in the development process, we can catch potential issues early. By automating the tests and making them part of the build pipeline, we ensure that the tests run on a regular basis. Automation and shifting tests earlier are great ways to ensure that builds are secure.

In this module, you looked at some tools you can use to scan your open-source references for known vulnerabilities and licensing types. You scanned the Space Game web project for issues that need to be addressed. Finally, you explored the report that the tool generated, which highlighted some vulnerabilities.

## Learn more

The open standards such as CVE that we discussed in this module are part of the [Security Content Automation Protocol](https://csrc.nist.gov/projects/security-content-automation-protocol) (SCAP).

There are other components to SCAP that you might want to get familiar with. Check out [National Institute of Standards and Technology](https://csrc.nist.gov/projects/security-content-automation-protocol) (NIST) for a list of components.