



Web Security Shorts

Part 2: Securing your GitHub code repository

Prior topics

- git, GitHub, and UW GitHub enterprise
- why secure repositories?
- managing access in GitHub and UW GitHub
- view [Part 1 slides](#)



Future topics

- repository security policies
- code scanning
- secret scanning



Today's topics

- Dependency management
- Setup in GitHub
- Dependency graph
- Dependabot alerts
- Security and version updates
- Dependency review



Dependency management



Software dependency - what is it?

- a software dependency can be a plugin, library, package, or a custom module that your application uses to run successfully
- direct dependency
 - dependencies your code calls directly
- transitive
 - dependencies your dependencies call

Dependency management - what is it?

In this presentation, it means tools that can be used to monitor and update your software dependencies

Dependency management - why?

- each dependency has the potential to have a security vulnerability
- keeping on top of security updates and responding quickly can keep your application more secure

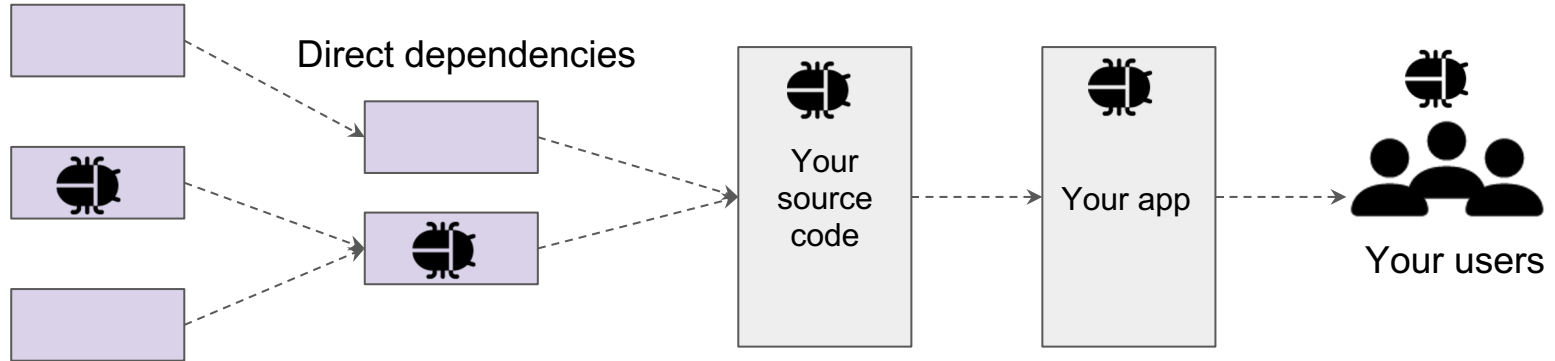
How do dependencies become vulnerable?

some examples ...

- a contributor to a third party package might add malicious code
- a contributor's account can be taken over and malicious code added
- package typosquatting

A vulnerability working through the chain

Transitive dependencies



Based on illustration from <https://blog.gitguardian.com/supply-chain-attack-6-steps-to-harden-your-supply-chain/>

Dependency management - why GitHub?

- UW IT provides a UW GitHub service and GitHub is a popular git repository host in general
- covers several language ecosystems, e.g. npm, pip, Composer, etc.
- however, there are many tools for dependency management that can be used (OWASP dependency checker, npm audit etc.)



Why not monitor and update myself?

Modern projects can easily have thousands of dependencies

- for example using create-react-app to create a React.js project alone can add over 1000 direct and transitive dependencies to your project
- a single developer can't track them all

Set up in GitHub



Setup

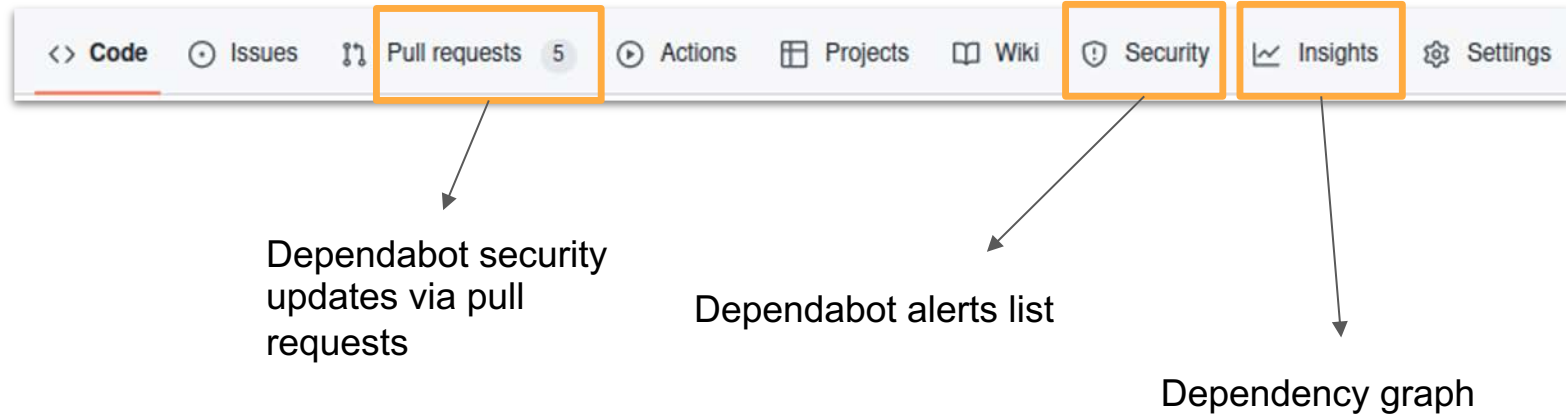
The screenshot displays the GitHub repository settings page, specifically the 'Code security and analysis' section. The page is annotated with four numbered orange boxes:

- 1.** Points to the 'Settings' tab in the top navigation bar.
- 2.** Points to the 'Code security and analysis' option in the left-hand sidebar.
- 3.** Points to the 'Code security and analysis' section header and its introductory text.
- 4.** Points to the 'Private vulnerability reporting', 'Dependency graph', 'Dependabot alerts', 'Dependabot security updates', and 'Dependabot version updates' settings.

The 'Code security and analysis' section includes the following settings:

- Private vulnerability reporting:** Allow your community to privately report potential security vulnerabilities to maintainers and repository owners. [Learn more about private vulnerability reporting.](#)
- Dependency graph:** Understand your dependencies. Dependency graph is always enabled for public repos.
- Dependabot:** Keep your dependencies secure and up-to-date. [Learn more about Dependabot.](#)
- Dependabot alerts:** Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications.](#)
- Dependabot security updates:** Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.
- Dependabot version updates:** Allow Dependabot to open pull requests automatically to keep your dependencies up-to-date when new versions are available. [Learn more about configuring a dependabot.yml file.](#)

Where to find the tools



Dependency graph

what dependencies do you have?

Dependency graph

- summary of your dependencies, the ecosystems and packages it depends on
- dependency information derived from your particular manifest and lock files, e.g. npm, pip, yarn
- also lists any apps dependent on your repository

Dependency graph










Dependencies

Dependents

Dependabot

These dependencies are defined in **dependency-example**'s manifest files, such as [package-lock.json](#) and [package.json](#).

Dependencies defined in **package-lock.json** 1,174

>	 adobe / css-tools @adobe/css-tools	4.0.1
>	 ampproject / remapping @ampproject/remapping	2.2.0
>	 apideck-libraries / better-ajv-errors @apideck/better-ajv-errors	0.3.6
>	 babel / babel @babel/code-frame	7.18.6
>	 babel / babel @babel/compat-data	7.19.0
>	 babel / babel @babel/core	7.19.0
>	 babel / babel @babel/eslint-parser	7.18.9
>	 babel / babel @babel/generator	7.19.0
>	 babel / babel @babel/helper-annotate-as-pure	7.18.6

Dependency graph

- public repositories
 - automatically generated
 - anyone can view
- private repositories
 - manually enabled
 - view restricted to certain roles, but any member can be added to a view list

Dependabot alerts



What is a Dependabot?

Dependabot is GitHub's automatic tool used to find and fix vulnerable dependencies in a repository.



Dependabot alerts

- reports existing dependency vulnerabilities
- when enabled, alerts are displayed on the security tab and the dependency graph
- available in public or private repos, but needs to be manually enabled
- can set at the repository or organization level
- can enable by default for new repositories



Security tab view

Dependabot alerts Configure ▾

Q is:open

ⓘ **8 Open** ✓ 1 Closed Package ▾ Ecosystem ▾ Manifest ▾ Severity ▾ Sort ▾

- ⓘ **Prototype pollution in webpack loader-utils** Critical
#2 opened 3 months ago • Detected in loader-utils (npm) • package-lock.json
- ⓘ **Prototype Pollution in JSON5 via Parse Method** High 🔗 #14
#9 opened last month • Detected in json5 (npm) • package-lock.json
- ⓘ **Prototype Pollution in JSON5 via Parse Method** High 🔗 #14
#8 opened last month • Detected in json5 (npm) • package-lock.json
- ⓘ **loader-utils is vulnerable to Regular Expression Denial of Service (ReDoS) via url variable** High
#7 opened 3 months ago • Detected in loader-utils (npm) • package-lock.json
- ⓘ **loader-utils is vulnerable to Regular Expression Denial of Service (ReDoS)** High
#6 opened 3 months ago • Detected in loader-utils (npm) • package-lock.json
- ⓘ **loader-utils is vulnerable to Regular Expression Denial of Service (ReDoS) via url variable** High
#5 opened 3 months ago • Detected in loader-utils (npm) • package-lock.json
- ⓘ **loader-utils is vulnerable to Regular Expression Denial of Service (ReDoS)** High
#4 opened 3 months ago • Detected in loader-utils (npm) • package-lock.json
- ⓘ **minimatch ReDoS vulnerability** High 🔗 #11
#3 opened 3 months ago • Detected in minimatch (npm) • package-lock.json



Dependency graph view

Dependency graph

Dependencies Dependents Dependabot

⚠️ We found potential security vulnerabilities in your dependencies.
Dependencies defined in these manifest files have known security vulnerabilities and should be updated:
package-lock.json 8 vulnerabilities found

[View Dependabot alerts](#)

Only the owner of this repository can see this message.

These dependencies are defined in **dependency-example**'s manifest files, such as **package-lock.json** and **package.json**.

Dependencies defined in **package-lock.json** 1,174

> json5 / json5	Known security vulnerability in 1.0.1
> json5 / json5	Known security vulnerability in 2.2.1
> webpack / loader-utils	Sponsor Known security vulnerability in 3.2.0
> webpack / loader-utils	2 known vulnerabilities found CVE-2022-37599 High severity CVE-2022-37603 High severity package-lock.json update suggested: loader-utils -> 3.2.1 Always verify the validity and compatibility of suggestions with your codebase.
> isaacs / minimatch	
> isaacs / minimatch	
> isaacs / minimatch	
> arduino / css-tools @arduino/css-tools	4.0.1

Security alerts bubble up to the top of the list



Dependabot updates

Security and Version



Dependabot security updates

- automatic pull requests to your default branch
- triggered by a Dependabot alert
- only updates to the minimum version that resolves a known vulnerability
- allows you to apply security updates quickly
- but to avoid breakage follow your testing process before merging



 5 Open ✓ 10 Closed

 **Bump web-vitals from 3.0.1 to 3.1.1** dependencies

#15 opened on Jan 15 by dependabot 

 **Bump json5 from 1.0.1 to 1.0.2** dependencies

#14 opened on Jan 8 by dependabot 

 **Bump loader-utils from 2.0.2 to 2.0.4** dependencies

#12 opened on Nov 16, 2022 by dependabot 

 **Bump minimatch and recursive-readdir** dependencies

#11 opened on Nov 13, 2022 by dependabot 

 **Bump @testing-library/user-event from 13.5.0 to 14.4.3** dependencies

#6 opened on Sep 18, 2022 by dependabot 



Dependabot version updates, 1 of 2

- automatically creates pull requests to update dependencies to latest version
 - even if there is not a vulnerability
- however, develop your version update strategy first before implementing automatic version updates
 - updating versions too quickly can have security and non-security implications
 - [*6 steps to protect your software supply chain](#)



Dependabot version updates, 2 of 2

- configuration includes options to
 - schedule
 - select only certain dependencies to update
 - designate a target branch like dev for testing/checks
- more reading
 - [About Dependabot version updates](#)
 - [Configuring Dependabot version updates](#)



Dependency review

(before merging)



Dependency review (before merging)

- allows you to review dependency changes before accepting a pull request from another developer
- reports on which dependencies were added, removed, or updated
- includes vulnerability data for the dependencies
- available in all public repositories and cannot be disabled
- private repositories need GitHub Advanced Security
 - which is not included in UW GitHub service

Pull request details > File Changes >

51 package-lock.json <> 📄 Viewed ...

+ @popperjs/core 2.11.6 released 6 months ago	📦 1.85m	🔗 MIT
+ bootstrap 5.2.3 released 3 months ago	📦 4.21m	🔗 MIT
□ @testing-library/user-event updated to 14.4.3 released 6 months ago	📦 6.65m	🔗 MIT

Give feedback on [dependency review](#)

3 package.json <> 📄 Viewed ...

+ bootstrap ^5.2.3
□ react updated to ^17.2.0

Give feedback on [dependency review](#)

More reading

- [Securing your repository](#)

Thank you! Questions?

Peter Giles
gilesp@uw.edu

Pete Graff
pgraff@uw.edu

Jeanne Marty
jeanem@uw.edu

