Keeping secrets secure with secret scanning

Let GitHub do the hard work of ensuring that tokens, private keys, and other code secrets are not exposed in your repository.

Secret scanning alerts for partners runs automatically on public repositories and public npm packages to notify service providers about leaked secrets on GitHub.com.
Secret scanning alerts for users are available for free on all public repositories. Organizations using GitHub Enterprise Cloud with a license for GitHub Advanced Security can also enable secret scanning alerts for users on their private and internal repositories. For more information, see "About secret scanning" and "About GitHub Advanced Security."
For information about how you can try GitHub Advanced Security for free, see "Setting up a trial of GitHub Advanced Security."