SNYK CHEATSHEET

10 GitHub Security Best Practices

GitHub

01 Enable and Enforce 2FA for GitHub

- IChoose between an authentication app or SMS for 2FA.
- Enable two-factor authentication (2FA) for your GitHub account.
- Enforce mandatory 2FA for your organization's repositories.

02 Limit Access to Repositories

- Apply the principle of least privilege (PoLP) to repository access.
- Utilize GitHub's access levels: Read, Triage, Write, Maintain, and Admin.
- Grant access based on the collaborator's role, providing the minimum required permissions.

03 Prevent Storing Credentials as Code/Config in GitHub

- Avoid storing sensitive information directly in repositories.
- Use environment variables or external configuration files.
- Employ tools to scan for and prevent credential exposure.

04 Connect Repositories to Snyk and Scan for Vulnerabilities

- Integrate GitHub repositories with Snyk for automatic Scanning.
- Perform Snyk Open Source, Code, Container, and IaC scans.
- Scan incoming pull requests in real-time for vulnerabilities.

05 Add a SECURITY.md File

- Establish a Disclosure Policy for responsible security issue reporting.
- Define a Security Update Policy for informing users about vulnerabilities.
- Provide security-related configuration settings and document known security gaps.

06 Use Branch Protection Rules

- Enforce code quality and collaboration controls.
- Require pull request reviews and passing status checks before merging.
- Restrict push access to matching branches and enforce a linear commit history.

07 Rotate SSH Tokens and Personal Keys

- Regularly rotate SSH tokens and personal keys.
- Manually replace old tokens with new ones.
- Consider automating token and key rotation using GitHub Actions or CI/CD pipelines.

08 Automatic Update Dependencies

- Automate the process of updating dependencies.
- Use Snyk to identify and open pull requests for outdated dependencies.

09 Use Private Repositories for Sensitive Data

- Utilize private repositories for protecting sensitive data and proprietary code.
- Consider disabling public repository creation for added security.

10 Be Smart About Your GitHub Apps

- Grant minimal permissions to GitHub apps.
- Evaluate the legitimacy and security of app developers.
- Regularly review and reassess the necessity of installed apps

snyk