01

Never store credentials as code/ config in Bitbucket

Some good practices:

1. Block sensitive data being pushed to Bitbucket by using the **git-secrets-scan** pipe or a git pre-commit-hook.
2. Break the build using the same tools when necessary.
3. Audit for slipped secrets with truffleHog or a pre-commit hook.
4. Connect to a secret manager like Vault using the Vault Secrets export pipe.

02

Removing sensitive data

1. Invalidate tokens and passwords.
2. Remove the information and clear the Git history force push rewrite history.
3. Assess impact of leaked private information.

ScriptRunner makes these integrations simple.

03

Tightly control access

Failures in security are often the results of humans making poor decisions. Mandate the following practices for your contributors:

1. Require two-factor authentication for all your Bitbucket accounts.
2. Never let developers share Bitbucket accounts/ passwords.
3. Properly secure any laptops/devices with access to your source code.
4. Diligently revoke access from Bitbucket users who are no longer working with you.

Manage team access to data. Give contributors only access to what they need to do their work.

04

Add a SECURITY.md file

You should include a SECURITY.md file that highlights security - related information for your project. This should contain:

1. **Disclosure policy**
   Specify the process to report a security issue and identify a contact. Consider HackerOne's community edition or simply a 'security@' address at your company, or simply a 'security@' email.
2. **Security update policy**
   Describe how you provide updates to project users when you discover security vulnerabilities.
3. **Security-related configuration**
   Describe the settings that specify the security posture of this project, which may include HTTPS, authorization, and others.
4. **Known security gaps & future enhancements**
   These are security improvements you have not yet addressed.

05

Validate Bitbucket apps

Remember these apps are written by third-party developers, not Bitbucket. Validate:

1. The application access rights.
2. The author/organization credibility.
3. The security posture of the Bitbucket App because a breach gives attackers access to your code.

Monitor changes in #2 and #3 and follow the advice of administering your applications.

snyk | ATLASSIAN

06

Get security tips as part of your workflow with code insights

Perform scans on all your open PRs using Bitbucket Code Insights. The Snyk integration provides detailed in-line annotations about the new vulnerabilities that each PR introduces.

07

Add security testing to PRs

Use Bitbucket hooks to check that your PRs don't introduce new vulnerabilities:

1. Snyk - dependency vulnerability testing.
2. Bitbucket Pipe - code quality testing.
3. CodeClimate - automated code reviews.

Visit the new security tab

inside Bitbucket to manage risk using Snyk.

Bitbucket