Security Controls in Shared Source Code Repositories

Dan Zhu

CSD-380 Module 11.2 Assignment

10/05/2025

Agenda

- What is source code repository?
- Why do we need security the source code?
- What are common source security vulnerabilities?
- What are best practices of secure the source code?
- What do you do after the source code security breach?
- What is the developers’ role in source code security?

What is source code repository?

A code repository is a specialized storage systems where you can mange source code and other software development assets (Github, 2024).

Repository is the single source of the truth. Teams can work on the same main code by creating feature branches. So, each one can work on independently. All changes can be track in the repository and merge changes back to the main code when it is ready.

Why do we need security the source code?

Source code security is vital to the health of your organization, especially if you balance the potential risks and business impacts that security vulnerabilities can have (Endpoint Protector, 2022).

Source code could contain algorithms, business logic, and sensitive data, such as encryption keys, OAuth tokens, password, etc. If the information leaked, your competitor could release the product before you. Attackers could find the vulnerability to attack your product. If he source code leaked, it could damage the reputation of the company as well.

What are common source security vulnerabilities?

Wiz (n.d.) outlines a few common source security vulnerabilities:

- Injection attacks: When the input is not validating properly, attacker will try to inject SQL or other commands.
- Cross-site scripting: Attackers inject malicious scripts to steal cookies or session.
- Buffer overflows: Crash the application or inject malicious code by writing more data to memory.
- Insecure authentication and authorization: Attackers can access account due to weak login systems.
- Hardcoded secrets: Steal passwords, API keys or token from the source code when it leaked.

What are best practices of secure the source code?

According to Endpoint Protector (2022), here is a list of best practice of secure the source code:

- Create a source code protection policy: The policy should include documentation, training on implement the best practice of secure source code.

- Prevent the use of insecure source code: You can use tools like Static Application Security Testing to scan the source code and dependencies to detect vulnerabilities.

- **Access control:** Set up two-factor authentication and make sure only hand-on employees get the access to the source code.

- **Use encryption and monitoring:** Making sure sensitive data are encrypt and monitoring data all time.

- **Deploy network security tools:** Use firewalls, VPN, and anti-virus software to protect your source code.

- **Don’t forget about endpoint security:** Data loss prevention solutions helps you protect sensitive information both in physical and virtual environments.

- **Pay attention to patents & copyright:** Software code are protected by copyright and patents.

Endpoint Protector (2022)

What do you do after the source code security breach?

Assembla (2025) lists the steps that we can take while there is a code breach:

- Contain the breach
- Investigate the scope
- Notify relevant parties
- Implement patches and fixes
- Review access controls
- Improve monitoring and detection
- Review incident response plan

What is the developers’ role in source code security?

According to Wiz (n.d.), a developer who knows secure coding best practices and is equipped with the right tools can prevent vulnerabilities before they enter production.

Developer is the one who write the code and they should be at front line of practicing how to secure the source code. Developers can target the vulnerabilities at the beginning of the SDLC. When developers apply proper secure practice, it can reduce bugs and increase the security of the application.

Resources

Assembla. (2025, April 6). *Source code security best practices: A complete guide*. Assembla. https://get.assembla.com/blog/source-code-security/

Endpoint Protector. (2022, April 8). *Best practices for source code security*. Endpoint Protector. https://www.endpointprotector.com/blog/your-ultimate-guide-to-source-code-protection/

GitHub. (2024, December 6). *What are code repositories?* GitHub Resources. https://github.com/resources/articles/software-development/what-are-code-repositories

National Cyber Security Centre. (n.d.). *Protect your code repository*. National Cyber Security Centre. https://www.ncsc.gov.uk/collection/developers-collection/principles/protect-your-code-repository

Wiz. (n.d.). *Source code security: Basics and best practices*. Wiz. https://www.wiz.io/academy/source-code-security

Thank You