



Source Code Security

Michele Brand

Importance of Source Code Security

- + An organization's code is vital to keep secure from being compromised in any way.
- + Compromised applications and software under attack can lead to not only loss of company assets but could lead to the loss of customers as they lose trust in the corporations security.

Best Practices

- + **Control Access** - Making sure the proper people have access to the source code is one way to mitigate security risks.
- + Controlling who has access to the source code and tracking changes to the code can help identify potential faults in security systems.

Best Practices (Cont.)

- + **Protection Policies-** Creating a policy dedicated to protecting source code is a good practice that can help set up and maintain security protocol.
- + Updating this policy regularly to keep up with security threats is also important.

Best Practices (Cont.)

- + **Scan for Security Flaws** - Using threat modeling methods such as Static analysis tools can automatically find keywords that may have been left in the code that would potentially cause security breaches.

Best Practices (Cont.)

- + **Encryption** - data encryption is another practice to use when trying to protect source code from security threats.



Best Practices (Cont.)

- + **Known Vulnerabilities** – knowing if there are any predetermined security threats with an application or 3rd party security software is important to try to mitigate these issues.

Conclusion

- + Keeping software safe from attacks is important, knowing best practices for source code security is incredibly critical.
- + Taking into account all of these best practices can lead to a more secure source code.

Sources

- + <https://www.techtarget.com/searchsecurity/tip/Top-4-source-code-security-best-practices>
- + <https://get.assembla.com/blog/source-code-security/>