SYNOPSYS®

www.synopsys.com |

Secure Coding Guidelines

Practical guidance for fixing and avoiding vulnerabilities

We'll help your developers work off their "bug piles" by supplementing the typical generic coding rules with specific and actionable remediation advice.

3 reasons you need secure coding guidelines

1. Enables developers

Our actionable and comprehensive guidelines are written by and for developers using technology-specific risk explanations, best practices, and reusable code examples. They provide developers the framework, library, and language-specific advice they need to produce secure software and remediate vulnerability backlogs. We also enable you to include your own remediation best practices to better address and align to your unique security best practices.

2. Creates efficiencies through standard coding practices

Our secure coding guidelines provide a blueprint for creating security requirements and enable developers to build internal standardizations atop tested guidance. This ensures the use of consistent coding standards across your organization.

3. Generates an immediate impact

Our secure coding guidelines minimize the number of costly and time-wasting defects by showing developers how to produce secure software. They are also easy to deploy and use, so you'll recognize the benefits quickly.

Our list of guidelines is extensive in order to address the many source code vulnerabilities.

We have the expertise, tools, and services you need

Our guidelines aggregate over 23 years of our software security know-how with best-in-breed industry standard sources. We also continue to invest in internal research to ensure our content is up-to-date as vulnerabilities and remediation approaches evolve.

Our secure coding standards cover the following topic areas:

- Secure input handling
- Secure output handling
- Access control
- Secure session management
- Secure data transmission and storage

A tailored approach

As needed, we offer customized guidelines to address:

- Additional development languages / frameworks of interest
- Additional vulnerability types discovered
- Custom in-house security frameworks
- In-house coding standard integration

Frameworks and languages

- .Net
- C/C++
- COBOL
- JAVA
- Java Web Services
- MEAN
- Ruby on Rails
- Web 2.0 (HTML5, JavaScript)
- PHP

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com