AppCurity Secure Coding Guidelines

Enable developers with trustworthy and actionable secure coding guidance

AppCurity's Secure Coding Guidelines show developers how to produce secure software, minimizing the number of costly and timewasting defects. Our guidelines offer technology-specific risk explanations, best practices and reusable code examples.

Vetted secure coding expertise

Our guidelines provide developers the framework, library and language-specific advice they need to produce secure software and remediate vulnerability backlogs. These guidelines aggregate 30 years of AppCurity software security know-how with best-in-breed industry standard sources. And we continue to invest in internal research to ensure our content is up to date as vulnerabilities and remediation approaches evolve.

Cost-effective secure coding knowledge

Our guidelines offer a cost-effective educational reference for development teams. This bridges the comprehension barriers between vulnerability tools and developers' remediating findings. It also enables developers to build internal standardizations atop tested guidance.

AppCurity's Secure Coding Guidelines include:

- ✓ Risk prevention
- ✓ Risk mitigation
- ✓ Developer education
- ✓ Accessibility of knowledge
- ✓ Standardization of secure coding techniques
- ✓ How to address third-party secure coding expectations such as regulators

Technologies covered by AppCurity's Secure Coding Guidelines

- Java
- Java Web Services
- .Net
- C/C++
- Web 2.0 (HTML5 and JavaScript)
- Ruby on Rails

The benefits of using AppCurity's Secure Coding Guidelines

Benefits	Attributes
Enables developers	• Actionable and comprehensive guidance • Written by and for developers
Creates efficiencies through standard coding practices	• Consistent coding standards usage across organization • Blueprint for creating security requirements
Generates an immediate impact	• Ease of deployment and use • Cost-effective

There are language-specific details related to:

- Validate user input from HTTP requests before use
- Escape untrusted data before using in LDAP queries
- Validate untrusted XML input before use
- Web messaging API should validate message data
- Sanitize JSONP's callback method parameter
- Restrict public access to WSDL files
- Data in HTML5 localStorage should be cleared after use
- And more…

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

We customize too

As needed, AppCurity offers the customized guidelines to address:

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

We can also publish guidelines to your internal software security portal with navigation ability.

The AppCurity Difference

AppCurity is a leader in application and software security. We go beyond traditional testing services to help organizations find, fix and prevent vulnerabilities in the applications that power their business. Our holistic approach to application security offers a balance of managed services, professional services and products tailored to fit your specific needs. 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 applications.