31 SECURITY TIPS FOR DEVELOPERS

SEE HOW #SECUREDEVAWARE YOU ARE

Never trust user input - All user input should be considered ‘evil’ until validated otherwise.

#1 TOP TIP

Perform threat modeling before testing to tell you where to focus your testing.

#2 TOP TIP

Consider storing business logic code on the server side.

#3 TOP TIP

Use a layered approach to security testing to dramatically cut down on security issues before deployment.

#4 TOP TIP

Use generic error messages like “Incorrect username or password” to keep brute force attacks at bay. Never tell the user what the wrong data was.

#5 TOP TIP

Consider breaking the build for medium and high risk findings and never ship with potentially dangerous vulnerabilities.

#6 TOP TIP

Using third-party code? Either run security tests on the original code or insist on a security analysis report from the code supplier.

#7 TOP TIP

Apply a hashing algorithm using salt to your user’s passwords before storing them in your database.

#8 TOP TIP

Separate your application's dynamic content from its static content.

#9 TOP TIP

Test your code throughout the SDLC to save time and money in the long run.

#10 TOP TIP

Implement two-factor authentication wherever possible and logical.

#1 MOBILE SECURITY

Limit application permissions only to components required for the app to function properly.

#2 MOBILE SECURITY

Implement SSL or TLS and ensure HTTPS is used.

#3 MOBILE SECURITY

Invalidate user sessions upon logout or after a certain length of time.

#4 MOBILE SECURITY

Protect user interface data and user credentials by storing them properly using encryption.

#5 MOBILE SECURITY

Ensure your app meets all necessary regulatory and compliance requirements, especially for financial and health apps.

#6 MOBILE SECURITY

Don’t allow third party keyboard use for iOS apps when sensitive content is entered.

#7 MOBILE SECURITY

Involve the security team in your feedback loop, offering your feedback and requesting theirs on the current state of security in your builds.

#1 AGILE SECURITY

Integrate security processes as early as possible in your build process to cut back on time spent fixing issues later.

#2 AGILE SECURITY

Teach the security team about how your team writes code, so they can better understand how and where security can be integrated.

#3 AGILE SECURITY

Establish a shared discipline of agile development between the developer, operations, and security - throughout the SDLC.

#4 AGILE SECURITY

Push smaller releases more often to lower the overall risk posture of the applications.

#6 AGILE SECURITY

Analyze security practices and tools in your agile retrospectives and adapt accordingly.

#7 AGILE SECURITY

Take advantage of online games and ‘vulnerable’ sites designed to be hacked to test your AppSec knowledge and improve your skills.

#1 EDUCATION

Dive into the OWASP Top 10 and learn all you can about the 10 most dangerous vulnerabilities that should be prevented or fixed in code.

#2 EDUCATION

Find yourself interested and excited about AppSec? Volunteer as a security evangelist and help teach other developers.

#3 EDUCATION

Develop a work relationship with a member of the security team who you feel comfortable asking security questions and answering coding questions.

#4 EDUCATION

Get involved in the threat modeling process to better understand the risks involved in application design and development.

#5 EDUCATION

Learn how to use the security tools whether you get formal training or not – educating yourself in secure coding will take you further in your career!

#6 EDUCATION

Head to local OWASP meetings for interesting security discussions (and usually free food and/or beer!)

#7 EDUCATION

Visit **securedevkit.com** for more resources on secure coding best practices.

CHECKMARX

Application Security Made Easy