31 Tips to Keep You #SecureDevAware

Top Tips for Application Security

1. Never trust user input - All user input should be considered 'evil' until validated otherwise.
   https://www.checkmarx.com/wp-content/uploads/2015/10/1.jpg

2. Perform threat modeling before testing to tell you where to focus your testing.
   https://www.checkmarx.com/wp-content/uploads/2015/10/2.jpg

3. Consider storing business logic code on the server side.
   https://www.checkmarx.com/wp-content/uploads/2015/10/3.jpg

4. Use a layered approach to security testing to dramatically cut down on security issues before deployment.
   https://www.checkmarx.com/wp-content/uploads/2015/10/4.jpg

5. 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.
   https://www.checkmarx.com/wp-content/uploads/2015/10/5.jpg

6. Consider breaking the build for medium and high risk findings, and never ship with potentially dangerous vulnerabilities.
   https://www.checkmarx.com/wp-content/uploads/2015/10/6.jpg

7. Using third-party code? Either run security tests on the original code or insist on a security analysis report from the code supplier.
   https://www.checkmarx.com/wp-content/uploads/2015/10/7.jpg

8. Apply a hashing algorithm using salt to your user's passwords before storing them in your database.
   https://www.checkmarx.com/wp-content/uploads/2015/10/8.jpg

9. Separate your application's dynamic content from your static content.
   https://www.checkmarx.com/wp-content/uploads/2015/10/9.jpg

10. Test your code throughout the SDLC to save time and money in the long run.
    https://www.checkmarx.com/wp-content/uploads/2015/10/10.jpg

Tips for Mobile Security

1. Implement two-factor authorization wherever possible and logical.
   https://www.checkmarx.com/wp-content/uploads/2015/10/11.jpg

2. Limit application permissions only to components required for the app to function properly.
   https://www.checkmarx.com/wp-content/uploads/2015/10/12.jpg

3. Implement SSL or TLS and ensure HTTPS is used.
   https://www.checkmarx.com/wp-content/uploads/2015/10/13.jpg

4. Invalidate user sessions upon logout or after a certain length of time.
   https://www.checkmarx.com/wp-content/uploads/2015/10/14.jpg

5. Protect user interface data and user credentials by storing them properly using encryption.
   https://www.checkmarx.com/wp-content/uploads/2015/10/15.jpg

6. Ensure your app meets all necessary regulatory and compliance requirements, especially for financial and health apps.
   https://www.checkmarx.com/wp-content/uploads/2015/10/16.jpg

7. Don't allow third party keyboard use for iOS apps when sensitive content is entered.
   https://www.checkmarx.com/wp-content/uploads/2015/10/17.jpg

Tips for Robust Agile Security

1. Involve the security team in your feedback loop, offering your feedback and requesting theirs on the current state of security in your builds.
   https://www.checkmarx.com/wp-content/uploads/2015/10/18.jpg

2. Integrate security processes as early as possible in your build process to cut back on time spent fixing issues later.
   https://www.checkmarx.com/wp-content/uploads/2015/10/19.jpg

3. Teach the security team about how your team writes code, so they can better understand how and where security can be integrated.
   https://www.checkmarx.com/wp-content/uploads/2015/10/20.jpg

4. Establish a shared discipline of agile development between the develop, ops, and security - throughout the SDLC.
   https://www.checkmarx.com/wp-content/uploads/2015/10/21.jpg

5. Automate as much as possible - including security processes using tools that integrate with your own.
   https://www.checkmarx.com/wp-content/uploads/2015/10/22.jpg

6. Push smaller releases more often to lower the overall risk posture of the applications.
   https://www.checkmarx.com/wp-content/uploads/2015/10/23.jpg

7. Analyze security practices and tools in your agile retrospectives and adapt accordingly.
   https://www.checkmarx.com/wp-content/uploads/2015/10/24.jpg

Tips on Security Awareness and Education

1. Take advantage of online games and 'vulnerable' sites designed to be hacked to test your AppSec knowledge and improve your skills.
   https://www.checkmarx.com/wp-content/uploads/2015/10/25.jpg

2. 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.
   https://www.checkmarx.com/wp-content/uploads/2015/10/26.jpg

3. Find yourself interested and excited about AppSec? Volunteer as a security evangelist and help teach other developers.
   https://www.checkmarx.com/wp-content/uploads/2015/10/27.jpg

4. Develop a work relationship with a member of the security team who you feel comfortable asking security questions and answering coding questions.
   https://www.checkmarx.com/wp-content/uploads/2015/10/28.jpg

5. Get involved in the threat modeling process to better understand the risks involved in application design and development.
   https://www.checkmarx.com/wp-content/uploads/2015/10/29.jpg

6. Learn how to use the security tools whether you get formal lessons or not - educating yourself in secure coding will take you further in your career!
   https://www.checkmarx.com/wp-content/uploads/2015/10/30.jpg

7. Head to local OWASP meetings for interesting security discussions (and usually free food and/or beer!)
   https://www.checkmarx.com/wp-content/uploads/2015/10/31.jpg