I'm new to application security...where should I start?

We strongly recommend you to look at some quick guidelines such as:
- Watch the APPEC tutorial series to get you started.
- OWASP Top Ten: the classic guidelines
- OWASP Cheat Sheets to get into the stuff without getting annoyed

I want to use pen testing tools to ‘hack’ my apps and test for vulnerabilities

If you want to get into pen testing, some cool tools will help you to learn more about it, and they can assist you with testing your website.
- OWASP ZAP: an attack proxy, crema de la creme tool for hacking your site
- OWFIS: A complete pen testing framework which includes test cases and is aligned with OWASP TWS
- Xenotek Exploit: Invade into XSS with this tool

Is there a checklist to make sure I don't forget anything?

OWASP ASVS is the ‘kit’ you can apply to your development process. The OWASP Application Security Verification Standard (ASVS) Project provides a baseline for testing web application technical security controls.

The Secure Coding Practices Quick Reference Guide is a technology agnostic set of general software security coding practices, in a comprehensive checklist format, that can be integrated into the development lifecycle. It contains over 170 pages long, it is easy to read and digest.

How can I check for vulnerable libraries in my application?

Keeping up to date with the latest vulnerabilities is not easy, let alone finding them in your dependency libraries. What about a tool that helps you check this automatically?

Dependency-Check is a utility for identifying project dependencies and checks if there are any dependencies that are vulnerable.
- Currently Java, .NET, and Python dependencies are supported. This tool is used as part of a solution to the OWASP top 10 2013

What about a Developer’s Guidelines?

The OWASP Developer Guide is the original book that was first published in 2002, when Ajax was only a mote in Microsoft’s eye with the new e-mail notification in Outlook. Since then, it has come a long way.

I want to see vulnerabilities and learn how they happen...

We have some cool ‘vulnerable applications’ to learn how you should not code them:
- Security Shepherd: Great app for understanding vulnerable web apps including lessons
- WebGest: OWASP classic, jShark vulnerable site with lessons, all solutions can be found in YouTube videos
- OWASP Bricks: A PHP vulnerable site with lessons

OK. Is time to secure my site!

If you are looking for specific code libraries to protect your application against some nasty vulnerabilities and attacks, there are some great ones.
- Appenser: Intrusion detection for your site
- OWASP HTMLD: Spotted is written in Java which allows you to include HTML, authored by third-parties in your web application while protecting against XSS
- CSRFGuard: Protect your site against CSRF attacks

I want to analyse my code deeper...

OWASP has also Guidelines and Static Analysis tools like:
- Code Review Guidelines: How to check and review your code for common vulnerabilities
- Q2 Platform: Static Analysis tool which can also be a very powerful prototyping and fast development tool for .NET

Check more projects
Visit OWASP projects wiki page to learn more about application security:
https://www.owasp.org/index.php/Category:OWASP_ProjectsWiki_Project_Inventory