A Quick Developer's Guide

To OWASP Projects

Learn how to secure your web applications against the most common web vulnerabilities

OWASP

2015

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

#1

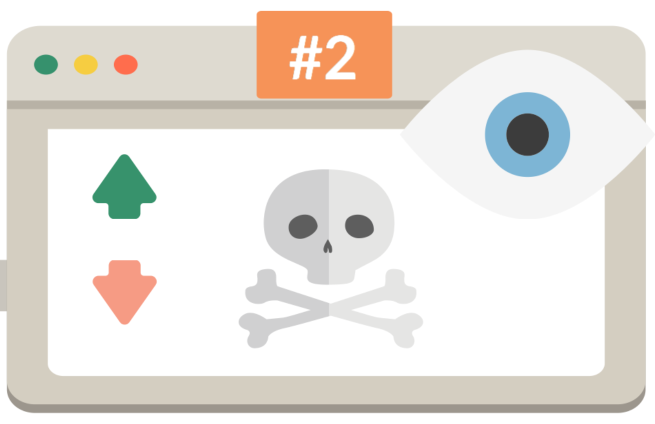
We strongly recommend you to look at some quick guidelines such as:

Watch the APPSEC 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 'see' vulnerabilities and learn how they happen...



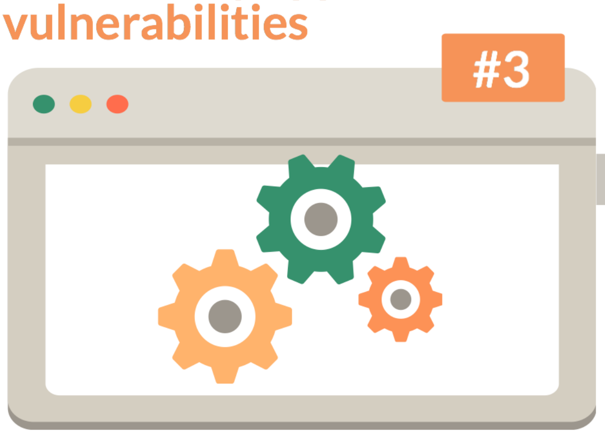
We have some cool 'vulnerable applications' to learn how you should not code them:

Security Shepherd: Great app for understanding vulnerable web apps including lessons

WebGoat: OWASP classic JAVA vulnerable site with lessons, all solutions can be found in Youtube videos

OWASP Bricks: A PHP vulnerable site with lessons

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



If you wan 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 , creme de la creme tool for hacking your site

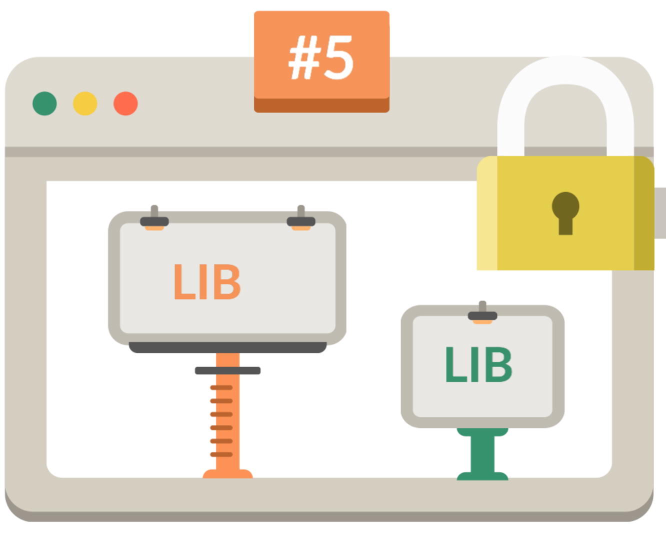
OWTF: A complete pen testing framework which includes test cases and it's aligned with the latest security standards

Xenotix Exploit: Indulge into XSS with this tool

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

OWASP ASVS is 'the list' you can apply to your development process. The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security control

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. At only 17 pages long, it is easy to read and digest.



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, here are some great ones:

Appsensor: Intrusion detection for your site

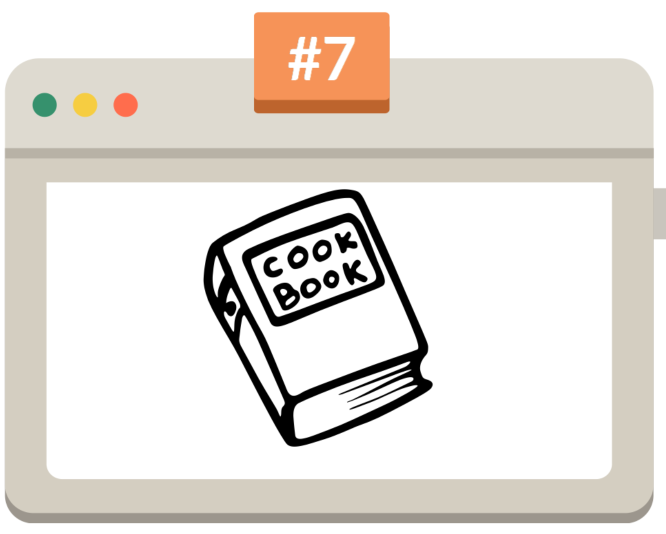
OWASP HTML Sanitizer is written in Java which lets you include HTML authored by third-parties in your web application while protecting against XSS

CRSFGuard: Protect your site against CRSF attacks

How can I check for vulnerable libraries in my application?

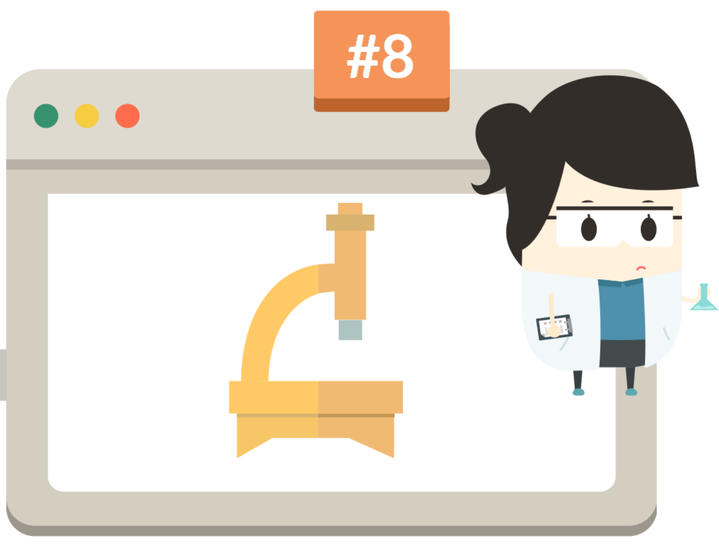
Keeping up to date with the latest vulnerabilities is not easy, let alone finding them in your dependency libraries . What about a tool that helps you check this automatically ?

Dependency-Check is a utility that identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities. Currently Java, .NET, and Python dependencies are supported. This tool can be part of a solution to the OWASP Top 10 2013



What about a Developer's Guidelines?

The OWASP Developer Guide is the original OWASP project. It was first published in 2002, when Ajax was only a mote in Microsoft's eye with the new e-mail notification in Outlook Web Access (and only if you used Internet Explorer). Since then, the web has come a long way.



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

O2 Platform : Strong 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_Project#tab=Project_Inventory