Learning Secure Coding in College?

This document is a modified version of the list I included with handouts for participants in a session at BarCampAlbany 2011 (http://barcamp.org/w/page/21340409/BarCampAlbany), which I have formatted as a web page and to which I have added the following explanatory text:

The topic discussed at this barcamp session was an aspect of the insecure software problem, namely that many programmers are not familiar with how to write secure code. I briefly presented a tactic aimed at a root of this problem, proposing that accreditation of college computer science programs require that secure code be written in all courses for CS majors; and then led a discussion to bring out opinions about the proposal. The idea being that such tactic takes the software insecurity problem as seriously as it deserves, and that implementing the tactic could be straightforwardly phased in over time through usual academic and social processes. For example, one facet might be to require that all programming assignments pass some automated security checker at turn-in, similar to the way homeworks involving coding must pass a plagiarism checker or must compile cleanly with no compiler warnings. That is, security not only as a central topic of maybe one or two courses, but as a real, general concern in all courses. This proposal was stated in more detail in my Letter published on page 6 of the December 2010 issue of **IEEE Computer** magazine, http://www.computer.org/csdl/mags/co/2010/12/mco2010120006.pdf, or via http://www.computer.org/csdl/mags/co/2010/12/index.html.

Note, some of the URLs below include words separated by underscores which may not be visually obvious when displayed in a browser which follows the default of underlining all links

---

This list is URLs of background resources for a session at BarCampAlbany 2011, held at Hudson Valley Community College, Troy, NY on February 19, 2011. Session topic "Learning Secure Coding in College?", led by Tom Reynolds.

FWIW some handouts:

• SANS NewsBites Feb. 1, 2011, section "High School Competition Launched To Fill Pipeline of Skilled Cyber Pros":
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=13&issue=9

• http://www.theregister.co.uk/2007/03/29/secure_coding_tests/print.html
(about those exams: http://www.sans-ssi.org/blueprint.php (not handed out))

• http://blogs.oracle.com/security/2008/11
/training_development_staff_in_secure_coding_practices_pays_huge_dividends.html

• http://www.computerweekly.com/Articles/2008/03/17/229885/Making-software-secure-from-first-principles.htm?printerfriendly=true

• https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices
(and for extra credit, what do you see in the photo of the parking lot security gate?)

• http://www.computerweekly.com/Articles/2008/03/17/229883/Seven-categories-of-software-security-flaws.htm?printerfriendly=true

• https://www.securecoding.cert.org/confluence/display/seccode/AA.+Bibliography
(handout p.1 of 70+/- pages)

• http://www.owasp.org/index.php/OWASP_Podcast
(ho p.1 only)

• http://www.cigital.com/silverbullet/
(ho p.1 only) (another software security podcast)

• http://www.owasp.org/index.php/Secure_Coding_Principles
(ho p.1 only)

• http://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
(ho p.1 only) (a pdf version is there, too)

• http://www.dwheeler.com/secure-programs/
(ho p.1 only) (free downloadable secure programming book)

• http://wiki.altium.com/display/ADOH/Static+Code+Analysis+-+CERT+C+Secure+Code+Checking
(ho p.1&2 only)

• http://www.cert.org/secure-coding/

• http://www.theregister.co.uk/2010/02/17/top_25_programming_errors/print.html
(ho p.1 only)

• http://cwe.mitre.org/top25/
(ho p.1 only)

• https://buildsecurityin.us-cert.gov/bsi/securecoding.html

FWIW a few more URLs, non-handout:

• Apple's "Secure Coding Guide", 2010 (a pdf version is there, too):
http://developer.apple.com/library/mac/#documentation/Security/Conceptual/SecureCodingGuide/Introduction.html

• Microsoft's "Writing Secure Code" web page:
http://msdn.microsoft.com/en-us/security/aa570401

• OWASP ESAPI (Enterprise Security API), a free, open source, web application security control library:
http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

• "Secure Coding Standards", 2008, by Robert C. Seacord and Jason A. Raifail, at the Software Engineering Institute and CERT/CC at Carnegie Mellon Univ.:
www.ioc.orni.gov/csiirw/07/abstracts/Raifal_Abstract.pdf

• A strong statement about the need for teaching software security in college:
http://blogs.oracle.com/maryanndavidson/2008/04/the_supply_chain_problem.html

• Flawfinder, an automated security checker:
www.dwheeler.com/flawfinder

• self-advertisement: **The Art of War of Cybersecurity**, by Thomas Reynolds:
www.trafford.com/07-1219

this URL: http://www.pair.com/cogitage/SecAccred/somesecurecodingURLs.pdf
web page URL: http://www.pair.com/cogitage/SecAccred/somesecurecodingURLs.html