

What Every (Software) Engineer Needs To Know About Security

-- and --

Where To Learn It

Neil Daswani

<http://www.neildaswani.com>
<http://www.learnsecurity.com>

Is the sky falling? (yet?)

TJX (March 2007)

owns TJ Maxx, Marshalls, and other dept stores

attacks exploited WEP used at branches

over 47 million credit card (CC) #s dating back to 2002

CardSystems (June 2005)

credit card payment processing company: out of business

263,000 CC #s stolen from database via SQL Injection

43 million CC #s stored unencrypted / compromised

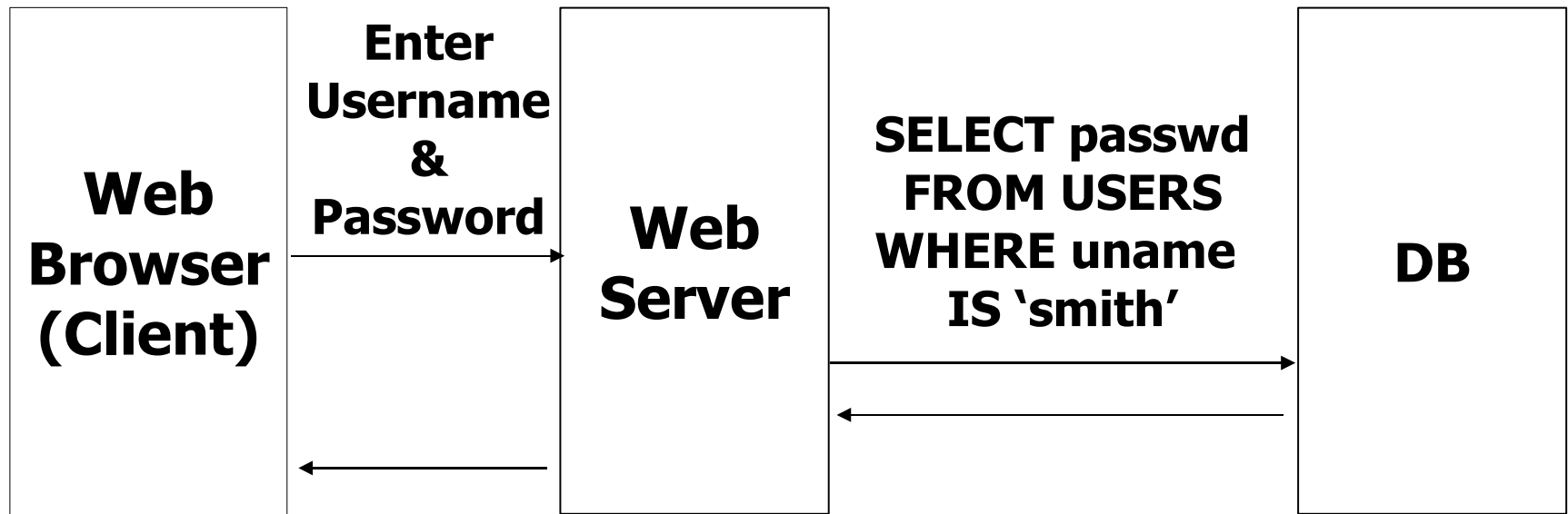
Enter “sql injection” on news.google.com for more...

Additional Data Theft:

www.privacyrights.org/ar/ChronDataBreaches.htm

(153M compromised records; over 300 incidents in 2006 alone)

SQL Injection: Example



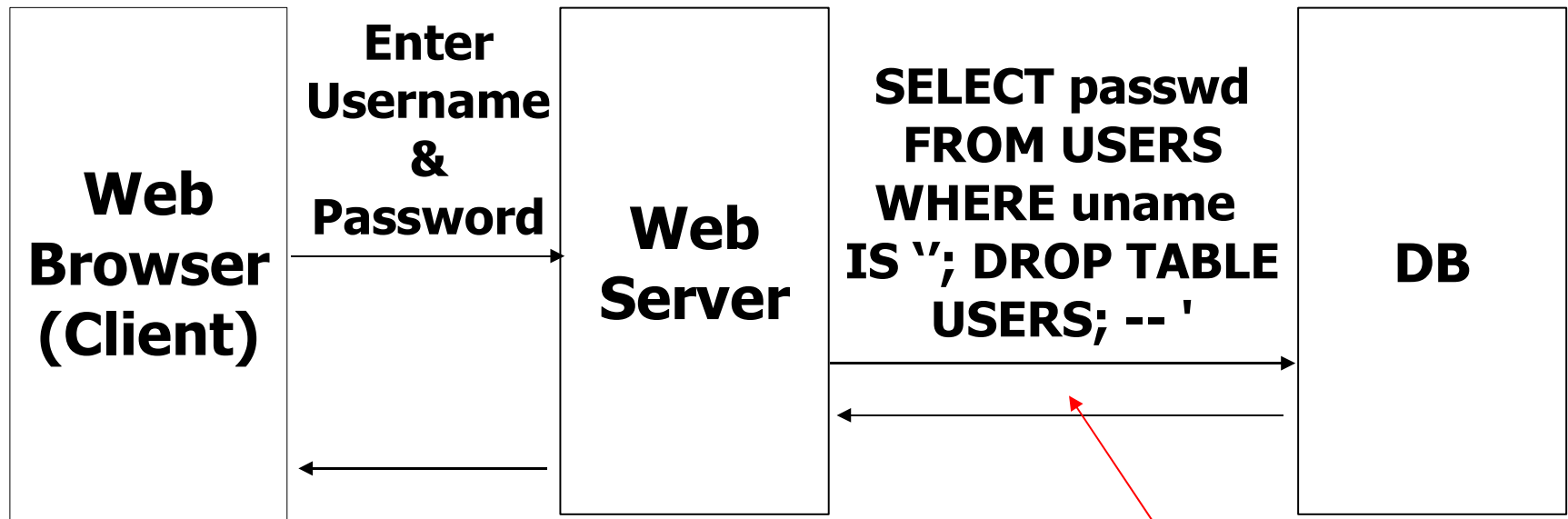
Normal Query

SQL Injection: Example



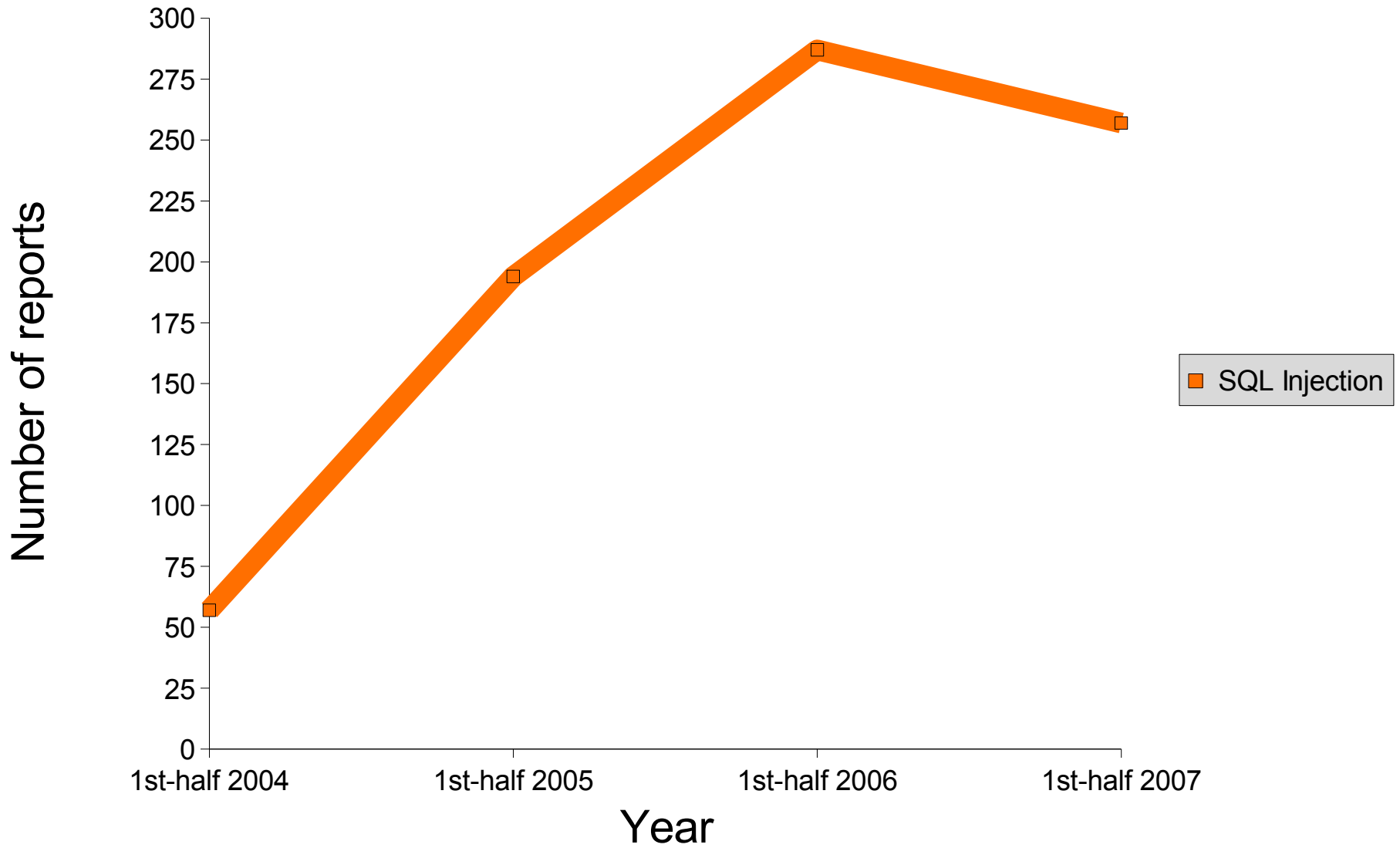
SQL Injection: Example

Malicious Query



Eliminates all user accounts

SQL Injection Trends



Source: securityfocus vulnerability database

Threats Due to Unvalidated Input

SQL Injection is a type of command injection attack possible due to unvalidated input

Others common vulnerabilities are:

- Cross-Site-Scripting (XSS)

- Buffer Overflows

Vulnerabilities Stats

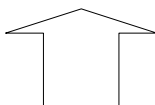
Disclaimer on Categorization

Input Validation

1st-half 2007	1304
1st-half 2006	1294

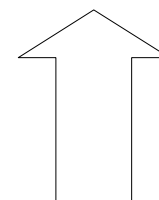
Design Errors

1st-half 2007	295
1st-half 2006	213



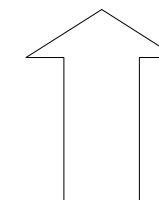
Boundary Conditions

1st-half 2007	417
1st-half 2006	204



Exception Handling

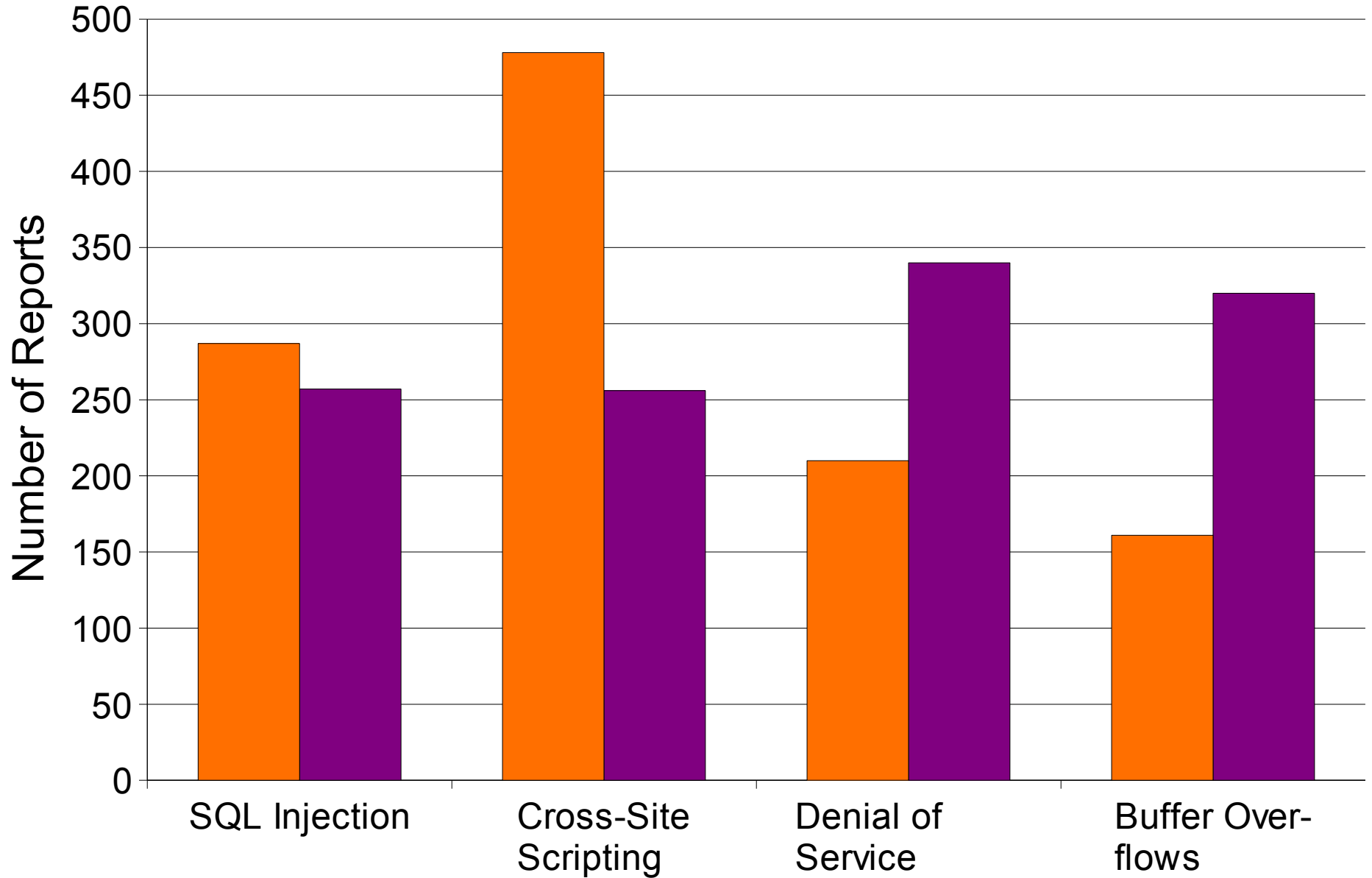
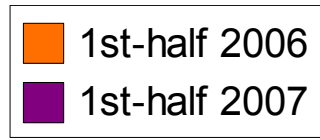
1st-half 2007	206
1st-half 2006	110



Access Validation

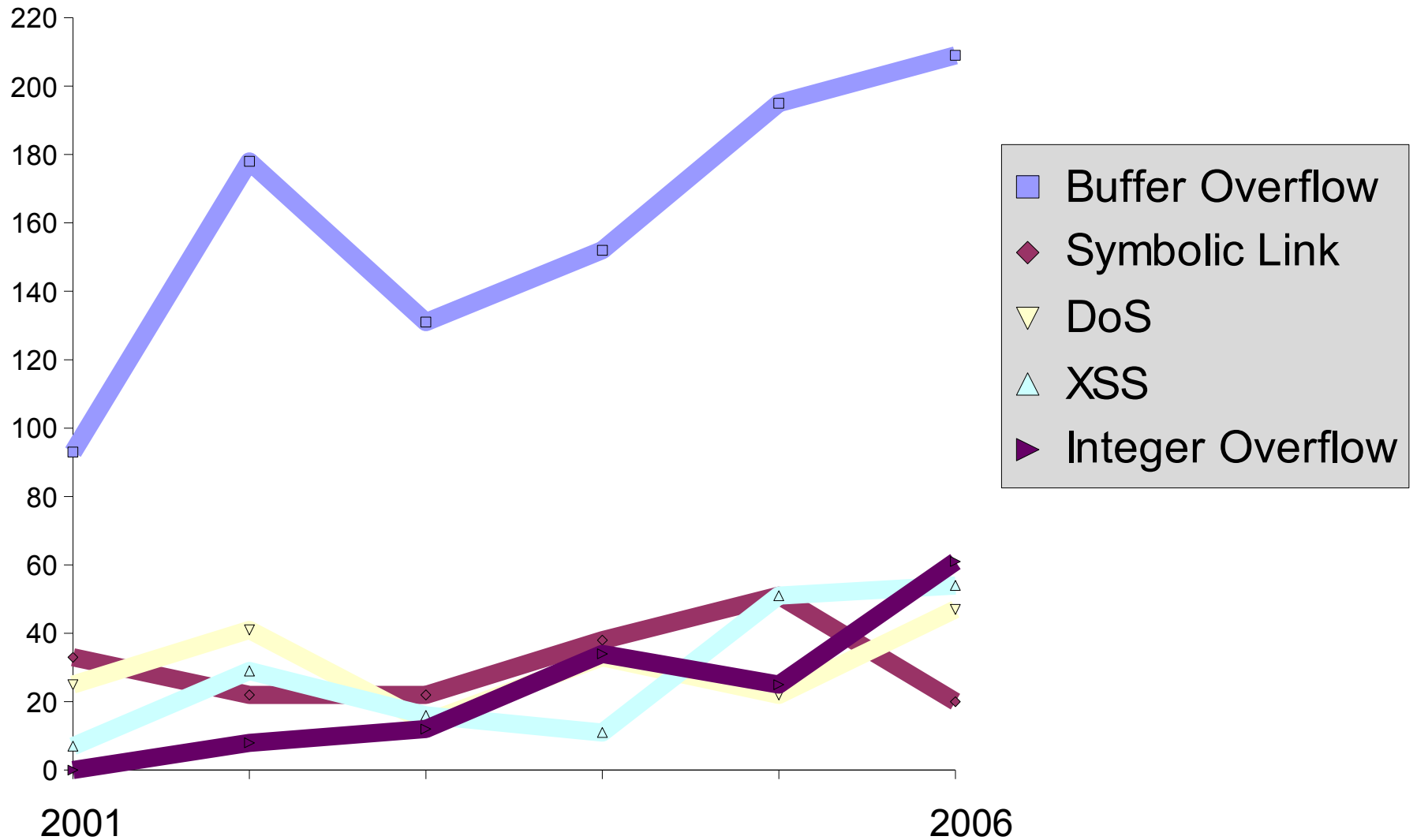
1st-half 2007	87
1st-half 2006	97

Recent Vulnerability Trends

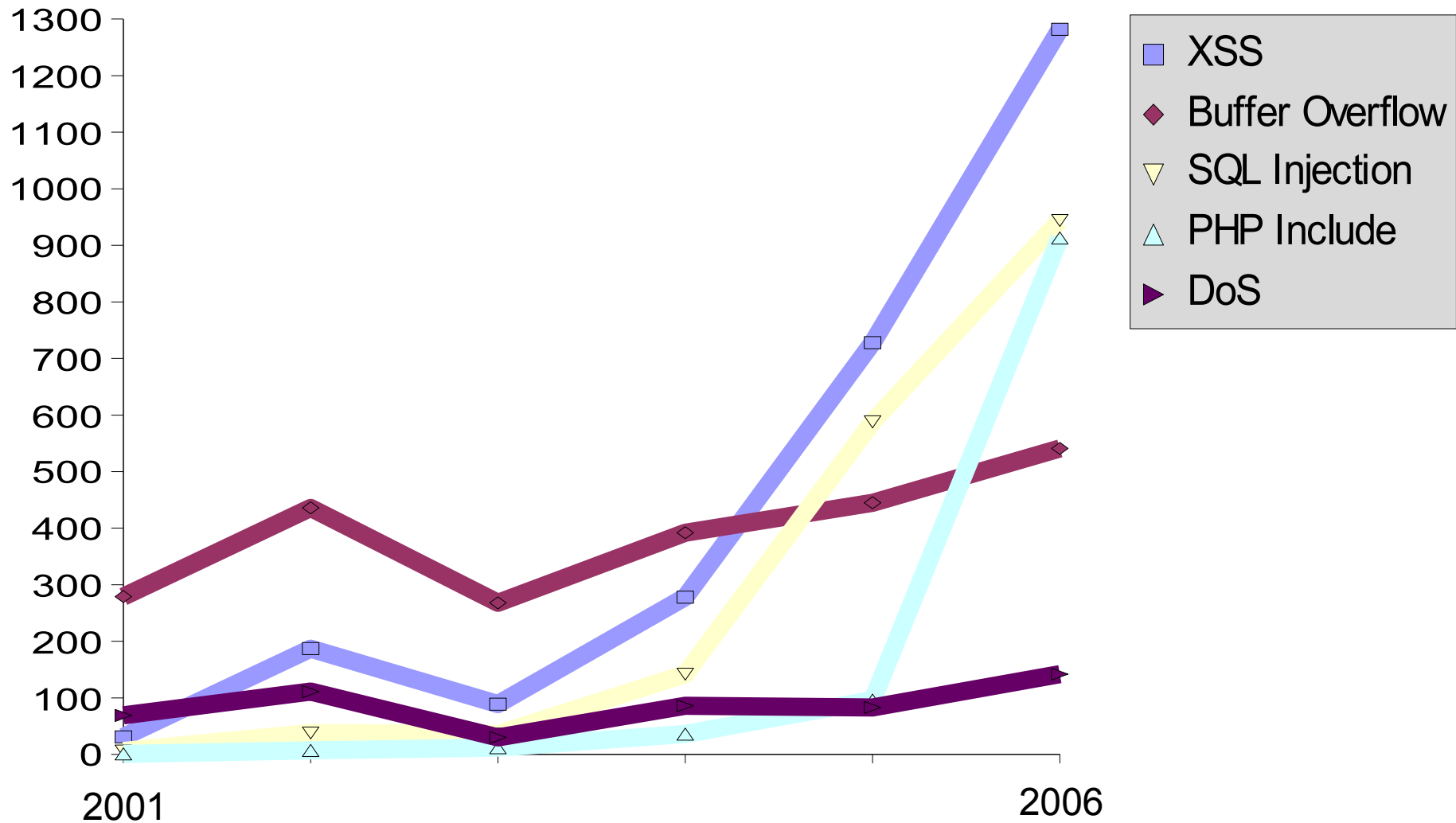


source: securityfocus vulnerability database

Vulnerability Trends (OS Vendors/MITRE)



Vulnerability Trends (Overall/MITRE)



Overall Trends

Detected vulnerabilities are increasing

Big four are about the same
(regardless of vuln database):

- Cross-Site-Scripting (XSS, XSRF, XSSI)

- Injection (SQL, PHP-includes)

- Memory Corruption (buffer overflows, integer overflows, format strings, etc)

- Denial-of-Service

What Every Engineer Needs To Know About Security

Secure Design: least privilege, fail-safe stance, weakest link, etc.

Technical Flaws:

- XSS / XSRF / XSSI
- Injection / Remote Code Execution
- Directory Traversal
- Race Conditions (e.g., TOCTOU)
- Memory Corruption

Attacks:

- Data Theft
- Authentication / Authorization Bypass
- Denial-of-Service
- Privilege Escalation
- Information Leakage

So, where you go to learn this stuff?

Security in Top CS Programs



U.S. News & World Report logo. Search U.S. News. Sunday, July 1, 2007. Nation & World | Health | Money & Business | Education | Opinion | Photos



About the Rankings | Help | Log In
America's Best Graduate Schools 2008
BEST GRAD SCHOOLS INDEX TOOLS ARTICLES
Get the Premium Online Edition Now!
LEARN MORE > BUY! >

Computer Science (Ph.D.)

Ranked in 2006*

Rank/School	Average assessment score (5.0 = highest)
1. Carnegie Mellon University (PA)	5.0
Massachusetts Institute of Technology	5.0
Stanford University (CA)	5.0
University of California-Berkeley	5.0

Security in Top CS Programs: CMU

Carnegie-Mellon University (CMU): B.S. in Computer Science (CS)

Required:

15-100 Introductory/Intermediate Programming and

15-111 Intermediate/Advanced Programming (students with no prior programming experience take

15-123 Effective Programming in C and UNIX

15-128 Freshman Immigration Course

15-211 Fundamental Data Structures and Algorithms

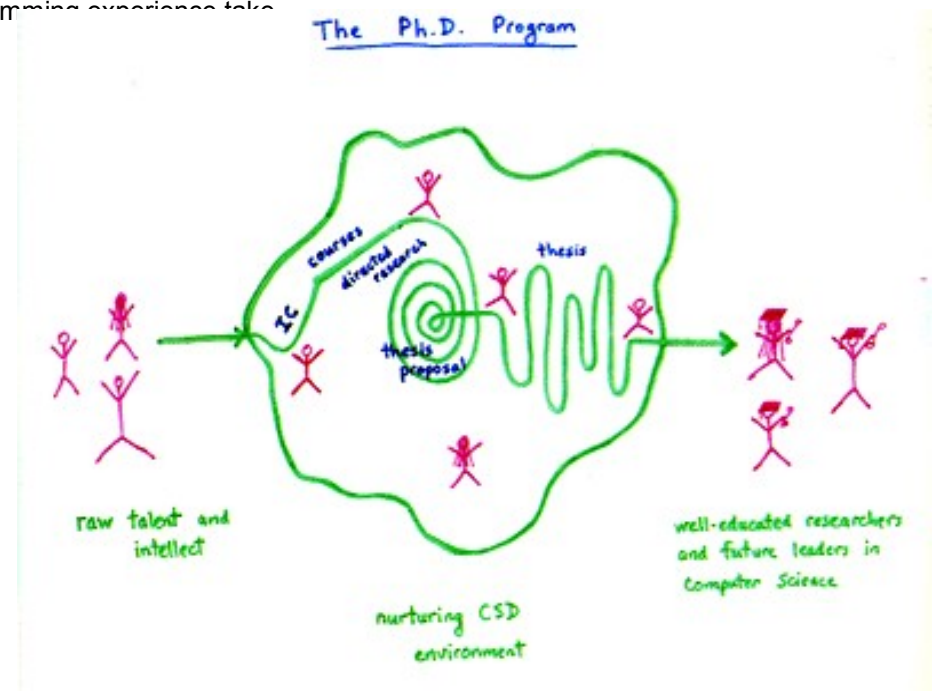
15-212 Principles of Programming

15-213 Introduction to Computer Systems

15-251 Great Theoretical Ideas in Computer Science

15-451 Algorithm Design and Analysis

Security not listed as an elective.



From <http://www.csd.cs.cmu.edu/education/bscs/index.html>

Security in Top CS Programs: MIT

Undergraduate Objectives and Learning Outcomes

The educational objectives of the undergraduate programs of the MIT Department of Electrical Engineering and Computer Science are:

...

2. Students will develop a professional understanding of electrical engineering and computer science so that they are prepared for immediate employment.

...

4. Students will develop an understanding of the importance of the social, business, technical, and human context in which a process or product being designed will work.

From <http://www.eecs.mit.edu/ug/objectives.html>

Security in Top CS Programs: MIT

Computer Science Concentrations

- * Artificial Intelligence and Applications. Header: 6.034. Electives: ...
- * Computer Systems and Architecture Engineering. Header: 6.033. Electives: ...
- * Theoretical Computer Science: Header: 6.046J. Electives: ...

6.033: Computer Systems Engineering (M. F. Kaashoek, H. Balakrishnan)

Security (last two weeks of course)

16. Jonathan Pincus and Brandon Baker. Beyond stack smashing: recent advances in exploiting buffer overruns. IEEE Security and privacy, August 2004.
17. Ross J. Anderson. Why cryptosystems fail. Proceedings of the 1993 ACM Conference in Computer and Communications Security, (1993) pages 32-40.
18. A. Kumar, V. Paxson and N. Weaver. Exploiting Underlying Structure for Detailed Reconstruction of an Internet Scale Event. Proc. ACM IMC, October 2005.
19. Ken Thompson. Reflections on Trusting Trust. Communications of the ACM 27, 8 (August 1984) pages 761-763.

What's the point?

“It has been too long that security has not been part of the required coursework for bachelor degree computer science candidates, and we are seeing some of the effects: software security vulnerabilities plague electronic commerce, resulting in data, identity, and monetary theft as evidenced regularly in the press.” -- Dr. Zvi Galil, Dean of the School of Engineering and Applied Science, Columbia University

Where to learn more?

Courses

Certification Programs

Books

Websites / Organizations

(not comprehensive)

Security Courses

Cryptography Upper Division Courses
(at almost every major university)

Some systems security courses
(e.g., CS155 @ Stanford,
CS161 @ UC Berkeley)

More crypto and security courses listed at:
<http://avirubin.com/courses.html>

Google security courses:
some offered today and more to come...
Contact Mike Wiacek

Stanford Advanced Security Certificate



Online (anytime) or On-Campus (one week)

Next on-campus offering: July 23 - 27

required: 3 core courses; 3 electives

Hands-on labs conducting attacks &
constructing defenses

Security Foundations Certificate also available

Contact:

Stephanie Chiang at in engEDU to sign up!

Stanford Advanced Security Certificate



CORE COURSES

Using Cryptography Correctly

Writing Secure Code

Security Protocols

ELECTIVES

Computer Security Management – Recent Threats, Trends & the Law

Designing/Building Secure Networks

Emerging Threats and Defenses

Securing Web Applications

Systems Security

SPECIAL ELECTIVE

Computer Security Foundations Certificate

Security Certification Programs: CISSP

CISSP (offered by ISC²)

prepares for administration / gov't jobs in security
multiple-choice test

10 domains: Access Control, Application Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security and Risk Management, Legal, Regulations, Compliance and Investigations, Operations Security, Physical (Environmental) Security, Security Architecture and Design, Telecommunications and Network Security

Security Certification Programs: GSSP

GIAC (Global Information Assurance
Certification) Secure Software Programmer
offered by SANS

secure programming assessment

multiple choice (questions in development)

new offering: first exam Aug 14, 2007

Books

Security Engineering

Building Secure Software

Foundations of Security

Hacking Exposed: Web 2.0

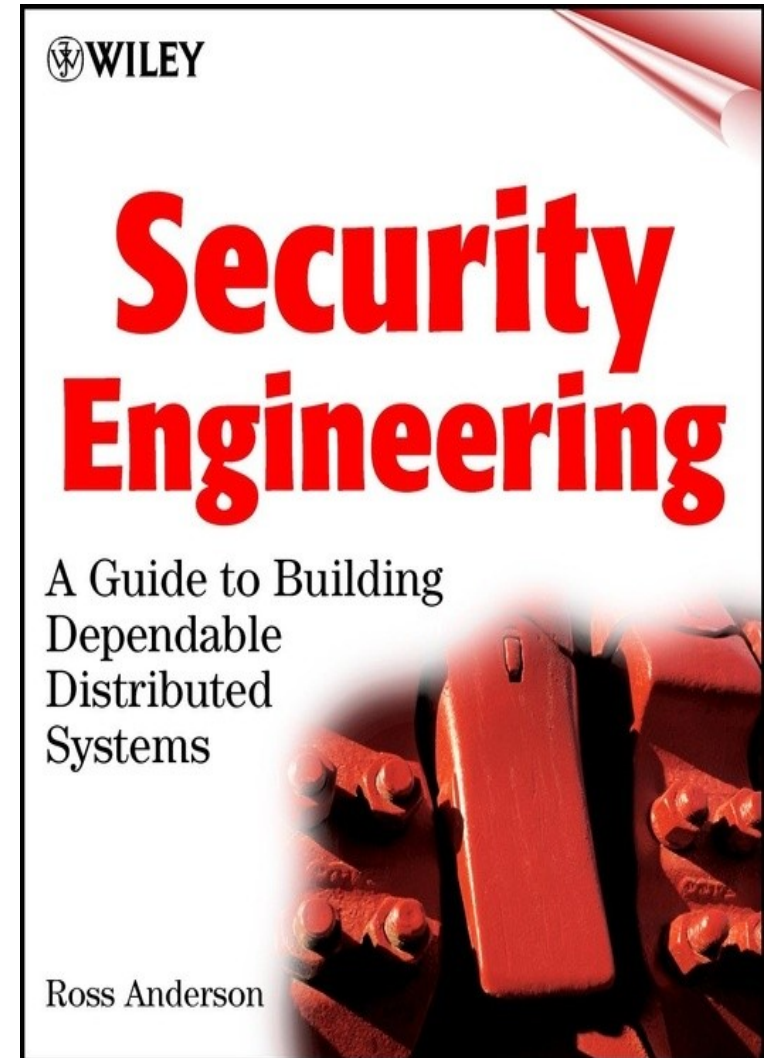
Secure Programming Cookbook

Security Books

Security Engineering

Ross Anderson

Available online
(for free)



<http://www.cl.cam.ac.uk/~rja14/book.html>

Security Books

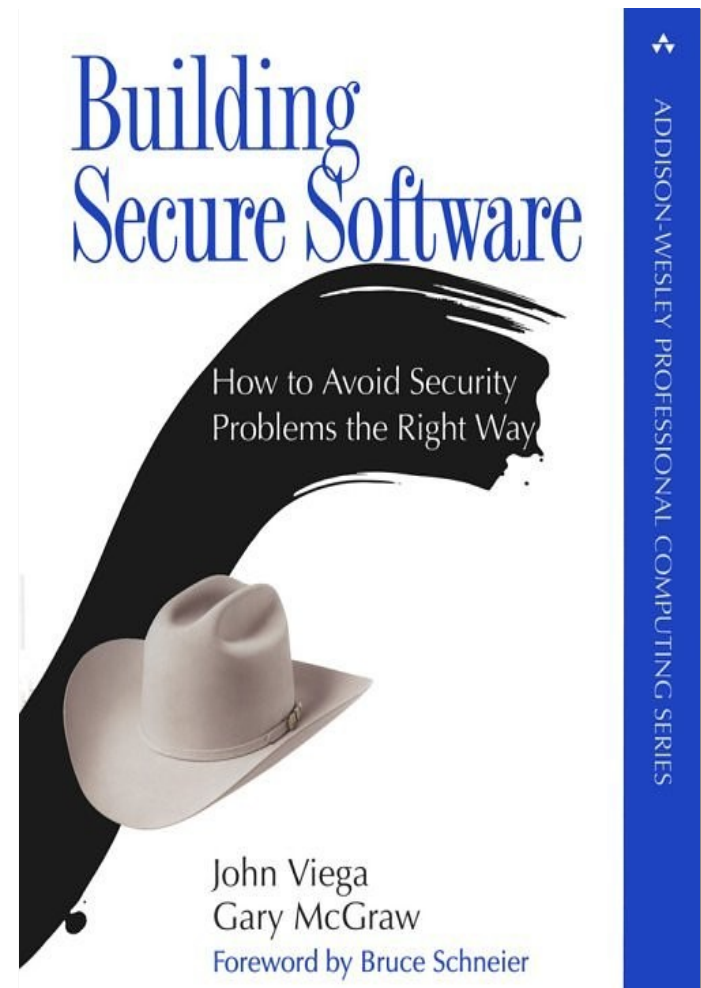
Building Secure Software

Viega / McGraw

“Classic Text”

Other books by
McGraw & Co:

- Exploiting Software
- Software Security



Security Books

Foundations of Security: What Every Programmer Needs To Know

Daswani / Kern / Kesavan

Get your copy from
B46-Anare or B46-284

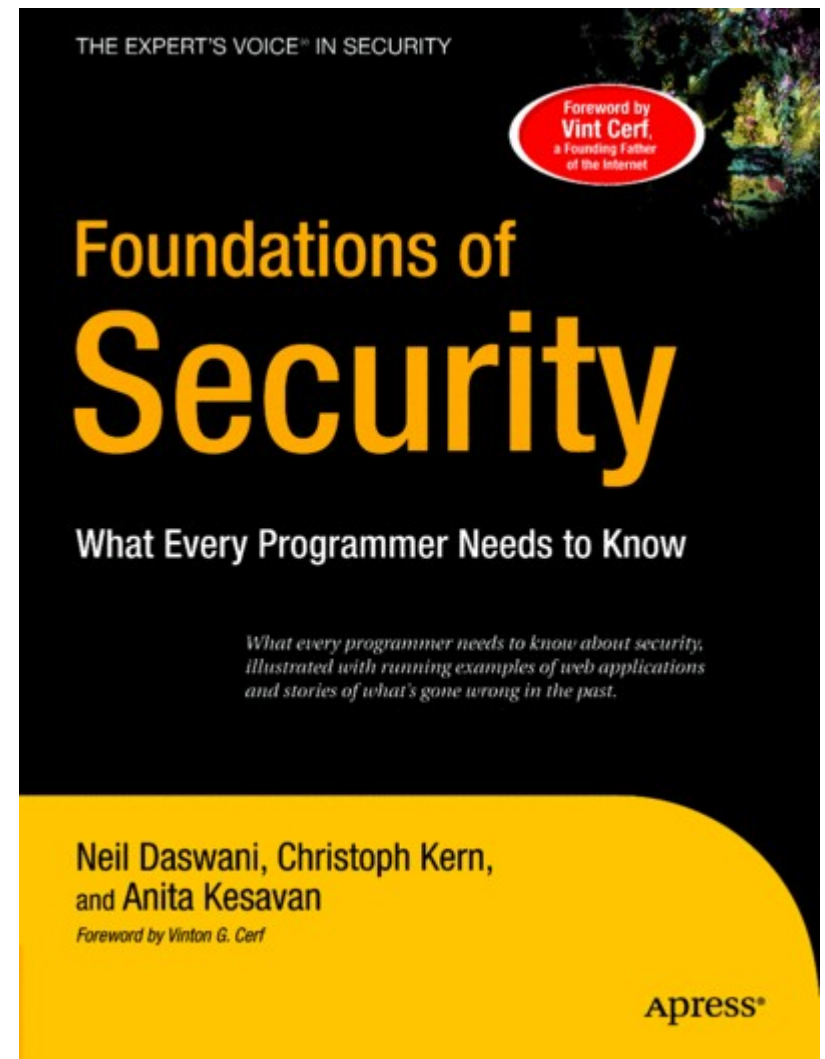
Topics:

- Secure design principles

- Web application
attacks & defenses

- Intro. to Cryptography

Free slides @
www.learnsecurity.com

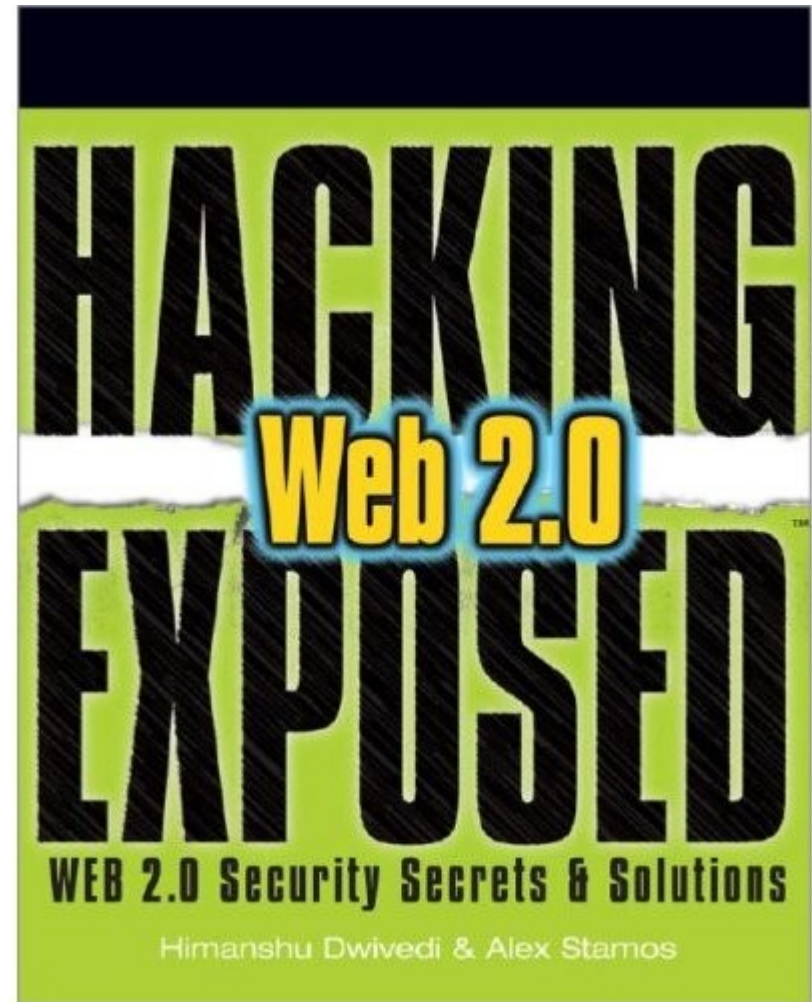


Security Books

Hacking Exposed:
Web 2.0

Dwivedi / Stamos /
Lackey / Cannings

Focuses on attack
patterns. Available
for pre-order.

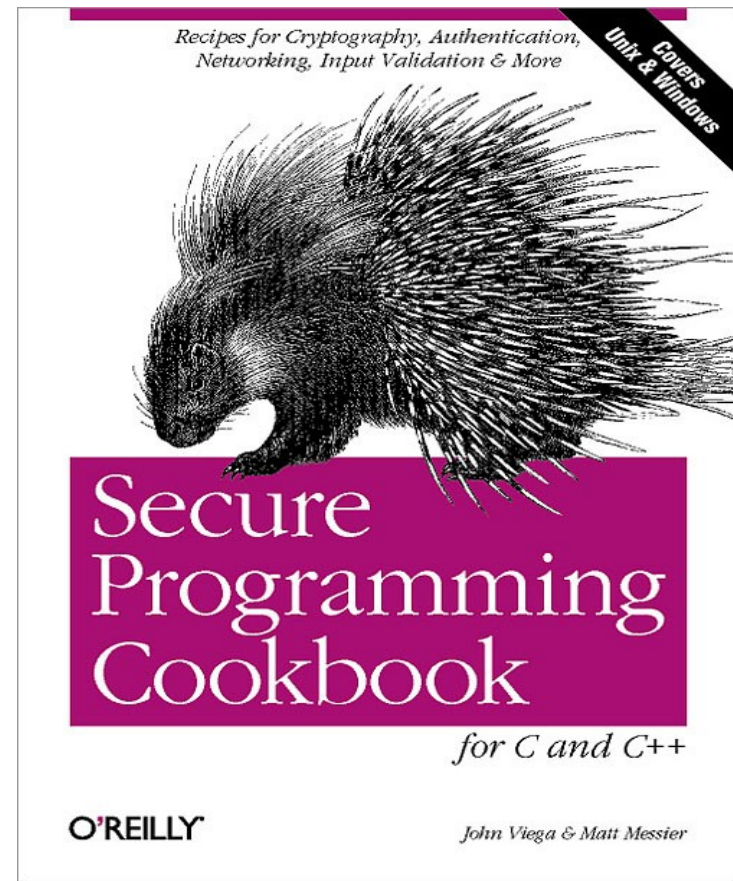


Security Books

Secure Programming Cookbook
for C and C++

Viega / Messier

Lots of code examples
on how to use crypto
correctly



Websites / Organizations

OWASP / Top Ten

www.owasp.org

(chapters in almost every major city)






Security Focus / Bugtraq

www.securityfocus.com






code.google.com/edu

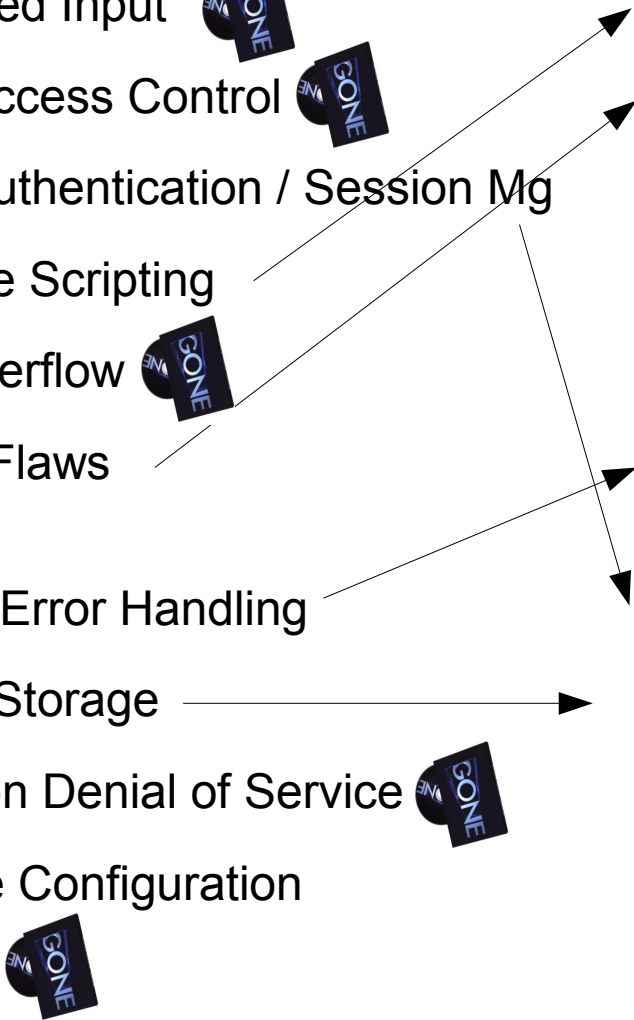
OWASP Top 10

2004

- A1 Unvalidated Input 
- A2 Broken Access Control 
- A3 Broken Authentication / Session Mg
- A4 Cross Site Scripting
- A5 Buffer Overflow 
- A6 Injection Flaws
- A7 Improper Error Handling
- A8 Insecure Storage
- A9 Application Denial of Service 
- A10 Insecure Configuration Management 

2007

- A1 Cross Site Scripting (XSS)
- A2 Injection Flaws (e.g., SQL injection)
- A3 Malicious File Execution (i.e., PHP) 
- A4 Insecure Direct Object Reference 
- A5 Cross Site Request Forgery (CSRF) 
- A6 Information Leakage and Improper Error Handling
- A7 Broken Authentication / Session Mg
- A8 Insecure Cryptographic Storage
- A9 Insecure Communications 
- A10 Failure to Restrict URL Access 



Security Focus

www.securityfocus.com / Home of Bugtraq

Articles / Mailing Lists / Vuln. Reports

Focus areas:

Foundations

Microsoft / Unix

IDS

Incident Response

Viruses / Malware

Penetration Testing

Firewalls

code.google.com/edu: Web Security



Code for Educators

[Home](#)

[CS Curriculum Search](#)

Tutorials

[AJAX Programming](#)

[Distributed Systems](#)

Sample Course
Content

[Distributed Systems](#)

Web Security

Google Code for Educators

[Google Code Home](#) > [Code for Educators](#) > [Sample Course Content](#) > **Web Security**

Web Security

This page contains course material submissions from industry and academia that is designed to help teach web security to students around the world.



[Introduction to Web Security](#)

by Neil Daswani

This submission contains two lectures and a programming assignment that is designed to introduce students to web based security.

[Lectures](#) - [Programming Assignments](#)

Free & available for external use

Ex. DoS against web server

We're looking for additional contributors!

Learn About Security!

Every engineer should be a software security practitioner

Links / Pointers:

<http://www.learnsecurity.com>
Click on “Resources”

Neil Daswani
daswani@learnsecurity.com
<http://www.neildaswani.com>

