

Software Reliability and Security

Module 2

Winter 2017

Presentation/Lecture Schedule and Report Due Dates

- Presentation 1
 - Related background paper
 - Jan 27, Feb 1, 3
- Presentation 2
 - Project proposal
 - March 1, 3, 8
- Presentation 3
 - Final project report
 - March 24, 29, 31
- Lectures
 - Jan 13, 18, 20, 25, 27
 - Feb 1, 3, 8, 10, 15, 17
 - March 1, 3, 8, 10, 15, 17, 22, 24, 29, 31
- Project Proposal Due
Tuesday, February 28
- Final Project Report Due
Monday, April 10
- Final Exam
Wednesday, April 12, 10:00am

Outline

- General Course Information
 - Overview and some preliminary concepts
 - Lecture schedule
 - Topics and references
 - Assessment with report due dates
 - Warm-up presentation
- Software Crisis
 - Reliability and security
 - An assignment – recent incidents about software failures and intrusions
- Course Project
 - Guidelines
 - Some suggested topics

Software's Chronic Crisis

- The phrase "Software Engineering" was introduced by a NATO study group in 1967
 - To address "current" software crisis through "engineering" practices to software development
- "Current" Software Crisis
 - Software projects are late, defective, incomplete (do not provide all functionalities) and get cancelled
- Even today the software crisis is a significant problem that software engineering must address

Software Hall of Shame

SOURCES: *BUSINESS WEEK*, *CEO MAGAZINE*, *COMPUTERWORLD*, *INFOWEEK*, *FORTUNE*, *THE NEW YORK TIMES*, *TIME*, AND *THE WALL STREET JOURNAL* (IEEE Spectrum, 2005)

YEAR	COMPANY	OUTCOME (COSTS IN US \$)
2005	Hudson Bay Co. [Canada]	Problems with inventory system contribute to \$33.3 million* loss.
2004-05	UK Inland Revenue	Software errors contribute to \$3.45 billion* tax-credit overpayment.
2004	Avis Europe PLC [UK]	Enterprise resource planning (ERP) system canceled after \$54.5 million† is spent.
2004	Ford Motor Co.	Purchasing system abandoned after deployment costing approximately \$400 million.
2004	J Sainsbury PLC [UK]	Supply-chain management system abandoned after deployment costing \$527 million.†
2004	Hewlett-Packard Co.	Problems with ERP system contribute to \$160 million loss.
2003-04	AT&T Wireless	Customer relations management (CRM) upgrade problems lead to revenue loss of \$100 million.
2002	McDonald's Corp.	The Innovate information-purchasing system canceled after \$170 million is spent.
2002	Sydney Water Corp. [Australia]	Billing system canceled after \$33.2 million† is spent.
2002	CIGNA Corp.	Problems with CRM system contribute to \$445 million loss.
2001	Nike Inc.	Problems with supply-chain management system contribute to \$100 million loss.
2001	Kmart Corp.	Supply-chain management system canceled after \$130 million is spent.
2000	Washington, D.C.	City payroll system abandoned after deployment costing \$25 million.
1999	United Way	Administrative processing system canceled after \$12 million is spent.
1999	State of Mississippi	Tax system canceled after \$11.2 million is spent; state receives \$185 million damages.
1999	Hershey Foods Corp.	Problems with ERP system contribute to \$151 million loss.
1998	Snap-on Inc.	Problems with order-entry system contribute to revenue loss of \$50 million.
1997	U.S. Internal Revenue Service	Tax modernization effort canceled after \$4 billion is spent.
1997	State of Washington	Department of Motor Vehicle (DMV) system canceled after \$40 million is spent.
1997	Oxford Health Plans Inc.	Billing and claims system problems contribute to quarterly loss; stock plummets, leading to \$3.4 billion loss in corporate value.
1996	Arianespace [France]	Software specification and design errors cause \$350 million Ariane 5 rocket to explode.
1996	FoxMeyer Drug Co.	\$40 million ERP system abandoned after deployment, forcing company into bankruptcy.
1995	Toronto Stock Exchange [Canada]	Electronic trading system canceled after \$25.5 million** is spent.
1994	U.S. Federal Aviation Administration	Advanced Automation System canceled after \$2.6 billion is spent.
1994	State of California	DMV system canceled after \$44 million is spent.
1994	Chemical Bank	Software error causes a total of \$15 million to be deducted from 100,000 customer accounts.

Software Hall of Shame – Reliable?

- **Blackout 2003** (August 14) affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states
 - A race condition bug of GE Energy's Unix-Based XA/21 energy management system stalled automatic alarm
- **Toronto Stock Exchange (TSX) Failure** – down for a whole day
 - "a network firmware issue resulted in data sequencing problem" – May 09
 - "all efforts are being made to ensure that such a disruption in trading does not happen again." – Dec 08
 - Similar outages in **Tokyo** Stock Exchange (TSX) in 1997, 2005, 2006 and twice in 2008.
- **Software failure caused London** tube closure (Nov 2006)

Software Hall of Shame – Reliable?

- The Role of Software in Fifteen Recent Catastrophic Accidents (Wong et al. 2009)
 - Shutdown of the Hartsfield–Jackson Atlanta International Airport, 2006
 - Loss of Communication between the FAA Air Traffic Control Center, and Airplanes, 2004
 - Crash of Air France Flight 447, 2009
 - Crash of Korean Air Flight 801, 2007
 - Crash of American Airlines (AA) Flight 965, 1995
 - ...
- “Air Canada software outage briefly halts computerized check-ins” (CBC, January 17, 2017)
- “Software update, not hackers, caused Customs computer meltdown at airports” (USA Today, January 3, 2017)

Software Hall of Shame – Reliable?

- Trading company Knight shows how to lose \$440 million in 30 Minutes"

45 minutes to identify the problem (10million /minute):
(Bloomberg Businessweek, 2012)

- Software bug made Swedish Exchange Go Bork, Bork, Bork for four hours:

" ... dealing with the increasingly complex web of electronic exchanges and high-frequency trading still is one of the major challenges .." (Bloomberg Businessweek , 2012)

Software Faults and Security Problems

- “the root of most security problems is software that fails in unexpected ways when under attack” (McGraw, 2002)
- “A security failure results from an attack that exploits a vulnerability, where a vulnerability can be viewed as a fault ” (Wolf, 2004)

Software Faults and Security Problems

- Software Reliability is Security (Lindner, 2006)
 - "The science of software testing names software faults according to their root cause. "
 - "Hackers name security issues according to bug class, a type of software defect they are able to exploit."

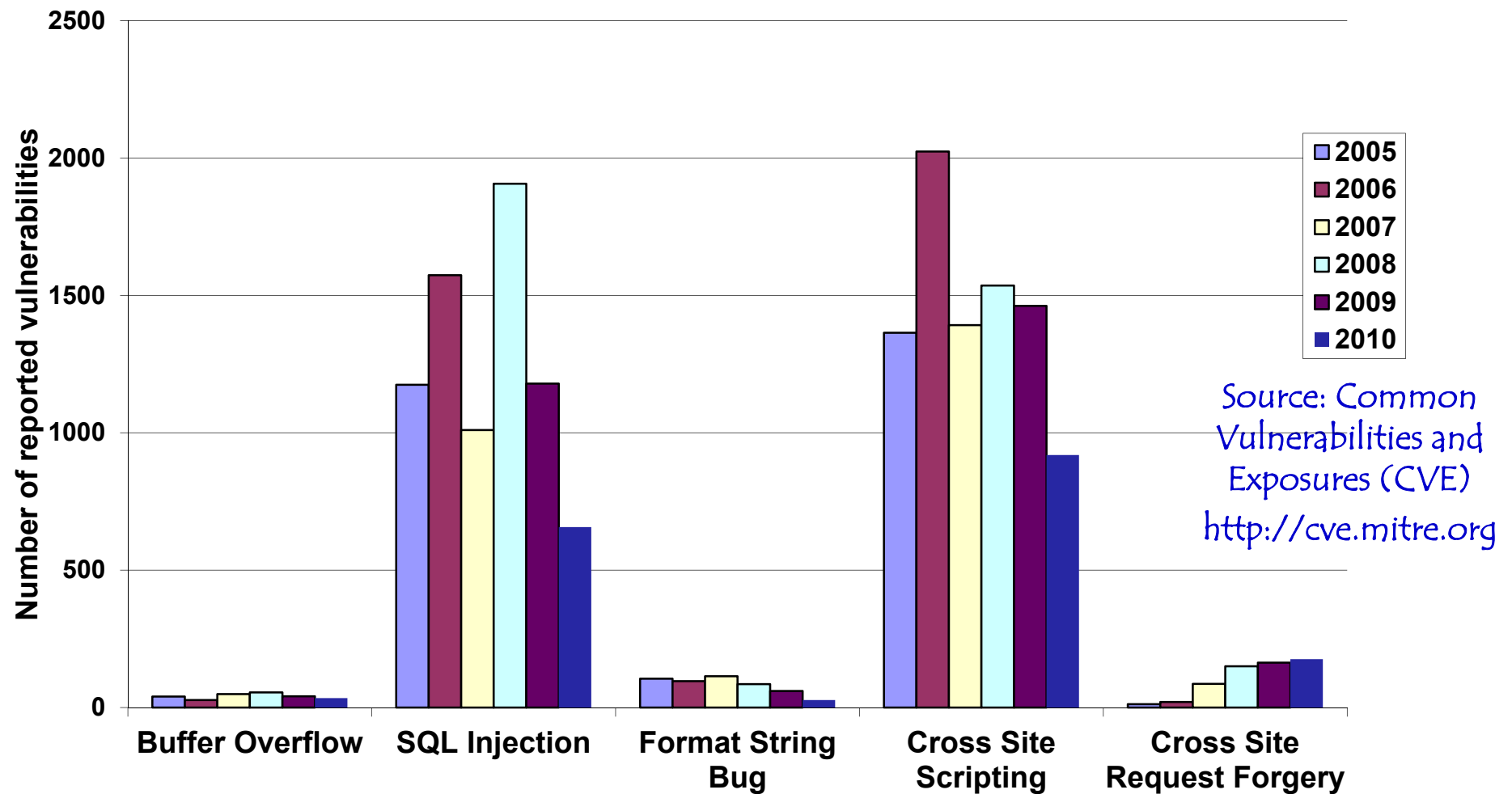
Bug classes	Software faults
Buffer overflow	Data reference failure (or DoS)
Format string bug	Interface failure
SQL Injection	Input/Output error
Cross site scripting	Input/Output error

Software Security?

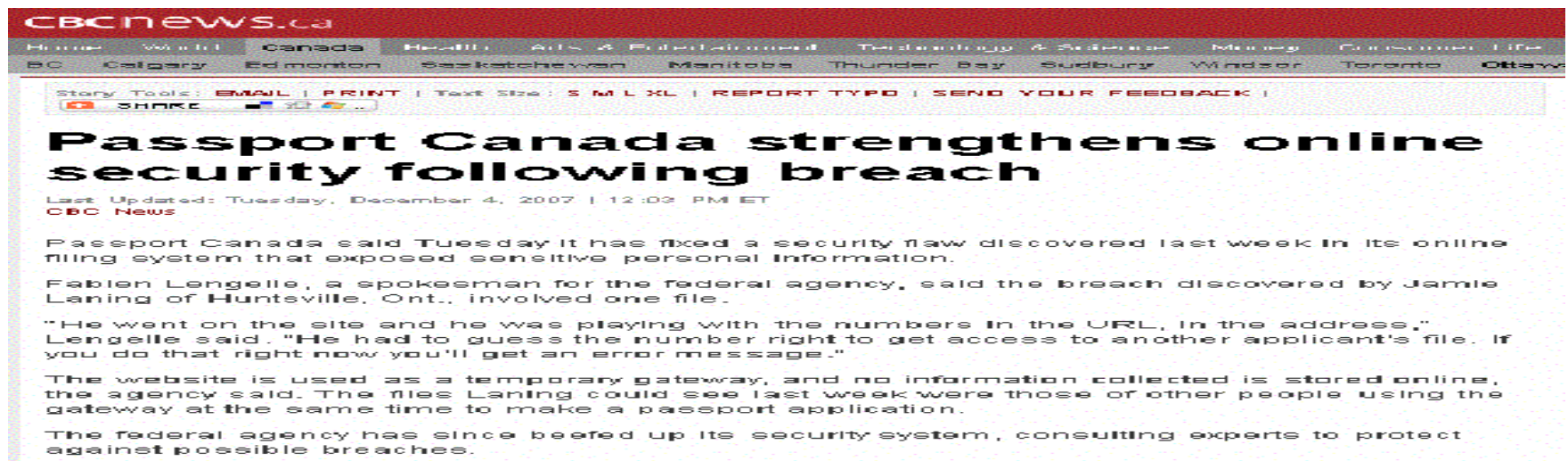
"We wouldn't have to spend so much time and effort on network security if we didn't have such bad software security"

Bruce Schneier

Software Hall of Shame – Secure?



Software Hall of Shame – Information Leakage

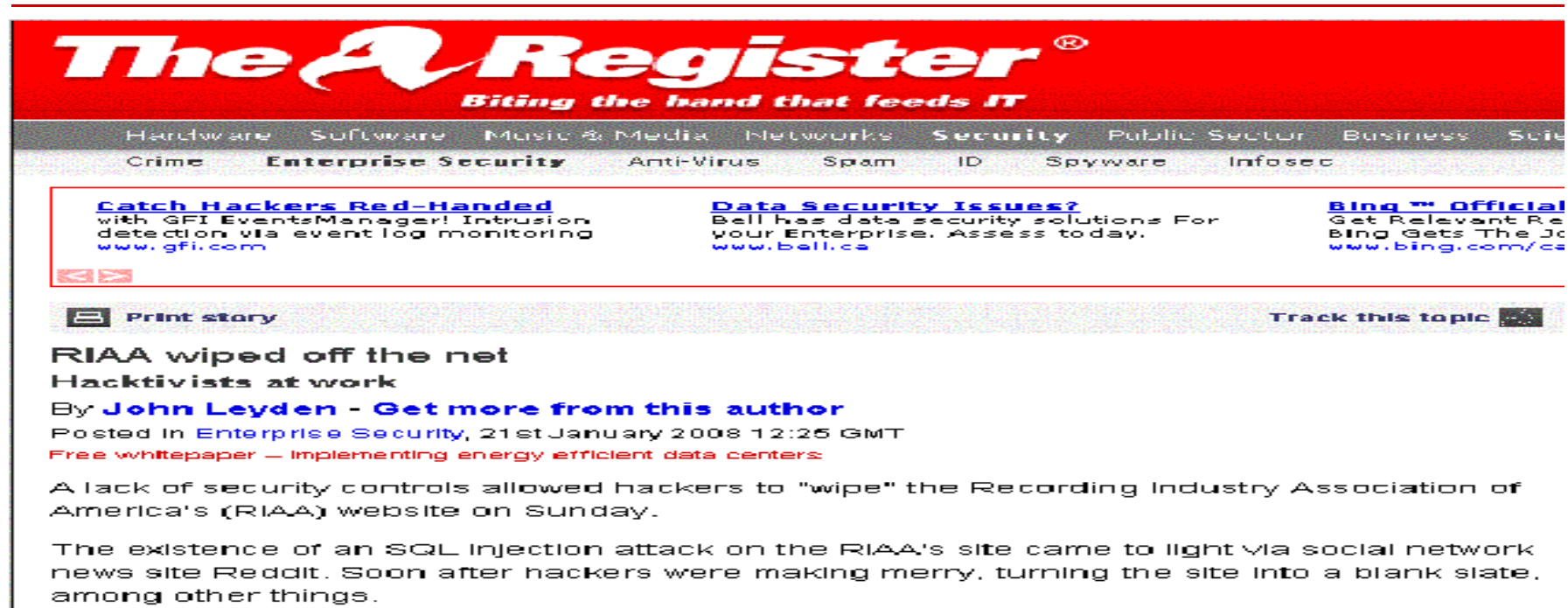


“A security flaw in its online filing system exposed sensitive personal information - guess the number right to get access to another applicant's file.”

"We've tested the system to make sure it's foolproof and we've also sought external help to ensure that applicants' information cannot be accessed through Passport Online," - Passport Canada, Dec 2007

Source: www.cbc.ca/canada/ottawa/story/2007/12/04/passport-security.html

Software Hall of Shame – Information Deletion



The screenshot shows the top of a web browser displaying the homepage of 'The Register'. The site's logo is prominently displayed at the top, followed by a navigation bar with links to various sections: Hardware, Software, Music & Media, Networks, Security, Public Sector, Business, and Site. Below the navigation bar, there are three main content areas. The left area features a headline 'Catch Hackers Red-Handed' with a sub-headline 'with GFI EventsManager! Intrusion detection via event log monitoring' and a link to 'www.gfi.com'. The middle area has a headline 'Data Security Issues?' with a sub-headline 'Bell has data security solutions For your Enterprise. Assess today.' and a link to 'www.bell.ca'. The right area has a headline 'Bing™ Official' with a sub-headline 'Get Relevant Re Bing Gets The Jo' and a link to 'www.bing.com/cs'. Below these areas, there is a 'Print story' button and a 'Track this topic' button. The main article title is 'RIAA wiped off the net' with a sub-headline 'Hacktivists at work'. The author is 'John Leyden' and the article was posted on '21st January 2008 12:25 GMT'. The article text begins with 'A lack of security controls allowed hackers to "wipe" the Recording Industry Association of America's (RIAA) website on Sunday.' and continues with 'The existence of an SQL Injection attack on the RIAA's site came to light via social network news site Reddit. Soon after hackers were making merry, turning the site into a blank slate, among other things.'

The Register
Biting the hand that feeds IT

Hardware Software Music & Media Networks Security Public Sector Business Site

Crime Enterprise Security Anti-Virus Spam ID Spyware Infosec

Catch Hackers Red-Handed
with GFI EventsManager! Intrusion detection via event log monitoring
www.gfi.com

Data Security Issues?
Bell has data security solutions For your Enterprise. Assess today.
www.bell.ca

Bing™ Official
Get Relevant Re Bing Gets The Jo
www.bing.com/cs

Print story Track this topic

RIAA wiped off the net
Hacktivists at work

By **John Leyden** - [Get more from this author](#)

Posted In [Enterprise Security](#), 21st January 2008 12:25 GMT

[Free whitepaper – Implementing energy efficient data centers](#)

A lack of security controls allowed hackers to "wipe" the Recording Industry Association of America's (RIAA) website on Sunday.

The existence of an SQL Injection attack on the RIAA's site came to light via social network news site Reddit. Soon after hackers were making merry, turning the site into a blank slate, among other things.

"A lack of security controls allowed hackers to "wipe" the Recording Industry Association of America's (RIAA) website" - through an SQL Injection attack?

"The RIAA has restored RIAA.org, although whether it's any more secure than before remains open to question" - January 2008

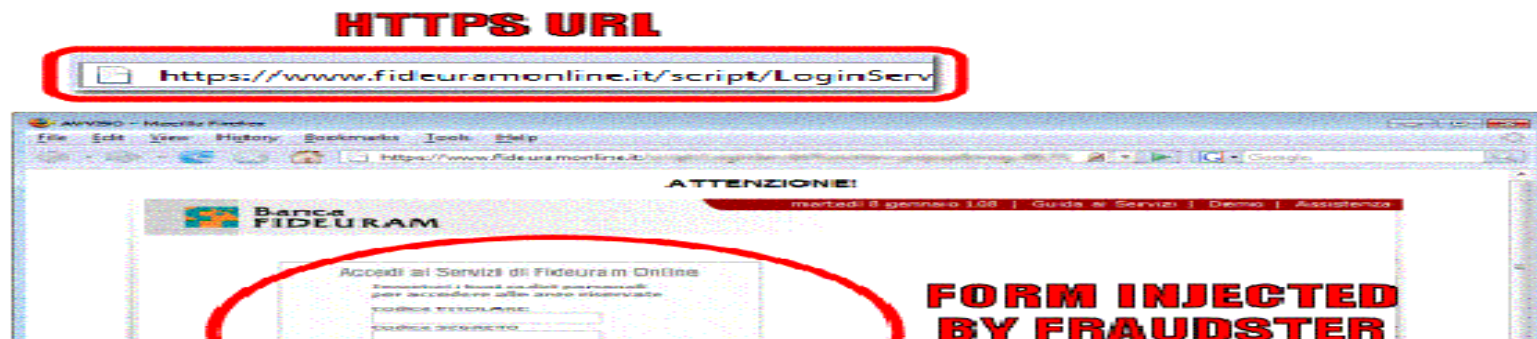
Source: http://www.theregister.co.uk/2008/01/21/riaa_hackivism/

Software Hall of Shame – Information Stolen

Italian Bank's XSS Opportunity Seized by Fraudsters

An extremely convincing phishing attack is using a cross-site scripting vulnerability on an Italian Bank's own website to attempt to steal customers' bank account details. Fraudsters are currently sending phishing mails which use a specially-crafted URL to inject a modified login form onto the bank's login page.

The vulnerable page is served over SSL with a bona fide SSL certificate issued to Banca Fideuram S.p.A. in Italy. Nonetheless, the fraudsters have been able to inject an IFRAME onto the login page which loads a modified login form from a web server hosted in Taiwan.



“Injected an IFRAME onto the login page of Banca Fideuram which loads a modified login form from a web server hosted in Taiwan” - January 2008

“A phishing attack using a XSS vulnerability to steal customers' bank account details”

Source: http://news.netcraft.com/archives/2008/01/08/italian_banks_xss_opportunity_seized_by_fraudsters.html

Software Hall of Shame – Information Modified

XSS flaw makes PM say: "I want to suck your blood"

By Liam Tung, ZDNet Australia | 2007/10/09 16:52:02

Tags: cross-site scripting, flaw, labor, liberal, security, xss

Change the text size: [a](#) | [A](#)



Print this



E-mail this



Leave a comment



Clip this



The Web sites of Australia's two major political parties contain cross-site scripting (XSS) flaws, which could be exploited to fraudulently acquire political donations, say security experts.

A short line of script developed by a security enthusiast, Bsonic, causes the Liberal Party's Web site to read: "John Howard says: I want to suck your blood", while another script caused a window to pop up on the Labor Party's Web site, urging viewers to "Vote Liberal!"

Carl Jongsma, security expert at Sunnet Beskerming, said although the vulnerabilities on each party's Web sites have been exploited for comedic purposes, it would be possible to use the script to fraudulently target people for political donations.

“The Web sites of Australia's two major political parties contain cross-site scripting (XSS) flaws” - October 2007

Source:<http://www.builder.au.com.au/news/soa/XSS-flaw-makes-PM-say-I-want-to-suck-your-blood-/0,339028227,339282682,00.htm>

Unexpected Program Behavior

- A very long URL in the address bar of Microsoft Internet Explorer (6.0) (Source: CVE 2006-3869)
 - Cause
 - Internet Explorer fails to due to **buffer overflow**
 - Impact
 - With a specially crafted request, an attacker can execute arbitrary code

Source: Common Vulnerabilities and Exposures (CVE) <http://cve.mitre.org>

Unexpected Program Behavior

- Arbitrary filename in smbclient utility of Samba (3.2.0-3.2.12), a Windows interoperability suite of programs for Linux and Unix (Source: CVE-2009-1886)
- Cause
 - A format string vulnerability where commands dealing with file names treat user input as malicious **format string**
- Impact
 - Program crashes and arbitrary code execution with crafted filename

Source: Common Vulnerabilities and Exposures (CVE) <http://cve.mitre.org>

More List of Incidents

- Common Vulnerabilities and Exposures (CVE)
<http://cve.mitre.org>
- Open Source Vulnerability Database (OSVDB),
<http://osvdb.org>
- Web-Application Security Consortium (WASC)
<http://www.webappsec.org/projects/whid/>
 - Attack method
 - Outcome
 - Location
 - ...

(Not) Secure and Reliable Software?

- Poorly defined reliability and security requirements
- Inadequate security and reliability risk analysis and management
- Software engineers only worries about functionalities – not security and reliability risks during development and testing
- Security and reliability engineers do not follow software engineering principles that make software better

Projects

- Work should be reasonably proportional to the number of group members
- Analysis and extension of any published work
- Evaluation and possible extension of an existing tool
- In depth comparison or transformation between two different techniques/tools/languages

Suggested Topics for Projects/Presentations

- Open to discussions – must be related to course topics (see the list of topics of this course)
- Software reliability
 - Fault tolerance
 - Component failure detection
 - Fault, failure. classification and propagation analysis
 - Component and system reliability
 - Automated testing, diagnosis, and repair
- Software security
 - Security requirements specifications, design, and testing for secure software development
 - Mitigation of program security vulnerabilities

Mitigation of Program Security Vulnerabilities

- Some most common vulnerabilities
 - Buffer Overflow (BOF), Format String Bug (FSB), SQL Injection (SQLI), Cross Site Scripting (XSS)
- Software Security Testing
 - Software testing strives to detect all bugs, but security testing intends to detect all exploitable bugs [Lindner, 2006]
- Static Analysis
 - Analyze program code and applies specific rules or algorithms to detect vulnerable code present in a program
- Runtime Verification
 - Vulnerabilities can be detected while a program is executing
- Hybrid Approaches
 - A combination of the above techniques

Suggested Topics for Projects/Presentations

- Some Recent hot topics
 - Web Browsers (including mobile browsers)– security and reliability issues, browser extension security, plugin security
 - Cloud Computing – security, privacy, trust, and reliability (cloud outage and fault tolerance) (<http://cloudsecurity.org/>)
 - Android OS – security (including mobile security and IOT)

A Project Area: Cloud Computing Security/Reliability

- Cloud Computing – <http://cloudcomputing.sys-con.com>
- Cloud Security – <http://cloudsecurity.org/>
- Cloud Reliability
 - “Cloud Reliability Will Be Bigger than Cloud Security for 2010-11: establishing multi-cloud reliability and fault tolerance”
<http://cloudcomputing.sys-con.com/node/1231917>
 - Both Amazon and Rackspace, suffered an outage in 2009
 - Fault-tolerant cloud?
- Some interesting links
 - IBM – Cloud computing (<http://www935.ibm.com/services/ca/en/igs/cloud/>)
 - Intel – Cloud computing
(<http://www.intel.com/content/www/us/en/cloud-computing/intel-s-cloud-computing-vision.html>)

Summary

- Software Crisis
 - Reliability and Security
 - Discussions on recent incidents about software failures and intrusions
- Course Project
 - Guidelines
 - Some suggested topics

Lecture Sources

- W. Gibbs, Software's Chronic Crisis, Scientific American, pages 86–95, September 1994
- Statistics over IT projects failure rate., IT Cortex http://www.it-cortex.com/Stat_Failure_Rate.htm
- IEEE Spectrum, September 2005
- The Role of Software in Recent Catastrophic Accidents (Wong et al. 2009), IEEE Reliability Society 2009 Annual Technology Report
- J. Viega and G. McGraw, "Building Secure Software: How to Avoid Security Problems the Right Way," Addison-Wesley Pub Co, 2001
- M. Dowd, J. McDonald, and J. Schuh, *The Art of Software Security Assessment*, Addison-Wesley publications, 2007.
- R. Anderson, "Security Engineering – A Guide to Building Dependable Distributed Systems," Wiley, January 2001
- Alexander L. Wolf. "Is Security Engineering Really Just Good Software Engineering?, Keynote Talk, ACM, SIGSOFT '04/FSE-12, October 2004, Newport Beach, CA, USA.
- F. Lindner, "Software Reliability is Security," *Communications of the ACM*, pp. 57–61, vol. 49, no. 6, June 2006.