

Did you know?

Hacks Happen

Jeremiah Grossman

Founder & CTO WhiteHat Security



2000 – 2001

YAHOO!

Official Title
“the hacker yahoo”

Job Description:
Hack Everything!



Protect this website and the ~599 others

Find the vulnerabilities before the bad guys

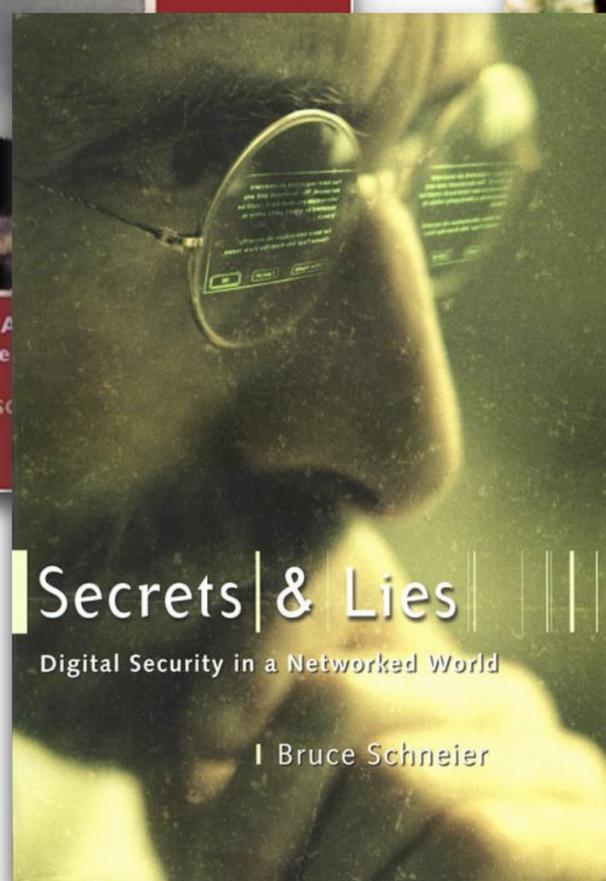
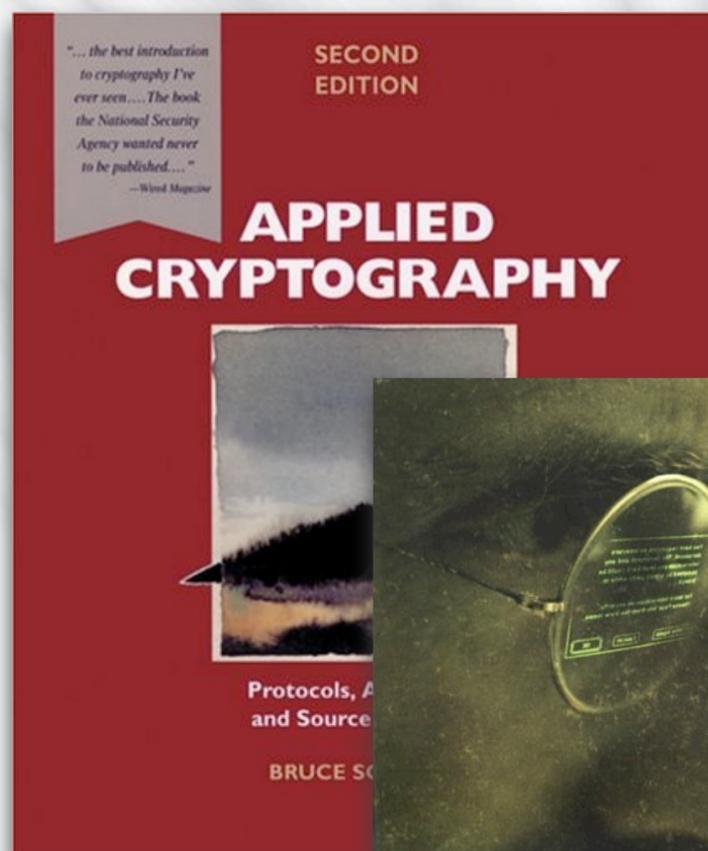
The screenshot shows the Yahoo! homepage with the following elements:

- Navigation icons: What's New, Check Email, Personalize, Help.
- Yahoo! Auctions: Pokemon, Beanies.
- Yahoo! Mail: free email for life.
- Search bar with "Search" button and "advanced search" link.
- Yahoo! Shopping: Apparel, Computers, Videos, DVDs, CDs, Toys, Electronics and more.
- Main navigation links: Shopping - Auctions - Yellow Pages - People Search - Maps - Travel - Classifieds - Personals - Games - Chat - Clubs - Mail - Calendar - Messenger - Companion - My Yahoo! - News - Sports - Weather - TV - Stock Quotes - more...
- Category links:
 - Arts & Humanities**: Literature, Photography...
 - Business & Economy**: Companies, Finance, Jobs...
 - Computers & Internet**: Internet, WWW, Software, Games...
 - Education**: College and University, K-12...
 - Entertainment**: Cool Links, Movies, Humor, Music...
 - Government**: Elections, Military, Law, Taxes...
 - Health**: Medicine, Diseases, Drugs, Fitness...
 - News & Media**: Full Coverage, Newspapers, TV...
 - Recreation & Sports**: Sports, Travel, Autos, Outdoors...
 - Reference**: Libraries, Dictionaries, Quotations...
 - Regional**: Countries, Regions, US States...
 - Science**: Animals, Astronomy, Engineering...
 - Social Science**: Archaeology, Economics, Languages...
 - Society & Culture**: People, Environment, Religion...
- Specialized sections:
 - In the News**: Report: EgyptAir crash to become criminal probe, ATM fee bans blocked by judge, Comdex, more...
 - Marketplace**: Y! Travel - plan your holiday travel, Looking for a car? job? house?, more...
 - Inside Yahoo!**: Yahoo! GeoCities - build your free home page, Y! Games - hearts, backgammon, chess, Y! Greetings - free greeting cards, more...

...and play foosball



First Book I Read on Website Security



"It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics. It's just not true.

Cryptography can't do any of that."



5

What I'd like to do in the next hour is present the industry in a new and larger context than we're used to experiencing. Most of us are mired down in our day to day jobs and don't have the time or the cause to look up and consider where we are headed. As such this presentation is not about coming to conclusions, but as a community asking the same questions about computer security and hoping we'll get different answers. In fact I'm going to do my best not to make a point.

Its for this reason I'd like to ask you to clear your minds of any preconceived notions about computer security. For the next hour consider that you are new to the industry and attempting understand the current state things. You'd like to figure out what to do going forward. Because these days we have a lot more experts and less expertise. More products and less coverage. More best practices and less security. More news and less information. This type of environment is exactly why hacks happen every minute of every hour of every day.

Make no mistake, the bad guys are winning. Most users are in a war for control over their own computers, they can't trust what they see on the screen, and even clicking, the fundamental basis of a GUI, is a perilus act. The only reason we tolerate the situation is because the Web is still going at a furious pace. But I think we'll soon reach a tipping point where the value of the system is impacted by the inherent risks involved.

Im my opinion we need to take a second look at what we know, reconsider what we think we know, and possibly come to a new set of assumptions.

Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition
<http://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp/0471117099>

Secrets and Lies: Digital Security in a Networked World
<http://www.amazon.com/Secrets-Lies-Digital-Security-Networked/dp/0471253111>

Did you know?

By the End of 2008...

17 million programmers worldwide

Writing 6,000 lines of code per year (each)



Who here codes, but is not a programmer?

[A1] 17 million programmers worldwide
<http://www.itjungle.com/tlb/tlb011607-story06.html>
<http://deepfreeze9.blogspot.com/2007/08/factoid-19-million-programmers-by-2010.html>
<http://blogs.zdnet.com/ITFacts/?p=12808>

U.S. Department of Labor Bureau of Labor Statistics - Computer Programmers
<http://www.bls.gov/oco/ocos110.htm>

[A2] ~6 KLOC per year per developer
<http://blogs.msdn.com/philipsu/archive/2006/06/14/631438.aspx>
<http://fixunix.com/linux/370267-attackers-hose-down-microsoft-s-jet-db-engine-5.html>
<http://blogs.msdn.com/eldar/archive/2006/07/07/647858.aspx>

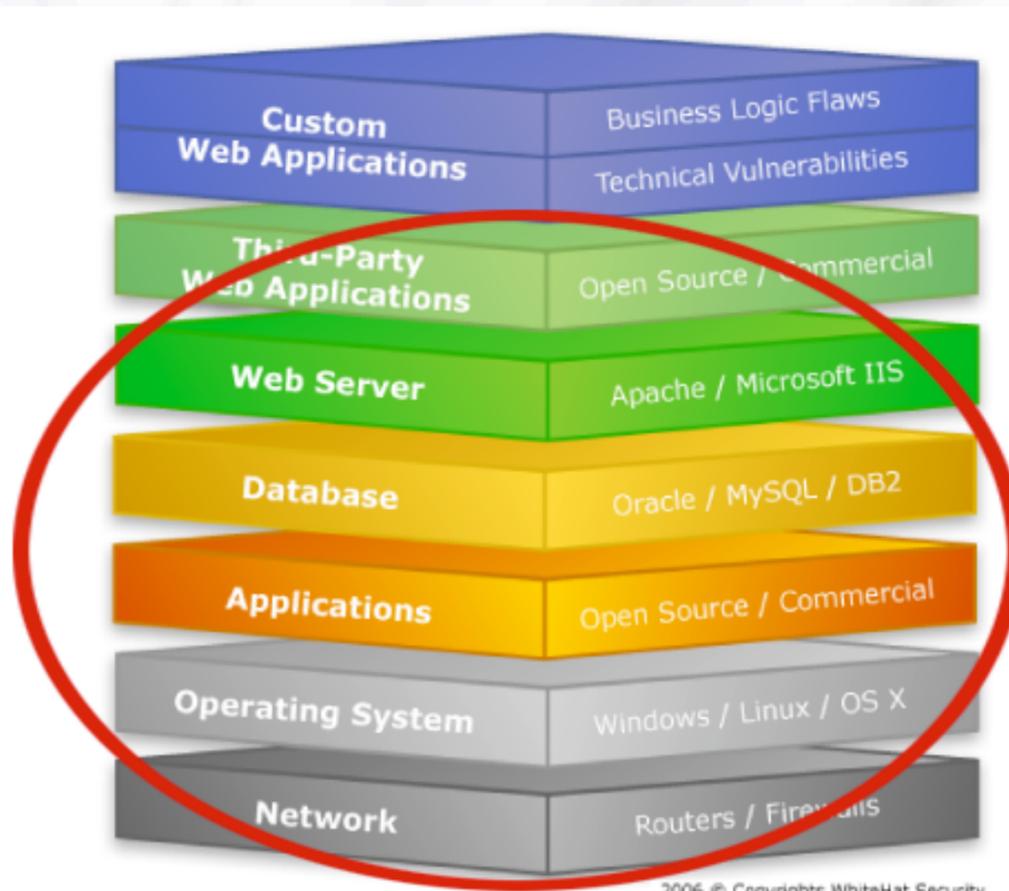
= 102 Billion

New lines of code pushed per year

Windows 2000	29 Million
Red Hat Linux 7.1	30 Million
Windows XP	40 Million
Windows Vista	50 Million
Mac OS X 10.4	86 Million



Conservative research says: 1 security defect for every 10,000 lines of code



(potentially) new
undiscovered
vulnerabilities

10,200,000
per year

850,000 per month
28,000 per day



If only 1% of new undiscovered vulnerabilities are exploitable:

102,000

zero-days per year



Not all vulnerabilities are created equal.

$A6 = A5 * .01 = 102,000$ zero-days per year

Total vulnerabilities EVER
reported in National
Vulnerability Database CVE

30,253

Publication rate: 16 vulnerabilities / day

In 2007 IBM X-force
reported vulnerabilities

6,437

Location of the other ~95,000: *unknown*

By the end of this presentation:

10 million newly written lines of code

2,739 new websites

10,000 new undiscovered vulnerabilities

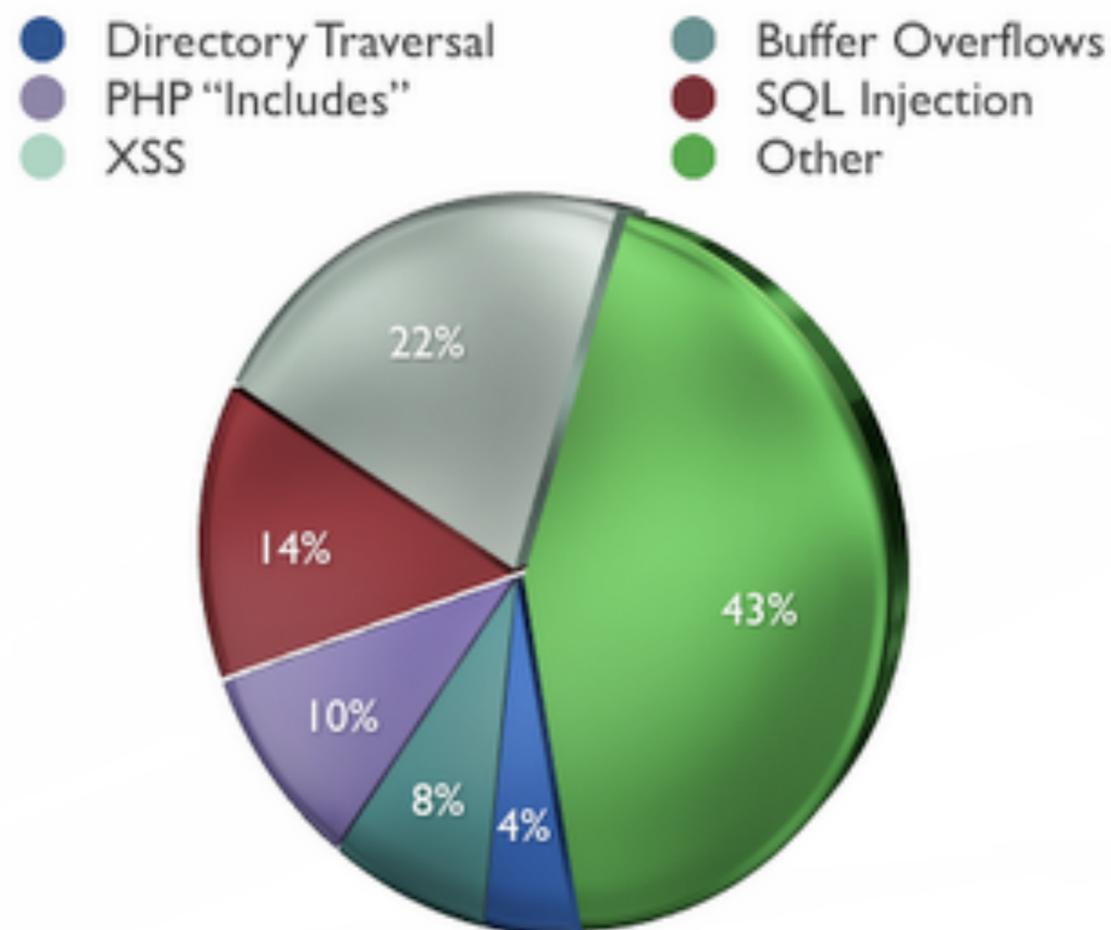


- 102,000,000,000 lines of code written per year / 8,766 (hours) in a year.
- 2,000,000 new websites per mo/ 730 hours in a month
- 10,000,000 lines of code during this hour/ 10,000 (A4) – security defects

Did you know?

Roughly 70% of developers work on Web-related projects

Web application flaws account for 4 of the top 5 spots in well-known vulnerabilities



Qualys: from Q3/2002 to Q3/2005
performed **32,147,000** vulnerability ip-scans...

Identified **21,347,000** critical issues

*providing an attacker the ability to gain full control of the system, and/or leakage of highly sensitive information



**THE AVERAGE WINDOW OF EXPOSURE (BEFORE PATCHING)
FOR WELL-KNOWN VULNERABILITIES AFFECTING
ENTERPRISE VENDORS:**

55 DAYS

ENOUGH TIME FOR...

15 BILLION NEW lines of code

15 THOUSAND POTENTIAL ZERO-DAYS

880 DISCLOSED WELL-KNOWN VULNERABILITIES

80% OF EXPLOITS ARE AVAILABLE WITHIN

19 DAYS

OF DISCLOSURE.



“The average window of exposure for vulnerabilities affecting enterprise vendors was 55 days. This is an increase over the 47-day average in the second half of 2006.”

IBM Internet Security Systems X-Force 2007 Trend Statistics
http://www-935.ibm.com/services/us/iss/pdf/etr_xforce-2007-annual-report.pdf

- $(102,000,000,000 / 365) * 55 = \sim 15$ billion
- $15 \text{ billion} / 10,000 * .01 =$
- $(\text{CVE per day}) * 55 = 880$

<http://www.qualys.com/laws>

IF ALL NEW CODE IS INSPECTED
TO FIND 1 UNDISCOVERED
VULNERABILITY EVERY
60 SECONDS...



WE'D NEVER FIND THEM ALL.

IF EVERY 10 SECONDS...



IT WOULD TAKE ABOUT **3 YEARS** TO
FIND ALL THE NEW VULNERABILITIES
FOR **JUST THIS YEAR.**



STARTING IN 2006

**THE DEPARTMENT OF HOMELAND SECURITY SPENT
\$300,000 (US) ON A PROJECT TO FIND AND FIX
SECURITY DEFECTS IN 180 OPEN SOURCE PROJECTS.**

**FOUND 1 SECURITY DEFECT PER 1,000 LINES
(NOT 10,000)**

7,826 DEFECTS FIXED

1 DEFECT REMEDIATED EVERY 2 HOURS

\$38 PER VULNERABILITY

BY 2012 OVER 90% OF ENTERPRISES WILL USE OPEN SOURCE



WORLD-OF-WARCRAFT L-70 ACCT	\$4
PAYPAL OR EBAY ACCT	\$8
CREDIT CARDS W/ CCV & EXP	\$25
BANK ACCT	\$1,000
WMF EXPLOIT	\$4,000
REALPLAYER 1 1	\$10,000
OS X	\$10,000 + 15-INCH MACBOOK PRO
WINDOWS VISTA	\$50,000
INTERNET EXPLORER	\$100,000
WHAT MICROSOFT PAYS FOR O-DAYS...	\$0



WHAT MICROSOFT PAYS FOR O-DAYS...

<http://www.bestsecuritytips.com/news+article.storyid+116.htm>

http://securitywatch.eweek.com/browsers/russian_firm_demos_realplayer_zero_day_exploit.html

* <http://blogs.technet.com/security/archive/2008/04/10/rsa-2008-keynote-john-thompson.aspx>

http://www.theregister.co.uk/2007/04/20/pwn-2-own_winner/

<http://www.arnnet.com.au/index.php/id;741896054;pp;2;fp;4194304;fpid;1>

<http://www.letemps.ch/template/economie.asp?page=9&article=228747>

China-based online “Password Recovery” services:

1. 300 Yuan (\$43) to break an overseas mailbox password, with 85% probability of success.
2. 200 Yuan (\$29) to break a domestic mailbox password, with 90% probability of success.
3. 1000 Yuan (\$143) to break a company’s mailbox password (no success rate given).

Also on the menu:

passwords for 163, 126, QQ, Yahoo, Sohu, Sina, TOM, Hotmail, MSN...etc.



Did you know?

THERE ARE
162,000,000
WEBSITES

MILLIONS MORE ADDED PER MONTH



809,000 WEBSITES USE SSL

HAVE SOMETHING WORTH PROTECTING



MORE THAN A YEAR AFTER EXTENDED VALIDATION CERTIFICATES OFFERED TO “FIGHT PHISHING SCAMS”



LESS THAN 5,000 WEBSITES UPGRADED



Multiple experts report

9 out of 10 websites have vulnerabilities

potentially allowing hackers unauthorized access

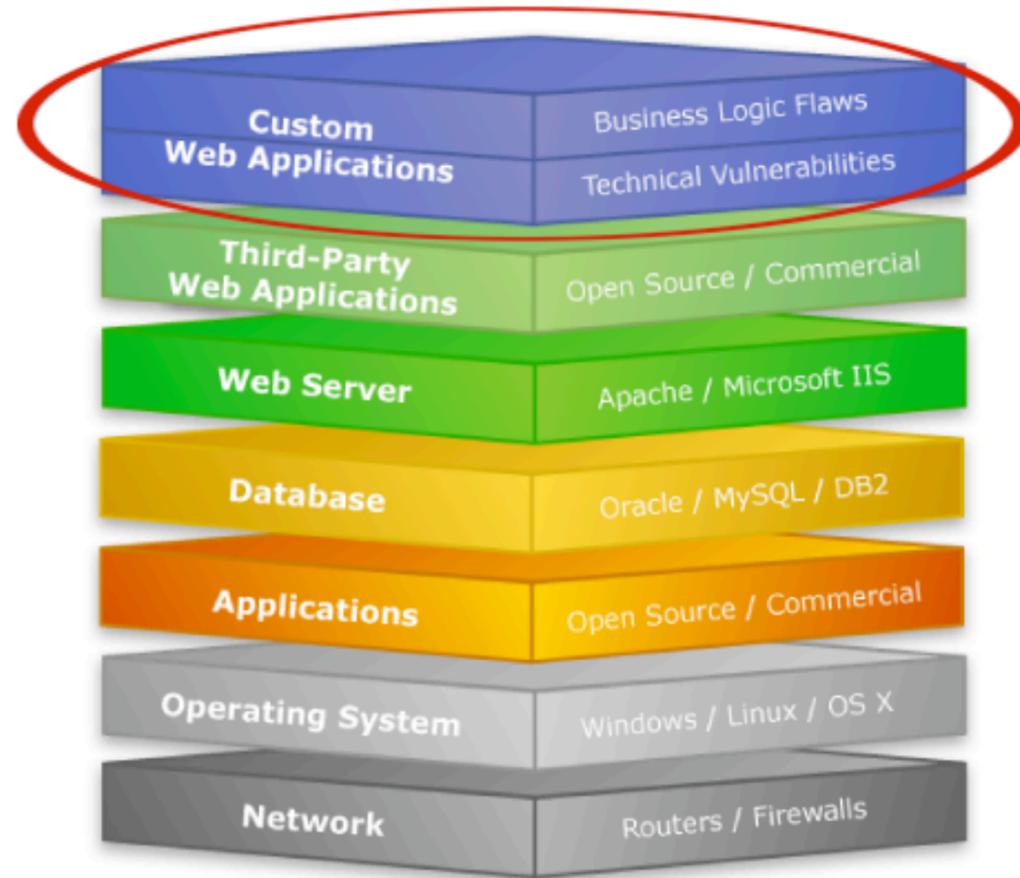


If there's just 1 vulnerability on 90% of the SSL websites...

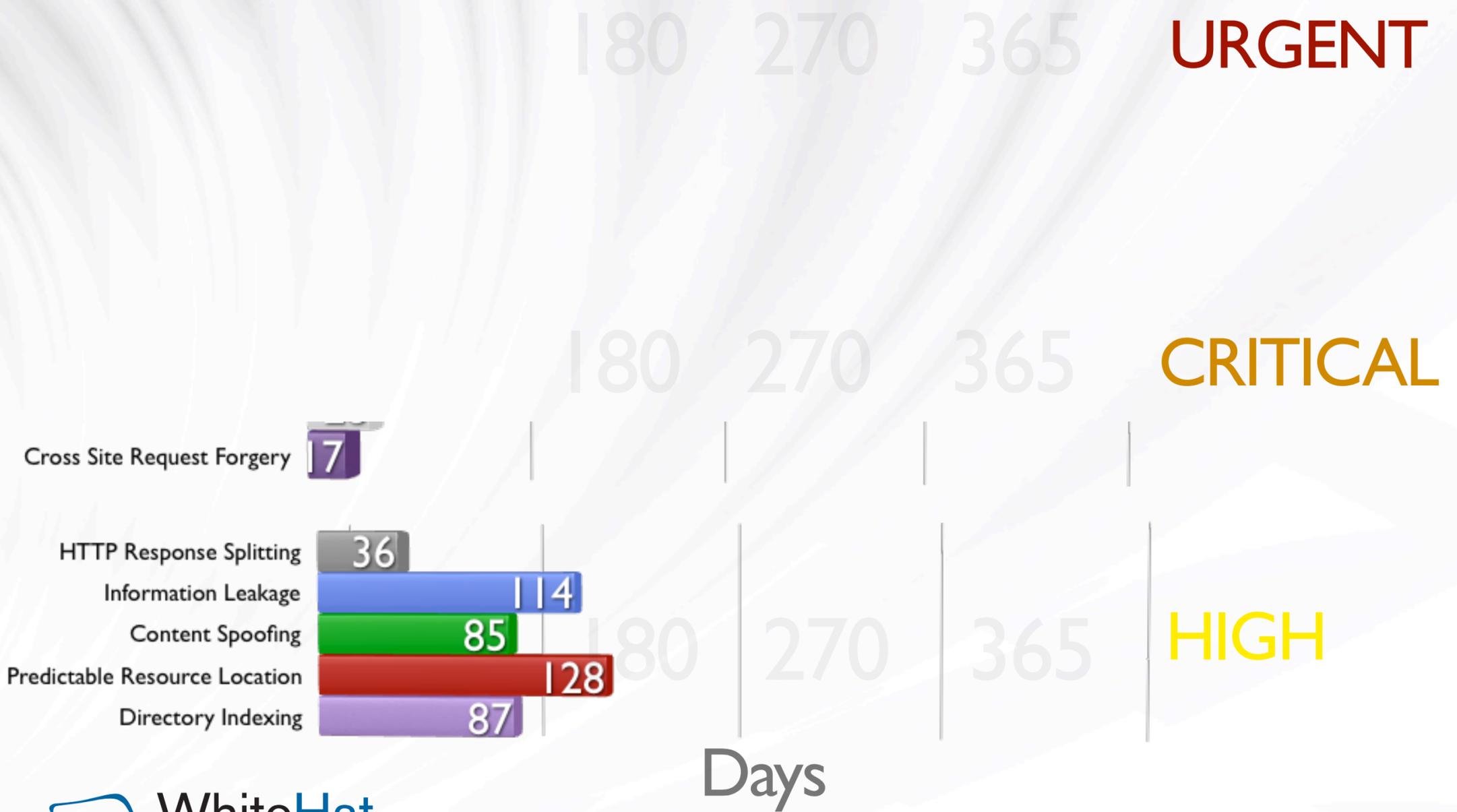
Other reports say an average of 7

728,100

total vulnerabilities



Time to Fix

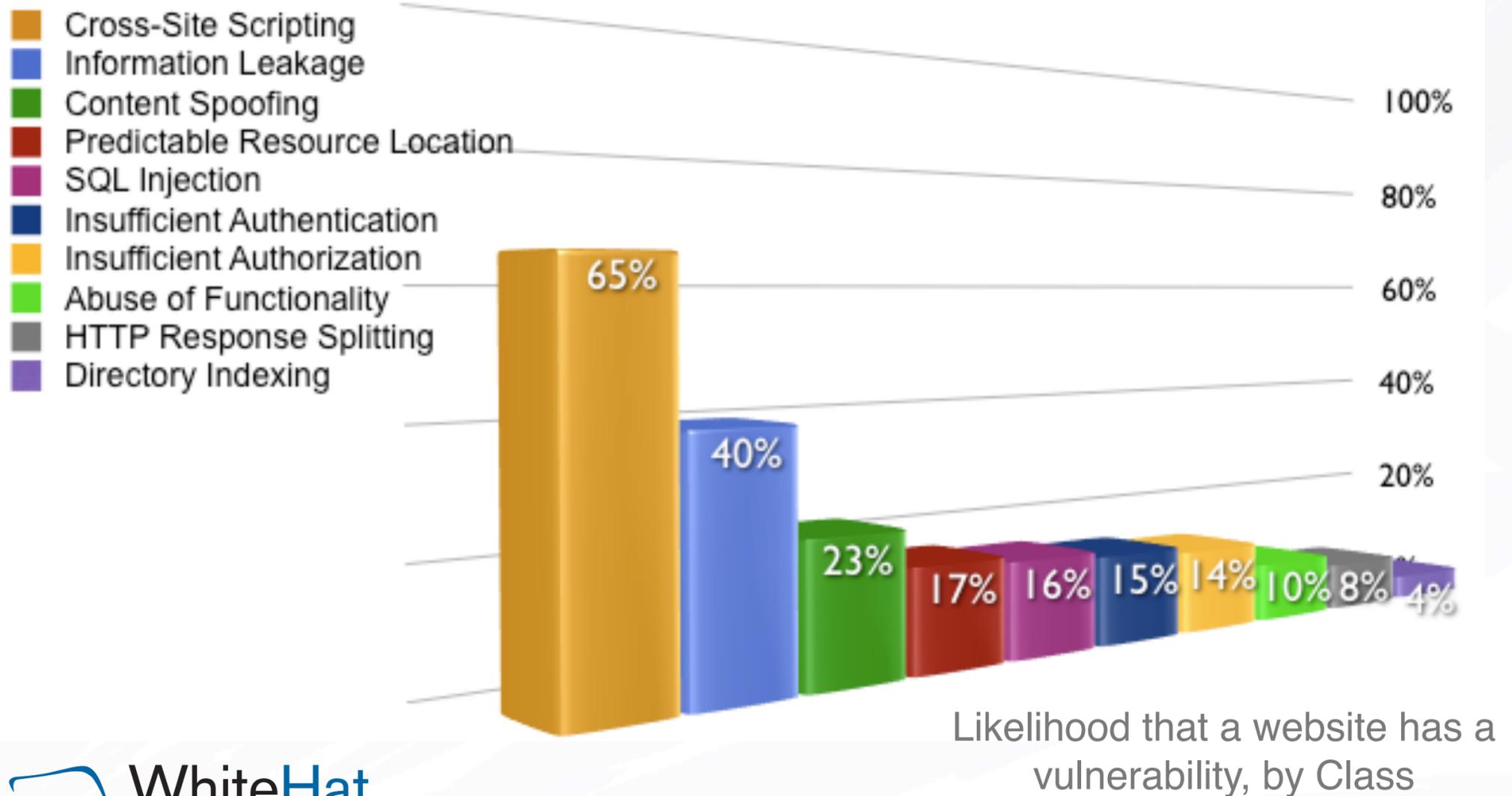


XSSed.com has reported:

20,843 total vulnerabilities

1,072 fixed (5%)

Experts say 90% of externally accessible applications today are Web-enabled, and two-thirds have exploitable vulnerabilities.



InformationWeek DEFINING THE BUSINESS VALUE OF TECHNOLOGY

new age of **INNOVATION**
a blog about transform your business mode

NEWS BLOGS SOFTWARE SECURITY HARDWARE
Browsers • E-Business • Search • Web development • All

symantec. United States

The Register On TechRepublic: top

intel Science

cnet **NEWS.com** Search: _____

Today on CNET Reviews News Downloads Tips & Tricks CNET TV Compare Prices

Business Tech Cutting Edge Green Tech Wireless Security Media Markets Personal Tech

LINUX JOURNAL

Find out why Houston is the next big thing in open source and startups

Home Topics Newsletter Community Resources Forums Shop Magazine

Home

Hackers Take Down Pennsylvania Government
January 10th, 2008 by Justin Ryan

Products Services Solutions & In

ise Webcasts Events

Symantec.com >

Drive-by Phishing
In a previous blog about the concept of attack, all a hacker simply view the which could be the attacker's...

Samy opens new front in worm war

By Munir Kotadia
Staff Writer, CNET News.com
Published: October 17, 2005 11:40 AM PDT

Welcome Google user!

Add News.com to Google

More headlines related to "f":

- **Harnessing the power of wind and waves**
- **Police Blotter: Armed robbers nabbed through text messages**
- **Microsoft-Yahoo the mother of all clusterbombs**
- **Week in review: Apple goes into thin 'Air'**
- More matching headlines >

Tools

- Talkback
- Print
- E-mail
- Share

The newly discovered Samy worm is one of the first to exploit a cross-site scripting vulnerability, a technique security experts fear could be used to open a new front in attacks.

Digg

submit

After a series of attacks on state government web sites pulled the plug, rendering them inaccessible. In what sounds like a repeat of October's access servers hosting Pennsylvania's injection attempt. The activities were...

NETCRAFT Every Rack Is Private 10GigE Cisco Network Public & Private Networks

SOFTLAY do it faster. do it better. do it right.

Webserver Search
What's that site running?...

Search
Example: .google.com
Example: www.netcraft.com

Netcraft Services

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...

Reprints & Permissions | **RSS**

Mixx it

Other ways to share:

Yahoo! Buzz

Digg

Newsvine

Reddit

Facebook

What's this?

washingtonpost.com > Technology > Special Reports > Privacy

TechNews.com

Print This Article
E-Mail This Article

QUICK QUOTES

Enter Symbol go
Tables | Portfolio | Index

MOST VIEWED ARTICLES

Technology On the Site

Updated 2:03 p.m. ET

- [Intel has a chip, but where are the MIDs?](#)
- [Rep. Barton Seeks Probe In Theft of Computer](#)
- [Intel Unveils New Classmate PCs](#)

40 Million Credit Card Numbers Hacked
Data Breached at Processing Center

By Jonathan Krim and Michael Barbaro
Washington Post Staff Writers
Saturday, June 18, 2005; Page A01

More than 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker and are at risk of being used for fraud, MasterCard International Inc. said yesterday.

In the largest security breach of its kind, MasterCard officials said all credit card brands were affected, including 13.9 million cards bearing the MasterCard label. A spokeswoman for Visa USA Inc. confirmed that 22 million of its card numbers may have been breached, while Discover Financial Services Inc. said it did not yet know if its cards were affected.

been secretly tainted by hackers. They will usually be taken to the Web page they expect. But at the same time, they are invisibly redirected to a computer server that installs a hidden program.

This program enables hackers to use the PC to spread spam and carry out scams. Typically, it also lets the attacker embed a keystroke logger, which collects and transmits your passwords and any other sensitive data you type online.

Any website indexed by Google (GOOG) that fails to carefully handle JavaScript — the coding that activates many cool Web features, such as changing the color of a button when someone mouses over it — is a potential target. That's seven in 10 sites, says tech security firm WhiteHat Security. Hackers have discovered ways to trick the website application to run malicious JavaScripts.

"We're in a phase where one or two smart guys are attacking a few dozen major websites," says David Dewey, manager of IBM's X-Force security division. "In the next few weeks I would expect to see copycats attacking hundreds of high-profile websites."

See what's new at IDF >

a home page or product page from the database. But for the fact it used an old and already guarded against Windows exploit, it might still be spreading across the Internet, security experts said.

"I don't think we've seen this scale of database intrusion before. SQL injection attacks are usually on a one-at-a-time basis," said Phil Neray, VP of marketing at Guardium, a Waltham, Mass., firm that makes database protection software.

malware and sites targeted, the campaign is still up and running, poisoning what looks like over a million search queries with loadable state entirely relies on the site's web application the lack of.

The Register » Security » Enterprise Security »

RIAA wiped off the net

Hackers at work

By [John Leyden](#) → [More by this author](#)
Published Monday 21st January 2008 12:25 GMT

[Improve IT Culture and employee satisfaction in your business - Sign up for the latest RegCast here](#)

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.

SECURITY

Do you know about XSLF?

No one does

Because XSLF doesn't exist

Yet.

How can we secure applications against technologies and attacks that don't exist?



More major websites were launched before significant classes of attack were “well-known”

Website	Founded
Amazon	1994
Yahoo	1995
eBay	1995
Bank of America	1997
Google	1998
MySpace	2003
YouTube	2005

Vulnerability	Attack
Buffer Overflow	1996
Command Injection	1996
SQL Injection	2004
XSS	2005
Predictable Resource Location	?
HTTP Response Splitting	2005 / ?
CSRF	?

Newest Web Hacking Techniques

The Attack of the TINY URLs
Backdooring MP3 Files
Backdooring QuickTime Movies
CSS history hacking with evil marketing
I know where you've been
Stealing Search Engine Queries with JavaScript
Hacking RSS Feeds
MX Injection : Capturing and Exploiting Hidden Mail Servers
Blind web server fingerprinting
JavaScript Port Scanning
CSRF with MS Word
Backdooring PDF Files
Exponential XSS Attacks
Malformed URL in Image Tag Fingerprints Internet Explorer
JavaScript Portscanning and bypassing HTTP Auth
Bruteforcing HTTP Auth in Firefox with JavaScript
Bypassing Mozilla Port Blocking
How to defeat digg.com
A story that diggs itself
Expect Header Injection Via Flash
Forging HTTP request headers with Flash
Cross Domain Leakage With Image Size
Enumerating Through User Accounts
Widespread XSS for Google Search Appliance
Detecting States of Authentication With Protected Images
XSS Fragmentation Attacks
Poking new holes with Flash Crossdomain Policy Files
Detecting Privoxy Users and Circumventing It
Using CSS to De-Anonymize
- Response Splitting Filter Evasion
Adultspace XSS Worm

CSS History Stealing Acts As Cookie
Detecting FireFox Extensions
Stealing User Information Via Automatic Form Filling
Circumventing DNS Pinning for XSS
Netflix.com XSRF vuln
Browser Port Scanning without JavaScript
Widespread XSS for Google Search Appliance
Bypassing Filters With Encoding
Variable Width Encoding
Network Scanning with HTTP without JavaScript
AT&T Hack Highlights Web Site Vulnerabilities
How to get linked from Slashdot
F5 and Acunetix XSS disclosure
Anti-DNS Pinning and Circumventing Anti-Anti DNS pinning
Google plugs phishing hole
Nikon magazine hit with security breach
Governator Hack
Metaverse breached: Second Life customer database hacked
HostGator: cPanel Security Hole Exploited in Mass Hack
I know what you've got (Firefox Extensions)
ABC News (AU) XSS linking the reporter to Al Qaeda
Account Hijackings Force LiveJournal Changes
Xanga Hit By Script Worm
Advanced Web Attack Techniques using GMail
PayPal Security Flaw allows Identity Theft
Internet Explorer 7 "mhtml:" Redirection Information Disclosure
Bypassing of web filters by using ASCII
Google Indexes XSS
XML Intranet Port Scanning
IMAP Vulnerable to XSS
Selecting Encoding Methods For XSS Filter Evasion

Anonymizing RFI Attacks Through Google
Google Hacks On Your Behalf
Google Dorks Strike Again
Cross-Site Printing (Printer Spamming)
Stealing Pictures with Picasa
HScan Redux
ISO-8895-1 Vulnerable in Firefox to Null Injection
MITM attack to overwrite addons in Firefox
Microsoft ASP.NET Request Validation Bypass Vulnerability (POC)
Non-Alpha-Non-Digit 3
Steal History without JavaScript
Pure Java™, Pure Evil™ Popups
Google AdSense CSRF hole
There's an OAK TREE in my blog!?!?!
BK for Mayor of Oak Tree View
Google Docs puts Google Users at Risk
All Your Google Docs are Belong To US...
Java Applets and DNS Rebinding
Scanning internal Lan with PHP remote file opening.
Firefox File Handling Woes
Firefoxurl URI Handler Flaw
Bugs in the Browser: Firefox's DATA URL Scheme Vulnerability
Multiviews Apache, Accept Requests and free listing
Optimizing the number of requests in blind SQL injection
Bursting Performances in Blind SQL Injection - Take 2 (Bandwidth)
Port Scan without JavaScript
Favorites Gone Wild
Login Detection without JavaScript
Anti-DNS Pinning (DNS Rebinding) : Online Demonstration
Username Enumeration Timing Attacks (Sensepost)
Google GMail E-mail Hijack Technique
Recursive Request DoS
Exaggerating Timing Attack Results Via GET Flooding
Initiating Probes Against Servers Via Other Servers

Effects of DNS Rebinding On IE's Trust Zones
Paper on Hacking Intranets Using Websites (Not Web Browsers)
More Port Scanning - This Time in Flash
HTTP Response Splitting and Data: URI scheme in Firefox
Res:// Protocol Local File Enumeration
Res Timing Attack
IE6.0 Protocol Guessing
IE 7 and Firefox Browsers Digest Authentication Request Splitting
Hacking Intranets Via Brute Force
Hiding JS in Valid Images
Internet Archiver Port Scanner
Noisy Decloaking Methods
Code Execution Through Filenames in Uploads
Cross Domain Basic Auth Phishing Tactics
Additional Image Bypass on Windows
Detecting users via Authenticated Redirects
Passing Malicious PHP Through getimagesize()
Turn Any Page Into a Greasemonkey Popup
Enumerate Windows Users In JS
Anti-DNS Pinning (DNS Rebinding) + Socket in FLASH
Iframe HTTP Ping
Read Firefox Settings (PoC)
Stealing Mouse Clicks for Banner Fraud
(Non-Persistent) Untraceable XSS Attacks
Inter Protocol Exploitation
Detecting Default Browser in IE
Bypass port blocking in Firefox, Opera and Konqueror.
LocalRodeo Detection
Image Names Gone Bad
IE Sends Local Addresses in Referer Header
PDF XSS Can Compromise Your Machine
Universal XSS in Adobe's Acrobat Reader Plugin
Firefox Popup Blocker Allows Reading Arbitrary Local Files
IE7.0 Detector

overwriting cookies on other people's domains in Firefox.
Embedding SVG That Contains XSS Using Base64 Encoding in Firefox
Firefox Header Redirection JavaScript Execution
More URI Stuff... (IE's Resouce URI)
Hacking without Odays: Drive-by Java
Google Urchin password theft madness
Username Enumeration Vulnerabilities
Client-side SQL Injection Attacks
Content-Disposition Hacking
Flash Cookie Object Tracking
Java JAR Attacks and Features
Severe XSS in Google and Others due to the JAR protocol issues
Web Mayhem: Firefox's JAR: Protocol issues (bugzilla)
ODAY: QuickTime pwns Firefox
Exploiting Second Life
Injecting the script tag into XML
Cross-Browser Proxy Unmasking
Spoofing Firefox protected objects

Most of them unresolved

GOOGLE HACKING (CODE SEARCH)

(REQUEST.FORM|REQUEST.QUERYSTRING) LANG:ASP

RESULTS 1 - 10 OF ABOUT 15,400

(RESPONSE.WRITE) (REQUEST.FORM) LANG:ASP

RESULTS 1 - 10 OF ABOUT 8,000



We're sorry...

... but your query looks similar to automated requests from a computer virus or spyware application. To protect our users, we can't process your request right now.

We'll restore your access as quickly as possible, so try again soon. In the meantime, if you suspect that your computer or network has been infected, you might want to run a [virus checker](#) or [spyware remover](#) to make sure that your systems are free of viruses and other spurious software.

If you're continually receiving this error, you may be able to resolve the problem by deleting your Google cookie and revisiting Google. For browser-specific instructions, please consult your browser's online support center.

If your entire network is affected, more information is available in the [Google Web Search Help Center](#).

We apologize for the inconvenience, and hope we'll see you again on Google.

To continue searching, please type the characters you see below:



Welcome to Web 2.0



WhiteHalo
SECURITY

OpenSocial

OpenSocial

Did you know?

Studies indicate that 75% of security breaches are due to **flaws in software**.

71% of vulnerabilities reported during Q4 2007 **affected Web apps**, up 3% from Q3.

90% of IT security spending is on **perimeter security** such as firewalls



Bill rate for a source code reviewer **\$150 (US)**
per hour

Source code review for the average
small to mid-sized website **\$25,000 (US)**

To cover 10% of the SSL Websites (~80,000) ...

Total man hours **13,360,000**

Source code reviewers **6,680**

Annual economic burden **\$2,000,000,000 (US)**



And then we still have to fix the vulnerabilities

Hackers just need to exploit one to get in.

"Personally, I'd love to see everyone go through an OWASP-based source-code review, but certainly, that's not going to happen."

Bob Russo
PCI Standards Council General Manager



“ There is no "secure development lifecycle" in the vast majority of universities' degree programs - that is, security is not "baked into" graduates of relevant programs (e.g., computer science) throughout their degree programs. And that is a problem, perhaps the problem plaguing the software industry.”

Mary Ann Davidson
Chief Security Officer at Oracle



Survey of the Web application security community

69% Hunt for website vulnerabilities without permission

50% Said they'd disclose findings to the owner.

73% Believe PCI-DSS will make little to no difference

90% Say the average user has no way to protect themselves from being exploited online.



What does this mean?

Hacks Happen

Website Defacements

493,000 in 2005

752,000 in 2006

480,000 in 2007

~1 defacement every second

Over **50%** of websites hosting *malicious code* are legitimate

(compromised by attackers)

A new infected Web page is discovered every:

14 seconds

24 hours a day

365 days a year

2006, 0.3% of all Internet queries return at least one URL containing **malicious content**.

2007, 1.3%

The Google logo is displayed in its characteristic multi-colored font (blue, red, yellow, blue, green, red) with a trademark symbol (TM) to the right. It is centered on a white rectangular background.

THE EXPLOSION OF BOTNETS HAS MANDATED
A NEW WARNING LABEL:



COPYRIGHT © 2008 J.D. "THEHACK" PALMER [HTTP://WWW.USERFRIENDLY.ORG](http://www.userfriendly.org)

UserFriendly.org

MySpace Samy Worm

1 millions profiles infected

Code Red

359,000 infected computers

Code Red II

275,000 infected computers

Slammer's

55,000 - 75,000 (10 minutes)

Blaster

336,000 infected computers

**1st generation
malware
(first 24 hours)**



52,771 active bot-infected
computers were observed per
day in the first half of 2007

Kraken

400,000 infected computers

Srizbi

315,000 infected computers

Storm

200,000 infected computers

**2nd generation
malware**



Did you know?

Conservative estimates put the total annual IT security spend in the US at \$50 billion and **e-crime losses at \$100 billion.**

We're losing two dollars for every dollar spent.



In 2007 the FBI's Internet Crime Complaint Center:

220,000 Online fraud complains

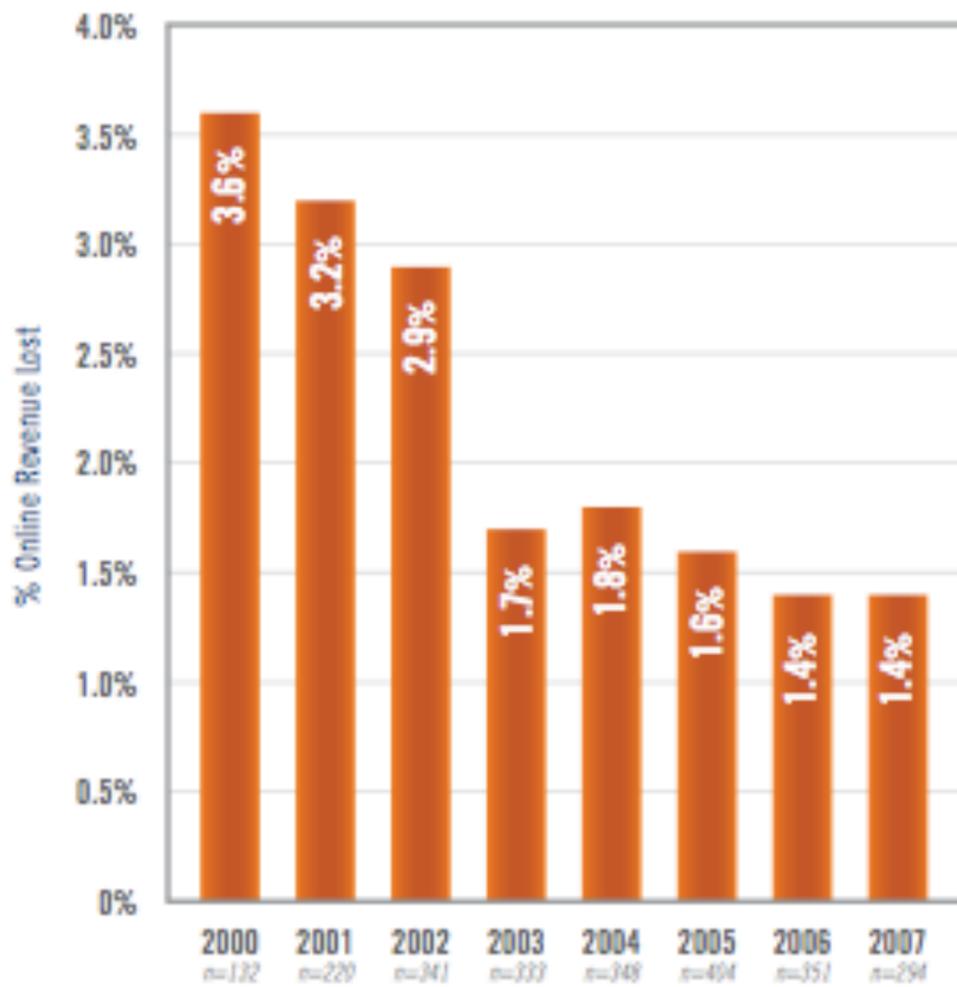
US consumers losing more than \$239 million

Up from \$198 million in 2006

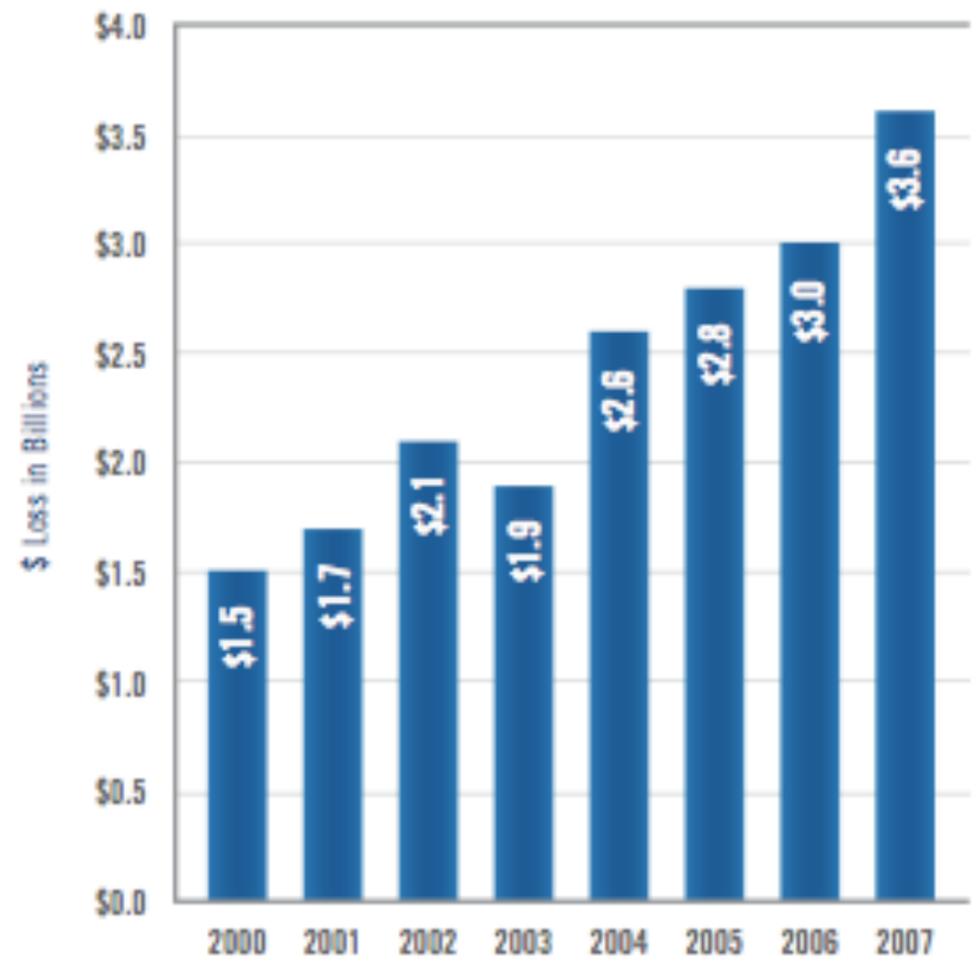
Most cyber-fraud is not reported



% Revenue Lost to Online Fraud

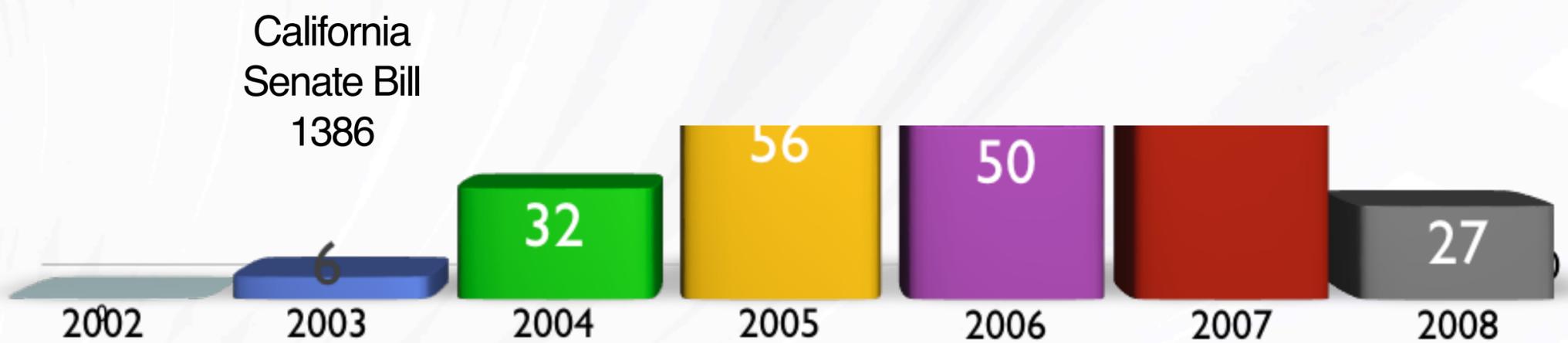


Online Revenue Loss Due to Fraud \$3.6B in 2007



Loss of personal information

measured in millions of records



TJX, CardSystems, America Online, TD Ameritrade, Hannaford, etc.

Records lost/stolen per second

2008	0.50
2007	5
2006	1.6

In the first three months of 2008, the number of data breaches more than doubled over the same period last year.



What Do We Do?

- 1. TURN OFF THE INTERNET**
- 2. STOP DEVELOPING SOFTWARE**
- 3. CASH ONLY**

JUST KIDDING!

SORT OF...

**BEST PRACTICES RECOMMENDED
BY THE FBI, EBAY, PAYPAL,
MICROSOFT, GOOGLE, YAHOO,
ETC. ALL SAY THE SAME THING.**

FIREWALLS

ANTI-VIRUS / ANTI-SPYWARE SOFTWARE

KEEP PATCHES UP TO DATE

BE CAREFUL WHAT YOU DOWNLOAD

TURN OFF YOUR COMPUTER

Good ideas, but no longer effective.



There is a proverb that illustrates the way to quickly determine whether or not someone is sane. The individual is shown a river flowing into a pond. He is given a bucket and asked to drain the pond. If he walks to the stream to dam the inflow into the pond he will be considered sane. If, instead, he decides to empty the pond with his bucket without first stopping the in-flow then he would be considered insane.

http://www.fbi.gov/cyberinvest/protect_online.htm

IS STANDALONE ANTI-VIRUS DEAD?

“The net effect of the increase has been, as one anti-virus senior manager put it, “a denial of service against our labs.” Worse, private bench tests by host-based intrusion prevention system (HIPS) vendors suggest that detection rates against new malware variants are less than 70%. Anti-virus labs are typically 30 to 60 days behind for run-of the mill malware.”

“The signature files of the market-leading anti-virus product that Yankee Group uses, for example, exceed 9 MB, encompassing 200,000 signatures. Full-disk scans of a typical PC’s 100,000-plus files exceed 90 minutes.”



“The user's going to pick dancing pigs over security every time.”

Bruce Schneier, founder and CTO of BT Counterpane

“The relationship between signature-based antivirus companies and the virus writers is almost comical. One releases something and then the other reacts, and they go back and forth. It's a silly little arms race that has no end.”

Greg Shipley, CTO of Neohapsis

“SSL is like using an armored truck to transport rolls of pennies between someone on a park bench and someone doing business from a cardboard box.”

Eugene H. Spafford, Professor Purdue University

Thank You

For more information visit: www.whitehatsec.com/

Jeremiah Grossman, founder and CTO
blog: <http://jeremiahgrossman.blogspot.com/>
email: jeremiah@whitehatsec.com

