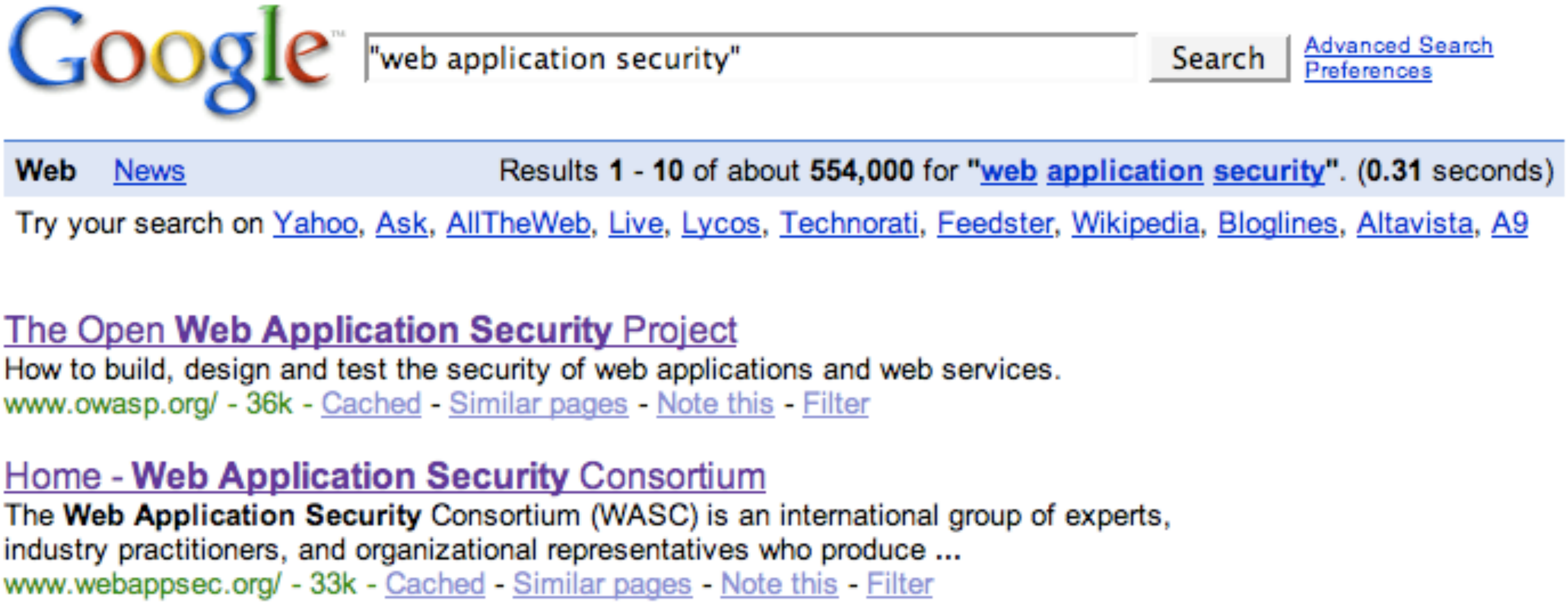
An Introduction to WASC and its projects

Web Application Security Consortium

Jeremiah Grossman
Co-founder of the WASC
WhiteHat Security Founder & CTO

OWASP & WASC AppSec 2007
San Jose
November 12 - 15, 2007

The OWASP Foundation
http://www.owasp.org/



Results **1** - **10** of about **554,000** for "**web application security**". (**0.31** seconds)

Try your search on Yahoo, Ask, AllTheWeb, Live, Lycos, Technorati, Feedster, Wikipedia, Bloglines, Altavista, A9

The Open **Web Application Security** Project

How to build, design and test the security of web applications and web services.

www.owasp.org/ - 36k - Cached - Similar pages - Note this - Filter

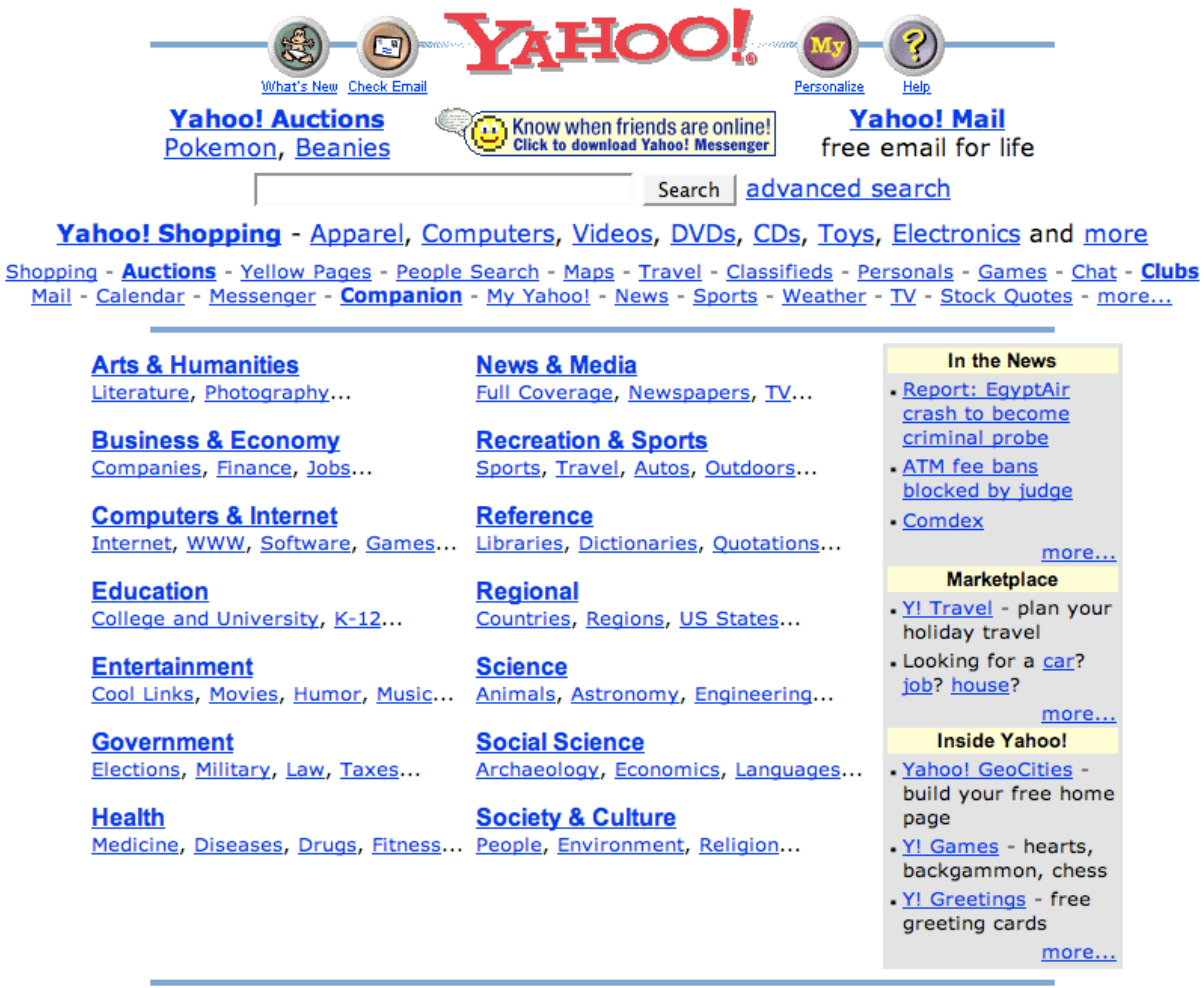
Home - **Web Application Security** Consortium

The **Web Application Security** Consortium (WASC) is an international group of experts, industry practitioners, and organizational representatives who produce ...

www.webappsec.org/ - 33k - Cached - Similar pages - Note this - Filter

Started my professional ~~Web Application Security~~ career in 2000... CGI Security

YAHOO!®



Yahoo! Auctions
Pokemon, Beanies

Know when friends are online!
Click to download Yahoo! Messenger

Yahoo! Mail
free email for life

advanced search

Yahoo! Shopping - Apparel, Computers, Videos, DVDs, CDs, Toys, Electronics and more

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...

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...

In the News

- Report: EgyptAir crash to become criminal probe
- ATM fee bans blocked by judge
- Comdex

more...

Marketplace

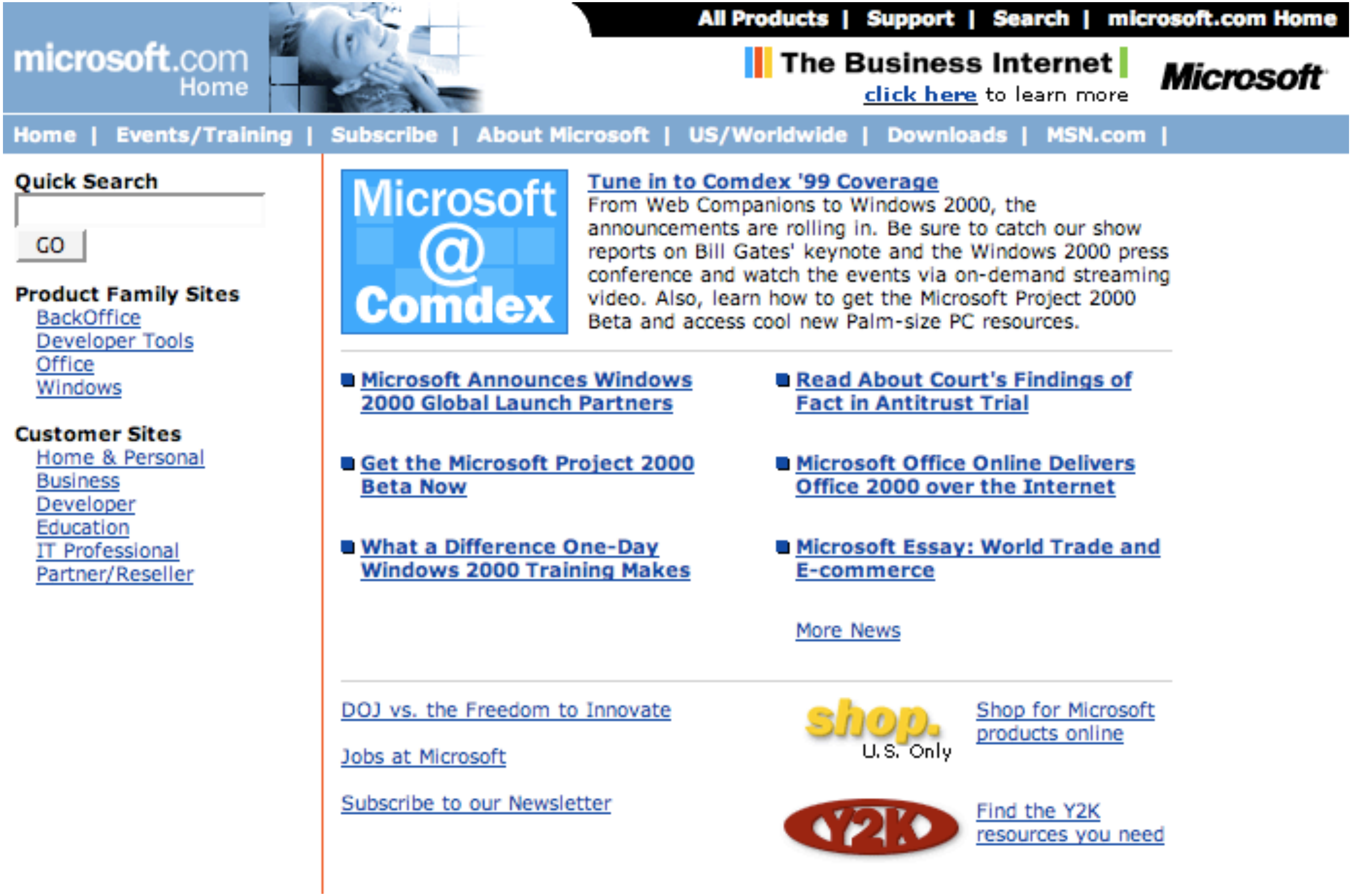
- Y! Travel - plan your holiday travel
- Looking for a car? job? house?

more...

Inside Yahoo!

- Yahoo! GeoCities - build your free home page
- Y! Games - hearts, backgammon, chess
- Y! Greetings - free greeting cards

more...



All Products | Support | Search | microsoft.com Home

microsoft.com Home

The Business Internet

click here to learn more

Microsoft

Home | Events/Training | Subscribe | About Microsoft | US/Worldwide | Downloads | MSN.com |

Quick Search

GO

Product Family Sites

- BackOffice
- Developer Tools
- Office
- Windows

Customer Sites

- Home & Personal
- Business
- Developer
- Education
- IT Professional
- Partner/Reseller

Tune in to Comdex '99 Coverage

From Web Companions to Windows 2000, the announcements are rolling in. Be sure to catch our show reports on Bill Gates' keynote and the Windows 2000 press conference and watch the events via on-demand streaming video. Also, learn how to get the Microsoft Project 2000 Beta and access cool new Palm-size PC resources.

- **Microsoft Announces Windows 2000 Global Launch Partners**
- **Get the Microsoft Project 2000 Beta Now**
- **What a Difference One-Day Windows 2000 Training Makes**
- **Read About Court's Findings of Fact in Antitrust Trial**
- **Microsoft Office Online Delivers Office 2000 over the Internet**
- **Microsoft Essay: World Trade and E-commerce**

More News

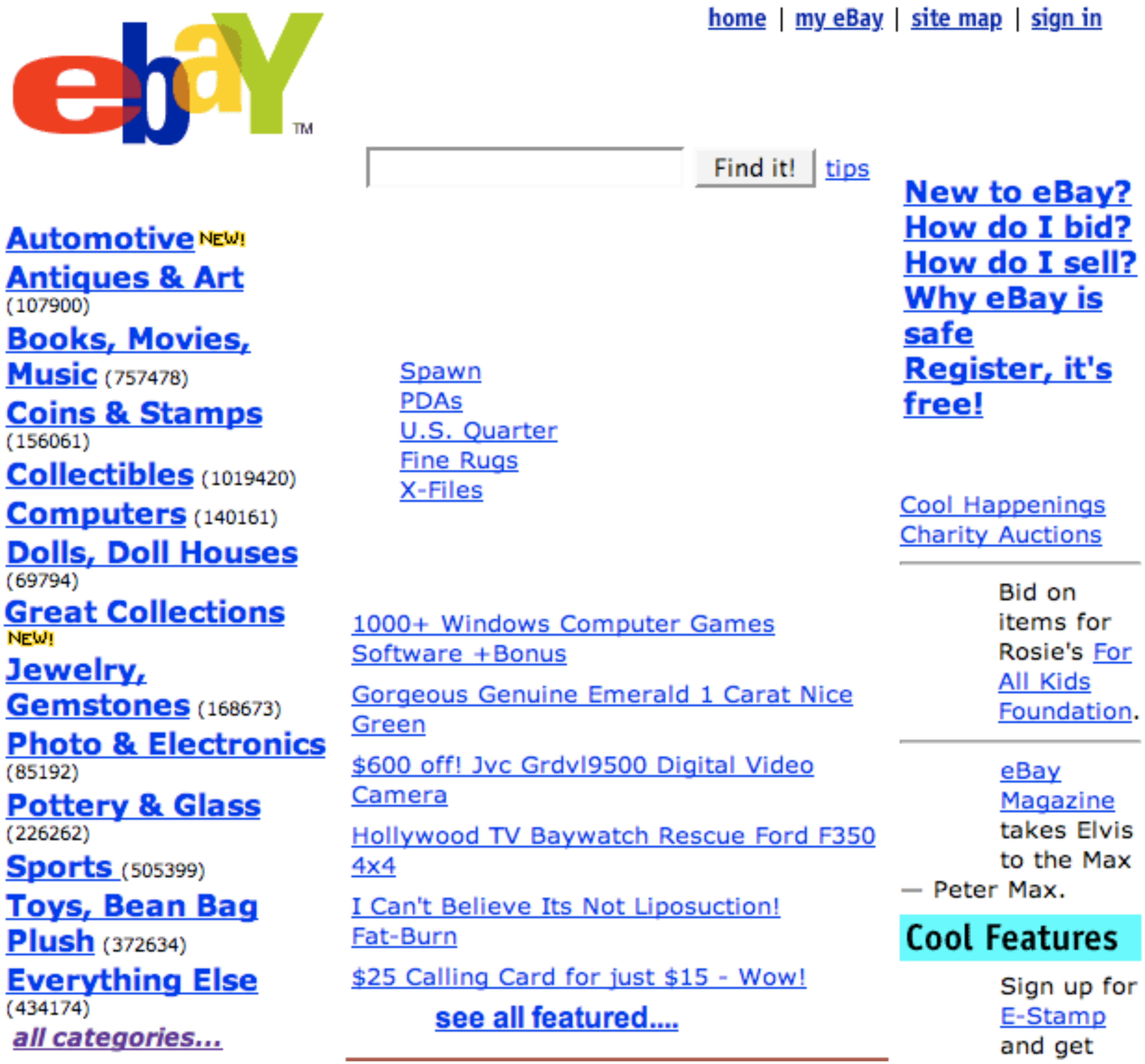
DOJ vs. the Freedom to Innovate

Jobs at Microsoft

Subscribe to our Newsletter

Shop for Microsoft products online

Find the Y2K resources you need



home | my eBay | site map | sign in

Find it! tips

Automotive NEW!

Antiques & Art (107900)

Books, Movies, Music (757478)

Coins & Stamps (156061)

Collectibles (1019420)

Computers (140161)

Dolls, Doll Houses (69794)

Great Collections NEW!

Jewelry, Gemstones (168673)

Photo & Electronics (85192)

Pottery & Glass (226262)

Sports (505399)

Toys, Bean Bag Plush (372634)

Everything Else (434174)

all categories...

Spawn
PDAs
U.S. Quarter
Fine Rugs
X-Files

1000+ Windows Computer Games Software +Bonus

Gorgeous Genuine Emerald 1 Carat Nice Green

$600 off! Jvc Grdvl9500 Digital Video Camera

Hollywood TV Baywatch Rescue Ford F350 4x4

I Can't Believe Its Not Liposuction! Fat-Burn

$25 Calling Card for just $15 - Wow!

see all featured....

New to eBay?
How do I bid?
How do I sell?
Why eBay is safe
Register, it's free!

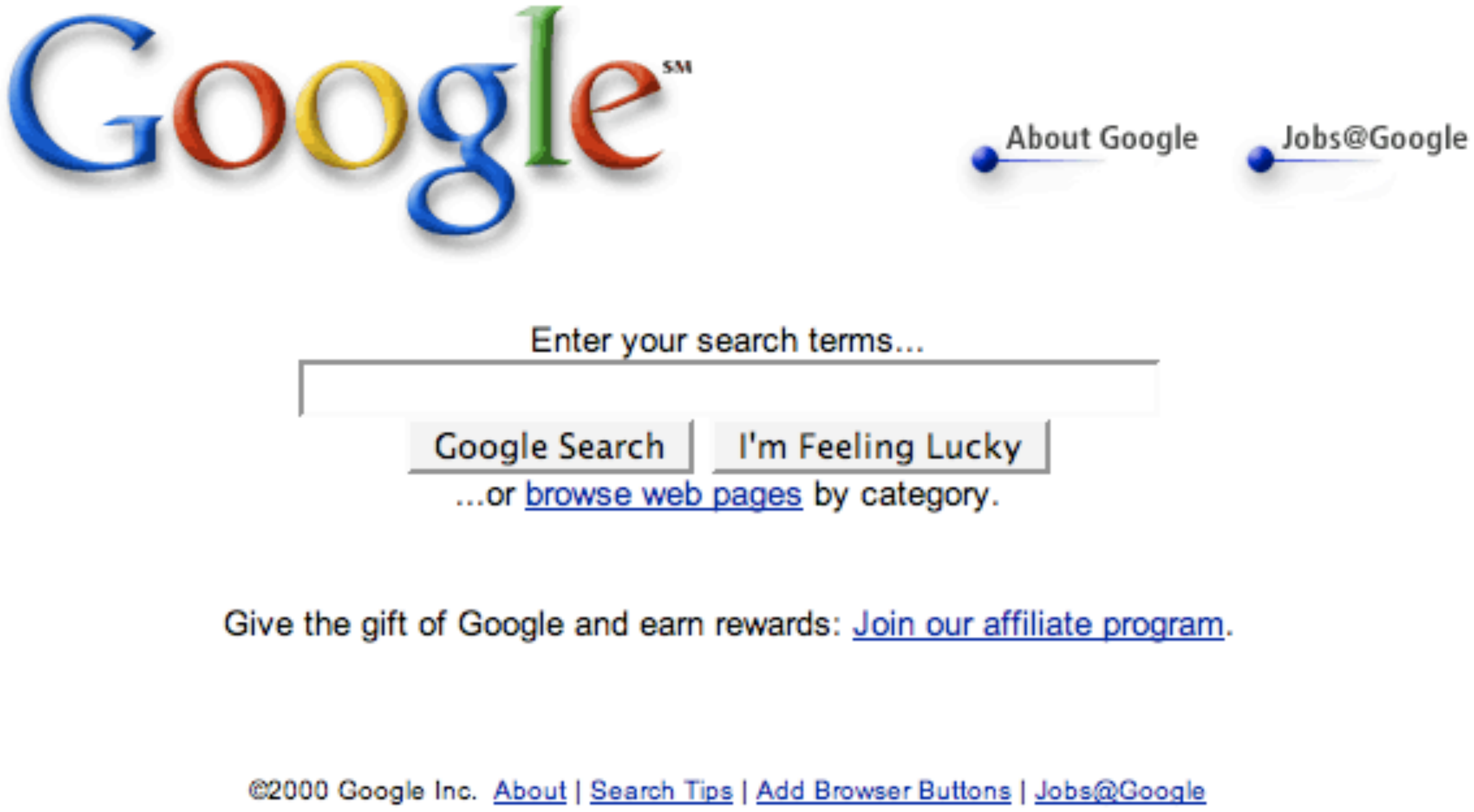
Cool Happenings
Charity Auctions

Bid on items for Rosie's For All Kids Foundation.

eBay Magazine takes Elvis to the Max — Peter Max.

Cool Features

Sign up for E-Stamp and get



Enter your search terms...

...or browse web pages by category.

Give the gift of Google and earn rewards: Join our affiliate program.

©2000 Google Inc. About | Search Tips | Add Browser Buttons | Jobs@Google

Who?

February, 2000

11,000,000

Web servers

Netcraft
http://survey.netcraft.com/index-200002.html

October, 2007

142,000,000

Web servers

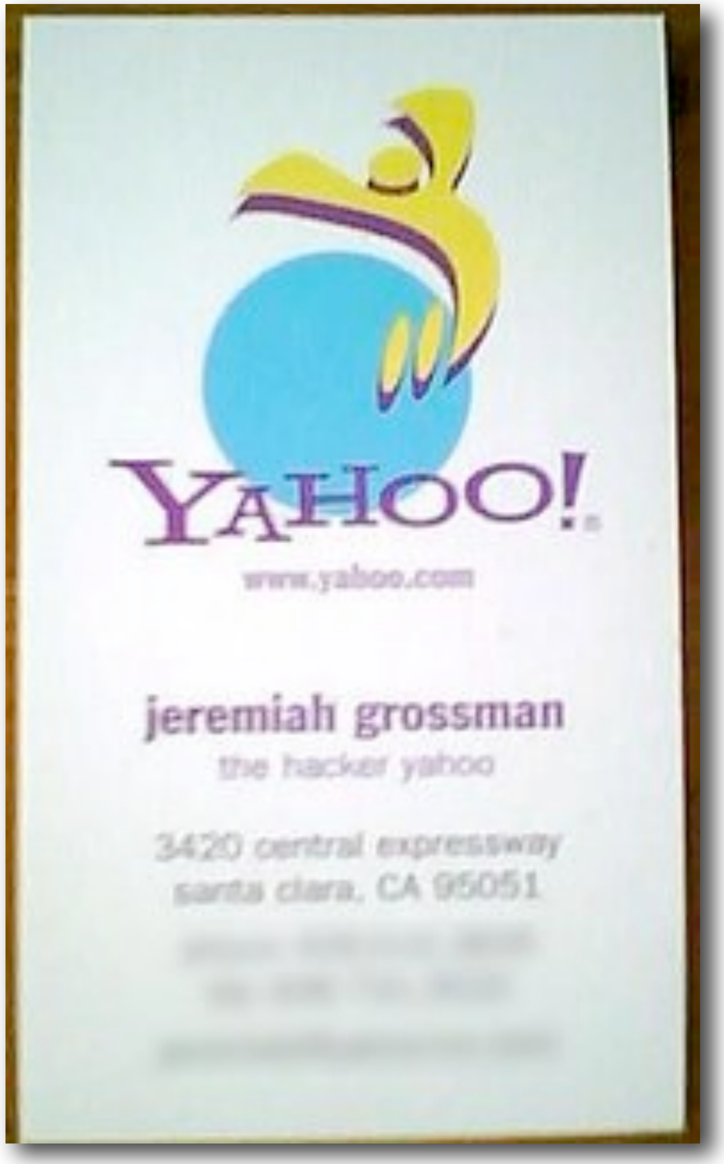
Netcraft

http://survey.netcraft.com/index-200002.html

YAHOO!®

600 websites, 17,000 publicly facing web servers, and 120 millions users

2000-2001



YAHOO!

www.yahoo.com

jeremiah grossman
the hacker yahoo

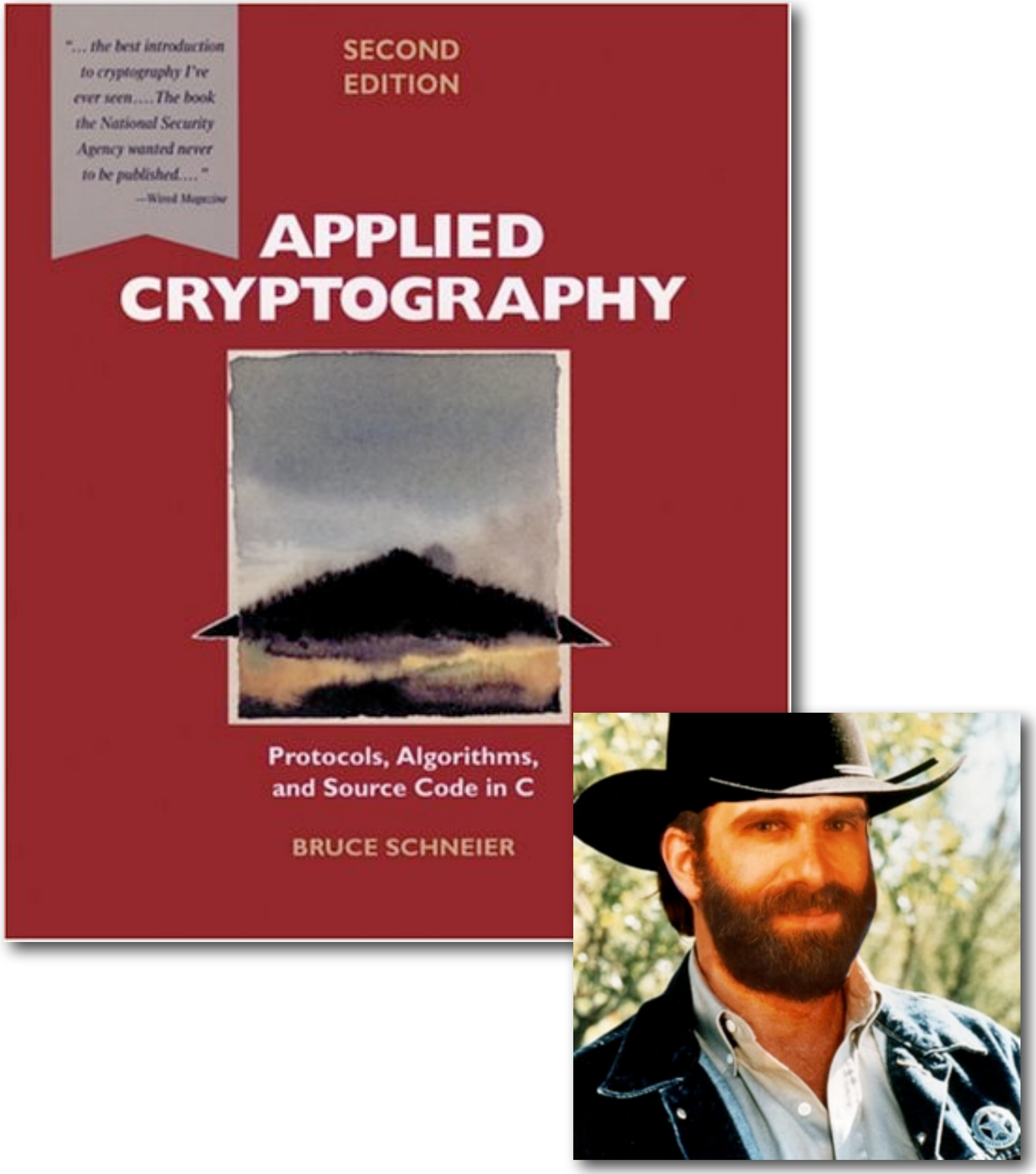
3420 central expressway
santa clara, CA 95051

[redacted]

Official Title

“the hacker yahoo”

Hack Everything!



"... the best introduction to cryptography I've ever seen.... The book the National Security Agency wanted never to be published...."

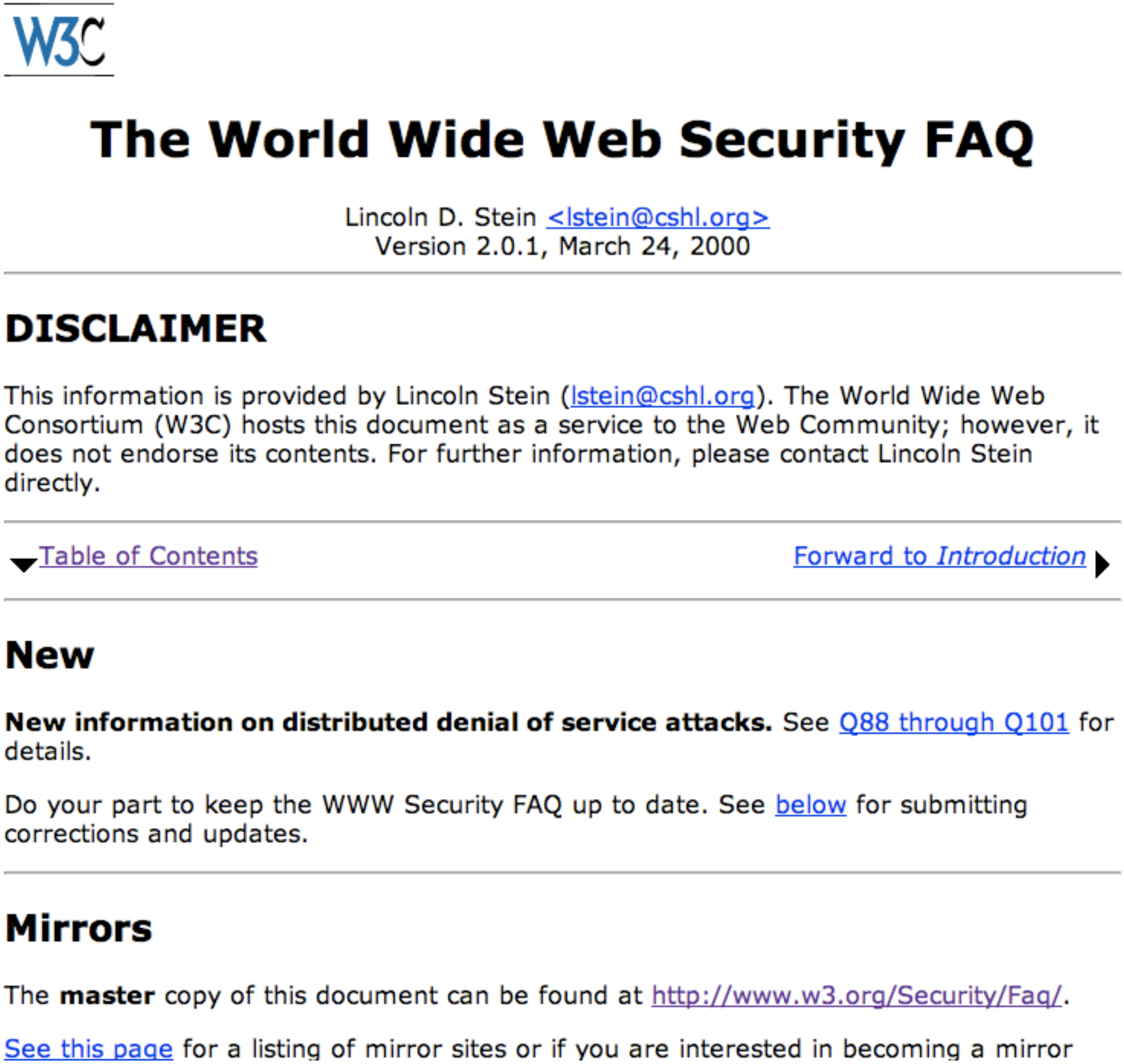
—Wired Magazine

SECOND EDITION

APPLIED CRYPTOGRAPHY

Protocols, Algorithms, and Source Code in C

BRUCE SCHNEIER



The World Wide Web Security FAQ

Lincoln D. Stein <lstein@cshl.org>
Version 2.0.1, March 24, 2000

DISCLAIMER

This information is provided by Lincoln Stein (lstein@cshl.org). The World Wide Web Consortium (W3C) hosts this document as a service to the Web Community; however, it does not endorse its contents. For further information, please contact Lincoln Stein directly.

▼Table of Contents Forward to *Introduction* ▶

New

New information on distributed denial of service attacks. See Q88 through Q101 for details.

Do your part to keep the WWW Security FAQ up to date. See below for submitting corrections and updates.

Mirrors

The **master** copy of this document can be found at http://www.w3.org/Security/Faq/.

See this page for a listing of mirror sites or if you are interested in becoming a mirror

http://www.w3.org/Security/Faq/

Security for Users, Administrators & ISPs

2nd Edition
Expanded & Updated

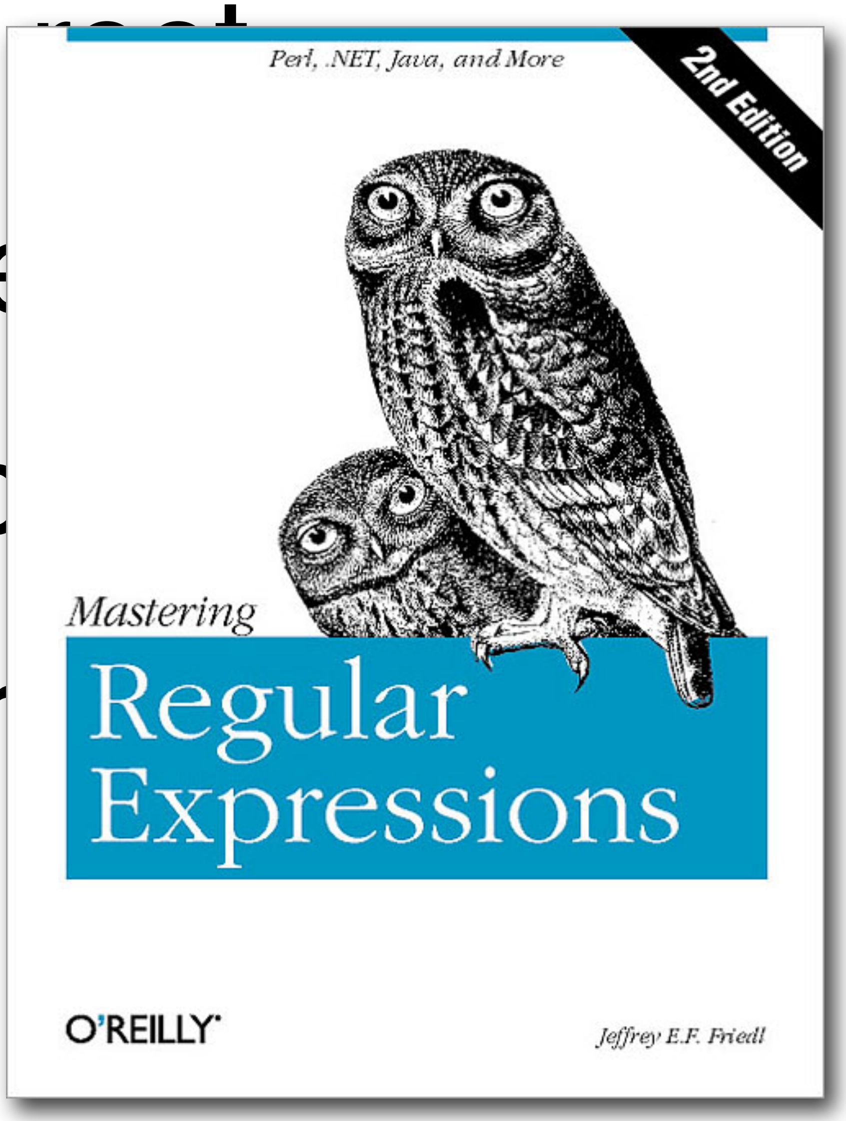
Web Security, Privacy & Commerce

O'REILLY®

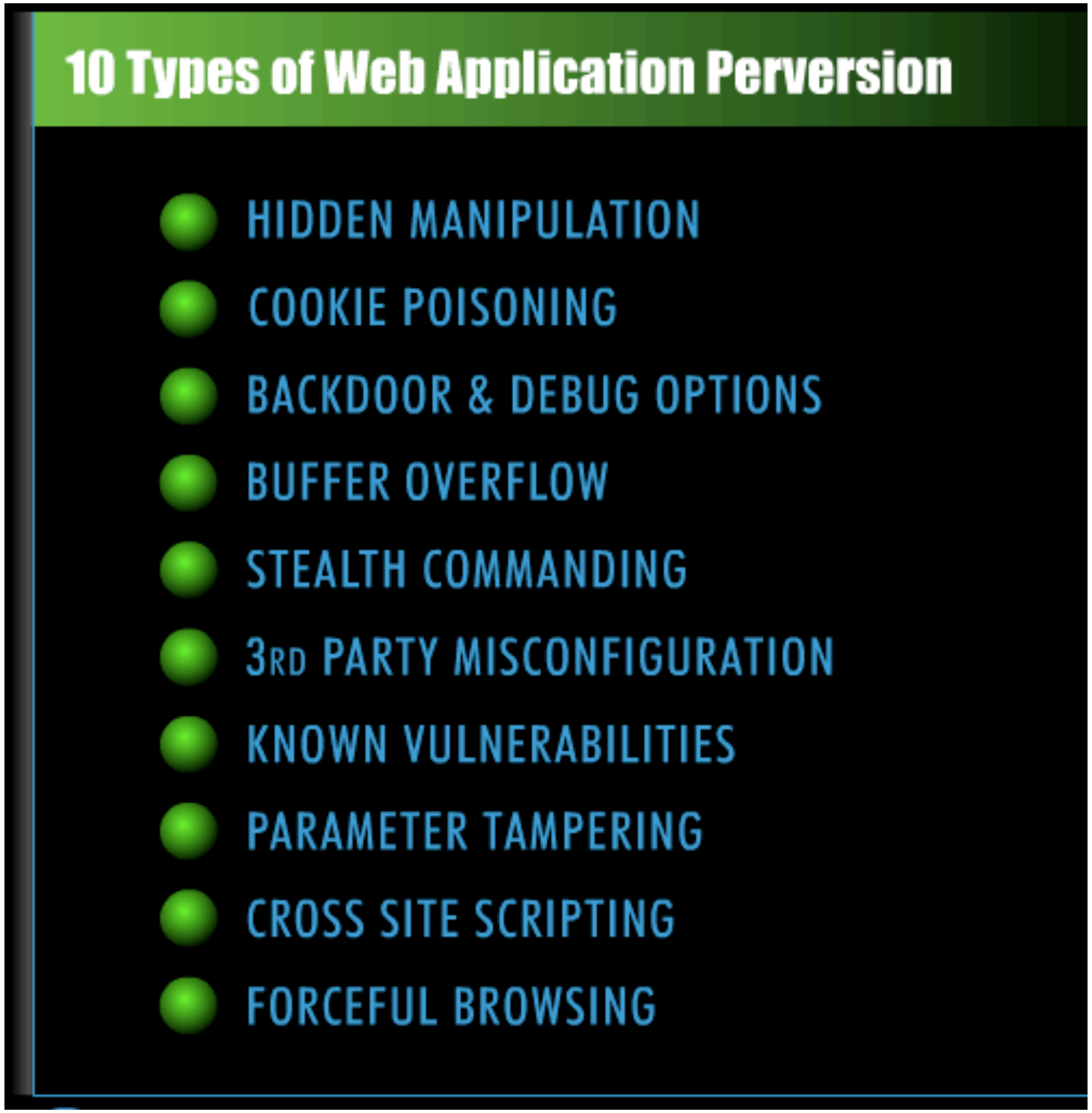
Simson Garfinkel with Gene Spafford

- ☑ Don’t write your own crypto algorithms
- ☑ Don’t run web servers as
- ☑ Use Secure Sockets Laye
- ☑ Have proper file system p
- ☑ A paragraph about the vir

Validation!



Wait, how does this make a website secure?



10 Types of Web Application Perversion

- HIDDEN MANIPULATION
- COOKIE POISONING
- BACKDOOR & DEBUG OPTIONS
- BUFFER OVERFLOW
- STEALTH COMMANDING
- 3RD PARTY MISCONFIGURATION
- KNOWN VULNERABILITIES
- PARAMETER TAMPERING
- CROSS SITE SCRIPTING
- FORCEFUL BROWSING

And nothing else.

...No books...

...No white papers...

...No methodologies...

NOTHING!

...except for some guy named **rain.forest.puppy** would was writing something obscure about poison null-byte and SQL Injection.

www-mobile-code

From: Mark Curphey (markcurphey.com)
Date: Wed Sep 19 2001 - 01:23:05 CDT

Methodology - That sounds like a great idea and a great opportunity! You know what; I can even donate 50 mb of web space on a hosted server I have access to, to house it and I am sure it can go back on the securityfocus site as well. Hows that...

Maybe we could do it like this.....

Consensus agreement on a template of what to include, mission statement, licensing model, format, development model etc.

Things to think about.

Mission I think we should aim to build an open-source, recognized standard that covers design, development and deployment. It could include as a minimum both "How to design and build secure web applications" and " How to test the security of web applications" (black box and white box). Any thing else ? David Wheeler has done a good job of some of this stuff, you may want to take a look. www.dwheeler.com

If subject matter experts came forward they could be ultimately responsible for each section. We could take the content template and assign a week on the list when that topic could be debated along-side regular stuff. The subject matter expert could prepare his draft for submission at the beginning of that week, amendments / inclusions proposed during the week with the finalized section being represented a week after. **I guess some topics may need several weeks ?**

...
should first agree on the mission and development model, ideas for nominating subject matter experts, the subject matter, licensing models etc...I'll summarize discussions in to a plan at the end of say next week and we can go from there !

Great idea !

http://archives.neohapsis.com/archives/sf/www-mobile/2001-q3/0089.html

Dennis Groves

Me

Bill Pennington

OWASP.ORG

OWASP focused on “Application” and “Software” security...

The industry still desperately needed standardized terminology, processes to compare methodologies, and visibility into web application security.

Robert Auger	CGISecurity
Ryan C. Barnett	Breach Security
Yuval Ben-Itzhak	Finjan
Erik Caso	NT OBJECTives, Inc.
Jeremiah Grossman	WhiteHat Security
Sverre Huseby	Heimdall
Amit Klein	Individual
Aaron C. Newman	Application Security, Inc.
Steve Orrin	Watchfire / Intel
Bill Pennington	WhiteHat Security
Ivan Ristic	Thinking Stone (ModSecurity)
Ory Segal	Watchfire
Ofer Shezaf	Breach Security
Caleb Sima	SPI Dynamics

WEBAPPSEC.ORG

To develop, adopt, and advocate standards for web application security.

WASC is an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web.

2004

Web Security Mailing List

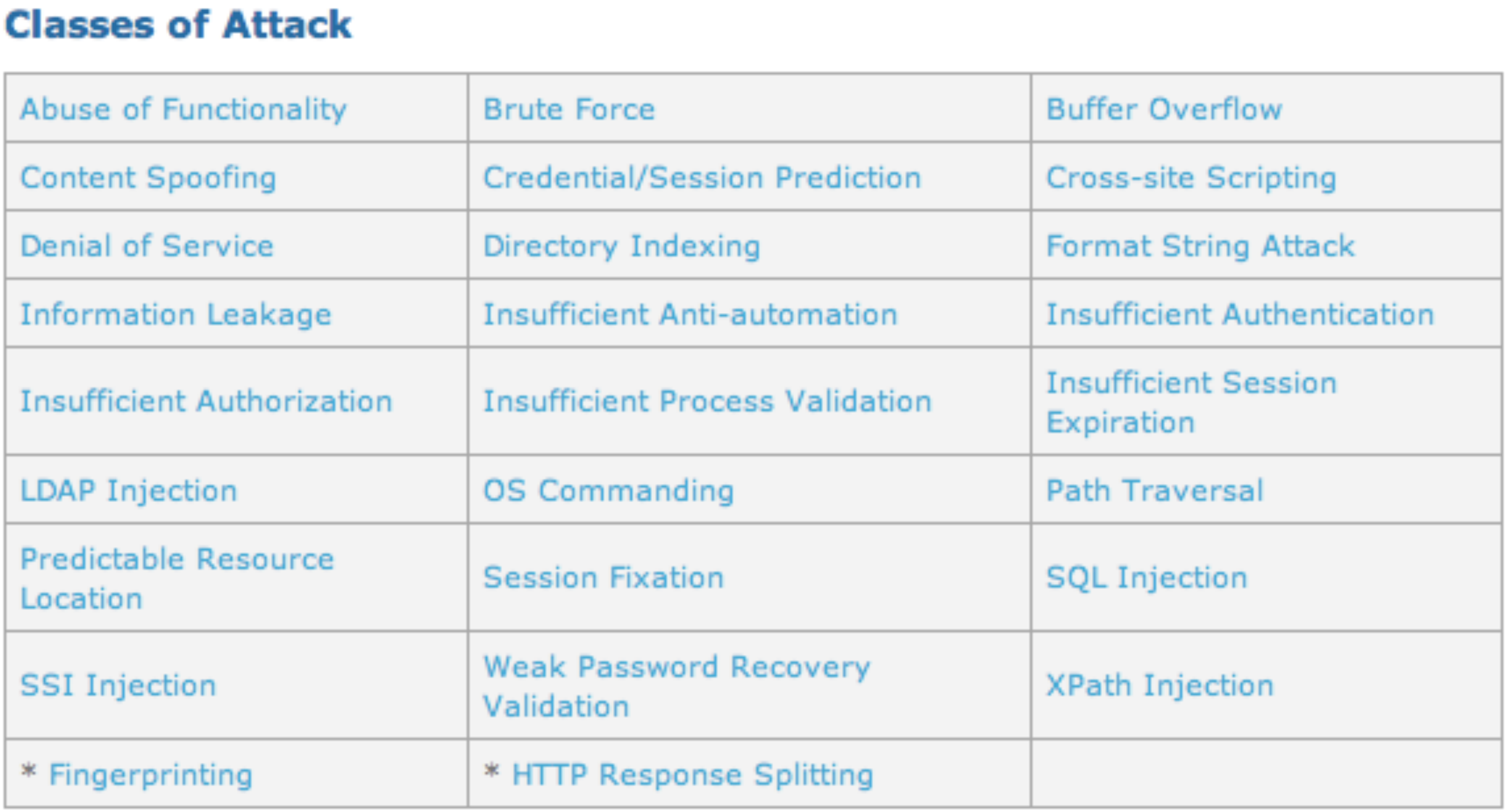
#1 Mailing List

2,600 Subscribers

http://www.webappsec.org/lists/websecurity/

Threat Classification

“A cooperative effort to clarify and organize the threats to the security of a web site”



Classes of Attack

Abuse of Functionality	Brute Force	Buffer Overflow
Content Spoofing	Credential/Session Prediction	Cross-site Scripting
Denial of Service	Directory Indexing	Format String Attack
Information Leakage	Insufficient Anti-automation	Insufficient Authentication
Insufficient Authorization	Insufficient Process Validation	Insufficient Session Expiration
LDAP Injection	OS Commanding	Path Traversal
Predictable Resource Location	Session Fixation	SQL Injection
SSI Injection	Weak Password Recovery Validation	XPath Injection
* Fingerprinting	* HTTP Response Splitting	

81 pages authored by 18 web security pros

Wide industry support and adoption

Translated into 6 languages

Version 2 underway, led by Robert Auger (eBay)

hacked

myspace.com a place for friends
verizon
TIFFANY & Co.
PayPal
XLI
NOKIA Connecting People
Georgia Tech
Macworld Conference & Expo
DUKE UNIVERSITY School of Medicine
T·J·maxx
Microsoft Passport Network
Google
STANFORD UNIVERSITY»
CNBC
Mizzou University of Missouri-Columbia
Scottrade More broker for your money.
SUNTRUST
University of Idaho Open Space. Open Minds.
THE UNIVERSITY OF CHICAGO
USDA
UNIVERSITY of VIRGINIA
ebay
PAPA JOHN'S Better Ingredients. Better Pizza.
USC
travelocity
VICTORIA'S SECRET

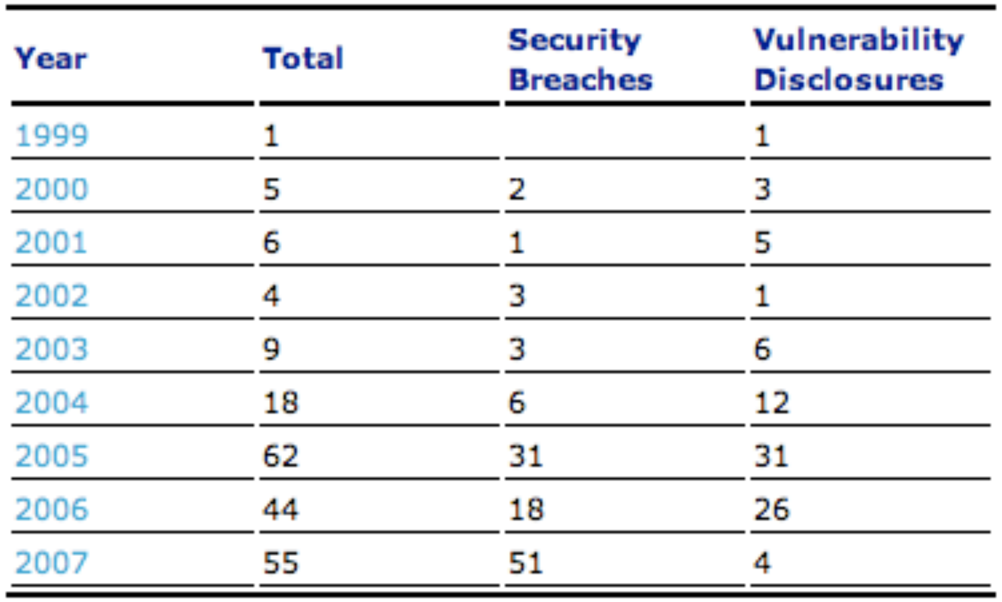
Web Hacking Incident Database

“Web hacking incident database (WHID) is dedicated to maintaining a list of web applications related security incidents.”

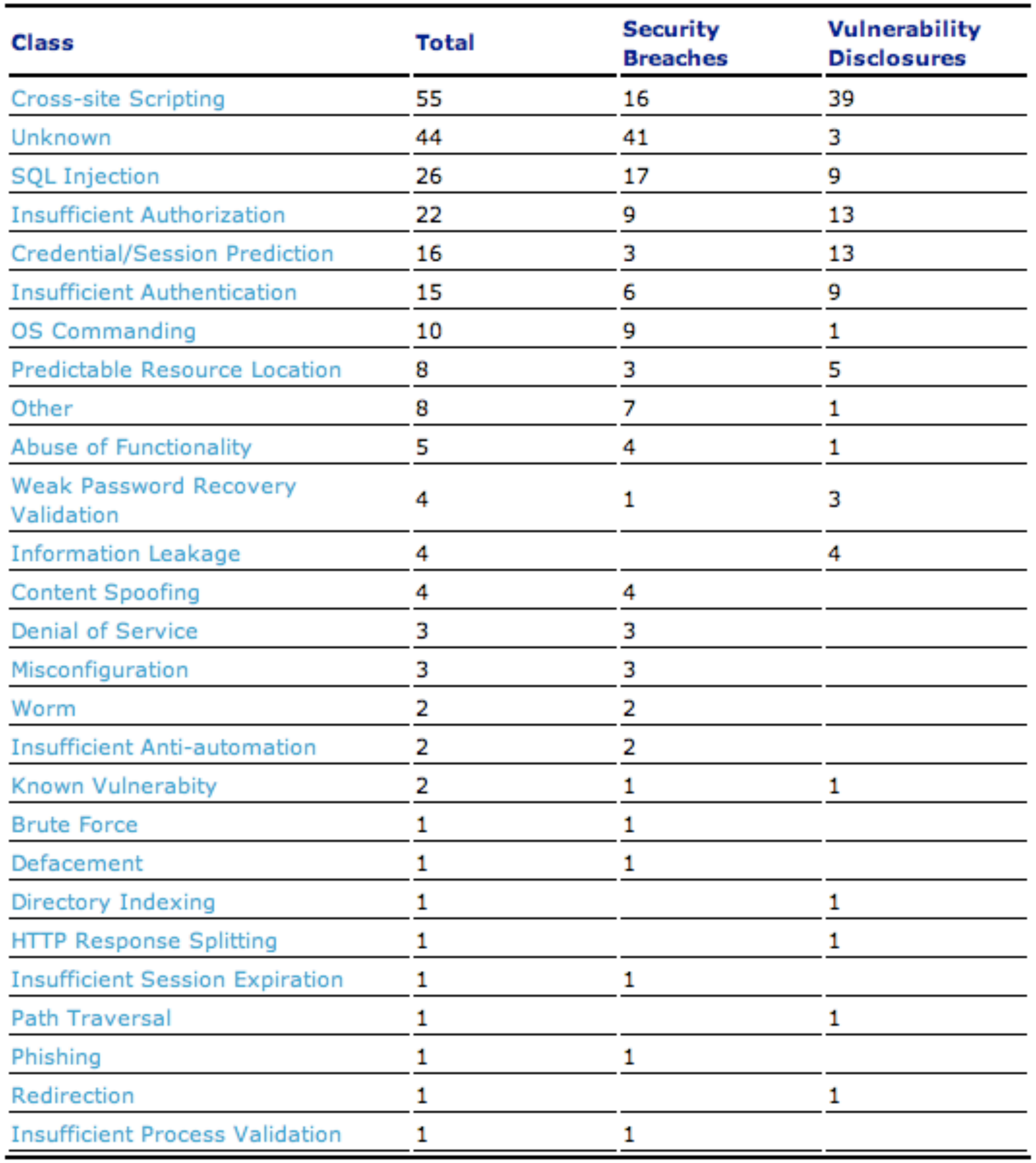
Managed and updated by O

The most comprehensive gu

related security incidents.



Year	Total	Security Breaches	Vulnerability Disclosures
1999	1		1
2000	5	2	3
2001	6	1	5
2002	4	3	1
2003	9	3	6
2004	18	6	12
2005	62	31	31
2006	44	18	26
2007	55	51	4



Class	Total	Security Breaches	Vulnerability Disclosures
Cross-site Scripting	55	16	39
Unknown	44	41	3
SQL Injection	26	17	9
Insufficient Authorization	22	9	13
Credential/Session Prediction	16	3	13
Insufficient Authentication	15	6	9
OS Commanding	10	9	1
Predictable Resource Location	8	3	5
Other	8	7	1
Abuse of Functionality	5	4	1
Weak Password Recovery Validation	4	1	3
Information Leakage	4		4
Content Spoofing	4	4	
Denial of Service	3	3	
Misconfiguration	3	3	
Worm	2	2	
Insufficient Anti-automation	2	2	
Known Vulnerabity	2	1	1
Brute Force	1	1	
Defacement	1	1	
Directory Indexing	1		1
HTTP Response Splitting	1		1
Insufficient Session Expiration	1	1	
Path Traversal	1		1
Phishing	1	1	
Redirection	1		1
Insufficient Process Validation	1	1	

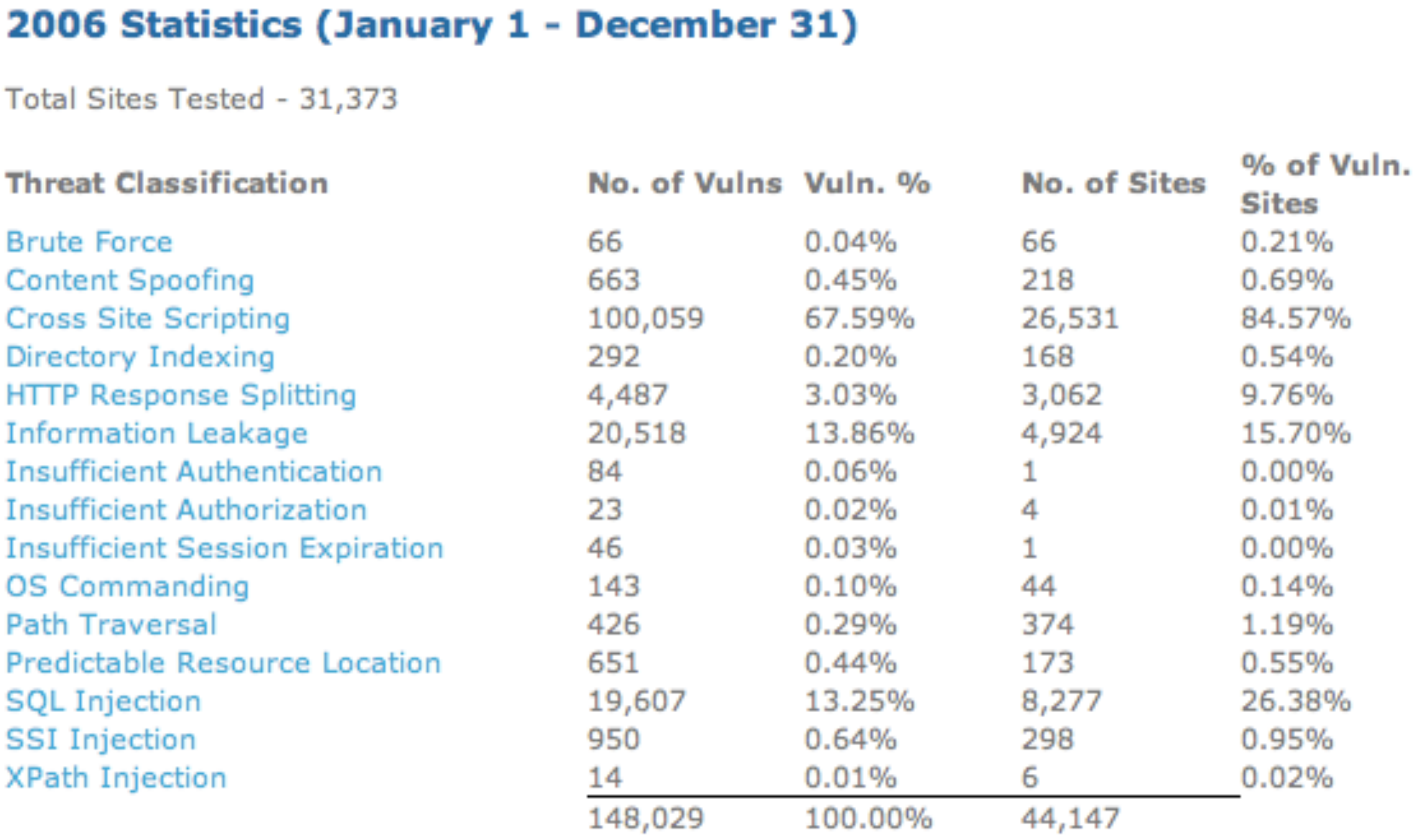
Statistics

“Industry wide collection of application vulnerability statistics in order to identify the existence and proliferation of application security issues on enterprise websites.”

Led by Michael Sutton (HP)

5 organizations currently contributing data

First report has been released



2006 Statistics (January 1 - December 31)

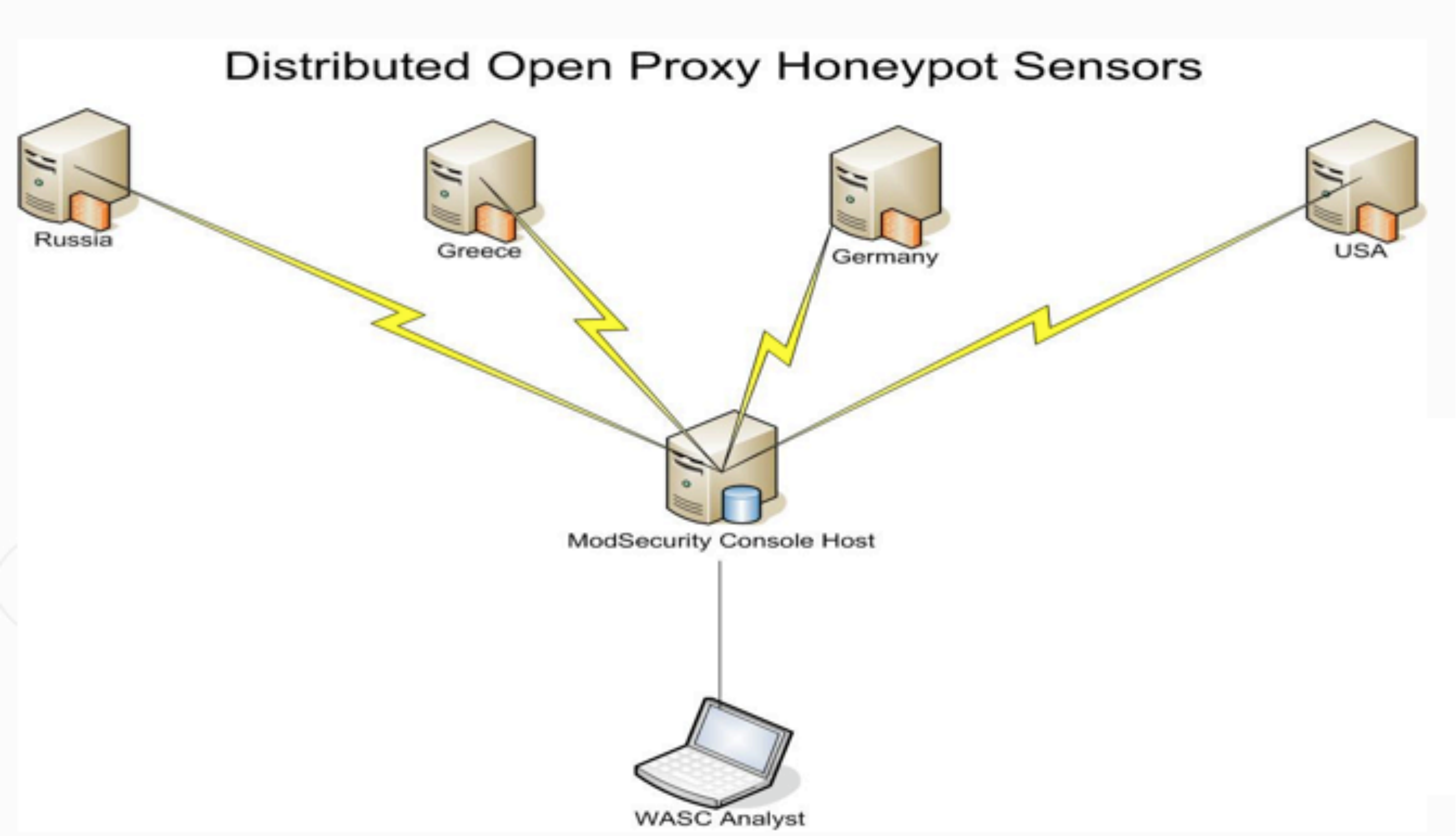
Total Sites Tested - 31,373

Threat Classification	No. of Vulns	Vuln. %	No. of Sites	% of Vuln. Sites
Brute Force	66	0.04%	66	0.21%
Content Spoofing	663	0.45%	218	0.69%
Cross Site Scripting	100,059	67.59%	26,531	84.57%
Directory Indexing	292	0.20%	168	0.54%
HTTP Response Splitting	4,487	3.03%	3,062	9.76%
Information Leakage	20,518	13.86%	4,924	15.70%
Insufficient Authentication	84	0.06%	1	0.00%
Insufficient Authorization	23	0.02%	4	0.01%
Insufficient Session Expiration	46	0.03%	1	0.00%
OS Commanding	143	0.10%	44	0.14%
Path Traversal	426	0.29%	374	1.19%
Predictable Resource Location	651	0.44%	173	0.55%
SQL Injection	19,607	13.25%	8,277	26.38%
SSI Injection	950	0.64%	298	0.95%
XPath Injection	14	0.01%	6	0.02%
	148,029	100.00%	44,147	

Distributed Open Proxy Honeypot

“Use one of the web attacker's most trusted tools against him - the Open Proxy server. Instead of being the target of the attacks, we opt to be used as a conduit of the attack data in order to gather our intelligence”

Led by Ryan Barnett (Breach)
Web Security Threat Report, Volume 1: January April 2007
9 million requests in Oct, and 3 million were “attacks”



Web Application Firewall Evaluation Criteria (WAFEC)

“Develop a detailed web application firewall (WAF) evaluation criteria; a testing methodology that can be used by any reasonably skilled technician to independently assess the quality of a WAF solution.”

Led by Ivan Ristic (Breach)
26 contributors, most WAF vendors onboard
Basis in the Forrester WAF evaluation in 2006
Regularly cited when RFIs are sent to WAF vendors

Web Application Security Scanner Evaluation Criteria (WASSEC)

“Set of guidelines to evaluate web application security scanners on their identification of web application vulnerabilities and its completeness.”

Led by Anurag Agarwal
90 participants, most scanner vendors contributing

Hundreds of contributors

...OWASP...

...NIST...

...SANS...

Its a community

Web Hacking
Attacks and Defe
Stuart McClure
Saumil Shah
Shreeraj Shah
Web Application Security
Apache Security
The Complete Guide to Securing Your Apache Web Server
O'REILLY
Hacker's Challenge 3
20 Brand New Forensic Scenarios & Solutions
Hack Notes
Web Security Portable Reference
Mike Shema
How to Break Software Security
James A. Whittaker
Herbert H. Thompson
Innocent Code
a security wake-up call for web programmers
Sverre H. Huseby
Exploiting Software
How to Break Code
Hack Proofing Your Web Applications
Hacking Web Applications Exposed
Web Security Secrets & Solutions
Joel Scambray, Mike Shema & Caleb Sima
Search Inside!
The Web Application Hacker's Handbook
Discovering and Exploiting Security Flaws
Testing Web Security
Assessing the Security of Web Sites and Applications
WILEY
XSS Exploits
Cross Site Scripting Attacks and Defense
4 Free Booklets
Seth Fogie
Jeremiah Grossman
Robert Hansen
Anton Rager
Preventing Web Attacks with Apache
Improving Web Application Security
Threats and Countermeasures
Web Application Security Assessment
Microsoft
Web Security, Privacy & Commerce
O'REILLY
Professional Pen Testing
Pen Testing Web Applications
Wrox
Hacking the Code
ASP.NET Web Application Security
Mark M. Burnett
James C. Foster

A lot still needs to be done...

Browser Security

Ajax Development

Security standards

Thank You!