Welcome to OWASP Bay Area Application Security Summit July 23rd, 2009

OWASP

July 23rd, 2009

Mandeep Khera
OWASP Bay Area Chapter Leader
mkhera@owasp.org
mandeep@cenzic.com
Phone: 408-200-0712

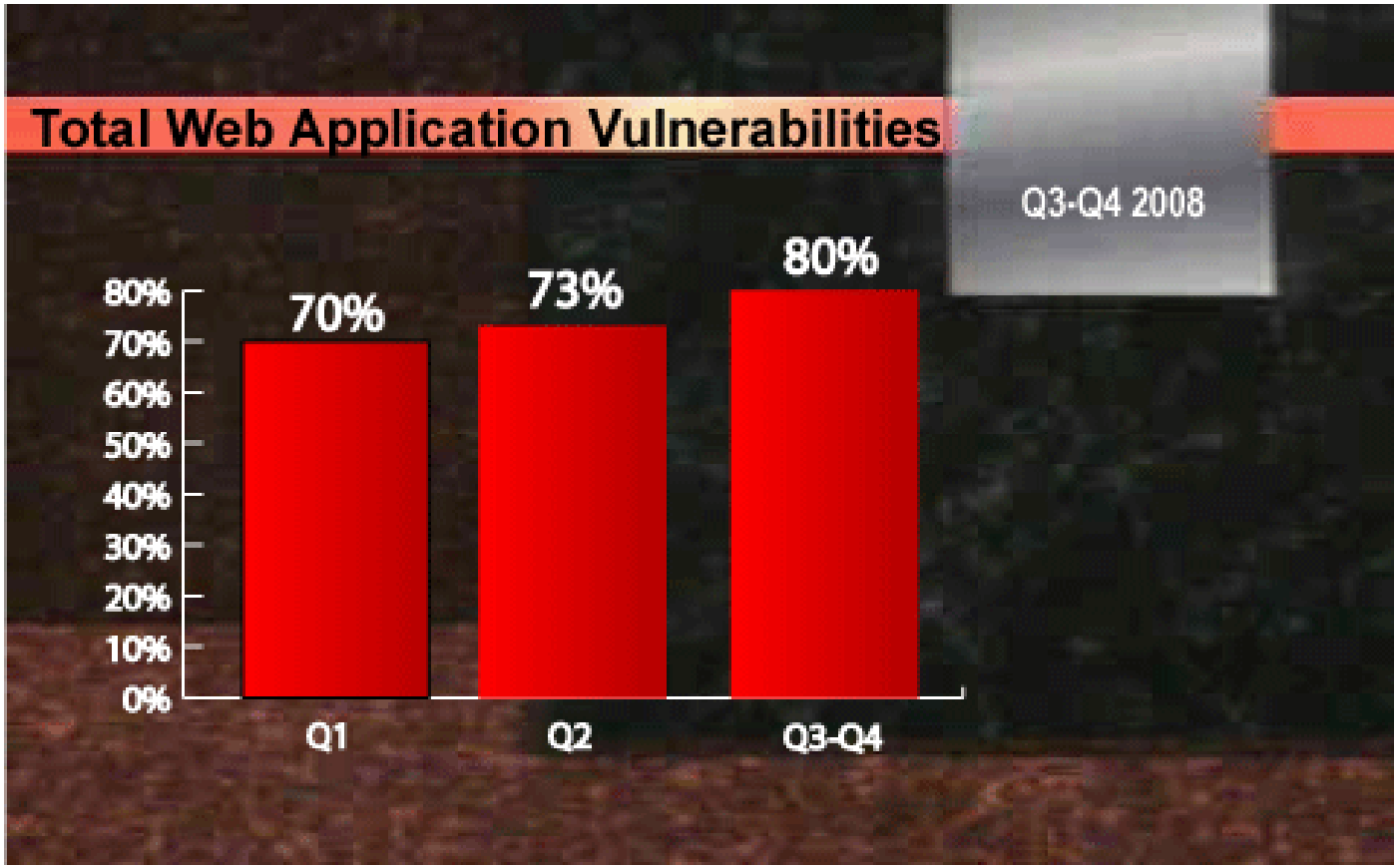
The OWASP Foundation
http://www.owasp.org

Agenda

- 1.30 – 1.45 - Welcome, Overview – Mandeep Khera
- 1.45 – 2.30 - Development Issues within AJAX Applications: How to Divert Threats - Lars Ewe, CTO, Cenzic
- 2.30 – 3.30 – Building a Corporate App Security Assessment Program- Rob Jerdonek and Topher Chung, Intuit
- 3.30 – 4.00 - Networking Break
- 4.00 – 5.00 – Mastering Session Management - Siva Ram, Lead Security Consultant, AppSec Consulting
- 5.00 – 6.00 – From Rivals to BFF: WAF & VA Unite - Brian Contos, Chief Security Strategist, Imperva
- 6.00 – 8.00 – Networking Reception – Food and Drinks

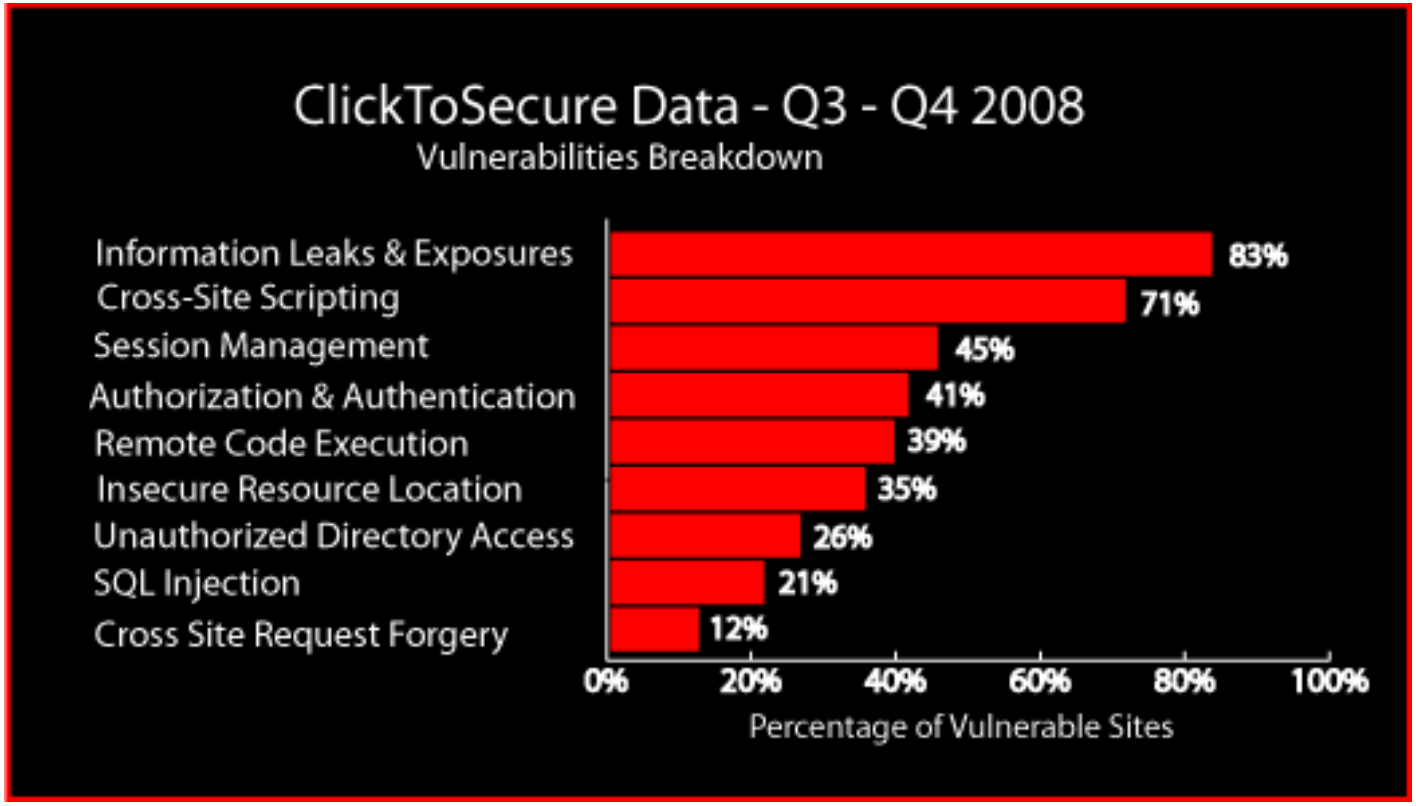
Thanks to our sponsors!!

Web Vulnerabilities Trend



Source: Cenzic Q3-Q4 Trends Report

Breakdown of Vulnerabilities



Source: **Cenzic Q3-Q4, 2008 Application Trends Report**

No One Wants To Be in the Press

TJX hack is biggest ever

30th March 2007

By Kevin Murphy

Print Friendly | Email Article | Your Opinion | Email Alerts

At least 45.7 million credit card numbers were stolen by criminal hackers from TJX, a major global retailer, making the attack the largest recorded such data theft to date.

Hackers breach Heartland Payment credit card system

Theft Could Possibly be the Largest Credit Card Crime in History

By Byron Acohido, USA TODAY

January 20, 2009

USA TODAY

33 comments

Obama site hacked, redirects clicks to Clinton's site - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://computerworld.com/action/article.do?command=

Security

JUMP TO More Resources SEARCH

VeriSign View our white papers » | Business Should Know Security and Consumer Trust | Maximizing Site Visitor Trust Using Extended Validation SSL | The Latest Advancements in SSL Technology

Home | News | E-mail Newsletters | Blogs

Obama site hacked, redirects clicks to Clint

Cross-site scripting bug fixed, but researchers say others exist

By Gregg Keizer Comments 5 Recommended 95 Share

April 21, 2008 (Computerworld) A cross-site scripting vulnerability in the social networking section of Sen. Barack Obama's campaign site was

RESOURCE ALERTS

SIGN-UP to receive Securi Alerts

Technology & science / Security

Categories: U.S. news | World news

Hacker forces 1,500 Pentagon computers offline

Defense secretary: Department sees hundreds of cyber attacks a day

E-mail this page | Print this page | BOOKMARK

Firefox prevented this site from opening 2 popup windows. Options

Security

JUMP TO More Resources SEARCH

VeriSign | How to Offer the Strongest SSL Encryption | Using EV Certificates Overstock.com Sees Less Shopping Cart Abandonment | What Every about SSL

Home | News | E-mail Newsletters | Blogs | Tech Dispenser

Mass hack infects tens of thousands of sites

Then they serve visitors multiple exploits, including October RealPlayer attack

Gregg Keizer Today's Top Stories » or Other Security Stories »

Report: Mass Injection Attack Affects 40,000 Websites

Exploit appears similar, but unrelated, to Gumblar, researchers say

Subscribe: GET OUR E-NEWSLETTER | RSS FEEDS | FOLLOW US ON TW

cnet news

Latest News | Crave | Webware | Business Tech | Green Tech | Wirele

Home » News » Security

Security

May 7, 2009 3:59 PM PDT

Report: Hackers broke into FAA air traffic control systems

by Elinor Mills

Font size | Print | E-mail | Share | 37 comments

CIA: Hackers have already attacked the electric grid

By Preston Gralla, March 26, 2009

« Prev Post | All Posts | Next Post »

EMAIL | PRINT | RSS | READ COMMENTS

In the past week, there's been a good deal of publicity about security holes in the Smart Grid, making it a potential hacker's

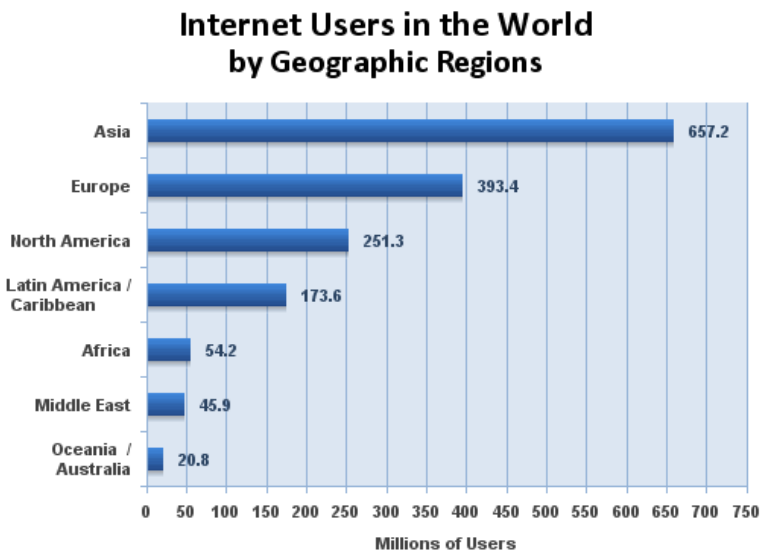
Why Is App Security a Must Now?

- Over 285M records compromised in 2008
  - 99.6% compromised from servers and applications
- Hackers are attacking every one
  - Banks, Credit Unions, Government Agencies, Small companies, Large companies – **Equal opportunity**
- 80% of vulnerabilities are in apps
  - Hacker go where there are holes
- Regulations
  - Payment Card Industry (PCI) continues to drive the need for app security; other new regulations also coming

Internet Usage Continues to Grow

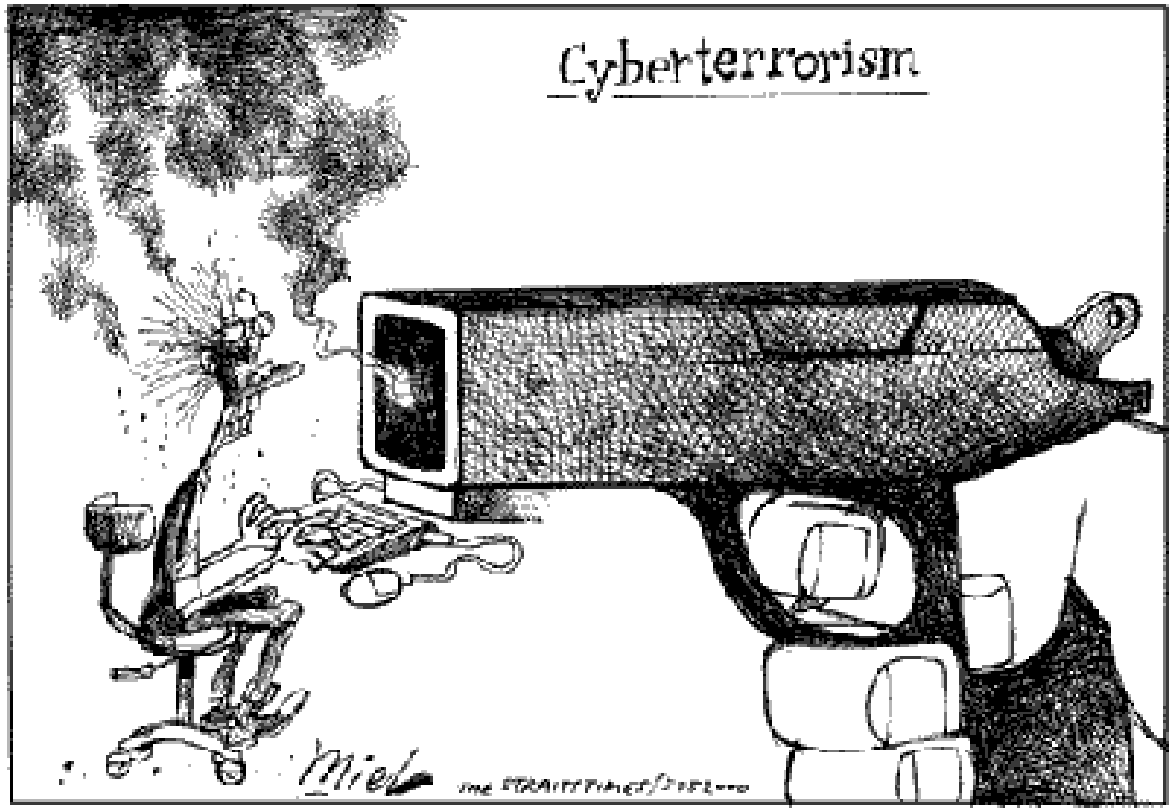
WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2008 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Users Growth 2000-2008	Users % of Table
Africa	975,330,899	4,514,400	**54,171,500**	5.6 %	1,100.0 %	3.4 %
Asia	3,780,819,792	114,304,000	**657,170,816**	17.4 %	474.9 %	41.2 %
Europe	803,903,540	105,096,093	**393,373,398**	48.9 %	274.3 %	24.6 %
Middle East	196,767,614	3,284,800	**45,861,346**	23.3 %	1,296.2 %	2.9 %
North America	337,572,949	108,096,800	**251,290,489**	74.4 %	132.5 %	15.7 %
Latin America/Caribbean	581,249,892	18,068,919	**173,619,140**	29.9 %	860.9 %	10.9 %
Oceania / Australia	34,384,384	7,620,480	**20,783,419**	60.4 %	172.7 %	1.3 %
WORLD TOTAL	6,710,029,070	360,985,492	**1,596,270,108**	**23.8 %**	342.2 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for March 31, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com.



Source: Internet World Stats - www.internetworldstats.com/stats.htm

Cyberwars..



www.owasp.org

Home
News
Projects
Downloads
Local Chapters
Conferences
Presentations
Video
Papers
Mailing Lists
About OWASP
Membership

eference
How To...
Principles
Threat Agents
Attacks
Vulnerabilities
Countermeasures
Activities
Technologies
Glossary
Code Snippets
.NET Project
Java Project

earch
Go Search

oolbox
What links here

Guide
Top Ten
WebGoat
CLASP
WebScarab
Contracting
Testing
Code Review
More...

Statistics · Recent Changes

Welcome to OWASP

the free and open application security community

About · Searching · Editing · New Article · OWASP Categories

OWASP Overview

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all.

Join webappsec! The OWASP mail list
Get Started Find out more...
Contact OWASP owasp@owasp.org
Become a Member Support our efforts...

Featured Story

Announcing the OWASP Sprajax Project - the first AJAX Security Scanner

OWASP thanks Denim Group for the donation of Sprajax, an open source security scanner for AJAX-enabled applications. Sprajax, a Microsoft .Net-based application is the first web security scanner developed specifically to scan AJAX web applications for security vulnerabilities.

"Denim Group is committed to furthering the field of application security," said Dan Cornell, principal of Denim Group, "and by donating Sprajax to OWASP, we intend to generate more discussion around security

OWASP Conferences

Register for OWASP AppSec Conference in Seattle Oct. 16-

Oct 17-18

The Open Web Application Security Project
AppSec Seattle Conferenc

Join us for our 5th AppSec Conference October 16-18 in Seattle. Microsoft's Michael Howard will be giving the keynote and you'll h presentations on topics like Web Services Security, PCI status, Securing AJAX, the Microsoft Secure Development Lifecycle, all t new OWASP projects, and much more. Check the full agenda website.

OWASP is a not-for-profit, and the OWASP AppSec Conference incredible bargain ($450, $400 for OWASP members, and $250 fc students). You can attend one of 3 full-day training sessions on tl 16th, and the main conference is two full days of presentations, p and discussion on the 17th and 18th. You can read all the details then register online.

OWASP Community (add)

OWASP

- The Open Web Application Security Project (OWASP)
- International not-for-profit charitable Open Source organization funded primarily by volunteers time, OWASP Memberships, and OWASP Conference fees
- Participation in OWASP is free and open to all

OWASP Mission

- To make application security "visible," so that people and organizations can make informed decisions about application security risks

OWASP Resources and Community

Documentation (Wiki and Books)

- Code Review, Testing, Building, Legal, more …

Code Projects

- Defensive, Offensive (Test tools), Education, Process, more …

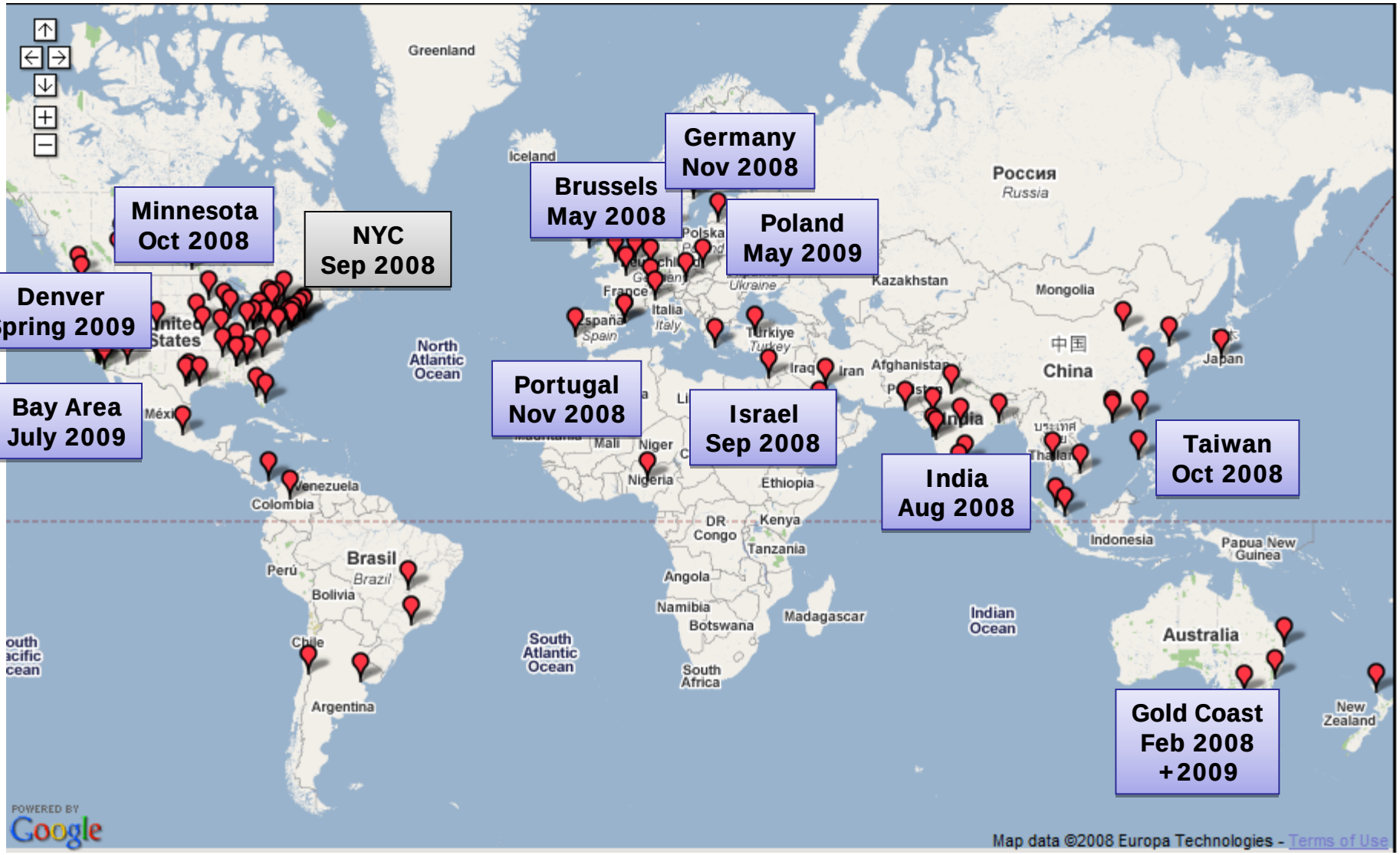
Chapters

- Over 130 and growing

Conferences

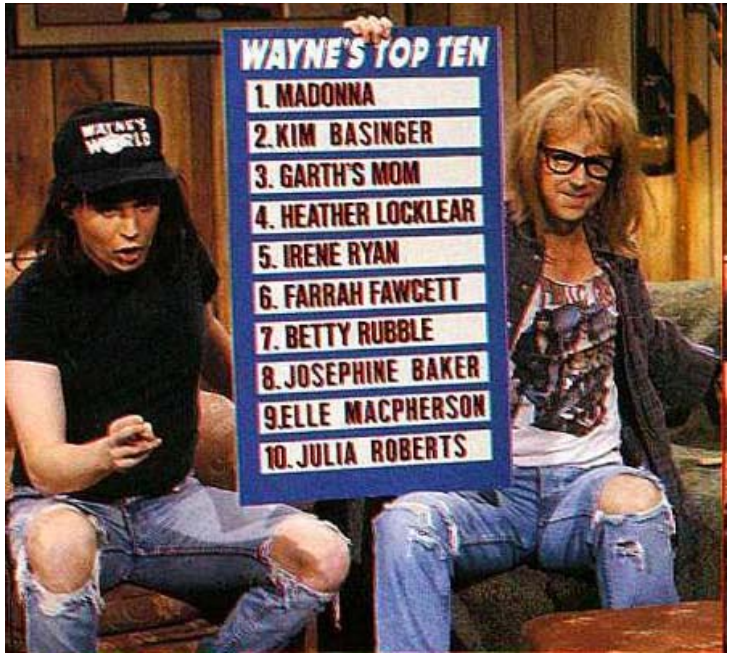
- Major and minor events all around the world

OWASP Conferences (2008-2009)



OWASP Top 10

- The Ten Most Critical Web Application Security Vulnerabilities
- 2007 Release
- A great start, but not a standard



Key Application Security Vulnerabilities

- A1: Cross Site Scripting (XSS)
- A2: Injection Flaws
- A3: Malicious File Execution
- A4: Insecure Direct Object Reference
- A5: Cross Site Request Forgery (CSRF)
- A6: Information Leakage and Improper Error Handling
- A7: Broken Authentication and Session Management
- A8: Insecure Cryptographic Storage
- A9: Insecure Communications
- A10: Failure to Restrict URL Access

OWASP
The Open Web Application Security Project
http://www.owasp.org

www.owasp.org/index.php?title=Top_10_2007

Lot more than OWASP Top 10

- OWASP .NET Project
- OWASP ASDR Project
- OWASP AntiSamy Project
- OWASP AppSec FAQ Project
- OWASP Application Security Assessment Standards Project
- OWASP Application Security Metrics Project
- OWASP Application Security Requirements Project
- OWASP CAL9000 Project
- OWASP CLASP Project
- OWASP CSRFGuard Project
- OWASP CSRFTester Project
- OWASP Career Development Project
- OWASP Certification Criteria Project
- OWASP Certification Project
- OWASP Code Review Project
- OWASP Communications Project
- OWASP DirBuster Project
- OWASP Education Project
- OWASP Encoding Project
- OWASP Enterprise Security API
- OWASP Flash Security Project
- OWASP Guide Project
- OWASP Honeycomb Project
- OWASP Insecure Web App Project
- OWASP Interceptor Project
- OWASP JBroFuzz
- OWASP Java Project
- OWASP LAPSE Project
- OWASP Legal Project
- OWASP Live CD Project
- OWASP Logging Project
- OWASP Orizon Project
- OWASP PHP Project
- OWASP Pantera Web Assessment Studio Project
- OWASP SASAP Project
- OWASP SQLiX Project
- OWASP SWAAT Project
- OWASP Sprajax Project
- OWASP Testing Project
- OWASP Tools Project
- OWASP Top Ten Project
- OWASP Validation Project
- OWASP WASS Project
- OWASP WSFuzzer Project
- OWASP Web Services Security Project
- OWASP WebGoat Project
- OWASP WebScarab Project
- OWASP XML Security Gateway Evaluation Criteria Project
- OWASP on the Move Project

What Does Membership Do For OWASP?

- Funds OWASP Speakers via OWASP On the Move
- Funds Season of Code projects
- Helps Support Local Chapters
  - A portion of your membership fees helps fund your local chapter

Membership Benefits

- Individual Members
- Organizational Supporters
- University Supporters

Individual Members

- Cost: $50/year
- First Time Members Get A Membership Pack:
  - Membership card and certificate
  - OWASP DVD
  - Attractive OWASP t-shirt
  - OWASP tote bag
  - Pen
- 10% discount on OWASP conferences

Organizational Supporters

- Cost: $5000/year
- Logo on OWASP website
- Online job postings on OWASP website
- Invitation to special OWASP events such as Industry Outreach
- Two complimentary attendees to OWASP annual Summit
- Employees get 10% discount on OWASP conferences
- Onsite OWASP briefing

University Supporters

- No cost (!) – Universities must agree to provide meeting space twice per year and to include OWASP in their curriculum
- Must be an accredited University
- Logo on OWASP website
- OWASP briefings for University – students and staff

Upcoming Conferences

- August 26th, 2009 – UC Irvine -AppSec Academia Symposium

- Nov 10 – 13, 2009 – Wash DC, OWASP Appsec USA,