Welcome to OWASP Bay Area Application Security Summit July 1st, 2010

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

OWASP
July 1st, 2010

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

Agenda

- 8.45 – 9.00 Registration, Breakfast
- 9.00 – 9.15 - Welcome, Overview – Mandeep Khera
- 9.15 –10.00 – Drive by Downloads – *Neil Daswani, Co-Founder, Dasient*
- 10.00-10.45 – Building Secure Web Apps – *Misha Logvinov, VP of Online Operations, IronKey and Alex Bello, Director of Technical Operations and Product Security, IronKey*
- 10.45 –11.15- Networking Break
- 11.15–12.00 – Cloudy with a Chance of Hack - *Lars Ewe, CTO and VP of Engineering, Cenzic*
- 12.00- 1.30 – Networking Lunch
- 1.30 – 2.15 – Application Security Deployment Tradeoffs - *Anoop Reddy, Senior Manager, Products, Citrix*
- 2.15 – 3.00 – MashUp SSL - Extending SSL for Security Mashups - *Siddharth Bajaj, Principal Engineer, VeriSign*

Thanks to our sponsors!!

AppSec CONSULTING
Security Compliance & Assurance

Security testing services, Compliance assessments and validation, Education and training, and Solving complex IT security problems.

CENZIC
Securing Enterprise Applications

Web application scanning – Software, Managed Service, and Cloud; Compliance, Training, Best Practices consulting

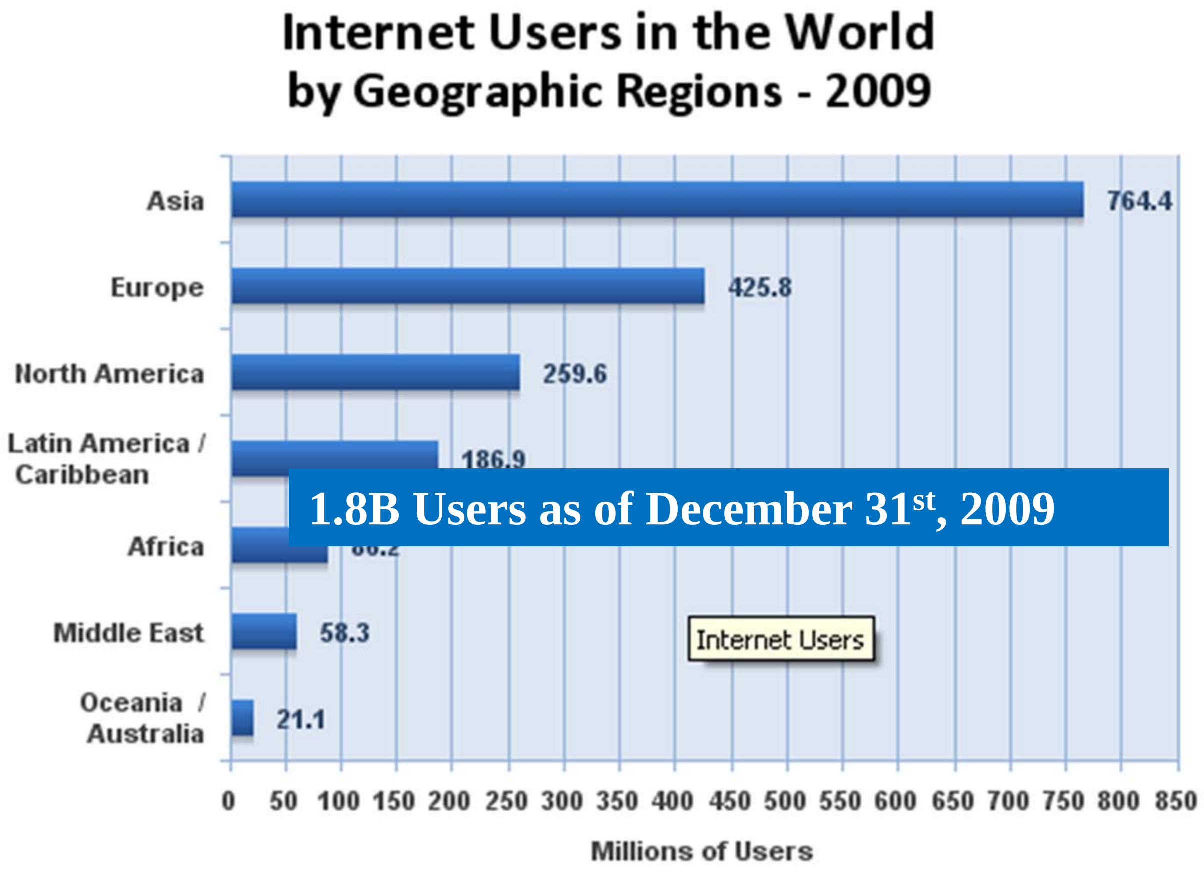
Dasient

Protects businesses from web-based malware attacks. Provides a complete Web Anti-Malware (WAM) service that can automatically identify and quarantine malware on websites.

SAP

Founded in 1972, SAP is one of the leading international providers of business software and, based on market capitalization, it’s the world's third-largest independent software manufacturer.

Internet Usage Continues to Grow

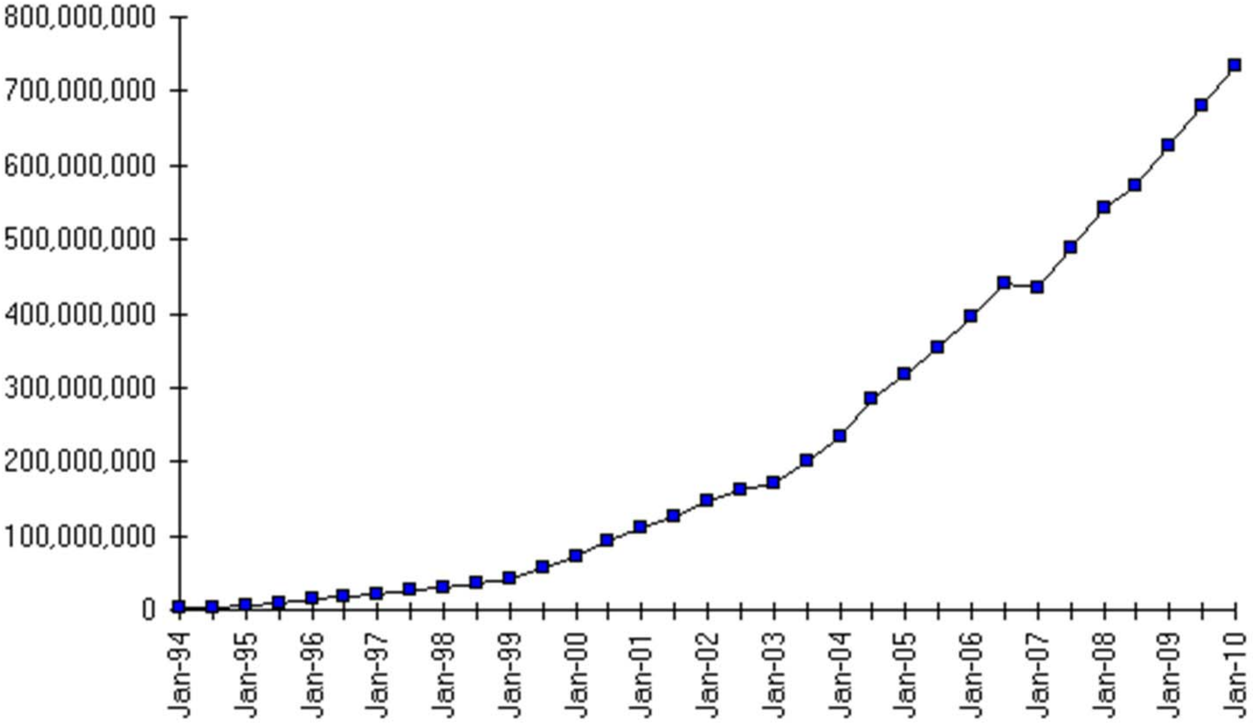

Internet Users in the World
by Geographic Regions - 2009

1.8B Users as of December 31st, 2009

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 1,802,330,457 for December 31, 2009
Copyright © 2010, Miniwatts Marketing Group

Internet Usage Continues to Grow

Internet Domain Survey Host Count

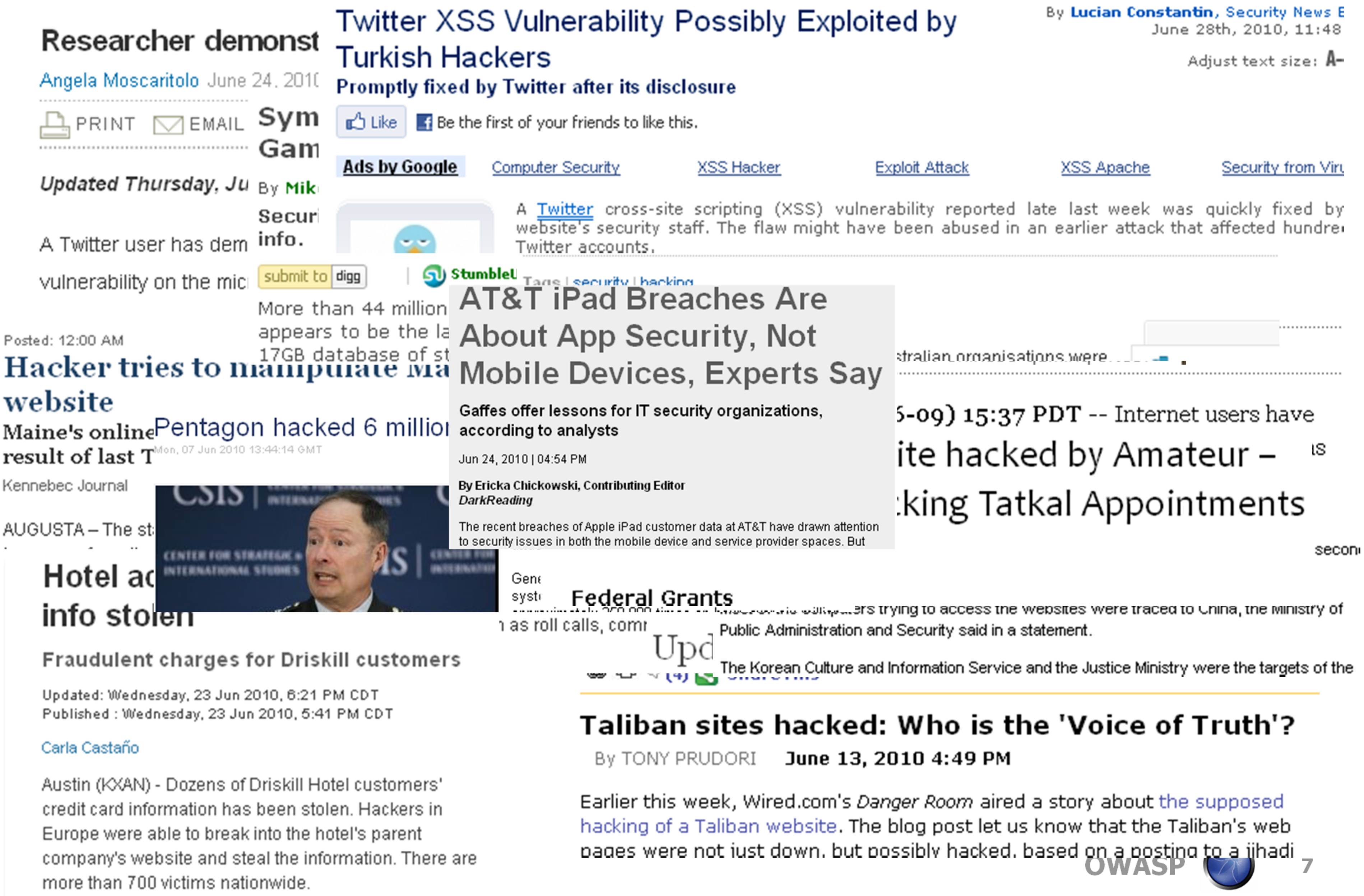


Source: Internet Systems Consortium (www.isc.org)

Internet Usage Continues to Grow

- Over 120M Domain Names
- Over 100M Web applications
- Less than 5% secure
- And the hacking through the applications continues... 60% to 90% of attacks through Web applications..

Hacking continues…



Researcher demonst

Angela Moscaritolo June 24, 201(

PRINT EMAIL

Updated Thursday, Ju

A Twitter user has dem

vulnerability on the mic

Sym
Gam

By Mik

Securi
info.

submit to digg | StumbleU

More than 44 million
appears to be the la
17GB database of st

Twitter XSS Vulnerability Possibly Exploited by Turkish Hackers

Promptly fixed by Twitter after its disclosure

Like Be the first of your friends to like this.

Ads by Google Computer Security XSS Hacker Exploit Attack XSS Apache Security from Viru

By Lucian Constantin, Security News E
June 28th, 2010, 11:48

Adjust text size: A-

A Twitter cross-site scripting (XSS) vulnerability reported late last week was quickly fixed by website's security staff. The flaw might have been abused in an earlier attack that affected hundre Twitter accounts.

Tags | security | hacking

Posted: 12:00 AM

Hacker tries to manipulate Ma
website

Maine's online
result of last T

Kennebec Journal

AUGUSTA – The st

Pentagon hacked 6 millior

Mon, 07 Jun 2010 13:44:14 GMT

AT&T iPad Breaches Are About App Security, Not Mobile Devices, Experts Say

Gaffes offer lessons for IT security organizations, according to analysts

Jun 24, 2010 | 04:54 PM

By Ericka Chickowski, Contributing Editor
DarkReading

The recent breaches of Apple iPad customer data at AT&T have drawn attention to security issues in both the mobile device and service provider spaces. But

stralian organisations were

5-09) 15:37 PDT -- Internet users have

ite hacked by Amateur –
king Tatkal Appointments

ıs

secon

Gene
syst

Federal Grants

n as roll calls, com

ers trying to access the websites were traced to China, the Ministry of Public Administration and Security said in a statement.

Upd

The Korean Culture and Information Service and the Justice Ministry were the targets of the

(4)

Hotel ac
info stolen

Fraudulent charges for Driskill customers

Updated: Wednesday, 23 Jun 2010, 6:21 PM CDT
Published : Wednesday, 23 Jun 2010, 5:41 PM CDT

Carla Castaño

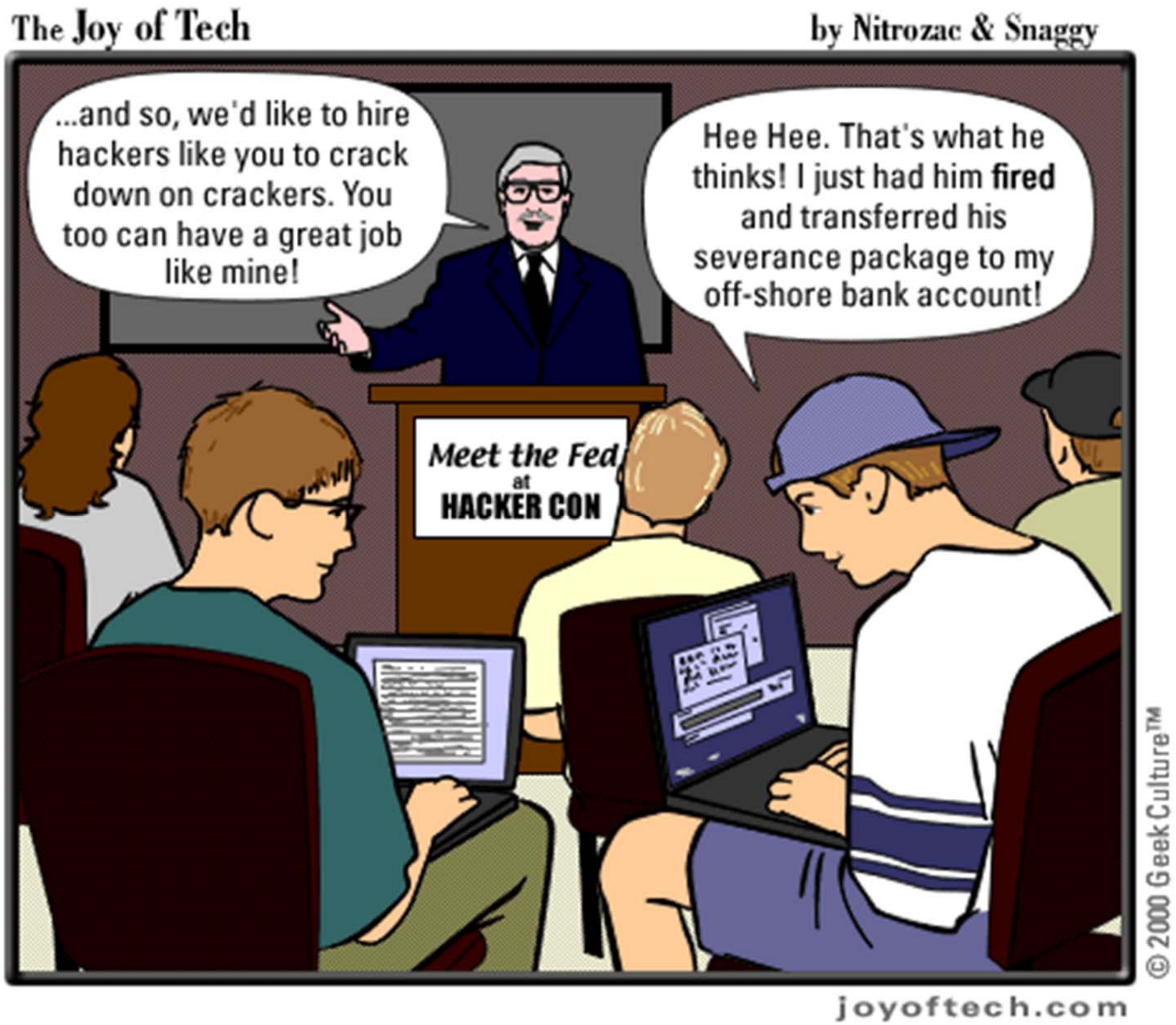
Austin (KXAN) - Dozens of Driskill Hotel customers' credit card information has been stolen. Hackers in Europe were able to break into the hotel's parent company's website and steal the information. There are more than 700 victims nationwide.

Taliban sites hacked: Who is the 'Voice of Truth'?

By TONY PRUDORI **June 13, 2010 4:49 PM**

Earlier this week, Wired.com's *Danger Room* aired a story about the supposed hacking of a Taliban website. The blog post let us know that the Taliban's web pages were not just down, but possibly hacked, based on a posting to a jihadi

Are we prepared for a new breed of hackers?


The Joy of Tech
by Nitrozac & Snaggy
...and so, we'd like to hire hackers like you to crack down on crackers. You too can have a great job like mine!
Hee Hee. That's what he thinks! I just had him **fired** and transferred his severance package to my off-shore bank account!
Meet the Fed at HACKER CON
© 2000 Geek Culture™
joyoftech.com

OWASP

The Open Web Application Security Project

http://www.owasp.org

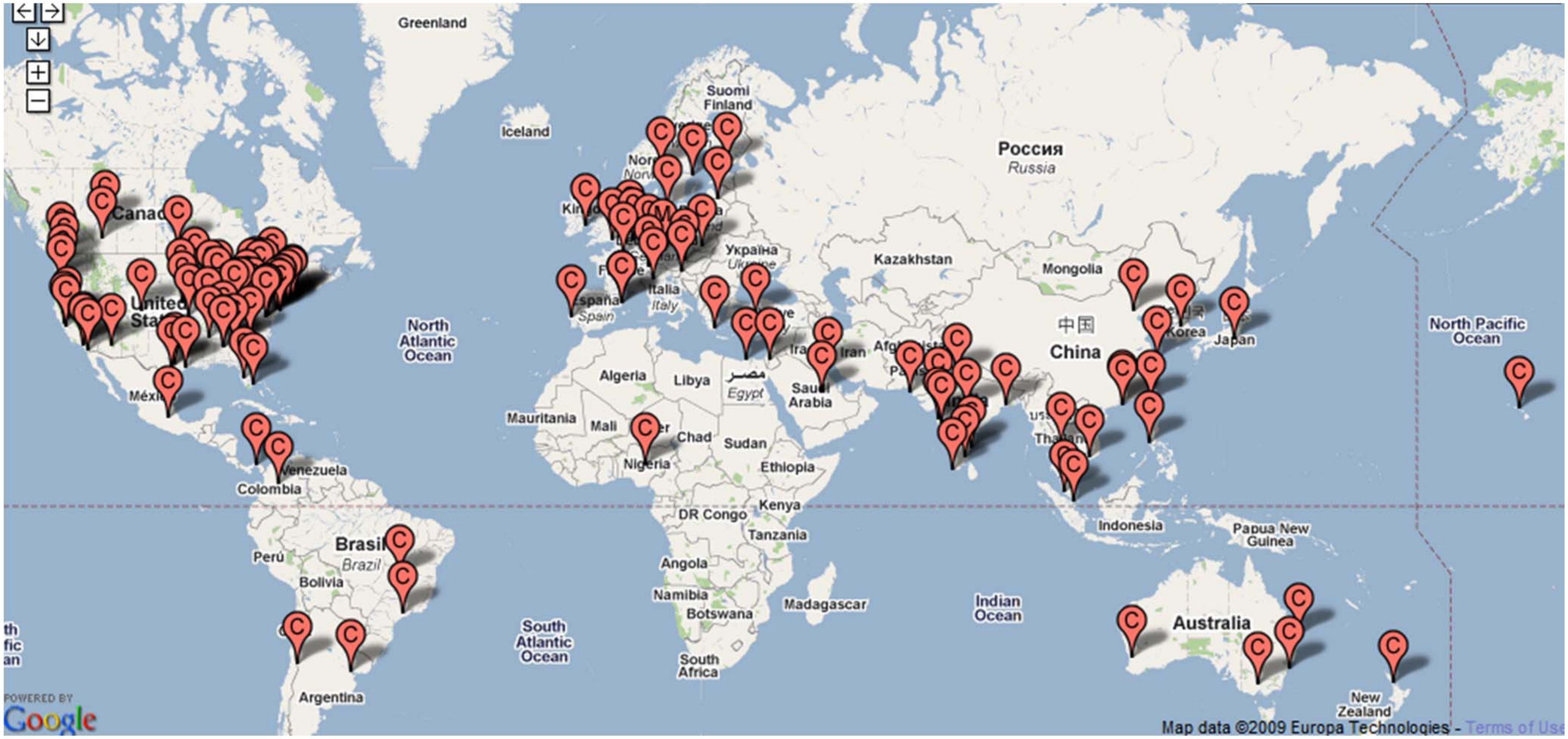
OWASP is a worldwide free and open community focused on improving the security of application software.

Our mission is to make application security visible so that people and organizations can make informed decisions about application security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

OWASP Worldwide Community



Membership

Individual: 750
Organizations: 27

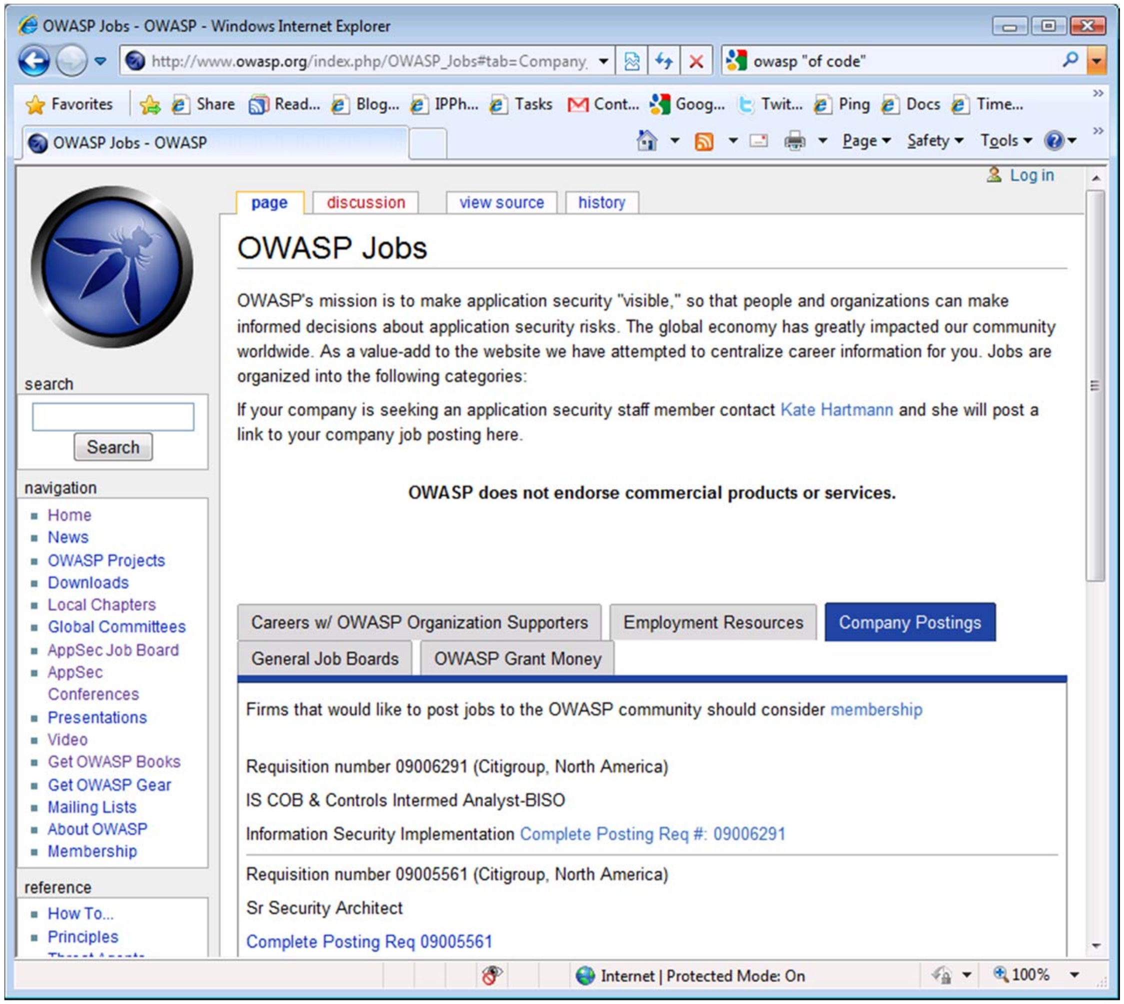
Chapters

158 around world

Participants

1,470 Wiki accounts
+20,000 users

OWASP AppSec Job Board



OWASP Jobs

OWASP's mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. The global economy has greatly impacted our community worldwide. As a value-add to the website we have attempted to centralize career information for you. Jobs are organized into the following categories:

If your company is seeking an application security staff member contact Kate Hartmann and she will post a link to your company job posting here.

OWASP does not endorse commercial products or services.

Firms that would like to post jobs to the OWASP community should consider membership

Requisition number 09006291 (Citigroup, North America)

IS COB & Controls Intermed Analyst-BISO

Information Security Implementation Complete Posting Req #: 09006291

Requisition number 09005561 (Citigroup, North America)

Sr Security Architect

Complete Posting Req 09005561

OWASP Top 10 –
Mapping from 2007 to 2010 Top 10

OWASP Top 10 – 2007 (Previous)		OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	↑	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	↑	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	=	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	+	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	-	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	-	<dropped from T10 2010>

SANS Top 25

OWASP Top 10	SANS 25
A1 – Injection	CWE-89 (SQL), CWE-78 (OS Command)
A2 – Cross Site Scripting (XSS)	CWE-79 (XSS)
A3 – Broken Authentication and Session Management	CWE-306, CWE-307, CWE-798
A4 – Insecure Direct Object References	CWE-285
A5 – Cross Site Request Forgery (CSRF)	CWE-352
A6 – Security Misconfiguration (NEW)	CWE-209 (somewhat)
A7 – Insecure Cryptographic Storage	CWE-285
A8 – Failure to Restrict URL Access	CWE-601
A9 – Insufficient Transport Layer Protection	CWE-327, CWE-311
A10 – Unvalidated Redirects and Forwards (NEW)	CWE-311

Other SANS 25

SANS 25
CWE-120 – Buffer Overflow
CWE- 807 – Reliance on untrusted inputs in a security decision
CWE- 22- Path Traversal
CWE-434 – Unrestricted file upload
CWE-805 - Buffer Access with Incorrect Length Value
CWE- 98 - Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')
CWE-129 - Improper Validation of Array Index
CWE-754 - Improper Check for Unusual or Exceptional Conditions
CWE-190 - Integer Overflow or Wraparound
CWE-131 - Incorrect Calculation of Buffer Size
CWE-494 - Download of Code Without Integrity Check
CWE-732 - Incorrect Permission Assignment for Critical Resource
CWE-770 - Allocation of Resources Without Limits or Throttling
CWE-362 - Race Condition

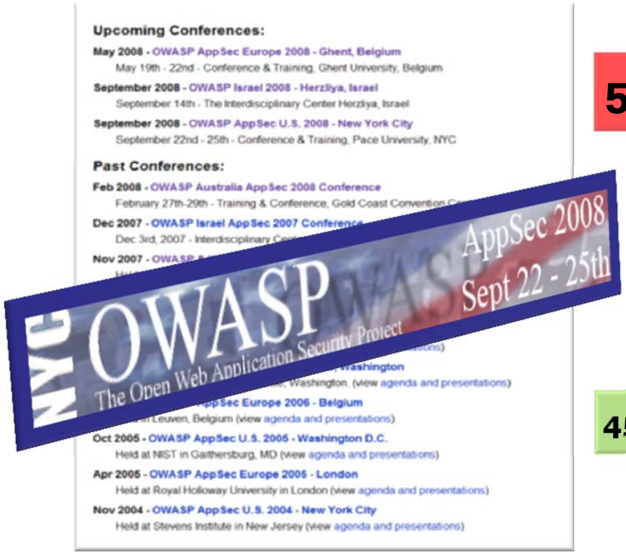
Lot more than OWASP Top 10

- 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

Finances and Grants

Organization Supporters of OWASP's mission
AccessIT GROUP INC.
acunetix
ascure
ASPECT SECURITY
art.defence
BEST BUY
Booz | Allen | Hamilton
BREACH
CENZIC
cigital
City & Guilds
CorporateOne
denyall SECURITY SOLUTIONS
ETS
FORTIFY
Foundstone
GOTHAM
HARRIS CONNECT
hp invent
Hurricane
IMPERVA
INFOVISION
(ISC)²
Microsoft
mnemonic
NOKIA
North Texas
protiviti
PSC
SECURE SOLVE
SOGETI
symantec.
The University of Texas Health Science Center at Houston

100 %



Upcoming Conferences:

May 2008 - OWASP AppSec Europe 2008 - Ghent, Belgium
May 19th - 22nd - Conference & Training, Ghent University, Belgium

September 2008 - OWASP Israel 2008 - Herzliya, Israel
September 14th - The Interdisciplinary Center Herzliya, Israel

September 2008 - OWASP AppSec U.S. 2008 - New York City
September 22nd - 25th - Conference & Training, Pace University, NYC

Past Conferences:

Feb 2008 - OWASP Australia AppSec 2008 Conference
February 27th-29th - Training & Conference, Gold Coast Convention C

Dec 2007 - OWASP Israel AppSec 2007 Conference
Dec 3rd, 2007 - Interdisciplinary Ce

Nov 2007 - OWASP

ations)

Washington
Washington. (view agenda and presentations)

ppSec Europe 2006 - Belgium
Leuven, Belgium (view agenda and presentations)

Oct 2005 - OWASP AppSec U.S. 2005 - Washington D.C.
Held at NIST in Gaithersburg, MD (view agenda and presentations)

Apr 2005 - OWASP AppSec Europe 2005 - London
Held at Royal Holloway University in London (view agenda and presentations)

Nov 2004 - OWASP AppSec U.S. 2004 - New York City
Held at Stevens Institute in New Jersey (view agenda and presentations)

55 %

45 %

OWASP Grants

OWASP Autumn of Code 2006
$20,000 budget

OWASP Spring of Code 2007
$117,500 budget

OWASP Summer of Code 2008
$126,000 budget

OWASP Foundation

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

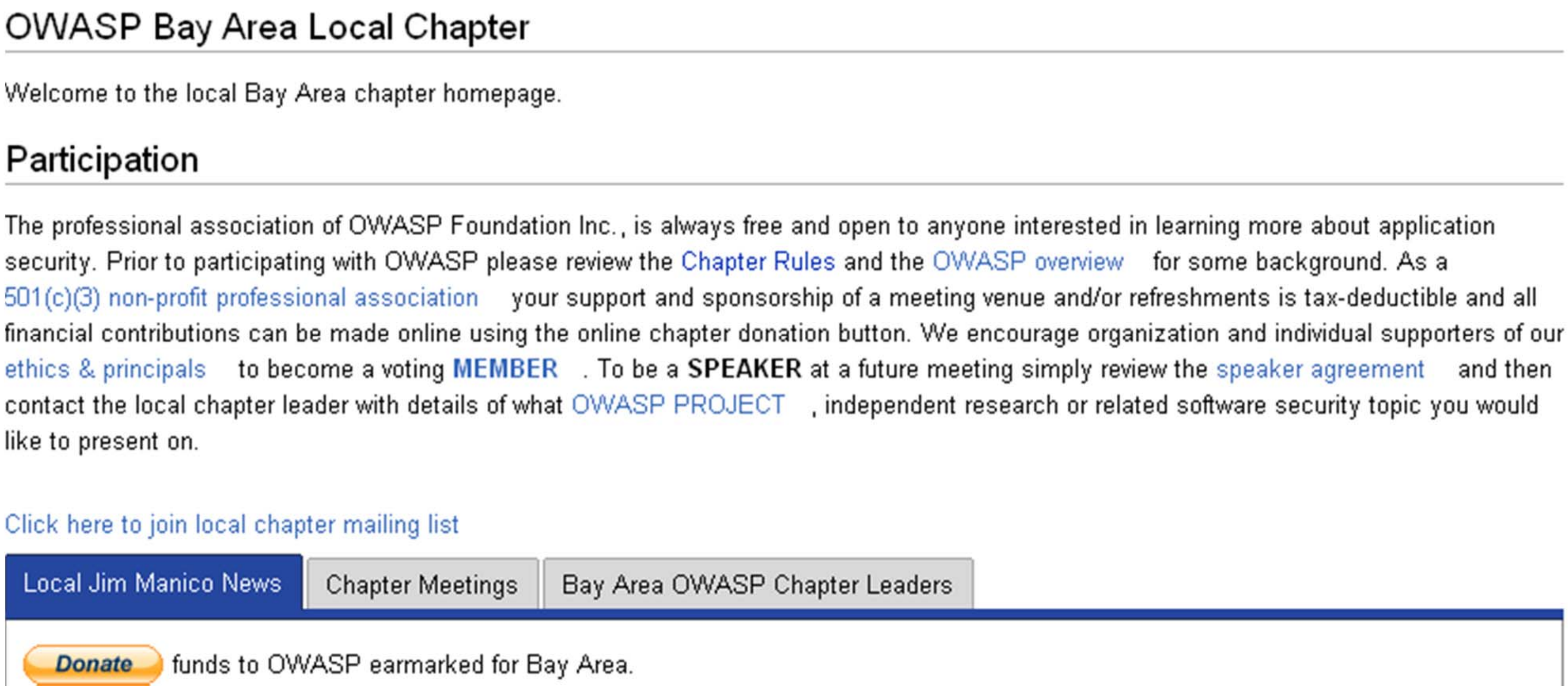
Membership Benefits

- 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

Individual Members



OWASP Bay Area Local Chapter

Welcome to the local Bay Area chapter homepage.

Participation

The professional association of OWASP Foundation Inc., is always free and open to anyone interested in learning more about application security. Prior to participating with OWASP please review the Chapter Rules and the OWASP overview for some background. As a 501(c)(3) non-profit professional association your support and sponsorship of a meeting venue and/or refreshments is tax-deductible and all financial contributions can be made online using the online chapter donation button. We encourage organization and individual supporters of our ethics & principals to become a voting **MEMBER** . To be a **SPEAKER** at a future meeting simply review the speaker agreement and then contact the local chapter leader with details of what OWASP PROJECT , independent research or related software security topic you would like to present on.

Click here to join local chapter mailing list

funds to OWASP earmarked for Bay Area.

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

- AppSec USA
  - www.AppSecUSA.org
- Looking for speakers, and sponsors
- Contact me for both