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

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

[Logos for AppSec Consulting, CENZIC, and IMPERVA]
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

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

Report: Mass Injection Attack Affects 40,000 Websites
Exploit appears similar, but unrelated, to Gumblar, researchers say

CIA: Hackers have already attacked the electric grid
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

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>976,300,089</td>
<td>4,514,400</td>
<td>54,171,500</td>
<td>5.6%</td>
<td>1,100.0%</td>
<td>3.4%</td>
</tr>
<tr>
<td>Asia</td>
<td>3,780,619,732</td>
<td>114,364,000</td>
<td>657,170,846</td>
<td>17.4%</td>
<td>474.5%</td>
<td>41.2%</td>
</tr>
<tr>
<td>Europe</td>
<td>803,903,540</td>
<td>105,056,003</td>
<td>393,373,398</td>
<td>48.9%</td>
<td>274.3%</td>
<td>24.8%</td>
</tr>
<tr>
<td>Middle East</td>
<td>196,776,014</td>
<td>3,284,800</td>
<td>45,861,346</td>
<td>23.3%</td>
<td>1,296.2%</td>
<td>2.9%</td>
</tr>
<tr>
<td>North America</td>
<td>337,572,943</td>
<td>108,096,000</td>
<td>251,290,489</td>
<td>74.4%</td>
<td>132.6%</td>
<td>15.7%</td>
</tr>
<tr>
<td>Latin America/Caribbean</td>
<td>561,249,092</td>
<td>18,066,919</td>
<td>173,619,140</td>
<td>29.9%</td>
<td>860.9%</td>
<td>10.9%</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>34,944,384</td>
<td>7,320,480</td>
<td>20,783,419</td>
<td>60.4%</td>
<td>172.7%</td>
<td>1.3%</td>
</tr>
<tr>
<td><strong>WORLD TOTAL</strong></td>
<td>6,710,029,070</td>
<td>380,886,492</td>
<td>1,596,270,108</td>
<td>23.8%</td>
<td>342.2%</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

*NOTE:* (1) Internet Usage and World Population Statistics are for March 31, 2008. (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 Internet World Stats by the International Telecommunications Union by CAIDA and other reliable sources. (5) For definitions, disclaimer, and navigation help please refer to the Site Design Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 – 2008, Internet Marketing Group. All rights reserved worldwide.

## Internet Users in the World by Geographic Regions

![Internet Users by Geographic Regions](https://via.placeholder.com/150)

*Source: Internet World Stats - www.internetworldstats.com/stats.htm*
Cyberwars..
www.owasp.org
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 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

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 J BroFuzz
- 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,