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

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

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!!

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

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

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

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

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...

Twitter XSS Vulnerability Possibly Exploited by Turkish Hackers
Promptly fixed by Twitter after its disclosure
A Twitter user has discovered a cross-site scripting (XSS) vulnerability reported late last week was quickly fixed by the website's security staff. The flaw might have been abused in an earlier attack that affected hundreds of Twitter accounts.

AT&T iPad Breaches Are About App Security, Not Mobile Devices, Experts Say
Gaffes offer lessons for IT security organizations, according to analysts
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

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

Taliban sites hacked: Who is the 'Voice of Truth'?
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 jihad
Are we prepared for a new breed of hackers?
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 Top 10 - Mapping from 2007 to 2010 Top 10

<table>
<thead>
<tr>
<th>OWASP Top 10 - 2007 (Previous)</th>
<th>OWASP Top 10 - 2010 (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A2 - Injection Flaws</strong></td>
<td><strong>A1 - Injection</strong></td>
</tr>
<tr>
<td><strong>A1 - Cross Site Scripting (XSS)</strong></td>
<td><strong>A2 - Cross Site Scripting (XSS)</strong></td>
</tr>
<tr>
<td><strong>A7 - Broken Authentication and Session Management</strong></td>
<td><strong>A3 - Broken Authentication and Session Management</strong></td>
</tr>
<tr>
<td><strong>A4 - Insecure Direct Object Reference</strong></td>
<td><strong>A4 - Insecure Direct Object References</strong></td>
</tr>
<tr>
<td><strong>A5 - Cross Site Request Forgery (CSRF)</strong></td>
<td><strong>A5 - Cross Site Request Forgery (CSRF)</strong></td>
</tr>
<tr>
<td><strong>&lt;was T10 2004 A10 - Insecure Configuration Management&gt;</strong></td>
<td><strong>A6 - Security Misconfiguration (NEW)</strong></td>
</tr>
<tr>
<td><strong>A8 - Insecure Cryptographic Storage</strong></td>
<td><strong>A7 - Insecure Cryptographic Storage</strong></td>
</tr>
<tr>
<td><strong>A10 - Failure to Restrict URL Access</strong></td>
<td><strong>A8 - Failure to Restrict URL Access</strong></td>
</tr>
<tr>
<td><strong>A9 - Insecure Communications</strong></td>
<td><strong>A9 - Insufficient Transport Layer Protection</strong></td>
</tr>
<tr>
<td><strong>&lt;not in T10 2007&gt;</strong></td>
<td><strong>A10 - Unvalidated Redirects and Forwards (NEW)</strong></td>
</tr>
<tr>
<td><strong>A3 - Malicious File Execution</strong></td>
<td><strong>&lt;dropped from T10 2010&gt;</strong></td>
</tr>
<tr>
<td><strong>A6 - Information Leakage and Improper Error Handling</strong></td>
<td><strong>&lt;dropped from T10 2010&gt;</strong></td>
</tr>
</tbody>
</table>
# SANS Top 25

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

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

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

- **OWASP Autumn of Code 2006**
  - 100%

- **OWASP Spring of Code 2007**
  - 55%

- **OWASP Summer of Code 2008**
  - 45%
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

Local Jim Marico News  Chapter Meetings  Bay Area OWASP Chapter Leaders

Donate 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](http://www.AppSecUSA.org)
- Looking for speakers, and sponsors
- Contact me for both