We are living in a Digital environment, in a Connected World

- Most of websites vulnerable to attacks
- 75% of Attacks at the Application Layer (Source: Someone paid Gartner to say this)
- Important % of web-based Business (Services, Online Store, Self-care)
The True Story

The Open Web Application Security Project

OWASP:

Swarms of WASPS:
Local Chapters
Mission Driven

Nonprofit | World Wide | Unbiased

OWASP does not endorse or recommend commercial products or services
Community Driven

30,000 Mail List Participants
200 Active Chapters in 70 countries
1600+ Members, 56 Corporate Supporters
69 Academic Supporters
Around the World

200 Chapters, ~1600 Members, 30000+ Builders, Breakers and Defenders
Statistics!

200+ Projects
15,000+ downloads of tools, documentation
250,000+ unique visitors
2,000,000+ page views
A Vision for OWASP

Outreach
Projects
Stakeholders
Focus
Support
Platform

Global Committees
Board

OWASP
Security Resources

Secure Lifecycle

- **Builders**
  - ESAPI
  - AntiSamy
  - Development Guide
  - SAMM
  - ASVS

- **Breakers**
  - Cheat Sheets
  - Testing Guide
  - Code Review Guide
  - Zed Attack Proxy
  - JBroFuzz

- **Defenders**
  - AppSensor
  - ModSecurity Core Rule

- **Knowledge**
  - Top 10
  - AppSec Tutorial Videos

- **WebGoat**
- **LiveCD**
- **Podcast**
- **AppSec RSS Feed**
The OWASP Top Ten

TOP 10 WEB APPLICATION SECURITY RISKS
News
a Blog
A Podcast
Membership
Mailing Lists
A Newsletter
Apple App Store
Video Tutorials
Training Sessions
Social Networking
<table>
<thead>
<tr>
<th>OWASP Global Committee</th>
<th>Projects</th>
<th>Membership</th>
<th>Education</th>
<th>Conferences</th>
<th>Industry</th>
<th>Chapters</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee Chair</td>
<td>Jason Li</td>
<td>Helen Gao</td>
<td>Martin Knobloch</td>
<td>Mark Bristow</td>
<td>Rex Booth</td>
<td>Josh Sokol</td>
<td>Jim Manico</td>
</tr>
<tr>
<td>Members</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Brad Causey</td>
<td>• Dan Cornell</td>
<td>• Eduardo Neves</td>
<td>• Lucas Ferreira</td>
<td>• Mauro Flores</td>
<td>• Seba Deleersnyder</td>
<td>• Ludovic Petit</td>
<td></td>
</tr>
<tr>
<td>• Chris Schmidt</td>
<td>• Ofer Maor</td>
<td>• Cecil Su</td>
<td>• John Wilander</td>
<td>• Alexander Fry</td>
<td>• Luiz Eduardo Dos Santos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Justin Searle</td>
<td>• Aryavalli Gandhi</td>
<td>• Fabio Cerullo</td>
<td>• Richard Greenberg</td>
<td>• Eoin Keary</td>
<td>• L. Gustavo C. Barbato</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Larry Casey</td>
<td></td>
<td>• Kuai Hinjosa</td>
<td>• Ralph Durkee</td>
<td>• Mateo Martinez</td>
<td>• Justin Clarke</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Keith Turpin</td>
<td></td>
<td>• Sebastien Goria</td>
<td>• Mohd Fazli Azran</td>
<td>• Colin Watson</td>
<td>• Jerry Hoff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Tony Gottlieb</td>
<td></td>
<td>• Carlos Serrão</td>
<td>• Lorna Alamri</td>
<td>• Marco Morana</td>
<td>• Chen Min</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Luiz Otavio Duarte</td>
<td></td>
<td>• Benny Ketelslegers</td>
<td></td>
<td>• Christian Papanas</td>
<td>• Dr. Yuan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applicants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Zhendong Yu</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Michael Scovetta</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committee Looking For</td>
<td></td>
<td>More Members</td>
<td>New Members with Education Background</td>
<td>More Members Outside U.S.</td>
<td>More Members Outside U.S. and Europe</td>
<td>More Members Outside U.S.</td>
<td>More Members</td>
</tr>
<tr>
<td>New Members with OWASP Project Leadership Experience</td>
<td>More Members</td>
<td>New Members with Education Background</td>
<td>More Members Outside U.S.</td>
<td>More Members Outside U.S. and Europe</td>
<td>More Members Outside U.S.</td>
<td>More Members</td>
<td></td>
</tr>
</tbody>
</table>
Developer Cheat Sheets
§ OWASP Top Ten Cheat Sheet
§ Authentication Cheat Sheet
§ Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet
§ Cryptographic Storage Cheat Sheet
§ Input Validation Cheat Sheet
§ XSS (Cross Site Scripting) Prevention Cheat Sheet
§ DOM based XSS Prevention Cheat Sheet
§ Forgot Password Cheat Sheet
§ Query Parameterization Cheat Sheet
§ SQL Injection Prevention Cheat Sheet
§ Session Management Cheat Sheet
§ HTML5 Security Cheat Sheet
§ Transport Layer Protection Cheat Sheet
§ Web Service Security Cheat Sheet
§ Logging Cheat Sheet
§ JAAS Cheat Sheet

Mobile Cheat Sheets
§ IOS Developer Cheat Sheet
§ Mobile Jailbreaking Cheat Sheet

Draft Cheat Sheets
§ Access Control Cheat Sheet
§ REST Security Cheat Sheet
§ Abridged XSS Prevention Cheat Sheet
§ PHP Security Cheat Sheet
§ Password Storage Cheat Sheet
§ Secure Coding Cheat Sheet
§ Threat Modeling Cheat Sheet
§ Clickjacking Cheat Sheet
§ Virtual Patching Cheat Sheet
§ Secure SDLC Cheat Sheet
§ Web Application Security Testing Cheat Sheet
§ Application Security Architecture Cheat Sheet
Project Leader: Simon Bennetts (aka Psiinon), psiinon@gmail.com

Purpose: The Zed Attack Proxy (ZAP) provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually in web applications.

Last Release: ZAP 1.4.1 – August 2012

Project Leader: Jack Mannino, Jack@nvisiumsecurity.com

Purpose: Establish an OWASP Top 10 Mobile Risks. Intended to be platform-agnostic. Focused on areas of risk rather than individual vulnerabilities.

Deliverables

- Top 10 Mobile Risks (currently Release Candidate v1.0)
- Top 10 Mobile Controls (OWASP/ENISA Collaboration)
  - Wiki OWASP, ‘Smartphone Secure Development Guidelines’ (ENISA)
- Mobile Cheat Sheet Series
- OWASP GoatDroid Project
- OWASP Mobile Threat Model Project

Top 10 Mobile Risks

• M1. Insecure Data Storage
• M2. Weak Server Side Controls
• M3. Insufficient Transport Layer Protection
• M4. Client Side Injection
• M5. Poor Authorization and Authentication
• M6. Improper Session Handling
• M7. Security Decisions via Untrusted Inputs
• M8. Side Channel Data Leakage
• M9. Broken Cryptography
• M10. Sensitive Information Disclosure
“If you think education is expensive, you should try ignorance!”
• You can’t improve what you can’t measure

• **We need to...**
  • Experiment
  • Share what works and what does not
  • Collaborate our efforts

• Expect another 10 years!
The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on improving the security of software.

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

Everyone is welcomed to participate in OWASP and all of our materials are available under free and open software licenses.
**OPEN** Everything at OWASP is radically transparent from our finances to our code.

**INNOVATION** OWASP encourages and supports innovation/experiments for solutions to software security challenges.

**GLOBAL** Anyone around the world is encouraged to participate in the OWASP community.

**INTEGRITY** OWASP is an honest and truthful, vendor agnostic, global community.
Approach = “Open”

- Open means rough consensus and running code
- Open means free to use and modify
- Open means independent
- Open means open information sharing
- Open means wider audience and participation
- Open means everyone is a peer in this global community
WHY OWASP WILL WIN?
BECAUSE OF YOU!