2nd OWASP IL mini conference at the Interdisciplinary Center (IDC) Herzliya, May 21th 2007

Ofer Shezaf,
CTO, Breach Security
March, 2006
ofers@breach.com

OWASP

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

Introduction

Sponsoring this evening:

And from this point on:

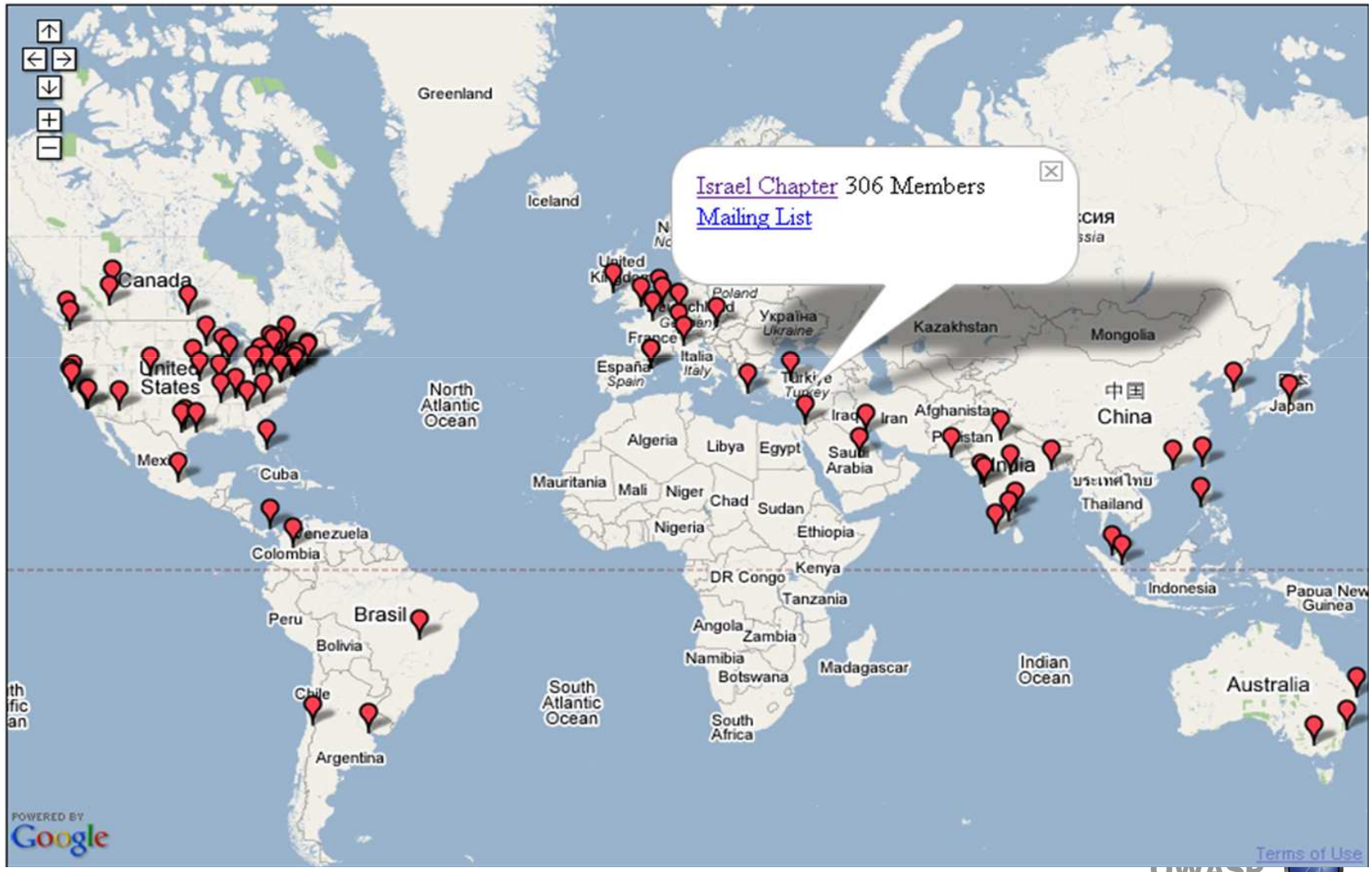
OWASP cannot recommend the use of commercial products, services, or recommend specific companies.

What is OWASP?

Open Web Application Security Project

- Non-profit, volunteer driven organization:
  - All members are volunteers
- Activities:
  - Projects (~40 of them):
    - Publications: OWASP TOP 10, OWASP Guide, OWASP Testing Guide, CLASP
    - Testing and Training Software: WebGoat, WebScarab
  - Chapters (~80 of them)
  - Conferences (6 so far)
- Membership:
  - No need. A contribution.

All Over The World



Reflections from OWASP Europe

- The most professional conference I have been too:
  - Nobody snored even after an Italian lunch ☺
- Small (but highly focused) crowed:
  - US conferences are much bigger
  - Italy may be the wrong place (northern Europe more receptive to application security).

The XSS elephant

- Many advances in XSS technology:
  - JavaScript Hijacking with AJAX
  - Overtaking Google Desktop using XSS
  - Same Origin Policy Unification Techniques using public services
  - A new attack vector for XSS and XSFlashing
  - The Universal PDF XSS
- Easier to research
  - But than also to exploit
- Too much talking about vulnerabilities and too little about solutions:
  - Nobody wants to hear about eating broccoli.

14:00 - 14:15 **Updates from OWASP Europe, Milan**
Ofer Shezaf, OWASP IL chapter leader, CTO, Breach Security

14:15 - 15:00 **Pen-Testing at Microsoft: FuzzGuru fuzzing framework**
John Neystadt, Lead Program Manager, Microsoft Forefront Edge, Microsoft

15:00 - 15:40 **Unregister Attacks in SIP**
Ronit Halachmi-Bekel, Efi Arazi school of Computer Science at Interdisciplinary Center (IDC) Herzliya

15:40 - 16:00 **Break**

16:00 - 16:40 **Application Denial of Service; is it Really That Easy?**
Shay Chen, Hacktics

16:40 - 17:10 **Behavioral Analysis for Generating A Positive Security Model For Applications**
Ofer Shezaf, OWASP IL chapter leader, CTO, Breach Security

17:10 - 17:50 **Overtaking Google Desktop - Leveraging XSS to Raise Havoc**
Yair Amit, Senior Security Researcher, Watchfire

17:50 - 18:00 **Break**

18:00 - 18:20 **Application Security is Not Just About Development**
David Lewis, CISM, CISA, CISSP, Rosenblum Holtzman

18:20 - 19:20 **.NET reverse engineering**
Erez Metula, Application Security Department Manager, 2Bsecure