OWASP Helsinki –Tervetuloa!

Mikko Saario
OWASP Helsinki Chapter Leader

OWASP
12.12.2006

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

OWASPin Missio

< Mahdollistaa organisaatioiden kehittää, ylläpitää ja hankkia luotettavia sovelluksia

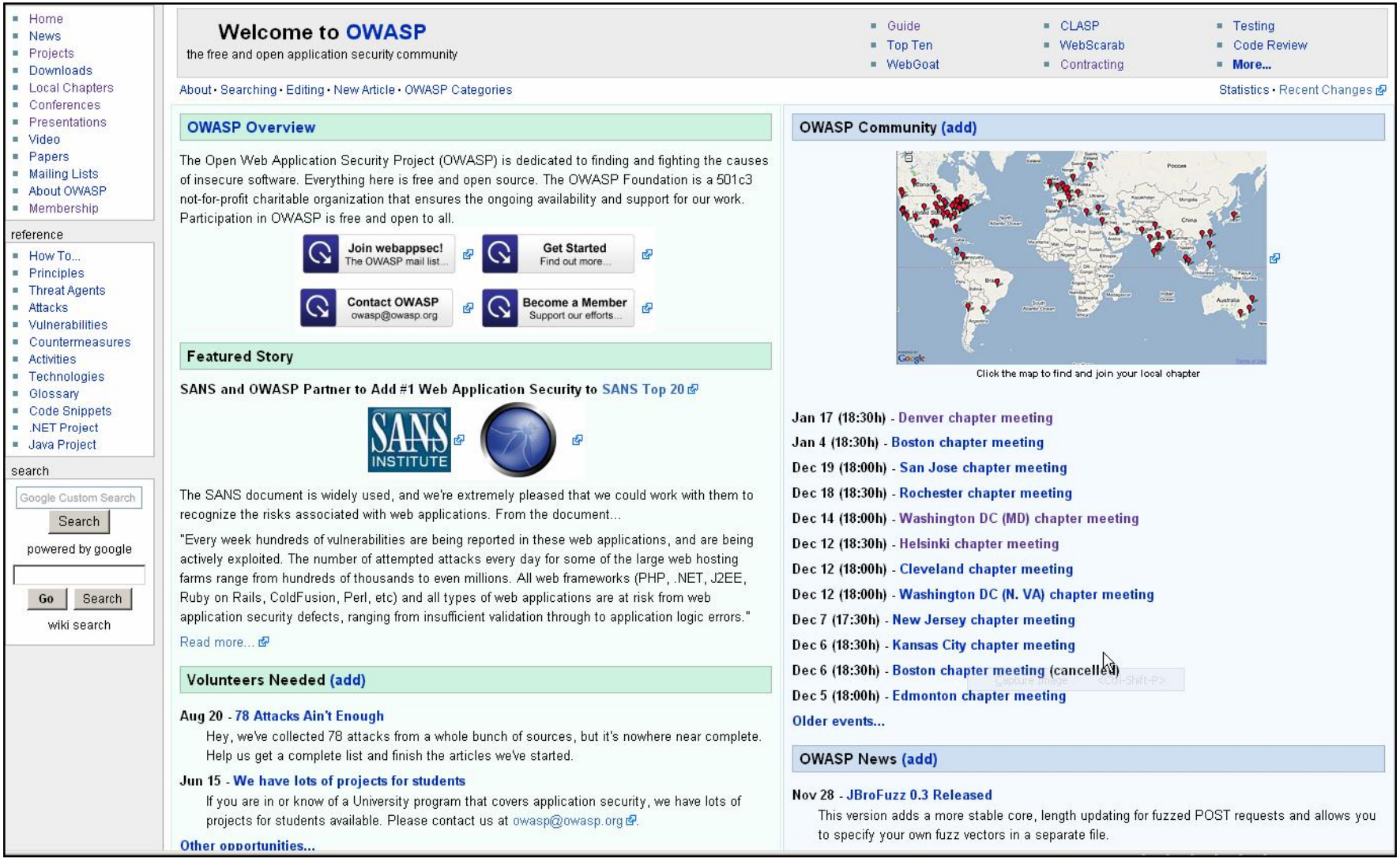
OWASP Foundation

- Rekisteröity USA:ssa ”501c3 not-for-profit charitable organization ” –tyyppiseksi organisaatioksi
- Osallistuminen on vapaata ja avointa kaikille
- Taloudelliset tiedot tulossa webiin

Tausta

- < 2000: Mark Curphey ja Microsoft Word
- < 2001: OWASP Guide 1.0
- < 2002: Guide 1.1.1 vapaaehtoisvoimin
- < 2002: "owasp-leaders"
  - 4 Projektien vetäjät
  - 4 Sama rakenne jatkuu edelleen
- < 2003: "OWASP Foundation" luotiin
- < 2004: Ensimmäinen konferenssi NYC
- < -> 2006: Toiminta laajeni uusien projektien myötä

www.owasp.org



Mitä OWASP tekee?

- Projektit
  - Ohjeita, työkaluja, … -> AppSec-asiaa
- Konferenssit
  - 2 x vuodessa; USA syksyllä & Eurooppa keväällä

...

- < Paikalliset jaokset (chapters)
  - 4 Avointa vapaata toimintaa
  - 4 Ks esim. Israel (mini-konferenssi)

OWASP IL mini conference, Monday, November 13th, together with IDC

OWASP IL and the Interdisciplinary Center Herzliya (IDC) held a half day conference on application security on Nov 13th 2006. The event marked the establishment of a new academic program on information security in the net era at IDC Computer Science. More than 90! people attended the conference, enjoyed professional catering and heard no less than 7 presentations.

The meeting was sponsored by Breach Security and Applicure Technologies.

BREACH AppliCure Technologies

Use the links in the event program to access the presentations themselves:

14:30 – 15:00 Gathering and refreshments (hopefully more elaborate than Pizza this time!)

15:00 – 15:10 Introducing the new information security program at the net era at the Efi Arazi School of Computer Science, IDC Herzliya

Dr. Anat Bremler-Barr, Program Academic Director.

15:10 – 15:40 Sophisticated Denial of Service attacks

Dr. Anat Bremler-Barr, Efi Arazi School of Computer Science, IDC Herzliya

In Denial of Service attack, the attackers consume the resources of the victim, a server or a network, causing degradation in performance or even total failure of the victim. The basic DDoS attack is a simple brute force flooding, where the attacker sends as much traffic as he can to consume the network resources. In contrast, the sophisticated DDoS attack aims to hurt the weakest point in the victim's applications by sending specific traffic type that burdens the application the most. In this talk we will cover recent works that show that several common mechanisms are vulnerable to sophisticated DDoS attacks. For example, Crosby and Wallach showed that using bandwidth of less than a typical dialup modem can bring a dedicated Bro server to its knees. We will discuss some basic guidelines of how to design applications to be resilient to sophisticated attacks.

15:40 – 16:00 Malicious content in enterprise portals

Shalom Carmel, A security icon, the world's authority on hacking AS/400 and a BlackHat 2006 speaker

In 2005, enterprise portals rank in the top 10 of CIO technology focus areas in many surveys. The main drivers of the portal business growth are the horizontal portal suites, which provide content management capabilities, application integration tools, and specific solutions for collaboration and knowledge management. This lecture will address the security problems an enterprise may have due to the various content management abilities in a typical Portal implementation, and will focus on cross site scripting attacks.

16:00 – 16:30 Information Warfare against commercial companies – lessons from dealing with hostile internet entities

”Autumn of Code 2006 ”

< Uusi projekti, jonka kautta jaettiin rahallisia ”stipendejä ”9:lle projektille

- 4 5 kpl @ $3,500 USD
- 4 4 kpl @ $5,000 USD

< Odotettavissa lisää vastaavia stipendejä

PDF-XCHANGE Click to buy NOW! www.docu-track.com

Autumn of Code 2006 - Projektit

- WebScarab NG –Rogan Dawes
- Live CD –Joshua Perrymon
- CAL9000 –Chris Loomis
- SiteGenerator and ORG –Mike de Libero
- Pantera –Simon Roses
- Web Goat –Sherif Koussa
- Testing Guide –Matteo Meucci
- OWASP .NET Tools –Boris Maletic
- OWASP Website and Branding –Aaron M. Holmes

Nykyisten projektien jaottelu

< Julkaisuvalmiit

- 4 OWASP WebGoat Project
  an online training environment for hands-on learning about application security
- 4 OWASP WebScarab Project
  a tool for performing all types of security testing on web applications and web services
- 4 OWASP AppSec FAQ Project
- 4 OWASP Guide Project
  a massive document covering all aspects of web application and web service security
- 4 OWASP Legal Research
  a project focused on contracting for secure software
- 4 OWASP Top Ten Project
  an awareness document that describes the top ten web application security vulnerabilities

< Beta-taso (11 työkalua, 4 dokumenttia)

< Alpha-taso (5 työkalua, 11 dokumenttia)

< Teknologia, tutkimus ja oppaat

Rahoitusmalli

- Konferenssit
- Yritysten ja yksityishenkilöiden jäsenyys
- Mainonta
- Sponsorointi

Paikalliset jaokset

OWASP Helsinki

- ”Kansalaisaktivismia ”
- Ei ole ry:tä
  - Ainakaan vielä
- Minimoidaan byrokratia
- Tarvitaan sponsoreita
  - Tilat, tarjoilu
- Muutama aktiivi mukana käynnistämässä toimintaa
- ”Tilaa ”löytyy vielä!

Miten voit itse vaikuttaa?

- Kuka tahansa voi suoraan osallistua OWASPin toimintaan
- Oman projektin perustaminen mahdollista
  - Mutta ”kannattaa ”vain jos pystyt sitoutumaan siihen?
  - Suoraan emo-OWASPin kautta
- Projektit kaipaavat osallistujia –kuten aina
- Voit perustaa oman jaoksen J
  - Vaikkapa ”OWASP Kauniainen ”

Mitä SINÄ odotat?

- Kuinka usein olisi hyvä tavata?
- Missä? Eli alatko sponsoriksi J
- Mihin aikaan (iltapäivä, ilta)?
- Halutaanko enemmän esityksiä, keskustelua, verkostoitumista, koulutusta vai mitä toimintaa?
- Miten voit itse osallistua toimintaan? (muuta kuin tulemalla paikalle)
  - 4 Tule kertomaan omista kokemuksistasi