

OWASP Helsinki – Tervetuloa!

Mikko Saario
OWASP Helsinki Chapter Leader

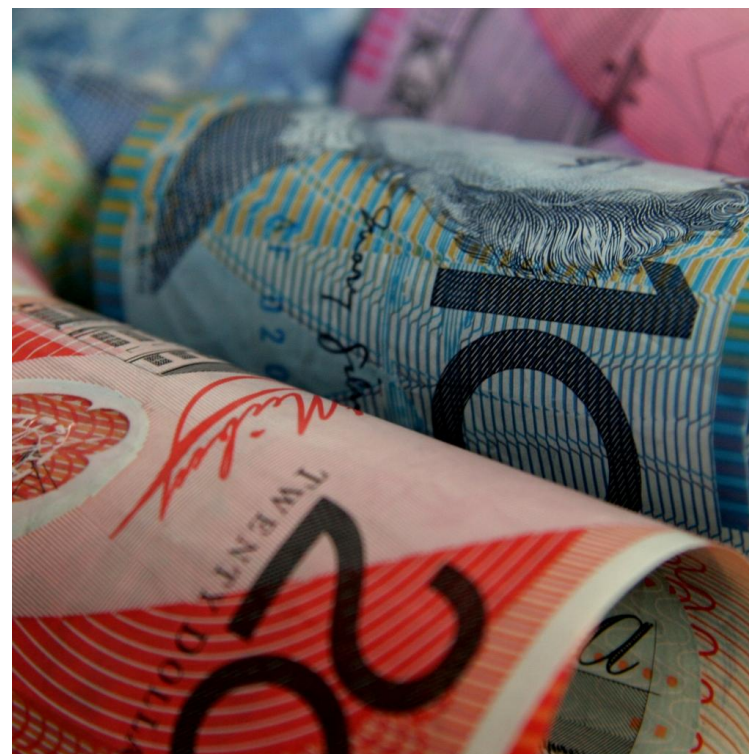
OWASP
12.12.2006

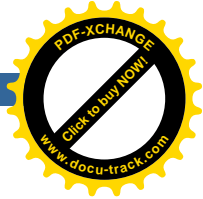
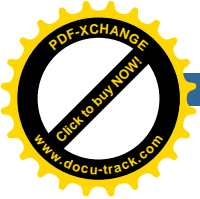
Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

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

OWASPin Missio

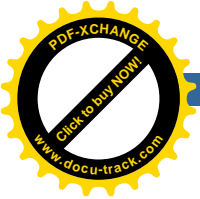
< Mahdollistaa organisaatioiden kehittää, ylläpitää ja hankkia luotettavia sovelluksia





OWASP Foundation

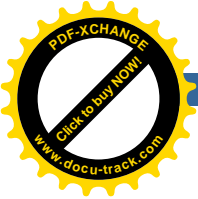
- < Rekisteröity USA:ssa " 501c3 not-for-profit charitable organization" –tyyppiseksi organisaatioksi
- < Osallistuminen on vapaata ja avointa kaikille
- < Taloudelliset tiedot tulossa webiin



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

- Home
- News
- Projects
- Downloads
- Local Chapters
- Conferences
- Presentations
- Video
- Papers
- Mailing Lists
- About OWASP
- Membership

- reference
- How To...
 - Principles
 - Threat Agents
 - Attacks
 - Vulnerabilities
 - Countermeasures
 - Activities
 - Technologies
 - Glossary
 - Code Snippets
 - .NET Project
 - Java Project

search

Google Custom Search

powered by google

wiki search

Welcome to OWASP

the free and open application security community

[About](#) • [Searching](#) • [Editing](#) • [New Article](#) • [OWASP Categories](#)

OWASP Overview

The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all.

Join webappsec! The OWASP mail list...	Get Started Find out more...
Contact OWASP owasp@owasp.org	Become a Member Support our efforts...

Featured Story

SANS and OWASP Partner to Add #1 Web Application Security to SANS Top 20



The SANS document is widely used, and we're extremely pleased that we could work with them to recognize the risks associated with web applications. From the document...

"Every week hundreds of vulnerabilities are being reported in these web applications, and are being actively exploited. The number of attempted attacks every day for some of the large web hosting farms range from hundreds of thousands to even millions. All web frameworks (PHP, .NET, J2EE, Ruby on Rails, ColdFusion, Perl, etc) and all types of web applications are at risk from web application security defects, ranging from insufficient validation through to application logic errors."

[Read more...](#)

Volunteers Needed (add)

Aug 20 - 78 Attacks Ain't Enough

Hey, we've collected 78 attacks from a whole bunch of sources, but it's nowhere near complete. Help us get a complete list and finish the articles we've started.

Jun 15 - We have lots of projects for students

If you are in or know of a University program that covers application security, we have lots of projects for students available. Please contact us at owasp@owasp.org.

[Other opportunities...](#)

- Guide
- Top Ten
- WebGoat
- CLASP
- WebScarab
- Contracting
- Testing
- Code Review
- More...

[Statistics](#) • [Recent Changes](#)

OWASP Community (add)



Click the map to find and join your local chapter

- Jan 17 (18:30h) - [Denver chapter meeting](#)
- Jan 4 (18:30h) - [Boston chapter meeting](#)
- Dec 19 (18:00h) - [San Jose chapter meeting](#)
- Dec 18 (18:30h) - [Rochester chapter meeting](#)
- Dec 14 (18:00h) - [Washington DC \(MD\) chapter meeting](#)
- Dec 12 (18:30h) - [Helsinki chapter meeting](#)
- Dec 12 (18:00h) - [Cleveland chapter meeting](#)
- Dec 12 (18:00h) - [Washington DC \(N. VA\) chapter meeting](#)
- Dec 7 (17:30h) - [New Jersey chapter meeting](#)
- Dec 6 (18:30h) - [Kansas City chapter meeting](#)
- Dec 6 (18:30h) - [Boston chapter meeting \(cancelled\)](#)
- Dec 5 (18:00h) - [Edmonton chapter meeting](#)

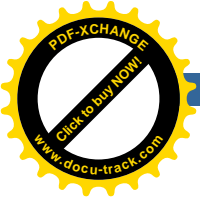
[Older events...](#)

OWASP News (add)

Nov 28 - JBroFuzz 0.3 Released

This version adds a more stable core, length updating for fuzzed POST requests and allows you to specify your own fuzz vectors in a separate file.





Mitä OWASP tekee?

< Projektit

4 Ohjeita, työkaluja, ... -> AppSec-asiaa

< Konferenssit

4 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 [Applique 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.

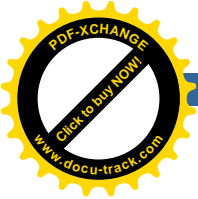
15:40 – 16:00 Malicious content in enterprise portals

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





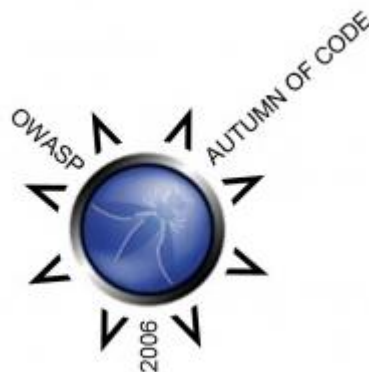
"Autumn of Code 2006"

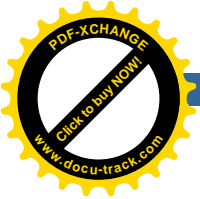
< Uusi projekti, jonka kautta jaettiin rahallisia "stipendejä" 9:lle projektille

45 kpl @ \$3,500 USD

44 kpl @ \$5,000 USD

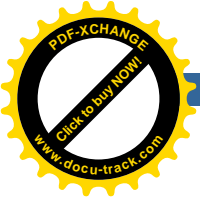
< Odotettavissa lisää vastaavia stipendejä





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

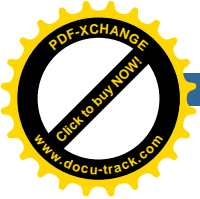
an awareness document that describes the top ten web application security vulnerabilities

< Beta-taso (11 työkalua, 4 dokumenttia)

< Alpha-taso (5 työkalua, 11 dokumenttia)

< Teknologia, tutkimus ja oppaat



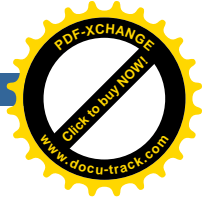
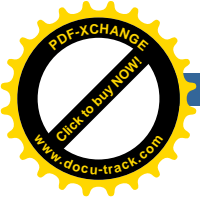


Rahoitusmalli

- < Konferenssit
- < Yritysten ja yksityishenkilöiden jäsenyys
- < Mainonta
- < Sponsorointi

Paikalliset jaokset





OWASP Helsinki

- < "Kansalaisaktivismia"
- < Ei ole ry:tä
 - 4 Ainakaan vielä
- < Minimoidaan byrokratia
- < Tarvitaan sponsoreita
 - 4 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
 - 4 Mutta "kannattaa" vain jos pystyt sitoutumaan siihen?
 - 4 Suoraan emo-OWASPin kautta
- < Projektit kaipaavat osallistujia – kuten aina
- < Voit perustaa oman jaoksen J
 - 4 Vaikkapa "OWASP Kauniainen"

Mitä SINÄ odotat?

- < Kuinka usein olisi hyvä tavata?
- < Missä? Eli alanko sponsoriksi J
- < Mihinkin 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