OWASP

Andrzej Targosz
OWASP Poland Chapter Leader
PROIDEA
andrzej.targosz{@}proidea.org.pl

OWASP

The OWASP Foundation

http://www.owasp.org

Misja

OWASP jest przeznaczony do znajdowania i walki z przyczynami powstawania niebezpiecznego oprogramowania

- Jakie sa przyczyny?
  - Bezposrednie podatnosci - kazdy software posiada bledy ale mamy narzedzia, ktorych powinnismy uzywac
  - Developerzy i administratorzy – dwa kroki wstecz
  - Struktura organizacyjna, proces developmentu, wsparcie technologii – brak testow, korzystania z narzedzi
  - Aspekty kulturowe programistow
  - Bledna analiza ekonomiczna

Bezpieczenstwo aplikacji dopiero raczkuje...

- Brak metryk do pomiaru bezpieczenstwa – trudno doskonalic konkretne umiejetnosci bez pomiaru
- Potrzebujemy:
  - Eksperymentow
  - Wymiany wiedzy
- Czas ok. 10 lat

Synonimy Open wg. OWASP

- Open = bezplatny
- Open = dostepny
- Open = niezalezny
- Open = wymiana informacji

- OWASP Tools & Docs
- OWASP Chapters
- OWASP Conferences

Co znajdziecie na stronie OWASP

- Dokumenty
  - Guide
  - TopTen
  - Testowanie
- Narzedzia
  - WebGoat
  - WebScarab
  - CAL9000
- Spolecznosc

Dualizm licencji

- OWASP nie jest przeznaczony dla zamknietej grupy
- Licencja OpenSource – mozliwosc uzywania materialow i narzedzi do celow polaczonych z projektami OWASP
- Licencja komercyjna – kazdy moze dowolnie uzywac w firmie
- Kwota zaangazowania jest zalezna od skali firmy

The Guide

- 293 stron – www.owasp.org
- Gnu Free Doc License
- Wiekszosc platform
  - PHP
  - J2EE
  - ASP.NET

Uzytkownicy Guide

- Developerzy
  - Implementowanie mechanizmow bezpieczenstwa
- PM
  - Organizowanie testow penetracyjnych, modelowanie, analiza ryzyka
- Zespoly bezpieczenstwa
  - Edukacja bezpieczenstwa
  - Testy

Top Ten

- Zestaw wytycznych z najczesciej popelnianymi bledami
- Stosowanie jest zalecane przez:
  - Komisje Handlu US
  - IBM
  - Price Waterhouse Coopers
  - Sun Microsystems
  - Bank of Newport
  - British Telecom

WebGoat

- Aplikacja e-learningowa z zakresu bezpieczenstwa
- Zastepuje systemy online
- 30 lekcji
  - CSS
  - Autehntication
  - Web Services
  - ...

WebScarab

- Aplikacja do anallizy komunikacji podczas ruchu http i https
- Narzedzie dla bardziej zaawansowanych uzytkownikow

Spring of Code 2007

- Sponsorowanie ciekawych projektow
- Mozliwosc uzyskania dofinansowania wkwotach od od 2500$ - 20000$
- Kazdy moze sprobowac...