



OWASP

Andrzej Targosz
OWASP Poland Chapter Leader
PROIDEA

andrzej.targosz{@}proidea.org.pl

OWASP

Copyright 2007 © 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>

Misja

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

■ Jakie sa przyczyny?

- ▶ Bezpośrednie podatności - każdy software posiada błędy ale mamy narzędzia, których powinniśmy używać
- ▶ Developerzy i administratorzy – dwa kroki wstecz
- ▶ Struktura organizacyjna, proces developmentu, wsparcie technologii – brak testów, korzystania z narzędzi
- ▶ Aspekty kulturowe programistów
- ▶ Błędna analiza ekonomiczna

Bezpieczeństwo aplikacji dopiero raczkuje...

- Brak metryk do pomiaru bezpieczeństwa – trudno doskonalić konkretne umiejętności bez pomiaru
- Potrzebujemy:
 - ▶ Eksperymentów
 - ▶ Wymiany wiedzy
- Czas ok. 10 lat

Synonimy Open wg. OWASP

- Open = bezpłatny
 - Open = dostępny
 - Open = niezależny
 - 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 zamkniętej grupy
- Licencja OpenSource – możliwość używania materiałów i narzędzi do celów połączonych z projektami OWASP
- Licencja komercyjna – każdy może dowolnie używać w firmie
- Kwota zaangażowania jest zależna od skali firmy

The Guide

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

Użytkownicy Guide

■ Developerzy

- ▶ Implementowanie mechanizmów bezpieczeństwa

■ PM

- ▶ Organizowanie testów penetracyjnych, modelowanie, analiza ryzyka

■ Zespoły bezpieczeństwa

- ▶ Edukacja bezpieczeństwa
- ▶ Testy

Top Ten

- Zestaw wytycznych z najczęściej popełnianymi błędami
- Stosowanie jest zalecane przez:
 - ▶ Komisje Handlu US
 - ▶ IBM
 - ▶ Price Waterhouse Coopers
 - ▶ Sun Microsystems
 - ▶ Bank of Newport
 - ▶ British Telecom

WebGoat

- Aplikacja e-learningowa z zakresu bezpieczeństwa
- Zastępuje systemy online
- 30 lekcji
 - ▶ CSS
 - ▶ Authentication
 - ▶ 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...