

# OWASP w praktyce – Test Penetracyjny

Jarosław Sajko  
OWASP meeting  
06/09/07, Kraków

# O czym będzie ta prezentacja?

- Co to jest test penetracyjny
- Jak taki test przebiega
- Kiedy testować
- OWASP Testing Guide

# Co to jest test penetracyjny?

## ● Test penetracyjny to:

- Test
- Sposób szacowania bezpieczeństwa przedmiotu testu za pomocą standardowych procedur i narzędzi, z wykorzystaniem wiedzy ogólnej: o bezpieczeństwie, o technologiach IT

# Czym nie jest test penetracyjny?

- Test penetracyjny to NIE:
  - NIE jest to audyt
  - NIE jest to proces w pełni automatyczny
  - Wynik testu NIE daje jednoznacznej odpowiedzi na pytanie odnośnie stanu bezpieczeństwa testowanego przedmiotu.

# Jak przebiega test penetracyjny?

## ● Rozpoznanie

- Wszystko co składa się na punkt wyjścia, a więc zarówno wiedza testera jak i dokumentacja przedmiotu testu
- Skanowanie, enumeracja, googling, etc.
- Identyfikacja słabych punktów
- Identyfikacja błędów implementacyjnych

# Jak przebiega test penetracyjny?

## ● Atak

- Próba wykorzystania zidentyfikowanych słabości oraz błędów implementacyjnych w celu kompromitacji poufności, integralności lub dostępności informacji
- Zbadanie wpływu poszczególnych błędów w bezpieczeństwie na bezpieczeństwo całości

# Jak przebiega test penetracyjny?

## ● Raport

- Dostarczenie informacji pozwalających zweryfikować oraz usunąć wykryte błędy
- Dostarczenie informacji pozwalających oszacować istotność wykrytych błędów dla biznesu (*impact, probability*)



# Kiedy testować?

- Im częściej tym lepiej
- W zależności od „krytyczności” systemu
- Po każdej zmianie konfiguracji
- Po każdej aktualizacji oprogramowania/treści; przed „wypuszczeniem nowej wersji”
- W określonych odstępach czasu



# Jakie są rodzaje testów?

## ● Black Box

- Skanowanie pod kątem błędów implementacyjnych specyficznych dla określonej technologii
- Skanowanie pod kątem podatności, o których wiedza jest publicznie dostępna

## ● White Box

- Przegląd kodu
- Przegląd konfiguracji

## ● Grey Box/ Crystal Box

- mix

# OWASP Testing Guide

## ● Projekt

- Free & Open

## ● Książka

- Zawiera szczegółowe informacje na temat błędów bezpieczeństwa występujących w aplikacjach internetowych
- [http://www.owasp.org/index.php/Testing\\_Guide](http://www.owasp.org/index.php/Testing_Guide)

## ● Społeczność

- Wyselekcjonowana i ugruntowana wiedza specjalistów z tej dziedziny

# Co zawiera ta książka?

## ● Książka zawiera:

- Podstawy testowania
- Jak testować aplikacje różnymi metodami
- Duża ilość odniesień do zewnętrznych dokumentów oraz narzędzi (niektóre również OWASP)
- Informacje o tym jak raportować

# Podsumowanie

- Testy penetracyjne są skuteczną metodą podnoszenia poziomu bezpieczeństwa aplikacji; są niezbędne w procesach zarządzania ryzykiem
- OWASP Testing Guide jest doskonałym wprowadzeniem do świata testów dla początkujących jak i przydatnym kompendium dla doświadczonych; stanowi też dobry punkt odniesienia dla tzw. „dobrych praktyk”

Dziękuję

