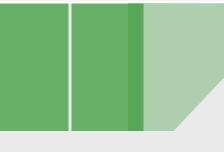


OWASP Meeting Wargame vs. OWASP Testing Guide



OWASP 2008.10.23

Przemysław Skowron Security Researcher Alior Bank S.A.

Przemyslaw.Skowron@gmail.com Tel. "fajny";-)

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

- O autorze
- "Wargame" na Confidence/OWASP EU 2008
- OWASP Testing Guide
- Krótka przypowieść o pentesterze
- Ewangelia wg. Przemka Skowron
- Bibliografia
- Podziękowania

- O autorze:
 - ▶ Specjalista ds. bezpieczeństwa w Alior Bank S.A.
 - Członek OWASP Foundation
 - http://www.owasp.org/index.php/User:Rezos

- "Wargame" na Confidence/OWASP EU 2008:
 - Międzynarodowy zawody dla pentesterów aplikacji webowych
 - Organizatorzy:
 Filip Palian, Andrzej Targosz, Pieter Danhieux, ja
 - ▶ 2 edycje:
 - Pierwsza na (i przed) Confidence 2008 Polska, Kraków
 - Zwyciężył HISPASEC Team
 - Druga na OWASP EU 2008 Belgia, Ghent
 - Zwyciężyli: Johannes Dahse, Frederik Braun, Mario Heiderich
 - ▶ Więcej na:
 - http://www.owasp.org/index.php/OWASP_CTF



■ OWASP Testing Guide:

- ▶ Dlaczego chcę o tym opowiedzieć? Bo wargame był eksperymentem, który się powiódł;)
- ▶ Kto z Was słyszał o OWASP Testing Guide?
- ▶ Kto z Was czytał OWASP Testing Guide?
- ▶ Kto z Was przeczytał OWASP Testing Guide?
- ▶ Kto z Was przetestował coś wg. OWASP Testing Guide?
- ▶ Jeżeli chociaż raz odpowiedziałaś/odpowiedziłeś "NIE" powinieneś zostać na miejscu do końca prezentacji ☺



- OWASP Testing Guide (II):
 - Przejdźmy od razu do konkretu!

START!



- Krótka przypowieść o pentesterze:
 - ▶ Dave Aitel z Immunity Inc. napisał, a ja się z nim zgadzam:
 - Pentesterzy dzielą się na trzy grupy:
 - I używający skanerów podatności ;-P
 - II potrafiący znaleźć błąd typu "Oday" ;-)
 - III potrafiący wykorzystać błąd typy "Oday" ☺

Cieszę się, że mój pracodawca chce bym należał do tych z grupy III! Chociaż nie zawsze jest czas na tyle zabawy... Dlaczego?

- Ewangelia wg. Przemka Skowron:
 - ▶ Co dałem?
 - OWASP Attacks Reference Guide (OWASP Spring of Code 2007)
 - 2x Wargame na imprezach pod brandem OWASP
 - 4 prelekcje na spotkaniach OWASP Poland Local Chapter
 - Co dostałem?
 - 2500 \$ za grant
 - 3 koszulki i trochę gadżetów
 - Pracę przy budowaniu nowego banku Alior Bank S.A.
 - Kontakt z EKSPERTAMI ds. bezpieczeństwa aplikacji
 - Szansę wpłynięcia na bezpieczeństwo, które mnie otacza!



- Ewangelia wg. Przemka Skowron (II):
 - ▶ Co możecie dać?
 - Potrzebujemy prelegentów! (regularne i ciekawe spotkania)
 - Zróżnicowana tematyka i poziom [blogi, artykuły, prace dyplomowe, etc.]
 - Nową jakość dla nowych i trwających projektów!
 - Wkrótce OWASP Winter of Code 2009 [poziomy jakości, trudniej o "byle jaki" grant]
 - Pokaz jak powinienem zacząć to robić ②
 - Dobry powód by spotkać się z kumplami (piłkarzyki, pizza, piwo i inne...;-)) – za co serdecznie dziękuję!



■ Bibliografia:

- http://www.owasp.org/index.php/Poland
- http://www.owasp.org/index.php/OWASP_CTF
- http://www.owasp.org/index.php/SpoC 007 -Refresh Attacks list
- http://www.owasp.org/index.php/Category:OWASP_T esting Project

- Podziękowania:
 - Społeczność OWASP
 - Moja Dziewczyna
 - ▶ Dla Was za to, że jesteście
 - ▶ Dla Andrzeja za to, że wystawił mnie jako pierwszego i nie uciekniecie, bo zaraz Łukasz i Paweł opowiedzą coś ciekawszego ☺

Q&A

Dziękuję!

Przemyslaw.Skowron@gmail.com