OWASP Day - Spring of Code 2k7

OWASP

06.09.2007

Przemysław 'rezos' Skowron
uczestnik Spring of Code 2007
przemyslaw.skowron@gmail.com

Spring of Code 2007

- Agenda:
  - Przemysław ‘rezos’ Skowron
  - NSRAV Security Research Group
  - Spring of Code 2007 (zasady, aplikacje, sponsorzy, etc.)
  - *„Attacks Reference Guide”* - grant
  - Inne (płatne) projekty OWASP’a
  - Podsumowanie

Spring of Code 2007

- Przemysław ‘rezos’ Skowron:
  - lat 24 (od 2001 zawodowo w *„branży”*)
  - na etacie Architekt Systemów (jeszcze…)
  - po etacie konsultant ds. bezpieczeństwa it/informacji
  - …
  - mam też inne hobby, poważnie ;-)
  - Po więcej zapraszam na mój blog: http://pskowron.blogspot.com

Spring of Code 2007

- NSRAV Security Research Group:
  - działający przy Uniwersytecie w Sao Paulo (Brazylia) jako centrum badań bezpieczeństwa, ponad 10 letnie doświadczenie
  - zespół składa się z pracowników naukowych, studentów którzy ukończyli studia, specjalistów ds. bezpieczeństwa z tytułami CISSP, GIAC/SANS
  - zajmują się m.in. tłumaczenie OWASP Testing Guide v2 na język portugalski
  - w wolnych chwilach interesują się dziewczynami (obiecałem Leo że o tym wspomnę ;-))

Spring of Code 2007

- Spring of Code 2007:
  - Zasady
    - Warunek uczestnictwa: nieważne {skąd,ile_masz_lat,cokolwiek} \ {Dinis,Dave,Jeff,Andrew} (także liderzy projektów OWASP)
    - Przekonać, że jesteś w stanie to zrobić
    - trzy miesiące na realizacje (w praktyce ciut więcej…)
  - Sponsorzy:
    - OWASP (92k $) – składki członkowskie, konferencje
    - SPI Dynamics (9k $) – nowy członek OWASP
    - EDS (9k $) – nowy członek OWASP

Spring of Code 2007

- Spring of Code 2007:
  - Aplikacje (27 na 27 zaakceptowano):
    - Inspekt (http://code.google.com/p/inspekt)
      - Biblioteka pozwalająca pisać bezpieczniejszy kod aplikacji webowych
    - OWASP WebGoat Solutions Guide
      - Podręcznik pozwalający efektywniej uczyć się z WebGoat'em
    - WebScarab NG Security Test Automation
      - wygodny framerowk, np..: łatwiejsze testy regresyjne (~, .bak, .old, ataki brute force, czytanie baz testów z innych aplikacji skanujących)
    - Wiele innych b. ciekawych, zapraszam na: www.owasp.org/index.php/OWASP_Spring_of_Code_2007

Spring of Code 2007

- *„Attacks Reference Guide”*
  - **Cel:** dokument, który będzie zawierał **rzeczowy** spis i opis ataków na aplikacje webowe
  - Ścieżka do celu:
    - Sprawdzić i ocenić co już jest, a czego nie ma (wiki)
    - Poddać kategoryzacji liste ataków (aktualnie fatalne…)
    - Dodać ataki, których nie ma w spisie (a są *„znane”*), a także jeśli będzie czas *„poszukać”* nowych
  - Problemy:
    - Pomieszane artykuły (kategorie, guide’y), czasem *„ żarty”*

Spring of Code 2007

- *„Attacks Reference Guide”*
  - Problemy c.d.:
    - **KATEGORYZACJA** ataków:
      - Aktualnie CWE (Common Weakness Enumeration)
      - Będzie CAPEC (Commoon Attack Pattern Enumeration and Classification) i WASC Threat Classification v2
    - Stadium projektu: ~70%
    - **ZAPRASZAM** na prezentacje *„Attacks Reference Guide”* jesienią/zimą 2007!!!
    - … a jeśli się nie uda to może troche później gdy uda mi się namówić Leo na przyjazd do Polski!

Spring of Code 2007

- Inne (płatne) projekty OWASP'a:
  - Gdy Spring of Code 2007 trwa, a są $ to…:
    - OWASP organizuje granty sponsorowane wyłącznie przez sponsorów, w związku z tym nie pojawiają się one w ramach X of Code 2kX
    - OSG – OWASP Site Generator (5k $)
    - OWASP Corporate Application Security Rating Guide (3k $)
    - Questions for SANS (5k $)
    - Source Code Review OWASP Projects (5k $)
    - BlackTop – Runtime coverage analysis tool (10k $)

    - Wszystkie poza OSG jeszcze **WOLNE !!!**

Spring of Code 2007

- Podziękowania:
  - Kasia B. – za motywacje i wiele więcej
  - Robert ‘shadow’ Pająk – za namówienie mnie do startowania o grant
  - Leonardo Cavallari Militelli – za miłą prace przy grancie i opowiadanie o tym jak jest w Brazyli
  - OWASP – za organizacje Spring of Code !!!
  - OWASP Poland Local Chapter – za zaproszenie ;-)
  - Was! – za to, że nie opuściliście do tej pory sali!

Spring of Code 2007

Dziękuję za uwagę!

Przemyslaw.Skowron@gmail.com