I tool OWASP per la sicurezza del software

Paolo Perego
OWASP Project Leader

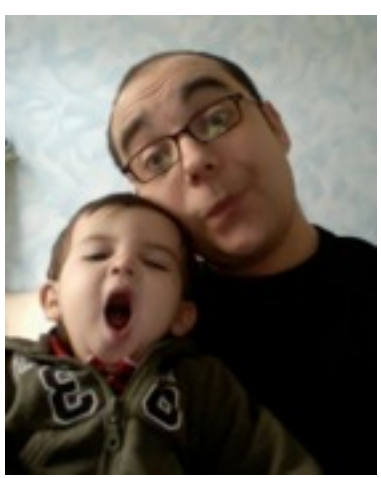
thesp0nge@owasp.prg

OWASP
Security Summit '11

The OWASP Foundation
http://www.owasp.org

$ whoami

- Senior software engineer
  - Ruby on Rails, CMS
- Freelance && startupper
  - Ruby on Rails, iOS, web apps, code review & more
  - pernataleiovorrei.com
  - nuvola.armoredcode.com
  - ...
- Owasp
  - R&D director del capitolo italiano
  - Project leader
- http://about.me/thesp0nge



Parleremo un po' di...

- Tool per l'offesa
  - webscarab
  - jbrofuzz
  - zap
- Tool per la difesa
  - Owasp O2
  - Owasp Orizon
- Tool per gli sviluppatori
  - webgoat
  - ESAPI

Stato dell'arte dei tool Owasp

- I project leader hanno un elevato livello come security professional
- I tool Owasp sono utilizzati in attività reali in tutto il mondo
- Il bacino dei "contributors" ai progetti è basso.
- Il gap tra sviluppatori e Owasp non è ancora colmato
  - Developers outreach project https://lists.owasp.org/mailman/listinfo/developer-outreach

Owasp O2

- Piattaforma per l'application security a 360 gradi
  - Code review sfruttando engine esterni
    - Commerciali (Ounce // Fortify)
    - Opensource (Code Crawler)
  - Test a runtime sfruttando le potenzialità di scripting
  - Owasp O2 viene programmato in C#
- Pensato per dare un'interfaccia grafica evoluta a chi effettua test di sicurezza
- http://www.owasp.org/index.php/OWASP_O2_Platform

Owasp Webscarab

- Tool per l'analisi dinamica di applicazioni web
- Funzionalità base
  - spidering
  - proxying
  - analisi dei session id
  - fuzzing parametri
- ... estendibili con plugin
  - xss / crlf response splitting
  - analisi soap
  - ...
- http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

Owasp Webgoat

- Palestra per penetration tester
- Applicazione J2EE
  - vulnerabile “by design”
  - stabile
- Compendio ideale a
  - Testing guide
  - Building guide
- Must have anche per gli sviluppatori
- http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

Owasp JBroFuzz

- Fuzzer: data un'espressione regolare vengono generate delle stringhe pseudo casuali che ne rispettano il pattern
- Un must have per
  - penetration tester
  - sviluppatori
  - scoprire comportamenti anomali di una certa API a fronte di input non attesi
- http://www.owasp.org/index.php/JBroFuzz

Owasp Live CD

- Distribuzione GNU/Linux “live”
- Contiene materiale Owasp pronto all’uso
  - tool
  - documentazione
- http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

Owasp ZAP

- Proxy applicativo
- Utile per esaminare il traffico tra browser e web application
  - passaggio di parametri
  - parametri nascosti
  - metodi di cifratura utilizzati
- Fork di Paros
  - la versione open di Paros non era più attivamente sviluppata
  - presenta miglioramenti evidenti soprattutto per quello che riguarda la stabilità

Drum roll...

Owasp Orizon

- Motore per la code review
- Basato su parser generati da antlr
  - le grammatiche formali dei linguaggi mantenute da esperti in questo campo dell'IT
  - antlr è lo standard de facto per quello che riguarda i generatori di parser
- Quello che al momento funziona
  - parsing di codice sorgente in Java, PHP, C
  - crawling
- Quello che al momento NON funziona
  - generazione del modello della web application
  - ne segue che... la code review di fatto non è affidabile.

Owasp Orizon / II

- "Si può usare in una code review reale?" - <Nì, usa la versione 1.19 lancia solo il crawling e filtra i molti falsi positivi>
- Molti ostacoli lungo la via
  - mancanza di tempo
  - mancanza di aiuto
- Al momento il progetto è fermo da 7 mesi

Owasp Orizon / 2011 - ultima chiamata prima dell'abbandono

- Ridefinizione degli obiettivi
  - 1 solo linguaggio supportato: Java
  - code review verticale = 2 test di sicurezza
    - xss
    - injection fault
- Nuovo team: abbiamo un nuovo sviluppatore
- Ultima deadline: 31 Dicembre 2011
- Chi vuole aiutare?
- http://www.owasp.org/index.php/Category:OWASP_Orizon_Project

Owasp ESAPI

- ESAPI = Enterprise Security API
  - libreria di controlli di sicurezza
  - disponibile nei principali linguaggi di programmazione (Java, C#, PHP, Ruby, ...)
- Un *must have* in ogni vostro progetto software
  - perché inventare controlli di sicurezza quando Owasp li ha scritti per voi?
- Pensato per gli sviluppatori
  - di immediato utilizzo
  - poca documentazione da leggere
- Uno dei progetti software più importanti e meglio riusciti al momento presente in Owasp
- http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

Owasp ESAPI for Ruby

- Porting della libreria ESAPI in Ruby
- Perché Ruby?
  - comunità in forte espansione
  - molte applicazioni web comunemente usate sono in Ruby (tumblr, yellowpages.com, ...)
- Progetto iniziato a Febbraio 2011
- Abbiamo appena rilasciato la versione 0.30 della "gemma" ESAPI [$ gem install owasp-esapi-ruby]
- Stima del termine del porting: Autunno/Inverno '11
- http://www.owasp.org/index.php/Projects/Owasp_Esapi_Ruby