



The art of code reviewing

OWASP
Italy Day '09

Paolo Perego
OWASP Italy R&D director
OWASP Orizon Project leader

thesp0nge@owasp.org

Copyright 2009 © 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>

I promise

- Few slides
- No in deep technical details about
 - ▶ code
 - ▶ tools
 - ▶ whatever
- Some live code review using opensource tools
 - ▶ findbugs
 - ▶ orizon

\$ whoami



\$ whoami



\$ whoami



\$ whoami



■ A consultant

- ▶ Senior consultant @ Security Reply
- ▶ Application security team leader
- ▶ Code reviewer and Penetration tester



■ A developer

- ▶ Web Based (Java, Ruby, Rails, Grails, ...)
- ▶ Classic UI (Objective-C, C, Ruby)
- ▶ Linux Kernel



■ An Owasp fellow

- ▶ R&D director of Owasp Italy
- ▶ Owasp Orizon project leader
- ▶ Owasp Code review guide co-author

"What is "art"? How do you define "art"?" (courtesy by "The Matrix", 1999)

■ From wikipedia

- ▶ "art is the process or product of deliberately arranging elements in a way that appeals to the senses or emotions. It encompasses a diverse range of human activities, creations, and modes of expression, including music, literature, film, sculpture, and paintings. The meaning of art is explored in a branch of philosophy known as aesthetics"



Is programming an “art”?

- Programming is
 - ▶ taking an algorithm
 - ▶ choosing a language
 - ▶ using that language to
 - implement the algorithm
 - model the reality
 - solve real life problems
 - ...
 - using a calculator
- Programming is made by
 - ▶ humans
 - ▶ people with certain skills
 - ▶ people with creativity
- Software leads its user to have feelings
- Software is art (a sort of...)

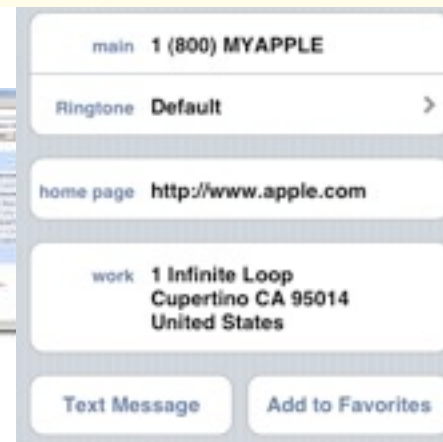


THE CLASSIC WORK
NEWLY UPDATED AND REVISED

The Art of Computer Programming

VOLUME I
Fundamental Algorithms
Third Edition

DONALD E. KNUTH



The SDLC as an “art school”

■ Requirements are

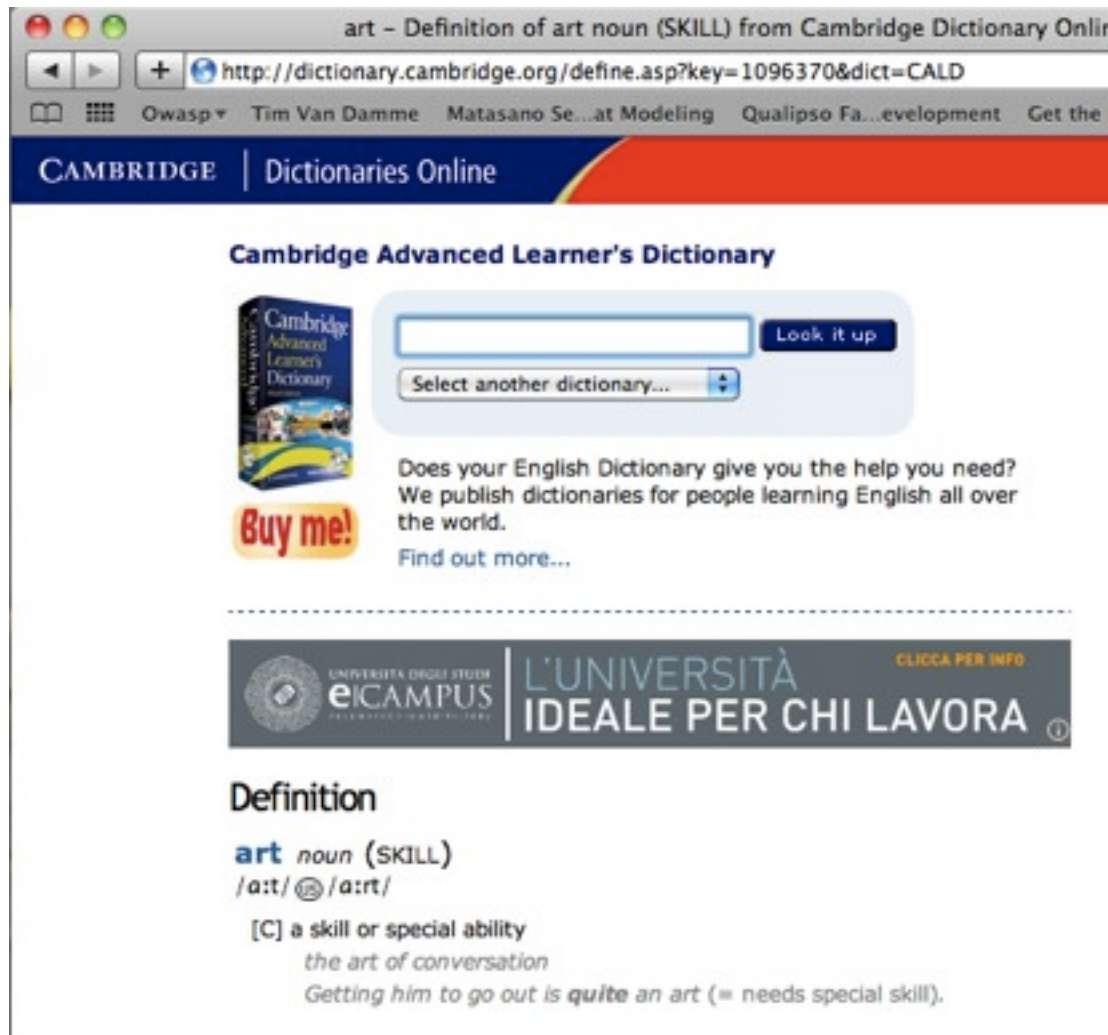
- ▶ gathered - what my customer wants!
- ▶ analyzed - how can I model my customer needs!
- ▶ implemented - I implement a solution!
- ▶ deployed - my customer needs are matched (hopefully)

■ Development team make possible to have a “real world” needs implemented in a “software”

What is a “code review”?

- A human activity
- Performed by
 - ▶ someone with skills
 - in software development
 - in IT security
 - ▶ someone not involved in the development team
- It requires
 - ▶ skills
 - ▶ time
 - ▶ fantasy
 - ▶ defensive programming mindset
 - ▶ attacker point of view
- Can be called... an “art”?

Yes... by definition



The screenshot shows a web browser window with the address bar displaying the URL: <http://dictionary.cambridge.org/define.asp?key=1096370&dict=CALD>. The browser's address bar also shows the text "art - Definition of art noun (SKILL) from Cambridge Dictionary Online". The browser's address bar also shows the text "Owasp Tim Van Damme Matasano Se...at Modeling Qualipso Fa...velopment Get the". The browser's address bar also shows the text "CAMBRIDGE | Dictionaries Online". The browser's address bar also shows the text "Cambridge Advanced Learner's Dictionary". The browser's address bar also shows the text "Buy me!". The browser's address bar also shows the text "Does your English Dictionary give you the help you need? We publish dictionaries for people learning English all over the world. Find out more...". The browser's address bar also shows the text "L'UNIVERSITÀ IDEALE PER CHI LAVORA". The browser's address bar also shows the text "CLICCA PER INFO". The browser's address bar also shows the text "Definition". The browser's address bar also shows the text "art noun (SKILL)". The browser's address bar also shows the text "/ɑ:t/ @ /ɑ:rt/". The browser's address bar also shows the text "[C] a skill or special ability". The browser's address bar also shows the text "the art of conversation". The browser's address bar also shows the text "Getting him to go out is quite an art (= needs special skill).".

art - Definition of art noun (SKILL) from Cambridge Dictionary Online

http://dictionary.cambridge.org/define.asp?key=1096370&dict=CALD

Owasp Tim Van Damme Matasano Se...at Modeling Qualipso Fa...velopment Get the

CAMBRIDGE | Dictionaries Online

Cambridge Advanced Learner's Dictionary

Buy me!

Does your English Dictionary give you the help you need? We publish dictionaries for people learning English all over the world. Find out more...

L'UNIVERSITÀ IDEALE PER CHI LAVORA

CLICCA PER INFO

Definition

art noun (SKILL)
/ɑ:t/ @ /ɑ:rt/

[C] a skill or special ability
the art of conversation
Getting him to go out is *quite* an art (= needs special skill).

The art of code reviewing

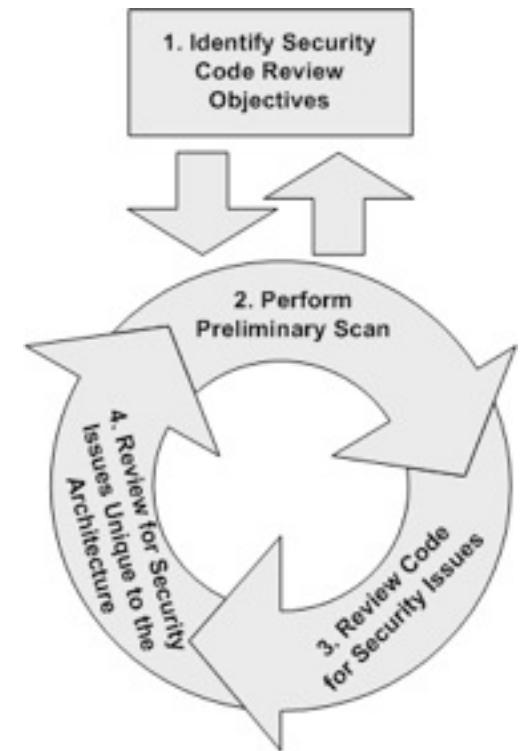
■ “a fool with a tool is still a fool”

■ Code reviewing IS NOT

- ▶ run a tool over a source code
- ▶ do a penetration test! (sic)

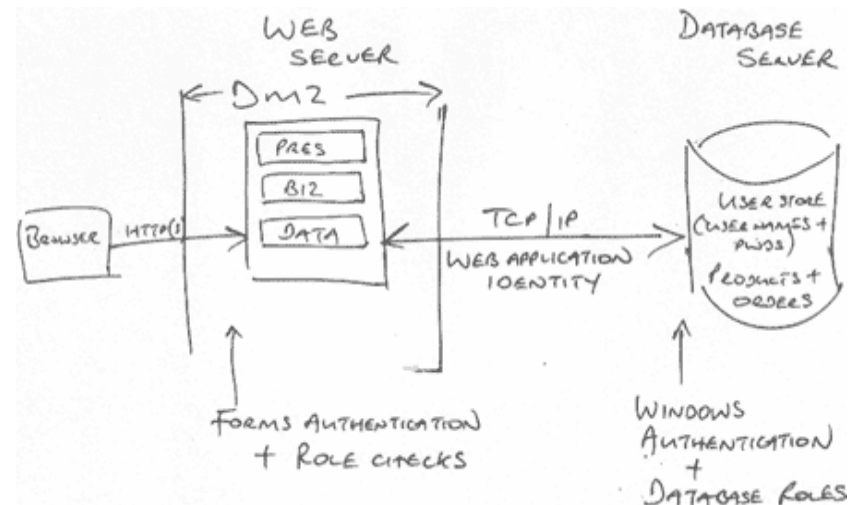
■ Code reviewing IS

- ▶ engage your developers
- ▶ assess application designers
- ▶ obtain use cases, threats and vulnerabilities trees from the source code
- ▶ run the tool
- ▶ read, understand and organize the results



The art of code reviewing

- Information coming from threat modeling are important
- Use cases tell me how people interact with the code
- A threats tree tell me which are the bad programming patterns to check first
- All these information are generally NOT available for a reviewer
- Reverse analysis is the norm



The artist

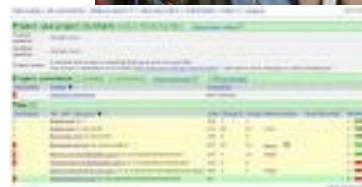
■ Human interaction

- ▶ developers
- ▶ testing team
- ▶ project managers

■ Able to

- ▶ write code
- ▶ break in a web application

■ A passion driven work



What does making a “code review” really means?

- Live demo with opensource tools
 - ▶ Owasp Orizon
 - ▶ Findbugs
- Code reviewing opensource code
 - ▶ Pebble
 - ▶ Wordpress
 - ▶ Grails
 - ▶ Apache Tomcat