OWASP: An Introduction

Sebastien Deleersnyder
CISSP
May, 2005
sdl@ascure.com

OWASP

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

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

Introduction

- Sponsor this evening:
  - www.ascure.com

- Call for additional sponsors
  - Chapter meeting places & catering
  - Support for local projects

- OWASP cannot recommend the use of products, services, or recommend specific companies

Introduction

Program for this evening:

- 18h00 - 18h45:

  Sebastien Deleersnyder, Ascure
  OWASP Introduction

- 19h00 - 19h45:

  Erwin Geirnaert, Security Innovation
  How to Break Web Application Security

- 20h00 - 20h45:

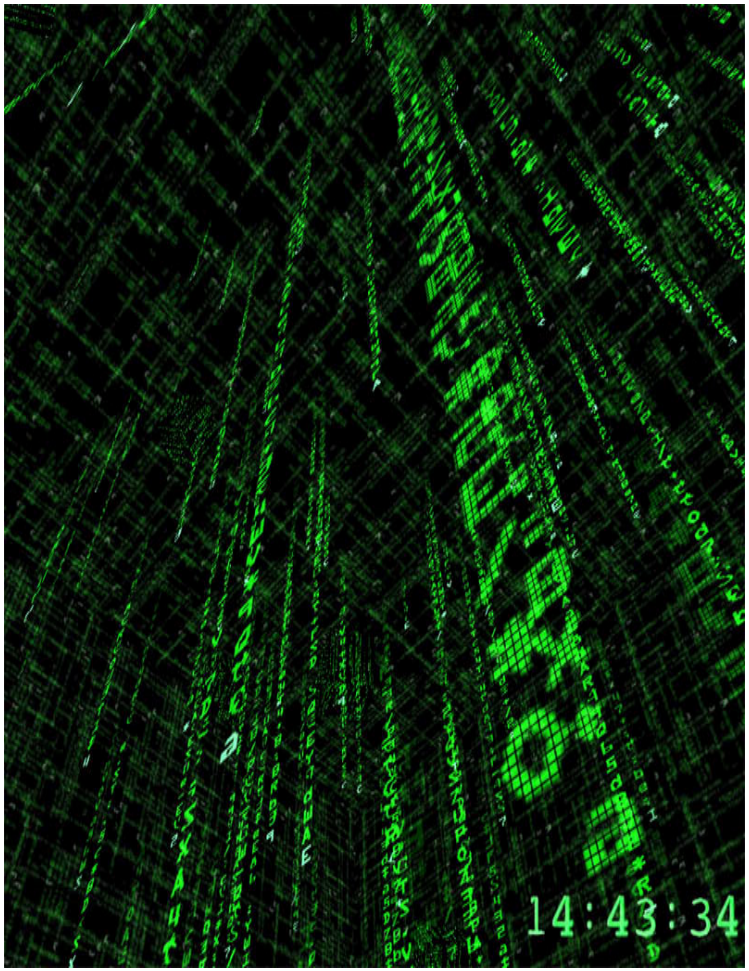
  professor Frank Piessens, KU Leuven
  How to Build Secure Web Applications

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

Software Is A Black Box

- Complex
  - Millions of lines of code
  - Leaky abstractions
  - Massively interconnected
- Compiled
  - Difficult to reverse engineer
  - Different on every platform
- Legal Protections
  - No peeking
  - We're not liable



Application Security Is In Its Infancy

- Nobody understands
- Nobody cares
- Snake oil rules
- No proof anything works
- No metrics
- One application at a time
- Getting easier to write bad code
- We can't even stamp out buffer overflows

- Formal Modeling
- Process Assurance
- Penetrate and Patch
- Manual Code Review
- Static Analysis
- Developer Training
- Top Ten Lists
- Programming Books
- Bugtraq
- Common Criteria
- Certification
- Peer Review
- Guidelines
- Penetration Test Tools
- Vulnerability Scanning
- Proxy Solutions
- … and more

Enter OWASP

- OWASP is dedicated to finding and fighting the causes of insecure software

- People
- Projects
- International
- Community

- "Charitable Open Source"

What is OWASP?

- Open Web Application Security Project
  - Non-profit, volunteer driven organization
    - All members are volunteers
    - All work is donated by sponsors
  - Provide free resources to the community
    - Publications, Articles, Standards
    - Testing and Training Software
    - Local Chapters & Mailing Lists
  - Supported through sponsorships
    - Corporate support through financial or project sponsorship
    - Personal sponsorships from members

What is OWASP?

- What do they provide?
  - Publications
    - OWASP Top 10
    - OWASP Guide to Building Secure Web Applications
  - Software
    - WebGoat
    - WebScarab
    - .NET Projects
  - Local Chapters
    - Community Orientation

Looking for a second breath

- OWASP finally achieved 501c3 status in Dec.
  - Charitable not-for-profit
- OWASP needs more contributors
  - We should provide everything contributors need
  - Better infrastructure
  - Project management
  - Technical editing
- OWASP needs funding
  - Need full time director

OWASP Roadmap for 2005

- Continue to deliver on existing projects
- Gather requirements from industry
- Find a full time director

- New projects
  - **OWASP Standard** – minimum criteria for people, process, and technology
  - **OWASP Legal** – guidance on contracts, gov't regulations, RFP language
  - **J2EE** – guidelines, methodologies, tools
  - **Web Services** – guidelines, methodologies, tools
  - **OWASP Training Course**

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

OWASP Current Status

- WebGoat **Great**
- WebScarab **Great**
- DotNet **Great**
- Validation **No Progress**
- oLabs **No Progress**

- Local Chapters **Excellent**
- International **Great**
- Conferences **Great**

- Legal **Great**
- Guide **Great**
- Papers **Great**
- Testing **Great**
- Metrics **No Progress**
- AppSec FAQ **No Progress**
- Top Ten **No Progress**
- ISO17799 **No Progress**

OWASP Testing Project

- Create a "best practices" testing framework
- "low level" testing guide to find issues
- Phase 1 released Dec 2004
  - The scope of what to test
  - Principles of testing
  - Testing techniques explained
  - The OWASP testing framework explained
- Currently 2nd phase ongoing (TOC)
- Lead by Daniel Cuthbert

WebScarab Project

- Tool for anyone involved with HTTP-based applications (e.g. web applications)
- Key features
  - Full visibility into the HTTP protocol
  - Also supports HTTPS (incl client certs)
  - Persistent audit trail can easily be reviewed
- Primary uses
  - Security analysis
  - Application debugging
- Lead by Rogan Dawes

Conferences

- Previous Conference
  - UK April 05 – Royal Holloway
- Next Conference
  - US Oct 05 – NIST Washington DC

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

Belgium Chapter -What do we have to offer?

- Quarterly (?) Meetings
- Mailing List
- Presentations & Groups
- Open forum for discussion
- Meet fellow InfoSec professionals
- Create (Web)AppSec awareness in Belgium
- Local projects:
  - Dutch & French Top 10 / Guide ?

Belgium Chapter – House Rules

- Free & open to everyone
- Language
  - English preferred
  - Native language: no problem!
- No vendor pitches or $ales presentations
- Respect for different opinions
- No flaming (including M$ bashing)

Next Chapter Meetings program proposal

- Short OWASP intro
- Presentation on one specific topic
- Follow-up
  - Open discussion on topic (with panel?)
  - Split up per topic + feedback into group

OWASP Local Chapters

- Next Meeting: Sep + Dec 2005
- Topics:
  - ?
- Location:
  - ?

Agenda

- Introduction
- OWASP
- OWASP Projects
- Belgium Chapter
- (Web)AppSec Resources

Resources Online

- OWASP Project Mailing lists
- Secure Coding List
- WebAppSec@securityfocus.com
- websecurity@webappsec.org (WASC)
  - Low signal-to-noise ratio
- www.threatsandcountermeasures.com

Resources - Blogs

- Michael Howard's Web Log
- Keith Brown Blog
- T&C BLOGS
  - Mark Curphey
  - Michael Silk
  - …

Resources Hard Copy

- IEEE Security & Privacy (bimonthly)

- Security Engineering – Anderson
- Building Secure Software – Viega & McGraw
- Exploiting Software : How to Break Code – Hoglund & McGraw
- Writing Secure Code – Howard & Leblanc
- Enterprise Java Security – Pistoia, et al
- Securing Web Services with WS-Security – Rosenberg & Remy

That's it…

- Any Questions?

http://www.owasp.org/local/belgium.html

sdl@ascure.com

Thank you!

Subscribe to Chapter mailing list

- Keep up to date!
- Post your (Web)AppSec questions
- Contribute to discussions!