OWASP: An Introduction

By Marco Morana
January 29th, 2008
Marco.Morana@OWASP.ORG

OWASP

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

Agenda

1. What is OWASP
2. OWASP Publications
3. OWASP Tools Demo By Blaine Wilson
4. OWASP Cincinnati Local Chapter
5. Final Questions

What is OWASP?

- Open Web Application Security Project
  - Promotes secure software development
  - Support application security risk decision making
  - Focused on the security of web applications as software products of the SDLC
  - Provides free resources to developer teams
  - Encourages active participation and information sharing

What is OWASP?

- Open Web Application Security Project
  - Non-profit, volunteer driven organization
    - All members are volunteers
    - Some projects are supported 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 Guides to Building/Testing Secure Web Applications
  - Release Quality Tools/Documentation
    - WebGoat
    - WebScarab
  - Beta and Alpha Quality Tools/Documentation
    - Beta Tools (16) ,Alpha Tools(10)
    - http://www.owasp.org/index.php/Category:OWASP_Project
  - Local Chapters
    - Community Orientation

OWASP Publications

- Release Publications
  - Top 10 Web Application Security Vulnerabilities
  - Guide to Building Secure Web Applications
  - Legal Project
  - Testing Guide
  - AppSec Faq

OWASP Publications

- Common Features
  - All OWASP publications are available free for download from http://www.owasp.org
  - Publications are released under GNU “Lesser” GNU Public License agreement, or the GNU Free Documentation License (GFDL)
  - Living Documents
    - Updating as needed
    - Ongoing Projects
  - OWASP Publications feature collaborative work in a competitive field

OWASP Publications – OWASP Top 10

- Top 10 Web Application Security Vulnerabilities
  - A list of the 10 most severe security issues
  - Updated on a yearly basis
  - Address issues with applications on the perimeter
  - Growing industry acceptance
    - Federal Trade Commission (US Gov)
    - US Defense Information Systems Agency
    - VISA (Cardholder Information Security Program)
  - A good starting point for developing web application security standards for organizations
  - List of Adopters
    - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Publications - OWASP Top 10

- Current (2007)Top Ten Issues
  - A1. Cross Site Scripting
  - A2. Injection Flaws
  - A3. Malicious File Execution
  - A4. Insecure Direct Object Reference
  - A5. Cross Site Request Forgery
  - A6. Information Leakage and Improper Error Handling
  - A7. Broken Authentication and Session Management
  - A8. Insecure Cryptographic Storage
  - A9. Insecure Communications
  - A10. Failure to Restrict URL Access

  https://www.owasp.org/index.php/Top_10_2007

OWASP Publications - OWASP Top 10

- Addressing the Top Ten
  - In Presentation (Future Meetings)
    - February 26 – OWASP Top Ten will be discussed
    - March 25 – OWASP Testing Guide will be discussed
  - On the Mailing List
    - The mailing list is a public forum, and as such is suitable for asking questions in general
    - Specific application issues should be discussed in private, especially with regards to business projects
  - Focus Groups
    - If there is sufficient interest, focus groups can be created to discuss specific issues from the perspective of secure design/threat modeling, secure coding, source code analysis, security tests

OWASP Publications - OWASP Guide

- Guide to Building Secure Web Applications
  - Provides a baseline for developing secure software
    - Introduction to security in general
    - Introduction to application level security
    - Discusses key implementation areas
      - Architecture
      - Authentication
      - Session Management
      - Access Controls and Authorization
      - Event Logging
      - Data Validation

      http://www.owasp.org/index.php/OWASP_Guide_Project

OWASP Publications - OWASP Guide

- Future Topics regarding the Guide
  - In Presentation (Future Meetings)
    - Following the Top Ten presentations specific issues will be addressed in monthly meetings
  - On the Mailing List
    - The focus of the OWASP group is to address all questions pertaining to application security, of any level of technical ability
  - Focus Groups
    - If there is sufficient interest, focus groups can be created to discuss specific issues

OWASP Publications – OWASP Legal

- Legal Project
  - Project focused on contracting for secure software
  - Secure Software Contract Annex
    - Targeted towards consultants
    - Addresses secure software concerns between customers and vendors
  - Secure software contracting hypothetical case study
    - Company outsourced web application development to a software shop
    - Company sue the developers on breach of contract for negligence
  - This project does NOT provide legal advice, but rather guidelines from which legal documents can be drafted

OWASP Publications – Testing Project

- Security Testing Guide
  - A framework for testing web applications
    - Testing Best Practices (when to test, what to test and how)
    - Testing Methodologies (manual reviews, threat modeling, code reviews, penetration testing)
    - Testing Tools (black box, white box static parsers, dynamic analyzers, acceptance test tools)
    - Test Cases For Common Web Application Vulnerabilities
    - Criteria for Evaluating The Risk Severity For The Vulnerabilities
    - Reporting
  - Getting the Guide
    - http://www.owasp.org/index.php/OWASP_Testing_Project

OWASP Tools Demo By Blaine Wilson

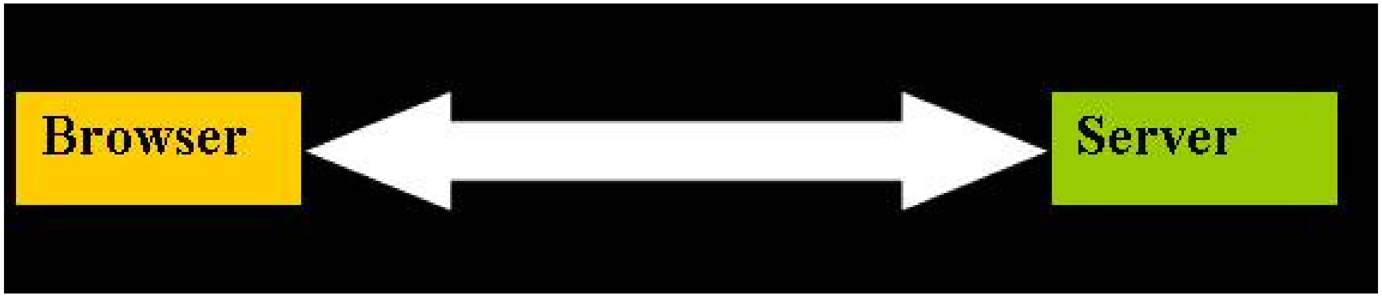
- Webscarab web proxy
- Webgoat Training web site

OWASP Software - WebScarab

- WebScarab
  - A framework for analyzing HTTP/HTTPS traffic
  - Written in Java
  - Multiple Uses
    - Developer: Debug exchanges between client and server
    - Security Analyst: Analyze traffic to identify vulnerabilities
  - Technical Tool
    - Focused on software developers
    - Extensible plug-in architecture
    - Open source; easy to extend core system
    - Very powerful tool
  - Getting the Tool
    - http://www.owasp.org/software/webscarab.html

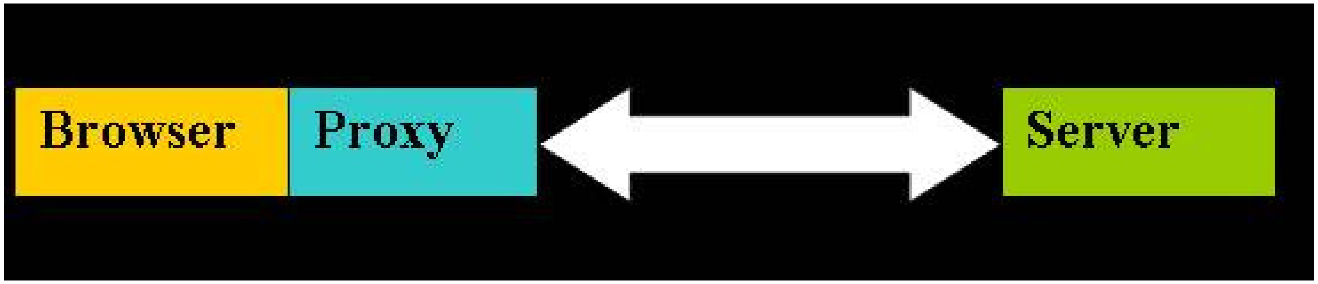
OWASP Software - WebScarab

- WebScarab
  - Client server application using HTTP as the transport
  - Delegation of tasks between the client and the server



OWASP Software - WebScarab

- WebScarab
  - Resides between the client and the server
  - Services requests on behave of the client
  - Benefits include; Caching, Content filtering, Reformatting for special browsers (cell phones), Track usage



OWASP Software - WebScarab

DEMO

OWASP Software - WebGoat

- WebGoat
  - Primarily a training application
  - Provides
    - An educational tool for learning about application security
    - A baseline to test security tools against (i.e. known issues)
  - What is it?
    - A J2EE web application arranged in “Security Lessons”
    - Based on Tomcat and JDK 1.5
    - Oriented to learning
      - Easy to use
      - Illustrates credible scenarios
      - Teaches realistic attacks, and viable solutions

OWASP Software - WebGoat

- WebGoat – What can you learn?
  - A number of constantly growing attacks and solutions
    - Cross Site Scripting
    - SQL Injection Attacks
    - Thread Safety
    - Field & Parameter Manipulation
    - Session Hijacking and Management
    - Weak Authentication Mechanisms
    - Many more attacks added
  - Getting the Tools
    - http://www.owasp.org/software/webgoat.html
    - Simply download, unzip, and execute

OWASP Software – WebGoat

DEMO

Warning

- Using what you have learned on your company’s web applications will get you fired.

OWASP Cincinnati Local Chapter

- The main objective it to building a community
  - Local Chapters provide opportunities for OWASP members to share ideas and learn information security, several locations around the world: http://www.owasp.org/apps/maps/index.jsp
  - Open to all; any level of proficiency
  - Provide a forum to discuss issues based on local regulation and legislation
  - Provide venue for invited guests to present new ideas and projects
  - To join a chapter, simply sign up on the mailing list: https://lists.owasp.org/mailman/listinfo/owasp-cincinnati

OWASP Cincinnati Local Chapter

- Started October 2007
  - Need to establish a web application security community to serve security professionals
  - Support from Citigroup (location, speakers)
- What do we have to offer?
  - Monthly Meetings
  - Mailing List
  - Presentations & Groups
  - Open Forums for Discussion
  - Vendor Neutral Environments

OWASP Cincinnati Local Chapter

- What do we have to offer?
  - Monthly Meetings
    - An opportunity to listen to monthly presentations introducing OWASP (prior to regular meetings)
    - An opportunity to attend special presentations focused on OWASP projects, and focusing on specific areas of interest
    - An opportunity to work with organizers to show additional presentations and develop workshops to address specific issues
    - An open environment for discussion of information security suitable for novices, professionals, and experts
    - Free Coffee!!!!!

OWASP Cincinnati Local Chapter

- What do we have to offer?
  - Mailing Lists
    - A wide selection of mailing lists are available from the OWASP main page, including specific mailing lists for all topics covered today https://lists.owasp.org/mailman/listinfo
    - A local mailing list which can be used to arrange focus groups, monthly meetings, and discuss issues of importance locally https://lists.owasp.org/mailman/listinfo/owasp-cincinnati
  - Rules
    - Keep it professional; most subscribers currently receive messages to business accounts
    - No sales or marketing materials; the list will be restricted to subscribers, however if spam becomes an issue moderation will be enforced

OWASP Cincinnati Local Chapter

- What do we have to offer?
  - Informative Presentations
    - Every monthly meeting will host a 60 minute presentation on a new topic or area of interest
    - Strong focus on building understanding of technical issues
    - If enough interest is generated, specialized presentations can be scheduled
  - Focus Groups
    - As the organization grows focus groups may form allowing for focused discussion outside of monthly meetings
    - Formalized focused groups can be created to tackle specific issues

OWASP Cincinnati Local Chapter

- What do we have to offer?
  - Vendor Neutral Environments
    - Learn about security without the sales pitches
    - OWASP does not sells: all revenue generated from either website advertising or donations
    - Vendor Neutral Environments
  - Strict guidelines for chapter presentations and sponsorship
    - All sponsors must be approved by The OWASP Foundation.
    - No product presentations !
    - Presentations that focus on a problem or set of problems and discuss solution approaches that may refer to or show examples of various products are allowed.
    - Sponsorship shall be in the form of donations to The OWASP Foundation in the name of the local chapter and to provide food / beverages at meeting events.

OWASP Cincinnati Local Chapter

- What do we have to offer?
  - Stable location to held meeting at Citigroup

    9997 Carver Road
    Blue Ash, Ohio
- Proposed Meeting Schedule
  - Last Tuesday of Each Month
    - » Jan 29
    - » Feb 26
    - » Mar 25

    TBDs

OWASP Cincinnati Local Chapter

- What can you offer?
  - Mailing Lists
    - Participate to the mailing lists, meetings, and focus groups are open forums for discussion of any relevant topics
    - Mailing Lists
  - Become a Member

    http://www.owasp.org/index.php/Membership
  - Participate in OWASP projects
    - Contribute to existing projects
    - Propose new projects
    - Spearhead new ventures
  - Participate in the Local Chapter
    - Reach out the executive board (email contact information is available on local chapter site)
    - Encourage others to subscribe to the email list (full contact information can be elicited via email)

OWASP Cincinnati Local Chapter

- Next Meeting
  - Feb 26, 2007 5.30 PM-7 PM
  - Presentation:
    - 2007 OWASP Top Ten, Marco Morana
  - Location:

Citigroup Campus
Buckeyes Room First Floor
9997 Carver Road
Blue Ash, Ohio

Final Questions

- Further questions on OWASP organization, local chapter, tools demo

Presentation is online:

http://www.owasp.org/index.php/Cincinnati

Thank you for attending!