OWASP: An Introduction

By Yvan Boily
March, 2005
yboily@gmail.com

OWASP

The OWASP Foundation

http://www.owasp.org

Agenda

- What is OWASP

Discuss anything *during* the presentation!

32 slides.

What is OWASP?

- Open Web Application Security Project
  - Promotes secure software development
  - Oriented to the delivery of web oriented services
  - Focused primarily on the “back-end” than web-design issues
  - An open forum for discussion
  - A free resource for any development team

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
    - oLabs Projects
    - .NET Projects
  - Local Chapters
    - Community Orientation

OWASP Publications

Major Publications

Top 10 Web Application Security Vulnerabilities

Guide to Building Secure Web Applications

Legal Project

Metrics & Measurements Project

Testing Project

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)
  - Strong push to present as a standard

OWASP Publications - OWASP Top 10

- Current Top Ten Issues
  - A1. Unvalidated Input
  - A2. Broken Access Controls
  - A3. Broken Authentication and Session Management
  - A4. Cross Site Scripting Flaws
  - A5. Buffer Overflows
  - A6. Injection Flaws
  - A7. Improper Error Handling
  - A8. Insecure Storage
  - A9. Denial of Service
  - A10. Insecure Configuration Management

OWASP Publications - OWASP Top 10

- Addressing the Top Ten
  - In Presentation (Future Meetings)
    - March 28 – OWASP Top Ten A1-A5 will be discussed
    - April 25 – OWASP Top Ten A6-10 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 (e.g. Data Validation, Session Management, Access Controls)

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
  - Under continuous development

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
  - This project is under development
  - First Stage – Secure Software Contract Annex
    - Targeted towards consultants
    - Addresses secure software concerns between customers and vendors
  - Long term objectives
    - Provide boilerplates for application security
    - Cover legal issues from both perspectives (customer & vendor)
  - This project does NOT provide legal advice, but rather guidelines from which legal documents can be drafted

OWASP Publications – Ongoing Projects

- Ongoing Projects
  - Metrics & Measurements Project
    - Aim to address the need for useable security metrics to support business-critical decisions
    - Currently in early development
  - Testing Project
    - Aim to produce a “best practices” framework which can be implemented
    - Aim to produce a “low level” testing framework to identify certain issues
  - AppSec Faq
    - Ongoing FAQ for application security developers
    - Provides answers to questions about application security

OWASP Software

Major Applications

WebGoat

WebScarab

.Net Projects

oLab Projects

OWASP Software

- Common Features
  - All OWASP software are provided free for download from http://www.owasp.org
  - Software is released under GNU “Lesser” GNU Public License agreement
  - Active Projects
    - Updating as needed
    - Ongoing Projects
    - Many maintainers and contributors
  - OWASP Software is free for download and can be used by individuals or businesses

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 - 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

- What can it do?
  - Features
    - Fragment Analysis – extract scripts and html as presented to the browser, instead of source code presented by the browser post render
    - Proxy – observe traffic between the browser and server, includes the ability to modify data in transit, expose hidden fields, and perform bandwidth manipulation
    - BeanShell – the ability to execute Java code on requests and responses before being transmitted between the browser and server; allows runtime extension of WebScarab
    - Spider – identifies new URLs within each page viewed
    - SessionID Analysis – Collection and analysis of cookies to determine predictability of session tokens
    - Much more…

OWASP Software – oLab Projects

- oLab Projects
  - Clearing house for projects contributed by OWASP members
  - Smaller tool sets, proofs of concept, etc
  - Current Tools
    - CodeSpy – Attempts to analyze Java code for Top 10 issues
    - WebSphinx – Java Webcrawler designed for extensibility
    - C# Spider – basic framework for spidering web pages, and excellent starting point for a security tool
    - PHP Filters – a collection of PHP functions for sanitizing user input to protect against Cross Site Scripting and SQL injection issues
  - http://www.owasp.org/software/labs.html

OWASP Software - .NET Projects

- .Net Projects
  - A collection of tools focused on securing ASP.NET projects
  - Include security analyzers and documentation projects
  - Current Projects
    - Asp.Net Baseline Security – a suite of tools to assist administrators in identifying common issues in Asp.Net deployments
    - SAM'SHE – Security Analyzer for Microsofts Shared Hosting Environments – toolkit for administrators to identify issues in IIS 5 or 6 Asp.Net deployments
    - ANSA – Asp.Net Security Analyzer written in C# to identify configuration and software issues that impact security
    - Asp.Net Security Guides – a set of documents covering the design and deployment of secure software in Asp.Net hosting environments
  - http://www.owasp.org/software/dotnet.html

OWASP Local Chapters

- Building Communities
  - Local Chapters provide opportunities for OWASP members to share ideas and learn information security
  - 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

OWASP Local Chapters

- What do we have to offer?
  - Monthly Meetings
  - Mailing Lists
  - Presentations & Groups
  - Vendor Neutral Environments
  - Open Forums for Discussion

OWASP Local Chapters

- 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 Local Chapters

- 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
    - A local mailing list which can be used to arrange focus groups, monthly meetings, and discuss issues of importance locally
      - Discuss any OWASP related topic; application security, information security related topics, etc
    - A couple of rules
      - Lets keep it professional; most subscribers currently receive messages to business accounts
      - No sales or marketing materials; the list will be restricted to subscribers without moderation, however if spam becomes an issue moderation will be enforced

OWASP Local Chapters

- 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 Local Chapters

- What do we have to offer?
  - Vendor Neutral Environments
    - Learn about security without the sales pitches
    - OWASP does not sell
      - All revenue generated from either website advertising or donations
    - Strict guidelines for chapter presentations and sponsorship
      - All sponsors must be approved by The OWASP Foundation.
      - No product presentation may take place at any meeting of a local chapter.
      - 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 Local Chapters

- What do we have to offer?
  - Vendor Neutral Environments
    - Vendor Neutral Meeting Environments
      - Future meetings to be held at the University of Winnipeg campus
      - Location:

        Room 403

        294 William Ave.

        Winnipeg, MB
    - Meeting Schedule
      - Last Tuesday of Each Month
        - » Mar. 29
        - » Apr. 26
        - » May 31
        - » June 28
        - » July 26
        - » Aug. 30

OWASP Local Chapters

- What do we have to offer?
  - What can you offer?
    - The mailing lists, meetings, and focus groups are open forums for discussion of any relevant topics
    - Members are encouraged to bring forward questions
    - Members are encouraged to participate in OWASP projects
      - Contribute to existing projects
      - Propose new projects
      - Spearhead new ventures
    - Local chapter executive team will work towards building the organization as a free, open, and technically oriented resource for the general public and members
      - Email contact information is available on local chapter site
      - Full contact information can be elicited via email

OWASP Local Chapters

- Next Meeting
  - March 29, 2003
  - Presentation:
    - OWASP Top Ten (Part 1), Yvan Boily
  - Location:

    Room 403

    294 William Ave.

    Winnipeg, MB

That’s it…

- Any final words?

- Presentation will be online:
  http://www.owasp.org/local/winnipeg.html

Thank you!