Summit Overview
OWASP Summit Overview

Portugal, 3rd - 7th Nov 2008

OWASP Summit EU 2008 is a worldwide gathering of OWASP leaders and Key Industry Players to present and discuss the latest OWASP tools and documentation projects.

In addition to 40+ presentations from the OWASP Leaders granted 250,000 USD for web application security research, the summit will host multiple Working Sessions designed to improve collaboration, achieve specific objectives and decide roadmaps for OWASP projects, chapters and for the OWASP community itself.

Containing both technical and business tracks, the Summit is the perfect place to learn what resources OWASP has available for use today.

And with the confirmed presence of its most active leaders (OWASP is covering their expenses), the Summit will provide a relaxed but professional environment to meet the OWASP Leaders and to contribute to those project’s roadmaps for 2009.

Following and expanding the tradition started at OWASP conferences, the Summit will also host the largest offering of training courses, covering multiple OWASP specific and Web Application Security Topics

The OWASP European Summit 2008 will be hosted at the Grande Real Santa Eulalia 5 start Resort in Algarve Portugal (http://www.GrandeRealSantaEulaliaHotel.com), and all travel arrangements should be handled via the assigned travel agency Diplomata Tours http://www.DiplomataTours.pt/

For Summit related queries please contact Kate Hartmann (kate.hartmann@owasp.org)
OWASP Summit Working Sessions

Portugal, 4\textsuperscript{rd} - 5\textsuperscript{th} Nov 2008

OWASP is bringing together its Leaders with the world’s best application security experts to meet at the OWASP Summit in order to work on targeted Working Sessions

Everyone who attends is invited to join, share opinions and make the difference. All outcomes produced during the working session will be presented during the Summit’s conference and discussed at a special OWASP Board meeting who will vote on the proposed Initiatives, Statements or Decisions.

The following OWASP specific Working Sessions are currently scheduled

<table>
<thead>
<tr>
<th>Tuesday, November 4</th>
<th>Wednesday, November 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP Strategic Planning for 2009 - 3h</td>
<td>OWASP Top 10 2009 - 3h</td>
</tr>
<tr>
<td>OWASP Tools Projects - 3h</td>
<td>OWASP Education Project - 2h</td>
</tr>
<tr>
<td>ISWG: Browser Security - 7h</td>
<td>OWASP Enterprise Security API Project -4h</td>
</tr>
<tr>
<td>OWASP Documentation Projects - 3h</td>
<td>OWASP Code Review Guide 2009 - 2h</td>
</tr>
<tr>
<td>OWASP .NET Project - 2h</td>
<td>OWASP Certification - 2h</td>
</tr>
<tr>
<td>2-way Internationalization of OWASP - 2h</td>
<td>App Security Desk Reference (ASDR) - 4h</td>
</tr>
<tr>
<td>A.R.C.A.: Metrics and Vulnerabilities - 2h</td>
<td>OWASP Intra Governmental Affairs - 2h</td>
</tr>
<tr>
<td></td>
<td>OWASP Awards - 2h</td>
</tr>
<tr>
<td></td>
<td>OWASP Website - 2h</td>
</tr>
<tr>
<td></td>
<td>ISWG:Web App Framework Security - 4h</td>
</tr>
<tr>
<td></td>
<td>OWASP Live CD&amp;DVD - 2h</td>
</tr>
<tr>
<td></td>
<td>Best Practices for OWASP Chapter Leaders 2h</td>
</tr>
</tbody>
</table>

OWASP Summit Conference

Portugal, 6th - 7th Nov 2008 (Thu & Fri)

OWASP Summit Conference is a two-day immersion into OWASP projects and initiatives. The world’s finest security professionals will present their latest application security research. In addition, project leaders and reviewers will be presenting OWASP Summer of Code 08 results and new challenges brought up during 2-day Working Sessions.

There are 4 technical tracks and one special Business Track (aimed at managers and decision-makers).

The objective is to present the attendees with a global view of the enormous resources available today at OWASP.

- **Business Track**: Business-focused sessions covering application security, strategic OWASP projects and how to get involved.

- **Technical Track 1: Secure Design & Defensive Strategies**: tools and modules to use and improve application security

- **Technical Track 2: OWASP Internals**: projects and initiatives that make application security more visible

- **Technical Track 3: Cutting Edge Tools**: new and innovative tools designed to test, detect and prevent web application security issues

- **Technical Track 4: Security Guidance and Knowledge**: documentation, books and references to keep people informed about application security

The Conference finishes with an open OWASP Board Meeting, where the audience is invited to participate and contribute on topics presented during the previous days.
# Technical Tracks Agenda

## Day 1 – November 6th (Thursday morning)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00</td>
<td>KeyNote</td>
<td></td>
</tr>
<tr>
<td>09:45</td>
<td>About OWASP</td>
<td></td>
</tr>
</tbody>
</table>
| 10:40 | **T1: Secure Design & Defensive Strategies** | OWASP Enigform and mod_Openpgp (SoC 08)  
Arturo Alberto Busleiman (a.k.a Buanzo) |
|       |          | OWASP OpenSign Server Project (SoC 08)  
Phil Potisk, Richard Conway - pending or Mark Roxberry |
| 11:00 |          | OWASP AntiSamy (SoC 08)  
Arshan Dabirsiaghi |
| 11:20 |          | OWASP AppSensor (SoC 08)  
Michael Coates |
| 11:40 |          | OWASP Securing WebGoat using ModSecurity (SoC 08)  
Stephen Craig Evans, Christian Folini |
| 12:00 |          | OWASP Book Cover & Sleeve Design, OWASP Individual & Corporate Member Packs (SoC 08)  
Deb, LX Studios |
| 12:20 | **T2: OWASP Internals** | OWASP Internationalization Guidelines (SoC 08)  
Juan Carlos Calderon |
|       |          | OWASP Spanish Project (SoC 08)  
Juan Carlos Calderon |
|       |          | OWASP Positive Security (SoC 08)  
Eduardo Vianna de Camargo Neves |
|       |          | OWASP Source Code Review  
OWASP Projects (SoC 08)  
James Walden |
|       |          | OWASP Education (SoC 08 Working Session)  
Sebastien Deleersnyder, Martin Knobloch |
<table>
<thead>
<tr>
<th>Time</th>
<th>T3: Cutting Edge Tools</th>
<th>T4: Security Guidance and Knowledge</th>
</tr>
</thead>
</table>
| 14:00 | OWASP Access Control Rules Tester Project (SoC 08)  
*Andrew Petukhov*                | OWASP Classic ASP Security Project (SoC 08)  
*Juan Carlos Calderon*            |
| 14:20 | OWASP Skavenger Project (SoC 08)  
*Matthias Rohr*                    | OWASP .NET Project (SoC 08 & Working Session)  
*Mark Roxberry*                    |
| 14:40 | OWASP JSP Testing Tool (SoC 08)  
*Jason Li*                          |                                                                        |
| 15:00 | WebScarab-NG (SoC 08)  
*Rogan Dawes*                         | OWASP SQL Injector Benchmarking Project (SoC 08)  
*Kevin Fuller*                      |
| 15:20 | OWASP Pantera (SoC 08)  
*Simon Roses Femerling*               | OWASP Code Review Guide (SoC 08 & Working Session)  
*Eoin Keary*                         |
| 15:40 | OWASP Live CD 2008 (SoC 08)  
*Matt Tesauro*                        |                                                                        |
| 16:00 | OWASP Teachable Static Analysis Workbench (SoC 08)  
*Dmitry Kozlov*                     | OWASP Backend Security Project (SoC 08)  
*Carlo Pelliccioni*                  |
| 16:20 | TDB                                                                                 | OWASP Application Security Desk Reference (ASDR) (SoC 08 & Working Session)  
*Leonardo Cavallari Militelli*      |
| 16:40 | OWASP Orizon Project (SoC 08)  
*Paolo Perego (aka thesp0nge)*         | OWASP Ruby on Rails Security Project (SoC 08)  
*Heiko Webers*                       |
| 17:00 | OWASP Application Security Tool Benchmarking Environment and Site Generator Refresh Project (SoC 08)  
*Dmitry Kozlov*                     | OWASP Testing Guide (SoC 08 & Working Session)  
*Matteo Meucci*                      |
| 17:20 | TBD                                                                                 |                                                                        |
| 17:40 | OWASP Application Security Verification Standard Project  
*Jeff Williams*                     |                                                                        |

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>19:00</td>
<td>OWASP Gala Dinner</td>
</tr>
</tbody>
</table>
### Day 2 – November 7th (Friday morning and afternoon)

<table>
<thead>
<tr>
<th>Time</th>
<th>T3: Cutting Edge Tools</th>
<th>T4: Security Guidance and Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>ISWG: Browser Security (Working Session)</td>
<td>Certification (Working Session)</td>
</tr>
<tr>
<td>10:20</td>
<td>Enterprise Security API Project (Working Session)</td>
<td>Awards (Working Session)</td>
</tr>
<tr>
<td>10:40</td>
<td>Tools Projects (Working Session)</td>
<td>OWASP Website (Working Session) [2h]</td>
</tr>
<tr>
<td>11:20</td>
<td>Documentation Projects (Working Session)</td>
<td>Strategic Planning for 2009 (Working Session)</td>
</tr>
<tr>
<td>11:40</td>
<td>OWASP Top 10 2009 (Working Session)</td>
<td>Board Meeting (public session)</td>
</tr>
<tr>
<td>12:00</td>
<td>Intra Governmental Affairs (Working Session)</td>
<td>OWASP Live CD&amp;DVD (Working Session)</td>
</tr>
</tbody>
</table>

**14:00-17:00**

<table>
<thead>
<tr>
<th>Time</th>
<th>Board Meeting</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:00-17:00</td>
<td>Board Meeting</td>
</tr>
</tbody>
</table>
# Business Track Agenda

## Day 1 - November 6th (Thursday)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:45</td>
<td>About OWASP</td>
</tr>
<tr>
<td>11:00</td>
<td>Real World Usage of OWASP Material</td>
</tr>
<tr>
<td>14:00</td>
<td>OWASP Intergovernmental Activities and Compliance</td>
</tr>
<tr>
<td>15:00</td>
<td>Panel: Security Threats Landscape and Future Trends</td>
</tr>
<tr>
<td>16:00</td>
<td>OWASP Projects: Internationalization, Education, Certification and OWASP Books</td>
</tr>
<tr>
<td>19:00</td>
<td>OWASP Gala Dinner</td>
</tr>
</tbody>
</table>

## Day 2 - November 7th (Friday)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>OWASP Projects: ESAPI, ASDR, CLASP, ISWG Browser Security and Web Application Security Framework</td>
</tr>
<tr>
<td>11:00</td>
<td>OWASP Roadmap for 2009</td>
</tr>
<tr>
<td>12:00</td>
<td>Panel: What do you want from OWASP?</td>
</tr>
<tr>
<td>14:00</td>
<td>OWASP Board Meeting over Working Session</td>
</tr>
<tr>
<td>15:00</td>
<td>Panel: Security Threats Landscape and Future Trends</td>
</tr>
<tr>
<td>16:00</td>
<td>What's in our sponsors minds?</td>
</tr>
</tbody>
</table>
Training
OWASP Summit Training Sessions
Portugal, 3\textsuperscript{rd} - 4\textsuperscript{th} Nov 2008

OWASP is bringing together the world's best application security experts to teach you on OWASP tools, methodologies and how to build secure web software. The OWASP creators of tools will bring you up to speed on how to dissect, test, improve and construct secure software. Join us Portugal for the biggest concentration of OWASP training so far.

OWASP & Software Security Courses

<table>
<thead>
<tr>
<th>Monday - November 3</th>
<th>Tuesday - November 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Web Application Security Testing (2 days)</td>
<td>Ajax Security (0.5 day AM)</td>
</tr>
<tr>
<td>Building Secure Web Services (2 days)</td>
<td>How to Win AppSec Hacking Contests and Deploy Better Web Applications (1/2 day - PM)</td>
</tr>
<tr>
<td>Uncovering WebScarab's Secret Treasures (1 day)</td>
<td>Secure Programming with Java (1 day)</td>
</tr>
<tr>
<td>Secure Programming with Java (1 day)</td>
<td>Building Secure Web Applications with OWASP's Enterprise Security API (ESAPI) (1 day)</td>
</tr>
<tr>
<td>Building Secure Web Applications with OWASP's Enterprise Security API (ESAPI) (1 day)</td>
<td>Securing WebGoat with ModSecurity (1/2 day)</td>
</tr>
<tr>
<td>Building Secure Web 2.0 Applications (1 day)</td>
<td>Flash Player Security (1/2 day)</td>
</tr>
<tr>
<td>Web server/services hardening using SELinux (1 day)</td>
<td>Auditing Flash Applications (1/2 day)</td>
</tr>
<tr>
<td>Web Application Assessments (1/2 day)</td>
<td>OWASP Top 10 - What Developers Should Know on Web Application Security (1/2 day)</td>
</tr>
<tr>
<td>Hacking OWASP Orizon Project v1.0 (1/2 day)</td>
<td>OWASP Testing Guide (1/2 day)</td>
</tr>
<tr>
<td>Classic ASP Security using OWASP tools (1 day)</td>
<td></td>
</tr>
</tbody>
</table>
Web server/services hardening using SELinux

Instructor: Pavol Luptak
Duration: 1 day

Summary: Security-Enhanced Linux (SELinux) is a FLASK implementation integrated in the Linux kernel with a number of utilities designed to provide mandatory access controls (MAC) through the use of Linux Security Modules (LSM) in the Linux kernel. SELinux generally supports many kinds of mandatory access control policies, including those based on the concepts of type enforcement, role-based access control, and multi-level security. This training provides basic concepts of SELinux, its differences to classical UNIX/Linux systems, describe security advantages of mandatory access control policies and teach how to effectively and rapidly configure a fully functional LAMP environment on SELinux system.

Secure Programming with Java

Instructor: Lucas C. Ferreira
Duration: 1 Day

Summary: This training class will present best practices of secure programming in the Java language. It includes Java specific practices (i.e. how to avoid problems that arise from the compilation of Java source code to the bytecode language used by the JVM) and practices that may arise in other programming languages (with examples in Java). Some tools that may be used to verify the security of Java code and systems will be shown.

OWASP Top 10 - What Developers Should Know on Web Application Security

Instructor: Sebastien Deleersnyder and Martin Knobloch
Duration: 4 h To be scheduled on Tuesday.

Summary: Application security is an essential component of any successful project; this includes web applications, open source PHP applications, web services and proprietary business web sites. Web application security education and awareness is needed throughout the entire development and deployment organization. Each area and level of development or deployment organizations have specific needs and requirements regarding web application security education. This Education Track provides in a 4 hour session covering what developers should know on web application security. It starts with an explanation of web application security and why it is important. Then the OWASP Top 10 is used to explain the nastiest vulnerabilities and how these can be prevented or remedied.

Classic ASP Security using OWASP tools

Instructor: Juan Carlos Calderon
Duration: 1 day

Summary: Classic ASP 2.0 and 3.0 applications are still largely used as this technology is more than 10 years old and was largely used. There are thousands of
sites on the wild that need guidance on the security arena. This is where OWASP can come up and provide help for “making the Web a better place”.

**Web Application Assessments**

*Instructor:* Vicente Aguilera Diaz  
*Duration:* 4h  
*Summary:* As in the physical world, the "professionals" attackers spend most of their time to analysing its objective and try to gather as much information as possible about it. The more information becomes available and is more detailed and accurate, the attack is more likely to succeed. The aim of this course is to identify patterns and tools to perform this analysis (step prior to the attack), and is supplemented by a case study on a practical application.

**Hacking Owasp Orizon Project v1.0**

*Instructor:* Paolo Perego  
*Duration:* 4h  
*Summary:* In the course it will be presented Owasp Orizon v1.0 framework. The major APIs will be fully explained and it will be built a simple scanning tool using the Orizon framework. The course goal is to let people fully understand Orizon internals and let people understand how to use the framework in a real world.

**Securing WebGoat with ModSecurity**

*Instructor:* Stephen Craig Evans  
*Duration:* 4h  
*Summary:* ModSecurity, normally a tool of the network security group, has capabilities that can allow a software security specialist with programming skills to mitigate business logic flaws and other vulnerabilities that are out-of-reach of basic blacklists.

**How to Win AppSec Hacking Contests and Deploy Better Web Applications**

*Instructors:* Lann Martin and Lebbeous Fogle-Weekley - winners of the CTF contest at OWASP AppSec NYC ’08  
*Duration:* 4 hours  
*Summary:* This class will demonstrate how an attacker approaches potentially vulnerable web applications, taking advantage of both poor server configuration and poor application implementation to discover and exploit vulnerabilities of several types.

**Uncovering WebScarab's Secret Treasures**

*Instructor:* Rogan Dawes  
*Duration:* 1 day
Summary: OWASP WebScarab has a lot of hidden features that probably no one but the author really knows about. This in depth hands on session will show delegates how to access these features, and how to use them to their full potential.

Advanced Web Application Security Testing

Instructor: Michael Coates, Aspect Security
Duration: 2 days.

Summary: While all developers need to know the basics of web application security testing, application security specialists will want to know all the advanced techniques for finding and diagnosing security problems in applications. Aspect’s Advanced Web Application Security Testing training is based on a decade of work verifying the security of critical applications. The course is taught by an experienced application security practitioner in an interactive manner.

Building Secure Web 2.0 Applications

Instructor: Arshan Dabirsiaghi, Aspect Security
Duration: 1 day

Summary: Web 2.0 applications using technologies like Ajax, Flash, ActiveX, and Java Applets require special attention to secure. this one day training addresses the special issues that arise in this type of application development.

Building Secure Web Services

Instructor: Dave Wichers, Aspect Security
Duration: 2 days.

Summary: The movement towards Web Services and Service Oriented architecture (SOA) paradigms requires new security paradigms to deal with new risks posed by these architectures. this session takes a pragmatic approach towards identifying Web Services security risks and selecting and applying countermeasures to the application, code, web servers, databases, application, and identify servers and related software. Many enterprises are currently developing new Web Services and/or adding and acquiring Web Services functionality into existing applications -- now is the time to build security into the system.

Building Secure Web Applications with OWASP's Enterprise Security API (ESAPI)

Instructor: Jeff Williams, Aspect Security
Duration: 1 day.

Summary: This course will teach you about OWASP’s new Enterprise Security API (ESAPI), what it is composed of, and how to use it to improve the security and reduce the cost of developing those applications. This class covers each interface within the API, how it is intended to be used, and what the benefits are of using this interface, over other techniques for addressing the same security concerns.
The course also discusses how to bring ESAPI into your organization and how to tailor it for your organization specific needs and application infrastructure.

**Ajax Security**

**Instructor:** Brad Causey  
**Duration:** 1 day  
**Summary:** This course will provide an introductory to AJAX, its inherent security issues, how to detect them, and how to resolve them.

**Flash Player Security**

**Instructor:** Peleus Uhley  
**Duration:** 1/2 day  
**Summary:** This course will provide an overview of the Flash Player security model and common architectures for Flash deployment. The course is targeted at people who need to understand the fundamentals of Flash Player security and how it will affect their website such as CSOs, web designers and web architects. The goal of the course is to provide the student with the enough information to architect a secure Flash deployment. The follow-on Auditing Flash Applications course will continue to build on this knowledge on an API by API level.

**Auditing Flash Applications**

**Instructor:** Peleus Uhley  
**Duration:** 1/2 day  
**Summary:** This course is a follow on to the Flash Player Security course for those who want to do a deep dive into the security of Flash applications. This course is targeted at Flash authors and web-site auditors who need to validate Flash code and provide meaningful recommendations and best practices for improving Flash deployments. The goal of the course is to provide the student with the tools and information to audit a Flash website and provide quality feedback on how to remediate any issues.

**Testing Guide Training**

**Instructor:** Matteo Meucci, Giorgio Fedon - Minded Security.  
**Duration:** 4h  
**Summary:** This course will discuss the new OWASP Testing Guide v3 methodology and the most relevant tests of the 66 total controls of the Guide. You can learn how to test a web application and how to write a report.
OWASP EU Summit
Portugal

Sponsorship
OWASP Summit Sponsorship

Portugal, 3rd - 7th Nov 2008

The EU Summit 2008 OWASP Conference is the premier gathering of Information Security leaders. Executives from Fortune 500 firms along with technical thought leaders such as security architects and lead developers will be traveling to hear the cutting-edge ideas presented by Information Security's top talent. OWASP events attract a worldwide audience interested in “what’s next”. As an OWASP Conference sponsor, your brand will be included as an answer.

OWASP is providing sponsors exclusive access to its audience in Faro through a limited number of Expo floor slots, providing a focused setting for potential customers. Attendees will be pushed through the Expo floor for breakfast, lunch and coffee breaks. The conference is expected to draw over 350 attendees, including 100 OWASP project leaders financed by OWASP Foundation, who will be looking for ways to spend the rest of their 2008 budget and planning for 2009.

Sponsorship opportunities are filling up rapidly. All proceeds from sponsorship support the conference and the mission of the OWASP Foundation (501c3 Not-For-Profit). Supporting these events drives the funding for research grants, tools and documents, local chapters, and more.

Contact us today or visit https://www.owasp.org/index.php/OWASP_EU_Summit_2008

OWASP Contacts

Kate Hartmann
OWASP Operations Director
9175 Guilford Road, Suite 300
Columbia, MD 21046, USA
Phone: 301-575-0189
Facsimile: 301-604-8033
Email: kate.hartmann@owasp.org

Eduardo Vianna de Camargo Neves
OWASP EU Summit Organization Committee
Rua Conselheiro Laurindo 600, 15º Floor
Curitiba, PR, 80060-903, Brazil
Phone: +55 (41) 3075-3080
Email: eduardo.neves@owasp.org
Items available for sponsorship

As a sponsor you can purchase any of the following items individually:

- **OWASP Leader Trip** - €1,000 - Cost of bringing an OWASP Leader to the Summit
- **VIP Pass** - €1,500 - Training, Summit, and Accommodation for 1 person
- **Vendor Expo** - €2,500
- **Lunch** - €5,000 (5 slots available)
- **Dinner** - €5,000 (3 slots available)
- **Coffee Breaks** - €1,250 (10 slots available)
- **Special Dinner and Party** - TBD

Sponsorship packages

The following table shows 3 different sponsorship packages OWASP is offering for this particular Summit.

<table>
<thead>
<tr>
<th>Contents</th>
<th>Total value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platinum</strong></td>
<td></td>
</tr>
<tr>
<td>10x OWASP Leader Trip €10,000</td>
<td></td>
</tr>
<tr>
<td>10x VIP Passes - €15,000</td>
<td></td>
</tr>
<tr>
<td>1x Vendor Expo €2,500</td>
<td>€35,000</td>
</tr>
<tr>
<td>1x Lunch : €5,000</td>
<td></td>
</tr>
<tr>
<td>2x Coffee break: €2,500</td>
<td></td>
</tr>
<tr>
<td><strong>Gold</strong></td>
<td></td>
</tr>
<tr>
<td>5x OWASP Leader Trip €5,000</td>
<td>€15,000</td>
</tr>
<tr>
<td>5x VIP Passes €7,500</td>
<td></td>
</tr>
<tr>
<td>1x Vendor Expo €2,500</td>
<td>€12,000 for OCM</td>
</tr>
<tr>
<td><strong>Silver</strong></td>
<td></td>
</tr>
<tr>
<td>2x OWASP Leader Trip €2,000</td>
<td>€5,000</td>
</tr>
<tr>
<td>2x VIP Passes €3,000</td>
<td>€4,000 for OCM</td>
</tr>
</tbody>
</table>

OCM = OWASP Corporate Members
For Platinum, Gold and Silver sponsorship packages, we are adopting a distribution/allocation model based on the type of sponsorship for:

- Placement of company logo on every direct mail pieces and Summit proceedings
- Company logo placed on OWASP Web Site as Summit Sponsor
- Company description included in every pre-Summit brochures
- Your company’s banner placed in one high traffic area of the Summit
- Your company’s literature placed in every attendee bag

Frequently Asked Questions

**Audience: Who is the target of the Summit?**
Application Developers, Managers and Decision-makers, OWASP Members and Leaders.

**Is it possible to know which are the others sponsors?**
Yes, their logos will be published in the website and all printed materials.

**Which is the difference between OWASP NYC and OWASP Summit in Portugal**
OWASP Summit is a worldwide gathering of OWASP leaders and Key Industry Players to:

- Present and discuss the latest OWASP Season of Code results, tools and documentation projects
- Use Working Sessions to improve collaboration and achieve specific goals
- Define roadmaps for OWASP projects, chapters and OWASP itself
- Integrate Business audience to OWASP management and strategic initiatives
OWASP – Open Web Application Security Project

- Open source non-profit charitable foundation dedicated to enabling organizations so they can develop, maintain, and acquire software they can trust

- **Making Security Visible**, through...
  - Documentation
  - Tools
    - WebGoat, WebScarab, Site Generator, Report Generator, ESAPI, CSRF Guard, CSRF Tester, Stinger, Pantera, ...
  - Working Groups
  - Security Community and Awareness
    - Local Chapters, Conferences, Tutorials, Mailing Lists
changing the software market
commercial products or services
zero-day exploits

OWASP Main Site Traffic

Worldwide Users

Most New Visitors

Monthly Downloads (GB)

5,022,937 Pageviews

OWASP Conferences

Participants

OWASP Community

Participants
OWASP KnowledgeBase

- 3,913 total articles
- 427 presentations
- 200 updates per day
- 179 mailing lists
- 180 blogs monitored
- 31 doc projects
- 19 deface attempts
- 12 grants

OWASP Tools and Technology

- Vulnerability Scanners
- Static Analysis Tools
- Fuzzing
  Automated Security Verification

- Penetration Testing Tools
- Code Review Tools
  Manual Security Verification

- ESAPI
  Security Architecture

- AppSec Libraries
- ESAPI Reference Implementation
- Guards and Filters
  Secure Coding

- Reporting Tools
- AppSec Management
  AppSec Education

- Flawed Apps
- Learning Environments
- Live CD
- SiteGenerator
# 10 Projects you should know about

<table>
<thead>
<tr>
<th>Project</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - Cross Site Scripting (XSS)</td>
<td>XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.</td>
</tr>
<tr>
<td>A2 - Injection Flaws</td>
<td>Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker’s hostile data tricks the interpreter into executing unintended commands or accessing data that it should not.</td>
</tr>
<tr>
<td>A3 - Malicious File Execution</td>
<td>Code-vulnerable remote file inclusion (RIF) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML, and any framework which accepts filenames or files from users.</td>
</tr>
<tr>
<td>A4 - Insufficient Direct Object Reference</td>
<td>A direct object reference flaw occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.</td>
</tr>
<tr>
<td>A5 - Cross-Site Request Forgery (CSRF)</td>
<td>A CSRF attack forces a logged-in victim’s browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim’s browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.</td>
</tr>
<tr>
<td>A6 - Information Leakage and Improper Error Handling</td>
<td>Applications can unintentionally leak information about their configuration, internal workings, or validate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.</td>
</tr>
<tr>
<td>A7 - Broken Authentication and Session Management</td>
<td>Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users’ identities.</td>
</tr>
<tr>
<td>A8 - Insufficient Cryptographic Storage</td>
<td>Web applications need use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.</td>
</tr>
<tr>
<td>A9 - Insufficient Communications</td>
<td>Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.</td>
</tr>
<tr>
<td>A10 - Failure to Restrict URL Access</td>
<td>Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.</td>
</tr>
</tbody>
</table>

Table 1: Top 10 Web application vulnerabilities for 2007
OWASP Secure Software Contract Annex

The initial project is a Secure Software Contract Annex that helps software buyers and vendors discuss security and capture the important terms of the contract. This project should not be considered legal advice, and we strongly recommend that you find competent counsel to assist with your contract negotiations. The contract annexes have been placed in the public domain to facilitate use in private contracts.

- OWASP Secure Software Contract Annex
- Secure software contracting hypothetical case study

You can download the Microsoft Word version Image:OWASP Secure Software Contract Annex.doc and modify it to suit your needs. Please consider contributing back any enhancements you make.

4) Code Review (Beta Quality)

Preface

This document is not a "How to perform a Secure Code review" walk-through but more a guide on how to perform a successful review. Knowing the mechanics of a code inspection is half the battle but I'm afraid people are still the other half.

A proper code reviewer will not only identify vulnerabilities, but will assess which vulnerabilities are at the greatest risk for exploitation.

This document describes how to make the most of a secure code review..
5) EASPI (Beta Quality)

The EASPI is a free and open collection of all the security methods that a developer needs to build a secure web application. You can use the interface and build your own implementation using your company's infrastructure. Or, you can use the reference implementation as a starting point. In concept, the API is language independent. However, the first deliverables from the project are a Java API and a Java reference implementation. Efforts to build EASPI in .NET and PHP are already underway.

Unfortunately, the available platforms, frameworks, and toolkits (Java EE, Struts, Spring, etc.) simply do not provide enough protection. This leaves developers with responsibility for designing and building security mechanisms. This means that the entire line of every application leads to wasted time and massive security holes.

The cost savings through reduced development time and the increased security due to using heavily analyzed and carefully designed security methods provide developers with a massive advantage over organizations that are trying to deal with security using existing ad hoc secure coding techniques. This API is designed to automatically take care of many aspects of application security, making these issues invisible to the developers.

---

7) Web Goat (Release Quality)

WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons. In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat application. For example, in one of the lessons the user must use SQL injection to steal fake credit card numbers. The application is a realistic teaching environment, providing users with hints and code to further explain the lesson.

Why the name “WebGoat”? Developers should not feel bad about not knowing security. Even the best programmers make security errors. What they need is a scapegoat, right? Just blame it on the “Goat”.

To get started, read the WebGoat User and Install Guide.

Goals

Web application security is difficult to learn and practice. Not many people have full blown web applications like online book stores or online banks that can be used to scan for vulnerabilities. In addition, security professionals frequently need to test tools against a platform known to be vulnerable to ensure that they perform as advertised. All of these needs happen in a real and legal environment. Even if your intentions are good, we believe you should never attempt to find vulnerabilities without permission.

The primary goal of the WebGoat project is simple: create a defacto interactive teaching environment for web application security. In the future, the project team hopes to extend WebGoat into becoming a security benchmarking platform and a Java-based Web site HoneyPot.
9) WebScarab (Release Quality)

Welcome to the WebScarab Project

WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. It is written in Java, and is thus portable to many platforms. WebScarab has several modes of operation, implemented by a number of plugins. Its most common use, WebScarab operates as an intercepting proxy, allowing the operator to review and modify requests created by the browser before they are sent to the server, and to view and modify responses returned from the server before they are received by the browser. WebScarab is able to intercept both HTTP and HTTPS communication. The operator can also review the conversations (requests and responses) that have ensued through WebScarab.

OotM Marketplace

Current demand

Add your demand here:
- Helsinki is looking for OWASP speakers on the SDLC topic for a mini-conference. Expected timing is sometime in May. Sponsors and potential speakers are requested to contact Antti.
- Edmonton is looking for an OWASP speaker on any topic to coincide with the CPS Edmonton ICE Conference[1]. The talk would be during November 5-7, 2007. Looking for a quick reply if possible as we are trying to finalise the conference program very shorty. Keynotes at the conference include Bruce Schneier and Jim Christy, so this could be a great opportunity to showcase OWASP to an interested audience.
- Rochester is looking for an OWASP speaker for the Rochester Security Summit on October 30, 2008.

Current offerings

If you want to offer an OWASP related presentation, propose them here with your availability boundaries (time/ geographical)
- Marcella Barbey will happily talk about the WebAppSec industry, SDL etc around Europe. You can see him in action at HITB with John Viega (big download)
- Paolo Pongiglo is available to talk about Siteon project, safe coding and code review issues around Europe in the near October-December
- Marco Morana is available to talk about Software Security Framework and Secure Code Reviews see Cost conference as reference in USA around November-December and in Europe around January-February.
- Sébastien Genia is available to talk about WebAppSec, educational purpose on AppSec in French or at least in english around France/Europe/Canada from middle of March 08. You can find some talk on the Owasp France Chapter
- y?

Upcoming OWASP on the Move Events

- October 30, 2008 - Rochester Marco Morana will speak at Rochester Security Summit about Software Security Framework
OWASP’s grant / sponsorship model

- 100% of OWASP membership fees are used to sponsor innovative research projects.
- So far 3 “season of code” sponsored by OWASP.
  - **OWASP Autumn Of Code 2006**
    - $20,000 budget
  - **OWASP Spring Of Code 2007**
    - $117,500 budget
  - **OWASP Summer of Code 2008**
    - $126,000 budget

### OWASP Summer of Code 2008

- 31 grants to promising application security researchers as part of the **OWASP Summer of Code 2008**.

<table>
<thead>
<tr>
<th>Application</th>
<th>Applicant’s Name</th>
<th>Assessment Selection</th>
<th>Sponsorship</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP Code review guide, v1.1</td>
<td>Eric Hively</td>
<td>By Vote</td>
<td>$5,000 USD</td>
</tr>
<tr>
<td>OWASP Best Practices Guide</td>
<td>Mark Madsen</td>
<td>By Vote</td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP UML Component Verification Project (a.k.a. OWASP JUnit Testing Tool)</td>
<td>James Lee</td>
<td>By Vote</td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP Application Security Guide Reference, v1.0</td>
<td>Juan Carlos Calderon</td>
<td></td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP .NET Project Leadership</td>
<td>Matthew Vincini</td>
<td></td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP Education Project</td>
<td>Robert Knoblock</td>
<td></td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP Testing Guide</td>
<td>William McIlvain</td>
<td></td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP Application Security Verification Standard</td>
<td>Mike Dobkins</td>
<td></td>
<td>$1,250 USD</td>
</tr>
<tr>
<td>OWASP Online code signing and integrity verification service for open source community</td>
<td>Phil Pindell and Richard Conway</td>
<td></td>
<td>$2,500 USD</td>
</tr>
<tr>
<td>OWASP Best Practices for Web Security</td>
<td>Stephen Everet</td>
<td></td>
<td>$2,500 USD</td>
</tr>
<tr>
<td>OWASP Site Cover &amp; Home Design</td>
<td>Lillian Lasara</td>
<td></td>
<td>$2,500 USD</td>
</tr>
<tr>
<td>OWASP Individual &amp; Corporate Member Patches, Conference Attendee Patches Brief</td>
<td>Lillian Lasara</td>
<td></td>
<td>$2,500 USD</td>
</tr>
</tbody>
</table>

And many more!!!
OWASP Structure

- OWASP Board
- OWASP leaders (Tools, Chapters & Working Groups)
- OWASP Members
- Subscribers to mailing lists
- Anonymous consumers

OWASP Employees

- Alison McNamee - Admin and Accounts (2 days week)
- Paulo Coimbra - Owasp Projects & Summer of Code Management
- Kate Hartmann - Operations manager

These are the only ones directly paid by OWASP, apart from Seasons of Code sponsorships no Board Member, Project leader or chapter leader is paid.
**OWASP Membership**

- Members have the ability to allocate their membership fees to projects, working groups or chapters they are interested in.
- Members will have the ability to vote on specific OWASP governance issues (Tom to figure this out).
- Membership makes a public statement of support to OWASP.

**Very important: There is no ‘member-only content’**

Apart from the (under construction) OWASP Member packs, there is NOTHING that an member gets that it doesn't already have (i.e. all OWASP materials and participation are available to everybody (members and non members)).
Benefits of Membership

<table>
<thead>
<tr>
<th>Annual Membership Fee</th>
<th>$100 USD</th>
<th>$250 USD</th>
<th>$500 USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (1-100) - $2,000 USD *</td>
<td>Large (101) - $7,000 USD *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Small (101) - $3,000 USD *</td>
<td>Large (101) - $6,000 USD *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$0.00 USD *</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Benefits that also apply to all OWASP participants (even non-members):
1. Active role in the development of OWASP Materials that are being widely accepted as an application security standard by all organizations.
2. Early electronic notification of updates to the OWASP Materials.
3. Collaboration with other highly skilled people from organizations around the world, both virtually and in person during periodic OWASP conferences and chapter meetings.
4. Authorization to create an account and edit pages on the www.owasp.org website (Wiki based)
5. Network with your technical peers on LinkedIn (OWASP Group Membership)

Please Help OWASP Grow

- Push us to do better!

- Be an active contributor
  - OWASP Chapter Leaders
  - OWASP Project Leaders, Participants and Reviewer
  - OWASP Conference Committee
  - Stub articles – wiki contributions
  - New technologies to analyze

- Be an OWASP members
  - Corporate Members
  - Individual Members

- Please join us and share what you know!