

**OWASP**  
**EU Summit**  
**Portugal**

# Summit Overview



# OWASP Summit Overview

Portugal, 3<sup>rd</sup> - 7<sup>th</sup> 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.

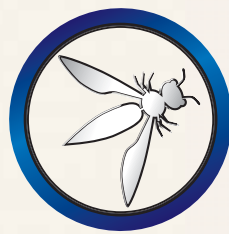
Containing both technical and business tracks, the Summit is the perfect place to learn what resources OWASP has available for use today.

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](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](mailto:kate.hartmann@owasp.org))



OWASP  
EU Summit  
Portugal

Working Sessions







# OWASP Summit Working Sessions

Portugal, 4<sup>rd</sup> - 5<sup>th</sup> Nov 2008

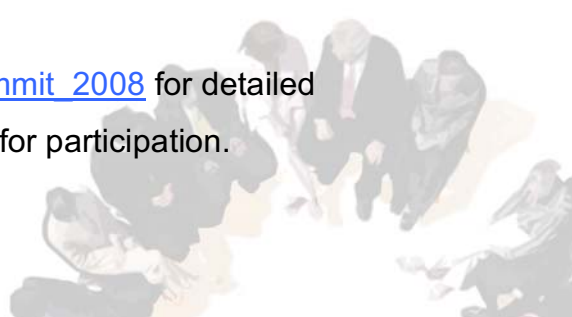
OWASP is bringing together its Leaders with the world's best application security experts to meet at the OWASP Summit in order to work on targeted Working Sessions

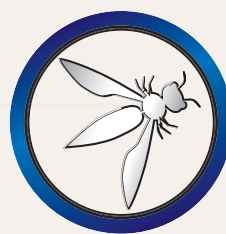
Everyone who attends is invited to join, share opinions and make the difference. All outcomes produced during the working session will be presented during the Summit's conference and discussed at a special OWASP Board meeting who will vote on the proposed Initiatives, Statements or Decisions.

The following OWASP specific Working Sessions are currently scheduled

| Tuesday, November 4                         | Wednesday, November 5                       |
|---|---|
| OWASP Strategic Planning for 2009 - 3h      | OWASP Top 10 2009 - 3h                      |
| OWASP Tools Projects - 3h                   | OWASP Education Project - 2h                |
| ISWG: Browser Security - 7h                 | OWASP Enterprise Security API Project - 4h  |
| OWASP Documentation Projects - 3h           | OWASP Code Review Guide 2009 - 2h           |
| OWASP Winter Of Code 2009 - 4h              | OWASP Testing Guide Next Version - 2h       |
| OWASP .NET Project - 2h                     | OWASP Certification - 2h                    |
| 2-way Internationalization of OWASP - 2h    | App Security Desk Reference (ASDR) - 4h     |
| A.R.C.A. : Metrics and Vulnerabilities - 2h | OWASP Intra Governmental Affairs - 2h       |
|   | OWASP Awards - 2h                           |
|   | OWASP Website - 2h                          |
|   | ISWG: Web App Framework Security - 4h       |
|   | OWASP Live CD&DVD - 2h                      |
|   | Best Practices for OWASP Chapter Leaders 2h |

See [https://www.owasp.org/index.php/OWASP\\_EU\\_Summit\\_2008](https://www.owasp.org/index.php/OWASP_EU_Summit_2008) for detailed information about each Working Session and to register for participation.





OWASP  
EU Summit  
Portugal

Conference



# OWASP Summit Conference

Portugal, 6<sup>th</sup> - 7<sup>th</sup> 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 6<sup>th</sup> (Thursday morning)

|       |             |
|-------|-------------|
| 09:00 | KeyNote     |
| 09:45 | About OWASP |

|       | T1: Secure Design & Defensive Strategies   | T2: OWASP Internals  |
|-------|--|--|
| 10:40 | OWASP Enigform and mod_Openpgp (SoC 08)<br><i>Arturo Alberto Busleiman (a.k.a Buanzo)</i>                      | OWASP Internationalization Guidelines (SoC 08)<br><i>Juan Carlos Calderon</i>              |
| 11:00 | OWASP OpenSign Server Project (SoC 08)<br><i>Phil Potisk, Richard Conway - pending or Mark Roxberry</i>        | OWASP Spanish Project (SoC 08)<br><i>Juan Carlos Calderon</i>                              |
| 11:20 | OWASP AntiSamy (SoC 08)<br><i>Arshan Dabirsiaghi</i>   | OWASP Positive Security (SoC 08)<br><i>Eduardo Vianna de Camargo Neves</i>                 |
| 11:40 | OWASP AppSensor (SoC 08)<br><i>Michael Coates</i>  | OWASP Source Code Review OWASP Projects (SoC 08)<br><i>James Walden</i>                    |
| 12:00 | OWASP Securing WebGoat using ModSecurity (SoC 08)<br><i>Stephen Craig Evans, Christian Folini</i>              |  |
| 12:20 | OWASP Book Cover & Sleeve Design, OWASP Individual & Corporate Member Packs (SoC 08)<br><i>Deb, LX Studios</i> | OWASP Education (SoC 08 Working Session)<br><i>Sebastien Deleersnyder, Martin Knobloch</i> |



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

|       | T3: Cutting Edge Tools   | T4: Security Guidance and Knowledge  |
|-------|--|--|
| 14:00 | OWASP Access Control Rules Tester Project (SoC 08)<br><i>Andrew Petukhov</i>   | OWASP Classic ASP Security Project (SoC 08)<br><i>Juan Carlos Calderon</i>   |
| 14:20 | OWASP Skavenger Project (SoC 08)<br><i>Matthias Rohr</i>   | OWASP .NET Project (SoC 08 & Working Session)<br><i>Mark Roxberry</i>  |
| 14:40 | OWASP JSP Testing Tool (SoC 08)<br><i>Jason Li</i>   |  |
| 15:00 | WebScarab-NG (SoC 08)<br><i>Rogan Dawes</i>  | OWASP SQL Injector Benchmarking Project (SoC 08)<br><i>Kevin Fuller</i>  |
| 15:20 | OWASP Pantera (SoC 08)<br><i>Simon Roses Femerling</i>   | OWASP Code Review Guide (SoC 08 & Working Session)<br><i>Eoin Keary</i>  |
| 15:40 | OWASP Live CD 2008 (SoC 08)<br><i>Matt Tesauro</i>   |  |
| 16:00 | OWASP Teachable Static Analysis Workbench (SoC 08)<br><i>Dmitry Kozlov</i>   | OWASP Backend Security Project (SoC 08)<br><i>Carlo Pelliccioni</i>  |
| 16:20 | TDB  | OWASP Application Security Desk Reference (ASDR) (SoC 08 & Working Session)<br><i>Leonardo Cavallari Militelli</i> |
| 16:40 | OWASP Orizon Project (SoC 08)<br><i>Paolo Perego (aka thesp0nge)</i>   |  |
| 17:00 | OWASP Application Security Tool Benchmarking Environment and Site Generator Refresh Project (SoC 08)<br><i>Dmitry Kozlov</i> | OWASP Ruby on Rails Security Project (SoC 08)<br><i>Heiko Webers</i>   |
| 17:20 | TBD  |  |
| 17:40 | OWASP Application Security Verification Standard Project<br><i>Jeff Williams</i>   | OWASP Testing Guide (SoC 08 & Working Session)<br><i>Matteo Meucci</i>   |
| 19:00 | OWASP Gala Dinner  |  |



## Day 2 – November 7<sup>th</sup> (Friday morning and afternoon)

|             | T3: Cutting Edge Tools                                    | T4: Security Guidance and Knowledge           |
|-------------|---|---|
| 10:00       | ISWG: Browser Security (Working Session)                  | Certification (Working Session)               |
| 10:20       | Enterprise Security API Project (Working Session)         | Awards (Working Session)                      |
| 10:40       | Tools Projects (Working Session)                          | OWASP Website (Working Session) [2h]          |
| 11:00       | ISWG:Web Application Framework Security (Working Session) | Winter Of Code 2009 (Working Session)         |
| 11:20       | Documentation Projects (Working Session)                  | Strategic Planning for 2009 (Working Session) |
| 11:40       | OWASP Top 10 2009 (Working Session)                       | Board Meeting (public session)                |
| 12:00       | Intra Governmental Affairs (Working Session)              | OWASP Live CD&DVD (Working Session)           |
| 14:00-17:00 | Board Meeting   |   |



# Business Track Agenda

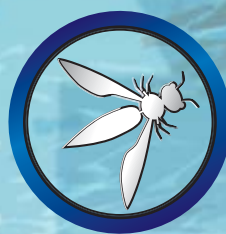
## Day 1 - November 6<sup>th</sup> (Thursday)

|       |  |
|-------|--|
| 09:45 | About OWASP  |
| 11:00 | Real World Usage of OWASP Material   |
| 12:00 | OWASP Projects: Top 10, Legal Contract, Testing Guide, Developer Guide, Code Review, Webgoat |
| 14:00 | OWASP Intergovernmental Activities and Compliance  |
| 15:00 | Panel: Security Threats Landscape and Future Trends  |
| 16:00 | OWASP Projects: Internationalization, Education, Certification and OWASP Books               |
| 19:00 | OWASP Gala Dinner  |

## Day 2 - November 7<sup>th</sup> (Friday)

|       |  |
|-------|--|
| 10:00 | OWASP Projects: ESAPI, ASDR, CLASP, ISWG Browser Security and Web Application Security Framework |
| 11:00 | OWASP Roadmap for 2009   |
| 12:00 | Panel: What do you want from OWASP?  |
| 14:00 | OWASP Board Meeting over Working Session   |
| 15:00 | Panel: Security Threats Landscape and Future Trends  |
| 16:00 | What's in our sponsors minds?  |





8

OWASP  
EU Summit  
Portugal

Training



# OWASP Summit Training Sessions

Portugal, 3<sup>rd</sup> - 4<sup>th</sup> 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

| Monday - November 3   | Tuesday - November 4   |
|---|--|
| Advanced Web Application Security Testing (2 days)                                    |  |
| Building Secure Web Services (2 days)   |  |
| Uncovering WebScarab's Secret Treasures (1 day)                                       | Ajax Security (0,5 day AM)   |
| Secure Programming with Java (1 day)  | How to Win AppSec Hacking Contests and Deploy Better Web Applications (1/2 day - PM) |
| Building Secure Web Applications with OWASP's Enterprise Security API (ESAPI) (1 day) | Securing WebGoat with ModSecurity (1/2 day)  |
| Building Secure Web 2.0 Applications (1 day)  | Flash Player Security (1/2 day)  |
| Web server/services hardening using SELinux (1 day)                                   | Auditing Flash Applications (1/2 day)  |
| Web Application Assessments (1/2 day)   | OWASP Top 10 - What Developers Should Know on Web Application Security (1/2 day)     |
| Hacking OWASP Orizon Project v1.0 (1/2 day)   | OWASP Testing Guide (1/2 day)  |
| Classic ASP Security using OWASP tools (1 day)  |  |



## **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 re mediated.

## **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, 3<sup>rd</sup> - 7<sup>th</sup> 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](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](mailto: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](mailto: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.

|                 | Contents                        | Total value     |
|-----------------|---------------------------------|-----------------|
| <b>Platinum</b> | • 10x OWASP Leader Trip €10,000 |                 |
|                 | • 10x VIP Passes - €15,000      | €35,000         |
|                 | • 1x Vendor Expo €2,500         |                 |
|                 | • 1x Lunch : €5,000             | €28,000 for OCM |
|                 | • 2x Coffee break: €2,500       |                 |
| <b>Gold</b>     | • 5x OWASP Leader Trip €5,000   | €15,000         |
|                 | • 5x VIP Passes €7,500          |                 |
|                 | • 1x Vendor Expo €2,500         | €12,000 for OCM |
| <b>Silver</b>   |                                 | €5,000          |
|                 | • 2x OWASP Leader Trip €2,000   |                 |
|                 | • 2x VIP Passes €3,000          | €4,000 for OCM  |

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.

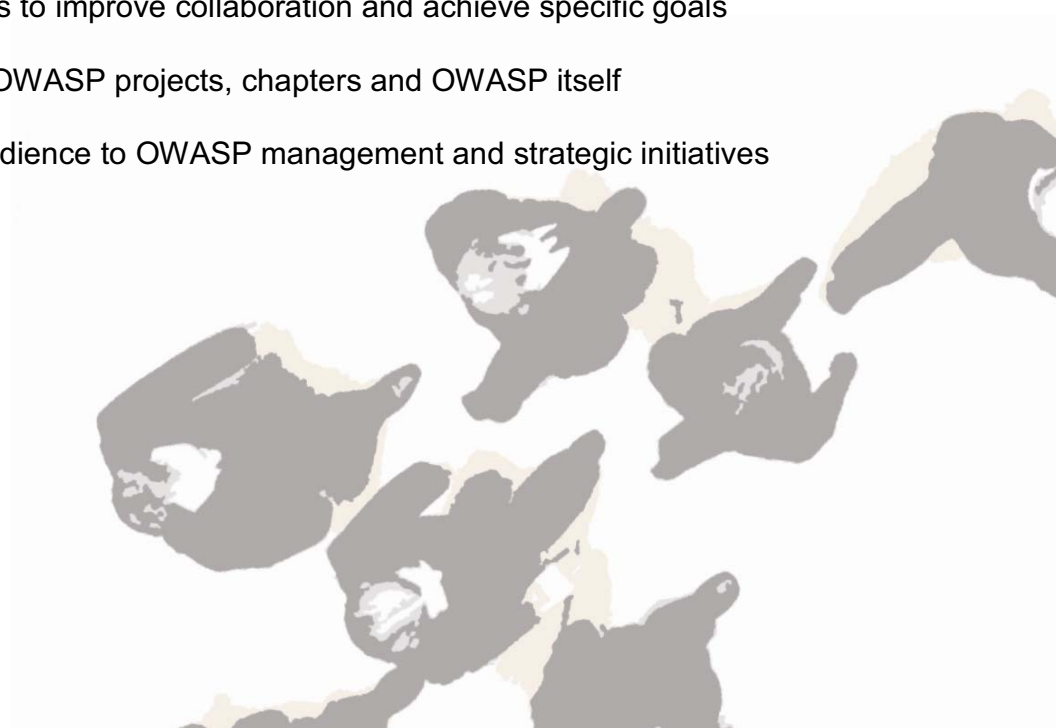
### **Is it possible to know which are the others sponsors?**

Yes, their logos will be published in the website and all printed materials.

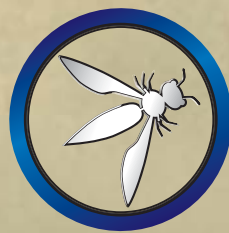
### **Which is the difference between OWASP NYC and OWASP Summit in Portugal**

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**  
**EU Summit**  
Portugal

# OWASP's World



## 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
  - Top Ten, Dev. Guide, Design Guide, Testing Guide, ...
- ▶ Tools
  - WebGoat, WebScarab, Site Generator, Report Generator, ESAPI, CSRF Guard, CSRF Tester, Stinger, Pantera, ...
- ▶ Working Groups
  - Browser Security, Industry Sectors, Access Control (XACML), Education, Mobile Phone Security, Preventive Security, OWASP SDL, OWASP Governance, RIA
- ▶ SecurityCommunity and Awareness
  - Local Chapters, Conferences, Tutorials, Mailing Lists

# WASP?



changing the software market  
commercial products or services  
-day exploits

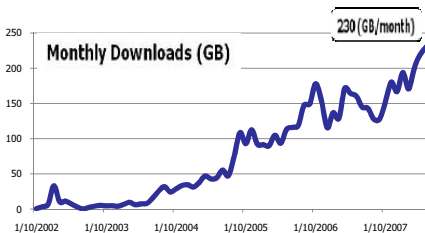


# OWASP Main Site Traffic

Worldwide Users



Most New Visitors

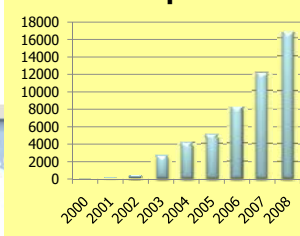


5,022,937 Pageviews

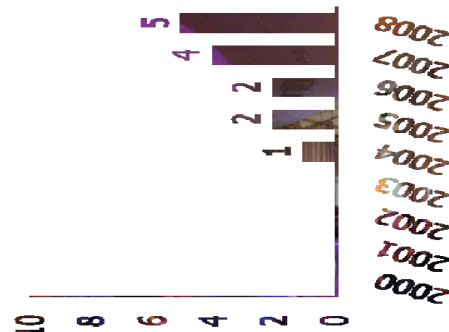
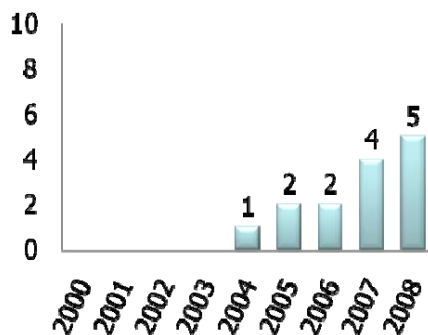


# Community

Participants



# OWASP Conferences





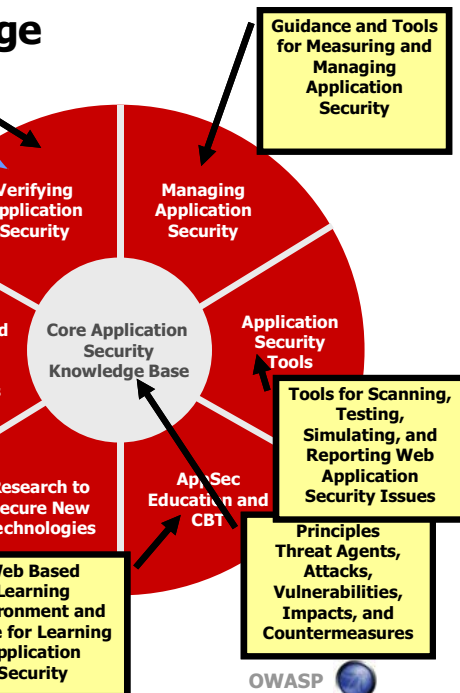


## OWASP KnowledgeBase

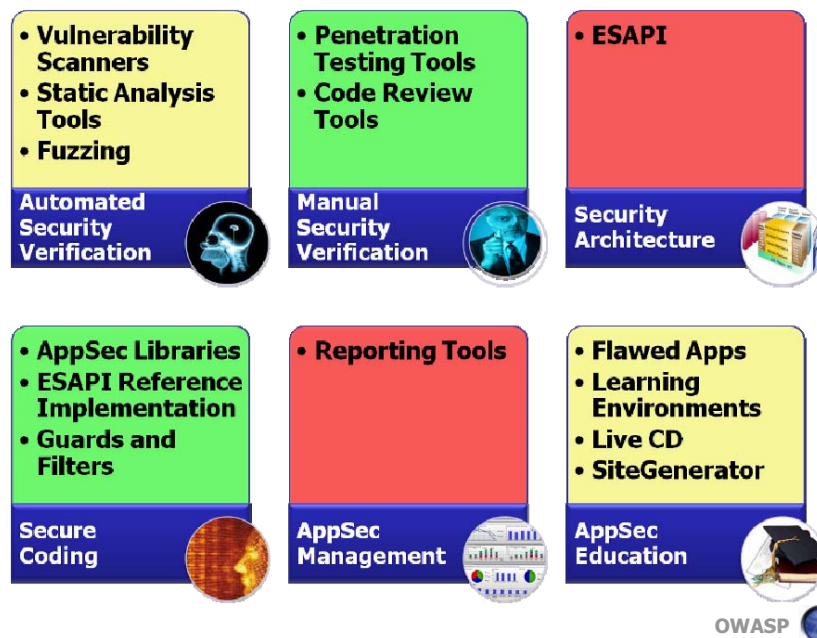
- 3,913 total articles
- 427 presentations
- 200 updates per day
- 179 mailing lists
- 180 blogs monitored
- 31 doc projects
- 19 deface attempts
- 12 grants



## ge



## OWASP Tools and Technology







# v2 (Release Quality)

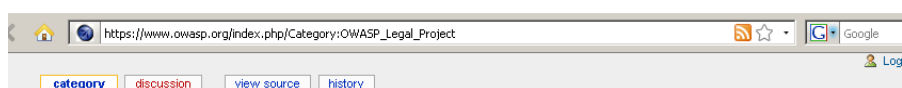


With this project, we wanted to help people applications, and not just provide a simple checklist or project is a complete Testing Framework, from which processes. The Testing Guide describes in details both the framework in practice.

|  |  |
|--|--|
| <b>Data Validation Testing</b>           | <b>1.2 Web Services Testing</b>                |
| 1 Testing for Cross Site Scripting       | 4.8.1 XML Structural Testing                   |
| 1.1 Testing for HTTP Methods and XST     | 4.8.2 XML Content-level Testing                |
| 2 Testing for SQL Injection              | 4.8.3 HTTP GET parameters/REST Testing         |
| 2.1 Oracle Testing                       | 4.8.4 Testing for Naughty SOAP attachments     |
| 2.2 MySQL Testing                        | 4.8.5 WS Replay Testing                        |
| 2.3 SQL Server Testing                   | <b>4.9 AJAX Testing</b>                        |
| 3 Testing for LDAP Injection             | 4.9.1 AJAX Vulnerabilities                     |
| 4 Testing for ORM Injection              | 4.9.2 How to test AJAX                         |
| 5 Testing for XML Injection              | <b>6. Writing Reports: value the real risk</b> |
| 6 Testing for SSI Injection              | 6.1 How to value the real risk                 |
| 7 Testing for XPath Injection            | 6.2 How to write the report of the testing     |
| 8 IMAP/SMTP Injection                    | <b>Appendix A: Testing Tools</b>               |
| 9 Testing for Code Injection             | • Black Box Testing Tools                      |
| 10 Testing for Command Injection         | • Source Code Analyzers                        |
| 11 Testing for Buffer overflow           | • Other Tools                                  |
| 11.1 Testing for Heap overflow           |  |
| 11.2 Testing for Stack overflow          |  |
| 11.3 Testing for Format string           |  |
| 12 Testing for incubated vulnerabilities |  |



# 3) Legal Project (Release Quality)



## Category:OWASP Legal Project

### Welcome to the OWASP Legal Project

The OWASP Legal project provides materials related to the legal aspects of secure software, including contracting, liability, and compliance.

## 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. 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 annex has 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.



## RECTIONS

Following few pages cover some frequently heard objections to using this language in software development contracts.

**NOT ALL THE TERMS ARE RIGHT FOR US...**

This document should be considered a starting point for your agreement. You may not like all the activities, or may want to propose more. You may want to responsibilities differently. This document is not intended to exactly capture the needs of all software Clients and Developers. It is intended to provide a common language for discussing the key topics that are important to ensuring that software ends up secure. After you have a security discussion and reach an agreement, you should tailor this agreement to match.

## WHO SHOULD PAY FOR THESE ACTIVITIES...

This document is NOT about putting more burden on the software developer. The question is not whether there are costs associated with security -- of course there are. Rather, the right question is what activities should be performed by both parties to minimize these costs, and when should they happen. This document is intentionally silent on the issue of who should pay for the activities described herein. While many of these activities should already be being done and are expected by many Clients, they are not regularly practiced in the software industry. The question of who pays (and how much) should be the subject of the negotiation.

Minimizing the costs of security is very difficult. While there are costs associated with performing security activities, there are also significant costs associated with getting them. We are convinced that the most cost-effective way to develop software is to reduce the likelihood that security flaws are introduced and to minimize the time between introducing a flaw and finding it. This agreement encourages early decisions on mechanisms to minimize these costs. Similarly, waiting until just before deployment to do security activities, such as code review and penetration testing, will also dramatically increase costs. We believe that the most cost-effective way to gain the most out of a secure code review is to do it as a constant level of effort into assurance throughout the lifecycle.

## THE LEVEL OF RIGOR IS WRONG....

This document assumes that the software being developed is reasonably important to a large enterprise or government agency. We've selected a "level of rigor" for software that is going to be used in critical applications, such as medical, financial, or defense related software. You may want to increase the rigor. You may want to add additional reviews, documentation, and testing activities. You may want to enhance the processes for finding, diagnosing, and remediating vulnerabilities. For less sensitive applications, you may want to reduce or remove activities.

## SECURITY REQUIREMENT AREAS

Following topic areas must be considered during the risk understanding and requirements definition, and, and testable requirements Both Developer and Client should be involved in this process and must be documented.

### Input Validation and Encoding

The requirements shall specify the rules for canonicalizing, validating, and encoding each input to the application, or external systems. The default rule shall be that all input is invalid unless proven otherwise. In addition, the requirements shall specify the action to be taken when invalid input is received. Specific examples include: injection, overflow, tampering, or other corrupt input attacks.

### Authentication and Session Management

The requirements shall specify how authentication credentials and session identifiers will be protected. This includes related functions, including forgotten passwords, changing passwords, remembering passwords, login attempts, and session timeouts.

### Access Control

The requirements shall include a detailed description of all roles (groups, privileges, authorizations) and the actions that can be performed by each role. The requirements shall fully specify the access control matrix for each role. An access control matrix is the suggested format for these rules.

### Error Handling

The requirements shall detail how errors occurring during processing will be handled. Some applications may require an error, whereas others should terminate processing immediately.



# 4) Code Review (Beta Quality)



## Preface

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

A proper code review 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.

|                                      |   |  |
|--------------------------------------|---|--|
| <b>Methodology</b>                   | <b>Examples by vulnerability</b>                        | <b>Language specific best practice</b> |
| • Introduction                       | 1. Reviewing Code for Buffer Overruns and Overflows     | <b>Java</b>                            |
| • Code Review Processes              | 2. Reviewing Code for OS Injection                      | • Java gotchas                         |
| • Steps and Roles                    | 3. Reviewing Code for SQL Injection                     | • Java leading security practice       |
| • Code Review and the SDLC           | 4. Reviewing Code for Data Validation                   | <b>Classic ASP</b>                     |
| • Transactional Analysis             | 5. Reviewing Code for Cross-site scripting              | • Classic ASP Design Mistakes          |
| • Application Threat Modeling        | 6. Reviewing Code for Cross-Site Request Forgery issues | <b>PHP</b>                             |
| • Code review Metrics                | 7. Reviewing Code for Error Handling                    | • PHP Security Leading Practice        |
| <b>Crawling Code</b>                 | 8. Reviewing Code for Logging Issues                    | <b>C/C++</b>                           |
| 1. Introduction                      | 9. Reviewing The Secure Code Environment                | • Strings and Integers                 |
| 2. First sweep of the code base      | 10. Reviewing Code for Authorization Issues             | <b>MySQL</b>                           |
| <b>Code Reviews and the PCI DSS</b>  | 11. Reviewing Code for Authentication                   | • Reviewing MySQL Security             |
| 1. Code Reviews and compliance       | 12. Reviewing Code for Session Integrity issues         | <b>Rich Internet Applications</b>      |
| <b>Examples by technical control</b> | 13. Reviewing Cryptographic Code                        | • Flash Applications                   |
| 1. Authentication                    | 14. Reviewing Code for Race Conditions                  | • AJAX Applications                    |
| 2. Authorization                     | <b>Example reports</b>                                  | • Web Services                         |
| 3. Session Management                | 1. How to write an application security finding         |  |
| 4. Input Validation                  | 2. How to determine the risk level of a finding         |  |
| 5. Error Handling                    | 3. Sample form  |  |
| 6. Secure Deployment                 | <b>Automating Code Reviews</b>                          |  |
| 7. Privacy                           | 1. Preface  |  |
|                                      | 2. Reasons for using automated tools                    |  |
|                                      | 3. Education and cultural change                        |  |
|                                      | 4. Tool Deployment Model                                |  |
|                                      | 5. Code Auditor Workbench Tool                          |  |
|                                      | 6. The Deep Ocean Framework                             |  |
|                                      | <b>The Owasp Code Review Top 10 flaw categories</b>     |  |
|                                      | • Preface   |  |
|                                      | <b>The Owasp Code Review Scoring System</b>             |  |
|                                      | • Preface   |  |
|                                      | <b>References</b>                                       |  |



## under a SoC 08 grant

Google

Log in / create account

ed or purchased books.

selling OWASP book. I have received many positive feedback from the OWASP fight against software insecurity. It has even convinced such people (Alessio Marziali) to open source their code review and a tool to support such an activity is very useful for secure application development. Proposal: I am proposing that we use the guide as a de facto secure code review guide in the future.

|  |   |                                     |
|--|---|-------------------------------------|
| First Reviewer<br>Shihm Jina<br>Curriculum | Second Reviewer<br>P.Satish Kumar<br>Curriculum | OWASP Board Member<br>Jeff Williams |
|--|---|-------------------------------------|

Sponsored Project/Guidelines/Roadmap

OWASP

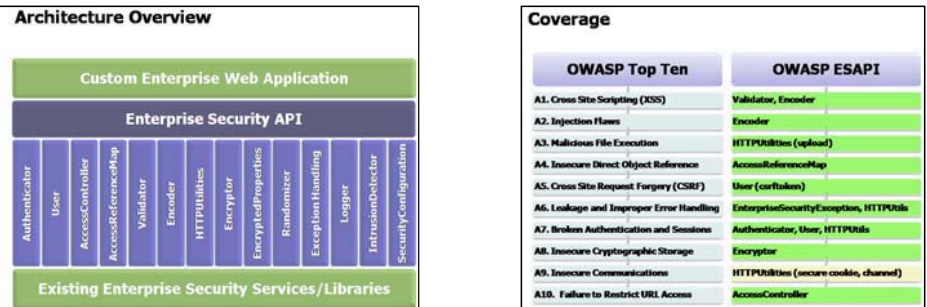
## 5) EASPI (Beta Quality)

### OWASP Enterprise Security API (ESAPI) Project

The ESAPI is a free and open collection of all the security methods that a developer needs to build a secure web application. You can just use the interfaces 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 ESAPI 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 reinventing the wheel for 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)

Google

Log in / create account

category discussion view source history

### Category:OWASP WebGoat Project

**OWASP Books** This project has produced a book that can be [downloaded or purchased](#). Feel free to browse the [full catalog of available OWASP books](#).

**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

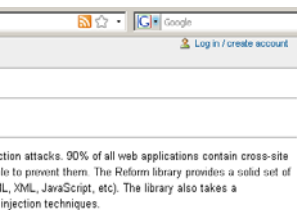
Web application security is difficult to learn and practice. Not many people have full blown web applications like online book stores or online banks that can be used to scan for vulnerabilities. In addition, security professionals frequently need to test tools against a platform known to be vulnerable to ensure that they perform as advertised. All of this needs to happen in a safe 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 de-facto 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.

Detailed solution hints

OWASP

## Beta/Release Quality)




, private implementations in use since 2002).



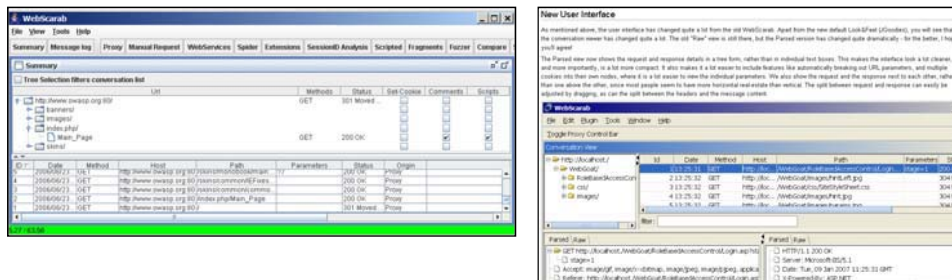
## 9) WebScarab (Release Quality)

Category:OWASP WebScarab Project

 This project has produced a book that can be [downloaded or purchased](#). Feel free to browse the [full catalog of available OWASP books](#).

**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. In its most common usage, 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 review 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 passed through WebScarab.



## Move (Release)



site.

isted in the [road map](#).

istance is needed to attend a conference, contact the

00 USD  
ther funding' below)  
funding' below)  
ar funding' below)  
value and ROI for OWASP and its community;



## 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 CIPS Edmonton ICE Conference<sup>[1]</sup>. The talk would be during November 5 - 7, 2007 . Looking for a quick reply if possible as we are trying to finalize the conference program very shortly. 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 (re)do an OWASP related presentation, propose them here with your availability boundaries (timing/geographical)

- Marc Curphey will happily speak about the WebAppSec industry, SDLC etc. around Europe. You can see him in action at [HTB with John Viega](#) (big download)
- [Paolo Perego](#) is available to talk about [Orizon project](#), safe coding and code review issues around Europe in the near October-December.
- [Marco Morana](#) is available to talk about [Software Security Frameworks](#) and Secure Code Reviews [see 07 CSI conference as reference](#) in USA around November-December and in Europe around January-February.
- [Sébastien Gloria](#) 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](#)
- you?

### Upcoming OWASP on the Move Events

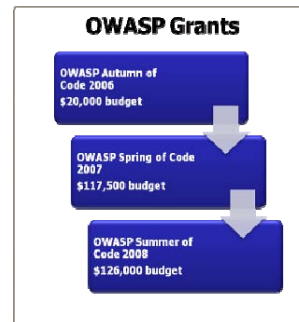
- October 30, 2008 - [Rochester](#) Marco Morana will speak at [Rochester Security Summit](#) about Software Security Framework



# OWASP's Seasons Of Code

## 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



## Spring of Code 2007

,000 USD  
amazing deliveries  
for community use)  
version  
validation)  
selection criteria  
(OWASP at academia)  
how know how to do it :) )  
es

## OWASP Summer of Code 2008

- 31 grants to promising application security researchers as part of the [OWASP Summer of Code 2008](#).

| Application  | Applicant's Name               | Assessment | Selection | Sponsorship |
|--|--------------------------------|------------|-----------|-------------|
| OWASP Code review guide, V1.1  | Eoin Keary                     | By vote    | YES       | 5,000 US\$  |
| The Ruby on Rails Security Guide v2  | Heiko Webers                   | By vote    | YES       | 2,500 US\$  |
| OWASP UI Component Verification Project (a.k.a. OWASP JSP Testing Tool)                | Jason Li                       | By vote    | YES       | 2,500 US\$  |
| Internationalization Guidelines and OWASP-Spanish Project                              | Juan Carlos Calderon           | By Vote    | YES       | 5,000 US\$  |
| OWASP Application Security Quick Reference (ASDR)                                      | Leonardo Cavallari Mittelli    | By vote    | YES       | 5,000 US\$  |
| OWASP .NET Project Leader  | Mark Roxberry                  | By vote    | YES       | 2,500 US\$  |
| OWASP Education Project  | Martin Knobloch                | By vote    | YES       | 2,500 US\$  |
| The OWASP Testing Guide v3   | Matteo Meucci                  | By vote    | YES       | 5,000 US\$  |
| OWASP Application Security Verification Standard                                       | Mike Boberski                  | By vote    | YES       | 2,500 US\$  |
| OWASP Online code signing and integrity verification service for open source community | Phil Potisk and Richard Conway | By vote    | YES       | 2,500 US\$  |
| Securing WebGoat using ModSecurity   | Stephen Evans                  | By vote    | YES       | 2,500 US\$  |
| OWASP Book Cover & Sleeve Design   | LXstudios                      | By vote    | YES       | 6,000 US\$  |
| OWASP Individual & Corporate Member Packs, Conference Attendee Packs Brief             | LXstudios                      | By vote    | YES       | 2,000 US\$  |

- And many more!!!

ance

ent  
als  
  
apters and Projects  
oney spender  
  
money goes to),

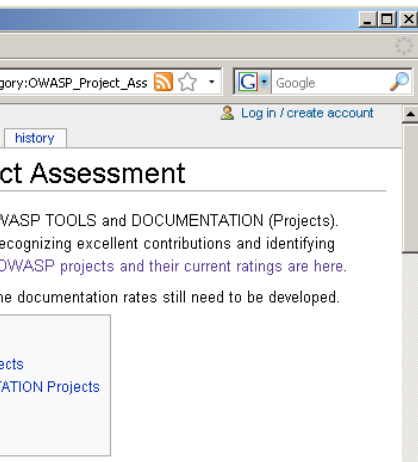
## OWASP Structure

- 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





## Assessment Scale for OWASP TOOLS Projects – Release Quality

| Class                          | Criteria   | Review Process   | Example                                  |
|--------------------------------|--|--|--|
| Release Quality<br>OWASP Tools | <p>All Beta Quality Requirements plus:</p> <ul style="list-style-type: none"> <li>Be reasonably easy to use</li> <li>Include online documentation built into tool (based on required user documentation)</li> <li>Include build scripts that facilitate building the application from source (Goal: One-click build)</li> <li>Publicly accessible bug tracking system established, ideally at the same place as the source code repository (e.g., at Google code, or Sourceforge)</li> <li>Be run through <a href="#">Fortify Software's open source review</a> (if appropriate) and <a href="#">FindBugs</a>.                             <ul style="list-style-type: none"> <li>WebGoat would not be appropriate for example since it would light up like a Christmas tree :-)</li> </ul> </li> <li>C/C++ apps (if we have any) should consider being run through <a href="#">Coverity's open source review</a>. Coverity also accepts submissions for open source Java applications.</li> <li>When approved to be Release Quality: Update the link to it on: the <a href="#">OWASP Project</a> page and update its project quality tag on its project page to be Release Quality.</li> </ul> <p><b>Recommendations:</b></p> <ul style="list-style-type: none"> <li>Conference style Powerpoint presentation that describes the use and status of the tool. (This could be used by others to discuss the tool at OWASP Chapter meetings, serve as easy to review offline documentation, etc.)</li> <li>UAT pass on functionality of the tool</li> <li>Developer documents any limitations</li> </ul> | <ul style="list-style-type: none"> <li><b>Requirement:</b> 2 Reviewers + 1 OWASP Board Member.</li> <li>If possible, the project's lead should suggest two Project Reviewers. One of them should be an OWASP Project or Chapter Leader.</li> <li>If the project's lead can't find the Project Reviewers, the OWASP Board will identify them. The same will happen whenever the reviewers suggested do not have the required approval.</li> </ul> | OWASP<br><a href="#">WebGoat Project</a> |

## OWASP TOOLS Projects –

|                        |   |   |
|------------------------|---|---|
| stand alone executable | <ul style="list-style-type: none"> <li><b>Requirement:</b> 2 Reviewers.</li> <li>If possible, the project's lead should suggest two Project Reviewers. One of them should be an OWASP Project or Chapter Leader.</li> <li>If the project's lead can't find the Project Reviewers, the OWASP Board will identify them. The same will happen whenever the reviewers suggested do not have the required approval.</li> </ul> | OWASP<br><a href="#">AntiSamy Project</a> |
|------------------------|---|---|

## Assessment Scale for OWASP TOOLS Projects – Alpha Quality

|                              |  |   |   |
|------------------------------|--|---|---|
| Alpha Quality<br>OWASP Tools | <ul style="list-style-type: none"> <li>Agree to <a href="#">OWASP's open source license</a></li> <li>The "main" page for any OWASP tool must be on the OWASP website. This page must:                             <ul style="list-style-type: none"> <li>describe the tool, the project leader, contact info, and include all relevant links, including a download link for the code and the executable version,</li> <li>includes a roadmap/guideline pointing out the steps to achieve the purpose of project.</li> <li>include the Alpha Quality Tool project tag. (Which we still need to define),</li> <li>be placed at <a href="#">OWASP Project</a> page.</li> </ul> </li> <li>Have its code and any documentation in Googlecode, or Sourceforge.</li> <li><a href="#">Mailing list for project created</a>.</li> <li>Solves a core application security need.</li> </ul> | <ul style="list-style-type: none"> <li><b>Requirement:</b> 1 Reviewer.</li> <li>If possible, the project's lead should suggest a Project Reviewer who is an existing OWASP Project or Chapter Leader.</li> <li>If the project's lead can't find a Project Reviewer, the OWASP Board will identify one. The same will happen whenever the reviewer suggested does not have the required approval.</li> </ul> | OWASP<br><a href="#">CSRFTester Project</a> |
|------------------------------|--|---|---|

## Practice: SoC 08

OWASP Summer of Code 2008 Projects Authors Status Target and Reviewers

This page contains Projects, Authors, Status Target and Reviewers of the sponsored programme OWASP Summer of Code 2008.  
\* Please note: The reference "Confirmed" means reviewed/ approved by both project authors and OWASP Board.

### DOCUMENTATION PROJECTS

| Application  | Author              | Status  | 1st Reviewer                | 2nd Reviewer                | OWASP Board Reviewer |
|--|---------------------|---------|-----------------------------|-----------------------------|----------------------|
| OWASP Application Security Verification Standard                         | Mika Dolski         | Data    | Jeff Williams (Confirmed)   | Peter Parnell (Confirmed)   | Not applicable       |
| OWASP AppSec - Detect and Respond to Attacks from Within the Application | Michael Conley      | Data    | Erik Stenlund (Confirmed)   | Walter Janssen (Confirmed)  | Not applicable       |
| OWASP Backend Security Project   | Carlo Pollicino     | Data    | Christian Blich (Confirmed) | John Sweeney (Confirmed)    | Not applicable       |
| OWASP Clean ASP Security Project   | Juan Carlos Calabro | Data    | Andrew Anderson (Confirmed) | Andrew Anderson (Confirmed) | Not applicable       |
| OWASP Code review guide, V1.1  | Erik Vanyi          | Quality | P. Satch (Confirmed)        | P. Satch (Confirmed)        | Jeff Williams        |
| OWASP Corporate Application Security Rating Guide                        | Parvathy Iyer       | Quality | David Satch (Confirmed)     | David Satch (Confirmed)     | Not applicable       |
| OWASP Education Project  | Matthias Kneiblich  | Quality | David Satch (Confirmed)     | David Satch (Confirmed)     | Not applicable       |

OWASP Application Security Verification Standard Project

| Project  | Author              | Status  | 1st Reviewer                | 2nd Reviewer                | OWASP Board Reviewer |
|--|---------------------|---------|-----------------------------|-----------------------------|----------------------|
| OWASP Application Security Verification Standard Project                 | Mika Dolski         | Data    | Jeff Williams (Confirmed)   | Peter Parnell (Confirmed)   | Not applicable       |
| OWASP AppSec - Detect and Respond to Attacks from Within the Application | Michael Conley      | Data    | Erik Stenlund (Confirmed)   | Walter Janssen (Confirmed)  | Not applicable       |
| OWASP Backend Security Project   | Carlo Pollicino     | Data    | Christian Blich (Confirmed) | John Sweeney (Confirmed)    | Not applicable       |
| OWASP Clean ASP Security Project   | Juan Carlos Calabro | Data    | Andrew Anderson (Confirmed) | Andrew Anderson (Confirmed) | Not applicable       |
| OWASP Code review guide, V1.1  | Erik Vanyi          | Quality | P. Satch (Confirmed)        | P. Satch (Confirmed)        | Jeff Williams        |
| OWASP Corporate Application Security Rating Guide                        | Parvathy Iyer       | Quality | David Satch (Confirmed)     | David Satch (Confirmed)     | Not applicable       |
| OWASP Education Project  | Matthias Kneiblich  | Quality | David Satch (Confirmed)     | David Satch (Confirmed)     | Not applicable       |

OWASP

## Finances and Grants

Revenue source: Members



100%

• All membership fees are used to fund grants

Revenue source: Conferences

| Upcoming Conferences:                                    |
|--|
| May 2008 - OWASP AppSec Europe 2008 - Ghent, Belgium     |
| May 2008 - OWASP AppSec Asia 2008 - Singapore            |
| September 2008 - OWASP AppSec 2008 - Hyderabad, India    |
| September 2008 - OWASP AppSec 2008 - London, UK          |
| September 2008 - OWASP AppSec 2008 - New York City       |
| September 2008 - OWASP AppSec 2008 - Paris, France       |
| September 2008 - OWASP AppSec 2008 - Tokyo, Japan        |
| September 2008 - OWASP AppSec 2008 - Vancouver, Canada   |
| September 2008 - OWASP AppSec 2008 - Warsaw, Poland      |
| September 2008 - OWASP AppSec 2008 - Zurich, Switzerland |
| Past Conferences:  |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |
| Feb 2008 - OWASP AppSec Asia 2007 - Singapore            |

55%

• Grants

45%

• OWASP employees  
• Conferences costs  
• OWASP Admin

### OWASP Grants

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 Foundation



OWASP 42

## 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 of 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))

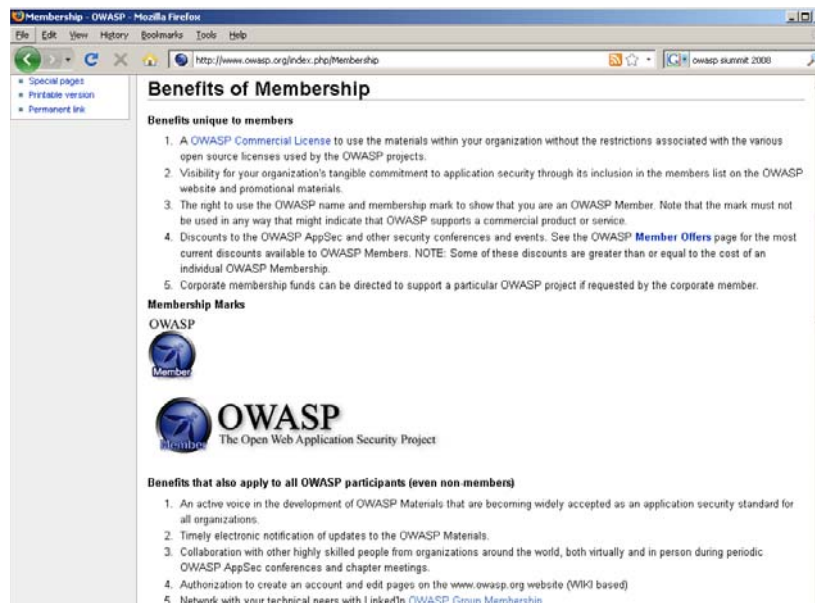
OWASP

44

on the type of organization and how the OWASP Materials are used. As a  
ctly to supporting OWASP's various projects and chapters.

|   | Annual<br>Membership Fee   |
|---|--|
| mission and would like to provide financial support to  | \$100 USD  |
| and government-approved non-profit organizations that<br>als in their courses, research, or other educational                             | \$250 USD  |
| OWASP Materials within their organization.<br>employees are considered large.   | Small (<100) -<br>\$2,000 USD *<br>Large (100+) -<br>\$7,000 USD * |
| t provide information security consulting, training, or<br>P Materials in their services or marketing. Organizations<br>considered large. | Small (<10) -<br>\$3,000 USD *<br>Large (10+) -<br>\$8,000 USD *   |
| urity products or other software and use OWASP<br>keting.   | \$9,000 USD *  |

## Benefits of Membership



## ers – Jul 2008



## 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!