Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) has been nominated by the London OWASP Chapter for the Best Security Initiative Award 2009.

About OWASP

The Open Web Application Security Project (OWASP) is a global open community dedicated to enabling organisations to develop, purchase and maintain applications that can be trusted by users to help maintain their privacy, protect against identity theft, protect data and enhance the security of computer systems.

OWASP builds documents, tools, teaching environments, guidelines, check lists, standards and other materials to help organisations improve their capability to produce secure code. All OWASP materials and chapter meetings are free and open to anyone interested in improving application security.

OWASP was formed in 2001 in an entirely organic fashion, continues to be a place where good people gather to help increase the awareness of the web application security problems. It is a grass-roots effort, with the driving force being the people who are dealing with these problems every day, and wanting to lend a hand to change the situation for the better. The Board is comprised completely of voluntary members, one of whom is based in the UK. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success.

There are two active OWASP chapters in the UK (London and Scotland), with another chapter currently in formation (Leeds). These UK chapters are part of a network of over 130 chapters around the world. OWASP has a growing number of individual members and a significant corporate membership base who, together with conference fees, are helping finance its activities. These activities are of special importance to people in organisations who do not necessarily have the resources to finance their own security research.

Progress and Successes

Following on the from Spring of Code 07, last year's Summer of Code 08, was another success, leading to the release of many new or updated free tools and guidance documents. A formal review process, assessment criteria and project management control, introduced by OWASP's project manger who is based in the UK, has improved the effectiveness and final quality of projects. As one example, the OWASP Testing Guide version 3 was completed. Like other OWASP materials this is available free of charge on the web site as text, as a free of charge PDF download and as an at-cost printed book (£10.57 for the 349-page document—we encourage all our books to be copied and distributed freely). Contributors to the OWASP Spanish Project in Latin America are currently translating this essential guide into Spanish as part of the 2008

OWASP Internationalization Project, along with other key materials. UK participants contributed by leading the DirBuster and JBroFuzz tool projects and by being authors and reviewers, including for the Code Review Guide Version 1.1 and the Securing WebGoat using ModSecurity Project. JBroFuzz was entered in the security award category of the IET Innovation Awards 2008.

OWASP undertook a new type of event in November 2008—an OWASP Summit held in Portugal, where active contributors from around the world were invited to a summit. The travel and accommodation costs for all 80+ participants were paid from OWASP's funds to ensure that no-one would be unable to attend due to inability to pay. Outcomes included new outreach programmes, plans for 2009, a definition of OWASP's principles, a new code of ethics and six new global committees of volunteers (including UK representation) to help the work of the Board.

We want to increase awareness and membership. The optional annual subscription for individual membership has been reduced by 50% in 2009.

Our outreach work has been extended—including academic organisations where we now have a special new partnership programme for universities. Since November 2008, we have been delivering a frequent podcast to improve awareness and access to our resources. We have also been active in raising awareness about how application security can affect the critical national infrastructure of countries and begun to engage more formally with legislators and standards organisations. For example, in recent months we have submitted responses to two draft British Standards and to the Digital Britain Interim Report, where we believe high standards of application security are needed for a better UK digital economy.

Our materials are increasingly being referenced by other organisations. In October 2008, the Payment Card Industry Security Standards Council released a new version of requirements for organisations worldwide who store or process credit card data. The PCI Data Security Standard (PCI DSS) version 1.2 includes as requirement 6.5:

> *"Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide."*

New projects and research are continually being developed—another project in 2008 developed a standard for conducting application security verifications. And this month OWASP released the first Security Spending Benchmarks Project Report, providing guidance and benchmarking to justify overall web application security spending. This week, the Software Assurance Maturity Model version 1 was released, an open framework for building security into software development, developed with assistance from UK participants.

Grants are available for some current research projects and another season of code for 2009 is being planned We have nine national and regional conferences planned for 2009, including the European conference which will be held in Poland.

Conclusion

OWASP is a new kind of organisation—very much part of civil society. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective

information about application security. OWASP is not affiliated with any company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way.

During the last year, many new initiatives have helped OWASP raise awareness about application security and provided new resources for all... anywhere in the world. We believe the model of collective knowledge, values and responsibility combined with outreach and engagement is worth sharing.