OWASP 安全支出基准项目
Boaz Gelbord

OWASP 的安全支出基准项目旨在产生指导和行业公认的整体 Web 应用程序开支的基准。此 OWASP 的项目定期发布这样的调查结果报告。该调查是完全匿名的，也不会收集受访者的个人资料。我们同时也会发表调查原始数据。最新的 OWASP 的安全支出基准调查一直开放到 4 月 15 号。

https://www.surveymonkey.com/s/TPYZLXK

密码: OWASP_Spending

OWASP 应用程序安全大会，美国，加州 2010 征集论文

大会将在加州大学欧文分校橙县的会议中心举行，会议时间 2010 年九月 7 号到 10 号。

提及论文应包括:
- 演讲人名字
- 演讲人邮件和电话号码
- 演讲人简介
- 题目
- 摘要
- 任何支持的研究和工具(不会被发布到 CFP 委员会之外)

提交期限 6 月 6 号 12 PM PST (GMT-8)

提交至:
http://www.easychair.org/conferences/

项目和全球委员会资金

会员的模式已扩展至项目和全球委员会。这些团体会现在可以自己寻找赞助商来创建他们自己的资金来源，以支持该项目或全球委员会。

这个模式如何操作：
项目和委员会现在可以寻找自己的赞助者提供资金给项目或委员会。OWASP 将以目前和各地小组 (chapters) 分享资金的方式来管理这些资金，即将企业的会费 4/6 分成。

资金将用来支付项目相关费用，但是不能用来支付 OWASP 的成员。

资金可以使用的方式包括：
- 用来支付项目成员关于该项目的演讲的差旅费用。
- 用来打印在各种会议中使用和发放的关于项目的文档
- 用于制作该项目的光碟
- 资金不能用来支付项目成员为这个项目工作的时间
- 要收集赞助者的资金，或者有更多问题，联系 Kate Hartmann

OWASP 董事会成员

Jeff Williams
Dinis Cruz
Dave Wichers
Tom Brennan
Sebastien Deleersnyder
Eoin Keary
Matt Tesauro

3 月 15, 2010
Last November 5th and 6th OWASP organized two big OWASP events in Rome and Milan, Italy.

The first was realized in collaboration with CONSIP, a company of the Italian Ministry of Economy and Finance (MEF), working for the Italian Public Administrations. Specifically the event was called “The Application Security as trigger for the Italian E-Government.” The audience was made up of the CISOs of all the Italian Ministries and Public Administrations. The Presentations are online here:

http://www.owasp.org/index.php/Italy_OWASP_Day_E-gov_09

OWASP—Italy Day IV in Milan—The Second day was in Milan with more than one hundred attendees. We just put the presentations, photos and videos on-line here.

OWASP—Italy Day at Security Summit 2010

March 18th OWASP—Italy will present the “OWASP Guidelines and tools for Web Applications Security at the Security Summit 2010 in Milan, Italy. https://www.securitysummit.it/eventi/view/73

Release—OWASP ESAPI ver. 1.4.4 for JAVA ver. 1.4 and above

Jim Manico

ESAPI 1.4.4 Javadoc’s can be found here: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4.4/index.html

Questions regarding ESAPI usage and configuration? Visit this link: https://lists.owasp.org/mailman/listinfo/esapi-user and join the mailing list.

Interested in contributing? Join this mailing list: https://lists.owasp.org/mailman/listinfo/esapi-dev

Man In The Middle Attack—Explained
From Michael Coates Blog 3/3/2010

“That’s vulnerable to a man in the middle attack!”

You’ve probably heard this before, but let’s dive into the details of this attack and understand exactly how it works.

Requirements for Attack
A MitM can be performed in two different ways:

1. The attacker is in control of a router along the normal point of traffic communication between the victim and the server the victim is communicating with.

2.a. The attacker is located on the same broadcast domain (e.g. subnet) as the victim.

2.b. The attacker is located on the same broadcast domain (e.g. subnet) as any of the routing devices used by the victim to route traffic.

The Attack
Finish the article at Michael Coates blog
**OWASP Common Numbering Project**
**Mike Boberski**

An exciting development, a new numbering scheme that will be common across OWASP Guides and References has been developed. The numbering was a team effort, led by Mike Boberski (ASVS project lead and co-author). OWASP Top Ten, Guide, and Reference project leads and contributors as well as the OWASP leadership worked together to develop numbering that would allow for easy mapping between OWASP Guides and References, and that would allow for a period of transition as Guides and References are updated to reflect the new numbering scheme. This project will track retired numbers and provide a centralized clearinghouse for mapping information. Please visit the project page for more information:

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

**OWASP ASVS**
**Mike Boberski**

A first complete translation into Japanese has been completed, and a Japanese language ASVS concept guide appendix is now being developed. Translations into French, German, Chinese, Hungarian, and Malay are now underway. The project is always on the lookout for translation volunteers, contact: mike.boberski@owasp.org if you are interested.

**OWASP Development Guide**
**Mike Boberski**

Work has begun on the next iteration of the guide. The next version of the OWASP Development Guide will be in effect the detailed design guide for the requirements of the OWASP ASVS. A team of 26 volunteers and counting have signed up so far. The project is always on the lookout for volunteers.

**OWASP ESAPI for PHP**
**Mike Boberski**

Work continues on the PHP port of ESAPI. Most core classes have been completed or are in the last mile of their initial development, including Security Configuration, Validator, Encoder, and Logger. A user base of early adopters has been emerging. Please visit the project page for more information.

**Two New Projects**
**Paulo Coimbra**

**OWASP Broken Web Application Project**

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

This project is sponsored in part by: Mandiant.

**OWASP Ecosystem Project**

We envision a partnership between technology platform vendors and a thriving ecosystem focused on the security of their technology. The ecosystem will include researchers (both Builders and breakers), tools, libraries, guidelines, awareness materials, standards, education, conferences, forums, feeds, announcements, and more.

http://www.owasp.org/index.php/Security_Ecosystem_Project
The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. We can be found at www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security.

OWASP is not affiliated with any technology 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.

The OWASP Foundation is a not-for-profit entity that ensures the project’s long-term success.