March 15, 2010

OWASP

The Open Web Application Security Project

OWASP Security Spending Project Survey

Boaz Gelbord

The OWASP Security Spending Benchmarks project seeks to produce guidance and an industry accepted benchmark for justifying overall Web application spending. This OWASP project publishes regular reports on the results of surveys such as this one.

The Survey is completely anonymous and no personal information will be collected from the respondents. Together with our published report we will also be making the raw survey data available to the community. The newest version of the OWASP Security Spending Benchmarks Project is now open until April 15th.

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

Password: OWASP_Spending

OWASP AppSec USA, California 2010 Call for Papers

Conference will take place at the UC Irvine Conference Center in Orange County, CA on September 7th—10th, 2010.

Submissions should include:

- Presenter(s) name(s)
- Presenter(s) emails and/or phone number(s)
- Presenter(s) bio(s)
- Title
- Abstract
- Any supporting research/tools (will not be released outside of CFP committee)

Submission deadline is June 6th at 12 PM PST (GMT-8)

Submit proposals to: https://www.easychair.org/conferences/?conf=appsec2010

Project and Global Committee Funding

The membership model has been extended to Projects and the Global Committee's. These groups can now find their own sponsors to create their own source of funds to support the project or Global Committee.

How this works:

Projects and committees can now find their own sponsors to contribute funds to the project or committee. OWASP foundation will manage the funds and shares the funds the same way as it is currently done with Chapters as a 40/60 split for corporate memberships.

Funds can be used to cover project related costs, but can not be used to pay OWASP members.

Examples of how funds can be used:

To cover travel expenses of a project member who is going to be speaking regarding the project.

To print documentation regarding project to be shared at an event.

To print CDs.

Funds can not be used to reimburse a project member for time spent working on the project.

Contact Kate Hartmann to collect funds from sponsors or if you have further questions regarding how this new program is set up.

OWASP AppSec Conferences

June 2nd, 2010
Froc 2010
Denver, Colorado

June 3rd—4th, 2010
OWASP Day Mexico
Aguascalientes, Mexico

June 21-24, 2010
AppSec Research 2010
Stockholm, Norway

September 7th–10th, 2010
AppSec USA 2010
Irvine, California

November 16th–19th, 2010
AppSec Brasil 2010
Campinas, Brasil

OWASP Board Members

Jeff Williams

Dinis Cruz

Dave Wichers

Tom Brennan

Sebastien Deleersnyder

Eoin Keary

Matt Tesauro

OWASP Podcasts Series

Hosted by Jim Manico

Ep 60 Jeremiah Grossman and Robert Hansen (Google pays for vulns)

Ep 59 AppSec Roundtable with Boaz Gelbord, Ben Tomhave, Dan Cornell, Jeff Williams, Andrew van der Stock and Jim Manico (Aurora+)

Ep 58 Interview with Ron Gula (Web Server Scanning, IDS/IPS)

Looking for an AppSec job? Check out the OWASP Job Page

Have an AppSec job you need posted?

Contact:

Kate Hartmann

OWASP Italy Days
Matteo Meucci

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

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.

Definition

First, a quick definition, a man in the middle (MitM) attack is an attack where the communication which is exchanged between two users is surreptitiously monitored and possibly modified by a third, unauthorized, party. In addition, this 3rd part will be performing this attack in real time (i.e. stealing logs or reviewing captured traffic at a later time would not qualify as a MitM).

While a MitM could be performed against any protocol or communication, we will discuss it in relation to HTTP Traffic in just a bit.

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

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

Changelog:

http://owasp-esapi-java.googlecode.com/svn/branches/1.4/changelog.txt

Other important links:

Download the complete .zip release at: http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip

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

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 Development Guide Project Page

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/intex.php/OWASP_Broken_Web_Applicaitons_Project#tab=project_Details

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

134K people spent 1.5 million minutes at OWASP website in February!

Haiti Donations:

OWASP's total

donation: $1378.67

Sent to: Doctors Without Borders.

The funds went directly to the Haiti relief efforts.

Thank you to our Corporate Members who renewed their support of the OWASP Foundation in January and February.

Booz | Allen | Hamilton

hp invent

INFOVISION

protiviti Independent Risk Consulting

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Phone: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

The free and open application security community

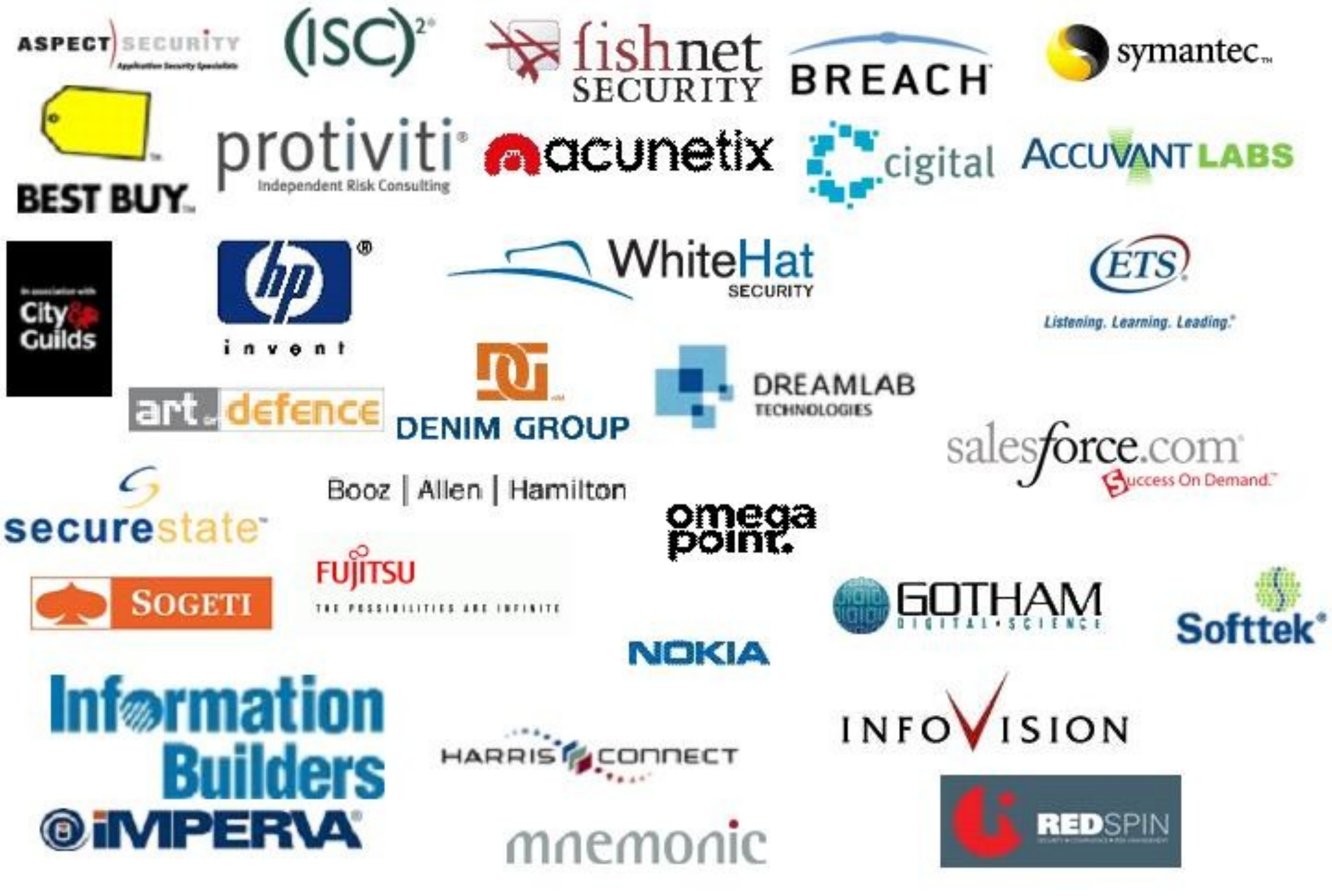
The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving 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.

OWASP Organizational Sponsors



Newsletter Editor: Lorna Alamri