2010年5月17日

OWASP AppSec 会议

2010年6月2日
Froc 2010
丹佛, 科罗拉多州

2010年6月3日至4日
OWASP Day Mexico
阿瓜斯卡连特斯州, 墨西哥

2010年6月21日至24日
AppSec Research 2010
斯德哥尔摩, 瑞典

2010年6月30日
OWASP Argentina Day
布宜诺斯艾利斯, 阿根廷

2010年9月7日至10日
AppSec USA 2010
欧文, 加利福尼亚州

2010年9月17日
AppSec Ireland
都柏林, 爱尔兰

2010年11月16日至19日
AppSec Brasil 2010
坎皮纳斯, 巴西

OWASP
The Open Web Application Security Project

2010年瑞典OWASP AppSec Research会议

该大会提供完整的会议和培训计划。晚宴将于6月23日，星期三，在斯德哥尔摩市政大厅举行。该市政大厅曾经颁发了诺贝尔奖项。市政大厅的相关信息请点击此处。

2010年美国加州OWASP AppSec 会议的关键出席演讲人

AppSec 美国会议将于2010年9月7日至10日，在位于加利福尼亚州欧文的加利福尼亚大学会议中心举行。

关键出席演讲人将包括:

Bill Cheswick—AT&T Research
HD Moore—Metasploit/Rapid7
David Rice—Geekonomics
Jeff Williams—Aspect Security

会议网站将会尽快发布。其网址将是：

www.appsecusa.org

2010年巴西OWASP AppSec 会议的关键出席演讲人

巴西OWASP AppSec 会议宣布了关键的出席演讲人为Bruce Schneier和Jeremiah Grossman。该会议将于2010年11月16日至19日举行。 欲知更多信息请访问：

www.owasp.org/index.php/AppSec_Brasil_2010).

2010年版OWASP Top 10现已发布

2010年版OWASP Top 10已于2010年4月19日发布。OWASP受到了对该新版本发布的极大关注。这里提供了一些来自国际新闻媒体关注OWASP的链接。如果你还没有看过该版本的Top 10，请花一点时间来审阅，并请你接受挑战，把应用程序安全做得更加清晰可见。

通过以下链接可阅读最新版本的Top 10:

http://www.owasp.org/index.php/OWASPTop10-2010-PressRelease

相关文章:

Logic Flaws and the OWASP Top 10, Steve Ragan—The Tech Herald

Top 10 Most Critical Web App Security Risks, Ericka Chickowski—Channel Insider

Injection tops list of web application security risks, Angela Moscaritolo—SC Magazine

OWASP Issues Top 10 Web Application Security Risks List, Kelly Jackson—DarkReading

Security: 10 Most Dangerous Web App Security Risks, Brian Prince—eWEEK

OWASP时事通讯—文章征集

OWASP现征集关于应用程序安全的文章，以发表于OWASP的时事通讯之中。所有征集文章的内容都不能包含商业信息。

欲知更多信息或者投稿，

请与Lorna.Alamri@owasp.org 联系。 in-

[OWASP Podcasts Series](#)

Hosted by Jim Manico

Ep 61 Richard Bejtlich (Network Monitoring)

Ep 62 Amichai Shulman (WAF)

Ep 63 Ed Bellis (eCommerce)

Ep 64 Andy Ellis (Availability)

Ep 65 AppSec Round Table: Boaz Gelbord, Dan Cornell, Jeff Williams, Johannes Ullrich & Jim Manico

Ep 66 Brad Arkin (Adobe)

Ep 67 Top Ten– Jeff Williams (XSS)

Ep 68 Top Ten— Kevin Kenan (Cryptographic Storage)

Ep 69 Top Ten—Eric Sheridan (CSRF)

Ep 70 Top Ten— Michael Coates (TLS)

Ep 71 Top Ten— Robert Hansen (Redirects)

Jim Manico的访谈活动

Lorna Alamri

OWASP最特别的地方之一，是它为那些对热衷于应用程序安全的人提供了一个论坛平台。Jim Manico已推出了关于与著名应用程序安全专家的Podcast访谈系列。他利用自己的才华开发了一个OWASP Podcast系列，从而帮助了他职业生涯的发展，并提高了OWASP知识基础和关于应用程序安全的意识。

你为什么决定做第一个Podcast?

早在2008年10月，我目睹了几次OWASP志愿者和OWASP eLists之间的交互活动，我被其谈话内容的深度所征服。我想，应该需要有人记录下这些。另外，我想播客会比较容易。因此，在没有得到允许的情况下，我就开始了录制。:）Arshan，Jeff Williams和Jeremiah Grossman表示愿意做我的第一个访谈对象，而我一直为OWASP进行Podcast至今。:）

你做Podacast的最初目标是什么？现在有所改变吗？如果有，是如何改变的？

我的最初目标是以“简单的方式”记录一个自由的电话会议服务已经刚发行的MP3音频。现在，我正在购买一个非常高端的工作室话筒，并专注于通过精心地编辑和掌握专业的技能，来保证最终产品的质量。这让我的最初目标发生了完全的转变，但我通过不断地努力改善节目的质量。

这个项目是如何发展的？

今天（3月中旬），我正在编辑第63个项目。我已经完成了多个项目并等待新Top 10的发布。

你如何准备一次访谈？

我从与嘉宾预约时间开始。我也每个月重复邀请嘉宾参加圆桌会议的活动。我在与嘉宾见面前就准备好相关问题。另外，我寻找一些聪明的评论，而不让我的嘉宾感到惊讶。

最受欢迎的Podcast是哪个？最有争议的是哪个？你最喜欢的又是哪个？

圆桌会议是最受欢迎的节目。我们曾经有一位嘉宾把所有OWASP成员称为“一群共产党员”，这引起了人们的震惊。我最喜欢的节目来自于惠普的Billy Hoffman，他说我的祖母值得被黑掉。;）Dave Aitel是这些人中最酷的。Richard Stallman来的那个节目，在我问他的Skype帐户后，狠狠地撞了我。（注：我只在ogg!中发布Stallman的访谈！我保证！）但我特别感谢Andre Gironda, Jeff Williams和Boaz对节目的支持。坦率地说，我的嘉宾们都太棒了！

如果你知道你现在知道的这些，你会做些什么不同？任何方面！

我再也不会宣称一个自由的电话会议服务会足够好到去录制一个podcast!:)

你开始Podcast时的最大挑战是什么？

尽管去做吧。一旦我们开始，Podcast的精髓就被吸取了。:）

你为什么觉得它成功了？

因为嘉宾们。我为那些在节目中拥有令人难以置信的智慧和才华的嘉宾们感到高兴。我们不能没有这个社区。

如果你要对某些嘉宾进行Podcast的访谈，你将邀请谁？

我将只对发明HTTP的微软员工进行访谈！:）但事实上，Bruce Schneier是我唯一仍然在追逐中的嘉宾。我在Podcast项目的初始阶段和Bruce进行了访谈，但是节目的录音质量太差以致于我至今无法将它发布出去（我的错！）。Bruce！我错了！请再给我一次机会吧。:）

下一步的计划是什么？

节目需要继续！有几个公司非常慷慨的为OWASP赞助了该节目，并给了我一小笔预算用于为将来的节目购买专业的设备器材。感谢Tenable，Adobe，Orbitz和Akamai给予OWASP的赞助！

你有什么学到的经验要和大家分享吗？还有其他什么你想和你的听众分享吗？

我已将我的设备列表和工序发布于http://www.owasp.org/index.php/Talk:OWASP_Podcast。该列表是我过去几年来获得的宝贵经验。

最重要的是，感谢你的收听！该节目如果没有我们那些难以置信的听众的话，就不会成功！

如果你有评论，请在podcast@owasp.org中给我留言。

你可以帮助OWASP让*每个*应用程序开发人员了解OWASP Top 10吗？
共享这个链接：
OWASP_Top_10_-_2010.pdf

OWASP伦敦分会
OWASP AppSec 培训计划

OWASP伦敦分会已于4月16号完成了它们的第一次培训活动。它们编制了一天的演讲活动，以解决以下这些问题：

- 除了OWASP Top 10，绝大多数OWASP项目并没有得到广泛使用和了解。在大多数情况下，这不是因为质量差和缺少有用的文档和工具项目，而是由于缺乏对企业安全生态系统或Web应用程序开发生命周期的了解。
- 该培训活动旨在提供一些精心挑选的成熟的和企业准备好的项目，并连同提供一些如何使用它们的实际案例。
- 该培训活动非常实用。它提供了相关示范并可以让活动参加者亲手操作那些工具软件。

相关材料可从以下链接下载：
你今天可以使用的OWASP项目和资源。
现在为其他OWASP分部提供相关材料和相关课程。

非常感谢我们的合作伙伴在今年3月和4月更新了对OWASP的赞助。

Booz | Allen | Hamilton

cigital

symantec

fishnet SECURITY

4月的最新合作赞助商：
Qualys
感谢您的支持！

QUALYS

跟随OWASP

OWASP的
Twitter feed

http://twitter.com/statuses/user_timeline/16048357.rss

IBWAS '10—征文

Carlos Serrão, Ph.D.

第2届Ibero-American Web应用软件安全会议（IBWAS'10）将于11月11日和12日在葡萄牙里斯本举行。本届会议的宗旨是让应用软件安全专家、教育家、研究人员以及开业者共聚一堂讨论应用软件安全的问题和解决办法。与会者将来自企业，学术界以及像OWASP这样的国际性团体。当学术研究人员把他们的研究成果与软件工程师的经验结合，将会产生有趣的结果。会议组织者已经发布了征文启事（CfP），有意者应根据要求在9月24日前提交文章。以下仅是建议题目(议题不限)：

- 应用软件开发的安全
- 服务结构安全
- 开发框架的安全
- Web应用软件威胁模型
- 云计算安全
- Web应用软件风险分析(程序审查，人工渗透测试，静态分析，等等)
- 应用软件安全的度量
- 安全编程技巧
- 对应用软件安全有帮助的平台或编程语言的特征
- 如何在web应用软件中使用数据库
- Web应用软件的访问控制检测
- Web应用软件如何保护隐私
- Web应用软件的规范，证明和安全验证标准
- 应用软件安全的意识和教育
- 攻击及漏洞的利用

所有被录用的文章都将被发表在Communications in Computer and Information Science (CCIS)系列并将给予ISBN编号。详情请看http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers
会议网站：http://www.ibwas.com

OWASP项目最新消息

Paulo Coimbra, OWASP Project Manager

新项目：

匈牙利文翻译项目

http://www.owasp.org/index.php/OWASP_Hungarian_Translation_Project#tab=Project_Details

RFP– Criteria
http://www.owasp.org/index.php/Projects/RFP-Criteria

新发布

JSReg: JavaScript regular expression based sandbox
https://code.google.com/p/jsreg/
HTML Reg: Java Script regular expression based sandbox for HTML
http://code.google.com/p/htmlreg/

JavaScript regular expression based sandbox for CSS
http://code.google.com/p/cssreg/

OWASP培训

London Training: OWASP projects and resources you can use today May 28th, 2010

London Training: OWASP projects and resources you can use today April 16th, 2010

培训录像链接

http://www.youtube.com/watch?v=pYp-kJTrzCE&feature=player_embedded

ASVS翻译及ESAPI 应用于PHP的项目的最新消息

Mike Boberski

应用安全验证标准(ASVS) 已经被翻译成三种语言：法文，德文，日文。

链接：ASVS Translations

其他正在翻译中的语言：马来文，中文，匈牙利文，波斯文，西班牙文和泰文。

将企业安全应用程式介面（ESAPI）应用于PHP的工程的首期工作已接近完成。现正在进行PEAR兼容，添加phpdoc，以及添加最后的几个控制。

链接：http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=PHP

OWASP 提高应用软件安全的可见度

今年OWASP将集中精力提高应用软件安全的可见度。其使用的方法之一是就是参与由非OWASP组织举行的活动。以下是几个例子。

法国：法国OWASP分会将出席RMML 2010: http://2010.rmll.info/OWASP.html?lang=en

关于RMLL2010:

Libre会议(LSM或RMLL代表法文Rencontres Mondiales du Logiciel Libre)是一个关于免费软件的会议。第一届LSM会议在2000年举行。自2003年每年召开一次，每次在不同的地点召开。啤酒和演讲一律免费:-)。今年的会议将在Bordeaux举行。时间是7月6日至11日。本届会议将主要讨论7个议题，每个议题将分成若干个分会，比如应用软件安全工具和技巧，OWASP Top 10, WebGoat/WebScraba例子等等。

希腊：希腊OWASP分会将出席AthCon会议(http://www.athcon.org/)。会议将在雅典举行，时间是6月3日和4日。OWASP会员可以得到15%的会议注册折扣。

马来西亚：马来西亚OWASP分会将出席2010年马来西亚开源会议。http://conf.oss.my

新加坡：新加坡OWASP分会将支持以下几个会议：

1) ISC2's SecureAsia@Singappore将于7月26和27举行。网站是http://www.informationsecurityasia.com/

2) Singapore Ministry of Home Affairs' GovernmentWare将于9月28至30举行。网站是http://www.govware.sg

斯洛文尼亚：斯洛文尼亚OWASP分会将出席6月15和16日在Maribor举行的OTS 2010会议(http://cot.uni-mb.si/ots2010/)。今年是OTS成立15周年。OWASP将负责会议关于应用软件安全部分。

美国：OWASP代表将在ICCS会议上发表专题演讲。http://www.iccs.fordham.edu/ ICCS是网络安全的国际性会议。会议由美国国家安全局和Fordham大学共同举办。会议将于8月2日至5日在纽约的Fordham法律中心举行。

OWASP Foundation
地址：9175 Guilford Road
Suite #300
Columbia, MD 21046

电话：301-275-9403
传真：301-604-8033
电子邮箱：
Kate.Hartman@owasp.org

免费的和开源的应用软件团

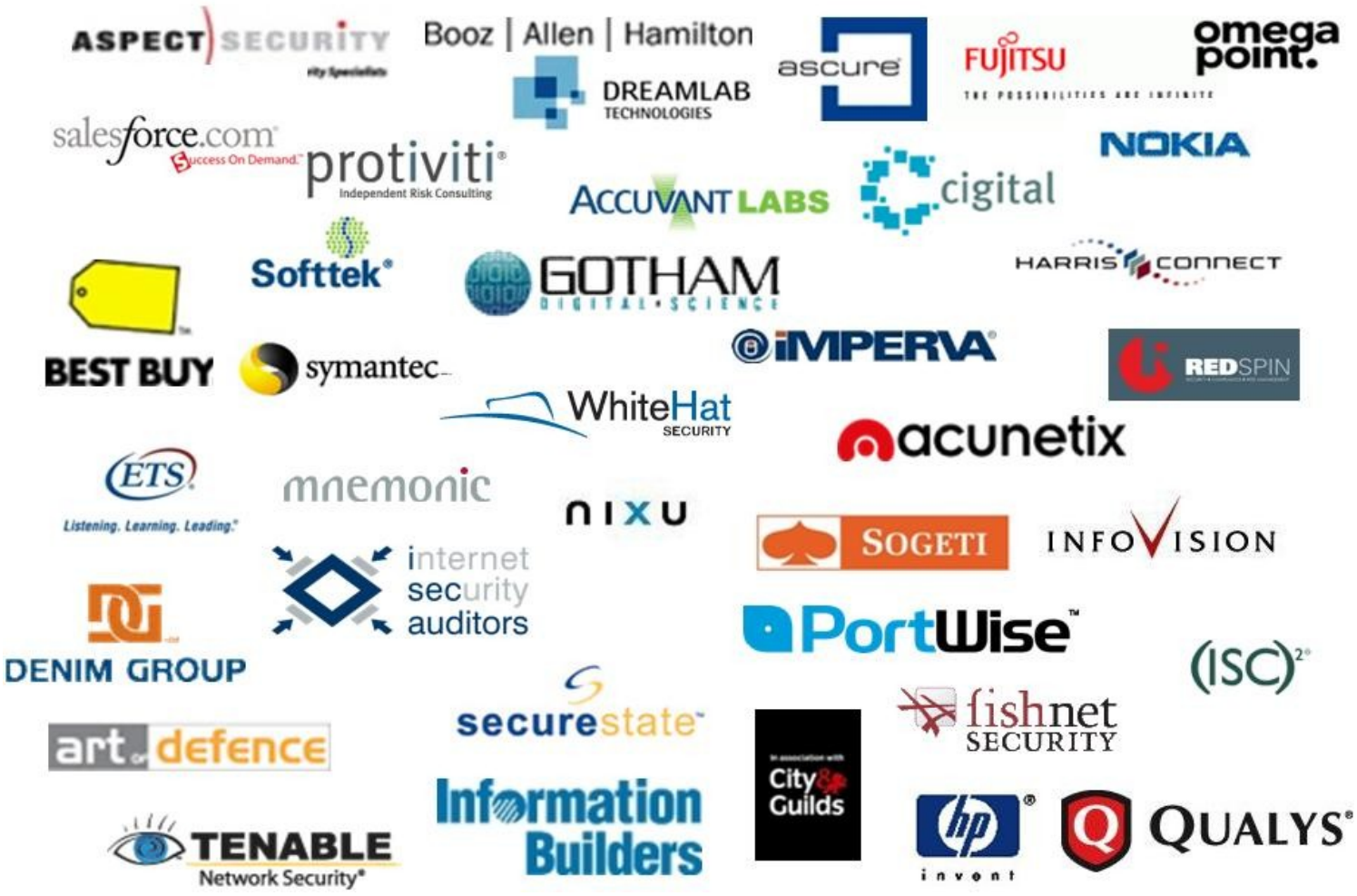
OWASP是一个开源的、非盈利性的组织，致力于帮助企业和组织设计、开发、获取、操作和维护安全的应用系统。为了改善应用软件的安全，OWASP的所有工具、文件、 论坛和分会都是免费和开源的。我们认为应用安全的问题是人、流程和技术的问题。同时处理这三个问题是到达应用安全的最佳途径。OWASP的网址是 www.owasp.org。

OWASP是一个新型的组织。由于没有商业压力，我们可以提供应用安全方面的的公正、实用和有效的信息。

虽然OWASP提倡使用商业技术，但是我们与任何技术公司都没有关联。跟许多开源项目类似，OWASP以合作和公开的方式制作了多种应用安全材料供大家使用。

作为一个非营利组织，OWASP基金为项目的长期成功打下了基础。

OWASP赞助者



编辑: Lorna Alamri 中文翻译: 王颉, 高雯