January 18, 2010

OWASP AppSec 会议

June 21-24, 2010
AppSec Research 2010
Stockholm

OWASP
The Open Web Application Security Project

AppSec USA 2010 大会通知

全球会议委员会高兴地向大家宣布OWASP AppSec USA 2010大会的时间和地点. 大会将在2010年九月7日至10日由加州大学Irvine分校支持. Irvine分校有一所专门的信息和计算科学学院, 这在加州大学系统里是独一无二的. 征集发言人等详情将随后公布.

委员会对Minneapolis分会的出色提案表示感谢. 虽然该地这次没有被选为会址, 我们希望在不久的将来在美国中西部举办活动.

OWASP 2010 研讨会议题征集

OWASP 研讨会议题种类:

同行切磋: 供同行评审的研究论文. 12页以下， LNCS格式.

介绍和演示: 1页简介及screenshot.

演示: 2页简介

http://tinyurl.com/yjv2otg 截稿日期： 2月7日。

IBWAS 09

约40个从业者和几十位学生和老师参加了Iberic Web App Security (IBWAS' 09). 会议于 2009年12月10日和11日在西班牙马德里的Escuela Universitaria de Ingenieriaa Tecnicaa de Telecomunicación， Universidad Politécnica de 举行 。

此次会议取得了巨大的成功. 会议由西班牙及葡萄牙OWASP分部举办. 其目的是促进安全专家、研究员、教育家以及产业界和学术界之间的联系，坦诚交流软件安全的新问题及解决办法。

在讨论政府在互联网应用软件安全中应该扮演什么角色的时候，与会者发言非常热烈。得出了以下几点结论. 这些结论应该在讨论和修改后, 由OWASP作为其建议出版.

1. 我们争取与政府合作, 共同增加互联网应用软件安全的透明度，特别是关于财政，健康和其他对隐私和机密性要求高的系统;
2. OWASP将寻求参与世界各地政府制定安全标准以及测试系统的工作;
3. 我们将帮助政府,民间组织以及公众明确和更新计算机安全法律，让他们在充分了解情况的前提下做出关于应用软件安全方面的决定;
4. 我们要求政府鼓励公司采用应用软件的安全标准，以堵塞安全漏洞, 防止泄密, ，避免非正当交易以及避免法律纠纷;
5. 我们帮助地方和国家政府提高软件安全的可见度.

OWASP 2010 董事会成员

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

OWASP Podcasts Series

Hosted by Jim Manico

Ep 57 David Linthicum (cloud Computing)

Ep 56 Adar Weidman (Regular Expression DOS)

Ep 55 AppSec Justification Roundtable with Boaz Gelbord, Jason Lam, Jim Manico and Jeff Williams

Ep 54 George Hesse

Ep 53 Amichai Shulman (WAF)

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

Have an AppSec job you need posted?

Contact: Kate Hartmann

WASC v2 威胁分类与 OWASP Top Ten 2010 RC1 的对照

Jeremiah Grossman的博客

经Jeremiah Grossman同意引用他的博客 http://jeremiah-grossman.blogspot.com/

“在Bil Corry (@bilcorry)所做的大量工作的基础上, 这是第一次正式把WASC最新发布的威胁分类 v2 和OWASP Top Ten作一一比照。 这将给使用其中一个或同时使用两个文件的人提供帮助。 “

WASC Threat Classification v2	OWASP Top Ten 2010 RC1
WASC-19 SQL Injection	A1 - Injection
WASC-23 XML Injection	
WASC-28 Null Byte Injection	
WASC-29 LDAP Injection	
WASC-30 Mail Command Injection	
WASC-31 OS Commanding	
WASC-39 XPath Injection	
WASC-46 XQuery Injection	
WASC-08 Cross-Site Scripting	A2 –Cross Site Scripting (XSS)
WASC-01 Insufficient Authentication	A3 - Broken Authentication and Session
WASC-18 Credential/Session Prediction	
WASC-37 Session Fixation	
WASC-47 Insufficient Session Expiration	
WASC-01 Insufficient Authentication	A4 - Insecure Direct Object References
WASC-02 Insufficient Authorization	
WASC-33 Path Traversal	
WASC-09 Cross-site Request Forgery	A5 - Cross-Site Request Forgery
WASC-14 Server Misconfiguration	A6 - Security Misconfiguration
WASC-15 Application Misconfiguration	
WASC-02 Insufficient Authorization	A7 - Failure to Restrict URL Access
WASC-10 Denial of Service	
WASC-11 Brute Force	
WASC-21 Insufficient Anti-automation	
WASC-34 Predictable Resource Location	
WASC-38 URL Redirector Abuse	A8 - Unvalidated Redirects and Forwards
WASC-50 Insufficient Data Protection	A9 - Insecure Cryptographic Storage
WASC-04 Insufficient Transport Layer Protection	A10 -Insufficient Transport Layer Protection

OWASP TOP 10 2010 RC1— 最新资料

Dave Wichers

OWASP Top 10 RCI在AppSec华盛顿会议上发表。 评审期于2009年12月31日结束。 项目小组希望在2010年2月4日发布新资料。

详情请参阅网页: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP JBroFuzz

OWASP JBroFuzz项目最近通过了OWASP评估标准2.0。 在2009年12月2日，它的最后版本(JBroFuzz 1.7)以成为一个稳定的版本。

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz_Project_-_Version_1.7_Release_-_Assessment

http://www.owasp.org/index.php/Assessment_Criteria_v2.0

祝贺项目负责人Yiannis Pavlosoglou和队友Matt Tesauro以及Leonardo Cavallari Militelli。 他们最先采用OWASP的新评审标准.

Global Industry Committee 全球产业协会

Colin Watson

产业协会的使命是向公营和私人部门，包括从事开发标准和最优方法的组织, 推广对软件安全的认识和最优方法。 协会拟在OWASP之内为这些组织的代言人。

为此，我们将在条件允许的前提下，经过审核，向外界有关单位作报告并提供援助。

在2009年期间, 北美洲的Rex Booth和David Campbell，欧洲的Georg Hess，Eoin Keary和Colin Watson，跟OWASP董事会代表Tom Brennan一起进行了19项拓展行动，领导或辅导了9份指导性文献，论文和标准，并开始了整理引用OWASP及其项目的外界文献的工作。今年我们有三个新成员，Joe Bernik, Alexander Fry 和 Yiannis Pavlosoglou。 OWASP董事会的新代表是Dave Wichers。我们将更主动地接触从事能源，医疗，财政工作的和政府机构里非技术和安全管理的人事，把OWASP的项目和资源推广给大众。如果OWASP人员已和外单位建立了联系，我们将帮助他们建立两个组织之间的对话。

Key links:

OWASP Global Industry Committee:
http://www.owasp.org/index.php/Global_Industry_Committee

Industry Committee Mailing List
http://lists.owasp.org/mailman/listinfo/global_industry_committee

OWASP Citations:
http://www.owasp.org/index.php/Industry:Citations

OWASP Project Update 新项目

Paulo Coimbra

OWASP Computer Based Training Project *(OWASP CBT Project)*, 项目领导 *Nishi Kumar*

OWASP ModSecurity Core Rule Set Project - ModSecurity 2.0.3即将由Ivan Ristic和Leonardo Cavallari出版。

The OWASP EnDe Project **OWASP**

OWASP Vicnum Project OWASP Vicnum - Release 1.4 (12/31/2009) .

OWASP Content Validation using Java Annotations Project

OWASP Application Security Verification Standard安全验证标准 (ASVS) – 日文和法文版本已经完成。德文和中文版本的翻译工作正在进行.

Reviewers drive: GPC将要发起征集评论员的活动 .

所有资料都将按照OWASP Assessment Criteria 2.0的规定出版。

Membership 会费

个人会员: 767

- 十二月份新会员: 26
- 十二月份继续注册会员: 0
- 十二月份退会会员 (没有继续注册): 9
- 个人会费：$900

团体会员: 27

- 十二月份新会员: 0
- 十二月份继续注册会员: 1 (Nokia)
- 十二月份退会会员 (没有继续注册): 1 (Corporate One Federal Credit Union)

十二月份会费收入：$5,900

Dinis Cruz presenting at IBWAS 09

IBWAS 09 Panel Speakers:

Thank you to Nokia who renewed their support of the OWASP Foundation in December.

NOKIA

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

OWASP是一个开放性的、非盈利的组织，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公开的。 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网址 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，我们与任何技术公司都没有关联。跟许多开放项目类似，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 Organizational Sponsors

时事通讯编辑: Lorna Alamri, 图像: Carlos Serrao, 中文翻译: Helen Gao, 高雯