2010年12月

OWASP AppSec 会议

2010年12月1日－2日
BeNeLux 2010
埃因霍温, 荷兰

2010年12月16日－17日
IBWAS ‘10
里斯本, 葡萄牙

2011年2月8日－11日
OWASP Global Summit 2011
里斯本, 葡萄牙

AppSec EU,
都柏林
2011年6月

AppSec USA
明尼阿波利斯
2011年9月19日－23日

OWASP
The Open Web Application Security Project

2011年美国OWASP AppSec大会—明尼阿波利斯

感谢IBM成为2011年美国AppSec大会的第一个赞助商，我们将其封为金牌赞助商。

请准备好你的论文。论文投稿将于2011年3月15日截止。

我们将很快开放 http://appsecusa.org 网址。

IBWAS ‘10
Carlos Serrao

IBWAS ‘10, 第二届OWASP伊比利亚美洲Web应用安全大会将于2010年12月16日和17日在葡萄牙里斯本举行。大会将在里斯本大学的ISCTE举办。相关的培训于16号进行，会议在17号进行。

该会议致力于将应用安全专家、研究人员、来自行业与学术界的实践者和教育人员、以及国际性的社团，比如OWASP，聚集在一起，以探讨应用安全领域的开放问题和新的解决方案。在会议内容方面，学术界的研究人员可以将有趣的研究结果与经验丰富的业界人士和软件工程师相探讨以进行结合。

2011年OWASP峰会
Tom Brennan

2011年OWASP峰会逐渐临近，http://www.owasp.org/index.php/Summit_2011。如果你已加入OWASP有一段时间的话，你可能还记得我们在2008年OWASP峰会上宣布的OWASP选举以及在2009年11月11号举行的2009年OWASP峰会。

* 请见Wiki提醒档案：http://www.owasp.org/index.php/Board_member

下一选举循环将于在2011年11月11日举行的OWASP峰会上开始进行。下一峰会仍由现任的OWASP成员组织举行。http://www.owasp.org/index.php/Membership#Categories_of_Membership_.26_Supporters

如果你想成为一名竞选者，我们希望你满足前提条件，并鼓励你在今天就加入OWASP的全球委员会！http://www.owasp.org/index.php/Global_Committee_Pages.

OWASP Podcasts Series

由Jim Manico主办

Ep 77 Rafal Los

Ep 78 AppSec Roundtable with Jeff Williams, Andrew van der Stock, Tom Brennan, Samy Kamkar, Jeremiah Grossman and Jim Manico (Complete Chaos)

Ep 79 Tony UV (Threat Modeling)

在Twitter上跟随OWASP @OWASP

OWASP项目更新

Paulo Coimbra

自上次新闻通讯发布了OWASP相关项目后， 关于项目的最新进展请查看以下信息。

1. OWASP项目总体新闻

1.1—ASVS项目的领导人职位已处于申请过程中，并得到了OWASP社团的热情回应—已有五位候选人表示出了领导或共同领导这个OWASP旗舰项目的兴趣。目前，全球项目委员会正制作相关推荐，以供OWASP董事会决定。

http://www.owasp.org/index.php/Request_For_Proposals/Seeking_New_Project_Leader_For/ASVS

1.2—在记录的时间中，**OWASP安全编码实践—快速参考指南**，已进行了第三个版本的评估，并被评定为稳定质量的等级。我们感谢并祝贺该项目负责人，Keith Turpin，以及相关的评审人员和编撰人员。

http://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

1.3—由Michael Coates领导的**OWASP AppSensor项目**, 有了重要的进展（新的工具），目前正处于评审阶段，其评审目标是稳定发布等级。

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

1.4—由Dinis Cruz领导的**OWASP O2平台项目**, 有了重要的进展（新的发布），目前正处于评审阶段，其评审目标是稳定发布等级。

http://www.owasp.org/index.php/OWASP_O2_Platform

1.5—**OWASP JBroFuzz项目**有了最新领导人。 我们感谢Yiannis Pavlosoglou对于推动该项目发展所作的所有贡献，欢迎并衷心祝愿新的领导人，Ranulf Green。

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

2. 新近建立的项目

2.1—OWASP统一报告指南，由Vlad Gostomelsky领导。

该项目将补充完善OWASP测试指南以及OWASP的RFP模板。这将是一个免费的报告模版，其基于了行业的最佳实践，并希望成为事实上的标准。

- http://www.owasp.org/index.php/OWASP_Uniform_Reporting_Guidelines

2.2—OWASP Zed攻击代理项目, 由Psiinon领导。

该项目提供了一个易于使用的集成渗透测试工具，以测试Web应用，并提供了自动扫描仪，以及一套工具让您手动找到安全漏洞。

- http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Project_About

2.3—OWASP安全Web应用框架声明，由Rohit Sethi领导。

这个项目是一个详细描述的安全需求的文档，以便让Web应用框架的开发人员遵守。

-http://www.owasp.org/index.php/OWASP_Secure_Web_Application_Framework_Manifesto

2.4—OWASP移动安全项目，由Jack Mannino和Mike Zusman领导。

OWASP移动安全项目将帮助社区更好的了解出现在移动应用中的风险，并教导大家防御这些风险。

-http://www.owasp.org/index.php/OWASP_Mobile_Security_Project

2.5—OWASP Fiddler Addons安全测试项目，由Chris Weber领导。

该项目（又名OWASP FAST）包括两个互补的项目：**看守人项目**，一个被动的漏洞扫描器；**X5S项目**，一个主动的XSS测试和输入/输出编码检测。

-http://www.owasp.org/index.php/OWASP_Fiddler_Addons_for_Security_Testing_Project

2.6—OWASP应用安全技能评估，由Neil Smithline领导。

该项目（又名OWASP ASSA）是一个在线的多项选择小测试，以帮助个人了解他们在特定应用安全技能方面的强项与弱项。

-http://www.owasp.org/index.php/OWASP_Application_Security_Skills_Assessment

2.7– OWASP浏览器安全项目，由Dave Wichers和Michael Coates初始创建。

该项目依然没有明确项目领导人，但是以上提到的两人已为该项目做出了很多的贡献。最终决定将尽快宣布。

http://www.owasp.org/index.php/OWASP_Browser_Security_Project#tab=Project_About

3. 即将成立的项目:

3.1 – OWASP ESAPI Objective C

3.2—OWASP PASSWD

3.3—OWASP Eclipse plug-in

4. 即将重新成立的项目:

所有关于跨站请求伪造攻击（CSRF）相关的内容。

OWASP Open-sourcing JXT

OWASP A10-Unvalidated Forwards

ESAPI

* .Net ESAPI项目的最新领导人 — Michael Weber。
* Java ESAPI项目目前正处于代码审核阶段，其审核通过的目标是总体可用发布等级。

OWASP Top 10的西班牙语和意大利语版本现已发布

2010年版的OWASP Top 10现已被翻译成西班牙语版。感谢翻译团队的以下成员为我们带来的成果：
团队领导：Fabio Cerullo (左边第一个)
团队成员： Juan Carlos Calderon (左边第二个)，Rodrigo Marcos (中间)，Vicente Aguilera (右边第二个)， Edgar Sanchez (右边第一个) 。其他没有提供照片的成员: Daniel Cabezas Molina, Jose Antonio Guasch, Paulo Corondo。

你可以通过以下链接找到相应的PPT和PDF版本：

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Spanish_Translation

意大利语版本链接:

http://www.owasp.org/images/f/f9/OWASP_Top_10_-_2010_ITA.pdf

非常感谢更新了对OWASP基金赞助的合作伙伴。

mnemonic
-securing your business

11月和12月的最新合作赞助商：感谢你们的支持！

ADP

AppliedTrust

ORACLE

OWASP正在为www.owasp.org（网页）寻找一个新家。如果您有意负责web服务器，请通过该电子邮件owasp@owasp.org获得更多信息。

OWASP培训模式

Sandra Paiva

通过努力，我们正制作一个稳定而巩固的OWASP培训模式，以作为一个强大的工具来传播OWASP的的知识和信息。OWASP正寻找培训教导人员以参与旗下的“今天你可以使用的OWASP项目和资源”活动。这种培训模式针对OWASP会员免费，并由OWASP的项目领导人（赞助旅行的费用）进行覆盖OWASP模块和/或项目的培训。如果你是一位OWASP的项目领导人，并希望将你的信息添加入OWASP的培训教导人员名单，这就是你的机会，把你的姓名和信息添加进入OWASP培训教导人员数据库吧！

现在就成为一名OWASP培训教导人员吧！点击此处查看相关数据库和条款：http://www.owasp.org/index.php/OWASP_Training#tab=Trainers_Database_-_Call_for_Trainers.21

预知所有关于OWASP培训活动，请查看：http://www.owasp.org/index.php/OWASP_Training。

1. **OWASP大学校园计划**, 由Jeff Williams领导。 该项目的创建宗旨是将应用安全引入全世界的大学校园课程。

2. **OWASP 炼金术士项目**, 由Bishan Singh, Chandrakanth Narreddy和 Naveen Rudrappa共同领导。该项目允许软件开发团队在高度安全的情况下，对防御软件内置防御/控制以针对安全有关的设计、编码和执行漏洞的认知。

第一届OWASP中国大会

高雯

第一届OWASP中国大会已于2010年10月20号至23号在北京举行。 超过500人参加了此次盛会。 OWASP的董事会成员Tom Brennen为此次大会揭开了序幕。来自美国、中国大陆、台湾、香港、新加坡等地区的信息安全专家陈述了关于最重要安全问题的最新信息。来自Forester的分析师王晨曦博士和OWASP的项目负责人Pravir Chandra做了发言。由于这次大会非常成功，我们预计在明年安排另外一次会议。

第一个乌拉圭OWASP日

乌拉圭的第一个OWASP活动在2010年12月9日举行。Mateo Martinez，Mauricio Campiglia和Cristian Borghello做了相关的演讲。更多信息请浏览：http://www.owasp.org/index.php?title=OWASP_Day_Uruguay_2010

感谢Mateo Martinez，Fabio Cerullo，Roberto Ambrosoni 和Kate Hartmann对于此次活动的组织。

OWASP 夺旗项目

Steven van der Baan

今年的夺旗项目分为8个分开的活动（从瑞典斯德哥尔摩的AppSec-EU 到新加坡的GovCert和埃因霍温的OWASP BeNe-Lux ）。夺旗项目现在有了自己的标志（http://www.owasp.org/images/8/87/CTFLogo.jpg）并收到了一套完整的框架以支持夺旗活动。该框架将很快发布。Steven van der Baan以替代Martin Knobloch作为此次夺旗项目的新领导人。

OWASP Modsecurity CRS v2.0.9

Ryan Barnett

我很高兴宣布OWASP ModSecurity Core Rule Set (CRS) v2.0.9版本现已发布。

最显着的变化是，用户现在可以轻松切换传统的或异常的评分检测模式。http://blog.modsecurity.org/2010/11/advanced-topic-of-the-week-traditional-vs-anomaly-scoring-detection-modes.html

改进：

- 将主要的config文件名字修改为 modsecurity_crs_10_config.conf.example，因此，将不会重写现有的配置设定。用户应更改该文件的名字以激活它。 - 传统的检测模式现已成为默认方式。 - 用户现在可以通过修改 modsecurity_crs_10_config.conf 文件，以轻松切换传统的或异常的评分检测模式。
- 更新了大多数规则的破坏性行动，用“阻止”代替“通过”的行动。这允许了传统的或异常的评分检测模式切换。
- 从绝大多数的规则中删除了注册行为，以便从SecDefaultAction的设置去控制modsecurity_crs_10_config.conf文件。
- 更新了modsecurity_crs_10_config.conf文件的异常分数，以针对使用了的PHPIDS规则做更贴近的比对。这些仍然有同样的因素，即使这些数字本身较小。
- 更新了第49和第59阻塞规则，包括了已匹配的数据。
- 更新了TAG数据以再次对于攻击或漏洞进行分组。
- 更新了SQL注入式攻击的过滤器以检测更多的布尔逻辑攻击。
- 将一些文档移到了optional_rules 目录下（phpids, Emerging Threats rules）。

修复的Bug:

- 已修复的规则ID 960023，在 optional_rules/modsecurity_crs_40_experimental.conf中缺少一个单引号 https://www.modsecurity.org/tracker/browse/CORERULES-63
- 在连锁规则中将所有的skipAfter动作移到了规则的起始行（必须有ModSec v2.5.13或更高版本） https://www.modsecurity.org/tracker/browse/MODSEC-159
- 修复受宏扩展限制的文件扩展名bug。 https://www.modsecurity.org/tracker/browse/CORERULES-60
- 在第49和第60文档中更新了SQLI TX变量宏扩展数据，已与SQL注入配置文件设定相匹配。
- 修复在SQL Injection regexs中的拼写错误—对于单词boundary缺少的反斜线符号(\b)。 https://www.modsecurity.org/tracker/browse/CORERULES-62

2010年11月OWASP网页数据统计

访问量：258, 568

网页查看量：654,677

平均在线时间：00:03:03

新访问百分比：58.28%

Mark Bristow在AppSec DC

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

电话: 301-275-9403

传真: 301-604-8033

电子邮件:
Kate.Hartman@owasp.org

免费的和开源的应用软件团体

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组织赞助商

编辑: Lorna Alamri， 参与人员: Leonel Navarro 和 Jayanthi Srinivasan，中文翻译：王颉