

2010年7月17日



# OWASP

The Open Web Application Security Project

## 应用程序安全大会



**2010年9月7日-10日 美国加州欧文** 开始注册! <http://www.appsecusa.org/register-now.html>



**2010年9月16日-17日 爱尔兰都柏林**

开始稿件和培训征集 - [http://www.owasp.org/index.php/OWASP\\_IRELAND\\_2010#Call\\_for\\_Papers](http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers) 开始注册 - [http://www.owasp.org/index.php/OWASP\\_IRELAND\\_2010#Registration](http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration)



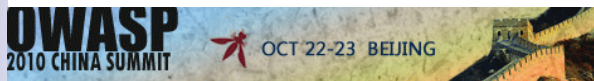
**2010年10月20日-21日 美国纽约州罗彻斯特** 开始征稿 - <http://www.rochestersecurity.org/call-for-presentations>



**OWASP**  
AppSec Germany  
20.10.2010

**2010年10月20日 德国纽伦堡**

开始征稿 - [http://www.owasp.org/index.php/OWASP\\_AppSec\\_Germany\\_2010\\_Conference#tab=Call\\_for\\_Papers\\_-\\_English\\_Version](http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version)



**2010年10月22日-23日 中国北京** 开始稿件和培训征集 - <http://www.owasp.org/index.php/>

OWASP China Summit 2010#tab=Call For Paper 在线注册 - [http://www.owasp.org.cn/index.php?option=com\\_rsform&Itemid=80](http://www.owasp.org.cn/index.php?option=com_rsform&Itemid=80)



**2010年10月29日 美国德州奥斯汀**

开始征稿 - [http://www.owasp.org/index.php/Lonestar\\_Application\\_Security\\_Conference\\_2010#tab=Call\\_for\\_Papers](http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers)



**2010年11月8日-11日 美国华盛顿市**

开始稿件和培训征集 - [http://www.owasp.org/index.php/OWASP\\_AppSec\\_DC\\_2010#tab=CFP](http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP)

开始注册 - [http://www.owasp.org/index.php/OWASP\\_AppSec\\_DC\\_2010#tab=Registration](http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration)



**2010年11月11日-12日 葡萄牙里斯本**

开始征稿 - [http://www.owasp.org/index.php/IBWAS10#tab=Call\\_for\\_Papers](http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers)



**OWASP AppSec Brasil 2010**

**2010年11月16日-19日 巴西圣保罗州坎皮纳斯**

开始稿件和培训征集 - <http://www.owasp.org/index.php/>



## OWASP Podcasts Series

Hosted by Jim Manico

Ep 72 [Interview with Ivan Ristic \(WAF\)](#)

Ep 73 [Jeremiah Grossman and Robert Hansen](#)

非常感谢我们的合作伙伴在今年6月和7月更新了对OWASP的赞助。



## 对话Matt Tesauro

### Lorna Alamri

OWASP最特别的地方之一，是它为那些热衷于应用程序安全的人提供了一个论坛平台。

Matt Tesauro是LiveCD项目的领导者。参加OWASP，为他的事业带来了帮助，并增加了他基于OWASP的安全知识以及关于应用程序安全的意识。

### 你为什么决定做第一个LiveCD?

我制作的OWASP LiveCD是2008年OWASP夏季代码活动（SoC）的一部分。我收到了来自OWASP关于SoC的电子邮件。当我了解到这是一个关于Linux和应用程序安全相融合的项目时，我知道这正是我想要的，因为这两样东西都是我最喜欢的。

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

LiveCD的最初目标是赶在SoC截止日前做好一个。；)

事实上，我试图收集最好的应用程序工具以整理到一个便于使用的工具包中。我一直专注于关于应用程序安全的工具，而不是做一个普通的“黑客”工具光盘。

自从2008年9月的第一个版本后，LiveCD已经发生了翻天覆地地改变。第一个大变化是将LiveCD分成了几个小项目。其中一个是对VMware和VirtualBox的虚拟安装。我们也得到了一个可以在USB驱动器上工作的虚拟机，但非常缓慢。

事实上，它的增长远远不只是一个LiveCD。出于这个原因，最新的版本已更名为OWASP Web测试环境（WTE）。我们已经在OWASP LiveCD的基础上，从SLAX迁移到Ubuntu Linux操作系统，并为WTE中所有的工具创建了独立、分开的安装包。

最大的改变是将允许以更容易的方式从安全专家手上获得测试工具。有了最新的软件包，你可以采用一个标准的Ubuntu安装，并指向WTE库，在几分钟内，安装所有已安装的WTE工具。

### 这个项目是如何发展的？

正如我上面提到的，它从一个可以启动的CD演变为一个获得你想要的工具的不同方法束。当我们完成从SLAX到Ubuntu的迁移时，我们将有许多为最终用户获得WTE的不同方法：

- Live CD
- 虚拟安装 (VMware, VirtualBox, Parallels, ...)
- 在已有的Ubuntu安装中添加安装包
- 存在U盘中的WTE
- Wubi—一个不需要分区就可以双重启动Windows和Ubuntu的方法
- 自定义的版本，例如：Java静态工具集合，工具和攻击目标版本，等等
- 全新种类的工具，例如静态分析工具

我也为有其他几个人对该项目做出贡献而感到幸运。Nishi Kumar为发布制作了图片。Brad Causey 和Drew Beebe也为项目贡献了很多很多时间。他们值得为他们所提供的帮助而被提及感谢。

我必须得承认，自从我搬到Trustwave的SpiderLabs，我花了很多时间去适应这个新且美好的办公地点，然后才去更新该项目。我很高兴与SpiderLabs工作人员的合作，并花了更多的时间讨论，然后为WTE制作了Debian软件包。虽然从来没有害怕过，但我发现自己常常为一个虚拟的WTE安装工作而感到恼火，所以这只是我重新开始去做以前的一个时间问题。

### LiveCD上最受欢迎的应用程序是哪个？最有争议的是哪个？你最喜欢的又是哪个？

漫漫的过程中，在LiveCD上评论最多的、问及可能使用的应用程序是WebGoat。我觉得有这样一个事实：WebGoat只是一个在准备好以前能快速启动，并为许多正在学习应用程序安全或授课的人提供的一个巨大恩惠。

我不确定添加了一个真正意义上存在争议的应用程序，或许Metasploit在严格意义上并不是一个Web应用程序安全工具。另外，我对Maltego CE是一个封闭源试用版而感到忧伤。Maltego的销售用于维持该软件作者的生计，因此我不反对他。

至于我最喜欢的一个—我讨厌只挑选一个出来。我经常使用的有WebScarab, Burp Suite, JBroFuzz, Nikto和DirBuster。还有一些最新喜欢上的工具，将添加在即将发布的最新WTE之中。

**如果你知道你现在知道的这些，你会做些什么不同？**

我非常喜欢使用SLAX制作LiveCD。它对该项目非常好。但是，我们延长了虚拟机的时间，并试图动态更新LiveCD，可惜它不太合适。

所以，如果我需要做什么，我会从一个适当版本的Linux包管理系统开始。Debian有已经工作了多年的管理软件包，为什么不直接使用它呢？顺便说一句，RPM也是一种很好的包管理系统。如果你有一个RPM向导，我很乐意和你一起从.deb包获得RPM。

**你开始做LiveCD项目时的最大挑战是什么？**

我最初的挑战之一是将工具的数量保持在一个合理的范围内。我从寻找各种应用程序安全的工具开始，并获得了一个超过330个工具清单。我花了很长一段时间对这些工具进行筛选，以获得一个理智的数目。此外，学习如何正确地创建包是一个痛苦的前期工作，但一旦你掌握了它，你就可以在有新版本的工具创建时自动更新工具包，从而获得长期的收益。

**你为什么觉得Live CD 成功了？**

我上次统计下载次数是在2009年11月，自首次SoC发布以来，共有超过33万次的下载次数。这对于了解OWASP和应用安全的人来说，是一个巨大的数字。我还了解到有一些老师使用它用于相关的培训课程。最令人惊奇的发展之一，是该OWASP LiveCD在一所大学被列入案文。在几个星期以前的斯德哥尔摩欧盟AppSec大会上，有一位参会者认出了我，并为最新的WTE发布向我表示感谢，所以我怎么能抱怨呢？

**这个LiveCD项目是如何影响你的职业生涯的？**

首先，积极参与OWASP的作用是巨大的。对我而言，OWASP的LiveCD是进入OWASP社区的一个好

的方式。由于我完成了LiveCD项目，我去了葡萄牙、波兰、巴西和美国的很多地方。我遇到了OWASP的许多出色人物，从而将我的名字打入了应用程序安全社区。

我也相信通过LiveCD的工作，和来自全球项目委员会的帮助，使我成为了一名OWASP基金会的董事会成员。帮助其他OWASP董事会成员完成OWASP任务工作，是一种难得的经验。

在务实的层面上，我也多次作为一名为LiveCD提供培训的有薪培训师。提到它说明我对OWASP的积极参与，而参与OWASP董事则是更加有益的。我确定，我的OWASP经验是我在Trustwave SpiderLabs目前位置上的重要因素。

**下一步的计划是什么？**

对于WTE，我想增加贡献者的数量，这样我就不会成为一个瓶颈，就象我在今年早些时候那样。我还想扩大部分WTE包，包括静态分析工具、Flash工具和其他可能的一些脆弱应用程序。

至于我在OWASP委员会的作用，我正积极的在运行OWASP操作的基础设施上工作。但愿，OWASP将有一个新的企业级基础设施，以帮助推动整个社区到一个新的成功等级。

**还有其他什么你想和该项目的拥护者分享吗？**

我不能对这些说得太多，不然会很容易找到相关的证书，常见的开源许可证有GPL，Apache或BSD。需要搞清楚的是，如果我可以将工具安全地收集在WTE中，那会比我的预期更加痛苦。你想象不到我下载和探索了多少项目，在这以前，我又是如何找到相应证书的。

需要告诉项目拥护者的是请将反馈信息、建议、投诉或其他任何事通过邮件列表或项目论坛发送给我们。让项目变得更好的最好方式，是让我们知道项目之中什么工作和什么不工作。

**6月和7月的最新合作赞助商。**

**感谢你们的支持！**





## 跟随OWASP

### OWASP的 Twitter feed

[http://  
twitter.com/  
statuses/  
user\\_timeline/  
16048357.rss](http://twitter.com/statuses/user_timeline/16048357.rss)

你可以帮助  
OWASP让每个应  
用程序开发人员拥  
有OWASP Top  
10的知识吗？  
分享以下链接：  
[OWASP Top 10 - 2010.pdf](#)

## ESAPI的最新进展

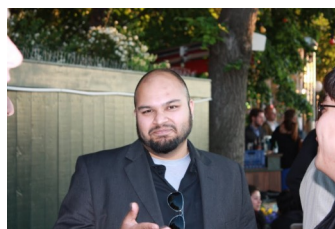
### Jeff Williams

美国国家安全局（NSA）已经表示愿意对ESAPI进行深入的安全审核，并提供结果。对于那些不了解NSA的人，NSA使命的重要组成部分是国防。在过去，NSA赞助支持了国家计算机安全大会，创建了彩虹系列，并资助了SSE—CMM。最近，他们已经参与了SCAP和SE-Linux项目。

支持OWASP的NSA团队在密码学和应用程序审核方面已经很有经验，他们将很快开始他们的工作。他们将重点放在第一个版本的Java ESAPI，并在他们准备好时可能支持其他语言版本，这意

味着他们的密码技术至少在Java 2.0水平。他们对审核工作的初步估计是需要数月时间才能完成。

我对这方面的进展感到非常兴奋，我将持续为你报告他们的进展。



## OWASP项目最新消息

### Paulo Coimbra, OWASP Project Manager

#### 新项目

[http://www.owasp.org/index.php/Projects/  
ESAPI\\_Swingset-](http://www.owasp.org/index.php/Projects/ESAPI_Swingset-)

[http://www.owasp.org/index.php/Projects/  
Owasp\\_Esapi\\_Ruby](http://www.owasp.org/index.php/Projects/Owasp_Esapi_Ruby)

[http://www.owasp.org/index.php/  
OWASP\\_Application\\_Security\\_Program\\_for  
\\_Managers](http://www.owasp.org/index.php/OWASP_Application_Security_Program_for_Managers)

#### 最近新发布的项目

[http://www.owasp.org/index.php/  
OWASP\\_JavaScript\\_Sandboxes](http://www.owasp.org/index.php/OWASP_JavaScript_Sandboxes)

#### 需要贡献者的新项目

[http://www.owasp.org/index.php/  
Cate-  
gory:OWASP\\_Testing\\_Project#tab=Project\\_  
About \(Testing Guide V 4.0\)](http://www.owasp.org/index.php/Cate-gory:OWASP_Testing_Project#tab=Project_About)

再次发布的项目[http://www.owasp.org/  
index.php/  
OWASP\\_Related\\_Commercial\\_Services](http://www.owasp.org/index.php/OWASP_Related_Commercial_Services)

#### OWASP ESAPI Swingset项目的新领导者

Cathal Courtney. 让我们欢迎他吧！

[http://www.owasp.org/index.php/  
ESAPI\\_Swingset#tab=Project\\_About](http://www.owasp.org/index.php/ESAPI_Swingset#tab=Project_About)

该项目已经发布的版本为 ESAPI Swingset RC 4, 敬请浏览！

[http://www.owasp.org/index.php/Projects/  
ESAPI\\_Swingset/Rzeleases/Current](http://www.owasp.org/index.php/Projects/ESAPI_Swingset/Rzeleases/Current)



5月份网站访问量: 233,765

网页访问量: 573,144

网页/网站访问: 2.45

访问平均时间: 00:02:57

58.3% 新访问者

<http://conf.oss.my>

内容概观:

[/index.php/Main\\_Page](/index.php/Main_Page) 有63,070 次网页访问

</index.php/>

Category:OWASP\_Top\_Ten\_Project 有21,610

次网页访问

</index.php/>

Category:OWASP\_WebScarab\_Project

有16,615次网页访问

[/index.php/Category:](/index.php/Category:OWASP_WebGoat_Project)

OWASP\_WebGoat\_Project

有13,502 次网页访问

## OWASP O2 平台

### Dinis Cruz

我很高兴宣布我终于发布了OWASP O2 平台的第一个主要版本（包括一个安装文件，文档+视频和一组关键或特殊的功能）。

这里有一个全新的GUI，很大的不同是在O2内部查找可用的代码、工具和APIS（如果你用过以前的版本，那么你将非常欣赏这种）。你可以看到新的GUI，并可以通过以下链接下载：[http://www.o2platform.com/wiki/O2\\_Release/v1.1\\_Beta](http://www.o2platform.com/wiki/O2_Release/v1.1_Beta)。

**请试用它**，并提供以下这些反馈信息：你喜欢什么，什么工作，什么不工作，什么需要改进，等等（如果你想报告一个bug，请使用以下网页<http://code.google.com/p/>

[o2platform/issues/list](http://www.o2platform.com/wiki/O2_Release/v1.1_Beta)）。

这个版本的O2有足够的功能+能力+力量，我终于有信心把这个直接展示给你，不管你从事于什么样的网络应用程序安全领域中，O2脚本/模块/工具都将让你的工作更有效率。

由于更新了GUI，大多数提供的文件和视频基于了以前的GUI。但因为我现在可以使用O2轻松地创建详细的wiki文件和/或视频，我的计划就是通过这种方式来回答你的问题（比如使用视频或wiki页面）。

## OWASP AppSec Research大会总结

### John Wilander

2010年6月21日至24日，扩大规模的欧洲OWASP AppSec会议在斯德哥尔摩召开。瑞典、挪威和丹麦三个分会连同斯德哥尔摩大学共同主办该活动，共有275名与会者在阳光灿烂的斯堪的纳维亚半岛齐聚一堂。

大会头两天在安全开发方面提供了培训、笔记、恶意软件分析和架构审核的活动。在星期一晚上的联合晚宴上，美国嘉宾学会了如何用刀叉吃汉堡—这是瑞典人的强项:)。

会议安排有三个不同的范围，并有来自业界和学术界的讲座和演示。主题演讲讲述了关于未来浏览器的安全和自上世纪90年代以来SDL的发

展。并从12家赞助商中授予了微软为钻石赞助商。

在周三晚上，与会人员和其他一些重要人物一起，参加了在斯德哥尔摩市政厅举行的欢迎宴会，其中包括了三个盛大晚宴。一个非常棒的社区庆祝活动由Google赞助。在晚宴上，大家通过三种不同类别的比赛—文化，才能和艺术，来获得香槟。最后的挑战是用管道清洁剂制造一个有OWASP灵感的塑像。这项活动引发了不少创意。或者是酒在作怪？

组织者要感谢那些支持并参加了第一届OWASP AppSec研究大会的人。明年在都柏林再见！

你在寻求应用软件安全方面的工作吗? 请查看 [OWASP Job Page](#)

你需要招聘应用软件安全方面的人才吗?

请联系:

[Kate Hartmann](#)

## 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 and 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](http://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 Organizational Sponsors

