立即发布

OWASP TOP 10 - 2010 版 正式发布

你可以帮助我们将其送到世界上所有程序员手里吗？

哥伦比亚，马里兰州 2010 年 4 月 9 号

从 2003 年以来，开源 web 应用安全项目（OWASP）遍布全球的应用安全研究人员和专家开始仔细监测 web 应用安全的状况，并且撰写了一个被全球各个组织，包括 PCI, DOD, FTC 和其他无数组织，广泛认可和依赖的文档，以提高人们对应用安全的关注。

今天, OWASP 发布了一个更新的报告，用以介绍 web 应用程序在企业使用中 10 项最严重的风险。这 22 页彩色的报告充满了例子和细节，用以对软件开发人员，管理人员，和任何对 web 安全感兴趣的人解释这些风险。OWASP 的所有资源都是免费和开放的，你可以到如下链接免费下载最新的 OWASP Top 10 报告:

http://www.owasp.org/index.php/Top_10

Dave Wichers, OWASP 董事会成员和 Aspect Security 公司的 COO, 从项目的创建期就开始管理这个项目。“今年我们重新修改了 Top 10，以明确我们是在讨论风险，而不是仅仅在讨论漏洞。在没有上下文的情况下试图对漏洞进行优先级的排序并没有意义。如果不了解对商业的威胁和影响，你没法做出正确的商业决定。” 对风险的最新关注是为了让各个组织对其内部的应用安全能够有更成熟的理解和管理。

是让对应用安全的认识走出安全社区，直接走进那些最需要了解它的人群的时候了。今年, 我们大胆的提出把 OWASP Top 10 送到**世界上每一个 web 开发人员**手里 – 但是我们需要你的帮助. 我们请求阅读这个文档的每个人: 你愿意为了帮助保护互联网的将来做一件简单的事情吗？如果你认识一个写 web 代码的人, 你可以将 OWASP Top 10 传给他，并且善意的询问他...

你对 OWASP Top 10 列举的所有的风险熟悉吗?

你今天可以做一个承诺：保护你的代码不存在 OWASP Top 10 所列举的风险吗？

在很长的时间里面，很多组织仅仅依靠偶尔的扫描或者入侵测试来保证他们内部和外部 web 应用程序的安全。这样的方法很昂贵而且并不能够提供足够的覆盖面。就像其他类型的安全，要提高应用安全，必须建立一个风险管理程序，在整个企业内所有程序和决策控制里提供应用安全的可视度。如果你的组织准备解决应用安全问题，OWASP 提供很多免费的书籍，工具，项目，论坛，邮件列表，以及其他很多资源。你可以参加遍布全球的 180 个分会，或者出席我们高质量而且不昂贵的应用安全（AppSec）大会。

2010 年版的 OWASP Top 10 是:

A1: 注入
A2: 跨站脚本 (XSS)
A3: 失效的认证和会话管理
A4: 不安全的直接对象引用
A5: 跨站请求伪造 (CSRF)
A6: 安全配置错误
A7: 不安全的密码储藏
A8: 限制 URL 访问失败
A9: 传输层保护不足
A10: 尚未认证的重定向和转发

和以往的版本相比，2010 年的更新采用了更多关于 web 应用漏洞的信息源来决定最新的 Top 10。新版将这些信息用更简洁，更具有说服力，和更方便使用的方式表现出来，同时提供了很多新的开源资源的链接，可以用来帮助解决各个问题，特别是 OWASP 最新的企业安全 API (ESAPI) 和 应用安全验证标准 (ASVS) 项目.

关于 OWASP

开源 web 应用安全项目（OWASP）是一个全球范围的免费和开放性社区，致力于解决应用软件的安全问题。我们的使命是提高人们对应用安全的关注，帮助人们和各个组织理解应用安全的真正风险，做出正确的决定。任何人都可以免费参加 OWASP，我们所有的资源都是免费和开源的。OWASP 组织是一个 501c3 非营利慈善组织，以保证我们的会员可以持续的获得我们的资源，并且支持我们的工作。我们的会员包括：个人, 组织支持者 和 学院支持者.

面试: Jeff Williams – OWASP 主席及 Top 10 项目创建人 (jeff.williams@owasp.,org)
面试: Dave Wichers – OWASP 董事会成员及 Top 10 项目领导人 (dave.wichers@owasp.org)
联系人: Lorna Alamri – 联系委员会 (lorna.alamri@owasp.org)
公司名称: 开源 Web 应用安全项目 (OWASP)
网址: http://www.owasp.org

# # #