atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

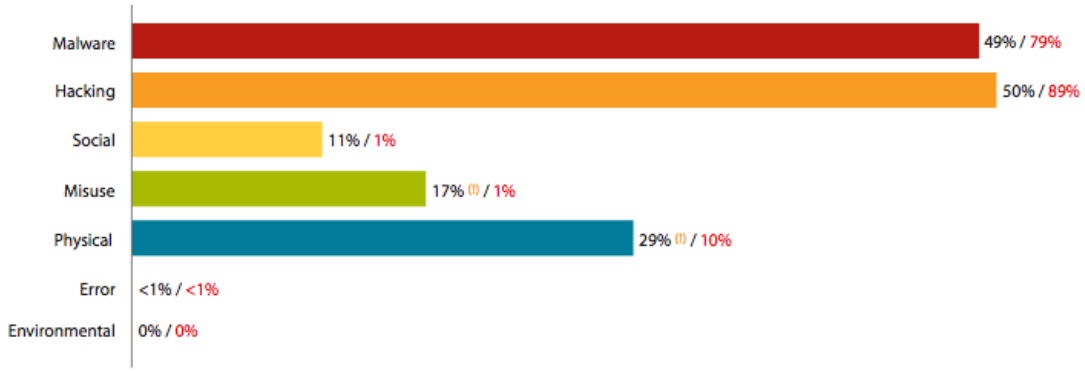
借助优秀业界实践经验，提升应用开发的安全性

atsec 高级咨询顾问 高向东

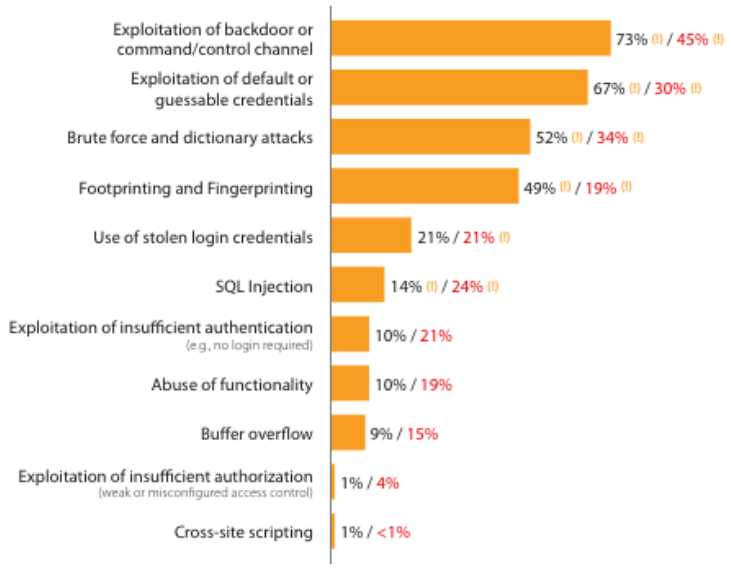
关键词： 应用安全 安全编码 安全性测试

一、实现应用安全开发的意义

当前越来越多的互联网应用通过 B/S 架构来实现，使得互联网的开放程度不断扩展，尤其是随着 web2.0 技术（如 Blog、twitter 等）的迅猛发展和普及，应用和内容的开放性得到空前的扩展。然而，不断开放的互联网应用也面临着越来越多的安全问题，如下图所示。



从上图来看，黑客攻击占据了相当大的比例。而基于黑客攻击的具体手段进行分析后发现，使用控制通道和探测密码等手段成为明显的薄弱点。具体如下图所示：



诚然现在有很多的安全设备以及加固手段，可以在确定安全隐患的前提下解决发现的安全问题，但通常是基于已知的安全问题，因而容易出现“头痛医头，脚痛医脚”的情况。更为严重的是，随着互联网本身应用价值的膨胀，攻击行为所带来的影响和损失也越来越大。

从应用的整个生命周期过程来看，产生安全弱点的源头在于应用的实现阶段，即软件开发过程。那如何从根本上解决应用本身的安全性问题呢？有效地将安全开发的方法和实践落实到开发过程。如果得到有效地实现，软件的安全开发将从根本上提升应用本身的安全性，从而将投入收益最大化，并将安全问题的影响最小化。

atsec information security

二、通过业界的最佳实践，构建安全开发的技术体系

除了与安全开发相关的业界安全标准（如通用评估准则 Common Criteria, PCI PA-DSS 等）以外，还有很多业界的最佳实践关注于安全开发的不同方面，如 OWASP（open web application security project）实践、微软的 SDL 软件生命周期计划、CERT 的 secure Coding 安全编码规范等等。OWASP 计划是一个开源项目，可在很大程度上节省组织在安全方面的资金投入。目前，该项目专注于 web 应用所提出的众多实践和指导，覆盖了规范指导、编码接口、测试工具等多个方面，这对于从根本上解决应用的安全问题有很强的实用价值。主要体现在：

1．完善应用开发生命周期的安全管理

OWASP 所提供的指导性文档，如“development guide”,“code review guide”,“testing guide”等，这些具体的规范分别对于开发过程、代码审核过程和软件测试过程中如何提升软件的安全性提出了具体的指导，推荐用于改进整个开发生命周期过程中的安全性。

另外，top 10 项目总结了当前最主流的 web 应用威胁，cheat sheet 则简明扼要地提出了针对 top 10 威胁的防范要点。这些无疑对开发安全的体系和规范具有很强的借鉴意义。

2．融入并建立应用开发的安全实践

首先，通过安全编码接口减少编码过程中产生的安全隐患。OWASP 计划提供了针对 Web 应用安全编码过程中的接口，其应用价值和参考意义在于提升编码实现的安全性。典型的安全编码接口编码如下：

- AntiSamy：AntiSamy 项目提供了编码过程中的过滤规则，这将有效降低来自客户端输入的安全风险，降低由跨站脚本等应用层面攻击带来的影响；
- ESAPI（Enterprise Security API）：此项目提供了一组安全控制的接口，可用于降低代码编写过程中的安全问题；
- EnDe：针对开发过程中的编码接口，避免因编码问题导致的安全事件，如不安全的对象引用等；

其次，通过工具化的方法实现有效的代码安全性审核。有效的代码安全性审核也是目前的一个难点，OWASP 项目提供的 LAPSE（Lightweight Analysis for Program Security in Eclipse）安全代码审核工具可在很大程度上帮助代码审核人员有效地完成任务。

最后，通过软件安全性测试工具，使安全问题在未产生影响之前得以发现和修复。软件生命周期过程中的测试阶段，除了进行功能性和性能性测试外，安全性的测试也非常重要。OWASP 项目中也有多款实用的安全性测试工具，这对于尽早并有效地发现软件的安全漏洞具有很重要的现实意义。其中，典型的安全性测试工具如下：

- w3af：一款针对 web 应用 top 10 漏洞的渗透工具；
- ZAP（Zed Attack Proxy）：一款用于发现 web 应用中的安全漏洞的渗透测试工具；
- WTE(Web Testing Environment)工作包：集中提供了大量的应用安全测试的工具。

有关 OWASP 计划的详细信息，请参见：http://www.owasp.org

三. 助力开发过程中安全性的合规建设

上述提及的应用安全开发实践指南和工具除了有助于提升软件开发过程的安全性外，对于组织在安全开发方面的合规性也有非常大的帮助。在此以支付卡行业数据安全标准（PCI-DSS）的合规建设为例，简要谈一下业界最佳实践对于安全性合规的意义。众多安全规范和实践（如 OWASP 实践、微软的 SDL 软件生命周期计划、CERT 的 secure Coding 安全编码规范等），在与符合 PCI-DSS 合规的组织充分融合后，将为开发安全的生命周期管理方面提供非常有力的支撑。

笔者在此谈一下理想化的组合，希望对组织的安全性合规建设思路有一些参考意义:

1．安全软件开发的体系合规

对于 PCI-DSS 要求的整个开发生命周期管理（详见 PCI-DSS Requirement 6.3-6.5.9），整个生命周期过程安全管理流程，如 NIST 的 SP-800-64 等具有较强的指导意义。而如何将安全管理流程和安全目标落实到应用安全开发的关键阶段中呢？如果组织自身进行实践并总结安全的具体方法，则需要极其大量的投入。CERT 所提供的 Secure Coding 编码规范以及 OWASP 计划中的“development guide”、“code review guide”以及“testing guide”等指导性文档则是业界最佳实践的总结，将极大地节省组织进行总结和归纳的资源投入，并为达到合规提供有力的支撑。

2．应用开发生命周期过程的合规

对于 PCI-DSS 针对生命周期过程各个阶段的要求，归纳的实践方法具体如下：

- 编码阶段(PCI-DSS Requirement 6.5.1-6.5.9)。OWASP 中 antiSamy、ESAPI 和 EnDe 等编码接口的使用，可较好地满足开发过程中的编码规范的要求。
- 代码审核阶段（PCI-DSS 6.3.2）。通过引入 OWASP 的 LASPE 工具，则可有效地应对并符合对具体代码进行检查和审核的要求。
- 测试阶段（PCI-DSS 要求 6.5.1-6.5.9）。通过使用 OWASP 计划中的测试工具，如 W3af，可有效地展开基于标准要求的 OWASP top 10 漏洞的测试工作。
- 生产阶段（PCI-DSS 要求 6.2）。通过使用 CVSS（通用脆弱性评分系统），可有效地对生产阶段所发现的漏洞进行评级，并确保关键的应用安全问题及早得到修复。

四．atsec 与安全开发

作为专注于信息安全领域的安全咨询和评估机构，atsec 一直关注于软件开发过程的安全性。除了为多家业界一流的厂商，如 IBM、HP、Microsoft 等提供基于标准的软件安全咨询和测评服务外，atsec 关注于涉及应用开发的厂商以及机构在安全开发方面的能力提升。在此有一个消息与大家分享，atsec 已于近期与中国信息安全认证中心（ISCCC）合作共同推出 CISAW 安全软件开发课程，并预计于 2012 年第一季度开展第一期培训。

编后语：

作为应用安全性方面的一个问题，即如何有效地将安全问题在未产生影响前得以识别和应对。而通常的情况是，作为开发人员来讲，通常很难把主要的精力投入到考虑软件的安全性本身，而专业的安全人员通常不会被分配完成代码的编写工作，软件的安全性提升并非一朝一夕，也并非一已之力所能解决。在此也希望与业界的各位同仁一道，共同为提升软件开发过程中的安全而努力！