CWASP

应用安全介绍

徐瑞祝

ShenZhen 2015.12

SECZONE 互联网安全研究中心

SECZONE 互联网安全研究中心

主题

- 软件安全定义
- 软件安全的重要性
- 软件安全的现状
- S-SDLC安全软件开发生命周期介绍
- 轻量级S-SDLC探讨

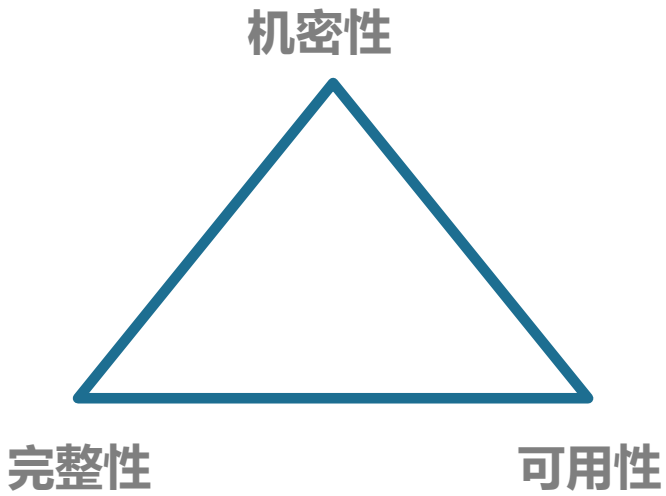
平均损失270万美元　34%↑

软件安全定义

SECZONE 互联网安全研究中心

软件安全的定义

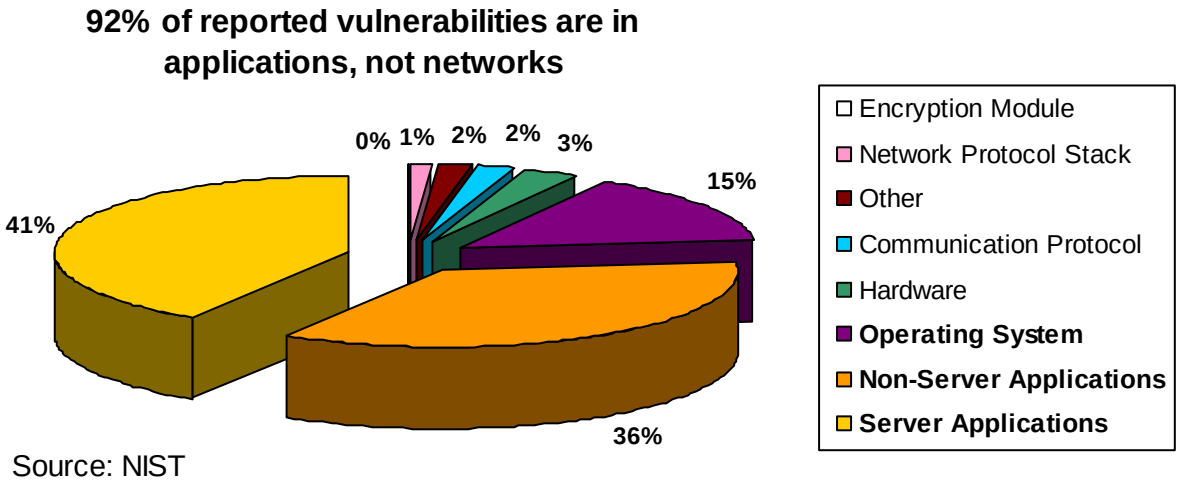
- 软件安全既应用安全是对预期保证**受保护的信息和系统**的机密性、完整性和可用性的应用程序功能的设计与实现。
- 软件的安全问题是由于不好的代码实现造成的。



软件安全的重要性

为什么软件安全重要？

- 根据NIST等权威机构的报告，超过90%的黑客安全事故都发生在软件本身，而不是在网络。



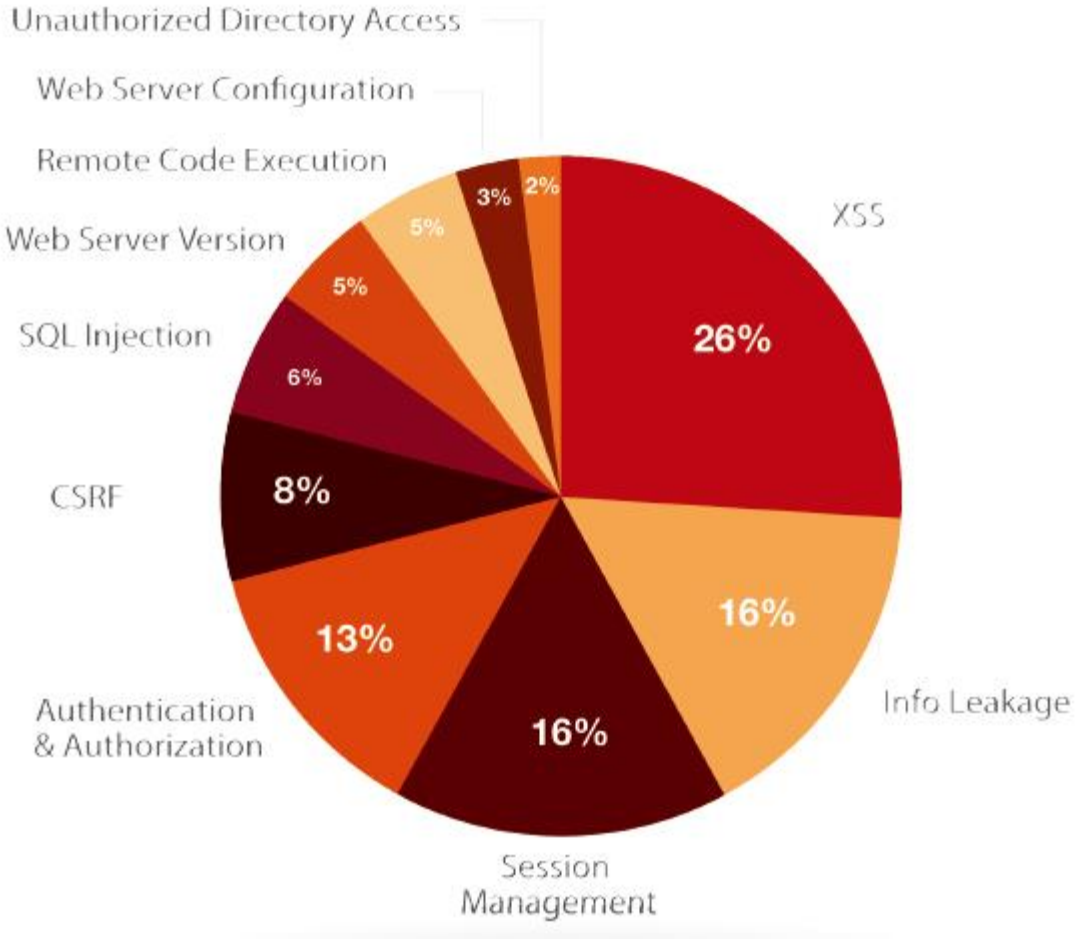
Source: NIST

SECZONE
互联网安全研究中心

软件安全的现状

软件安全现状


99%
99%
2013
2014


Unauthorized Directory Access
Web Server Configuration
Remote Code Execution
Web Server Version
SQL Injection
CSRF
Authentication & Authorization
Session Management
Info Leakage
XSS
26%
16%
16%
13%
8%
6%
5%
5%
3%
2%

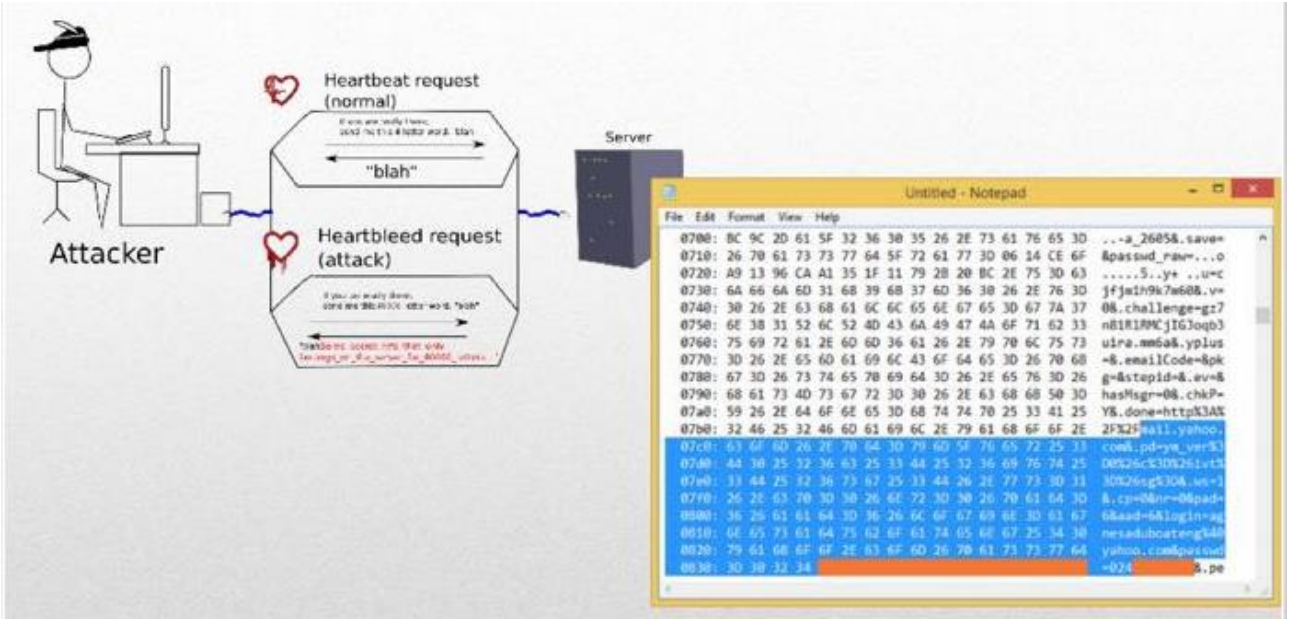
SECZONE 互联网安全研究中心

外部安全环境

- 美国早在2007就已把中国作为重点监听对象。从2009年开始大量入侵中国内地及香港的电脑和网络系统窃取重要的情报及信息。
- 斯诺登曾透露美国国安局曾入侵中国电迅公司以获得手机短信信息，并持续攻击清华大学的主干网络以及拥有区内最庞大的海底光纤电缆网络的电迅公司Pacnet香港总部。
- 美国对华监听涉及到众多领域，除公务信息外，商业信息，个人信息也在此之列。

2014-2015国内外重大安全事故

- **OpenSSL“心脏出血”漏洞**
  - 2014 4月8日，OpenSSL爆出年度最知名的安全漏洞Heartbleed，被形象地形容为致命的“心脏出血”。利用该漏洞，黑客坐在自己家里电脑前，就可以实时获取约30%的https开头网址的用户登录账号密码，其中包括网民最常用的购物、网银、社交、门户、微博、微信、邮箱等知名网站和服务，影响至少两亿中国网民。OpenSSL的“心脏出血”再一次把网络安全问题推到了公众面前。



2014-2015国内外重大安全事故

破解特斯拉智能汽车

- 通过利用特斯拉的应用程序系统漏洞，重现了该漏洞的安全隐患，成功利用电脑实现了远程开锁、鸣笛、闪灯、开启天窗等操作。

SECZONE 互联网安全研究中心

2014-2015国内外重大安全事故

- **携程日志泄露事件**
  - 2014年3月22日，有安全研究人员在第三方漏洞收集平台上报了一个题目为“携程安全支付日志可遍历下载导致大量用户银行卡信息泄露（包含持卡人姓名身份证、银行卡号、卡CVV码、6位卡Bin）”的漏洞。上报材料指出携程安全支付日志可遍历下载，导致大量用户银行卡信息泄露。
- **国内知名连锁酒店（锦江之星、速八..)及高端酒店（万豪、喜来登、洲际..)等网站存在高危漏洞，大量客户开房信息泄露**
  - 黑客可轻松获取到千万级的酒店顾客订单信息，包括顾客姓名、身份证名、手机号、开房时间、退房时间、房型、家庭信址、信用卡后四位、信用卡截止日期及邮件等大量敏感信息。

SECZONE 互联网安全研究中心

2014-2015国内外重大安全事故

- **海康威视被黑客植入代码，导致被远程监控**
  - 江苏省公安系统部分在互联网上的海康威视设备，因设备弱口令问题被黑客攻击，部分设备被境外IP控制远程监视。事件造成海康威视股价遭遇了大跌，并一度跌停，单日市值蒸发90亿元。

- **银信通漏洞，需一个手机号即可查到你的账户资金变动信息**
  - 银信通(FMS)是“银行信息通知系统(Instant Financial Messaging System)”，该系统是基于中国移动通信短信平台和银行金融数据库开发的金融数据通信平台，并充分利用互联网和GSM网络资源，以经济快捷的方式，让银行及银行的个人客户和企业客户可以随时随地享受金融服务 。
  - 由于银信通业务系统存在漏洞，导致银行通知给用户的短信记录，可被在线查到。

SECZONE 互联网安全研究中心

安全事故造成的影响

- **安全问题可以对一个组织的信息和软件资产产生不利的影响。**
- **引起关注软件安全的常见原因包括：**
  - 收益的减少
  - 品牌或公司形象的损坏
  - 经常性的抱怨
  - 客户安全需求
  - 因为有缺陷的软件的安全漏洞而导致的债务
  - 对业务的整体风险

索尼公司的“被攻击”史

- **2004年中国官网被涂鸦**
- **2011年4月 索尼PlayStation Network遭受攻击**
  - 1000万注册用户的数据被盗（包含信用卡数据）
  - 关闭服务数天时间
- **2011年6月索尼图片网站遭受攻击**
  - 黑客盗取了整个数据库的450条万记录。
  - 12，500个用户信息泄露（包括用户名、地址、生日、明文密码等敏感信息）

索尼公司的“被攻击”史

- **2014年11月索尼（美国）影视娱乐公司索尼遭到黑客攻击**
  - 黑客声称已获取索尼影业全部的网络数据，包括雇员及高层私密。
  - 长达数周，公司员工停止连接公司电脑，停止使用公司电脑，使用纸笔办公。
  - 黑客GOP在BT网站上泄露了5部新电影。
  - 黑客泄露大量内部员工信息，明文密码文件及证书等。
  - 公司遭到前员工起诉。
  - 损失超1亿美元。

SECZONE 互联网安全研究中心

索尼频造攻击的原因分析

- 管理层不重视软件安全。
- 众多系统存在严重的安全漏洞。
- 不重视客户资产。
- 对安全事件的产生的严重后果预计不足。
- 未实现纵深防御的策略。
- 没有很好的安全应对措施。

SECZONE 互联网安全研究中心

造成国内安全现状的原因

- **国内IT从业人员普遍安全意识淡薄。**
- **在信息安全上投入的资金占IT总投入占分过低。**
  - 国内IT企业平均2%，发达国家达到20%左右。
- **企业信息安全技术人员缺乏、管理薄弱。**
- **未建立安全代码开发及持续改进的过程（SDLC）**

SECZONE 互联网安全研究中心

为什么我们要评估软件？

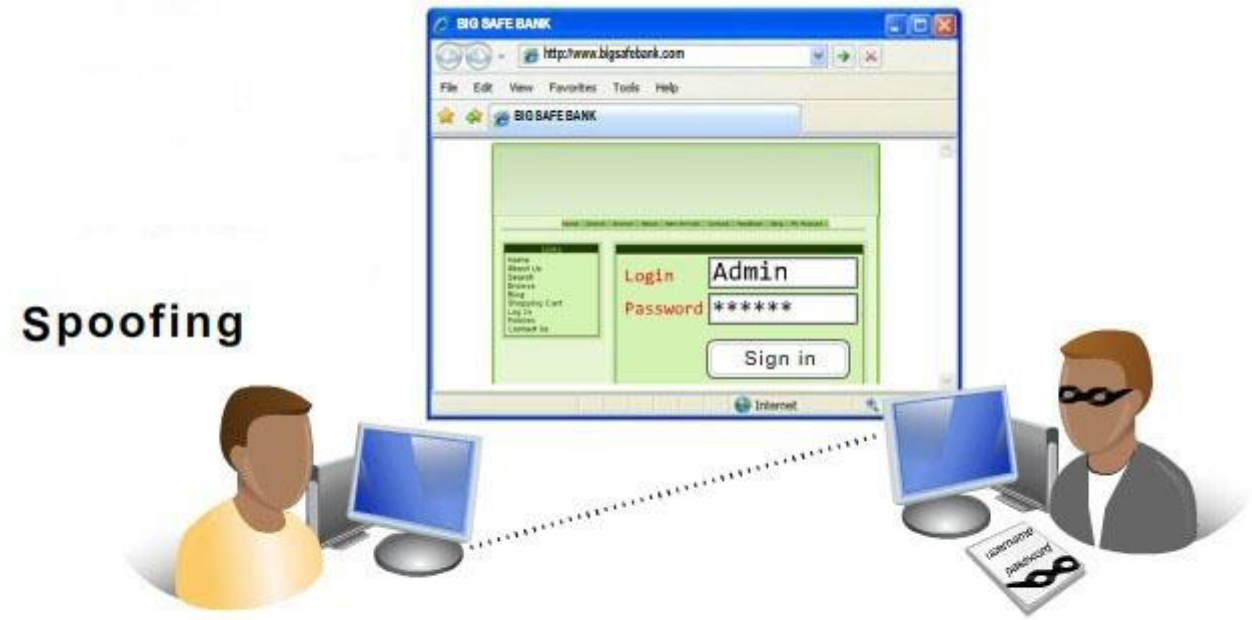
- **安全评估是评价一个应用程序安全性的关键机制。**
- **引导一个安全评估的关键原因是为了：**
  - 了解风险
  - 识别软件设计或实现上的缺陷
  - 提高整个代码的质量
  - 启用持续改进过程
  - 维护一个积极的公司形象

软件中存在的常见威胁

- 仿冒（Spoofing）
- 篡改（Tampering）
- 抵赖（Repudiation）
- 信息泄露（Information Disclosure）
- 拒绝服务（Denial of Service）
- 权限提升（Elevation of Privilege）

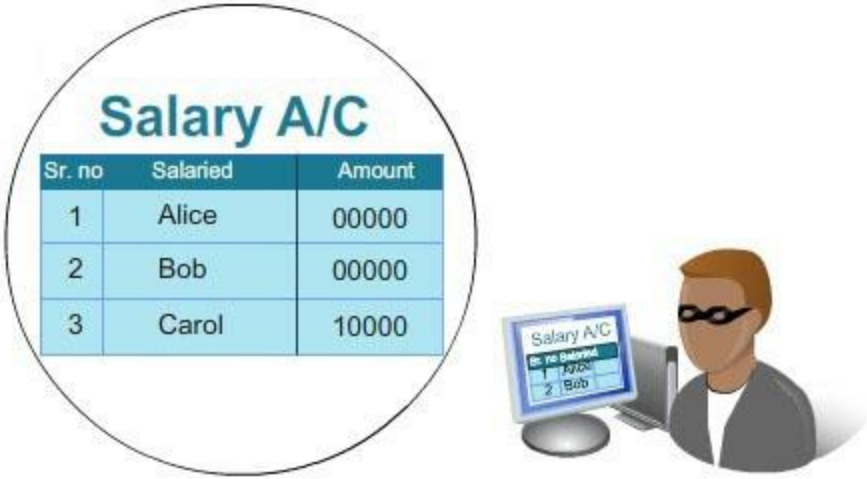
SECZONE 互联网安全研究中心

仿冒

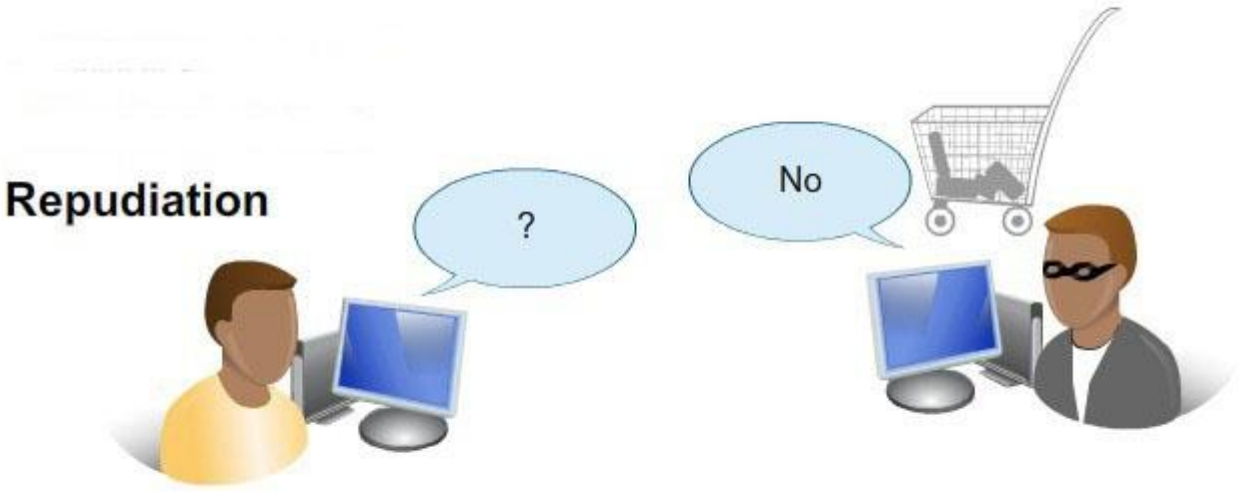


篡改

Tampering



抵赖



信息泄露

- Error Type:
  Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)
  [Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ' and password = ''.
  /loginprocess.asp, line 33

Information Disclosure

SECZONE 互联网安全研究中心

权限提升

安全测试 VS功能测试

传统的功能测试不同的安全测试，功能测度不能替代安全测试！

功能测试：

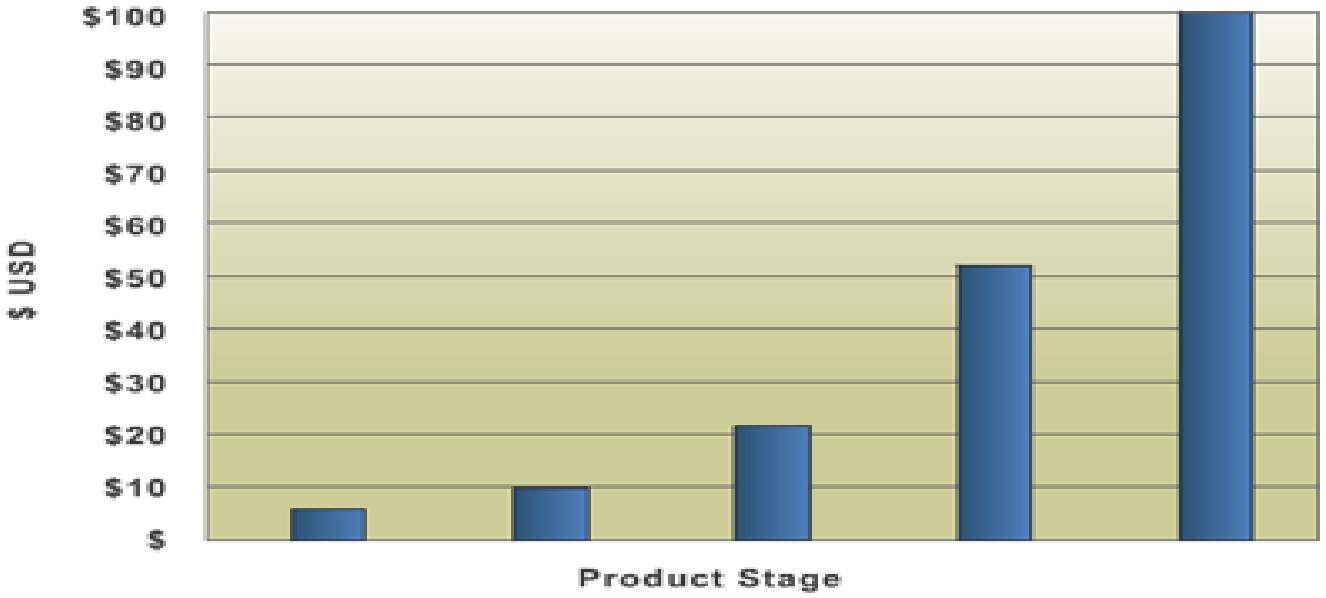
- 功能测试验证应用程序是否做它应该做的。
- 包括提交输入去验证正确的输出。
- 功能测试者会问“什么是软件应该做的？“

安全测试：

- 安全测试验证应用程序不做它不应该做的。
- 包括提交输入去验证不出现异常。
- 安全测试者会问“什么是软件不应该做的？”

在安全缺陷上的花费

- 移除一个安全漏洞的花费随着软件开发生命周期的过程呈指数级增长。行业调查显示：在测试阶段移除一个漏洞的总体花费要少于软件发布后移除费用的20%. 如果移除一个缺陷在更早的阶段，如开发阶段，那将远远比在测试阶段移除便宜。

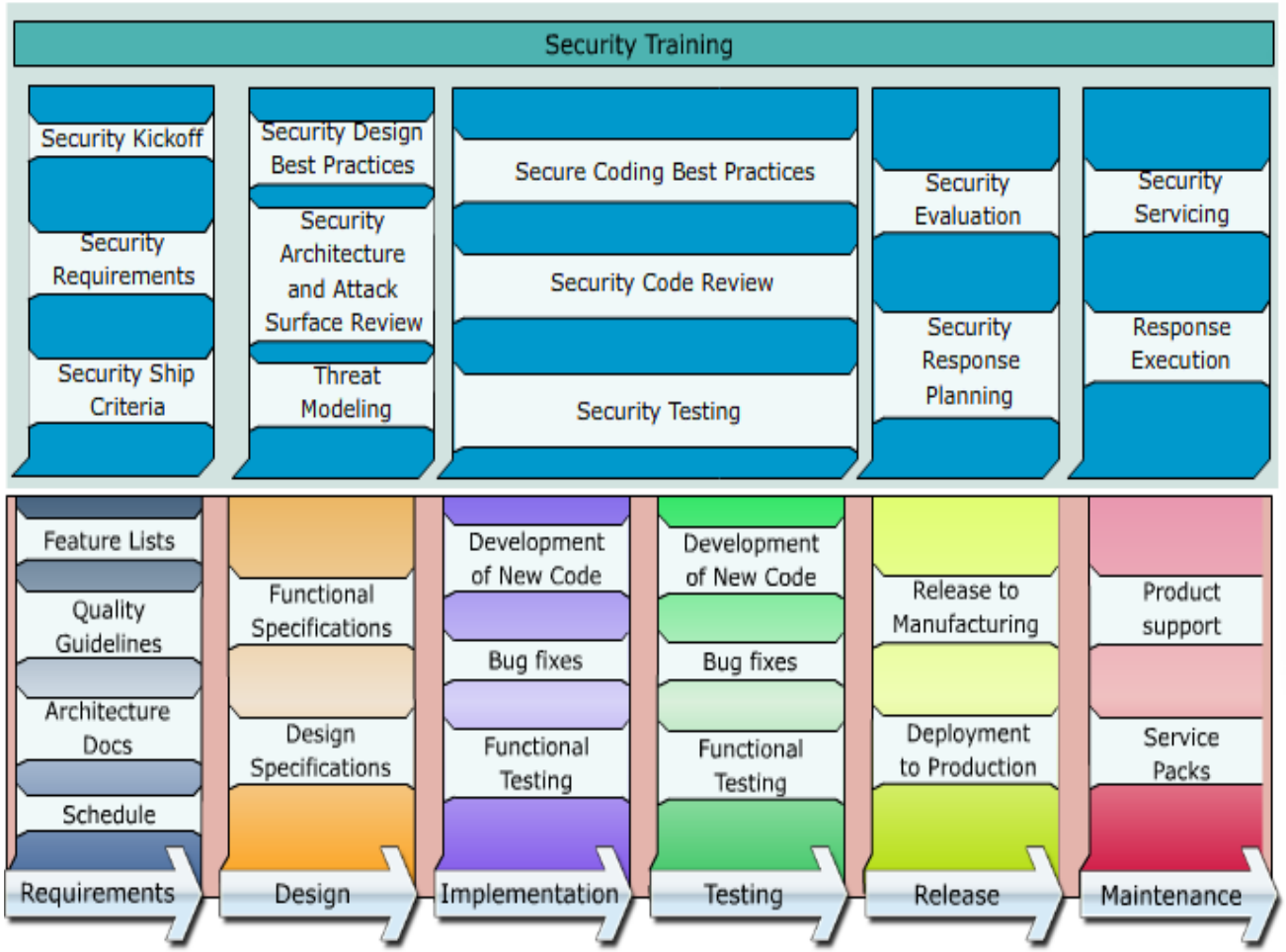


SECZONE
互联网安全研究中心

S-SDLC安全软件开发生命周期介绍

SECZONE 互联网安全研究中心

安全软件开发生命周期



SECZONE 互联网安全研究中心

软件安全生命周期安全活动介绍

需求	•安全需求分析
设计	•安全设计 •威胁建模
开发	•安全培训 •安全代码评估
测试	•安全测试 •渗透测试
发布	•安全环境测试 •安全响应计划
维护	•监控、扫描 •安全事件响应

S-SDLC安全需求

- **因为标记着一项研发计划的开始，需求阶段是最合适的阶段去开始设立您的安全开发流程。**
- **在需求阶段您应该做的是：**
  - **设立一个安全顾问**（内部的，或者第三方机构）。安全顾问必须是一个安全专家，他将会负责验证安全活动和输出。
  - 在每一个团队，如：开发、测试团队，**设立一个安全负责人，**负责在他们团队中推动安全活动。
  - **收集适用于您的软件项目的安全需求**，如任何安全标准或像PCI DSS，HIPAA，SOA，GLBA，BASEl II等软件从属的条例。
  - **确认、获取和配置在项目中需要的软件安全工具**，如Bug跟踪系统。
  - …

S-SDLC-安全设计

- 安全设计需求
- 所有的安全需求文档化
- 正确管理防火墙配置
- 威胁建模
- …

安全设计需求

- 输入验证
- 身份认证
- 授权
- 配置管理
- 敏感数据
- 会话管理
- 加密
- 参数操纵
- 例外管理
- 日志和审计

威胁建模

- 威胁建模是一个审查软件架构和确定软件可能存在的威胁的一个过程。威胁建模的目的是使开发团队高效开发出安全的软件。
- 设计、开发、测试团队的代表人物应该参与到威胁建模的过程当中，并且要在项目的安全顾问的指导下进行。

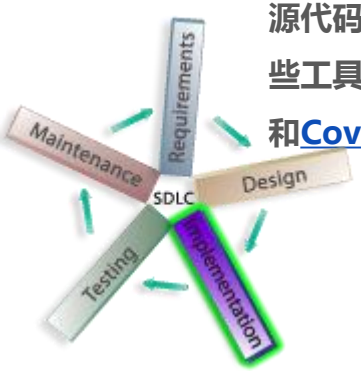
SECZONE 互联网安全研究中心

威胁建模步骤

- 定义资产
- 描述系统
- 定义信任边界
- 定义威胁

S-SDLC安全开发

- 从一个安全的角度出发，开发阶段是整个软件构思非常重要的阶段，因为有50%的缺陷是因为编程错误引起的。
- 为了避免引入漏洞，开发人员得意识到他们使用的每一种技术的安全特性。特定的技术常常会涉及到一些特别的安全编码最佳习惯。例如：根据您是否开发WEB应用程序，是否编写本地代码，是否是客户端-服务器模式，是否与数据库交互都有不同的最佳安全编程习惯要遵守。
- 不管开发人员使用的是什么技术,一些通用的安全编码习惯必须要遵守，包括：执行输入和输出验证、不要使用不安全的API、安全的错误处理、保护敏感数据、安全的管理帐户、采用适当的授权机制和安全的审计和记录程序。
- 为了跟踪这些好的编程习惯被执行，组织得在软件被测试之前执行手工的或自动化的安全代码复查。静态源代码分析工具可以帮助您在开发阶段找出漏洞。大多数工具都支持多种语言，如：C/C++,JAVA,C#. 这些工具比较有名的包括：Checkmarx CxSuite 、 Security Analys、Fortify Source Code Analyzer 和Coverity Integrity Center



S-SDLC安全测试

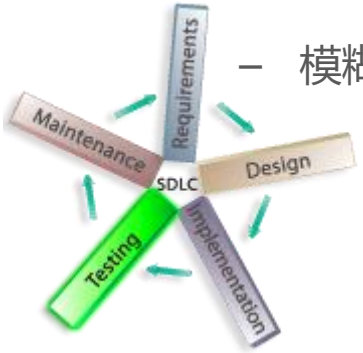
- 即便在设计和安全开发软件上做了最大的努力，但是难免还是会有一些漏洞。安全测试的作用应该是为了找出这些漏洞，并且提供一个软件发布给客户或者生产环境之前去除这些漏洞的机会。
- 安全测试非常不同于传统的功能性测试，因为它需要不同种类的技术和工具。安全测试主要包括对出现的已知类型的漏洞作分析。显然地，要在安全测试上做得出色，软件安全测试员应该意识到这些类别的漏洞，它们失败的症状和发现这些漏洞的最普通的方法。

特殊类型的漏洞的测试

- **对于安全测试人员来说，应当熟悉各种不同的软件漏洞， 知道怎样去测试它们，能够发现它们的存在。**
- **下面是几种类别的安全漏洞以及它们的定义：**
  - **Buffer overflows.** 一种编程错误，可能导致未被授权的内存访问和在受害的主机上执行恶意代码。
  - **SQL injection.** 以不正确的方式包含用户输入的参数到SQL查询语句当中，从而允许攻击者在这个查询语在后台数据库执行时改变它的行为。
  - **Cross-site scripting.** 这类漏洞通常存在于Web应用程序当中。恶意代码可以被恶意的Web用户注入到可被别的用户浏览的Web页面当中。
  - **Lack of server-side authorization.** 这类漏洞只由于权限认证在客户端执行。通过利用这种漏洞，攻击者可以合法的访问系统的资产。
  - **Weak authentication**. 这类漏洞允许攻击者绕过认证，从而不适当地访问系统资源。
  - **Weak authorization.** 这类漏洞允许攻击者绕过权限认证，从而可能潜在的提升他们访问系统资源的权限
  - **Improper use of cryptography**. 不正确的使用加密算法。
  - **Improper error handling.** 这类漏洞会导致敏感信息泄露给攻击者或者让应用程序处于一个不安全的状态。

利用安全测试工具

- **因为安全测试常常会用原本不会用的方式去监测、截取和修改数据，因此需要一些非常特别的工具。为了更有效率的做安全测试，测试者应该从适当的安全测试工具中得到帮助。包括：**
  - 监测工具，如： Windows SysInternals suite, Holodeck, 和 Lsof
  - 网络嗅探器，如： Tcpdump, Wireshark, 和 Ettercap
  - 调试器和解码器，如： WinDbg, OllyDbg, 和 IDA Pro
  - Web代理，如： 如： Burp, Paros, 和 Fiddler
  - Web应用程序扫描工具，如：Appscan, Acunetix, 和 WebInspect
  - 模糊测试工具，如COMRaider, SPIKE, 和 Peach Fuzzing Framework



SECZONE 互联网安全研究中心

企业执行SDLC所面临的问题

- 团队缺少安全专业人员。
- 项目组开发周期很紧，无法抽出专门的时间。
- 团队执行力不够。
- 安全标准与规范无法落地。

SECZONE
互联网安全研究中心

轻量级S-SDLC探讨

SECZONE 互联网安全研究中心

如何快速实施SDLC（安全软件开发生命周期）？

- **国内IT企业安全团队水平与执行力度等情况都各有不同。针对一些安全基础较薄弱，但又急于想实现的安全软件开发生命周期的企业，可以有一套轻量级的SDLC方案。**
- **轻量级SDLC包括如下的内容：**
  - 安全设计、开发与测试的培训
  - 企业开发所涉及语言的安全编码规范
  - 静态代码审查与动态的安全测试工具
  - 不同团队之间沟通的机制
  - 输出文档及跟踪模式

SECZONE 互联网安全研究中心

代码审核实施方案

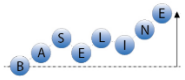
实现与定制化

L3使用与漏洞修复培训

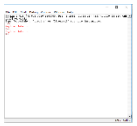
工具使用培训

漏洞修复培训

L2安全代码审查规范



漏洞基线



规则自定义

流程优化

L1安全编码规范

python

C PROGRAMMING LANGUAGE

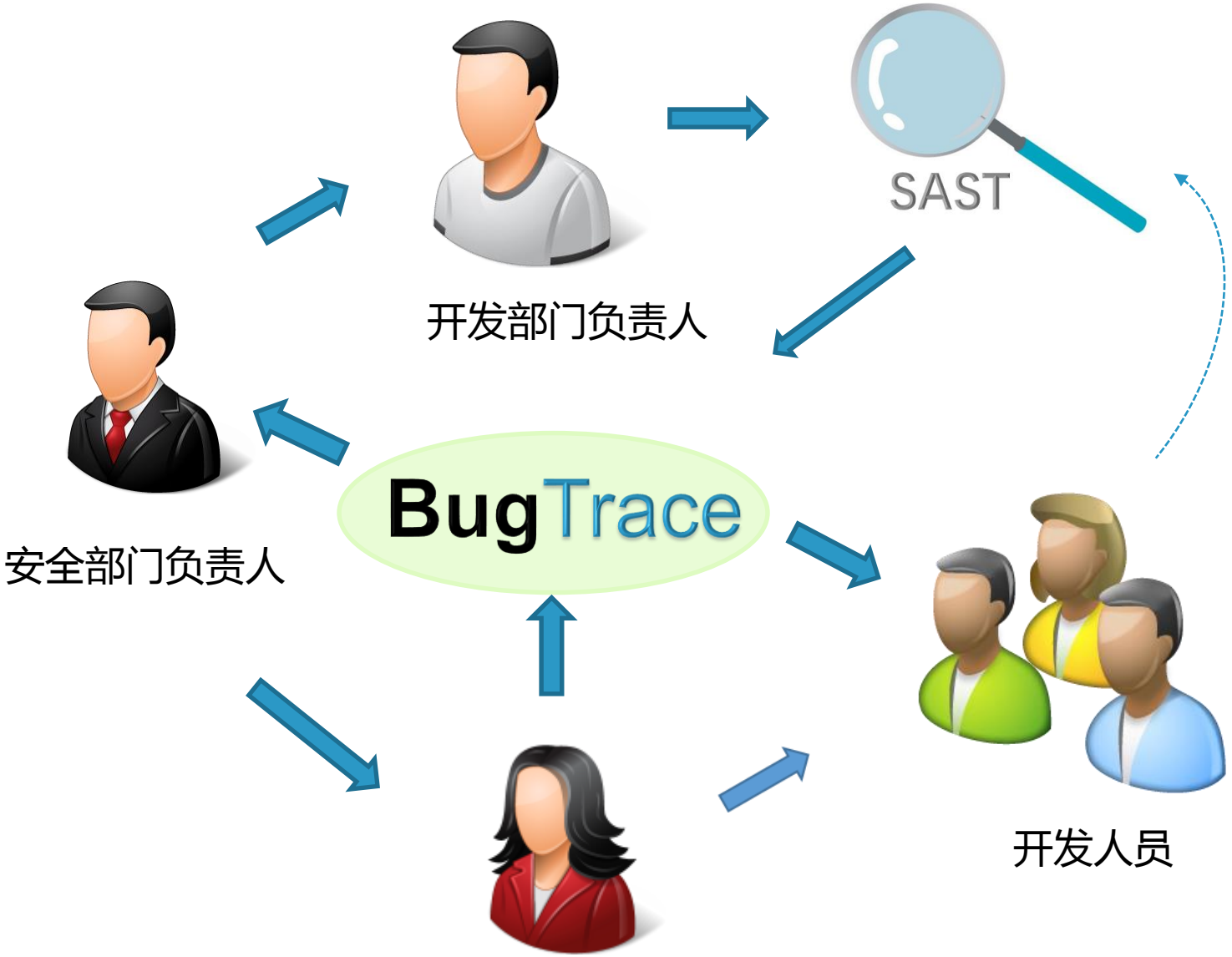
Java

C#

JS

SECZONE 互联网安全研究中心

扫描流程规范



SECZONE 互联网安全研究中心

S-SDLC所要实现的目标

- 使软件更像硬件一像成为一个标准流水线上的产品
- 每个程序员就像流水线上一名工人，他们必须按照标准操作以产出合格的产品。
- 不同的开发小组及测试小组就像多条不同阶段的流水线，最后组装成一个相对可控的、高质量的产品。

Thank you