2009.11.12/13

主办方

OWASP

CISRG

赞助方

DBAPPSecurity 安恒信息

ANTIY 安天实验室

OWASP China & ISF 2009 年会@上海

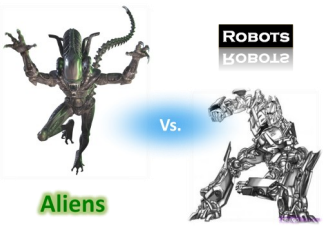
“冷冷的冬雨在脸上胡乱的拍”，刺骨一样的寒意却无法阻挡一群对信息安全有着异乎寻常热情、敏感及爱好的年轻人在上海相聚，分享其对于信息安全技术的理解，以此促进国内外信安业界的交流与沟通。这只是开始……

2009.11.12.0830

九时起，随着电焊工Burn-E那略显滑稽的开场片，正式拉开了此次由OWASP China与Cisrg共同主办的安全盛会的序幕。

此次参会来宾来自国内外多个地区，其中涵盖加拿大、法国、匈牙利、澳门以及深圳、成都、北京、济南、杭州、福州、合肥、沈阳等若干地区，而参会来宾既有来自国内一线安全厂商的资深工程师（如：启明星辰、绿盟、山石网科等），也有来自国际IT巨头的资深程序员（如：IBM、Microsoft、ZTE、TrendMicro、ActiveNetwork等），还包括来自东北、华南地区的运营商代表（如：辽宁移动、福建联通等），同时还有包括来自金融行业的IT管理人员（如：太平洋保险、兴业全球基金等）以及一线互联网公司的资深安全管理人员（如：淘宝、携程网、盛大网络、巨人互动娱乐、完美时空等）。

本次总参会人数预计超过120人，谁是特立独行的外星人Aliens？谁又是皆可预测的Robots？……拭目以待



目录

#1 网络犯罪取证调查与应急响应研究-Waterwave

计算机取证与网络取证的应用对象始终是数据本身。从操作系统的离线与在线式调查取证手段的多样化开始，Waterwave将取证过程中需关注的细节娓娓道来，如何去关心RDBMS中的用户变化，如何通过URL访问行为推测嫌疑人的经济状况及婚姻状况，如何通过Mount/Mont/Mout的击键细微差别而推断入侵者的国别、语言能力以及潜在活跃群体组织，如何通过拨打一个办公电话而直接采用社会工程学锁定某入侵黑客……一切并不神奇，更多的安全评估人员并非不具备足够的知识储备与技术能力，所欠缺的仅仅是将技术细节与案件推理相结合的融合能力，而修习心理学又擅长信息安全攻防的他，用温文尔雅且流利的法语证明给我们一个安全之外不一样的Waterwave……

#2 XSS两三事-思无邪

2009.11.12.1120

XSS攻击自从2002年被提出并广为传播以来，一直被认为是在Web应用层最为危险也最为有效的攻击方式。原本作为用户输入的数据却被恶意的控制成为页面脚本加以执行，从而使得应用逻辑被控制，而入侵者则得以破坏、劫持、窃取用户数据。在因用户输入、HTML标签滥用以及环境问题而导致的三类XSS问题中，第一类最为广泛。

思无邪通过对编码Encoding以及复合编码Composite Encoding的深入浅出的讲解，结合了大量的XSS攻击/误用案例，尤其是具备复杂应用逻辑的电子商务网站、协同工作站点所出现的特殊字符脚本XSS漏洞逐一分析并提供了解决建议。

思无邪认为，OWASP ESAPI提供了一个很好的编码Encoding的参考，但是在性能、非ASCII码的处理等方面仍需要进一步改进。

谨言慎行的他，作为Cisco旗下WebEx的应用安全组长曾在大宇工作数年……仙剑奇侠么？

#3 硬件Hacking-串串烧-Billy

“不懂信息安全的人是幸福的，而我们的责任是保卫他们的幸福”

——

安天实验室
程序员
Swordlea

在此前的安全焦点年会中，安天的硬件程序员以多种外设接口（并口/USB接口等）无线注入攻击终端主机呈现了安天工程师们的安全思想。此次会议上，Billy以USB DOS攻击为起点，通过大量照片呈现了安天更多硬件编程水平，从基于低成本、低功耗的ARM平台所衍生开来的蜜罐Honeypot、监控设备、杀毒/脱密门禁系统的一系列安全盒子到基于USB电开关的网闸、USB多头（8个）显控卡等，甚至安天包括AScope/GPU加速技术方面的研究都有所选择性的公诸于众。

Wiimote Hacking的演示视频为全场听众带来了阵阵欢笑，因为那一支在魂斗罗中Click2Die红外激光笔成本不足百元。

#4 二进制程序中整数溢出漏洞检测 –王铁磊

Google picasa中真实的案例

```
.text:004E576D    mov     eax, [esp+58h+var_3C]
.text:004E5771    mov     ebp, 1
.text:004E5776    cmp     eax, ebp
.text:004E5778    jb      short loc_4E5786
.text:004E577A    lea     ebx, [ebx+0]
.text:004E5780    add     ebp, ebp
.text:004E5782    cmp     ebp, eax
.text:004E5784    jbe     short loc_4E5780
```

2009.11.12..1245

擅长于漏洞挖掘、逆向工程、程序分析且来自北大的在读博士生王铁磊毫无争议的被诸多听众冠以“漏洞挖掘之王”称呼，作为Secunia、CVE上最近两年来上报漏洞最高的中国人以及在NDSS国际顶尖学术会议上以第一作者身份提交关于二进制程序中整数溢出漏洞检测方面论文的出生于85年的“他”确实当之无愧。

从一道简单的面试题切入，分析整数溢出的危害性，而通过多个类似Google Picasa以及多个播放器中存在的实际整数溢出0Day漏洞案例，区分了整数溢出与传统的堆（栈）缓冲区溢出的不同之处。其所开发的IntScope二进制整数漏洞挖掘工具可以缩减漏洞挖掘工作量并较为准确的定位至漏洞溢出点。Trust No one……

撰稿：Billy@Antiy

#5 互联网企业应对恶意网址的思科-林世飞

互联网帝国腾讯通过其庞大的客户端装机量成为最令人生畏的腾讯帝国，而其在安全方面的不断努力，在前端密码保护、QQ医生前置检测、QQ安全中心、无所不在的安全意识宣贯手段等都有所体现，来自腾讯安全中心的林世飞则为全场呈现了腾讯在后端挂马检测、恶意URL收集（钓鱼、欺诈、违反策略等）方面的日常工作片段。其以用户帐号为中心的评估中毒修复/挽救成本的金字塔模型也证明了用户安全意识的重要性可见一斑。

当然，威胁不仅来自于外部，动辄数千乃至近万员工的互联网公司复杂的办公网/管理网/业务网以及对外提供服务的网站也日趋复杂，而如何建立出口流量审计机制以及建立访问授权认证机制则成为另一个角度上应对内部恶意URL威胁并在威胁传播时尽可能隔离威胁在一个较小的范围内避免更进一步传播的有效手段。

QQ+QQ游戏+QQ影音……+QQ杀病毒=?

2009.11.12.1610

#6 A DIY Botnet Tracking System-Eric Chio

僵尸网络Botnet始终是安全业界的关注焦点，一是因其应利益而生，二是因其非常具有隐蔽性，三是因其数量规模都日趋庞大，动辄上百万量级的僵尸网络已浮出水面。如何对其进行监控乃至跟踪就成为亟需解决的问题。

来自微软的Eric Chio，生于澳门，就读于香港中文大学，作为ACM编程大赛的优胜者先后工作于Yahoo/Microsoft，并参与Forefront Protection for Sharepoint的程序员讲述如何加入僵尸网络大家庭的详尽过程，“沉默是金”的口头禅是他强调在跟踪僵尸网络活动时所应遵守的最基本原则。

他，86年生，果然英雄出少年。

“我们是不是老了？”

“你们老了，但你们也辩证了，宏观了，成熟了”

岁月无情，但岁月公平

——某网友语

#7 下一代安全架构设计-老鹰

2009.11.13.1400

作为IBM ITO首席安全顾问的老鹰热衷于潜水、滑翔伞、击剑、科幻等上天入地惊险刺激的运动，具备超过14年以上的信息安全从业经验，为我们带来IBM对于信息安全架构的深刻理解。事实上，大众未意识到IBM是一家具备信息安全积累的公司，然而AIX仍然是迄今为止最安全的操作系统之一，X-Force也是业内最顶尖的安全团队之一，而ISS安全产品系列也均具有世界级水准，甚至包括多个加密算法、新兴安全厂商的主要创始人均源出于IBM的信息安全研究部门。

从IBM ISF到MASS方法论，以及e-Business方面的安全设计理念，涵盖了从技术控制、流程控制、风险控制以及与客户特有文化所能融合的思想给更多的安全技术人员带来全新的视角。

#8 Web安全攻防经验谈-Aaron

Aaron通过对近8000余个政府相关网站的Web安全评估统计之后，得出的结论之一是天津及安徽地区的政务网站70%以上均存在显著可供入侵者利用的安全漏洞，远远高于其它省份地区。评估过程采用了自动化工具辅助，人工评估相结合的手段，自动化工具则是由杭州亚龙安恒所开发的Web安全评估套件，其较好的覆盖了OWASP TOP 10 Web漏洞类别以及包括数据库注入漏洞等在内的安全检查点。

Aaron参照Top 10漏洞的分类分别将其在评估过程中的心得体会，尤其是在针对每种漏洞选用黑盒、白盒、灰盒检查工具方面的优缺点逐一进行说明。

Aaron也是OWASP Security Testing Guide 3.0的中文版的翻译人员之一。

#9 Many Core In Network Security Appliance-Peter Liang

Tilera作为一家新兴的多核CPU厂商，超常规的发展，将CPU的微内核数量从16核到32核、64核直到数周前推出了具有100核的CPU芯片，而其板载80G级别的吞吐能力确实成为CPU中的怪兽级技术。以往网络安全设备，尤其是边界处部署的安全设备往往受限于性能，不得不在软件方面尽可能的优化、剪裁，付出相当大的努力而收效甚微，那么硬件方面的提升是否能够降低在软件方面的巨大投入而促使新一代的安全设备尽快上市呢?

从Peter Liang的演示来看，开源的Snort已可工作于Tilera的64核CPU平台之上，并已实现20G级别的线速吞吐能力，并还具有一定的扩展能力。现场听众的针对性能、调度、管理细节上的诸多问题引发了一阵阵热烈的讨论与交流。

建议意见

如果您有宝贵建议与中肯意见，合作想法可通过以下电子邮件与我们取得联络

rip@owasp.org
Cis7all@gmail.com

结语

时值2009岁末，通过近一个月来的筹备，在Rip、Frank、7all、Michelle等人多方努力协调下，终于促成此次上海会议的顺利召开。

在此，对以上以及众多参与本次会议组织、筹办、接待、后勤、协调、联络的热心的朋友们表示衷心的感谢!

正是你们的无私奉献温暖了寒冷的冬天。

去年的ISF2008是在不到两周的筹备下仓促召开，但也邀请到了全国各地超过40余位来宾的支持；今年与OWASP China的联合，进一步扩大了信息安全知识与技能分享的范围至国内外诸多来宾之中，作为最主要两届会议的组织者以及主持人、撰稿人的我，深感信息共享与沟通所产生的安全价值的重要性所在。

展望，2010……

2009.11.13.1830

2009.11.13.1740

http://www.cisrg.cn/isf/2009/speaker.html

http://www.owasp.org/index.php/China-Mainland

Billy.lee@antiy.com