安全小课堂第七十三期【白盒安全测试】

京东安全应急响应中心 2017-09-18

在进行白盒安全测试时，安全审计人员必须清楚地知道被测试环境的内部结构和技术细节。因此，这种测试方式向审计人员敞开了一扇大门，使他们能够以最小的代价来查看和评估测试目标中的安全漏洞。JSRC **安全小课堂第七十三期**，邀请两位老师分享白盒安全测试技术。

什么是白盒安全测试呢？

京安小妹

白盒测试（White-Box）是审计人员清楚地知道被测试环境的内部结构和技术细节，测试其正确性、完整性、安全性与质量。而这里只讲针对安全性的白盒测试，使他们能够以最小的代价来查看和评估测试目标中的安全漏洞。

白盒测试是相对黑盒测试来说的，黑盒测试根据执行结果来判断行为，白盒相对黑盒来说可以比较清楚的知道内部结构，可以更加深层基于理解去发现安全问题。

讲师： Monster、CongRong

白盒安全测试与黑盒安全测试的区别在哪里呢？

京安小妹

白盒安全是审计人员清楚地知道被测试环境的内部结构和技术细节，与黑盒安全测试恰巧相反。首先哪些情况下可以进行白盒测试：
1. 专门的开发人员或测试人员。
2. 纯开源软件，谁都可以进行白盒安全测试。
3. 如果黑客攻破的是脚本语言，那么就可以获得该源代码并审计出更多的漏洞。
白盒：白盒安全测试会比黑盒安全测试更方便的挖掘出漏洞。
黑盒：有些软件的特性漏洞只有通过FUZZ手段才能挖掘出来。：

讲师： Monster、CongRong

那么白盒安全测试的方法有哪些呢?

京安小妹

代码静态审计：
查找危险函数，并跟踪调用的点是否安全
可能存在的各种逻辑缺陷，例如二次触发的
验证是否严谨，确保不会被越权
代码动态审计：
针对某一处代码块，在了解了功能实现的前提下运行程序，并一步步进行调试。
运行环境审计：
软件环境：中间件 / 数据库 / 各环节且包含的插件是否安全
网络环境：加密协议（SSL等）是否可靠、合理配置iptables等
系统环境：服务器配置是否安全，补丁是否为最新等

测试方法的话其实从根本来讲安全的白盒测试和传统的白盒是一样的。

讲师： Monster、CongRong

白盒安全测试对企业的重要性?

京安小妹

我们知道，（系统的安全防御时间>漏洞检测时间+攻击响应时间）系统才是相对安全的。那么内部采用白盒安全测试就可以大大减少测试成本，毋庸置疑，稍微有点安全意识的公司都会在安全测试阶段采用白盒安全测试，也是促进公司内部对开发者们安全编码规范的过程。

：

讲师： Monster、CongRong

是否有成熟的白盒安全测试工具或者脚本推荐?

京安小妹

Taint（php插件）：https://github.com/laruence/taint
RIPS: https://www.ripstech.com/
Seay源代码审计系统: http://www.cnseay.com/3265/
定位危险函数等基本操作使用一些匹配命令（grep等）就够了。
Fortify sca
惠普公司出的一款源代码审计软件
（http://www.freebuf.com/sectool/95683.html商业级别Fortify白盒神器介绍与使用分析）
RIPS
RIPS是一款不错的静态源代码分析工具，主要用来挖掘PHP程序的漏洞
（http://blog.c1gstudio.com/archives/1492PHP源代码安全漏洞自动化挖掘工具RIPS）

：

讲师：Monster、CongRong

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文