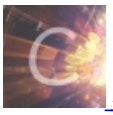
我看过的安全方面的好文章

原创

淡竹云开 于 2019-05-18 11:59:02 发布 608 收藏 2

分类专栏： 操作系统 学习

本文链接：https://blog.csdn.net/zhangpeterx/article/details/90313503


密码 同时被 3 个专栏收录

5 篇文章 0 订阅

订阅专栏


操作系统

12 篇文章 1 订阅

订阅专栏


学习

13 篇文章 1 订阅

订阅专栏

本文不定期更新，最后更新于2019-5-18

安全

- XSS的各种用途（窃取用户cookie、界面劫持…）
- 实战Teensy烧录渗透测试U盘
- 被长期忽视、却危害巨大的邮件追踪术
- 老歌新唱|PUNYCODE再利用
- 浅说 XSS 和 CSRF
- 我是如何拿下一个中学的官方网站的？ - 知乎专栏
- 黑客之死
- ROUTER HACKING HOW TO GET INSDE YOUR OWN ROUTER 855词
- 浅谈XML实体注入漏洞
- 在Linux中使用环境变量进行提权
- 谈一谈如何在Python开发中拒绝SSRF漏洞
- 【绿盟大讲堂】CTF夺旗赛最强秘籍Part1：密码学和隐写术
- CTF比赛中关于zip的总结
- XXE漏洞利用技巧：从XML到远程代码执行
- 如何攻击 LTE 4G 网络
- Wifi 四次握手认证过程介绍

- RFID 低频卡安全分析
- 轻松理解什么是 C&C 服务器
- Linux下几种反弹Shell方法的总结与理解
- 2017 年度文章汇总 信安之路
- sqlmap 内核分析 I: 基础流程
- XSS 笔记
- 关于Shell你想知道的都在这儿
- 目录遍历 git泄露 ISG 2018 Web Writeup
- 利用动态二进制加密实现新型一句话木马之Java篇
- XXE(XML External Entity attack)XML外部实体注入攻击
- SQL和NoSQL注入浅析（上）
- 从零开始内网渗透学习
- Android App渗透测试工具分享
- SQL注入ByPass的一些小技巧
- JavaScript中的堆漏洞利用（翻译）
- WAF攻防之SQL注入篇
- 用 javascript 框架绕过 XSS 防御
- 一个人的安全部之企业信息安全建设规划
- web狗要懂的内网端口转发
- **Windows 提权命令指南**
- 快速找出网站中可能存在的XSS漏洞实践(一)
- 你不曾察觉的隐患：危险的 target="_blank" 与 “opener”
- 谈谈我对NoSQL注入的一点研究
- 一份来自Savory Chicken的SQL注入学习笔记
- CTF中的PHP反序列化漏洞简单分析
- 新手科普 | MySQL手工注入之基本注入流程
- SQL注入的优化和绕过
- Crypto-RSA-公钥攻击小结
- Shodan自动化利用
- GraphQL安全指北
- noxCTF部分writeup(欢迎吐槽QAQ)
- 【CTF 攻略】第14届全国大学生信息安全与对抗技术竞赛（ISCC 2017）
- OpenSSL Command-Line HOWTO
- 使用 linux 操控小米手环 1 代
- 伪造电子邮件以及制造电子邮件炸弹的攻防探讨
- OpenSSL error alert handshake failure
- SQL和NoSQL注入原理剖析（上）
- SQL和NoSQL注入浅析（下）
- 破解Zip加密文件常用的几种方法

- 即时通讯安全篇（一）：正确地理解和使用Android端加密算法
- 即时通讯安全篇（二）：探讨组合加密算法在IM中的应用
- 即时通讯安全篇（三）：常用加解密算法与通讯安全讲解
- 即时通讯安全篇（四）：实例分析Android中密钥硬编码的风险
- 即时通讯安全篇（五）：对称加密技术在Android平台上的应用实践
- 即时通讯安全篇（六）：非对称加密技术的原理与应用实践
- 即时通讯安全篇（七）：如果这样来理解HTTPS，一篇就够了
- 我是如何拿下一个中学的官方网站的？ - 知乎专栏
- 浅谈PHP安全规范
- **如何在CTF中少走弯路（基础篇）**
- 新手指南：Bwapp之XSS –stored
- 老司机带你过常规WAF
- MD5哈希注入的两种方式
- linux下fuzz初试
- 关于 fuzz 的一些思考
- 前端安全系列（一）：如何防止XSS攻击？
- 前端黑魔法之远程控制地址栏
- 前端安全系列（一）：如何防止XSS攻击？
- RFID 破解基础详解
- 如何使用BackTrack破解WIFI无线网络的WEP密钥
- WPA2 “KRACK”漏洞简介与重现
- WEP算法的安全性
- iPad及BT4下的WEP破解实验与分析 | Network Security
- 短网址安全浅谈
- 警惕新的蓝牙技术：你的行踪，beacon网络全知道
- 14 - WEP Koreks Chopchop Attack
- 兜哥带你学安全
- 学点算法做安全之垃圾邮件识别（下）
- AI与安全的恩怨情仇五部曲「1」：Misuse AI
- 安全协议系列----WEP详解
- How ChopChop attack against WEP actually works?
- Chopchop theory
- 安全报告 | 从恶意流量看2018十大互联网安全趋势
- EMV新规范将实施，非接触支付中的中继攻击与近距离攻击是否完全得到防护？
- Getting Started with Bluetooth Hacking
- Kali下的蓝牙设备侦察方法介绍
- 基于LPN问题的RFID安全协议设计与分析
- 安全研究 | 传真机的攻击面研究报告

- 安卓手机搭建渗透环境（无需Root）
- 利用小米手机的门卡模拟功能模拟校园卡门禁
- RFIDHacKing硬件的有趣事情
- 【墨家】RFID入门：Mifare1智能水卡破解分析
- 一次对路边饮用水RFID供应机的跑路玩法
- RFID渗透工具教程
- RFID 破解基础详解
- Wfuzz初上手
- 如何使用基于整数的手动SQL注入技术
- 前端安全系列（二）：如何防止CSRF攻击？
- 使用Python CGIHTTPServer绕过注入时的CSRF Token防御
- How I hacked modern Vending Machines
- Unicode等价性浅谈
- 一键安装藏隐患，phpStudy 批量入侵的分析与溯源
- Bluetooth Hacking, Part 3: The BlueBourne Exploit
- 识别验证新花样：如何用心跳进行身份识别
- **Linux应急故事之四两拨千斤：黑客一个小小玩法，如何看瞎双眼**
- 老砖家深度解析WPA2安全漏洞
- KRACK Attacks: Breaking WPA2
- Understanding WPA/WPA2 PSK Hash Cracking
- 4-Way Handshake | WLAN by german engineering
- **Shellcode与加密流量之间的那些事儿**
- 记一次挖矿病毒分析 - FreeBuf互联网安全新媒体平台
- SQLMap Insert注入踩坑记 - FreeBuf互联网安全新媒体平台
- 使用 linux 操控小米手环 1 代
- Relay attack - Wikipedia
- 【永不消逝的电波（二）】HackRF入门：家用无线门铃信号重放
- 永不消逝的电波（三）：低功耗蓝牙（BLE）入门之如何调戏别人的小米手环
- 从车联网安全到BLE安全（二） - FreeBuf互联网安全新媒体平台
- nladuo/IoT-Firstep: 一个物联网(IoT)开发的入门教程。涉及单片机、上位机、移动应用、服务器后台开发的知识。以及蓝牙4.0、以太网模块的使用实例。
- 浅析SSTI(python沙盒绕过)_白帽子技术/思路_i春秋社区-分享你的技术，为安全加点温度.
- BLE安全初探之HACKMELOCK
- **Macr0phag3/Sniffer: A Sniffer for Open-WLAN**
- 初探APT 攻击
- Bypass 360主机卫士SQL注入防御（多姿势）_白帽子技术/思路_i春秋社区-分享你的技术，为安全加点温度.
- 【反欺诈专栏】互联网黑产剖析——虚假号码
- 学信安 莫装逼 否则追悔莫及
- 第20天：使用Scapy在15行代码中跟踪路由

- How to install Android Nougat on VMware Workstation 14 Pro - vPirate
- 网络利器之Scapy_白帽子技术/思路_i春秋社区-分享你的技术，为安全加点温度.
- Biased RSA moduli and ROCA
- Microsoft Word - A very simple example of RSA encryption
- 起底游戏、会员代充背后的洗钱之术，你可能是“帮凶”
- 腾讯云网站管家WAF体验：聊聊AI作为WAF市场转折的趋势
- AI in WAF | 腾讯云网站管家 WAF AI 引擎实践
- AI in WAF | 腾讯云网站管家 WAF AI 引擎实践（下篇）
- WAF开发之自学习模式开发实战
- **如何绕过 Web 应用程序防火墙（WAF）？**
- 关于WAF的那些事
- WAF开发之自学习模式开发实战
- 机器学习入门之像使用Print一样使用算法检测WebShell
- Java SQL 注入学习笔记
- **基于Docker的蜜罐平台搭建：T-Pot 17.10**
- Docker安全配置分析
- 【安全科普】Linux提权——利用可执行文件SUID
- 网赚灰产不归人——雅贼归来（上） -卢松松博客
- 权限系统设计模型分析（DAC，MAC，RBAC，ABAC）
- Meltdown漏洞利用解读（Part 1）：基础篇
- 浅谈处理器级Spectre Attack及Poc分析
- 宇宙最强，meltdown论文中英文对照版(一)
- 【年度大戏】勒索”嘿客“无间道之战
- 2018年Windows漏洞年度盘点
- 【权威发布】吾爱破解论坛2018年原创区TOP榜（下）
- 使用标签时，你可能会忽略的一个安全问题
- 利用分块传输吊打所有WAF
- **IC卡真的安全吗？—实战crack学校饭卡过程**
- 老瓶装新酒：认识IBM符号链接攻击及防御手段 - 推酷
- 基于docker搭建开源扫描器——伏羲_白帽子技术/思路_i春秋社区-分享你的技术，为安全加点温度.
- T-Pot Universal Installer and ISO Creator
- 树莓派：T-Pot多蜜罐平台使用心法 - FreeBuf互联网安全新媒体平台
- Windows ADS在渗透测试中的妙用 - FreeBuf互联网安全新媒体平台
- 什么是全同态加密？
- 完全同态加密 - xiaoluo91的专栏 - CSDN博客
- 全同态加密的发展与应用 - 安全内参 | 网络安全首席知识官
- 警惕！WinRAR漏洞利用升级：社工、加密、无文件后门 - FreeBuf互联网安全新媒体平台
- toplip：一款十分强大的文件加密解密 CLI 工具

- Automated Website Fingerprinting through Deep Learning
- DistriNet / DLWF：我们的NDSS'18论文"通过深度学习自动化网站指纹识别"的源代码
- StackOverFlow之Ret2ShellCode详解