

目录

前言	1.1
安全概览	1.2
安全通用知识	1.3
安全学习方法	1.3.1
CTF比赛	1.3.2
正向安全	1.3.3
漏洞编号	1.3.4
CVE	1.3.4.1
CNVD	1.3.4.2
Web端安全	1.4
渗透测试	1.4.1
常用工具	1.4.2
安全操作系统	1.4.2.1
Kali Linux	1.4.2.1.1
组织和标准	1.4.3
OWASP	1.4.3.1
设备端安全	1.5
计算机安全	1.5.1
移动安全	1.5.2
Android安全	1.5.2.1
iOS安全	1.5.2.2
工控物联网安全	1.5.3
特定设备安全	1.5.4
WiFi安全	1.5.4.1
Aircrack-ng	1.5.4.1.1
Wifiphisher	1.5.4.1.2
信息存储安全	1.6
硬件	1.6.1
TrustZone	1.6.1.1
软件	1.6.2
TEE	1.6.2.1
其他安全相关	1.7
代码审计工具	1.7.1
Checkmarx CxEnterprise	1.7.1.1
Armorize CodeSecure	1.7.1.2

Fortify	1.7.1.3
RIPS	1.7.1.4
相关工具	1.7.2
抓包工具	1.7.2.1
Wireshark	1.7.2.1.1
破解密码	1.7.2.2
John the Ripper	1.7.2.2.1
Hashcat	1.7.2.2.2
Hydra	1.7.2.2.3
代理工具	1.7.2.3
远程操作工具	1.7.2.4
附录	1.8
资料和文档	1.8.1
参考资料	1.8.2

信息安全概览

- 最新版本: v2.0
- 更新时间: 20210525

简介

边学习信息安全技术，边总结技术教程。已整理出宏观的各个方面的安全的分类和概念。以及基本的计算机安全、移动端安全、物联网安全等细节内容。目前已把部分内容抽出成独立子教程，包括渗透测试、二进制安全、iOS安全、Android安全、工控安全。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

Gitbook源码

- [crifan/information_security_overview: 信息安全概览](#)

如何使用此Gitbook源码去生成发布为电子书

详见：[crifan/gitbook_template: demo how to use crifan gitbook template and demo](#)

在线浏览

- [信息安全概览 book.crifan.com](#)
- [信息安全概览 crifan.github.io](#)

离线下载阅读

- [信息安全概览 PDF](#)
- [信息安全概览 ePUB](#)
- [信息安全概览 MOBI](#)

版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 admin 艾特 crifan.com，我会尽快删除。谢谢合作。

鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

更多其他电子书

本人 `crifan` 还写了其他 100+ 本电子书教程，感兴趣可移步至：

[crifan/crifan_ebook_readme: Crifan的电子书的使用说明](#)

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新： 2021-05-25 22:58:17

安全概览

背景

先说说写这个教程的背景：

- 之前已写过 安卓安全和破解 的教程
 - https://github.com/crifan/android_app_security_crack
 - 目前点赞不少： 600+ 个star
 - 看来大家比较关注这个领域
- 自己计划从事 计算机安全领域 ~≡ 信息安全 ~≡ 网络安全
 - 之前是小白，没这方面的经验
 - 打算边自学，边总结
 - 总结到此教程（和相关子教程）中
 - 供自己和他人参考

信息安全技术概览

信息安全技术概念包含内容较多，且涉及维度较广，下面以不同维度来阐述，常见分类和对应内容。

- 信息安全
 - 概述

Web应用程序	桌面应用
应用技术	
Apache AngularJS JavaScript ASP.NET Django OAuth HTML WebSockets WordPress Python Java Ruby Spring Framework PHP Nginx JSON Laravel RESTful APIs XML React WebRTC MVVM MVC HTTP Ruby on Rails Session Cookies Local Storage Cookie Flags	System Services PE Anatomy Protocol Analysis Privilege Rings Windows Internals COM WMI Impersonation Levels .NET Kernel Space C UAC MOF Calling Modes WCF User Space C# Device Drivers x86/x64 Assembly Process Tokens C++ Named Pipes Windows Registry
进攻性和防守性概念	
Certificate Pinning Code Execution Principle of Least Privilege Clickjacking XSS XXE LFI Open Redirect Authentication Bypass Authorization Issues SQLi RFI CSRF Password Policy Account Lockout Cookie Flags Fail Secure SSL/TLS Issues Defense in Depth Separation of Duties	Defense in Depth Code Execution Write Primitive Stack Pivot JIT Spray Mitigation Circumvention Stack Overflow PatchGuard Principle of Least Privilege Read Primitive SafeSEH Memory Corruption Stack Cookies Use-after-Free SMEP DEP ASLR Bootkits SMAP Write-What-Where Primitive Rootkits Heap Spray Information Leak CFG DSE ROP Gadgets Separation of Duties Fail Secure Evasion and Stealth Heap Overflow Exploit Mitigations

- 根据不同 端 = 目标 = 设备 或 侧重点 = 方向 分
 - 远程 -> Web端 : 网络安全 = Web安全 = 互联网安全
 - 不同侧重点 = 攻防
 - 攻 = 攻击: 渗透测试
 - 详见: [潜入你的网络: 渗透测试](#)
 - 防 = 防护:
 - 安全开发 = 安全功能开发
 - 安全分析
 - 不同数据源
 - 日志 -> 安全日志分析
 - (路由器、防火墙的) 数据包 -> 深度包检测 = DPI
 - 结果
 - 态势感知
 - 攻击溯源
 - 本地=本机 -> 设备端
 - PC端 = 桌面端 : 计算机安全
 - 包含
 - Windows
 - 最常见的、涉及的领域: 二进制安全 ~= PWN

- -> Window漏洞挖掘 ~= Windows漏洞分析
 - 详见：[探究底层机制：二进制安全](#)
 - 移动端：移动安全
 - 包含
 - Android
 - 详见：[安卓安全和破解](#)
 - iOS
 - 详见：[防止iPhone被黑：iOS安全](#)
 - 往往涉及到，在 Mac 和 Linux 中运行相关安全和破解的工具
 - -> 所以也就包含了 Mac 和 Linux 相关安全内容
 - IoT端：物联网安全 ~= 工控安全
 - 详见：[工控安全概览](#)
 - 其他特定设备
 - WiFi安全
- 广义的信息安全
 - 子领域=特殊领域
 - 信息存储安全
 - 典型应用场景：指纹、虹膜、信用卡PIN码等
 - 包含
 - 硬件
 - TrustZone
 - 软件
 - OP-TEE

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:45:14

安全通用知识

此处整理各方面的安全的基础和通用的知识。

破解 vs 开发

- 破解：属于 逆向
- 开发：属于 正向

常见术语和名词

- 常见术语和名词
 - 后渗透
 - 红方 蓝方
 - 威胁建模分析
 - PIA分析
 - malware
 - 恶意程序=恶意软件
 - 逆向工程师

常见问题

问：做安全的破解的，是否一定要会开发？

- 答：不一定。但最好会。
 - 做安全破解的，会开发，属于加分项。
 - 原因也很简单
 - 就像：做逆向破解的就像小偷去你别家偷东西
 - 肯定没有，作为正向开发，作为开发商建造房子的你，对房子内部构造更熟悉，更容易找到突破口，找到可能的漏洞，并充分利用漏洞去实现自己的攻击。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:45:03

安全学习方法

- 看漏洞公告
 - 在看的过程中理解漏洞
 - 在看的过程中学习调试和汇编指令
- 下载和研究POC
 - 来源
 - 看雪论坛
 - 等

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:48:40

CTF比赛

TODO:

继续看完：

Getting Started - CTF Wiki

<https://ctf-wiki.github.io/ctf-wiki/>

并整理过来。

- CTF比赛
 - =夺旗赛
 - =CTF= Capture The Flag
 - 是什么：一个比赛
 - 在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式
 - 起源：
 - 1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式
 - 2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的"世界杯"
 - 竞赛模式
 - 解题模式
 - 在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别
 - 大多数为线上比赛，选手自由组队（人数不受限制），出题者把一些信息安全实战中可能遇到的问题抽象成一个题目，比如一个存在漏洞的网站让选手入侵，一个有漏洞的程序让选手分析来写出漏洞利用程序，一段密文让选手解密，一个图片选手从里面找出隐藏的线索等等。在完成这些出题的题目后，可以获得一串奇怪的字符串，也就是所谓的flag，提交它，就能获得这道题目的分数
 - 攻防模式=Attack-Defense
 - 在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。
 - 大多数为线下比赛，参赛队伍人数有限制（通常为3到5人不等），参赛队伍保护自己的服务器，攻击其他队伍的服务器，每

个队伍的服务器开始拥有相同的配置和缺陷，比如几个有漏洞的二进制程序、有漏洞的Web应用、某些权限账户弱口令等等，然后队员需要找出这些漏洞并进行加固，同时利用这些漏洞来攻击别人的服务器，拿到其他队伍的权限后，会获取到相应flag后提交，从对方身上赚取相应的分数，每隔一段时间后，可以再次攻击并利用未加固的漏洞获取flag并赚取分数

- 混合模式=mix

- 结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。
- 解题模式和攻防模式同时进行，解题模式可能会根据比赛的时间、进度等因素来释放需解答的题目，题目的难度越大，解答完成后获取的分数越高；攻防模式会贯穿整个CTF比赛的始终，参赛队伍需不断积累分数，最终参赛队伍的名次由两种模式累积的分数总和决定。有些有趣的CTF比赛，还会引入一些情景剧情和现场观众的互动，来增加比赛的趣味性

- 题目类别

- WEB=网络安全

- WEB是CTF竞赛的主要题型，题目涉及到许多常见的WEB漏洞，诸如XSS、文件包含、代码执行、上传漏洞、SQL注入。也有一些简单的关于网络基础知识的考察，例如返回包、TCP-IP、数据包内容和构造。可以说题目环境比较接近真实环境。
- 所需知识：PHP、python、TCP-IP、SQL

- MISC=安全杂项

- MISC即安全杂项，题目涉及隐写术、流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广，主要考查参赛选手的各种基础综合知识。
- 所需知识：常见隐写术工具、wireshark等流量审查工具、编码知识。

- Crypto=密码学

- 题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术，以及一些常见编码解码，主要考查参赛选手密码学相关知识点。通常也会和其他题目相结合。
- 所需知识：矩阵、数论、古典密码学

- Reverse=逆向工程

- 题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。主要考查参赛选手的逆向分析能力。
- 所需知识：汇编语言、加密与解密、常见反编译工具

- PPC=编程类题目

- 题目涉及到程序编写、编程算法实现，当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。题目较少，一般与其他类型相结合。
- 所需知识：基本编程思路、C,C++,Python,php皆可

- PWN=二进制安全

- PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。主要考察参赛选手对漏洞的利用能力。

- 所需知识: C, OD+IDA, 数据结构, 操作系统

- 基础知识

- 语言运用

- 计算机语言可以大致分为机器语言, 汇编语言, 高级语言, 计算机每进行的一次动作, 一个步骤, 都是按照计算机语言编好的程序来执行。而在CTF比赛中, 计算机语言的了解与掌握会有事半功倍的效果, 进程的动态调试、防护脚本的编写、源代码审计等工作都是建立在对计算机语言有所掌握的基础上进行的。

- Web安全

- 目前国内大多数CTF比赛都以Web安全为主, 但是Web安全涉及的内容非常广泛, 就典型的Web服务来说, 其安全问题可能来自于Web服务器、数据库、Web程序本身与开发语言等。了解一个Web应用的组成架构、装载与配置、指令操作及组件缺陷, 是参赛者知识储备环节中不可或缺的部分。

- 安全加固

- 安全领域的精髓在于攻防, 在CTF比赛也是同样的道理, 比赛成绩不仅取决于在有效的时间内拿下多少flag, 还取决于能抵御多少次外来攻击。有一些比赛队伍不注重或者不善于漏洞加固, 即使得到很多分数, 但是优势还是会慢慢的蚕食掉。所以, 了解漏洞的产生原因、减小漏洞的影响范围以及行之有效的安全加固也是一个成功队伍的重要能力。

- 密码算法

- 参赛者需要了解主流的密码算法, 如对称密码、公钥密码、流密码、哈希密码算法等。在不断的攻防对抗中, 一些关键信息或者突破口, 往往会通过算法的加解密将它们“隐藏”起来增加解题难度。此外还会伴随着弱口令尝试, 密码字典的暴力猜解等。

- 网络取证

- 对于网络攻击行为的溯源分析、漏洞挖掘过程中的抓包分析往往是很参赛队伍在攻防对抗中忽略的问题, 能够在最短的时间内抓到线索并做出行之有效的响应, 这方面的能力也就成为了高手和顶尖高手之间的分水岭, 古人常说: “天下大事, 必作于细; 天下难事, 必成于易”, 我想应该就是这个道理

CTF赛事

- 国外

- DEFCON CTF: CTF赛事中的“世界杯”
- UCSB iCTF: 来自UCSB的面向世界高校的CTF
- Plaid CTF: 包揽多项赛事冠军的CMU的PPP团队举办的在线解题赛
- Boston Key Party: 近年来崛起的在线解题赛
- Codegate CTF: 韩国首尔“大奖赛”, 冠军奖金3000万韩元
- Secuinside CTF: 韩国首尔“大奖赛”, 冠军奖金3000万韩元
- XXC3 CTF: 欧洲历史最悠久CCC黑客大会举办的CTF
- SIGINT CTF: 德国CCCAC协会另一场解题模式竞赛
- Hack.lu CTF: 卢森堡黑客会议同期举办的CTF
- EBCTF: 荷兰老牌强队Eindbazen组织的在线解题赛

- Ghost in the Shellcode：由Marauders和Men in Black Hats共同组织的在线解题赛
- RwthCTF：由德国OldEur0pe组织的在线攻防赛
- RuCTF：由俄罗斯Hackerdom组织，解题模式资格赛面向全球参赛，解题攻防混合模式的决赛面向俄罗斯队伍的国家级竞赛
- RuCTF：由俄罗斯Hackerdom组织面向全球参赛队伍的在线攻防赛
- PHD CTF：俄罗斯Positive Hacking Day会议同期举办的CTF
- 国内
 - XCTF全国联赛：中国网络空间安全协会竞评演练工作组主办、南京赛宁承办的全国性网络安全赛事平台，2014-2015赛季五站选拔赛分别由清华、上交、浙大、杭电和成信技术团队组织（包括杭电HCTF、成信SCTF、清华BCTF、上交OCTF和浙大ACTF），XCTF联赛总决赛由蓝莲花战队组织。XCTF联赛是国内最权威、最高技术水平与最大影响力的网络安全CTF赛事平台
 - AliCTF：由阿里巴巴公司组织，面向在校学生的CTF竞赛，冠军奖金10万元加BlackHat全程费用
 - XDCTF：由西安电子科技大学信息安全协会组织的CTF竞赛，其特点是偏向于渗透实战经验
 - HCTF：由杭州电子科技大学信息安全协会承办组织的CTF
 - 杭州电子科技大学信息安全协会由杭州电子科技大学通信工程学院组织建立，协会已有七年历史，曾经出征DEFCON,BCTF等大型比赛并取得优异成绩，同时协会还有大量有影响力的作品。协会内部成员由热爱黑客技术和计算机技术的一些在校大学生组成，有多个研究方向，主要有渗透，逆向，内核，web等多个研究方向。至今已经成功举办6次CTF比赛
 - ISCC：由北理工组织的传统网络安全竞赛，最近两年逐渐转向CTF赛制
 - TCTF：TCTF由中国网络空间安全协会竞评演练工作委员会指导、腾讯安全发起、腾讯安全联合实验室主办，Oops战队和北京邮电大学协办的CTF竞赛

CTF平台

FBCTF

- FBCTF
 - GitHub
 - <https://github.com/facebook/fbctf/>
 - 简介
 - 一套开源比赛平台，包括游戏地图、团队登记和评分系统。还可以按需提供逆向工程逆向工程、Web应用安全、取证、二进制开发和加密等挑战。用户还可以使用Facebook CTF平台定制或自定义挑战项目

绿盟科技CTF平台

- 绿盟科技CTF平台
 - 架构：

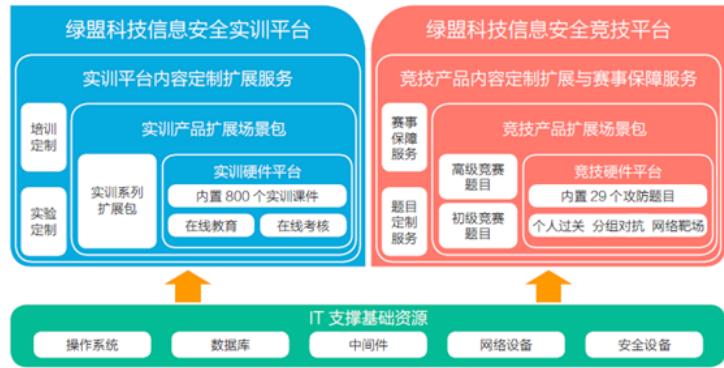


图1.1 绿盟科技信息安全攻防实训与竞技产品结构图

- 整体方案采用B/S架构对外提供新安全课件培训、实验训练和攻防保障服务。使用人员可以结合自身情况，灵活选取远程在线和线下面对面的实时教学形式。
- 两个平台可以支持进行课件培训、实验训练和攻防保障三大功能。课件培训主要以课件宣讲为主，实现信息安全知识的直接传递；实验训练以安全攻防模拟操作实验为主，使得被培训对象对安全技术的建立直观印象；攻防保障主要为被培训对象提供攻防的虚拟环境，实际检验被培训对象的安全水平。
- IT支撑基础资源主要包括安操作系统、数据库、中间件、网络设备和安全设备等，通过与虚拟技术相结合，用以保障上层的实训场景和竞技场景。
- 绿盟信息安全实训系统
 - ISTS -Information Security Trainning System
 - 信息安全培训、教学及科研提供一个完整的、一体化的实验教学环境
- 绿盟信息安全竞技系统
 - ISCS -Information Security Competition System
 - 围绕信息安全理论和知识，组建的信息安全对抗技能实战赛。也可以承载信息安全对抗攻防演练项目，考察攻防演练者网络安全理论知识与实际问题处理能力，旨在借助攻防演练培养一批具备信息安全素养的优秀实战专业的安全人员。
 - 模式：
 - 安全攻防竞赛平的攻防竞赛模式可以分为三种形式
 - 单兵作战挑战赛=个人挑战模式
 - 个人挑战模式每个赛题（关卡）是一个单独的靶场，并提供了七大类赛题，WEB、密码学、隐写、溢出、逆

向、编程、综合，全面考察参赛选手的安全能力，题目由易到难。



- 综合靶场
- 网络混战



看雪CTF

- 看雪CTF
 - <https://ctf.pediy.com>
 - 看雪CTF（简称KCTF）是圈内知名度最高的技术竞技，从原CrackMe攻防大赛中发展而来，采取线上PK的方式，规则设置严格周全，题目涵盖Windows、Android、iOS、Pwn、智能设备、Web等众多领域

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2021-05-25 22:53:18

正向安全

- 正向安全 防护手段
 - 混淆
 - Android
 - 加入 花指令
 - 用于干扰的垃圾代码
 - Mac
 - iOS
 - OC的混淆
 - Android 和 Windows
 - 加壳
 - 加固=防护 的一种手段
 - 不同系统=平台
 - Windows
 - vmprotect
 - 强壳
 - Linux
 - upx
 - Android
 - Mac
 - App Store的ipa
 - Android
 - SO的保护
 - 是什么
 - APP的核心（认证逻辑，加密等）算法采用C/C++编写并编译为SO文件
 - 目的 = 为何要SO防护
 - 增加被破解=反编译的难度
 - 增加黑客利用其业务的难度
 - 优势
 - SO中为原生ARM汇编，难以还原原始代码
 - 对比：DEX文件很容易被各种反编译工具直接还原成通俗易懂的Java代码
 - SO调试成本高
 - 对比：Java写的程序更容易被调试
 - 如使用SmaliIdea、Jeb、IDA、Xposed、插桩打日志等多种方式
 - SO难以在x86生产环境中黑盒调用
 - 对比：DEX文件可转换成class文件，在生产环境中使用JNI直接传参调用
 - 手段
 - 反调试
 - 区块加密
 - OLLVM 混淆

- OLLVM 混淆是逆向人员的噩梦，这招确实能有效提高 so 代码的安全性
 - 破解手段
 - unicorn
 - ARM VMP
 - ARM VMP 兼容性问题比较多，还无法商业化

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:56:09

漏洞编号

网络已存在的公开漏洞，一般都有个 漏洞编号

目前主要有2个漏洞编号相关组织：

- CVE
- CNVD

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:45:41

CVE

- CVE
 - 名称
 - CVE = Common Vulnerabilities and Exposures = 通用漏洞披露
 - 别称： 常见弱点与漏洞
 - 是什么： 一个与信息安全有关的数据库
 - 注意
 - 通常我们谈到的 CVE 指的是 CVE 编号 = CVE 漏洞编号
 - 是分配给每个安全漏洞的 CVE ID 编号
 - 作用： 收集各种信息安全弱点及漏洞并给予编号以便于公众查阅
 - 列出了已公开披露的各种计算机安全漏洞
 - 目的： 帮助 IT 专业人员协调自己的工作， 轻松地确定漏洞的优先级并加以处理， 从而提高计算机系统的安全性
 - 运营： 现由美国非营利组织 MITRE 所属的 National Cybersecurity FFRDC 所营运维护

CVE漏洞编号

- CVE 漏洞编号
 - 每一个通用漏洞披露都赋予一个专属的编号
 - 格式：
 - CVE-YYYY-NNNN
 - CVE： 固定的前缀字
 - YYYY： 西元纪年
 - NNNN： 流水编号
 - 原则上为四位数字，但必要时可编到五位数或更多位数
 - 例如
 - 于 2014 年发现的心脏出血漏洞 编号为 CVE-2014-0160

CVE 申请需要满足什么条件？

- 只有满足一系列特定条件的漏洞才会分配 CVE ID
 - 这些漏洞必须满足以下条件：
 - 1. 可以单独修复。
 2. 该漏洞可以独立于所有其他错误进行修复。
 - 2.
 - 已得到相关供应商的确认。
 - 软件或硬件供应商已确认错误，并承认其会对安全性造成负面影响。
 - 或者
 - 已记录在案。
 - 错误报告者已共享了一份相关的漏洞报告，表明错误会造成负面影响，且有悖于受影响系统的安全策略。

1. 会影响某个代码库。
2. 如果漏洞会对多个产品造成影响，则会获得单独的 CVE。对于共享的库、协议或标准，只有在使用共享代码会容易受到攻击时，该漏洞才会获得单个 CVE。否则，每个受影响的代码库或产品都会获得一个唯一的 CVE

CVE漏洞编号是谁颁发的？

CVE开始是由 MITRE Corporation 负责日常工作的。但是随着漏洞数量的增加，MITRE 将漏洞编号的赋予工作转移到了其 CNA = CVE Numbering Authorities 成员。

CNA 涵盖5类成员，目前共有69家成员单位：

1. MITRE：可为所有漏洞赋予 CVE 编号；
2. 软件或设备厂商：如 Apple、Check Point、ZTE 为所报告的他们自身的漏洞分配 CVE ID。该类成员目前占总数的80%以上。
3. 研究机构：如 Airbus，可以为第三方产品漏洞分配编号；
4. 漏洞奖金项目：如 HackerOne，为其覆盖的漏洞赋予 CVE 编号；
5. 国家级或行业级CERT：如 ICS-CERT、CERT/CC，与其漏洞协调角色相关的漏洞。

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:49:25

CNVD

- CNVD
 - = China National Vulnerability Database =中国 国家信息安全漏洞共享平台
 - 一句话介绍：中国版的 CVE
 - 简介
 - 由 国家计算机网络应急技术处理协调中心 （中文简称 国家互联应急中心，英文简称 CNCERT ）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库
 - 资料
 - 官网
 - 国家信息安全漏洞共享平台
 - <https://www.cnvd.org.cn>

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:45:54

Web安全

此处整理和Web网络相关的安全相关知识。

- Web安全
 - 根据攻防角度分
 - 进攻
 - 名字和概念
 - 漏洞扫描
 - 端口扫描
 - Web攻击 = Web漏洞攻击
 - Web挖掘 = Web漏洞挖掘
 - Web渗透
 - 攻击方式
 - SQL注入
 - XSS
 - CSRF
 - 越权
 - 文件包含
 - 文件上传
 - 命令执行
 - WAF绕过
 - URL跳转
 - 钓鱼
 - 社工 = 社会工程学
 - 防守
 - 代码审计 = 安全代码审计 = 安全审计
 - 目的：写出高质量的漏洞少的代码
 - 日志分析 = 安全日志分析 = 日志关联分析
 - 深度包检测
 - 程序行为监视
 - 防护设备
 - 防火墙
 - WAF = Web应用程序防火墙
 - IDS = Intrusion Detection Systems = 入侵检测系统
 - IPS = Intrusion Prevention Systems = 入侵防御系统
 - 相关组织和标准
 - 组织：OWASP
 - 标准：OWASP10
 - 主要工作方向和内容
 - 渗透测试
 - 漏洞挖掘
 - 安全开发
 - 代码审计
 - 代码审计 = 代码安全审计 = 安全编码审计 = 源代码审计 = 源代码安全分析
 - 网络安保

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:51:02

渗透测试

详见独立教程：

- [潜入你的网络：渗透测试](#)

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:45:30

常用工具

此处整理Web安全中常用的一些工具。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:45:00

安全操作系统

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:54:22

Kali Linux

- = Kali Linux
- 是什么：一个Linux操作系统，专门用于渗透测试，
 - Kali
 - = Kali Linux
 - 旧称： BackTrack Linux
 - 是什么：一个操作系统
 - 用途：专门用于安全、逆向、破解的
 - 特点：自带大量相关工具
 - 被称为
 - 网络安全人员的专用系统
 - 资料
 - 主页
 - Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution
 - <https://www.kali.org>
 - 包含工具
 - 首页
 - Penetration Testing Tools - Kali Linux
 - <https://tools.kali.org>
 - Kali Linux Tools Listing | Penetration Testing Tools
 - <https://tools.kali.org/tools-listing>
 - 根据分类
 - Information Gathering
 - ace-voip
 - Amap
 - APT2
 - arp-scan
 - Automater
 - bing-ip2hosts
 - braa
 - CaseFile
 - CDPSnarf
 - cisco-torch
 - copy-router-config
 - DMitry
 - dnmap
 - dnsenum
 - dnsmap
 - DNSRecon
 - dnstracer
 - dnswalk
 - DotDotPwn
 - enum4linux
 - enumIAX

- EyeWitness
- Faraday
- Fierce
- Firewalk
- fragroute
- fragrouter
- Ghost Phisher
- GoLismero
- goofile
- hping3
- ident-user-enum
- InSpy
- InTrace
- iSMTP
- lbd
- Maltego Teeth
- masscan
- Metagoofil
- Miranda
- nbtscan-unixwiz
- Nikto
- Nmap
- ntop
- OSRFramework
- p0f
- Parsero
- Recon-ng
- SET
- SMBMap
- smtp-user-enum
- snmp-check
- SPARTA
- sslaudit
- SSLsplit
- sslstrip
- SSLyze
- Sublist3r
- THC-IPV6
- theHarvester
- TLSSLed
- twofi
- Unicornscan
- URLCrazy
- Wireshark
- WOL-E
- Xplico
- Vulnerability Analysis
 - BBQSQL

- BED
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- copy-router-config
- Doona
- DotDotPwn
- HexorBase
- jSQL Injection
- Lynis
- Nmap
- ohrwurm
- openvas
- Oscanner
- Powerfuzzer
- sfuzz
- SidGuesser
- SIPArmyKnife
- sqlmap
- Sqlninja
- sqsus
- THC-IPV6
- tnscmd10g
- unix-privesc-check
- Yersinia
- Exploitation Tools
 - Armitage
 - Backdoor Factory
 - BeEF
 - cisco-auditing-tool
 - cisco-global-exploiter
 - cisco-ocs
 - cisco-torch
 - Commix
 - crackle
 - exploitdb
 - jboss-autopwn
 - Linux Exploit Suggester
 - Maltego Teeth
 - Metasploit Framework
 - MSFPC
 - RouterSploit
 - SET
 - ShellNoob
 - sqlmap
 - THC-IPV6
 - Yersinia

- Wireless Attacks
 - Airbase-ng
 - Aircrack-ng
 - Airdecap-ng and Airdecloak-ng
 - Aireplay-ng
 - airgraph-ng
 - Airmon-ng
 - Airodump-ng
 - airodump-ng-oui-update
 - Airolin-ng
 - Airserv-ng
 - Airtun-ng
 - Asleap
 - Besside-ng
 - Bluelog
 - BlueMaho
 - Bluepot
 - BlueRanger
 - Bluesnarfer
 - Bully
 - coWPAtty
 - crackle
 - eapmd5pass
 - Easside-ng
 - Fern Wifi Cracker
 - FreeRADIUS-WPE
 - Ghost Phisher
 - GISKismet
 - GqrX
 - gr-scan
 - hostapd-wpe
 - ivstools
 - kalibrate-rtl
 - KillerBee
 - Kismet
 - makeivs-ng
 - mdk3
 - mfcuk
 - mfoc
 - mfterm
 - Multimon-NG
 - Packetforge-ng
 - PixieWPS
 - Pyrit
 - Reaver
 - redfang
 - RTLSDR Scanner
 - Spooftooth

- Tkiptun-ng
- Wesside-ng
- Wifi Honey
- wifiphisher
- Wifitap
- Wifite
- wpaclean
- Forensics Tools=取证工具
 - Binwalk
 - bulk-extractor
 - Capstone
 - chntpw
 - Cuckoo
 - dc3dd
 - ddrescue
 - DFF
 - diStorm3
 - Dumpzilla
 - extundelete
 - Foremost
 - Galleta
 - Guymager
 - iPhone Backup Analyzer
 - p0f
 - pdf-parser
 - pdfid
 - pdgmail
 - peepdf
 - RegRipper
 - Volatility
 - Xplico
- Web Applications
 - apache-users
 - Arachni
 - BBQSQL
 - BlindElephant
 - Burp Suite
 - CutyCapt
 - DAVTest
 - deblaze
 - DIRB
 - DirBuster
 - fimap
 - FunkLoad
 - Gobuster
 - Grabber
 - hURL
 - jboss-autopwn

- joomscan
- jSQL Injection
- Maltego Teeth
- Nikto
- PadBuster
- Paros
- Parsero
- plecost
- Powerfuzzer
- ProxyStrike
- Recon-ng
- Skipfish
- sqlmap
- Sqlninja
- sqlsus
- ua-tester
- Uniscan
- w3af
- WebScarab
- Webshag
- WebSlayer
- WebSploit
- Wfuzz
- WhatWeb
- WPScan
- XSSer
- zaproxy
- Stress Testing
 - DHCPig
 - FunkLoad
 - iaxflood
 - Inundator
 - inviteflood
 - ipv6-toolkit
 - mdk3
 - Reaver
 - rtpflood
 - SlowHTTPTest
 - t50
 - Termineter
 - THC-IPV6
 - THC-SSL-DOS
- 其他方面对Kali的支持
 - Hopper Disassembler
 - Hopper - Download
 - <https://www.hopperapp.com/download.html?>
 - 专门提供Kali Linux的zip压缩包

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:47:18

组织和标准

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:54

OWASP10

- 在Web安全领域，有个组织叫：
 - OWASP
 - = Open Web Application Security Project
 - = 开源Web应用安全项目
 - = 开源Web应用安全组织
- 该组织每年会推出一个 标准： OWASP 10
 - OWASP列出了最重要的10个方面的安全攻击
 - 说明
 - 列出排名前10的攻击类型
 - 每年都会出一个报告
 - 最早：2003年
 - 最新：2017年
- 2017年的OWASP 10
 - Injection=注入攻击
 - 涉及方面
 - SQL
 - SQL Injection = SQL注入
 - NoSQL
 - OS
 - LDAP
 - LDAP Injection
 - 坏结果
 - 运行了不该运行的（恶意的）代码
 - Expression Language (EL) Injection
 - Command Injection
 - 获取了不该获取的数据=盗取数据
 - 心得
 - 编写接受数据的模块时要非常小心
 - 举例
 - request.getParameter()
 - request.getCookie()
 - request.getHeader()
 - Broken Authentication
 - =失效的身份
 - Sensitive Data Exposure
 - XXE
 - XML External Entities
 - Broken Access Control
 - =访问控制缺失
 - Security Misconfiguration
 - =安全配置错误
 - XSS
 - =Cross-Site Scripting
 - Insecure Deserialization

- Using Components with Known Vulnerabilities
 - =使用含有已知漏洞的组件
- Insufficient Logging & Monitoring
- 中文主页
 - Welcome to OWASP CHINA — OWASP-CHINA
 - <http://www.owasp.org.cn>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:18

设备端安全

和Web网络相对应的，可以统称为 设备端的安全。

主要包括：

- PC端
 - Windows
 - Mac
 - Linux
- 移动端
 - Android
 - iOS
- IoT =物联网设备

下面根据不同维度详细介绍。

可执行文件 逆向工程 工具

- Windows 的 PE 格式的 exe文件 、 dll文件
 - OllyDBG
 - IDA PRO
 - 二进制分析
 - Hiew
 - 反汇编 + 16进制编辑器
 - 命令行, 无GUI
- Linux 的 ELF 格式的文件
 - GDB
 - IDA PRO
 - Hopper
 - Disassembler + Pseudo C decompiler
 - Evan's debugger
 - Linux中类似于OllyDBG的工具
 - Insight
 - GDB的GUI
 - 有点过时了
- Mac 的 MACH-O 格式的文件
 - Hopper
 - IDA PRO
 - LLDB
 - MachOView
- Android 的 dex 格式的文件 (apk文件内的)
 - APK TOOL
 - Disassembler and Assembler (SMALI)
 - JEB
 - Android disassembler (SMALI) and decompiler (JAVA)
 - IDA PRO

- iOS 的可执行文件
 - IDA Pro
 - Hopper
 - otool

TODO:

【未解决】Mac中有哪些常用的破解逆向方面的工具软件

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:47:42

计算机安全

- PC端：计算机安全
 - 多平台
 - IDA
 - radare2
 - Windows
 - Windows安全
 - 详见：[探究底层机制：二进制安全](#)中的Windows部分内容
 - Mac+Linux
 - 详见：[防止iPhone被黑：iOS安全](#)中的Mac和Linux的部分
- 对比
 - 静态分析：IDA
 - 支持插件：
 - 最强大的：Hex-rays
 - 把汇编语言转换成C语言伪代码
 - 动态调试-》调试器：WinDBG、OllyDBG

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:47:41

移动安全

- 移动端：移动设备安全
 - Android
 - iOS

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:52:39

Android安全

- 概述
 - Apk逆向工具
 - Apktool
 - jd-gui
 - dex2jar
 - apk反编译
 - apk
 - 脱壳
 - 加壳
 - Smali/Baksmali代码
 - Android
 - Hook技术
 - Xposed
 - 虚拟化技术
 - VirtualApp
 - DroidPlugin
- 详解
 - [安卓应用的安全和破解](#)

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:27

iOS安全

- 详解
 - 防止iPhone被黑：iOS安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:48:29

工控物联网安全

工控安全，从概念上，基本上等价于最新出现的物联网安全

内容较多，且自成体系，现已整理至独立教程：

[工控安全概览](#)

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved，powered by
Gitbook最后更新：2021-05-25 22:48:07

特定设备安全

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:53:01

WiFi安全

- WiFi安全
 - Aircrack-ng
 - Wifiphisher
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:44:39

Aircrack-ng

- Aircrack-ng
 - 一句话描述：一种802.11 WEP和WPA-PSK密钥破解黑客工具
 - 可以在捕获到足够的数据包时恢复密码
 - 资料
 - 官网
 - <http://www.aircrack-ng.org>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:53:19

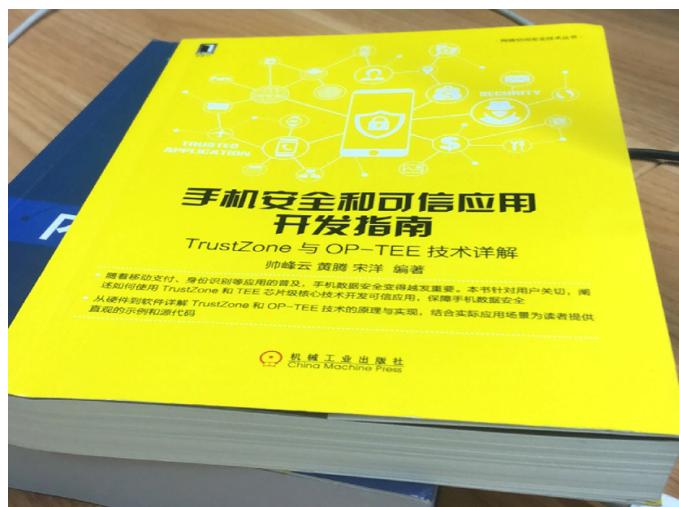
Wifiphisher

- Wifiphisher
 - 一句话描述：Wifiphisher是个伪造恶意接入点的工具，可针对WiFi网络发起自动化网络钓鱼攻击。
 - 于任务范围，Wifiphisher可致凭证获取或实际的感染

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:54:21

信息存储安全

- 信息存储安全
 - 应用场景和领域
 - 生物特征数据存储
 - 指纹
 - 虹膜
 - 信用卡PIN码（保存）
 - 私有密码（存储）
 - 客户数据（存储）
 - 受 DRM = Digital Rights Management = 数字版权管理 保护的媒体
 - 相关书籍
 - 《手机安全和可信应用开发指南》 TrustZone与OP-TEE技术详解



- 相关技术
 - 硬件层面
 - TrustZone
 - 软件层面
 - TEE

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:48:50

硬件

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:45:18

TrustZone

- TrustZone
 - ARM
 - 提出了 TrustZone 技术
 - 为了确保数据安全
 - 用一根 安全总线 (称为 NS 位) 来判断当前处于 secure world 还是 non-secure world 状态
 - 状态的切换由 ATF = ARM Trusted Firmware 来完成

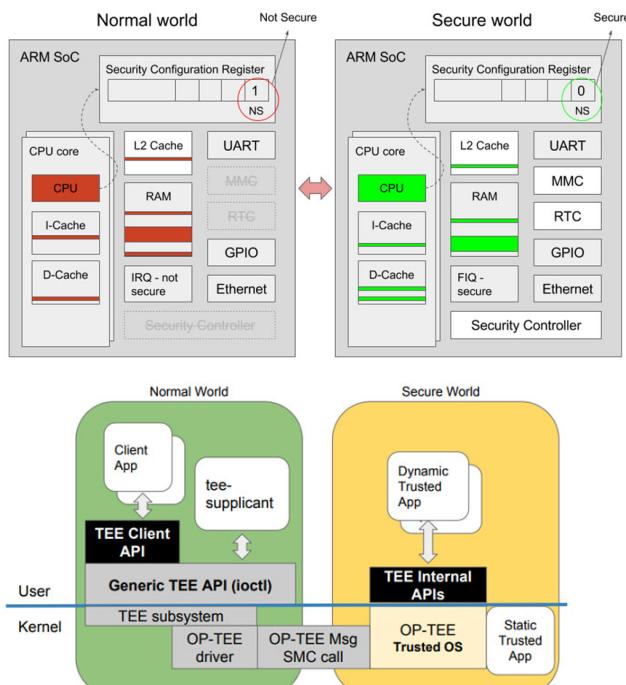
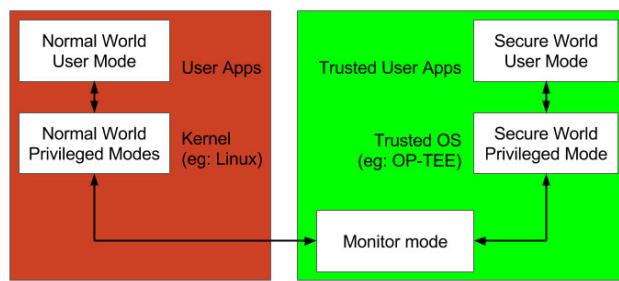
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:52:13

软件

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:52:57

TEE

- TEE = OP-TEE
 - 名称
 - TEE = Trusted Execution Environment = 信任执行环境 = 可信任执行环境
 - OP-TEE = Open Portable Trusted Execution Environment = Open-Source Portable Trusted Execution Environment = 开放可移植的可信任执行环境
 - 一句话描述
 - 基于TrustZone技术搭建的安全执行环境
 - designed as companion to a non-secure Linux kernel running on Arm
 - 注: Cortex-A cores using the TrustZone technology
 - 用途=目的=为什么
 - 为了更安全
 - 处理那些需要和安全密切相关的、需要保密处理的信息
 - 历史
 - 最早是ST-Ericsson开发的
 - <http://www.stericsson.com/>
 - 2013年, ST-Ericsson实现了兼容 GlobalPlatform
 - <https://globalplatform.org/>
 - 2013年之后, ST和Ericsson分开了
 - 现在TEE属于STMicroelectronics
 - https://www.st.com/content/st_com/en.html
 - 2013年后期, Linaro成立了 SWG = Security Working Group = 安全工作组
 - 其最重要的任务之一就是继续开发TEE
 - 在开源TEE之前, 花了很多个月去把之前部分私有模块, 换成开源实现
 - 包括: 密码库, 安全监控, 编译系统及其他
 - 2014-06-12, TEE开源了, 叫做OP-TEE
 - 目前现状主要是:
 - 项目属于STMicroelectronics
 - 但是Linaro和STMicroelectronics联合在开发
 - 2015年, 项目所有权从STMicroelectronics转给Linaro了
 - 资料
 - 官网
 - <https://www.op-tee.org>
 - GitHub
 - OP-TEE/optee_os: Trusted side of the TEE
 - https://github.com/OP-TEE/optee_os
 - 技术文档
 - OP-TEE Documentation — OP-TEE documentation documentation
 - <http://optee.readthedocs.io>
 - 主要设计目标
 - Isolation

- the TEE provides isolation from the non-secure OS and protects the loaded Trusted Applications (TAs) from each other using underlying hardware support,
- Small footprint
 - the TEE should remain small enough to reside in a reasonable amount of on-chip memory as found on Arm based systems
- Portability
 - the TEE aims at being easily pluggable to different architectures and available HW and has to support various setups such as multiple client OSes or multiple TEEs.
- OP-TEE 包含内容
 - Secure world OS= optee_os
 - 现有实现:
 - OP-TEE OS , Trusty , 高通的 QSEE , SierraTEE
 - 注: 所有方案的外部接口都会遵循 GP = Global Platform 标准
 - 对比: Normal world os
 - 普通操作系统: Linux、Android等
 - 问: 各家厂商和组织的 TEE OS 到底有何区别?
 - 答: TA 的添加和加载时的校验有所区别
 - 系统架构
 - 
 - 
- 相关概念

- TA = Trusted Application =可信应用
- CA = Client Application =客户端应用
- 原理
 - 产品开发团队负责开发一个运行在 Linux 上的 CA 和一个运行在 OP-TEE 上的 TA
 - CA 使用 TEE client API 与 TA 通信，并且从 TA 获取安全服务
 - CA 和 TA 使用 共享内存 进行通信
- 运行机制
 - 当处于 secure world 状态，那么就会执行 TEE OS 部分的代码
 - 当处于 non-secure world 状态时，就执行 linux kernel 部分的代码
- 举例

- 芯来科技和瓶钵信息合作开发基于RISC-V的TEE方案



- 其中也是符合TEE的架构
 - 可信区
 - 不可信区
- Normal world Client= optee_client
- test suite = optee_test/xtest
- linux驱动
- 常见问题
 - Linux内核
 - Linux内核能直接访问TEE部分的资源吗？
 - Linux kernel不能直接访问TEE部分的资源
 - Linux 内核如何才能访问TEE部分的资源呢？
 - Linux kernel能通过特定的 TA 和 CA 来访问TEE部分特定的资源

其他安全相关

安全方面的公司

- Veracode
 - Veracode提供一个基于云的应用程序安全测试平台
 - 无需购买硬件，无需安装软件，使用客户马上就可以开始测试和补救应用程序，另外Veracode提供自动化的静态和动态应用程序安全测试软件和补救服务

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:53:51

代码审计类

- 工具

- CxEnterprise
 - = Checkmarx CxEnterprise
- Armorize CodeSecure
- Fortify
 - = Fortify SCA
- RIPS

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:51:54

Checkmarx CxEnterprise

- Checkmarx CxEnterprise
-

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:29

Armorize CodeSecue

- Armorize CodeSecue
-

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:53:57

Fortify

- Fortify
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:48:15

RIPS

- RIPS
 -

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:52:26

相关技术和工具

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:46:38

抓包工具

- 网络流量分析 = 网络报文监听 = 网络协议分析
 - Wireshark

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:32

Wireshark

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:48:31

破解密码

- John the Ripper
- Hashcat
- Hydra

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:51:55

John the Ripper

- John the Ripper
 - 用GPU算力离线破解密码

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:50:03

Hashcat

- Hashcat
 - 评价
 - 世界上最快、最先进的密码恢复实用程序
 - 破解哈希的首选渗透测试工具
 - 功能
 - 支持多种猜测密码的蛮力攻击
 - 包括字典和掩码攻击
 - 说明
 - Hashcat在现代GPU显卡上运行最好
 - 传统的hashcat仍支持CPU上的哈希破解
 - 但是要提醒用户的是，这比显卡的处理能力要慢得多

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:52:43

Hydra

- Hydra
 - 可用于在线破解密码
 - 举例：SSH或FTP登录、IMAP、IRC、RDP等

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:53:01

代理工具

- 常见代理工具
 - Fiddler
 - 常用的抓包工具，有XSS自动化扫描插件
 - parosproxy
 - 一个对Web应用程序的漏洞进行评估的代理程序

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:45:37

远程操作工具

- `scp`
 - 终端命令，把远程设备的文件复制到另一个设备

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:52:39

附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:45:29

资料和文档

安全领域相关论坛

- 常见安全相关网站
 - 看雪
 - 简介：一个专注于PC、移动、智能设备安全研究及逆向工程的开发者社区！创建于2000年，历经20多年的发展，受到业内的广泛认同，在行业中树立了令人尊敬的专业形象。平台为会员提供安全知识的在线课程教学，同时为企业提供智能设备安全相关产品和服务
 - 特点
 - 历史悠久
 - 注重培养人才
 - 专业权威
 - 官网
 - <https://bbs.pediy.com/>
 - 安全客
 - 简介：安全客 - 安全资讯平台
 - 网站：<https://www.anquanke.com/>
 - FreeBuf
 - 简介：国内领先的互联网安全新媒体，同时也是爱好者们交流与分享安全技术的社区。
 - 官网
 - FreeBuf互联网安全新媒体平台
 - <https://www.freebuf.com>
 - t00ls
 - 简介
 - 十年民间网络安全老牌社区，聚合安全领域最优秀的人群，低调研究潜心学习讨论各类网络安全知识，为推动中国网络安全进步与技术创新贡献力量！
 - 当前国内为数不多的民间网络信息安全研究团队之一
 - wooyun=乌云
 - 最新：已关闭
 - 简介
 - 一个位于中国大陆的于企业与安全研究人员（白帽子）之间的安全漏洞报告平台，并提供最新的研究资讯。
 - 2016年7月20日凌晨，乌云官网突然关闭，仅显示一张“升级通告”的图片，并附言“与其听信谣言，不如相信乌云”。据外界推测可能是内部整顿
 - 有多方消息表示多名乌云高管被警方带走，但同时也有人辟谣称是谣言。截至2020年3月，网站依仅展示升级公告。
 - Seebug
 - 简介：一个权威的漏洞参考、分享与学习的安全漏洞平台，是国内权威的漏洞库，在国内和国际都享有知名度，于2006年上线。
 - 官网

- 知道创宇 Seebug 漏洞平台 - 洞悉漏洞，让你掌握第一手漏洞情报！
 - <https://www.seebug.org>
- exploit-db.com
 - 简介：一个面向全世界黑客的漏洞提交平台
 - 官网
 - Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers
 - <https://www.exploit-db.com>
- 吾爱破解
 - 简介：吾爱破解论坛致力于软件安全与病毒分析的前沿，丰富的技术版块交相辉映，由无数热衷于软件加密解密及反病毒爱好者共同维护
 - 网站：<https://52pojie.cn>
- Paper(知道创宇)
 - 简介：安全技术精粹
 - 网站：<https://paper.seebug.org/>
- CTFWIKI
 - 简介：CTF Wiki
 - 网站：<https://ctf-wiki.github.io/ctf-wiki/>
- CTFtime
 - 简介：Capture The Flag, CTF teams, CTF ratings, CTF archive, CTF writeups
 - 网站：<https://ctftime.org/>
- 先知社区
 - 简介：先知社区，先知安全技术社区
 - 网站：<https://xz.aliyun.com/>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2021-05-25 22:50:27

参考资料

- 【已解决】Mac中用otool查看IDA依赖的库
- 工控安全概览
- CTF.GS_CTF网站_CTF网址_CTF网址导航_CTF练习平台_CTF练习平台收集
- CTF大本营 - 网络安全竞赛服务平台-i春秋
- Hacker101 CTF
- CTFtime.org / All about CTF (Capture The Flag)
- optee开源项目的学习_fanguannan0706的专栏-CSDN博客_optee
- Open Portable Trusted Execution Environment - OP-TEE
- 什么是OPTEE-OS - 江召伟 - 博客园
- About OP-TEE — OP-TEE documentation documentation
- 【渗透测试工程师招聘】_暗泉信息招聘-BOSS直聘
- 漏洞利用 - 维基百科, 自由的百科全书
- 漏洞 - 维基百科, 自由的百科全书
- 计算机安全 - 维基百科, 自由的百科全书
- 网络安全 - 维基百科, 自由的百科全书
- 国内、国外网站安全渗透测试、漏洞扫描产品 | Venhow's Blog
- 渗透测试专业人员使用的11种工具 - FreeBuf互联网安全新媒体平台
- 谈谈我对逆向的一些认识 - 简书
- 「移动安全工程师招聘」_苏州极光无限信息...招聘-BOSS直聘
- 漏洞扫描原理——将主机扫描、端口扫描以及OS扫描、脆弱点扫描都统一放到了一起 - bonelee - 博客园
- 【知识科普】安全测试OWASP ZAP简介 - 知乎
- OWASP ZAP安全测试 - 简书
- 安全性测试：OWASP ZAP使用入门指南 - 哔哩哔哩
- Web安全测试-WebScarab工具介绍-云栖社区-阿里云
- 「网络安全」安全设备篇（防火墙-IDS-IPS） - 知乎
- 使用peach进行模糊测试从入门到放弃 - 安全客, 安全资讯平台
- Cain & Abel v4.9.44发布 - FreeBuf网络安全行业门户
- Layer子域名挖掘机5.0 SAINTSEC更新版 - 安全工具 - 互联网之家
- Layer子域名挖掘机 - guojia000 - 博客园
- 逆向分析之常见的汇编指令 - FreeBuf网络安全行业门户
- 十大黑客常用渗透测试工具 - 知乎
- 渗透测试专业人员使用的11种工具 - FreeBuf网络安全行业门户
- iOS App的加固保护原理 - 知乎
- iOS App 安全加固方案调研 - iOS - 掘金
- 对 iOS app 进行安全加固 - 我的学习历程
- iOS 应用加固方法 - 简书
- 为了保护公司的 App 安全, 我用遍了市面上的加固产品 - V2EX
- iOS逆向工程 介绍 | iOS 安全 Wiki
- iOS（十五）几种App砸壳工具对比 ~ gandalf
- iOS逆向工具之砸壳工具(MacOS&iOS)介绍 - 简书

- iOS攻防（四）：使用Dumpdecrypted 砸壳 & class-dump 导出头文件 | 曹雪松de博客|CoderBoy's Blog
- iOS攻防（六）：使用Cycrypt一窥运行程序的神秘面纱(入门篇) | 曹雪松de博客|CoderBoy's Blog
- class-dump的安装和使用 - 简书
- iOS攻防——（四）class-dump 与 Dumpdecrypted 使用 | 周小鱼の CODE_HOME
- class-dump的安装和使用 - 简书
- class dump使用方式和原理 - 简书
- Class-dump: class-dump-x和class-dump-z如何分析dylib等文件？ - Discussion | 技术讨论 - iOSRE
- iOS逆向之旅（进阶篇） — 工具(class-dump) - 掘金
- iOS逆向之class-dump - LeeGof - 博客园
- Tutorial · KJCracks/Clutch Wiki
- iOS攻防 - （六）iOS应用使用Clutch脱壳_移动开发_VictorZhang-CSDN博客
- iOS逆向工程之Clutch砸壳(图文多) - 简书
- iOS逆向之Clutch砸壳 - 简书
- iOS（十五）几种App砸壳工具对比 ~ gandalf
- sqlcipher/sqlcipher: SQLCipher is an SQLite extension that provides 256 bit AES encryption of database files.
- iOS安全攻与防(总篇) - 简书
- tianjifou/iOS-security-attack-and-prevent: iOS安全攻与防,详细的列出了，在iOS开发中，项目会存在的安全漏洞以及解决办法。
- 《iOS 应用逆向与安全》读后感 - 掘金
- iOS（十四）高版本越狱的坑 & killed 9 ~ gandalf
- OWASP Top Ten
- OWASP 10 大 Web 安全问题在 JEE 体系完全失控 - OneASP技术分享 - SegmentFault 思否
- What is OWASP? What Are The OWASP Top 10? | Cloudflare
- Akamai 如何增强您的安全实践以缓解 OWASP 10 大风险
- vmeyet/owasp10: Open Web Application Security Project Top10 (2017) - Presentation with demos
- OWASP - Wikipedia
- 【从零开始学习CTF】1、什么是CTF - 知乎
- CTF.GS_CTF网站_CTF网址_CTF网址导航_CTF练习平台_CTF练习平台收集
- CTF大本营 - 网络安全竞赛服务平台-i春秋
- Hacker101 CTF
- CTFtime.org / All about CTF (Capture The Flag)
- iOS（十四）高版本越狱的坑 & killed 9 ~ gandalf
- macos - Editing assembly on Mac OS X - Stack Overflow
- iOS逆向（八）逆向工具 otool 介绍 - 掘金
- otool 一些用途 - 简书
- otool命令查看App动态库 - 简书
- iOS 逆向---otool命令入门_嵌入式_ParadiseDuo-CSDN博客
- iOS程序逆向Mac下常用工具——Reveal、HopperDisassemble、IDA - 时间已静止 - 博客园
- Hopper Alternatives and Similar Software - AlternativeTo.net
- Detect-It-Easy：一款跨平台的PE查壳工具 - 体验盒子 - 关注网络安全

- [Exeinfo PE 0.0.5.1 - 下载](#)
- [漏洞挖掘需要哪些基础知识? - 知乎](#)
- [零基础如何学习挖漏洞? - 知乎](#)
- [人工找漏洞是怎么找到的? 需要什么必要基础知识? - 知乎](#)
- [二进制漏洞挖掘从理论到实践按照顺序有哪些知识需要学习, 哪些书籍值得去读? - 知乎](#)
- [有Android逆向基础如何学习Android漏洞挖掘? - 知乎](#)
- [零基础, 如何进行漏洞挖掘 - 知乎](#)
- [从ctf入门漏洞挖掘_网络_tangsilian的博客-CSDN博客](#)
- [网站漏洞挖掘 - 云+社区 - 腾讯云](#)
- [\[思路/技术\] 如何入门漏洞挖掘, 以及提高自己的挖掘能力。 \(干货\) - CanMeng'Blog - 一个WEB安全渗透的技术爱好者](#)
- [谈高效漏洞挖掘之Fuzzing的艺术 - FreeBuf互联网安全新媒体平台](#)
- [\[求助\]怎样学习漏洞挖掘?-『经典问答』-看雪安全论坛](#)
- [\[原创\]各类漏洞挖掘方法辨析-『二进制漏洞』-看雪安全论坛](#)
- [\[原创\]游戏漏洞挖掘概述-『二进制漏洞』-看雪安全论坛](#)
- [mhs6.2汉化版下载|MHS\(内存修改工具\)下载v6.2 汉化 版_IT猫扑网](#)
- [\[转载\] 漏洞挖掘小白入坑指南 - 个人文章 - SegmentFault 思否](#)
- [漏洞挖掘 | 安全脉搏](#)
 - [【技术分享】漏洞挖掘高级方法 - 安全客, 安全资讯平台](#)
 - [内存搜索、修改器 \(附VC6源码\) BeanJoy的专栏-CSDN博客内存搜索修改器](#)
 - [radare2 Alternatives and Similar Software - AlternativeTo.net](#)
- [Radare2 学习笔记: 从入门到精通 1. Radare2 简介, 及安装_Tangent's blog-CSDN博客_radare2 安装](#)
- [老司机带你玩转Radare2 - 简书](#)
- [Macho文件浏览器---MachOView - 简书](#)
- [一文带你快速理解CVE是什么意思? 从CVE ID分配到CVE漏洞处理](#)
- [提交CVE漏洞是一种怎样的体验? - 知乎](#)
- [聊聊CVE漏洞编号和正式公开那些事 | 技术博客](#)
- [通用漏洞披露 - 维基百科, 自由的百科全书](#)
- [通用漏洞披露 \(CVE\)](#)
- [国家信息安全漏洞库](#)
- [申请CVE的姿势总结 - FreeBuf互联网安全新媒体平台](#)
- [FreeBuf互联网安全新媒体平台](#)
- [全球最新漏洞库 - 安全客, 安全资讯平台](#)
- [逼格or随性?看我是如何混一波CVE编号! - FreeBuf专栏·OSPTECH攻防团队](#)
- [极光无限安全团队集结令 \(苏州\) - FreeBuf网络安全行业门户](#)
- [Microsoft Visual C++ - 维基百科, 自由的百科全书](#)
- [windows - How to disable buffer overflow checking in the Visual C++ Runtime? - Stack Overflow](#)
- [Intel® C++ Compiler 19.1 Developer Guide and Reference](#)
- [/GS \(Buffer Security Check\) | Microsoft Docs](#)
- [MSVC Compiler Options | Microsoft Docs](#)
- [GS buffer](#)
- [fstack-protector](#)
- [OllyDbg使用入门 | M0rk's Blog](#)
- [漏洞挖掘工程师](#)
- [strict_gs_check pragma | Microsoft Docs](#)

- [trailofbits/winchecksec: Checksec, but for Windows: static detection of security mitigations in executables](#)
- [c++ - How to check whether an EXE has /GS security protection on Windows? - Stack Overflow](#)
- [IMAGE_LOAD_CONFIG_DIRECTORY32 \(winnt.h\) - Win32 apps | Microsoft Docs](#)
- [GS cookie protection – effectiveness and limitations - Microsoft Security Response Center](#)
- [Security Features in MSVC | C++ Team Blog](#)
- [/SAFESEH \(Image has Safe Exception Handlers\) | Microsoft Docs](#)
- [MASM for x64 \(ml64.exe\) | Microsoft Docs](#)
- [On the effectiveness of DEP and ASLR - Microsoft Security Response Center](#)
- [exploit - How do ASLR and DEP work? - Information Security Stack Exchange](#)
- [DEP/ASLR 原理及攻击_运维_forevertingting的博客-CSDN博客](#)
- [windows - How to bypass DEP and ASLR at the same time? - Information Security Stack Exchange](#)
- [buffer overflow - How does SEH based exploit bypass DEP and ASLR? - Information Security Stack Exchange](#)
- [exploit - Stack Overflows - Defeating Canaries, ASLR, DEP, NX - Information Security Stack Exchange](#)
- [buffer overflow - Bypass Full ASLR+DEP exploit mitigation - Information Security Stack Exchange](#)
- [/DYNAMICBASE \(Use address space layout randomization\) | Microsoft Docs](#)
- [Whitepaper on Bypassing ASLR/DEP](#)
- [ASLR/DEP绕过技术概览 – ArkTeam](#)
- [Why it's important to turn on DEP and ASLR Windows security features](#)
- [安全保护技术ASLR绕过启示录 - FreeBuf互联网安新新媒体平台](#)
- [栈溢出基本ROP绕过ASLR和NX保护_网络_ditto的博客-CSDN博客](#)
- [“优雅”的Linux漏洞：用罕见方式绕过ASLR和DEP保护机制 - 云+社区 - 腾讯云](#)
- [Windows溢出保护原理与绕过方法概览 | riuskksk's blog](#)
- [Abysssec Information Security and Vulnerability Research Group](#)
- [IE漏洞学习笔记（一）Heap Spray - 安全客，安全资讯平台](#)
- [PWN入门系列（四）：栈终结篇 - 安全客，安全资讯平台](#)
- [pwn入门之栈溢出练习 - FreeBuf专栏·春秋学院](#)
- [Linux pwn入门教程\(1\)——栈溢出基础 - 知乎](#)
- [ctf中pwn入门指南 | ditto's blog](#)
- [\[原创\]GoParser——Yet Another Golang binary parser for IDAPro-『软件逆向』 -看雪安全论坛](#)
- [\[原创\]使用 mitmproxy 快速搭建软件网络验证API——以某音频处理软件为例-『软件逆向』 -看雪安全论坛](#)
- [神器如 dnSpy，无需源码也能修改 .NET 程序_walterlv - 吕毅-CSDN博客_dnspy](#)
- [dnSpy - 一款 .NET 程序逆向工具\]](#)
- [使用dnSpy对目标程序\(EXE或DLL\)进行反编译修改并编译运行 - jack_Meng - 博客园](#)
- [工具推荐：逆向破解利器OllyDbg - 知乎](#)
- [OllyDbg - Wikipedia](#)

- [Download OllyDbg 2.01](#)
- [七周年礼物第五弹之一：吾爱破解专用版Ollydbg 2016年1月21日更新](#)
- [OllyDbg Download \(2020 Latest\) for Windows 10, 8, 7](#)
- [OllyDbg使用入门 | M0rk's Blog](#)
- [极光无限安全团队集结令（苏州） - FreeBuf网络安全行业门户](#)
- [嵌入式设备漏洞研究员](#)
- [ReFirmLabs/binwalk: Firmware Analysis Tool](#)
- [Binwalk工具的详细使用说明运维子曰小玖的博客-CSDN博客](#)
- [binwalk windows安装和使用方法 - pcat - 博客园](#)
- [自动提取文件系统---binwalk\(一\) - blacksunny - 博客园](#)
- [Binwalk：固件分析利器 – ArkTeam](#)
- [Binwalk | Penetration Testing Tools](#)
- [BinWalk安装和命令参数详解 - 云+社区 - 腾讯云](#)
- [/NXCOMPAT \(Compatible with Data Execution Prevention\) | Microsoft Docs](#)
- [Control Flow Guard - Win32 apps | Microsoft Docs](#)
- [safebuffers | Microsoft Docs](#)
- [内存保护机制及绕过方案——通过覆盖虚函数表绕过/GS机制 - zhang293 - 博客园](#)
- [Windows安全机制---栈保护：GS机制_每昔的博客-CSDN博客_charshellcode](#)
- [绕过GS的栈溢出攻击原理 | Kumqu's Blog](#)
- [绕过GS安全编译的方法 | Introspelliam](#)
- [通关栈溢出（四）：缓冲区溢出的防御技术及绕过 - Hello! CytQ](#)
- [visual studio - safeseh gs on g++ - Stack Overflow](#)
- [SafeSEH利用（DEP/ASLR disabled） - 简书](#)
- [gdbinit/MachOView: MachOView fork](#)
- [The Ultimate Disassembly Framework – Capstone – The Ultimate Disassembler](#)
- [Capstone & LLVM – Capstone – The Ultimate Disassembler](#)
- [各种开源汇编、反汇编引擎的非专业比较 - simpower的个人空间 - OSCHINA](#)
- [Capstone引擎正式支持RISC-V架构 - 51CTO.COM](#)
- [KEYSTONE: Next Generation Assembler Framework](#)
- [OLLVM代码混淆移植与使用 | Heroims的博客](#)
- [利用ollvm进行代码混淆 | m4bln](#)
- [Low Level Virtual Machine \(LLVM\)](#)
- [LLDB \(debugger\) - Wikipedia](#)
- [LLDB Homepage — The LLDB Debugger](#)
- [Tutorial — The LLDB Debugger](#)
- [深入了解GDB和LLDB - 简书](#)
- [LLDB 知多少 - 掘金](#)
- [iOS（十六）一次通过lldb绕过越狱检测&反反调试实践 ~ gandalf](#)
- [debugserver - iPhone Development Wiki](#)
- [使用lldb+debugserver动态调试iOS应用 | La0s](#)
- [iOS 逆向指南：动态分析 – 小专栏](#)
- [iOS逆向, 基础工具之LLDB和debugserver - 简书](#)
- [一步一步用debugserver + lldb代替gdb进行动态调试 - Blog | 干货分享 - iOSRE](#)
- [Remote Debugging — The LLDB Debugger](#)
- [安全解决方案 - RISC-V IP方案](#)

•
crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2021-05-25 22:49:53