网络安全资料汇总！

原创

云先森SIR 于 2020-01-07 23:35:40 发布 1358 收藏 7

分类专栏： 笔记

本文链接：https://blog.csdn.net/weixin_46159811/article/details/103883572

1.网络安全资料汇总

web security：

《http权威指南》【图灵出品】 深入理解web http/https协议，了解超文本传输协议是如何进行传输和编译的。

《javascript权威指南》 淘宝前端团队翻译，深入了解前端js变量，注释，函数，表达式等，学习xss必备书籍。还提及了jquery类库。

《xss跨站脚本攻击与防御》 学习xss基础必备。也是目前国内唯一一本专门介绍xss技巧的书籍

《白帽子讲web安全》 阿里安全专家吴瀚清处女作，大佬级黑客ucloud创始人季昕华做序。已成为web安全从业人员入门必看学习书籍。

《web前端黑客技术揭秘》 主要包含Web 前端安全的跨站脚本（XSS）、跨站请求伪造（CSRF）、界面操作劫持这三大类，涉及的知识点涵盖信任与信任关系、Cookie安全、Flash 安全、DOM 渲染、字符集、跨域、原生态攻击、高级钓鱼、蠕虫思想等，这些都是研究前端安全的人必备的知识点。

《代码审计：企业级web安全代码架构》配合《细说php》最佳 阿里巴巴安全专家尹毅的新书，刚毕业就出书实在佩服。看了目录非常有料啊，预计12.8上货。

《kali linux&back track渗透测试实践》【图灵出品】（没看过，淘宝看了下目录还不错的样子）

《sql注入攻击与防御》 详细的介绍了sql盲注等各种注入技巧。web安全入门必看。

《网络扫描技术揭秘》 出版已超过三年的老书。主要介绍网络扫描技术。如：分布式扫描，高速扫描等。

《python黑帽子》 作者根据自己在安全界，特别是渗透测试领域的几十年经验，向读者介绍了Python 如何被用在黑客和渗透测试的各个领域，从基本的网络扫描到数据包捕获，从Web 爬虫到编写Burp 扩展工具，从编写木马到权限提升等

《黑客技术攻防宝典：web安全篇》【图灵出品】 看第一遍的时候可能看不懂讲的什么玩意儿。主要看目录，一本普及面非常广阔的知识性图书，但是每个知识点概括不会很详细。也很值得收藏。

mobile security：

android security：

《andriod软件安全与逆向分析》【图灵出品】我大非虫原创处女作，通俗易懂涉及面广。不管新手老手都适合看。全书主要讲解Android 环境搭建，Android组件，Android软件安全测试之法。

《android安全攻防指南》【图灵出品】 众多大牛推荐…内在自然是不少干货为白帽子提供了漏洞发现、分析和利用的使用工具。在详细介绍android操作系统工作原理和总体安全架构后，研究了如何发现漏洞，为各种系统部件开发利用，并且进行应对。移动设备管理者、安全研究员、android应用程序开发者和负责评估android安全性的顾问都可以在本书中找到必要的指导和工具。

《andriod安全攻防实战》 没看过。。。看看目录还行

《andriod安全技术揭秘与防范》 一本新书，红衣教主推荐的，已加入豪华购物车。未阅

《android系统安全和反汇编实战》 没看过。。-_-||

ios security：

《ios应用安全攻防实战》 如何保障自己的应用数据安全？本书提供一些用于防御常见攻击方法的方式。

《黑客攻防技术宝典ios实战篇》【图灵出品】 国际大牛之作，介绍iOS应用漏洞挖掘方式，模糊测试技巧。

《ios取证实战》 没看过。收藏很久了。

《ios应用逆向工程》 国内iOS老手杜总的力作。充分介绍iOS 安全机制，iOS反汇编技巧。

《移动应用安全》 主要从Android iOS windows mobile三个方向谈及安全知识。

《移动终端安全关键技术与分析》 我发现的唯一一本讲移动终端安全的书籍，纯知识性。没有代码分析等。很薄很薄。

bin or Reverse Engineering:

《intel微处理器》 （看雪坛友推荐，看了下目录是真心好啊，已加入豪华购物车…）

《逆向工程核心原理》【图灵出品】 韩国翻译过来的逆向书籍，深入浅出各种反汇编大法。调试大法，上钩大法。介绍利用各种工具。特别适合入门。

《加密与解密》 看雪论坛创始人锻钢著作。经典之经典。主要介绍软件逆向，调试。反汇编，加壳脱壳等技术。

《挖0day》 八进制核心成员编写，测试方法基本过期。但是对于软件特性，漏洞挖掘思路绝对脑洞一开。

《有趣的二进制》【图灵出品】 不仅仅是书有趣，作者也是个有趣的人~一本由日文翻译过来的二进制安全书籍，翻译的非常仔细，仔细到调试工具里的弹窗文字都要翻译注释下来。基础书籍，事宜入门。也学学岛国的安全技术吧（天呐，我这么纯洁的人岛国是什么鬼…）

《模糊测试 强制发掘安全漏洞的利器》 超经典书籍。里面介绍的挖掘方法基本过期。但是技术思路和全书介绍的不少fuzz工具绝对值得收藏。

《汇编语言》 了解汇编语言。寄存器，地址布局，汇编指令，数据段是件对逆向工程有好处的事儿~

《格蠹汇编 软件调试案例锦集》 其实第二个字我还是不认识，不过淘宝搜索格囊汇编就行了。全书通篇介绍作者软件调试实战。没有一点水货~也不扯淡。学软件调试就看这个了。

《软件调试》 上面那本书的姊妹篇，同一个作者。

《逆向工程实战》【图灵出品】 这本书一上来就分析栈操作和函数调用，对于新手来说不建议直接就啃。不过内容详细，看看上面的其他书籍或者了解一下汇编和C语言知识再啃这个比较合适。

《恶意代码分析实战》

稍偏门安全类：

无线：《无线网络黑客攻防》 详细介绍包括但不限于无线网络，无线蓝牙等无线攻防技术。了解什么是wpa，什么是cowpatty，mdk3。介绍 Auth Flood攻击 Deauth Flood攻击 Association Flood攻击 Disassociation Flood攻击RF Jamming攻击和各种漏洞测试方法。

《揭秘家用路由0day漏洞挖掘技术》 够详细，连指令表都有。从路由器web。客户端，以及硬件安全方面介绍，介绍了各种测试方法，利用方式，扫描技术。

内核：《内核漏洞的利用与防范》 不是很好理解的一本书，毕竟内核漏洞也不是想挖就挖的到的……

《windows内核安全与驱动开发》 （没看过，讲不来。在购物车里躺好久了。）

浏览器：《web之困》 这是一本不介绍漏洞，也不讲测试的经典书。全原理式讲解浏览器安全的前世今生~

数据安全：《数据驱动安全》 360某安全团队翻译过来的…大数据时代，当然用数据说话…只是对照着英文版发现有一丢丢的翻译错误。不过…也确实不可错过的好书，毕竟这类安全的中文书籍仅此一本。

云计算安全：《信息安全技术 云计算服务安全指南》

没看过，凑数用的…

tools books：（工具书就不用介绍了，干啥用的都知道。）

《metasploit渗透测试指南》《wireshark2数据包分析实战》《ida pro权威指南》【图灵出品】《kali linux渗透测试的艺术》《github入门与实践》【图灵出品】《fiddle调试权威指南》《计算机安全超级工具集》《雷神的微软平台宝典》

合集：

《黑客大曝光7》 这本书啥都有，简直就像黑客百科全书。

《深入理解计算机原理》 为什么我把这本书放在“合集”呢？因为只有先了解了计算机的运行原理，执行原理。你才知道上面看的那堆玩意儿他们在干嘛…

《互联网安全的40个智慧洞见》 2014年360ISC 演讲者PPT

《网络安全基础 第5版》 主要介绍网络安全解决方案中的密钥分配、用户认证、网络访问控制、云安全、传输层安全、无线网络安全、电子邮件安全和IP层安全等方面的重要协议或工业标准；第三部分为系统安全，主要介绍互联网系统中的恶意软件、人侵者和防火墙等方面内容。

linux类：

《linux内核源码剖析》上/下 几乎把Linux开源的每一段代码，每一条函数都拿出来分析。所以分成两本比较厚的书。了解Linux内核源码，操作原理就选这个了。

《鸟哥的linux私房菜》 Linux安装到使用，搭建到指令。最最基础的Linux学习用书，本应放在第一位，但是上面那套实在太好了。

《linux内核完全注释》

《ram linux内核源码剖析》

《linux内核设计与实现》 出版超过3年的经典书籍。从Linux内核进程，内核线程，调度，系统调用，中断和异常处理等方面概述了Linux内核的设计与实现原理。

《tcp/ip详解》 描述了属于每一层的各个协议以及它们如何在不同操作系统中运行。作者用lawrence berkeley实验室的tcpdump程序来捕获不同操作系统和tcp/ip实现之间传输的不同分组。对tcpdump输出的研究可以帮助理解不同协议如何工作。

IT思维：

《我的互联网方法论》 周鸿祎的龙头之作。他讲的方法其实就是他的产品理念，刚拿到的这本书的我是花一个下午一口气看完的~可见它内容的吸引力！

《增长黑客》 书名写着“黑客”讲的主题却是营销，用大数据说明如何利用“黑客”为自己增值。适合创业者看~

《德鲁克全书》 这本书本跟IT无关，但是里面的故事大多发生在互联网公司，并且适合创业者或者管理者阅读。一种把员工当成客户（上帝）的思维，层出不穷的管理体系理念。非常棒的管理思维。

《谷歌是如何运营的》 想运营好自己的公司或者部门，可以先从这里参考或者一下学习一下谷歌是怎么做的。

《乔布斯传》 乔布斯是我一直的偶像，真正的偶像。他的产品理念和创新思维绝对一流。不管是技术员，管理员，运维，CEO，都值得看看。

《腾讯传》 话说马化腾，道言张小龙。讲QQ，谈微信！

优质学习资源：

知乎周刊：http://zhuanlan.zhihu.com/

码农周刊：http://weekly.manong.io/

Pycoder’s Weekly：http://pycoders.com/archive/

Hacker News：https://news.ycombinator.com/

Startup News：http://news.dbanotes.net/

极客头条：http://geek.csdn.net/

InfoQ：http://www.infoq.com/cn

Stack Overflow：http://stackoverflow.com/

GitHub：https://github.com/

FreeBuf：http://www.freebuf.com/

WooYun：http://drops.wooyun.org/

csdn博客：blog.csdn.net

博客园：www.cnblogs.com

雷锋网：leiphone.com

吾爱破解：52pojie.cn

看雪论坛：bbs.pediy.com

绿盟科技博客：http://blog.nsfocus.net/

E安全：http://www.easyaq.com/

360播报:bobao.360.cn

游侠安全网 http://www.youxia.org

优质微信公众号：

EAQapp（E安全官方公众号，收集国内外一线资讯，翻译和原创技术文档）

Linux-cn（Linux中国网，Linux使用技巧，内核模块等与Linux有关的一些好文）

FreeBuf（国内外安全资讯，技术文章）

malwarebenchmark（各种apt样本分析，逆向工程实战！）

i77169（普及网络安全知识和发布资讯）

阿里聚安全（阿里移动安全部微信公众号）

腾讯玄武实验室（可能会推送一些玄武实验室的最新研究报告~新公众号，支持一下大教主）

301在路上（乌云首席铲屎官（不知道这样写三哥会不会打我＝ ＝）私人公众号，经常发表自己与网络安全的经验和言论）

云头条（国内外一线IT资讯）

youxia-org （国内外一线安全资讯和bugscan插件更新报道…）

heapstack_labs（国卫堆栈实验室公众号，每月开一期安全沙龙“安全说”每月主题都不一样，上个月主题“工控安全”）

anzer_sh（安在，信息安全媒体，主要采访信息安全大咖，传播信安热点）

sec-un（信息安全情报威胁）

lookvul（国内顶级黑客rayh4c个人公众号，主要推送情报威胁相关文章）

pojie_52（吾爱破解，不时推送详细逆向文章，样本分析，当然也有论坛的软广）

李宗洋一亩田（天融信VP李宗洋个人公众号，推送情报威胁和分享经验）

sex_91ri（91ri安全指南，最近好像没推出文章来，不过也是个很赞的公众号）

secpulse（一个很棒的新生信息安全团队，不时推送web安全文章）

oschina2013（开源中国，你懂的~）

droidsec（安卓中文网，mobile security~）

Security vulnerabilities platform（白帽子看这里~）

第三方漏洞平台：

乌云　http://www.wooyun.org/ 国内最棒的第三方漏洞平台，白帽子源地，1wb＝10rmb

补天漏洞响应平台　https://butian.360.cn/ 自称是全球最大的漏洞平台，拥有上万名白帽子，对通用型漏洞奖金略高。1kb＝3rmb

乌云众测　http://ce.wooyun.org/ 中国众测哪家强…（wooyun club 黑板上写的）

漏洞盒子　https://www.vulbox.com/ freebuf创办

Sobug 众测平台　https://sobug.com/ 冷焰创办

sebug漏洞库 https://www.sebug.net/ 一家以收集poc或exp为奖励的平台，据说挺赞的、

比戈大牛 http://www.bigniu.com 新平台，以收购android bin漏洞为主，奖励很丰厚

阿里云盾先知计划 http://xianzhi.aliyun.com/ 看到的第一反应是。阿里也收别人的漏洞了= =不过只收通用漏洞 最高奖金50w

企业SRC：

1　网易安全中心　http://aq.163.com （没刷过，不知道。看了商城，五块钱都可以换…）

2　腾讯安全应急响应中心　http://security.tencent.com/ （据说是全中国最好的SRC）

3　阿里巴巴安全应急响应中心　https://security.alibaba.com/ （有钱任性，平台负责人是个高颜值帅哥）

4　新浪安全应急响应中心http://sec.sina.com.cn/（渣浪据说不咋地，没刷过…）

5　百度安全中心　http://sec.baidu.com/ （奖励不是很高，作为bat却排在了最后）

6　京东安全应急响应中心　http://security.jd.com/ （奖励在步步提升了，并且和asrc一样有流动全国沙龙巡演）

7　360安全应急响应中心　http://security.360.cn/ （月排名奖金真的很吸引人！）

8　1号店安全应急响应中心　http://security.yhd.com/ （没刷过）

9　金山安全应急响应中心　http://sec.kingsoft.com/ （小气小气小气小气小气…）

10　携程安全应急响应中心　http://sec.ctrip.com/ （商城礼品略少正在逐步改善…）

11　去哪儿安全应急响应中心　http://security.qunar.com/ （没刷过…）

12　搜狗安全应急响应中心　http://sec.sogou.com/ （1安全币＝1RMB）

13　小米安全中心　https://sec.xiaomi.com/ （奖金不多，也不算少，直接打钱的src）

14　联想安全应急响应中心　http://lsrc.lenovo.com/index.htm （奖金正在逐步提升，不时翻倍）

15　深信服安全响应中心　http://security.sangfor.com.cn （我也不知道这里什么鬼规则，直接发京东卡的）

16　魅族安全响应中心　http://sec.meizu.com/ （一币＝10rmb，meizu pro5才280个币）

19　安全狗　http://security.safedog.cn （公告形式排名，运营比较温柔~）

20　迅雷　http://safe.xunlei.com （不了解…）

21　欢聚时代安全应急响应中心　http://security.yy.com （奖励略少…）

22　平安集团安全应急响应中心　http://security.pingan.com （直接以钱作为奖励方式，一个getshell大概4000块，积分比较狠。几十万来的）

23　唯品会安全应急响应中心　http://sec.vip.com/ （也算个良心src了，不过有个缺点就是，只以唯品卡为奖励方式，没满10的暂存。还挺不错。毕竟新生src）

24　苏宁安全应急响应中心 http://security.suning.com/ssrc-web/index.jsp （有个审核有点帅……一个币＝5rmb，商城目前未上线，不过快了。）

25　滴滴打车安全应急响应中心 http://sec.didichuxing.com/ （刚上线…排行榜都木有╮▂╰）

其实还有饿了么SRC（ESRC）还没有上线…

按照原风格附上手绘流程图

新手入门主要学习方向可以先从这张表找找

画的有点凌乱…

观众需求还是得要一张Linux相关流程图…

原文地址

2.最全前端资源汇集

作者 晚晴幽草 关注

2016.04.05 22:09 字数 1024 阅读 26060评论 86喜欢 462

前些日子从@张鑫旭微博处得一份推荐(Front-end-tutorial)，号称 最全的资源教程 ー前端涉及的所有知识体系；有粗略查看，果然“叹为观止”，至少比想象中涉猎丰富许多；果断有Fork了来：Front-end-tutorial;

感谢声明： 方才晓得这份良心分类清单，很大程度上得益于：JS前端开发群规 - 492107297；其 Github 在线地址为 http://t.cn/RL2NtqX。这492107297是 Vuejs 分享学习QQ群号，氛围大好，十分难得。此份清单已征得其群主 @豪情 同意，会在这基础上予以修改增减。各位看官也可移步JS前端开发群规 - 492107297：这寄存于 看云，分类清晰，也在持续更新中。(更新于2016-04-19夜)。

微注0:谈及对好文章链接收藏，这带有蛮严重不靠谱因素：尤其是这链接地址因各种缘由失效这个（故此还是遇见即读的好）；于此有小写脚本以甄别并删除之，有率先更新于：http://www.jeffjade.com/2016/03/30/104-front-end-tutorial/；

引者注：此上链接全为精华啊！

3.（翻译）2017 年你应该学习的编程语言、框架和工具

作者 IT程序狮 关注

2016.12.14 19:00 字数 5119 阅读 15787评论 80喜欢 785

2017 年你应该学习的编程语言、框架和工具

在过去的一年里，软件开发行业继续大踏步地向前迈进。回顾 2016 年，我们看到了更多新兴的流行语言、框架和工具，它们改变着我们的工作方式，让我们看到更多的可能。但在这个行业，紧随潮流是很难的。所以在每年年底，我们都会给你提供一些建议，它涉及什么是最重要的，以及你在未来一年中应该学习什么。

大趋势

渐进式 Web Apps

在 2016 年里，我们见证了 Progressive Web App 概念的蓬勃兴起。它意味着 Web 应用程序可以离线工作，并能提供原生移动应用的体验。它们可以添加到你的智能设备的主屏幕上，甚至可以给你发送推送通知，从而弥补与原生移动应用程序的差距。我们认为，在 2017 年，渐进式 Web Apps 将变得更加重要，也值得我们去探究。在这里查看相关概述。

聊天机器人

从运行聊天机器人的平台到构建其的框架，现在每个人都在谈论它。而社区里也正忙于此活动。（阅读我们的介绍）机器人是一款新兴的移动应用程序，它让我们感到兴奋。如果你快点的话，还可以赶得上这波浪潮。然而一旦新鲜感消失，那么它只会承担一些无聊的角色，例如自动化的客服支持。但是，相信我们可以实现梦想。

前端框架的合并

在 JavaScript 社区，随着令人难以置信的框架和工具的混合，每周都会出现新的东西。直到最近，人们希望旧工具将被新工具所取代，但这不是 2016 年我们所想看到的。相反，我们看到了流行框架交换的想法，以及纳入新诞生框架中的创新元素。所以在 2017 年，你该选择哪个 JS 框架无关紧要，因为它们的功能大多是可以比较的。

云端

就目前的形势看，众多的公司与开发者们都在积极地拥抱“云”。云是可根据不同的需求，并通过控制面板来完全配置的虚拟化计算机基础设施。目前三大云提供商为亚马逊 AWS、Google Cloud 和 微软 Azure. 由于它们的竞争价格一直在下跌，使得小公司和个人开发者也可以将云纳入其预算中，所以熟悉云工作流程将是 2017 年的一笔不错的投资。

机器学习

机器学习（ML）在去年一年中呈现爆炸式的增长。三月份 AlphaGo 与李世石的精彩对决，也让它成为了焦点。从原始数据中学习的智能计算机系统，正在改变我们与移动设备的交互方式。看样子，机器学习将在 2017 年成为更大的影响因素。

编程语言

编程语言

JavaScript 继续迈着令人难以置信的创新步伐在前进。由于 Web 浏览器的快速发布计划，JS 的标准定为了每年更新。故“ES2017”预计将在 2017 年中期完成，它也将带来 JS 开发者梦寐以求的新特性——用于处理异步函数的async/await。同时要感谢 Babel ，因为你现在可以在每个浏览器中编写 ES2017 了。

TypeScript 2.1 于 2016 年年底发布，它将为旧浏览器带来Async/Await异步解决方案，并改进了类型推断。TypeScript 是一种编译为纯 JavaScript 的静态类型语言。它增强了经典的 OOP 模型和可选的静态类型，使大代码库更易于维护。同时，它也是编写 Angular 2 应用程序的首选语言，我们建议你可以尝试下。 这是关于它的快速入门指南。

C#7.0 预计在 2017 年发布，作为一门优秀的编程语言，它也将得到更大的改进。当微软推出开源的 Visual Studio 代码编辑器和 .Net Core 时，这一举动让众人都感到惊讶万分。它们不仅可以在 Linux、Windows 和 macOS 操作系统中运行，而且你可以在 C＃ 中编写快速、高效的应用程序（在这里阅读更多）。同时，这两种工具也都形成了充满活力的社区。相信，它们将在 2017 年会给我们带来更多的惊喜。

Python 3.6 版本将于 12 月发布。它正在巩固自身在开发人员、IT 专业人员和科学家在脚本语言选择中的地位。它适用于自动化、Web开发、机器学习和科学计算。虽然 Python 2.X 与 3.X 版本的割裂，对于社区来说是一个长达数年的斗争，但是就目前而言，你可以自信地选择 Python 3 并享受完整的库支持。而对于那些需要额外性能的朋友，建议你们看看 PyPy，一个可启用 Python 运行时 JIT 的替代品。

Ruby 2.3 已在今年早些时候发布了，并带来了一些性能上的改进。同时，Ruby 也是学习通用脚本语言的一个好选择，但是只有当它和 Rails 相配合的时候才能发挥出其最大的功效。伴随 Ruby 3×3 计划的宣布，也促使了即将到来的 Ruby 3 版本比当前版本的运行速度快 3 倍。而你也可以在更多的情景中，打开使用 Ruby 的大门。

PHP 7.1 版本已在 12 月发布，并对该语言进行了小范围的增强。这个版本基于了去年 7.0 版本主要性能的改进，将 PHP 转变为构建 Web 应用程序的快速平台。如果你打算学习，我们推荐你看看 PHP 之道中的最佳实践。

Java 9 预计在 2017 年发布，它将带来一些备受开发者们所欢迎的新功能，例如评估代码的 repl、HTTP 2.0 的支持以及一些新的 API . 对于有才能的 Java 开发人员和广泛使用该语言进行项目研发的人来说，他们对这些新特性是有强烈需求的。如果 Java 不是你的“菜”，这里还有一些基于 JVM 的编程语言，像 Kotlin 和 Scala，你也可以了解下。

Swift 3 已经在今年早些时候发布了。简化 iOS 和 MacOS 上应用程序的开发，是苹果公司对现代编程语言的愿景。由于 Swift 是开源的，所以也涌现了大量的社区。Swift 4 计划于 2017 年发布，此版本将会改进语言并引入服务器 API，致力使其成为编写 Web 应用程序和后端的不错选择。

如果你在寻找一些让你感到兴奋的东西，你可以尝试下 Crystal 和 Elixir。它们都拥有类似与 Ruby 的友好语法以及卓越的性能，或者你也可以看看类似于 Haskell 或 Clojure 这类函数式语言。另外两种快速编程语言，我们推荐给你 Rust 和 Go 语言。

挑一个或多个学习： JS (ES2017)、TypeScript、C#、Python、Ruby、PHP7、Java/Kotlin/Scala.

前端开发

前端

近期 Web 平台取得了两个重大的进展：Web Assembly 字节码技术和 Service Workers 技术。它们打开了快速、高效的 Web 应用程序的大门，并且有效的弥补了编译本地应用上的差距。Service Workers 是针对渐进式 Web App 的启动技术，它为 Web 平台提供了通知上的支持，将来也会有更多的 API.

Angular.js 2 在今年也已经发布了。该框架由 Google 进行维护，受到了众多企业和大公司的青睐。它所具备众多的功能，也为从网络到桌面以及移动应用程序中编写任何东西成为了可能。而它的框架也是用 TypeScript 所编写的，这也是写应用程序推荐的编程语言。虽然学习它还需要阅读更多的内容，但我们认为在 2017 年学习 Angular 2 将是一个很不错的投资。

在今年我们也看到了 Vue.js 2.0 版本的发布，它借鉴了 Angular，React 和 Ember 中好的想法，并且比前两个框架更轻量、更快速。我们建议你今年要试一试，你可以从我们的 Vue.js 教程开始。

Ember 是 JavaScript 框架的另一个不错的选择。它支持数据双向绑定，并能够自动更新模板、组件以及服务器端渲染。与其他竞争者相比，使用它的好处是它更加成熟与稳定，而其框架的重大更改频率之低，社区重视向后的兼容性，也使得此框架成为开发较长生命周期的应用程序的不二之选。

另外两个值得一提的框架是 Aurelia 和 React。在过去的一年里 React 的生态系统变得越来越复杂，因此很难推荐给初学者。但经验丰富的开发者可以将库与 GraphQL、Relay、Flux 和 Immutable.js 组合成一个全面完整的全栈解决方案。

没有提及 Bootstrap 的前端终归是不完整的。而 Bootstrap 4 目前也正处于 Alpha 阶段，预计在 2017 年发布。值得关注的变化是新的通用卡片组件和 Flexbox 网格（查看与常规网格的对比），这使得框架更加现代化，并且让用户使用它进行工作时更加得舒心。

SASS 和 LESS 仍然是当前最流行的两种 CSS 预处理器。尽管 Vanilla CSS 已经实现了对变量的支持，但对 mixins、函数和代码组织上的支持，SASS 和 LESS 依然更胜一筹。如果您还没有了解它们，可以看看我们的 SASS 和 LESS 快速入门指南。

挑一个或多个学习：Angular 2、Vue.js、Ember、Bootstrap、LESS/SASS

后端开发

后端

后端有众多的选择，但所有的选择都取决于你对编程语言或特定性能需求的偏好上。Web 开发中的一个持续趋势是远离后端的业务逻辑，并将该层转换为由前端和移动应用程序使用的 API 上。但一个全栈的框架通常是能够更简单、快速的应用于开发，并且它仍然是 Web 应用程序最有效的选择。

Node.js 是在浏览器之外运行 JS 的主要方式。在今年，我们也看到了它发布了许多新的版本。除了提升了性能外，也添加了对整个 ES6 规范的覆盖。Node 具有构建快速 API、服务器、桌面应用程序甚至机器人的框架，同时它可以创建想象到的各种模块的庞大社区。这里有一些你可能想研究的框架：Express、Koa、Next、Nodal.

PHP 是一种拥有大量 Web 框架可供你选择的 Web 开发语言。由于其拥有出色的文档和功能，Laravel 已建成了一个活跃的社区。Zend Framework 发布了第 3 版，这标志着面向业务框架的巨大升级。在今年，我们也看到了 Symfony 发行了很多新的版本，使它成为了全栈解决方案中更好的选择。

对于 Ruby 来说，Rails 框架是首选的。Rails 5.0 版本已于今年发布，并为 Web Sockets、API 模型等方面提供了支持。对于小型应用程序而言，Sinatra 也是一个不错的选择，Sinatra 2.0版本预计在 2017 年发布。

Python 有着以 Django 和 Flask 为组合的全栈/迷你型框架。Django 1.10 已在今年 8 月发布了，它为 Postgres 引入了全文搜索和一个重大修改的中间件层。

Java 的生态系统中，依旧有很多流行的 Web 框架可供你选择。Play 和 Spark 便是两个必备的选择，同时它们也可以与 Scala 一起使用。

对于编程爱好者来说，你还可以选择 Phoenix，它是用 Elixir 编写的，它试图成为一个具有卓越的性能，并能完整替代 Rails 功能的框架。如果 Elixir 是你想在 2017 年学习的语言之一，不妨尝试下 Phoenix.

学习其中之一：全栈后端框架、一个微框架

数据库

数据库

PostgreSQL 在今年已经发行了两个完整的版本——9.5和9.6.它们带来了我们从 MySQL 就开始期盼的 UPSERT （aka ON DUPLICATE KEY UPDATE）功能，以及更好的全文搜索和速度改进功能，这多亏了并行查询，更高效的复制、聚合、索引和排序。Postgres 适用于大规模、TB 级规模的数据集以及繁忙的 Web Apps，这些优化都是很受欢迎的。

MySQL 8.0 将是数据库的下一个主要版本。预计在 2017 年发布，它将给系统带来更多的改进。MySQL 仍然是最受欢迎的数据库管理系统，整个行业都受益于这些新的版本。

对于 NoSQL 的粉丝们，我们推荐 CouchDB。它是一个快速、可扩展的 JSON 存储系统，同时公开了一个 REST-ful HTTP API. 此数据库易于使用，同时性能卓越。与 CouchDB 对应的是 PouchDB ，它可以完全在浏览器中工作，并且可以与 Couch 同步数据。所以你可以在离线应用程序上使用 PouchDB ，联网后它会自动同步数据。

Redis 是我们最喜欢的键-值存储型数据库。它体积小、快速并且有丰富的特性。作为 NoSQL 数据存储或进程消息和同步通道，你可以使用它作为智能分布式高速缓存系统的可替代方案。它提供了大量的数据结构可供选择，并且在即将到来的 4.0 版本中会有一个模块系统，并将改进复制功能。

学习其中之一：Postgres、MySQL、CouchDB、Redis.

编程工具

工具

Yarn 是由 Facebook 开发的 Node.js 包管理器。它是对 npm 命令行工具的升级，并提供了更快速地安装，更好的安全性以及确定性的构建。它仍然使用 npm 包注册表作为其后端，因此您甚至可以访问同一个 JavaScript 模块的生态系统。Yarn 与 npm 使用的 package.json 格式是兼容的，区别在于前者能实现快速安装。

作为两个最受开发者欢迎的开源代码编辑器——Visual Studio Code 和 Atom ，在过去一年中，我们看到了它们进行了很多不可思议的创新。这两个项目都是使用 Web 技术构建的，社区中也吸引了大量的粉丝。编辑器具备高扩展，提供了诸如语法检查、linting 和重构工具的相关插件。

作为最流行的源代码版本控制系统，Git 当之无愧。虽然它无服务器，但你可以将计算机上的任何文件夹转换为存储库。如果你想共享代码，像 GitLab、Bitbucket 和 GitHub 都是不错的选择。在 2017 年，我们建议你熟悉 git 命令行，因为它会比您想象的更加方便。

桌面应用程序依然没有消失。即使 Web App 变得越来越强大，有时你依然会需要强大的功能和 API，这是 Web 平台无法提供的。你可以使用诸如 Electron 和 NW.js 之类的工具，利用 Web 技术来创建桌面应用程序，同时你也可以完全访问操作系统和 npm 可用的广度模块。要了解这些工具的更多信息，请阅读有关 Electron 和 NW.js 的教程。

软件开发团队中的最新趋势是让开发人员负责自己软件项目中的部署，也称为 DevOps.这能产生更快地发布和更迅速地修复生产中出现的问题。而具有运维经验的开发人员将得到公司的高度重视，因此从现在开始熟悉能够实现这一目标的技术，将对你来说是一个巨大的提升。我们推荐的工具是 Ansible 和 Docker 。同时，具备 Linux 命令行和基本系统管理技能，也将为你的职场生涯大大的加分。

尝试一个或多个学习：Yarn、Git、Visual Studio Code、Electron、Ansible、Docker.

技术

技术

伴随着大型公司关闭数据中心，并调整其整个基础设施到云上，我们可以看到云已经赢得了整个软件行业。目前三个主要的平台是 AWS, Google Cloud 和 Azure。这三大平台都有着强大的功能，同时不断地扩展其功能集，涉及虚拟机、数据库托管、机器学习服务等。由于价格的迅速下降，小公司和个人开发者也都可以接触到云。对于 2017 年，在云上部署一个业余项目将是一个很好的学习积累。

人工智能是 2016 年的流行词。语音识别和图像分类只是该技术在面向用户应用程序的两个部分，人工智能设备的性能达到甚至超越了人类的水平。当下众多的创业公司也将 AI 和机器学习应用到其新的领域，同时许多相关的开源项目也已经发布，例如谷歌的 Tensor Flow 和微软的 Cognitive Toolkit。机器学习是一个与数学非常相关的主题，对于刚刚开始的人，这里有全面的在线课程供你学习。

虚拟现实（VR）和增强现实（AR）已经存在了一段时间，而最终该技术已经成熟到足以提供引人注目的体验。
Facebook（Oculus Rift），Google（Daydream）和 Microsoft（Windows Holographic）都有欢迎第三方开发者加入的虚拟现实平台。然而 VR 穿戴设备依然面临着艰巨的挑战。例如如何消除穿戴者恶心的感觉，以及脱离了游戏圈，又如何创造令人信服的使用案例。

挑一种学习：云部署、机器学习库、VR 开发

如果觉得文章不错，不妨点个赞。–

注：

若有翻译不当之处，还请大家多多指正，我会及时修改；

英文原文：The Languages, Frameworks and Tools You Should Learn in 2017
作者：Martin Angelov
译者：IT程序狮
译文源自：http://www.jianshu.com/p/a6f61bc3266c

4.Linux知识工具大全

引者注：首先不得不说一下：https://linux.cn/ 以及鸟哥的私房菜。

作者 威客安全 关注

2015.12.04 14:02 字数 109 阅读 323评论 4喜欢 7

简介：

Linux is a Unix-ish POSIX-compliant OS family. Most of the distros are GPL or otherwise FOSS. The defining component of Linux is the Linux Kernel, first released on 5 October 1991 by Linus Torvalds.

新版本

开始

受欢迎的网站

著名发行版本

Grok Linux

Linux Virt

可调参数

Linux日志

Book/ebooks

Kernel Matrix

内核地图

In Production

Linux论坛

shell指南

Linux安全

Linux桌面

防火墙

linux NAS

最佳实践

[本文转自微信公众号：Openskill]

5.Web 开发者必上的 10 个网站

作者 Aufree 关注

2015.03.11 10:51 字数 450 阅读 4234评论 6喜欢 288

原文出处:http://qr.ae/joLLK

由@李锦发完善并发布

同时也关于各位关注我的 GitHub

1.Codecademy

Codecademy 上面有许多不错的学习 Web 开发的文字或视频教程, 适合大多数 Web 开发初学者学习.

2.HTML Dog’s Beginning HTML Guide

HTML 教程, 从初级到中级再到高级, 分层学习 Web 开发, 一切从 HTML 开始.

3.Ruby on Rails Tutorial

Ruby on Rails 是一个非常流行的 Web 开发框架, 以开发速度敏捷迅速而受广大 Web 开发者的青睐, Ruby on Rails Tutorial 是非常著名的 Rails 教程, 适合开发者快速上手 Rails 的开发, 另外英语不好的同学可以看 Andor 翻译的中文教程

4.Mozilla Developer Network

Mozilla 开发者文档, 非常强大, 你想到的, 想不到的在上面都能找到

5.PHP 101 for the Absolute Beginner

PHP 开发的系列教程, 适合新手学习, 内容比较简单易懂, 学完之后可以上手 Laravel 玩玩.

6.GitHub for Beginners

Git 和 GitHub 对一名优秀的程序员来说是必用的工具和网站, 这篇文章主要讲解 Git 和 GitHub 的一些使用方法

7.Non-Programmer’s Tutorial to Python 3

简单讲解 Python3 的使用, 适合快速上手 Python

8.30 Days to Learn jQuery

30 天学习 jQuery 开发, 平均每个视频 20~30 分钟, 适合新手学习

9.A Roadmap for Beginning to Code

一位过来人教授如何学好 Web 开发, 从前端到后端, 从版本控制到部署上线, 看完之后能使你对 Web 开发的流程有个基本的概念

10.Coding Pitfalls for Beginners

主要分析和讲解 Web 初学者在实战中经常会遇到的坑.

Po 主微博: http://weibo.com/jinfali

6.逆向

至于逆向就坑了呀…这种东西只能看看书了。就像学开锁，你要找资料就难了呀。

我学习了两年的逆向工程，前期主要从事windows 平台的漏洞分析与利用研究，后期进行了android平台下的逆向分析研究，对windows平台下的逆向分析比较熟悉。针对如何学好逆向可以有以下几个方面可以参考：
1、具备基本的编程能力，如c、c++，c、c++作为很基础的语言，不要求精通，但是必须会写，写个小工具完全没有问题，同时要对c++的类、继承、虚表虚函数等很熟悉，很多游戏都用c++开发，而且比较庞大，只有基础掌握好，才能更好的从汇编层来读懂代码，很多时候我们看单条汇编指令时完全没有问题的，但是一旦组合起来就会完全不知所云了，通过必须对高级语言对应的汇编语言实现要掌握，比如函数工作的原理，几种调用约定、参数传递方式以及返回值等都必须掌握，这方面网上很多资料。最好能懂python，python作为一种脚本语言，可以用来开发许多逆向调试工具的插件，可以帮我们节省很多的体力活。
2、对windows系统知识比较了解，因为外挂会设计比较多的windows系统知识，因此要对windows底层要一定的掌握，比如windows api，以及外观常用的注入、钩子技术还有windows系统的异常处理机制等，可以到广海论坛学习外挂常用的较按键精灵、加速齿轮以及注入等同用知识，书籍可以可以参见《windows核心编程》，对底层知识了解越多，分析外挂技术也越容易。
3、对逆向分析工具的熟练使用，我们平时工作中面对的是二进制可执行程序，要做外挂我们首先的分析目标程序，因此对常用的调试工具windbg、ollydbg、静态分析工具ida一定要熟练使用。网上教程也比较多，可以到看雪论坛上利用相关的crackme练手学习。
4、掌握外壳原理和技巧，熟悉常见的加解密算法、反调试技巧，我们分析程序时经常会遇到很多加壳程序，因此我们必须对外壳的原理和基本知识比较熟悉，熟练掌握同用的脱壳技巧，同时对各种反调试技巧也必须要很熟悉，在分析程序时，一般会遇到很多加解密算法，因此必须要对各种加解密算法的特征有一定的快速识别能力，这样能更快得帮助我们分析目标程序的核心功能。这方面可以参看《加密与解密》这本书，讲的非常好与详细。

作者：梨梨喵
链接：https://www.zhihu.com/question/23999930/answer/26345155
来源：知乎

看题主的描述应该是想学外挂开发方面的吧，那我姑且把范围划到Windows下X86/X64的逆向与分析，提供一个入门学习的个人不完全的小意见:

1.学习C/C++语言与Windows下的32/64位汇编语言，大致学习掌握计算机组成，熟悉语言的各方面实现细节。了解程序特别是底层的运作机制，因为在实战中你将面对的是文档几乎为0的底层汇编代码，了解它们是如何工作很重要。而且还有一点现在几乎所有的游戏底层都是用C++编写的。

2.光有语言的基础还要懂如何运用到实战中去，这里推荐一本书:REVERSING:逆向工程揭密。一开始可能面对一个大型的项目可能会力不从心，比如现在不少游戏都有内核级的进程保护模块，而且代码量巨大，结构复杂。入门可以跟从书上的例子进行实践，或者在网上找些creakMe之类的先练练手。渐渐熟悉之后再找一些大型的程序逐渐深入。

3.学会使用工具很重要，在逆向中广泛使用的工具如静态反汇编IDA pro和动态调试器OllyDbg还有内核调试winDbg等等，要熟悉它们的使用方式，要懂得调试程序，掌握一些调试技巧，这方面资料在网络和书籍上都有很多。更进一步可以尝试编写些小插件辅助自己的分析。

4.多关注这方面的消息，比如国内的看雪论坛就有不少这方面的高手，也常常能见到这方面的分析讨论。同时最好能够广泛涉猎，多了解相关的知识如加密解密，网络原理，内核编程，反调试和代码混淆等等的会大有裨益。另外逆向分析别人的游戏外挂有时会有惊奇发现哦，比如发现种新的绕过方式，比如挖出个后面木马什么的然后反向社工爆菊什么哈哈哈。

手机码字，排版格式不太好，思路也不是很清晰，以后有时间修正。

作者：匿名用户
链接：https://www.zhihu.com/question/23999930/answer/26345853
来源：知乎

逆向想搞的好，首先最好得有windows应用层，开发的实战经验。系统理论也得打好。

学汇编可以搞好逆向？，，，，伪命题。

你应该具备以下知识：
c/c++语言基础
x86和x64汇编,
windows系统理论：
参考：windows核心编程，深入解析windows系统，windows内核原理及实现等，，
应用层：
sdk(必学啊),mfc(没饭吃),.net(微软目前的主流，建议添加)等
Windows PE
驱动开发
Rootkit
软件调试：
比如ida,od,windbg
套接字网络编程
…
这些书和资料你就去http://z.cn和jd买比较流行的吧，绝版了就去淘宝找买复印书的买盗版，
话说为啥要做黑客呢？
以上这些你比较用功花4、5年完成，，
然后你就面临一个坑爹的事实

这些只是基础啊，，，，，，，，，，
坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊坑爹啊

去学习，实用的技术吧，，看雪，52pojie啦

强烈建议购买业界良心【五年一剑】看雪论坛鼎力打造—《加密与解密(第三版)》[附:网购地址]:

作者：杨盼盼
链接：https://www.zhihu.com/question/23999930/answer/131331827
来源：知乎

逆向，是安全领域必备的技能之一。但凡有编程经验的人都应该熟知高级语言源代码从编译链接到执行的过程，逆向就是把这个过程反了过来…反病毒人员捕获到样本，需要对其逆向才能分析出该样本的行为，才能开发出有效的专杀工具。 研究0day的hack也是通过逆向的手段探寻二进制文件中包含的逻辑缺陷。 Cracker通过调试器定位到关键的注册算法，理解算法并写出注册机，也需要扎实的逆向功底。 说了这么多， 推荐一本良作《C++反汇编与逆向分析技术揭秘》作者钱林松，机械工业出版社。从书名就可知道，C++和汇编是逆向领域永远都绕不开的话题。 至于安卓逆向，不在笔者的专业范畴之中，也就不做讨论了。国内的看雪和吾爱都是较有影响力的站点吾爱破解-LCG-LSG|安卓破解|病毒分析|破解软件|www.52pojie.cn看雪安全论坛 - www.pediy.com

【技术分享】iOS & Mac OS X逆向工程学习资源汇总

调试

这是一份理解调试过程和应用程序运行机理的文档。

Mac OS X调试技巧笔记 (TN2124) (链接 - PDF镜像)

iOS调试技巧笔记 (TN2239) (链接 - PDF镜像)

了解和分析iOS应用程序崩溃(Crash)报告 (TN2151) (链接 - PDF镜像)

Malloc调试环境变量 (链接 - PDF镜像)

Mach-O Binaries

Mac OS X和iOS使用Mach-O文件格式的可执行二进制文件和共享库。

Mach-O 维基百科 (链接)

OS X ABI Mach-O文件格式参考 (链接 - PDF - PDF镜像)

Mach-O编程话题 (链接 - PDF - PDF镜像)

分析

二进制分析简介及入门指南。

分析Binaries with Hopper (链接)

System ABIs

ABI 维基百科 (链接)

Calling Conventions 维基百科 (链接)

Mac OS X ABI (链接 - PDF - PDF镜像)

iOS ABI (链接 - PDF - PDF镜像)

动态链接库编程话题 (链接 - PDF - PDF镜像) (文档 - 文档镜像)

OS X ABI动态加载程序参考 (链接 - PDF - PDF镜像)

编程语言学习资源

在理解程序运行的原理之前你需要又一个良好的编程语言基础。

英特尔x86架构 (PDF - PDF镜像)

x64汇编指南 (PDF - PDF镜像)

ARM体系结构(ARMv7) (PDF镜像)

ARM体系结构(ARM64) (PDF镜像)

OS X汇编指南 (链接 - PDF - PDF镜像)

Learn C The Hard Way (链接)

C语言函数库参考指南 (链接)

Objective-C语言 (链接 - PDF - PDF镜像)

Objective-C运行时(Runtime)(链接 - PDF - PDF镜像)

进阶

收集博客等阅读资源，从多角度深入理解编程语言和系统功能。

NSBlog (链接)

Reverse Engineering Mac OS X (链接)

Landon’s Blog (链接)

OS X Internals (链接)

Greg Parker’s Blog (链接)

Ridiculous Fish (链接)

Snare’s Blog (链接)

To The Apple’s Core (链接)

The Objective-C Runtime: Understanding and Abusing (链接)

工具

Mach-O二进制分析：

MachOViewer (主页)

16进制编辑器:

Hex Fiend (主页)

0xED (主页)

Synalyze It! (主页)

反汇编:

Hopper (主页)

IDA (主页)

otool (man page)

otx (主页)

反编译:

Hopper (主页)

Hex-Rays (主页)

classdump (主页)

codedump (i386) (下载链接)

调试器:

GDB (Not shipped on OS X anymore) (主页)

LLDB (主页)

PonyDebugger (链接)

内存编辑器:

Bit Slicer (主页 -源码)

命令行工具:

nm (man page)

strings (man page)

dsymutil (man page)

install_name_tool (man page)

ld (man page)

lipo (man page)

codesign (man page)

hexdump (man page)

dyld_shared_cache (链接)

vbindiff (链接)

binwalk (链接)

xpwntool (链接)

objdump (链接)

有用的代码仓库

Apple Source Code (链接)

PLCrashReporter (链接)

Mike Ash’s Github (链接)

Landon Fuller’s Github (链接)

Jonathan Rentzsch’s Github (链接)

fG!'s Github (链接)

文章最后发布于: 2020-01-07