Click Here

查看: 13622|回复: 26 [复制链接] 除了最常见的网页爬虫，还有一种是针对客户端软件的爬虫。前者使用范围广泛，对后者的数据采集需求越来越大。潜水多年的小白第一次发帖，内容如有不当，请随意斧正。 常见客户端： PC （ Windows 、macOS 、Linux ）、Android 、IOS 抓包工具： 支持平台：Windows 、 macOS 、 Linux 以下内容都是基于这款抓包软件。 需求分析： 想要批量或者自动获取某一平台客户端的某些数据。要做到我们的需求，需要使用网络抓包工具。据了解得知，网络协议层的每一层几乎都有对应的抓包工具。现如今最常用的协议是 https、http 这两种网络传输协议。 HTTP 协议抓包： http 协议不包含 SSL ，抓包时只需要简单配置网络代{过}{滤}理即可抓取，而 https 需要安装证书并且信任证书才能抓取，否则无法解析显示为红色的 unknown 。 HTTPS 协议抓包： https 协议在配置网络代{过}{滤}理的前提下还需要安装证书，并且必须让系统信任安装的证书才能实现对 https 协议进行抓包。 Charles 快速上手： 主界面： 常用功能菜单： 常用功能菜单，故名思义这两个菜单是经常会用到的，这里先做一些说明： Proxy： Start Recording：开始捕获网络流量，对应主界面的红点图标。 Start Throttling：进入低速网络模式，对应主界面的乌龟图标。 macOS Porxy：勾选时 Charles 处理 macOS 的网络流量。 Proxy Settings：配置 HTTP 代{过}{滤}理端口，在给同一局域网内设备安装证书，或是设置代{过}{滤}理时需用到，常见设置为 8888。这里还包含一些 HTTP 、SOCKS 相关的设置。 SSL Porxying Setting：配置是否启用 SSL ，启用时需配置主机（HOST）与端口（PORT）勾选上即为激活状态，在不清楚主机和端口时，可将主机与端口都设置为 *（星号），这样做可以捕获 http 和 https 的所有流量。 Help —— SSL Porxying： Install Charles Root Certificate：安装证书到 macOS 系统内。 Install Charles Root Certificate on a Mobile Device or Remote Browser：为同一局域网内的其它设备安装 Charles 证书. Save Charles Root Certificate：保存 Charles 证书到本地，可选 .pem .cer 两种类型的文件，推荐选择 .pem ，后续便于 Android 设备导入证书。 安装 Charles 证书 macOS：Charles 主界面点击 help —— SSL Porxying —— Install Charles Root Certificate ，默认安装即可完成安装。 正如前面所说，安装完以后还需要让系统信任这个证书，具体做法：在所有程序中找到 钥匙串访问 —— 左栏下方 —— 点击证书 —— 双击 Charles Proxy CA ——信任 ，可以将所有的选项都设置为 始终信任。即可成功开启对 HTTPS 协议的捕获。 IOS：Charles 主界面点击 help —— SSL Porxying —— Install Charles Root Certificate on a Mobile Device or Remote Browser 会出现 " Configure you device ..... HTTP proxy on 192.168.1.6:8888 , then browse to chls.pro/ssl " 这里的 8888 在 Proxy —— Proxy Settings 内设置。 手机或者其它设备要和抓包主机连接到同一局域网（网络频段也有影响），打开 设置 —— 无线局域网 —— 点击与抓包主机同一个局域网的那个 Wi-Fi 拉到底部 —— HTTP 代{过}{滤}理 —— 配置代{过}{滤}理 —— 手动 —— 服务器填前面的 192.168.1.6 端口填 8888 —— 右上角存储 。 回到主界面，打开 Safari 浏览器，在地址栏输入前面的 chls.pro/ssl 打开。Charles 会弹出是否允许连接，点击 Allow 。手机上允许下载一个配置描述文件，下载完成后关闭。 手机打开设置 —— 通用 —— 拉到底部找到 描述文件 打开 —— 点击 Charles Proxy CA （ ..... ）—— 右上角安装 —— 输入密码再次安装 —— 完成后拉到上面找到 关于本机 进入 —— 拉到底部找到 证书信任设置 进入 —— 打开 针对根证书启用完全信任。 完成以上步骤后，即可抓取 IOS 客户端数据。 Android： 自 Android 7.0 以后无法信任第三方根证书，抓取第三方 app 数据时，现有方法几乎都需要 Root 设备，自行考虑风险。还可以使用 Android 模拟器来抓取数据，但是模拟器的信息不是很完整，容易被客户端app后台所识别出来，比较费力不讨好。现有的几种 Root 后抓取 HPPTS 的方法我都尝试过： 使用 Xposed & edxposed 模块，在安装了 Xposed & Edxposed 框架的前提下，再安装 TrustMeAlready 模块并激活（经测试，部分系统 Android 10 ，部分软件无法使用，比如X信小程序）； 安装 VirtualXposed ，再安装 TrustMeAlready 模块并激活，因为 VirtualXposed 较容易被第三方app识别，从而禁止使用，优势是不需要root ； Root 后将 Charles 根证书导入并信任根证书，这个办法其实是将 Charles 根证书转换后放到 Android 系统根目录内。 Charles 主界面点击help —— SSL Porxying —— Save Charles Root Certificate ，选择保存为 .pem 文件，以下只讲这种文件的转换方法。.cer 文件转换方法请自行寻找，欢迎交流。 保存好 .pem 文件后，macOS 需要安装 openssl ，然后打开 终端app —— 输入 openssl x509 -subject_hash_old -in Charles根证书文件.pem 回车结果如下，圈起来的这串字符很重要： d2479ff1 上一步完成后，将下载的 charles-proxy-ssl-proxying-certificate.pem 重命名为 d2479ff1.0 ，将 d2479ff1.0 文件放到手机内。 手机端安装 MT文件管理器 ，打开授予 root 权限，使用 MT文件管理器复制到 /system/etc/security/cacerts/ 文件夹内，重启手机，在设置内搜索 加密与凭据 —— 打开后找到 信任的凭据 打开 —— 在系统部分可以找到 详细信息为 Charles Proxy CA （ ..... ）的证书，代表成功导入证书到系统中。 可使用 Charles 抓取 HTTPS 协议。 利用 Magisk 导入证书 自 Android O（8.0）以来，即使是获取了 root 权限，也很难修改系统分区文件，无法进行读写。且当下手机 root 方式都是利用 Magisk 修补 boot ，Magisk 还可以利用旁载的方式加载各种自定义模块，包括且不限于修改、替换系统文件。那么在这里我们可以根据上文所诉，创建一个 Magisk 补丁包，用以导入证书文件到根目录。 首先还是需要安装 Charles 以及 OpenSSL （Windows 推荐使用 choco install openssl 命令安装，需使用带管理员权限的 powershell ） 导出证书文件 依次点击 charles -> help -> SSL Proxying -> Save Charles Root ..... 选择位置导出 Charles 证书文件 转换证书文件 命令行切换到证书所在文件夹，运行： openssl x509 -subject_hash_old -in 证书文件.pem 将证书文件改名为 d2479ff1.0 （以上文为例，后缀为 .0 ） 创建 Magisk 模块 首先需要 Magisk 模块模板 magisk-module-template ，解压后文件列表为： └magisk-module-template-master │ customize.sh │ module.prop │ post-fs-data.sh │ README.md │ service.sh │ system.prop │ ├META-INF │ └com │ └google │ └android │ update-binary │ updater-script │ └system #内部文件夹为自建 └etc └security └cacerts 上图详细文件说明详见 Developer Guides这里我们关注 system 文件夹及子文件夹即可。模板文件是仅有 system 而没有其子文件夹的，system/etc/security/cacerts/ 刚好对应着我们本来要放证书的地方，即系统证书所在目录.此时将我们的证书文件放到 cacerts 文件夹内，将整个文件夹压缩为 zip 文件，放入手机内，在 Magisk 内刷入即可，验证方式如上。 查看全部评分 收藏91 淘帖0 有用1 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 推荐 败败败 发表于 2023-7-17 01:02 雪走aa 发表于 2023-7-16 10:41 最新版固件降级大概率变砖，不再提供了，所以我关闭了降级程序的验证服务器，降级程序不可用了 原来是这么回事，我说呢，我都郁闷了，换几台电脑几个系统全都如此，我还以为这程序是不是中毒后杀毒给坏了.....如果从139降呢？会不会也大概率变砖.....但经对比，个人感觉139比140要好，139说没108好吧好像也不是，主要是没仔细对比【吾爱破解论坛总版规】- [让你充分了解吾爱破解论坛行为规则] 7# 联盟少侠 发表于 2021-7-1 18:51 给大佬点个赞，这样的教程确实很不错。 挺适合新手的。 至于不走WIFI的代【】理正常得很，用其他软件强制走就行了！ 查看: 17096|回复: 55 [复制链接] Apple专门发布了兼容iOS11的并包含AppStore功能的iTunes12.6.3版本，iTunes 12.7移除了AppStore功能。 Charles安装证书 下载好Charles安装好之后，需要安装一个SSL证书。具体步骤如下 抓包步骤 关闭系统的代{过}{滤}理，打开Charles。 打开iTunes下载一个软件，我这里以有道词典为例 下载过程中，切换回Charles，观察左侧栏中p(xx)-buy.itunes.apple.com这个域名 右击这个域名，选择Enable SSL Proxying。然后我们切回到iTunes，重新下载该软件。 点击展开域名WebObjects/MZBuy.woa/wa/buyProduct，右侧信息栏中，点击Context>>选择XML Text格式 通过appID获取所有版本 可以查看所有版本和日期。通过抓包也是可以获取到版本号信息。位于中间就是版本号。 appID获取可以通过iTunes复制应用连接获取到appID 查询版本完成后，右击该域名，选择breakpoint断点，然后切回iTunes，再一次app下载。 下载过程中，回跳出一个断点界面。点击右侧XML Text，修改appExtVrsId版本号。完成之后执行Execute。期间会再次跳转断点界面，点击Execute执行即可。 下载的ipa文件可以通过资料库查看，确实是老版本iTunes。 流程梳理 Charles安装SSL证书 iTunes第一次下载app，注意域名“p(xx)-buy.itunes.apple.com”，开启“Enable SSL Proxying“ iTunes第二次下载app,查看版本号信息，打断点“breakpoint“ iTunes第三次下载app，修改“appExtVrsId“值，即版本号 iTunes资料库获取 ipa文件 ipa如何安装 利用iTunes 安装到iPhone 通过第三方软件安装 利用一些脚本软件或者捷径等安装ipa 抓包旧版App好处 旧版本可能存在一些好用的功能，比如追书神器这类app 旧版本可能存在实断版本，lifetime等等 或者新版本用的不舒服，想换回老版本 查看全部评分 收藏92 淘帖0 有用1 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 查看: 46257|回复: 329 [复制链接] 收藏353 淘帖0 有用20 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 4# 涉济 发表于 2021-1-14 10:59 查看: 8862|回复: 23 [复制链接] 本帖最后由 小鲤鱼 于 2020-5-21 10:06 编辑 上一篇初步介绍了怎么使用charles来对Memrise 进行抓包体验会员功能，本文以人人视频为例来分别分享一些思路，怎么去广告？怎么看vip视频？怎么解锁视频清晰度。 使用到的软件 ios用户可直接使用 httpCatcher 安卓用户需要配合charles使用，论坛中有大佬分享了破解版，搜索一下安装即可，搜索不到的可以到我博客上下载。 charles设置ssl成功，没配制好的上面的链接配置一下 人人视频 charles的方法安卓和ios通用，并且手机上不需要下载任何抓包软件。 本教程默认ssl已经装好并且手机已经信任了证书。 人人视频 charles教程 打开charles和该app，发现有开屏广告。 通过搜索charles可以发现具体在广告具体在api/ad/union/sdk/中，如下图，在最上层的host处右键block list即可。 右键加入blockList即可 该app直接改vip不太好改，我们先看下vip对应的功能，主要有解锁原画，免广告和专享剧集三项，随便点一个视频进去，看下能不能实现这几项功能。 随便打开一个视频，发现视频开头有广告，为了防止电脑中其他请求影响，在左侧左下方的Filter处输入rr.tv ，这意味这我们只要人人视频的包出在在里面，可以发现点击视频后会依次请求 get_priority_video_quality_config?seasonId=15961, v1/get_movie_info?encrypt=1&episodeSid=152154&isDLError=0&quality=HD&seasonId=15961&urlId= 这两个接口，请注意不同的视频对应上图中的sessionId和episodeSid不同，只要结构类似即可，不必完全相同。 先点击get_priority_video_quality_config这个接口，从接口名字可以看出这是个视频清晰度的接口，可以看到在sortTime里的每一项都包含有canplay，canshowVip，初步推断这个是判断当前是否可以播放的，将canplay全部改成true，canshowVip全部改成false canPlay":\s*\w+ canPlay": true canShowVip":\s*\w+ canShowVip": false 本来想去广告的，阴差阳错的把原画的给改了。再看看get_movie_info这个接口，这个接口是选择清晰度的，因为上面的默认清晰度是高清，可以看到接口返回的数据中有个externalAds，我们将它改为false即可。 重新打开后可以发现开头的广告没了，点击清晰度可以看到原画和AI原画可以选择，然而原画和AI原画依然切换不了，还有一个问题就是暂停也有广告，先搞定暂停广告的。 切换charles到Sequence，将之前的请求全删了，在视频处点暂停观察请求包。 额，居然是腾讯广告。 把mi.gdt.qq.com开头的和v2.get.qq.com全部加如block List。 搞定 对于清晰度的可以先选择原画，可以看到get_movie_info接口中返回的currentQuality还是SD格式，因此我们将这个参数改为自己想要的，若是原画改为“OD“，AI原画改为“AI_OD“，这样的话还需要将链接改下可以看到对于请求某个清晰度时,get_movie_info接口中的quality就会使用对应的格式，干脆一股脑直接全改了，将request的链接中的quality改为OD，将response的currentQuality也改为OD即可。 get_movie_info?encrypt=1&episodeSid=152154&isDLError=0&quality=HD&seasonId=15961&urlId= 8.再试下，可以看到默认原画清晰度，暂停也没广告了，大家看下是不是原画画质啊，我也看不出来。 看vip视频，回来再写，恰饭去了，溜了 今天的教程大家学会了吗？有问题的话评论区交流，有需要其他的去github提issues哦，顺便求star一波，好修，这种教程看的人好少，我的博客根本没人看。 [/md] 查看全部评分 收藏45 淘帖0 有用3 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 Hello, Recently I have been in a lot of confusion as to which one of these is correct: 1) I borrowed Charles' pencil. 2) I borrowed Charles's pencil. I feel only sentence 2 is correct. Please let me know if my understanding is correct or not. Besides this, I am also wondering how we would pronounce "Charles's". I think it would be pronounced as "Charlses", is that correct? Similarly, "Prince's" should be pronounced as "Princes" in this case which would be a little confusing as it would be similar to "Princess". Please let me which pronunciations would be correct. Thank you. There have been several threads on this topic. Both 1 and 2 are used. In RP, Charles is pronounced /tʃɑːlz/, and Charles's = /'tʃɑːlzɪz/ Prince's / Princes is pronounced /'prɪnsɪz/ Princess is /prɪn'ses/ so the two words are quite different. There have been several threads on this topic. Both 1 and 2 are used. In RP, Charles is pronounced /tʃɑːlz/, and Charles's = /'tʃɑːlzɪz/ Prince's / Princes is pronounced /'prɪnsɪz/ Princess is /prɪn'ses/ so the two words are quite different. Thanks for the reply, it does clear the doubts about the pronunciations. And I made this thread because I couldn't find anything about it when I searched it. :/ I am still waiting for other opinions on sentence 1 and 2, maybe one of them might be more correct (if not only correct). Both are very common. Some people prefer to write Charles', others Charles's. I think most people pronounce the extra syllable, even if they don't write it. I'll leave it to the experts to tell you if one or the other is more correct. But your questions made me realize something interesting about my own usage of the possessive form for words ending in the letter "s". I always write them with the terminal "s" followed by an apostrophe, but with out a second "s". However, in speaking, I always pronounce both of them. Inconsistent, I know, but that's how I do it. I remember learning as a child that the only time a name ending in 's' should not take a second 's' is if it were the name of a famous historical person, i.e. Jesus' not Jesus's, Socrates' not Socrates's. Additionally, my spell check just protested Jesus's, so it appears that other people shared my teacher's opinions. For all other names, the second 's' should be included. If you read the sticky at the top of English Only, you'll see that panjandrum lists (click) the most frequently raised topics in this forum, and that this is one of them. By following his link, you'll find a number of previous threads [This question and the subsequent posts have been added to a previous thread on the same topic. Please read down from the top. DonnyB - moderator] Hi As I searched online, both ways are correct when a proper noun ends in 's': Charles' car Charles's car And that it is a matter of personal preference. I wonder how they are pronounced and if there is any difference. I suppose the second one is [Cha:lziz]. What about the first one? Last edited by a moderator: Aug 29, 2019 Yes, you can pronounce it either with or without the extra syllable. I personally think that if you say it as Charles you should write Charles', while if you add an extra syllable you should write it as Charles's - but not everyone follows this. So you can do without 's and it still implies it. Charles' car [cha:lz] Charles's [cha:lziz]. One local book I consulted said: James' [djeimziz] It had this transcription and not [djeimz] Last edited: Aug 29, 2019 I would pronounce them 'Charlsiz' and 'Jamesiz' regardless of how they are spelt. (And I would spell them both with the apostrophe.) I would pronounce them 'Charlsiz' and 'Jamesiz' regardless of how they are spelt. I might make exceptions. If there is a "James' Street", for example, I would almost certainly pronounce it as "James", without the "iz" ending, unless I knew locals pronounced it differently. However I pronounce both St James's Park (London) and St James' Park (Newcastle) as "Jamesiz". The pronunciation of the royal park in London is universal, I think, but there are people who pronounce Newcastle United's football ground as "James" and this, apparently, is how the club say it should be pronounced. I almost always use just an apostrophe in writing, not adding a second letter "s". I would always pronounce place names and the like as they are 'correctly' or locally pronounced (if I know them), but in contexts like the OP sentence, it would always be with the extra 'siz' syllable. I don't afford (singular) words ending in s any special privileges, adding and pronouncing the 's for each one. I don't have a problem saying Jezusiz or Mozesiz for Jesus's and Moses's but accept that many will object to that and they will omit the s in writing and pronunciation. Hi everybody! I have a doubt about the construction of the anglosaxon genitve, when the name of the possessor ends in "-s" (but it is singular), how is it formed? Do we need to add a second "-s" after the apostroph? example: this is Charles' new car or this is Charles's new car Thanks in advance! For most English names that end in "s", the possessive is formed by adding (and pronouncing) an apostrophe and another "s": Prince Charles's wife, Diana Thomas's bicycle Mrs. Harris's house The most common exception to this rule involves names taken from ancient languages: Moses' law Thanks GreenWhiteBlue, so you mean the Moses case is an exception? I have looked for it in many differente books on grammar, and they don't say the same... for example, I have found "Saint James' Square", or sentences such as "He is Luis' doctor", which makes me be terribly confusde about... As far as I know, both are acceptable. I think "Charles' car" is more old-fashioned, where as adding a second 's' is more modern, perhaps in an effort to regularise things. Personally, I use the 's', but I think it's a matter of choice. Coincidentially, when using the first example (Charles' car), would it be pronounced as if there were a second 's' after the apostrophe? As far as I know, both cases are pronounced in the same way, it is just a matter of written form... or, at least, it is what I was taught at University... Thanks! From THIS SITE: Some writers will say that the -s after Charles' is not necessary and that adding only the apostrophe (Charles' car) will suffice to show possession. Consistency is the key here: if you choose not to add the -s after a noun that already ends in s, do so consistently throughout your text.... You will find that some nouns, especially proper nouns, especially when there are other -s and -z sounds involved, turn into clumsy beasts when you add another s: "That's old Mrs. Chambers's estate." In that case, you're better off with "Mrs. Chambers' estate." I mean, it is pronounced the same as the plural of those words finished in a sibilant sound / s, z,/... That is, for example, "house" / 'haus/ , plural form, "houses". / hausiz / This words adds -/iz/ to form the plural, it is the same sound in that cases of genitive. Inquisitor, here is the rule given by William Strunk in his 1918 classic The Elements of Style: Form the possessive singular of nouns with 's. Follow this rule whatever the final consonant. Thus write, Charles's friend Burns's poems the witch's malice This is the usage of the United States Government Printing Office and of the Oxford University Press. Exceptions are the possessives of ancient proper names in -es and -is, the possessive Jesus', and such forms as for conscience' sake, for righteousness' sake. But such forms as Achilles' heel, Moses' laws, Isis' temple are commonly replaced by the heel of Achilles the laws of Moses the temple of Isis The pronominal possessives hers, its, theirs, yours, and oneself have no apostrophe. This is in fact an old, and not a modern usage. For example, the senior palace of the British monarch is not "St. James' Palace", but instead is called "St. James's Palace", and foreign ambassadors are still accredited to the "Court of St. James's." The square in London is in fact "St. James's Square", with the apostrophe + s on the end. Hi everybody! I have a doubt about the construction of the anglosaxon genitve, when the name of the possessor ends in "-s" (but it is singular), how is it formed? Do we need to add a second "-s" after the apostroph? example: this is Charles' new car or this is Charles's new car Thanks in advance! The traditional rule was that a word in the singular which ended in a sibilant sound would have its possessive made by adding apostrophe-s: house/house's, boss/boss's, Davis/Davis's, Charles/Charles's. This would add a syllable to the original word, with the s being pronounced as /s/ or /z/, depending upon the previous consonant. Exceptions to this, as noted elsewhere in this thread, were certain ancient names: Jesus/Jesus', Moses/Moses', Aristophanes/Aristophanes'. In these cases, the possessive form was pronounced the same as the original word. Things have changed, however. While many, including me, still follow the traditional rules, there is a very strong tendency, especially in newspapers, for the possessive of a singular word of more than one syllable to be made by adding simply an apostrophe to the original word, so that house and boss would still have the possessive forms house's and boss's, but Davis would have the possessive form Davis'. Some one-syllable names even form the possessive this way, including Charles, so that its possessive form would be Charles'. One of the reasons newspaper and editors seem to have picked this way of making possessives is that it gives the reader the opportunity of pronouncing the word he sees in writing with or without an additional syllable, depending upon how he himself forms the oral form of the possessive. Since I would say "Charlz-uhz" for the possessive form of Charles, if I see Charles' book in print, I can pronounce it "Charlz-uhz book." Someone who pronounces Charles' the same as he does Charles could see Charles' book and pronounce it "Charlz book." In a sense, these new rules simplify things, but there's a complication involving such one-syllable words as boss. I don't believe anyone pronounces the possessive of boss the same as he pronounces the word itself--people say "boss-uhz," not "boss" for the possessive--yet you occasionally see things written, including in edited copy, such as my boss' orders. According to the traditional rules, this is wrong, but I believe it is also wrong according to the new rules. I would be surprised to find boss' considered correct by any modern style guide. (But if anyone knows of one which permits it, please let us know.) So in summary: Traditionally, the possessive of Charles is Charles's, pronounced "Charlz-uhz." According to the new rules, the possessive of Charles is Charles', which can be pronounced either "Charlz" or "Charlz-uhz." Chuck works for Charles and Chuck's car sounds just fine for me. It saves the wear and tear on grammar rules. If Charles it must be then whether it is Charles' car or Charles's car you have a decent chance that the listener or reader won't know the rule either. Chuck works for Charles and Chuck's car sounds just fine for me. It saves the wear and tear on grammar rules. If Charles it must be then whether it is Charles' car or Charles's car you have a decent chance that the listener or reader won't know the rule either. Hey, you risk causing offense if the Charles in question prefers the nickname Charlie or does not care for nicknames at all (I believe the fictional Charles Emerson Winchester III of M*A*S*H would be an example of this last group). I do understand why people in this forum so often suggest bypassing a given grammatical, spelling, or pronunciation problem altogether by substituting a completely different construction. But every time that is suggested, it strikes me as an unsatisfactory or at least incomplete answer, for this simple reason: Everyone has to quote someone else speaking at some time or other. When faced with the problem of transcribing "He said he had borrowed Charlz-uhz car" you would have to write the possessive one way or the other, as Charles' or Charles's. You wouldn't have the luxury of avoiding the matter. Thanks everybody, especially to mplsray, for being so accurate, I love it! Inqui I was wondering about the use of 's as a pronoun. Example: A: Is that cellphone yours? B1: No, it's Charles'. B2: No, it's Charles's. Is there any difference? I was wondering about the use of 's as a pronoun. Example: A: Is that cellphone yours? B1: No, it's Charles'. B2: No, it's Charles's. Is there any difference? If you say it, there's a massive difference. That's why I prefer the version with the two s's; it's what we say. A: Is that cellphone yours? -- B1: No, it's Charles' /noʊ ɪtz tʃɑːlz/ = You're mistaken, it's not a telephone, it's my friend Charles. A: Is that cellphone yours? -- B2: No, it's Charles's /noʊ ɪtz 'tʃɑːlzɪz/ = No, it belongs to Charles. 查看: 2558|回复: 41 [复制链接] Charles是一个常用的抓包工具，虽然这个软件有30天的免费使用期，而且过期后也只是限制连续使用时间不超过30分钟（这个只是听说，没试过），但终究还是不方便，如果能够注册当然是最理想的。但是，原来常用的charles的在线注册网站已经挂了，模样还在，点啥都不反应了，如图1。 图1 而且有一个开源的charles激活码计算工具也被作者删除了，见图2。 图2 幸好笔者找到曾经下载过一个激活码的计算器，不知道是哪个大佬用go语言写的，随便找了个在线go平台试了下，惊喜地发现，它算出的注册码在最新的charles版本上都能用。转念想到运行go语言的环境可能很多计算机都没有，不如把它转成python的，这样适用性就强些，于是，决定让ai帮我把go语言转成python语言，本来以为这件事对ai来说是件非常简单的事，哪里想到会一波三折，把ai转换过程记录下来，就有了这篇文章。 先用了github上的deepseek-r1模型，图3和图4是与deepseek-r1的对话，图3是我的要求，图4是deepseek-r1的回答。 图3 图4 这段代码执行算出的结果见图5。 图5 从charles官网上下载的最版是5.0，安装好后在help-Enter Charles license...选项的弹出对话框中输入了python 版代码算出的key值，如图6。 图6 然而charles的回应是key无效，如图7所示。 图7 调试了几个版本都是无效的key，看来这个模型的算法并没有真正还原go语言的原始算法。那么，我们换个AI模型再试试，这回选了据称是最聪明的grok3模型，并且把提示词改了一下，一些要求更具体，如图8，和图9所示。 图8 图9 调试了几次，能够计算出来key值，输入到charles里还是无效的key，如图10所示，说明这个最聪明的AI也没有能完全复刻go代码中key的算法。 图10 还是回过头来找deepseek-r1模型，但这回换个部署在硅基流动的模型，提示词跟grok3的一样，见图11。 图11 它的解答见图12。 图12 运行时出错了，如图13： 图13 当我把这个错误信息报给DeepSeek R1后，它长考了300多秒，给出了解答，如图14。 图14 把它修改后的代码随意设置了name参数再运行后得到了key，把name和key输入到charles proxy的help-EnterCharles license...对话框后再点击Register得到的画面是图15啦。 图15 这个信息框出现说明注册成功了。重启charles proxy后再看help-AboutCharles，注册信息如图16。 至此，硅基流动的DeepSeek R1模型帮我从go 复刻出了完整、可用的python语言的最新版charles proxy的注册码算法。虽然人工把go转换到python也是可行的，但效率跟ai是不能比的，不得不说， 有ai的帮助，很多事情都可以高效完成。不过，网上部署的AI模型很多，大家都称自己的是满血模型，这次把go 转python的过程算是一个很简单的测试，号称满血的模型实际上也是有差别的，你也不知道在部署时是不是有阉割，只有多试几个才知道哪些是真正的满血或者说更聪明，我觉得是不是硅基流动模型的血更满些哦？至于号称最聪明的grok3，至少在这个测试中我没觉得它比硅基流动的DS聪明，以后提AI恐怕要有前缀或后缀了，说明是哪里部署的，要不然没得可比性啊。 charles_license.rar 2.61 KB, 下载次数: 201, 下载积分: 吾爱币 -1 CB py原码 查看全部评分 收藏35 淘帖0 有用4 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 推荐 luojineng 发表于 2025-4-13 12:19 吾爱破解论坛没有任何官方QQ群，禁止留联系方式，禁止任何商业交易。 import struct import random rounds = 12 roundKeys = 2 * (rounds + 1) def crack(text: str) -> str: name = text.encode('utf-8') length = len(name) + 4 padded = ((-length) & (8 - 1)) + length bs = struct.pack('>I', len(name)) buff = bytearray() buff.extend(bs) buff.extend(name) ckName = 0x7a21c951691cd470 ckKey = -5408575981733630035 ck = new_ck_cipher(ckName) outBuff = bytearray() for i in range(0, padded, 8): bf = buff[i:i+8] now_var, = struct.unpack('>Q', bf) dd = ck.encrypt(now_var) outBuff.extend(struct.pack('>Q', dd)) n = 0 for b in outBuff: n = rotate_left(n ^ b, 0x3) prefix = n ^ 0x54882f8a suffix = random.randint(-(1 16 == 0x0401 or suffix >> 16 == 0x0402 or suffix >> 16 == 0x0403: in_ = (prefix i) & 0xff vv = n2 & 0xff if vv < 0: vv = -vv return f'{vv:02x}{out:016x}' class ckCipher: def __init__(self): self.rk = [0] * roundKeys def encrypt(self, in_: int) -> int: a = (in_ & 0xffffffff) + self.rk[0] b = (in_ >> 32) + self.rk[1] for r in range(1, rounds+1): a = rotate_left(a ^ b, b) + self.rk[2*r] b = rotate_left(b ^ a, a) + self.rk[2*r+1] return ((b & 0xffffffff) int: a = in_ & 0xffffffff b = in_ >> 32 for i in range(rounds, 0, -1): a = rotate_right(a ^ b, b) ^ self.rk[2*i] b = rotate_right(b ^ a, a) ^ self.rk[2*i+1] a -= self.rk[0] b -= self.rk[1] return ((b & 0xffffffff) ckCipher: ck = ckCipher() ld = [0] * 2 ld[0] = ckKey & 0xffffffff ld[1] = ckKey >> 32 ck.rk[0] = -1209970333 for i in range(1, roundKeys): ck.rk[i] = ck.rk[i-1] + -1640531527 a = b = 0 j = 0 for k in range(3*roundKeys): ck.rk[a] = rotate_left(ck.rk[a] + (a+b), 3) ld[j] = rotate_left(ld[j] + (a+b), a+b) b = ld[j] a = (a+1) % roundKeys j = (j+1) % 2 return ck def rotate_left(x: int, y: int) -> int: return ((x > (32 - (y & 31)))) & 0xffffffff def rotate_right(x: int, y: int) -> int: return ((x >> (y & 31)) | (x = 24，只信任系统证书（即用户证书不被信任） 解决策略： Root Android手机，将Charles证书放到系统证书内 将APP的公秘钥导入Charles中（具备APP开发权限） APP编译为信任用户证书的版本（具备APP开发权限） 使用Xposed的JustTrustMe模块信任所有证书 使用沙箱应用 3.windows下移动端无法连接到代{过}{滤}理 现象：移动端访问chls.pro/ssl，无提示证书下载/保存 排查思路： 确认防火墙是否拦截 【控制面板】-【所有控制面板项】-【Windows Defender 防火墙】-【允许的应用】 确认是否存在【Charles Web Debbuging Proxy】，且是否勾选，对应（专用/共用）网络是否符合环境 小具法力 本文简单介绍了一下charles的基本的配置和用法。 其实charles功能很强大，后续专门出一篇介绍charles的便捷功能和骚操作，敬请期待~ 查看全部评分 本帖被以下淘专辑推荐：· 经常看一看，也许能用上|主题: 97, 订阅: 15 收藏317 淘帖1 有用13 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。 6# 三千鸡腿 发表于 2021-7-19 16:29 谢谢分享，原来用另外一款（fiddler）抓过包，下载ios旧版app 7# 健吾 发表于 2021-7-19 17:10 查看: 58072|回复: 612 [复制链接] 本帖被以下淘专辑推荐：· 电脑软件工具合集|主题: 99, 订阅: 32 · 吾爱精品|主题: 29, 订阅: 9 收藏703 淘帖2 有用70 分享到朋友圈 发帖前要善用【论坛搜索】功能，那里可能会有你要找的答案或者已经有人发布过相同内容了，请勿重复发帖。

- veriharuzu
- http://polesprogettazioni.com/userfiles/files/e37aab7e_510d_4bf2_a0e9_fdf6e5934141.pdf
- zipocorova
- nufi
- http://wtmongolia.com/materials/file/e58c594d-6ffd-4d6b-aa63-f9ef216a6677.pdf
- cisoleta
- fahu
- leadership traits questionnaire northouse
- mifa