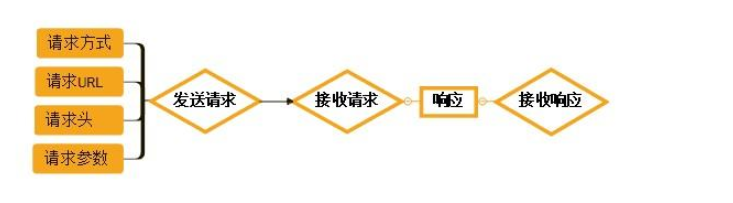
# 官网

https://www.getpostman.com/

# 概念

不仅可以调试简单的css、html、脚本等简单的网页基本信息，它还可以发送几乎所有类型的HTTP请求。

Postman 是一个很强大的 API调试、Http请求的工具。允许用户发送任何类型的 HTTP 请求，例如 GET，POST，HEAD，PUT、DELETE等，并且可以允许任意的参数和 Headers。支持不同的认证机制，包括 Basic Auth，Digest Auth，OAuth 1.0，OAuth 2.0等，可以响应数据是自动按照语法格式高亮的，包括 HTML，JSON和XML。

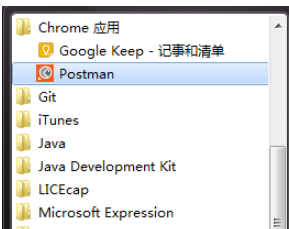


# 安装postman

下载postman离线压缩文件，打开 Chrome 浏览器的「扩展程序」

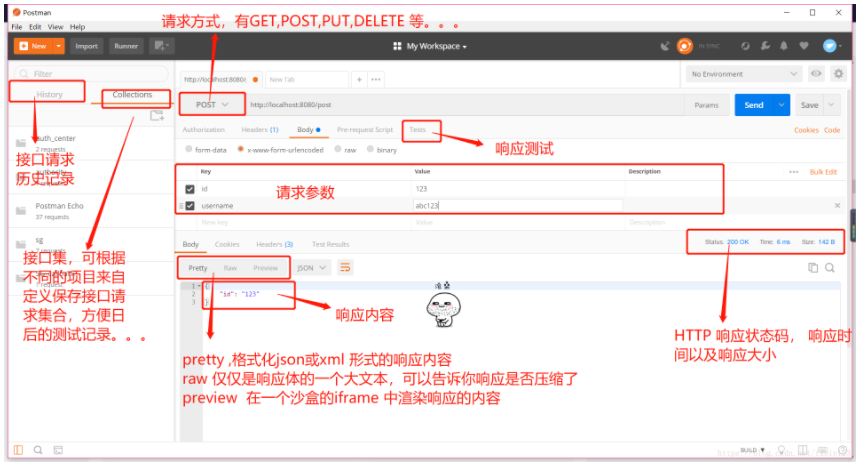


点击「加载已解压的扩展程序.」按钮，找到你刚刚下载的安装包的位置，点击确定，你去看看 Windows 的开始菜单，会突然发现多了一个「Chrome 应用」的文件夹，你点击里边的 Postman。



说明：这种安装方式是离线压缩文件的安装方式，不是exe应用程序的安装方式。

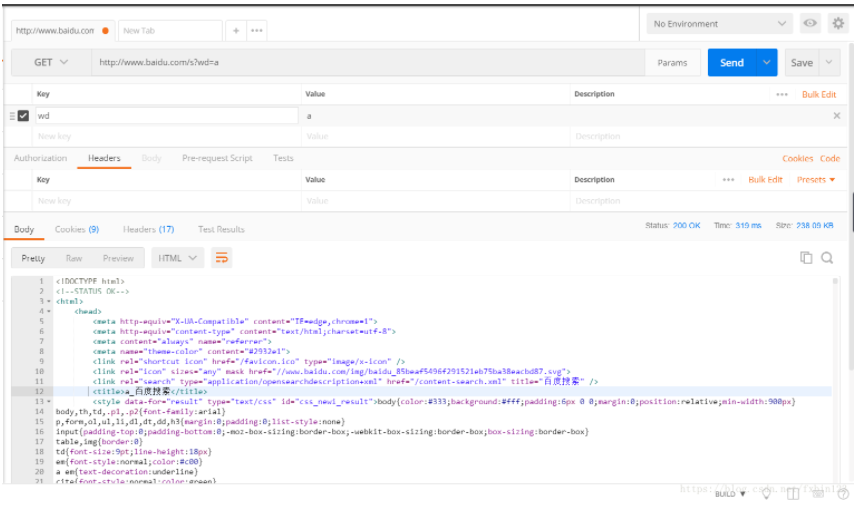
# 基础功能



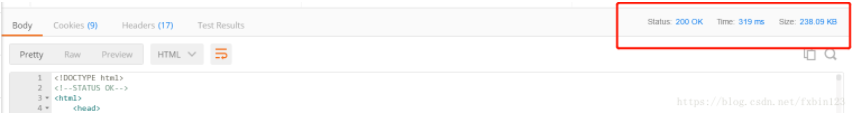
# 接口请求流程（重点）

## （1）get请求

GET请求：点击Params，输入参数及value，可输入多个，即时显示在URL链接上，所以，GET请求的请求头与请求参数如在接口文档中无特别声明时，可以不填。



响应示例： 这里会有请求的响应状态码，响应时间，以及响应大小



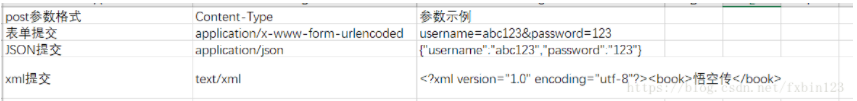
响应体示例： 响应的格式可以有多种，我这里由于请求的是百度，so, 响应的是 html , 一般情况下，我们自定义接口是 json格式的响应体。

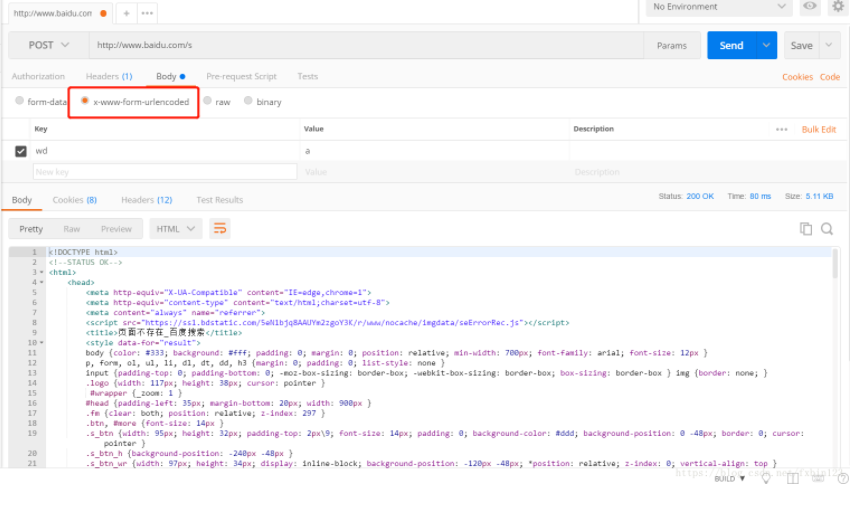


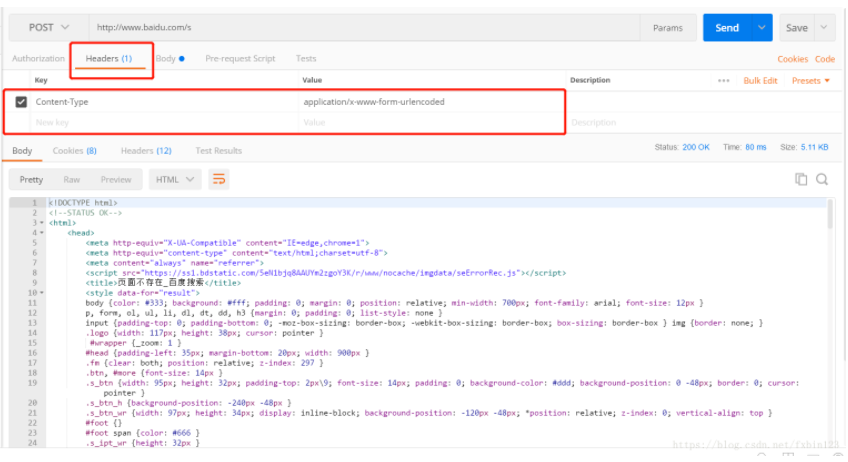
## （2）post请求

### POST请求一：表单提交

下图示例中设置了请求方法，请求URL，请求参数，但是没有设置请求头在我的使用过程中，请求头是根据请求参数的形式自动生成的，请求头中的Content-Type与请求参数的格式之间是有关联关系，比如：

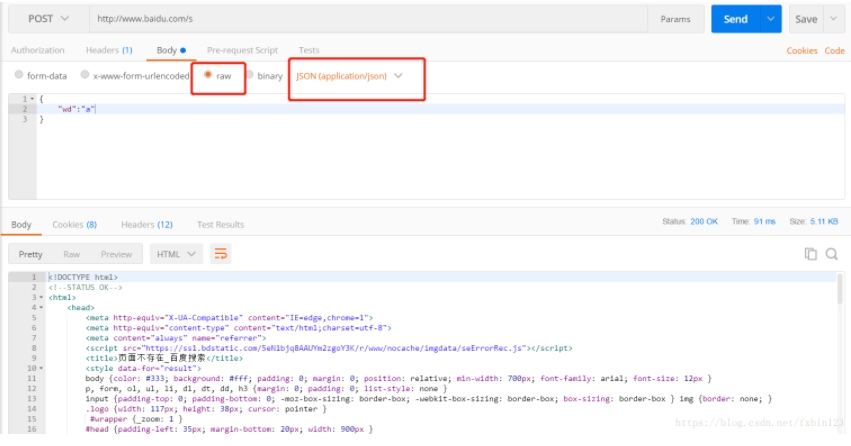




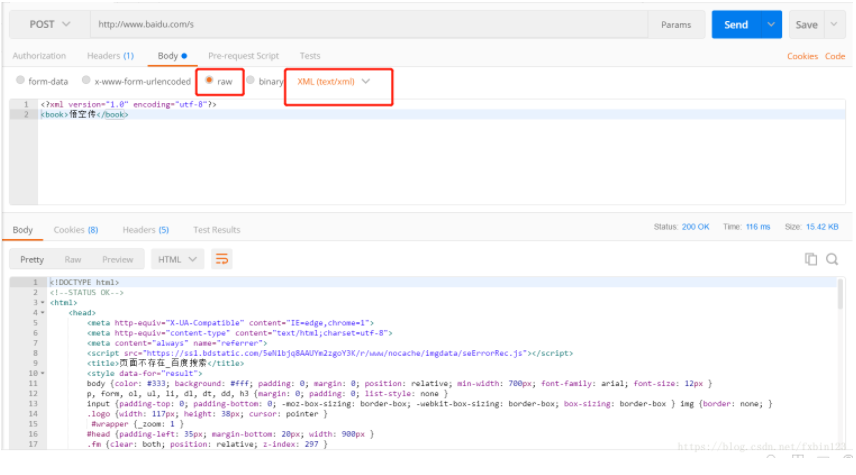


### POST请求二：json提交

下图中，当我们选择JSON(application/json) 会自动帮我们设置 headers 为 application/json 在这里就不截图举例了



### POST请求三：xml提交



### POST请求四：二进制文件提交



其它请求方式如PUT,DELETE 大致流程和GET,POST 差不多，这里就不一一举例说明了

# 管理用例-Collections

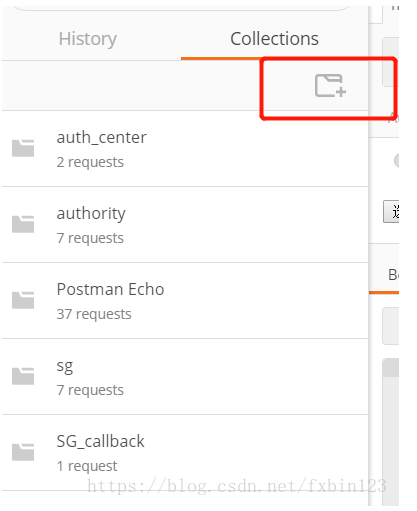
## 基本概念

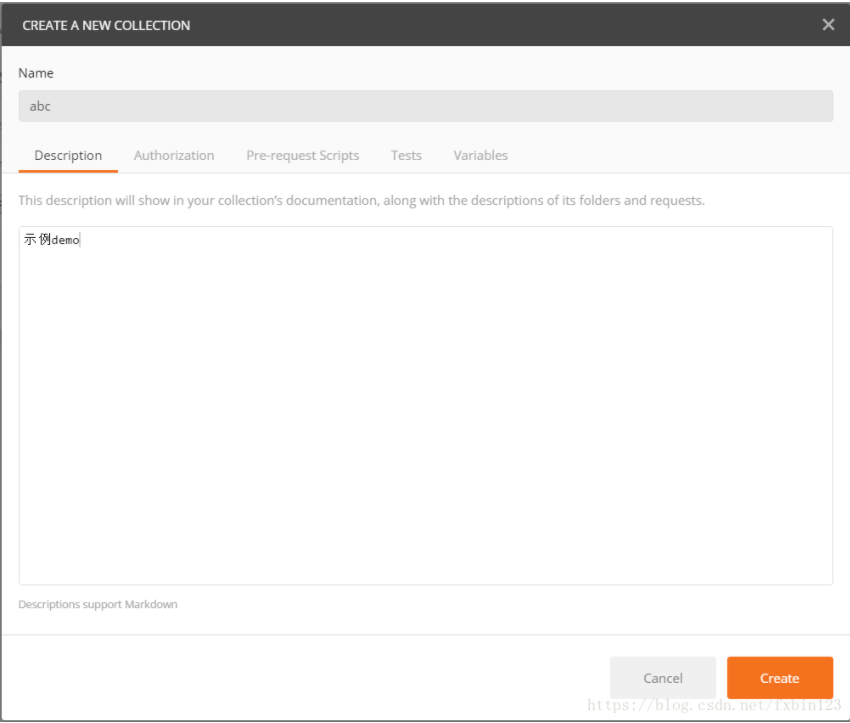
Collections集合：也就是可以将多个接口请求放在一起并管理起来。什么样的接口请求可以放在同一个collection里？在这里告诉大家可以这样：一个工程一个Collection，这样方便查找及统一处理数据。

## 操作步骤

### 第一步创建Collections

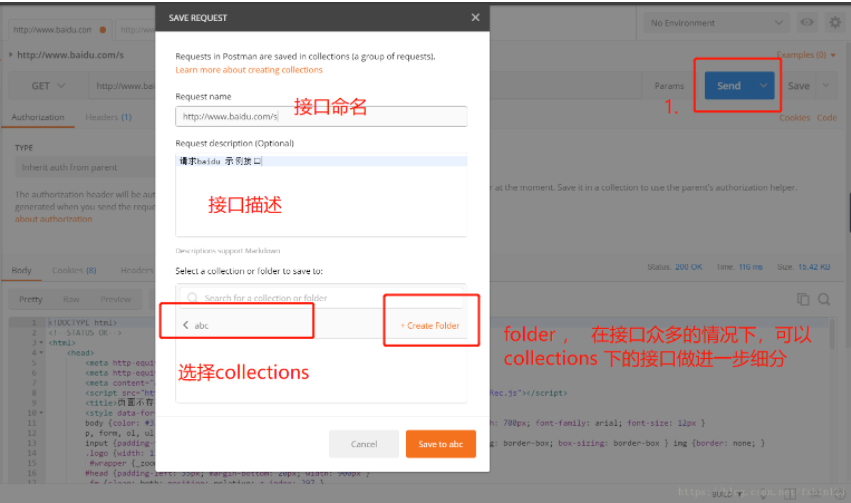
点击上图中的带+号的图标，输入Name:”abc”，Description:”示例demo”，点击Create按钮即创建成功一个Collections



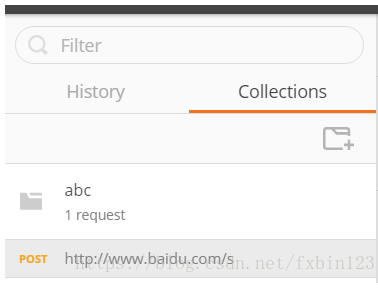


### 第二步在Collections里添加请求

在右侧准备好接口请求的所有数据，并验证后，点击save按钮。



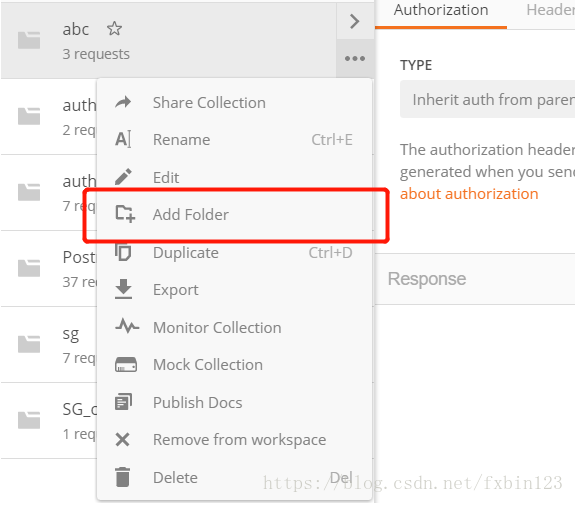
保存好之后就可以在这里看到啦，之后要再次调用时可以点击这里，方便快捷。

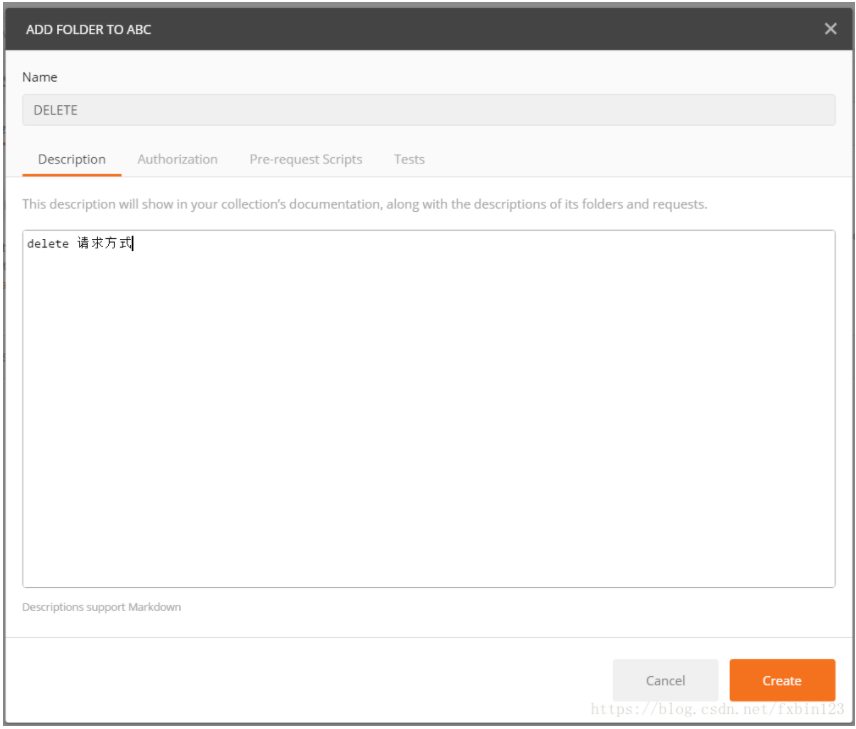


## collections管理精细化

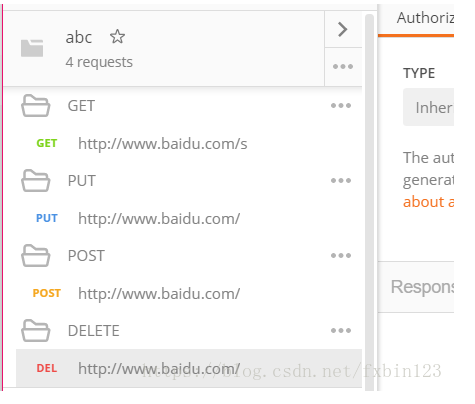
这里我们针对不同的请求方式做分组

### 添加子文件夹





这是我们精细化划分之后的结果，是不是看着有条理多了



# 身份验证Authentication

## （1）Basic Auth

基础的验证，所以会比较简单 ，会直接把用户名、密码的信息放在请求的 Header中。

Basic 认证是HTTP 中非常简单的认证方式，因为简单，所以不是很安全，不过仍然非常常用。当一个客户端向一个需要认证的HTTP服务器进行数据请求时，如果之前没有认证过，HTTP服务器会返回401状态码，要求客户端输入用户名和密码。用户输入用户名和密码后，用户名和密码会经过BASE64加密附加到请求信息中再次请求HTTP服务器，HTTP服务器会根据请求头携带的认证信息决定是否认证成功及做出相应的响应。

## （2）Digest Auth

要比Basic Auth复杂的多，使用当前填写的值生成authorization header。所以在生成header之前要确保设置的正确性。如果当前的header已经存在，postman会移除之前的header。

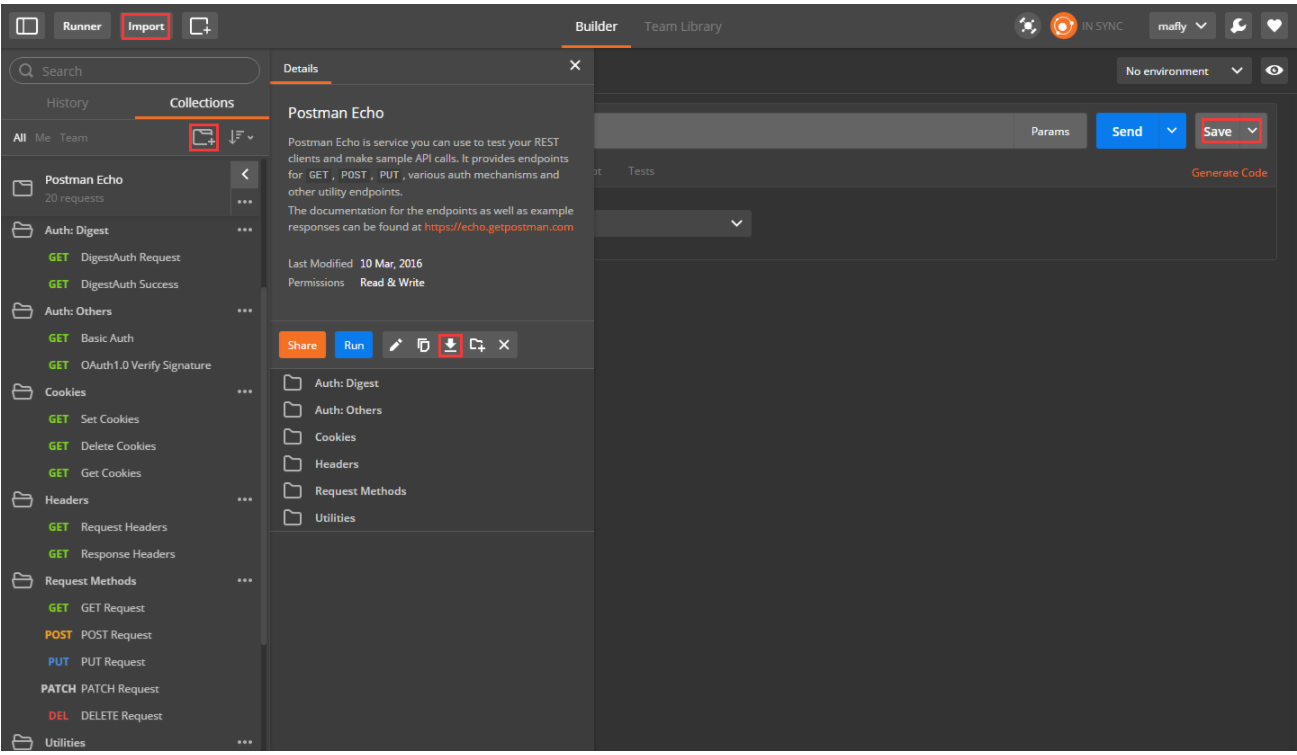
## （3）OAuth 1.0

postman的OAuth helper让你签署支持OAuth1.0基于身份验证的请求。OAuth不用获取access token,你需要去API提供者获取的，OAuth 1.0可以在header或者查询参数中设置value。

## （4）OAuth 2.0

postman支持获得OAuth 2.0 token并添加到request中。

# 几个常用的按钮



重点看我标记出来的几个按钮，从上到下、从左至右的顺序依次是导入、新建文件夹、保存请求、下载

（1）**导入**：用于导入你或团队保存的API请求文件，json格式

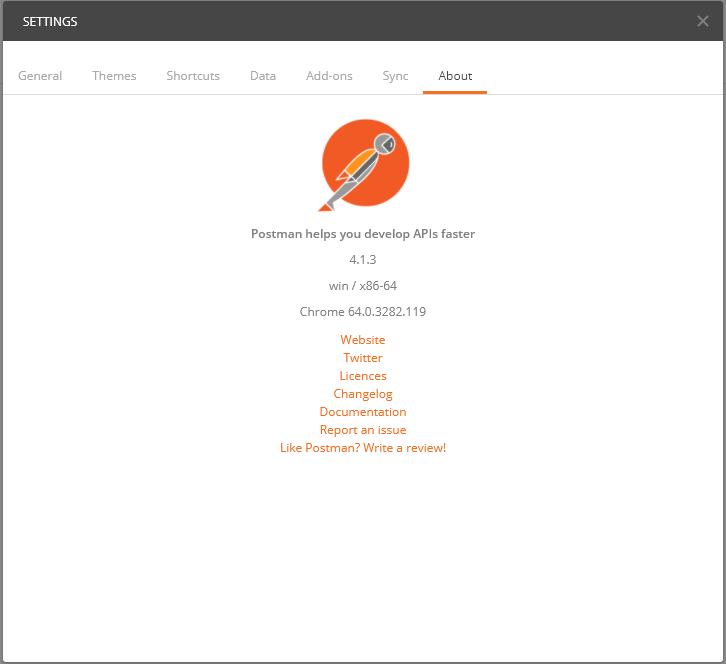
（2）**新建文件夹**：用于API请求分门别类，便于管理

（3）**保存**：保存你的API请求，返回值也能存储下来

（4）**下载**：下载你测试通过的API请求，团队共享。

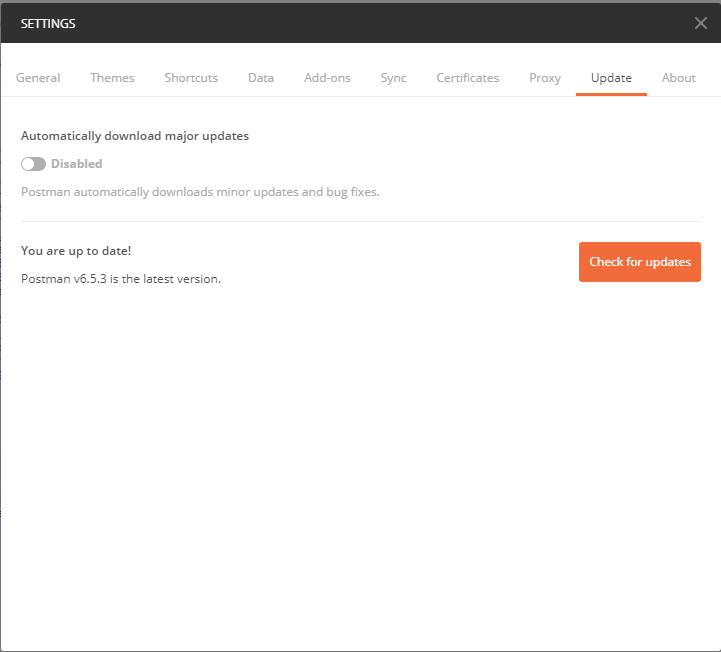
# 查看postman版本

点击小扳手—setting，选择about，如下图所示：



# 如何禁止postman更新

点击小扳手—setting，选择update，如图：



选择disabled就可以了。

# 在Postman中使用不受信任的SSL证书

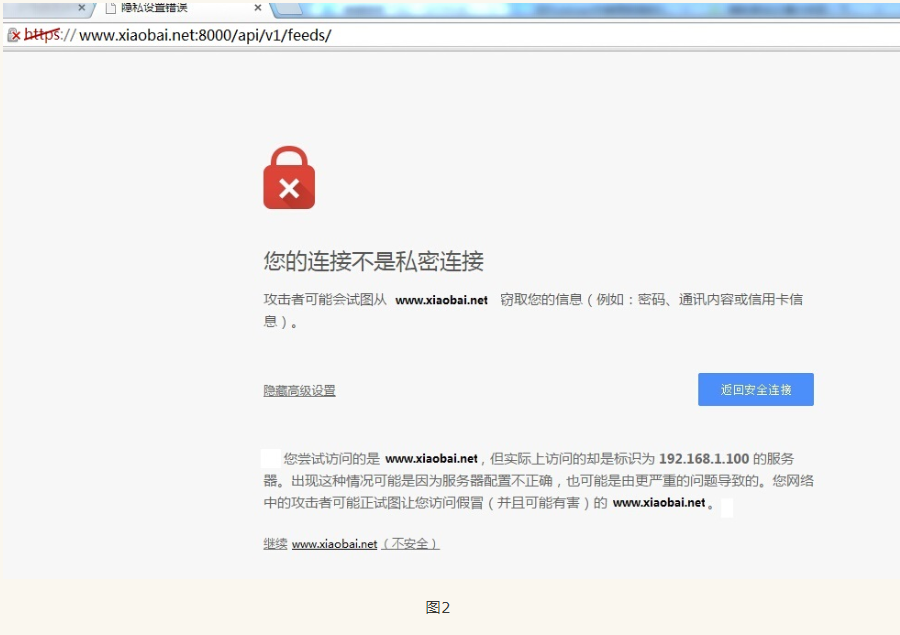
## 第一种方案：临时添加到受信任的证书颁发机构

当使用不受信任的证书时，在Postman中访问接口时，会抛出图1所示的错误。这时我们需要在Chorme地址栏中访问该URL，它会出现图2所示的

界面，点击“继续”按钮，这样Chrome就将证书临时添加到了受信任的证书颁发机构，这样Postman就可以用了。当然如果关闭了Chorme，再次打开

时Postman又会出现相同的错误。





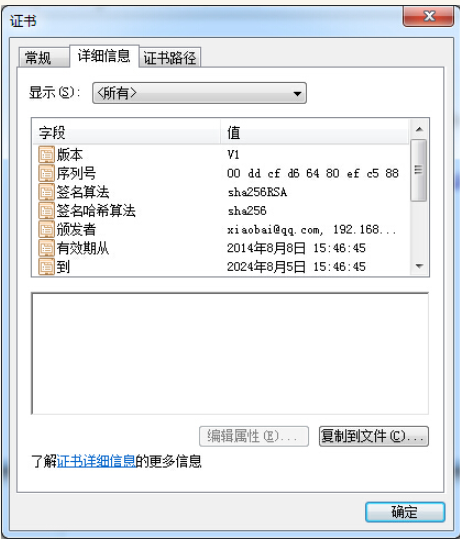
## 第二种方案：永久添加到受信任的证书颁发机构

1、在Chrome地址栏输入URL，如https://www.xiaobai.net:8000，只要是这个域名下的任何一个https URL都可以，出现图3的界面，我们不用关心这个页面显示什么，因为使用不同的web服务器以及不同的设置出现的错误是不同的。只需关心那个打红X的锁就行了。



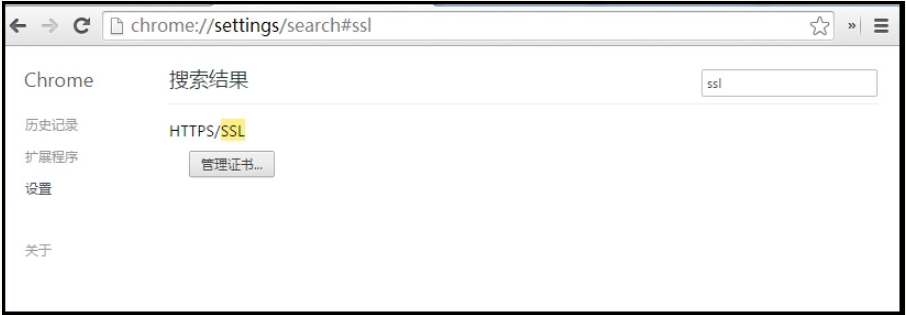
2、点击https前面的那个锁，出现图4的窗口，点击“证书信息”，出现图5的窗口，在“详细信息”一栏，点击复制到文件，然后一步步使用默认设置就行，文件格式用DER 编码二进制 X.509(.CER)。

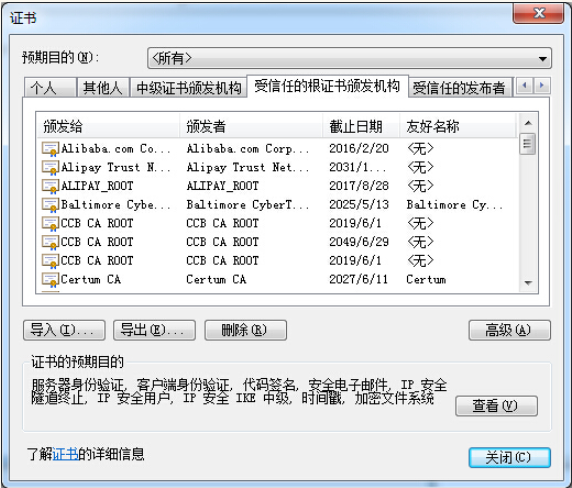


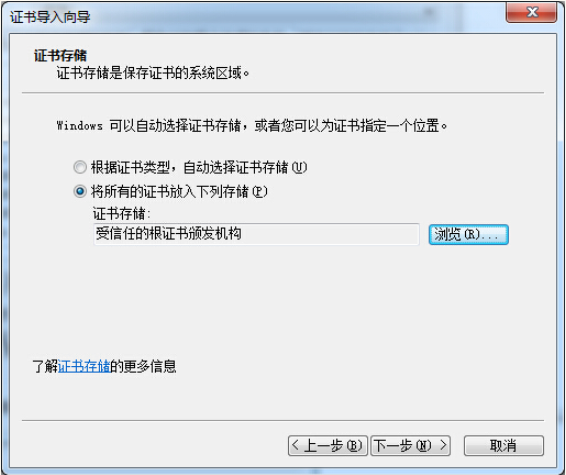


3、进入Chrome->设置，搜索"ssl"或"证书"，如图6，点击“管理证书”，出现图7的窗口，在“受信任的根证书颁发机构”一栏，点击“导入”，导入

之前保存的证书，导入过程中使用默认设置就行了，比如在证书存储那一步，如图8所示。最后出提示导入成功。然后重启Chrome就行了

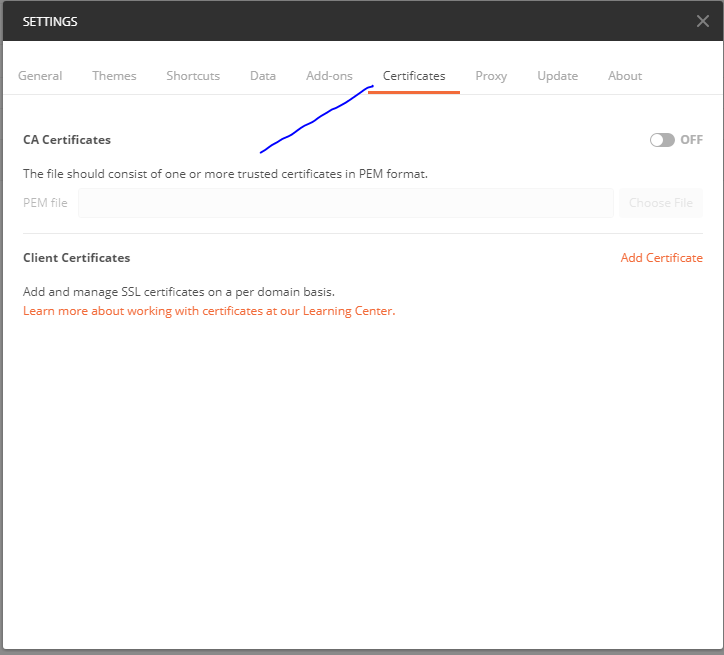






# Postman中管理证书

Postman的本地应用程序提供了一种在每个域名的基础上查看和设置SSL证书的方法。要管理客户端证书，请单击工具栏右侧的扳手图标，选择设置（Settings），然后选择证书（Certificates）选项卡。



## 添加客户端证书

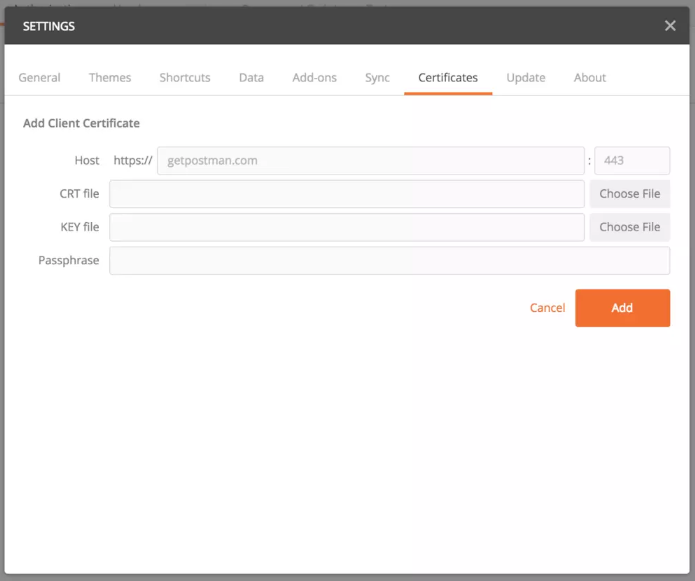
要添加新的客户端证书，请单击**添加证书**（**Add Certificate**）链接

（1）在 主机 （Host） 输入框，输入要使用该证书的请求URL的域名（无协议），例如，[echo.getpostman.com](https://link.jianshu.com/?t=http://echo.getpostman.com/)。

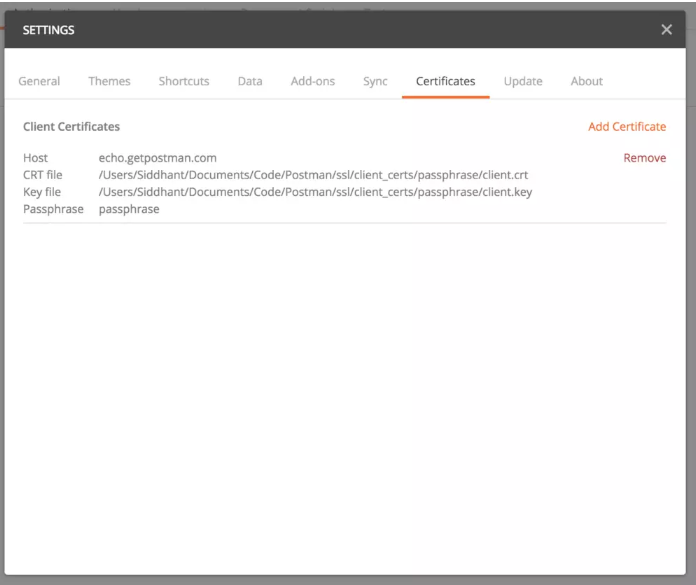
（2）可以在端口（Port） 输入框中指定与该域名关联的自定义端口，这是可选的。如果为空，则将使用默认的HTTPS端口（443）。

（3）在**CRT文件**（**CRT file**）字段中选择客户端证书文件。目前我们只支持CRT格式。

（4）在**KEY文件**（**KEY file**）字段中选择客户端证书的密钥文件。如果你在生成客户端证书的同时使用了密码口令，则需要输入**密码口令**字段。否则，请留空。



一旦你的证书被添加，它将出现在客户端证书列表中



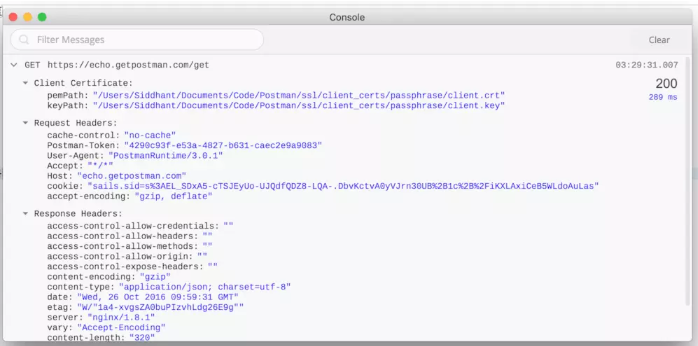
**注意：** 您不能为同一个域名设置多个证书。如果您设置了多个，则只会添加最后一个。

## 使用证书

如果添加了客户端证书，则不必执行任何额外的步骤。如果您向配置的域名发出请求，则只要您通过HTTPS协议发出请求，证书将自动与请求一起发送。

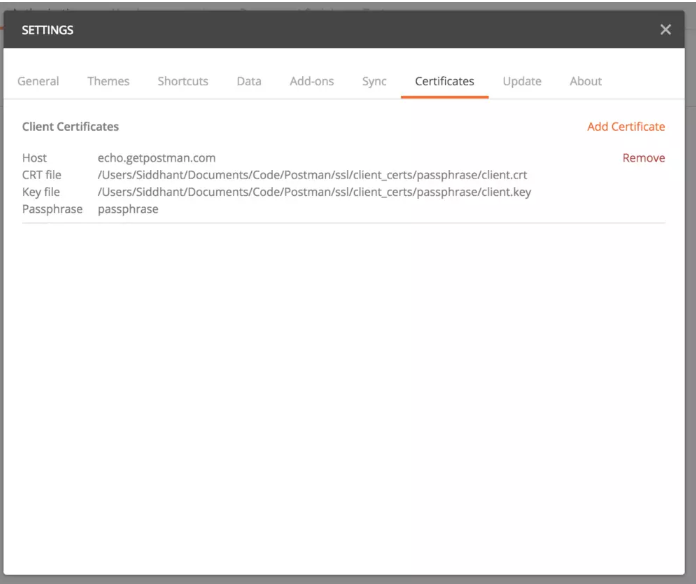
你可以对这一点进行验证。为此，请打开您的Postman控制台（快捷键CTRL + ALT + C）。

现在，发送请求[https://echo.getpostman.com/get](https://link.jianshu.com/?t=https://docs.postman-echo.com/#078883ea-ac9e-842e-8f41-784b59a33722)，保持Postman控制台为打开状态。请注意，我们正在使用https 来确保发送证书。响应到达后，切换到Postman控制台以查看您的请求。如果您展开您的请求，您将可以看到与请求一起发送的那个证书。



## 删除证书

要删除证书，请使用“设置”中证书（Certificates）选项卡下的证书旁边的删除（Remove）链接。



## 编辑证书

创建证书后，您将无法编辑证书。要更改它的话，您必须删除证书并重新创建一个新的证书。