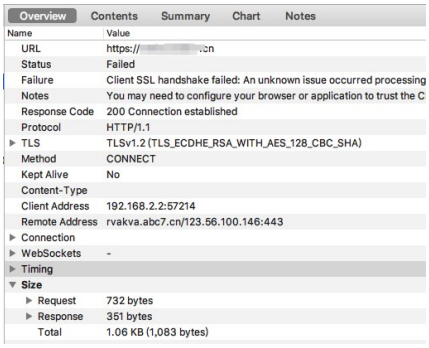
今天也要努力呀

Life is more than struggle !

【转载】http proxy原理

最近使用Charles抓https包时，发现get和post方式的请求都能抓到，但是method为connect的就是抓不到。而且提示如下：

You may need to configure your browser or application to trust the Charles Root Certificate. See SSL Proxying in the Help menu.



于是搜索connect方式与其他方式区别，才发现问题。以下内容系转载。

以下内容系转载

connect方法

http 1.1定义了8种方法，connect为其中之一，HTTP/1.1协议中预留给能够将连接改为管道方式的代理服务器。通常用于SSL加密服务器的链接(经由非加密的HTTP代理服务器)。

并非所有的http隧道支持connect方法，Http隧道分为两种：

1 不使用CONNECT的隧道

不使用CONNECT的隧道，实现了数据包的重组和转发。在Proxy收到来自客户端的Http请求之后，会重新创建Request请求，并发送到目标服务器，。当目标服务器返回Response给Proxy之后，Proxy会对Response进行解析，然后重新组装Response，发送给客户端。所以，在不使用CONNECT方式建立的隧道，Proxy有机会对客户端与目标服务器之间的通信数据进行窥探，而且有机会对数据进行串改。

2 使用CONNECT的隧道

而对于使用CONNECT的隧道则不同。当客户端向Proxy发起Http CONNECT Method的时候，就是告诉Proxy，先在Proxy和目标服务器之间先建立起连接，在这个连接建立起来之后，目标服务器会返回一个回复给Proxy，Proxy将这个回复转发给客户端，这个Response是Proxy跟目标服务器连接建立的状态回复，而不是请求数据的Response。在此之后，客户端跟目标服务器的所有通信都将使用之前建立起来的建立。这种情况下的Http隧道，Proxy仅仅实现转发，而不会关心转发的数据。这也是为什么在使用Proxy的时候，Https请求必须首先使用Http CONNECT建立隧道。因为Https的数据都是经过加密的，Proxy是无法对Https的数据进行解密的，所以只能使用CONNECT，仅仅对通信数据进行转发。

注意，proxy代理的是客户端发起的TCP连接，以下是wiki的解释

the client, using the "CONNECT" HTTP method, asks an HTTP Proxy server to forward the TCP connection to the desired destination. The server then proceeds to make the connection on behalf of the client. Once the connection has been established by the server, the Proxy server continues to proxy the TCP stream to and from the client. Note that only the initial connection request is HTTP - after that, the server simply proxies the established TCP connection.This mechanism is how a client behind an HTTP proxy can access websites using SSL (i.e. HTTPS).

http://en.wikipedia.org/wiki/HTTP_tunnel

与proxy相关字段

X-Forwarded-For(XFF)是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段；Squid 缓存代理服务器的开发人员最早引入了这一HTTP头字段，如果没有XFF或者另外一种相似的技术，所有通过代理服务器的连接只会显示代理服务器的IP地址(而非连接发起的原始IP地址)，这样的代理服务器实际上充当了匿名服务提供者的角色，如果连接的原始IP地址不可得，恶意访问的检测与预防的难度将大大增加。

X-Forwarded-Host和**X-Forwarded-Proto**分别记录客户端最原始的主机和协议。

Proxy-Authorization：连接到proxy的身份验证信息

Proxy-connection:它不是标准协议的一部分，标准协议中已经存在一种机制可以完成此协议头的功能，这就是Connection头域，与Proxy-Connection头相比，Connection协议头几乎提供了相同的功能，除了错误部分。而且，Connection协议头可用于任意连接之间，包括HTTP服务器，代理，客户端，而不是像Proxy-Connection一样，只能用于代理服务器和客户端之间。

http 1.1其余7种方法

OPTIONS：这个方法可使服务器传回该资源所支持的所有HTTP请求方法。用'*'来代替资源名称，向Web服务器发送OPTIONS请求，可以测试服务器功能是否正常运作。

HEAD：与GET方法一样，都是向服务器发出指定资源的请求。只不过服务器将不传回资源的本文部份。它的好处在于，使用这个方法可以在不必传输全部内容的情况下，

就可以获取其中"关于该资源的信息"(元信息或称元数据)。

GET：向指定的资源发出"显示"请求。使用GET方法应该只用在读取数据，而不应当被用于产生"副作用"的操作中，例如在Web Application中，其中一个原因是GET可能会被

网络蜘蛛等随意访问。

POST：向指定资源提交数据，请求服务器进行处理(例如提交表单或者上传文件)。数据被包含在请求本文中。这个请求可能会创建新的资源或修改现有资源，或二者皆有。

PUT：向指定资源位置上传其最新内容。

DELETE：请求服务器删除Request-URI所标识的资源。

TRACE：回显服务器收到的请求，主要用于测试或诊断。

http://zh.wikipedia.org/zh-cn/%E8%B6%85%E6%96%87%E6%9C%AC%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE

原文地址：http://blog.itpub.net/15480802/viewspace-1340982/

分类：接口测试/抓包

好文要顶 关注我 收藏该文

youreyebows
粉丝 - 2 关注 - 3

+加关注

0 推荐 0 反对

« 上一篇：Mac使用笔记大全

» 下一篇：Charles抓https请求详细步骤

posted @ 2018-07-31 17:03 youreyebows 阅读(3570) 评论(0) 编辑 收藏 举报

刷新评论 刷新页面 返回顶部

登录后才能查看或发表评论，立即 登录 或者 逛逛 博客园首页

编辑推荐：

· 帝团队后的日常思考(十一)
· 记一次使用 gdb 诊断 gc 问题全过程
· 深度剖析 Linux 伙伴系统的设计与实现
· SQLSERVER 的四个事务隔离级别到底怎么理解？
· 记一次线上 FGC 问题排查

阅读排行：

· 帝团队后的日常思考(十一)
· 朋友圈那串神秘字符背后的开源项目「GitHub 热点速览」
· chatGPT 桌面版安装教程
· C#实现聊天消息渲染、图文混排(支持Windows、Linux)
· .Net6 微服务之Polly入门看这篇就够了

< 2023年2月 >

日	一	二	三	四	五	六
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

搜索

找找看

随笔分类

Jmeter(4)
Monkey(2)
Python(7)
Selenium(3)
Spring Boot(1)
安全性测试(1)
服务器(3)
计算机网络(2)
接口测试/抓包(3)
数据库(3)

随笔档案

2022年6月(3)
2022年4月(7)
2021年1月(1)
2020年12月(1)
2020年11月(1)
2020年3月(1)
2019年11月(2)
2019年8月(1)
2019年6月(1)
2019年4月(2)
2018年9月(1)
2018年7月(2)
2018年4月(1)
2018年3月(2)
2017年12月(1)
更多

阅读排行榜

1. 解决删除镜像时image is referenced in multiple repositories(19257)
2. Java-Selenium，获取下拉框中的每个选项的值，并随机选择某个选项(9614)
3. Spring Boot-右键maven build成功但是直接运行main方法出错的解决方案(6547)
4. Jmeter csv文件进行参数化的两种方法(3843)
5. 【转载】http proxy原理(3570)

评论排行榜

1. Java-Selenium，获取下拉框中的每个选项的值，并随机选择某个选项(5)
2. Python 同一文件中，有unittest不执行"if __name__ == '__main__'"，不生成HTMLTestRunner测试报告的解决方案(1)