i春秋Web渗透测试工程师（初级）学习笔记（第三章）

原创

draper-crypto 于 2021-10-05 23:28:19 发布 72 收藏

文章标签： web 渗透测试 网络协议 http https

by draper-crypto

本文链接：https://blog.csdn.net/Suprman88/article/details/120617716

往期博文：

i春秋Web渗透测试工程师（初级）学习笔记（第一章）

i春秋Web渗透测试工程师（初级）学习笔记（第二章）

第三章:HTTP协议

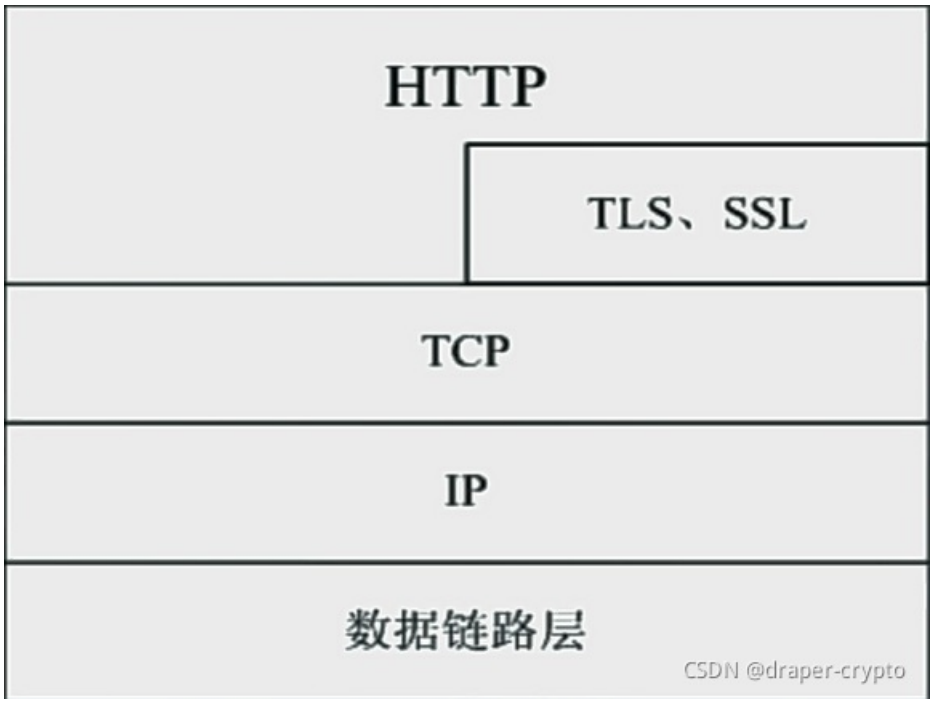
3.1 HTTP的基本概念

HTTP协议(超文本传输协议HyperText Transfer Protocol)，它是基于TCP协议的应用层传输协议，简单来说就是客户端和服务端进行数据传输的一种规则。它是无状态的协议，对于事务处理没有记忆能力，支持客户/服务器模式（C/S）端。

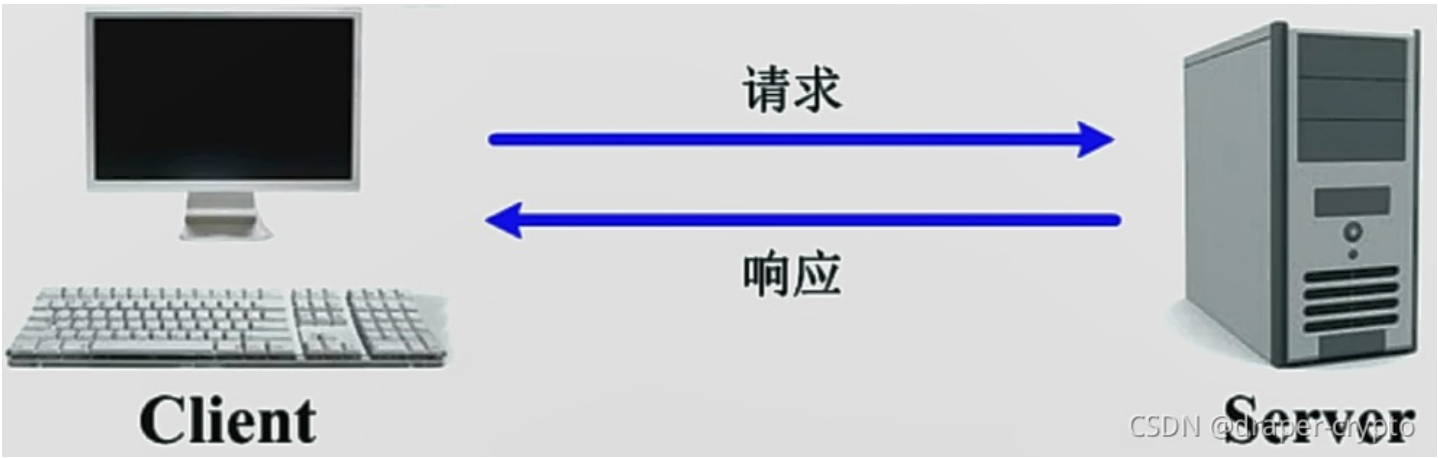
> 格式:http://host[":"port][abs_path]

3.2 TCP/IP中的位置

是一个应用层协议，它在协议栈中在TCP之上的，它是处于TCP、TLS、SSL之上的（PS:若处于TLS、SSL之上则是HTTPS，HTTP和HTTPS是完全不同的，HTTP的端口是80，而HTTPS的端口则是443）下图中HTTP块涵盖了**两层**。

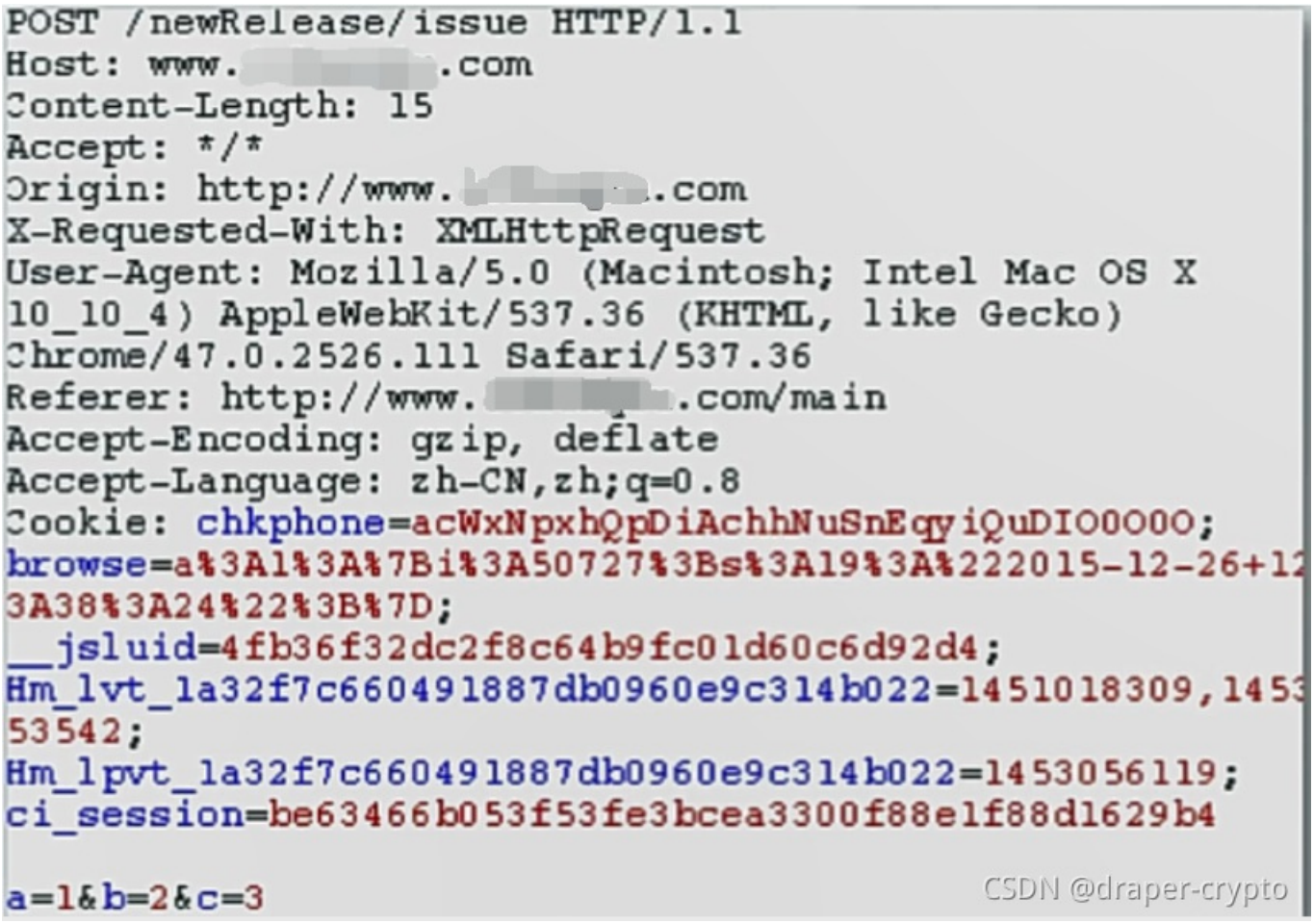


3.3 HTTP的请求和响应



3.3.1 请求

引用原视频中的抓包图片：



报文分析：

（1）HTTP请求状态行：状态行由三部分组成，包括方法符POST，资源路径（URI），HTTP版本号

```
GET /newRelease/issue HTTP/1.1
```

（2）访问位置：

```
Host:www.xxxxxx.com
```

（3）长度：

```
Content-Length:15
```

（4）浏览器发送的请求头，用于表示想要的资源类型：

```
objectivecAccept:*/*
```

（5）表示入口段，最初从哪个网址访问过来的就会列在后面：

```
Origin：http://www.xxxxxx.com
```

（6）客户自己的信息，包含系统版本、名称，浏览器的版本、名称，可以没有：

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X10_10_ 4)
AppleWebkit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36
```

（7）接受请求的网址，并回会给你包的网址：

```
Referer:http://www.xxxxxx.com/main
```

（8）规定了服务器接受的编码格式：

```
Accep-E ncoding: gzip, deflate
```

（9）使用语言，字体大小：

```
Accept- Language: zh-CN,zh;q=0.8
```

> **请求方法：**
> GET： 请求获URI所标识的资源
> POST： 在URI所标识的资源后附加新的数据
> HEAD：请求获取由URI所标识的资源的响应消息报头
> PUT： 请求服务器存储或修改一个资源，并用URI作为其标识
> DELETE：请求服务器删除URI所标识的资源
> TRACE： 请求服务器回送收到的请求信息，主要用于测试或诊断
> CONNECT： 保留将来使用
> OPTIONS： 请求查询服务器的性能，或者查询与资源相关的选项和需求

3.3.2 响应

引用原视频中的抓包图片：

（1）HTTP响应状态行： 状态行由三部分组成，包括HTTP协议的版本，状态码，状态码的文本描述。

```
HTTP/1.1 200 OK
```

（2）时间：

```
Date: Sun, 17 Jan 2016 18:57:24 GMT
```

（3）Content-Type和前面的objectivecAccept类似，charset是编码

```
Content-Type: text/html ;charset=UTF-8
```

（4）长度：

```
Content- Length: 71059
```

（5）保持连接：

```
Connection: keep-alive
```

> **HTTP响应状态码 状态代码有三位数字组成：**
> 1开头：指示信息 - 表示请求已接收，继续处理中
> 2开头：成功 -表示请求已被成功接收、理解、处理
> 3开头：重定向 - 要完成请求必须进行更进一步的操作
> 4开头：客户端错误 -用户请求时有语法错误或请求无法实现
> 5开头：服务器端错误 - 服务器未能实现**合法的**请求

> **常见状态代码如下：**
> 200：OK - 客户端请求成功
> 400：客户端请求有语法错误，不能被服务器所理解
> 401：请求未经授权，这个状态代码必须和Authenticate报头域一起使用
> 403：服务器收到请求，但是拒绝提供服务 ，比如权限问题
> 404：Not Found - 请求资源不存在，比如输入了错误的URL
> 500：服务器发生不可预期的错误
> 503：服务器当前不能处理客户端的请求，一段时间后,可能恢复正常

3.4 HTTP的报头

HTTP报头分为4类：
普通报头、请求报头、响应报头、实体报头

3.5 抓包工具

有chrome、firefox、wireshark、科来等