目录

1：通信协议 1

2：TCP/IP协议 2

3：HTTP协议 4

4：cookie的概念 5

5：cookie的特点 6

6：cookie的使用 7

应用： 8

7：cookie的封装 8

8：购物车的应用 9

9：XSS的攻击 9

应用： 10

综合应用： 10

## Cookie

## 1：通信协议

定义：通信协议是指双方实体完成通信或服务所必须遵循的规则和约定。协议定义了数据单元使用的格式，信息单元应该包含的信息与含义，连接方式，信息发送和接收的时序，从而确保网络中数据顺利地传送到确定的地方。

总结一句话：交流的规则。比如：汉语、英语、德语、日语等。

在计算机通信中，通信协议用于实现计算机与网络连接之间的标准，网络如果没有统一的通信协议，电脑之间的信息传递就无法识别。 通信协议是指通信各方事前约定的通信规则，可以简单地理解为各计算机之间进行相互会话所使用的共同语言。两台计算机在进行通信时，必须使用的通信协议。

常见的协议有：TCP/IP协议、HTTP协议、FTP协议等等。

FTP协议：File Transfer Protocol（文件传输协议），用于Internet上控制文件的双向传输。"下载"文件就是从远程主机拷贝文件至自己的计算机上；"上传"文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言来说，用户可通过客户机程序向（从）远程主机上传（下载）文件。

## 2：TCP/IP协议

Transmission Control Protocol/Internet Protocol的简写，中文名为传输控制协议/因特网互联协议，又名网络通讯协议，是Internet最基本的协议、Internet国际互联网络的基础，由网络层的IP协议和传输层的TCP协议组成。TCP/IP 定义了电子设备如何连入因特网，以及数据如何在它们之间传输的标准。通俗而言：TCP负责发现传输的问题，一有问题就发出信号，要求重新传输，直到所有数据安全正确地传输到目的地。而IP是给因特网的每一台联网设备规定一个地址。

IP地址 ipV4（0-255.0-255.0-255.0-255） 192.168.1.111 ipV6(zzzz:1111:2121:!212:1212:1212)

（url）<http://www.baidu.com> ->DNS(协议)把url转为ip地址

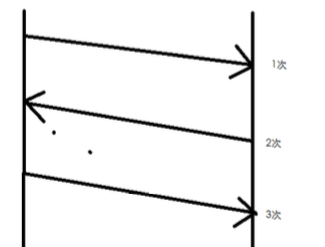
**UDP协议**：User Datagram Protocol的简称， 中文名是用户数据报协议。在网络中它与TCP协议一样用于处理数据包，是一种无连接的协议。

**TCP协议和UDP协议的区别：**

如果TCP比作是打电话,那么UDP就是在发短信。

**TCP面向连接的协议(通信之前必须先建立连接)**，于是,TCP相对可靠,它建立连接的过程称为3次握手。

第一个特点：**三次握手,建立连接。**



第二个特点：**所有的消息,需要对方确认送达。**

"土豆,土豆,我是茄子,收到请回答"

"茄子,茄子,我是土豆,收到消息"

**当消息发送失败,则对当前消息开始进行重复发送,直至收到回应为止。**

"茄子,茄子,我是土豆,我被人油炸了,我改名叫薯片,收到请回答"

............

"茄子,茄子,我是土豆,我被人油炸了,我改名叫薯片,收到请回答,第2遍"

............

"茄子,茄子,我是土豆,我被人油炸了,我改名叫薯片,收到请回答,第3遍"

............

"薯片,薯片,我收到消息"

**因此可以确保数据的准确送达。**

举例:

局域网游戏,往往都有这样的特点,当多人联机对战时,若有一个人掉线 其他所有玩家进入读秒状态,那么说明玩家和玩家之间采用了TCP协议。 因为对于游戏来讲,它不允许丢失任何数据,不然有可能出现两边不一致的情况: 我这边画面一刀把你砍死了,你那边画面却吃了个大血瓶抗住了。。。。。

**UDP面向数据报的协议 (不可靠的协议)：**无需建立连接 发送消息也无需对方确认 无法保证数据的发送顺序,以及准确率。

数据的发送顺序是 a.........b.........c...........d 由于网路延迟的原因,对方收到数据的顺序有可能是b...........d..........a。

UDP通常用于视频、语音等通信(丢掉了一帧画面是无所谓的)。

## 3：HTTP协议

超文本传输协议（HTTP，HyperText Transfer Protocol）是互联网上应用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。该协议用于从WWW服务器传输超文本到本地浏览器的传输协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。

HTTP协议是一个无状态的通信协议，一旦数据交换完毕，客户端与服务器端的连接就会关闭，再次交换数据需要建立新的连接。它基于TCP协议的一种高级协议，用于客户端和服务器直接的通信。http 默认端口号 80 https（secure）协议 默认端口号443

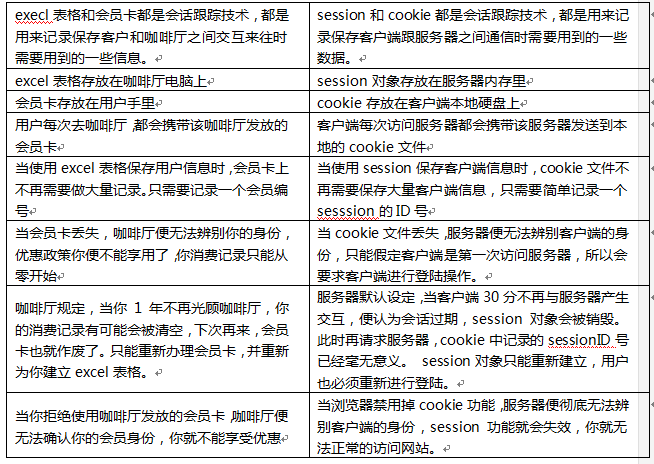
## 4：cookie的概念

指某些网站为了辨别用户身份，进行session（会话）跟踪而存储在用户本地终端上的数据（通常经过加密）。以文本形式存在。

谷歌浏览器存储地址： C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\文件夹下的Cookies文件。

/ 根目录 linux

禁用cookie：改变浏览器的cookie设置。如果浏览器完全禁止cookie功能的话，大多数网站的基本功能无法正常使用。



## 5：cookie的特点

1：chrome和safari没有对cookie的个数做限制，一般浏览器限制同一域名数量为50个。

2：cookie文件的总大小一般为4KB（同一个域名）。

3：只能使用文本文件。

4：读取有域名限制。 域名 [www.baidu.com](http://www.baidu.com) [www.taobao.com](http://www.taobao.com) so.com

不可跨域读取,只能由来自 写入cookie的 同一域名 的网页可进行读取。 简单的讲就是,谁写的cookie,谁才有权利读取 (身份牌是我发你的,当然只有我能读取,你媳妇儿的手机自动连接了邻居老王家的wifi,你知道这意味着什么吗?)

5：时效限制。

每个cookie都有时效,最短的有效期是,会话级别:就是当浏览器关闭,那么cookie立即销毁。

## 6：cookie的使用

添加cookie：document.cookie = “key=value”; // 一次写入一个键值对

读取cookie：document.cookie;

修改cookie：document.cookie = “key=value”; // 修改名为key的cookie值

删除cookie：将cookie值覆盖为空，并将失效时间设置为过去的时间。

失效时间：expires

var oDate = new Date();

oDate.setDate(oDate.getDate() + iDay);

设置失效时间：document.cookie = “key=value;expires=”+ oDate;

设置域名：domain

设置域名：document.cookie = “key=value;domain=baidu.com“;

注：必须在绑定域名的服务器才可以设置域名，上不同服务器之间的cookie文件不能共享。

设置路径：path

设置路径： document.cookie = “key=value;path=/“;

注：在同一路径下的网页可以共享cookie，路径不同时，不可以访问。

注：如果有中文内容，需要用encodeURIComponent(‘xxxx’)进行编码，再使用decodeURIComponent(‘xxxx’)进行解码，解决中文乱码的问题。

## 应用：

1：一周内免登录。

2：商品浏览记录。

## 7：cookie的封装

增加/修改cookie函数：

function setCookie(name,value,iDay){

var newDate = new Date();

newDate.setDate(newDate.getDate()+iDay);

document.cookie=name+"="+value+";expires="+newDate;

}

setCookie("user","andy",7);

获取cookie函数：

function getCookie(name){

var arr = document.cookie().split("; ");

for(var i =0; i<arr.length; i++){

var arr2 = arr[i].split("=");

if(arr2[0] == name){

return arr2[1];

}

}

}

删除cookie函数：

function removeCookie(name){

setCookie(name,1,-1);

}

removeCookie("user");

## 8：购物车的应用

## 9：XSS的攻击

跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆，故将跨站脚本攻击缩写为XSS。恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的。

跨站脚本攻击的核心在于脚本的成功注入，并二次展示。通常服务器端都会对文本内容进行安全性的过滤。

## 应用：

1：照片墙的记录。

2：购物车的多条记录保存。

## 综合应用：

1：掌握cookie的安全策略。

2：掌握cookie的封装。

3：掌握cookie与json的配合。