

# Web 系统测试

## 4.2 Web安全测试—HTTP请求流程

# 目 录

---

- HTTP协议介绍
- HTTP请求和响应
- 工具的使用

➤当我们访问一个网址的时候，这中间发生了什么

- 输入网址
- 浏览器查找域名的IP地址
- 浏览器给Web服务器发送一个HTTP请求
- 服务器处理请求
- 服务器发回一个HTTP响应
- 浏览器渲染显示HTML



## ➤什么是HTTP?

- 是一种按照URL指示，将超文本文档从一台主机(Web服务器)传输到另一台主机(浏览器)的应用层协议，以实现超链接的功能
- URL
- 超文本

➤ HTTP协议是一种无状态的协议

➤ 什么叫无状态

● Web浏览器与Web服务器之间不需要建立持久的连接



## ➤ HTTP请求

### ● 请求行

- 请求方法、URL、协议版本等请求头（消息报头）

### ● 请求头

- 由一个头域名、冒号和值域组成

### ● 请求正文

- 也叫请求数据，在使用POST请求提交表单数据的时候，这些表单数据就会被放在HTTP请求的请求正文中，以加密的形式向服务器传输

## ▼ Request Headers

view parsed

GET / HTTP/1.1

请求行

Host: www.itxdl.cn

Connection: keep-alive

请求头

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_12\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.86 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.8,en;q=0.6

Cookie: UM\_distinctid=15cae6aef3f2a-06f8414ac81c33

## ➤主要请求方法GET 和 POST

- GET方式：向特定资源发出请求，主要用于获取网络资源
- POST方式：用于向指定资源提交数据进行处理请求（如提交表单或者上传文件）。数据被包含在请求体中。POST请求可能会导致新的资源创建或已有资源的修改
- HEAD 向服务器索要GET请求相一致的响应，只不过响应体将不会被返回。这一方法可以在不必传输整个响应内容的情况下，就可以获取包含在响应信息头中的元信息



- 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** 请求服务器回送收到的请求信息，主要用于测试或诊断
- CONNECT** HTTP1.1协议中预留给能够将连接改为管道方式的代理服务器
- OPTIONS** 返回服务器针对特定资源所支持的HTTP请求方法。也可以利用Web服务器发送测试的请求来测试服务器的功能性

## ➤ 响应分为三部分

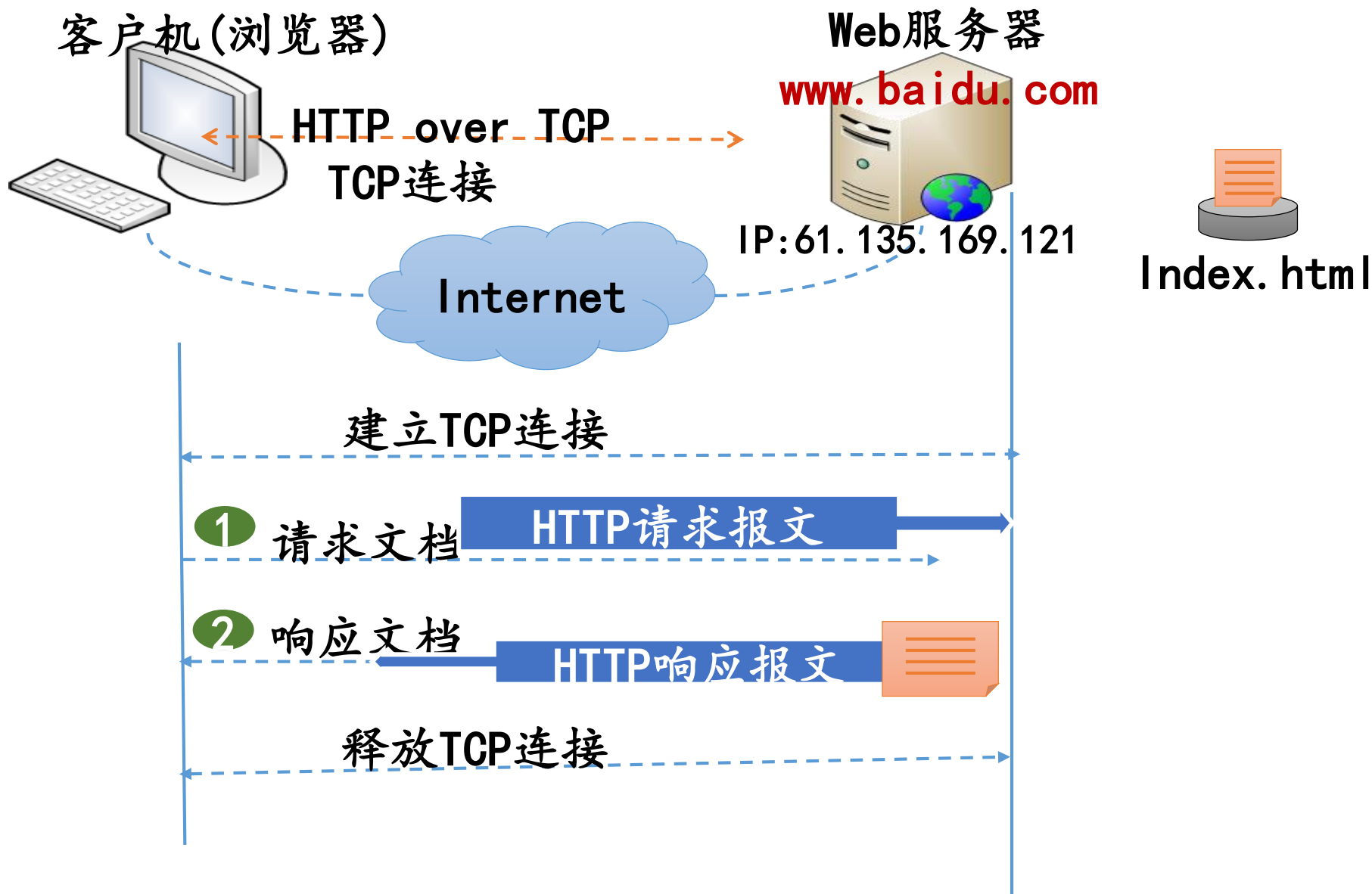
### ● 响应行

- 协议和状态码

### ● 状态码

1. 200: 客户端请求成功, 是最常见的状态
2. 302: 重定向
3. 404: 请求资源不存在, 是常见的状态
4. 400: 客户端请求有语法错误, 不能被服务器所理解
5. 401: 请求未经授权
6. 403: 服务器收到请求, 但是拒绝提供服务
7. 500: 服务器内部错误
8. 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

# HTTP工作原理



- 响应头
- 响应正文
  - 服务器向客户端发送的HTML数据

# HTTP报文结构--首部字段或消息头

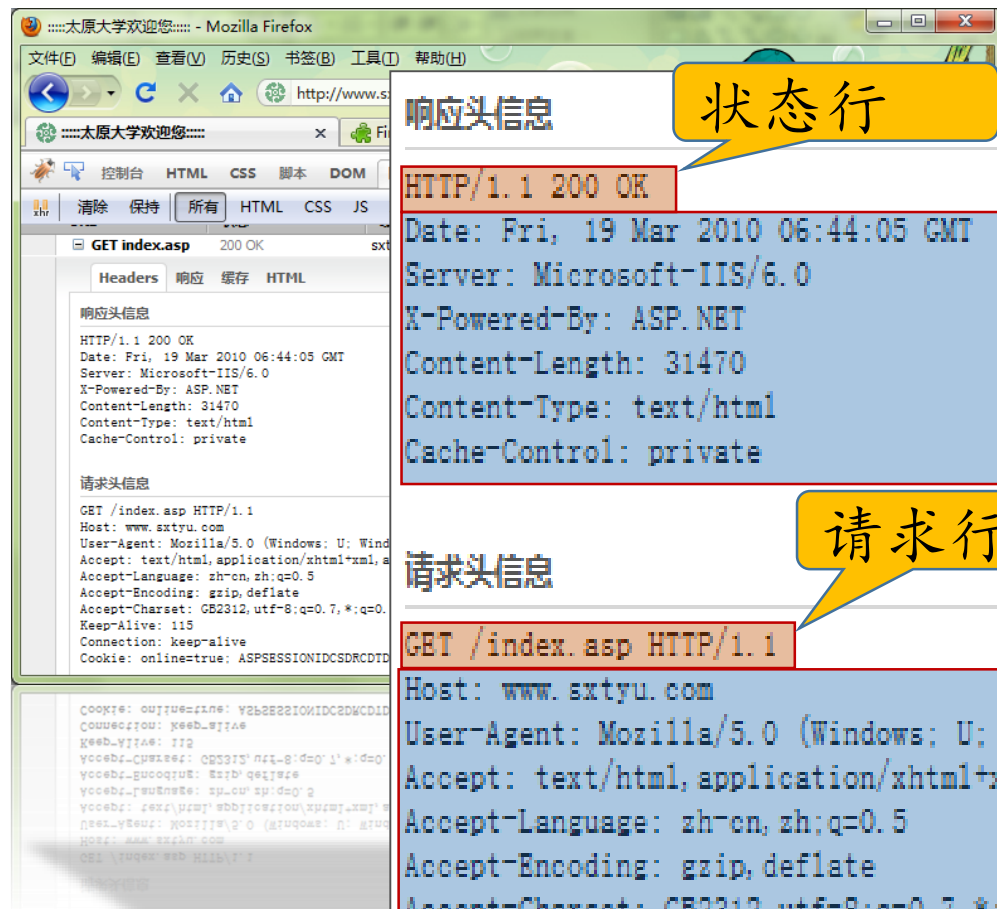


头(header)	类型	说明
User-Agent	请求	关于浏览器和它平台的信息，如Mozilla5.0
Accept	请求	客户能处理的页面的类型，如text/html
Accept-Charset	请求	客户可以接受的字符集，如Unicode-1-1
Accept-Encoding	请求	客户能处理的页面编码方法，如gzip
Accept-Language	请求	客户能处理的自然语言，如en(英语)，zh-cn(简体中文)
Host	请求	服务器的DNS名称。从URL中提取出来，必需。
Authorization	请求	客户的信息凭据列表
Cookie	请求	将以前设置的Cookie送回服务器，可用来作为会话信息

# HTTP报文结构--首部字段或消息头

头(header)	类型	说明
<b>Date</b>	双向	消息被发送时的日期和时间
<b>Server</b>	响应	关于服务器的信息，如Microsoft-IIS/6.0
<b>Content-Encoding</b>	响应	内容是如何被编码的（如gzip）
<b>Content-Language</b>	响应	页面所使用的自然语言
<b>Content-Length</b>	响应	以字节计算的页面长度
<b>Content-Type</b>	响应	页面的MIME类型
<b>Last-Modified</b>	响应	页面最后被修改的时间和日期，在页面缓存机制中意义重大
<b>Location</b>	响应	指示客户将请求发送给别处，即重定向到另一个URL
<b>Set-Cookie</b>	响应	服务器希望客户保存一个Cookie

# HTTP报文结构—实例



响应头信息

状态行

代码美化

HTTP/1.1 200 OK

Date: Fri, 19 Mar 2010 06:44:05 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
Content-Length: 31470  
Content-Type: text/html  
Cache-Control: private

首部字段(行)

请求头信息

请求行

代码美化

GET /index.asp HTTP/1.1

Host: www.sxtyu.com  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; zh-CN; rv:1.9.2) Gecko/20100115 Firefox/3.6  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-cn,zh;q=0.5  
Accept-Encoding: gzip,deflate  
Accept-Charset: GB2312,utf-8;q=0.7,\*;q=0.7  
Keep-Alive: 115  
Connection: keep-alive  
Cookie: online=true; ASPSESSIONIDCSDRCDTD=FPNEMIBBJJKEJMJLDDFIAHEM

首部字段(行)

- **Cookie:**当我们使用自己的电脑通过浏览器进行访问网页的时候，服务器就会生成一个证书并返回给我的浏览器并写入我们的本地电脑。这个证书就是cookie
- **Set-Cookie:** PHPSESSID=l89hpkrks06k82juj4vjoc4mu6; path=/
- 32位长度16进制编码
- C:\Windows\TEMP



➤ 保存在客户端

# HTTP协议与会话管理



## Cookie

Elements Network Sources Timeline Profiles Resources Audits Console									
	Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure	
Frames	__cfduid	7d493e0a2422287207df0ac9c8f21423187255	.gravatar...	/	2016-02...	51	✓		
Web SQL	_ga	1341763833.1423474362	.github.c...	/	2017-03...	30			
IndexedDB	_gh_sess	NzaW9uX2lkajYmY0NjY2ZGU3ZTc2MzhkM2Rk...	.github.c...	/	Session	226	✓	✓	
Local Storage	_octo	1399677830.1423474363	.github.c...	/	2017-02...	31			
Session Storage	doccom_user	93	.github.c...	/	2035-02...	18	✓	✓	
Cookies	logged_in		.github.c...	/	2035-02...	12	✓	✓	
github.com	tz	2FSshanghai	github.c...	/	Session	17		✓	
Annotations Panel	user_session	bNn58QGr-dPPnczs28x5FtDPwHbyzVloOTz69n0MV...	github.c...	/	2015-04...	92	✓	✓	

字段	说明
Name	Cookie名称
Value	Cookie的值
Domain	用于指定Cookie的有效域
Path	用于指定Cookie的有效URL路径
Expires	用于设定Cookie的有效时间
Secure	如果设置该属性，仅在HTTPS请求中提交Cookie
Http	其实应该是HttpOnly，如果设置该属性，客户端JavaScript无法获取Cookie值

- Session机制是一种服务器端的机制
- 当程序需要为某个客户端的请求创建一个session的时候，服务器首先检查这个客户端的请求里是否已包含了一个session标识 - 称为 **session id**，如果已包含一个session id则说明以前已经为此客户端创建过session，服务器就按照session id把这个session检索出来使用（如果检索不到，可能会新建一个），如果客户端请求不包含session id，则为此客户端创建一个session并且生成一个与此session相关联的session id，session id的值应该是一个既不会重复，又不容易被找到规律以仿造的字符串，这个session id将被在本次响应中返回给客户端保存

- Session 是 用于保持状态的基于 Web服务器的方法
- 允许通过将对象存储在 Web服务器的内存中在整个用户会话过程中保持任何对象

- Cookie的数据保存在客户端浏览器，Session保存在服务器
- 服务端保存状态机制需要在客户端做标记，所以Session可能借助Cookie机制
- Cookie通常用于客户端保存用户的登录状态

## ➤认识Burp Suit

- 用于攻击Web 应用程序的集成平台，包含了抓包、漏洞扫描、入侵、爬虫等工具

## ➤使用步骤

- 配置网络代理
- 查看拦截信息
- 拦截输入信息

- HTTP协议介绍
- HTTP请求和响应
- 工具的使用



# Question