



信息安全管理导论

第八章 Web安全

黄 珺



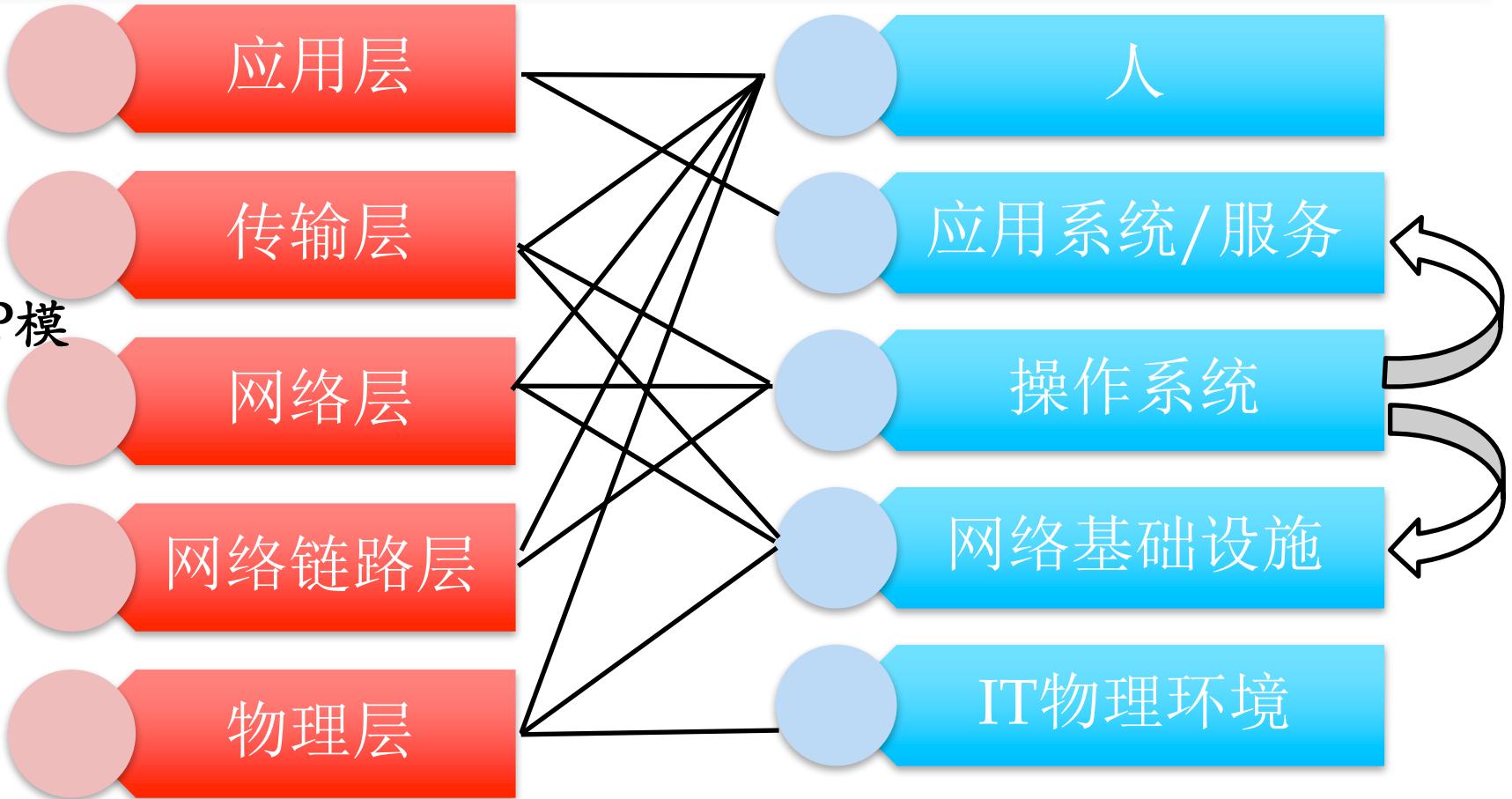
温故

- 网络安全概述
- 网络与系统渗透
- 网络与系统防御



网络安全概述——知己知彼，百战不殆

TCP/IP模
型



网络安全的根本目标是保证网络每一层**应用**的安全

网络安全要适应应用技术的持续发展而不断升级

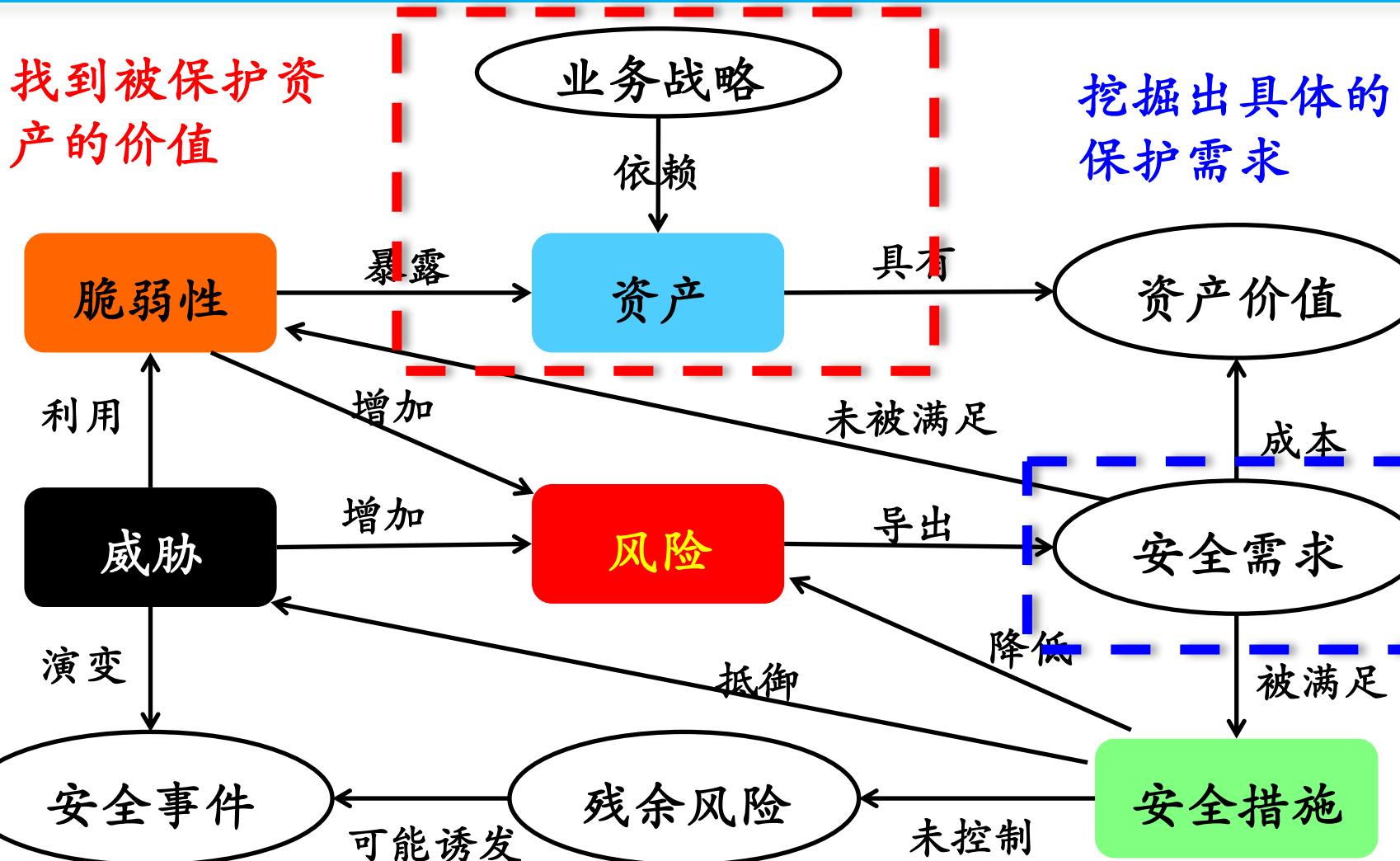


网络与系统渗透

- 渗透测试
 - 取得被测试目标的法律授权
 - 信息收集
 - 目标踩点
 - 网络扫描
 - 漏洞发现
 - 漏洞扫描（识别已知漏洞）
 - 漏洞挖掘（发现未知漏洞）
 - 漏洞利用
 - 提升权限
 - 提供测试报告
- 网络入侵
 - 信息收集
 - 目标踩点
 - 网络扫描
 - 漏洞发现
 - 漏洞扫描（识别已知漏洞）
 - 漏洞挖掘（发现未知漏洞）
 - 漏洞利用
 - 提升权限
 - 后门植入
 - 擦除痕迹



网络与系统防御





知新

- Web应用及开发技术简史
- Web应用开发技术大观
- Web应用常见缺陷与加固



互联网的早期历史

	Event Date:	Event Title:	Event Description:
	12/01/1969	Creation of ARPANET	(Advanced Research Projects Agency Network) this linked U.S. scientific and academic researchers. ARPAnet was the forerunner of today's Internet.
	12/31/1969	Creation of GML	GML (Generalized Markup Language) is the predecessor to SGML. GML was developed by IBM in efforts led by Charles Goldfarb. GML originated the use of , and / for markup and is still in use for document applications.
	10/28/1971	E-mail is invented	by: Ray Tomlinson
	10/28/1980	SGML is announced	(Standard Generalized Markup Language) by American National Standards Institute Committee. SGML is the parent language of HTML.
	10/28/1984	HTML is invented	HTML is the most popular markup language in use today, it is an application of SGML. HTML is one of the foundations of web development.
	10/28/1989	World Wide Web is introduced	Tim Berners-Lee proposed a set of protocols and software that allowed computers to browse the information in the Internet (World Wide Web). He also developed the first web server called Hypertext Transfer Protocol daemon (HTTP).
	08/01/1991	First website is launched	Tim Berners-Lee was responsible for the first website, info.cern.ch
	10/28/1993	Mosaic is released	Mosaic, the first internet browser, was released by NCSA. Mosaic allowed users to surf the Internet in a graphical way and also opened the web up to the general public.
	10/28/1994	W3C Consortium is founded	W3C Consortium is founded in order to set standards and direction of future development of HTML.
	10/28/1995	Windows 95 is released	Microsoft released Windows 95, the newest revision of the company's operating system. This featured a completely new user interface & a browser on the Windows platform, Microsoft Internet Explorer, which became popular worldwide.



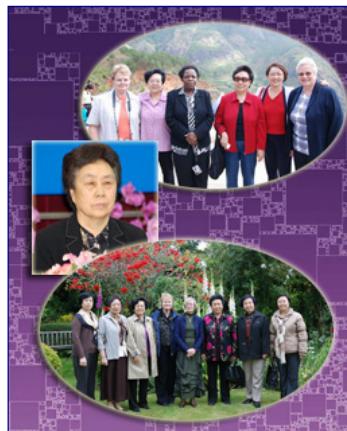
为什么要重点讲解Web安全？

- Web应用程序是最常见的网络渗透入口点
 - Web应用 == Web软件
- Web软件是最普遍的云服务实现载体
 - 云存储：Dropbox、DBank等
 - 即时通信：腾讯Web QQ
 - 微博：新浪微博、腾讯微博
 - 视频：优酷、奇艺、腾讯视频
- Web软件开发技术支撑着整个互联网应用
 - 电子商务、门户网站、搜索引擎、即时通信、网络电视……



Web软件是什么？

- 网页？
- 论坛？



[第四届世界大学女校长论坛正在筹备中](#)

发表论文

- 胡平：《双重角色下的冲突与发展——中国高校女教师生存状况研究》
- 胡平：《高等教育评价指标体系的构建与评价》
- 胡平：《高等教育评价指标体系的构建与评价》

通知公告

- 通知：关于《新编中国女性史》
- 通知：关于“世界大学女校长论坛”

世界大学女校长论坛

世界大学女校长论坛是由中国传媒大学和中央电视台社教部、全国妇联组织联络部联合主办的。它云集了来自不同国家和地区的100多名女校长、女书记。

第四届世界大学女校长论坛

第四届世界大学女校长论坛将于2009年举行，分别在云南丽江和新西兰举办的两次筹备会议上，就论坛的主题的具体举办地点以及时间进行了详细的讨论。

第一届回顾

- 综述：2001年8月在北京召开，主要围绕新世纪高等教育的主题进行探讨。
- 盛况：各界领导以及100多位女校长云集北京。
- 成果：出版《新世纪高等教育发展战略》

第二届回顾

- 综述：2004年9月7日在北京成功举办，历时两天，受到了各界人士的一致好评。

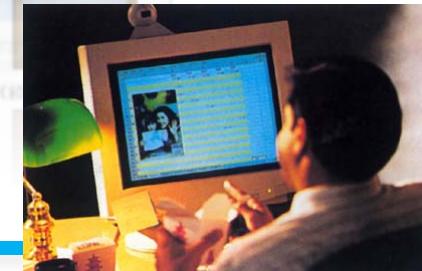
论坛组委会

- 刘继南：第三届世界大学女校长论坛主席，中国传媒大学名誉校长。
- 杨孟：第三届世界大学女校长论坛常务副主席，中国教育交流协会副秘书长。

相关研究

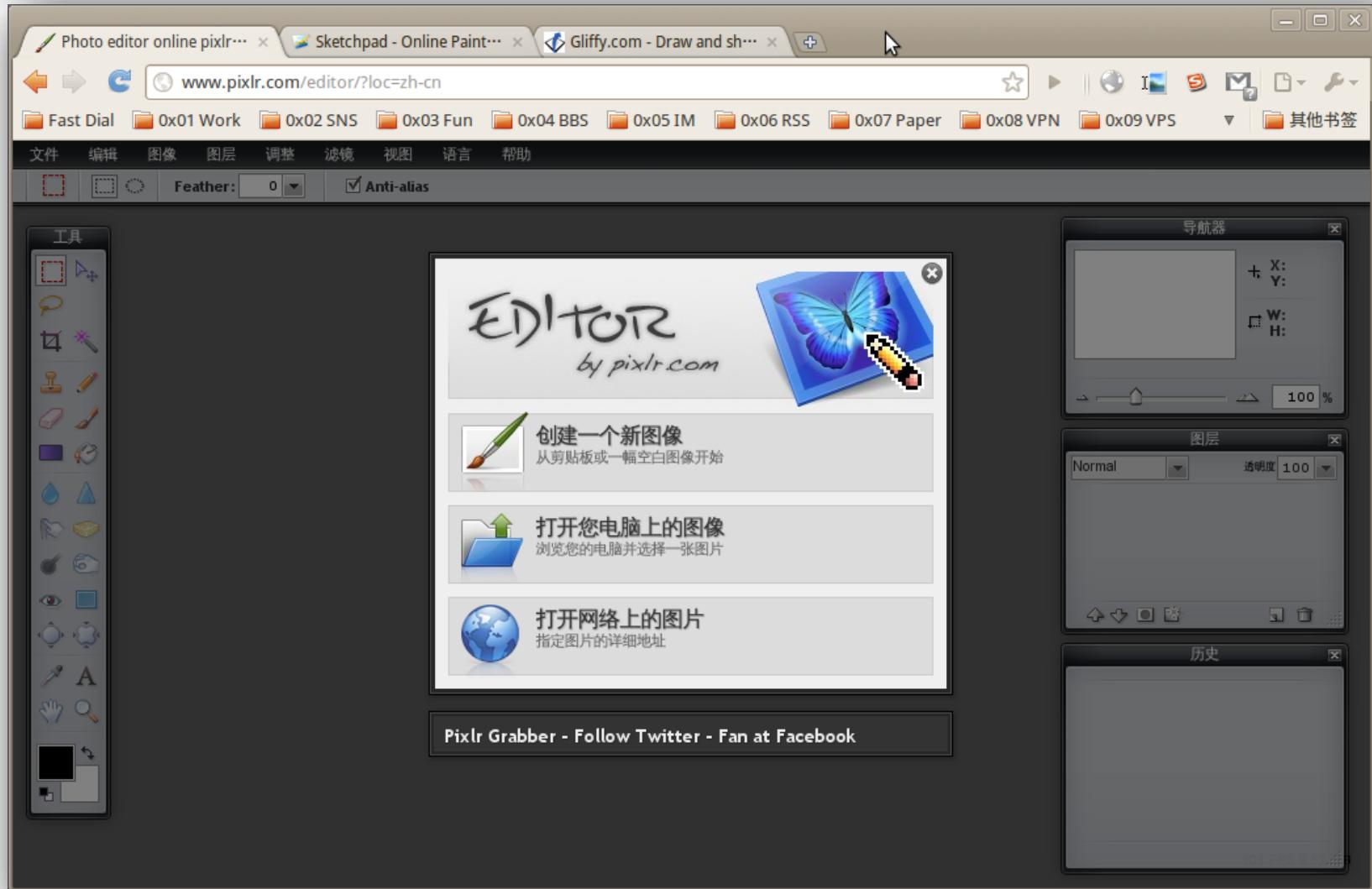
[《和谐世界 文化多样》](#)

[第二届大学女校长 国际论坛](#)





这些都是Web软件



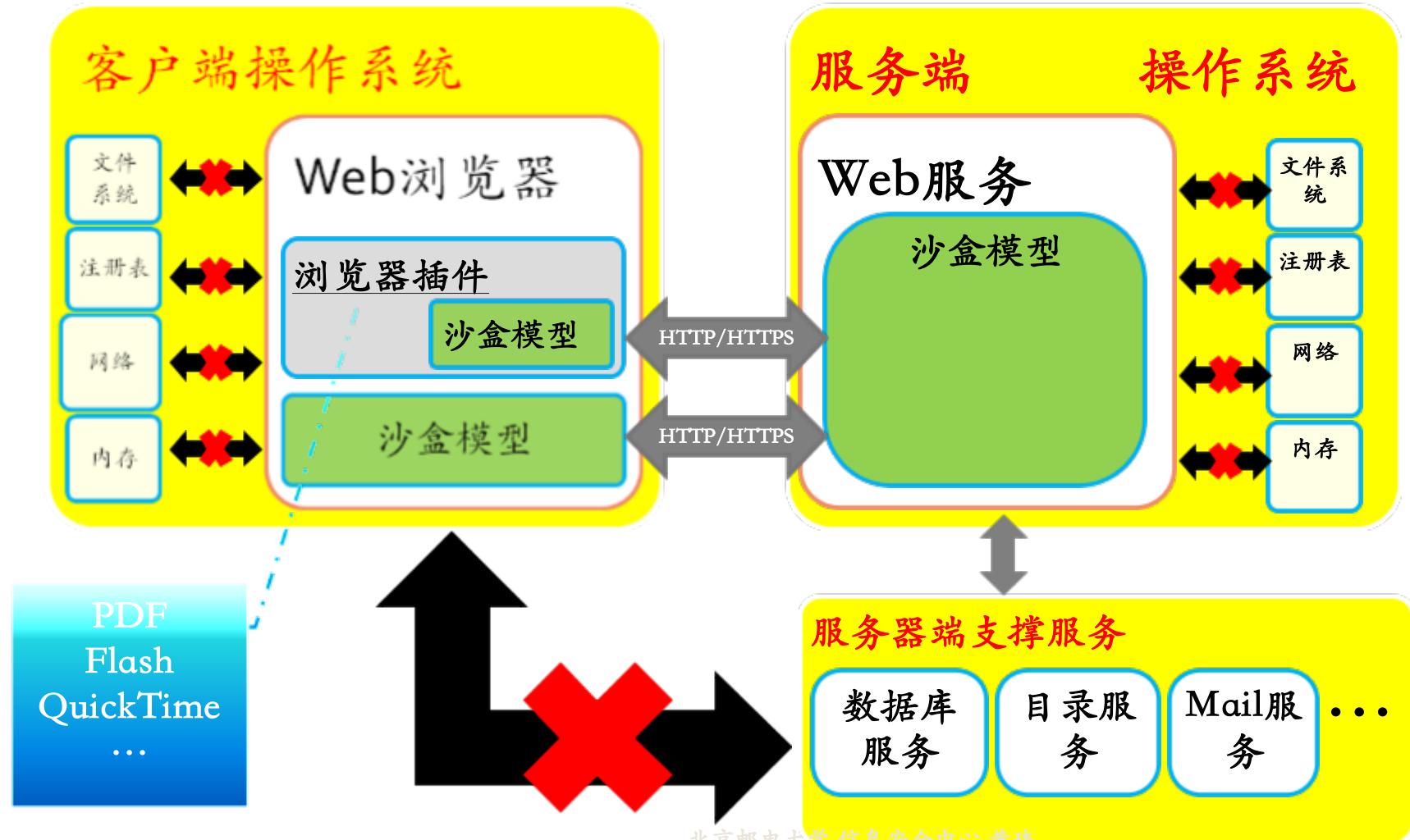


Web软件的定义

- 描述定义
 - 运行在Web服务器（如IIS、Apache）上、基于HTTP/HTTPS协议传输的应用程序
- 组成定义
 - 浏览器（**Browser**）
 - Web服务器（**Server**）
 - 其他？见安全模型
- 分类定义
 - 静态程序
 - 动态程序
 - CGI
 - JSP
 - PHP

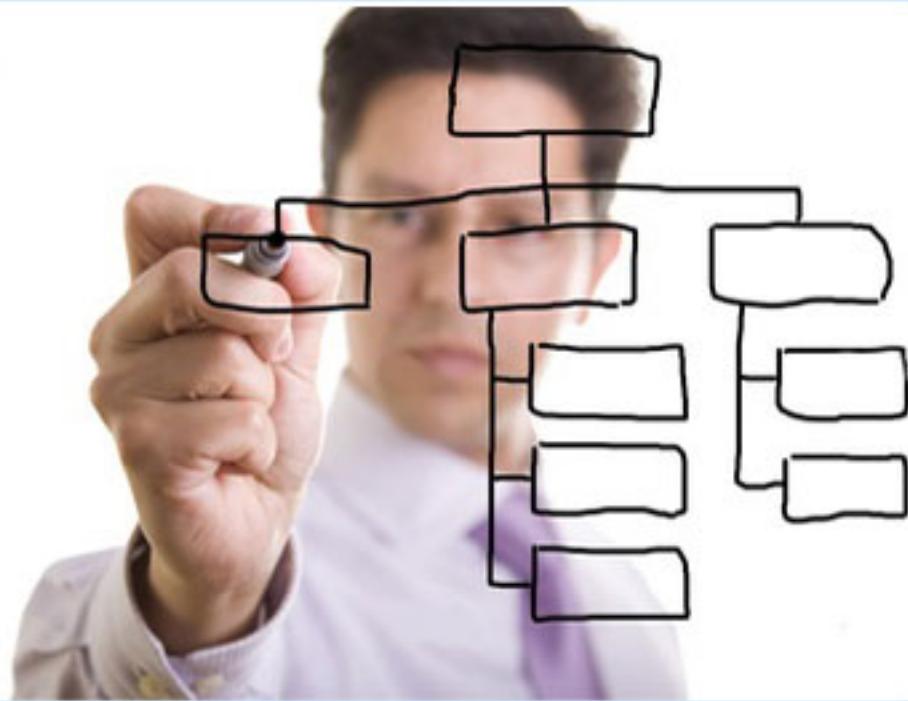


安全模型





Web Development



中国传媒大学



典型Web应用技术架构

- 客户端技术
- 服务端技术

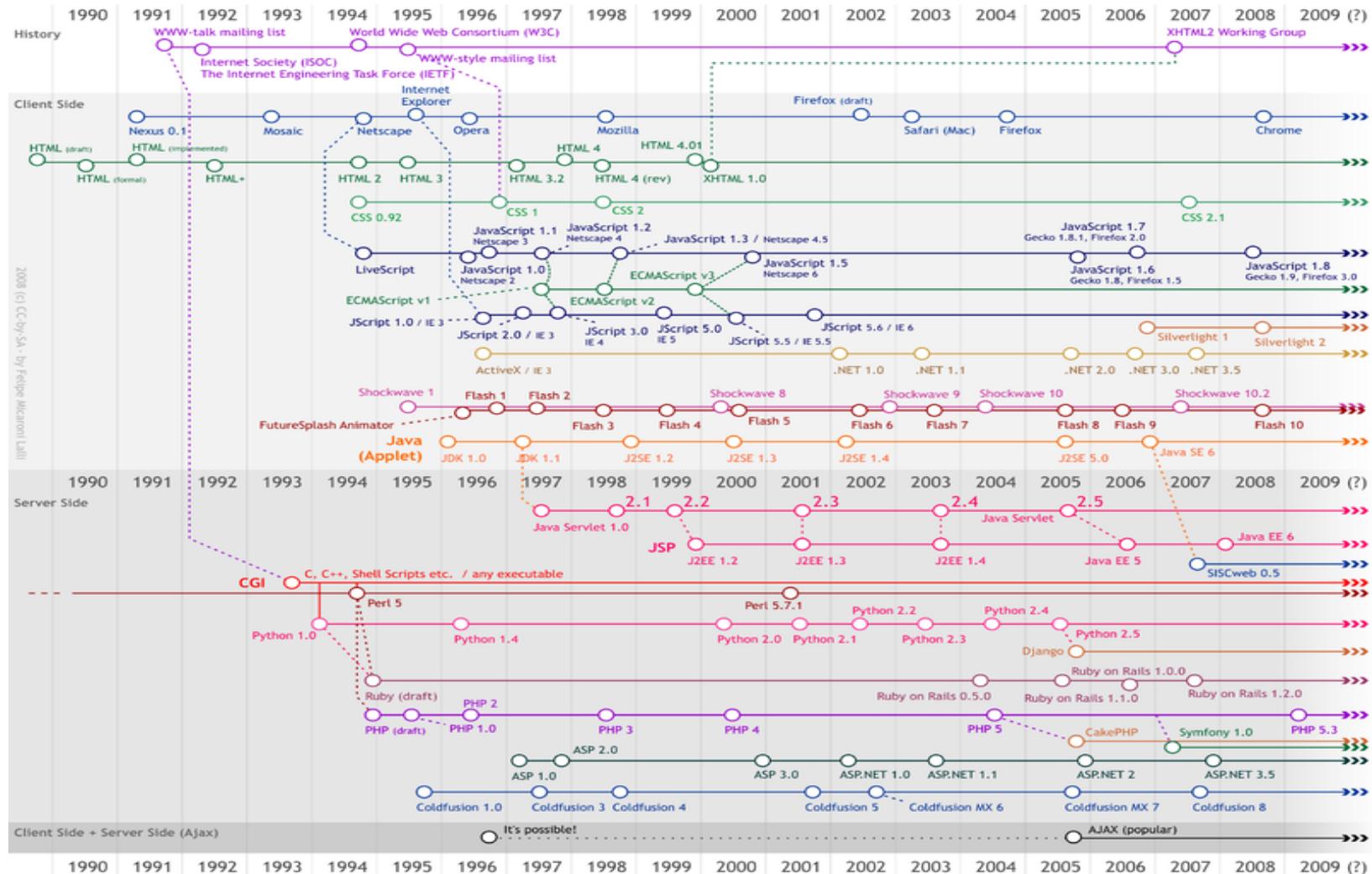
客户端

服务端





Web 开发技术简史



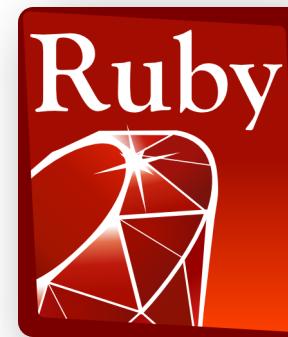
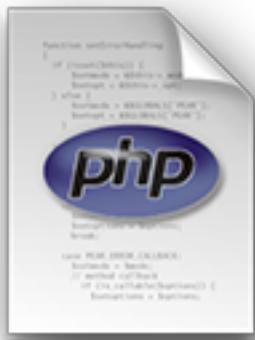
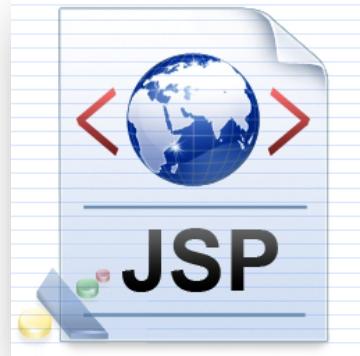
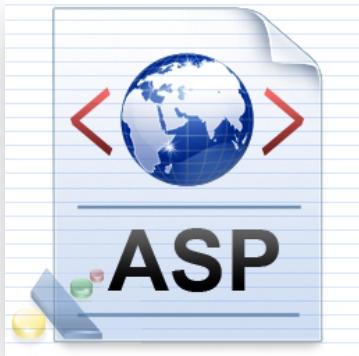


客户端编程语言





服务端编程语言





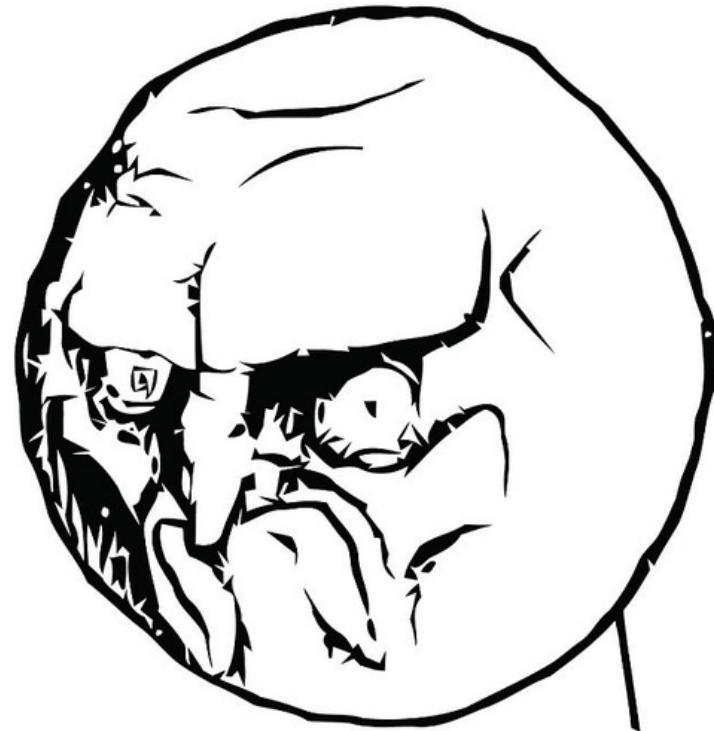
数据库



Microsoft®
SQL Server®20



Web应用开发技术 == 编程语言?



NO.



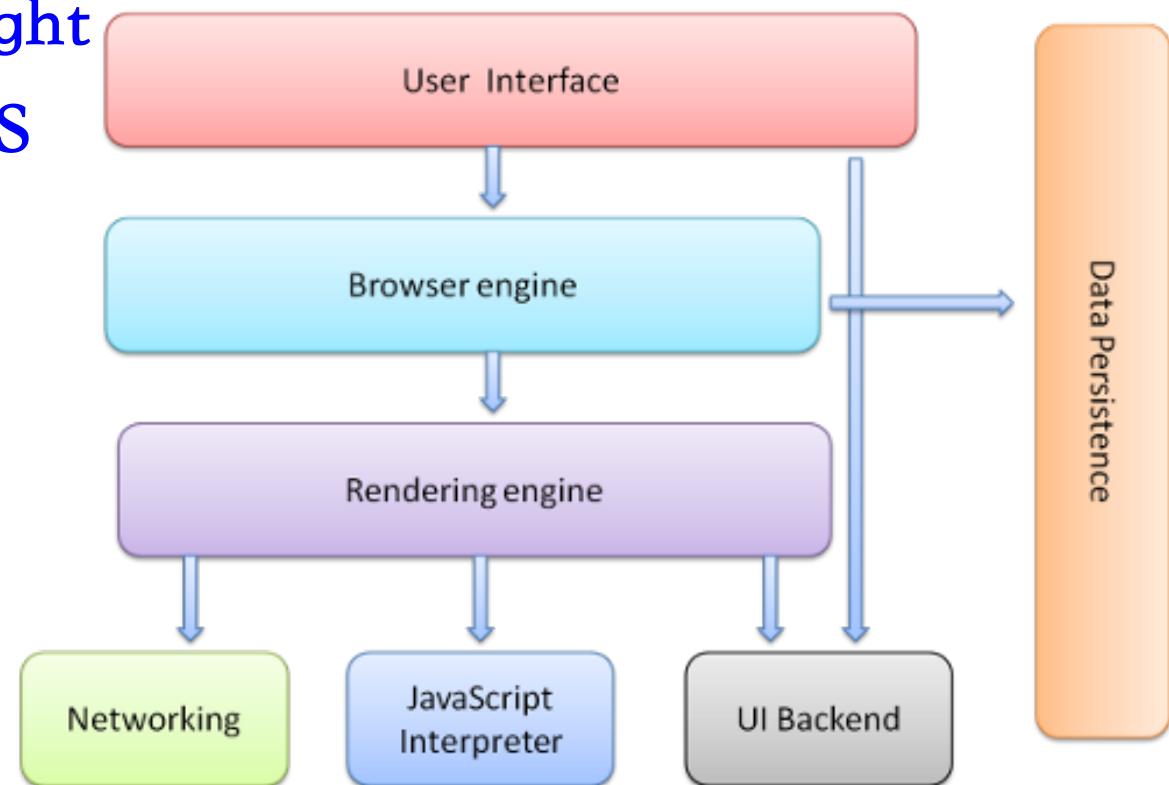
知新

- Web应用及开发技术简史
- Web应用开发技术大观
- Web应用常见缺陷与加固



客户端技术

- 浏览器
 - HTML/CSS/Javascript
 - Flash/Silverlight
 - HTTP/HTTPS
- 插件
 - 支付宝
 - 网银控件
 - PDF

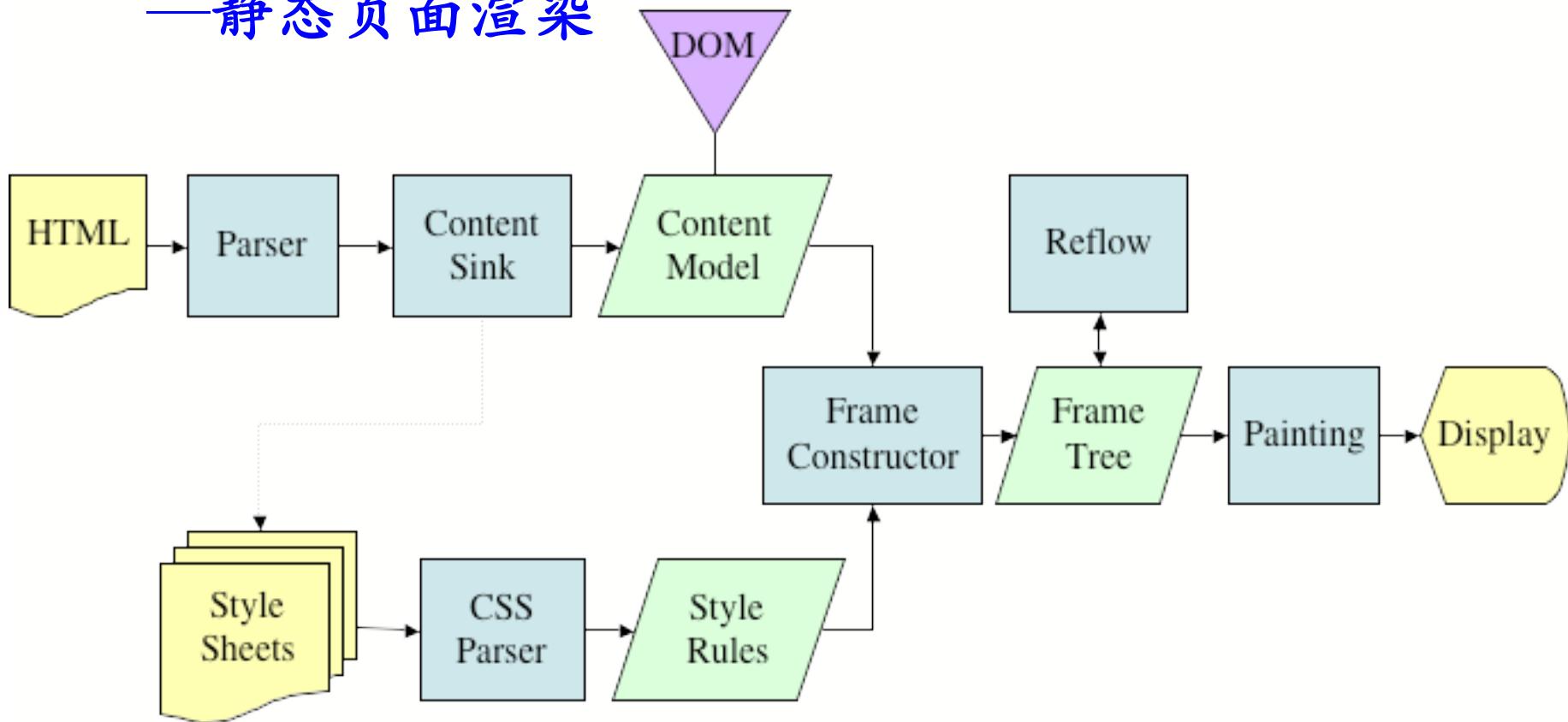




客户端技术

• 浏览器

—静态页面渲染

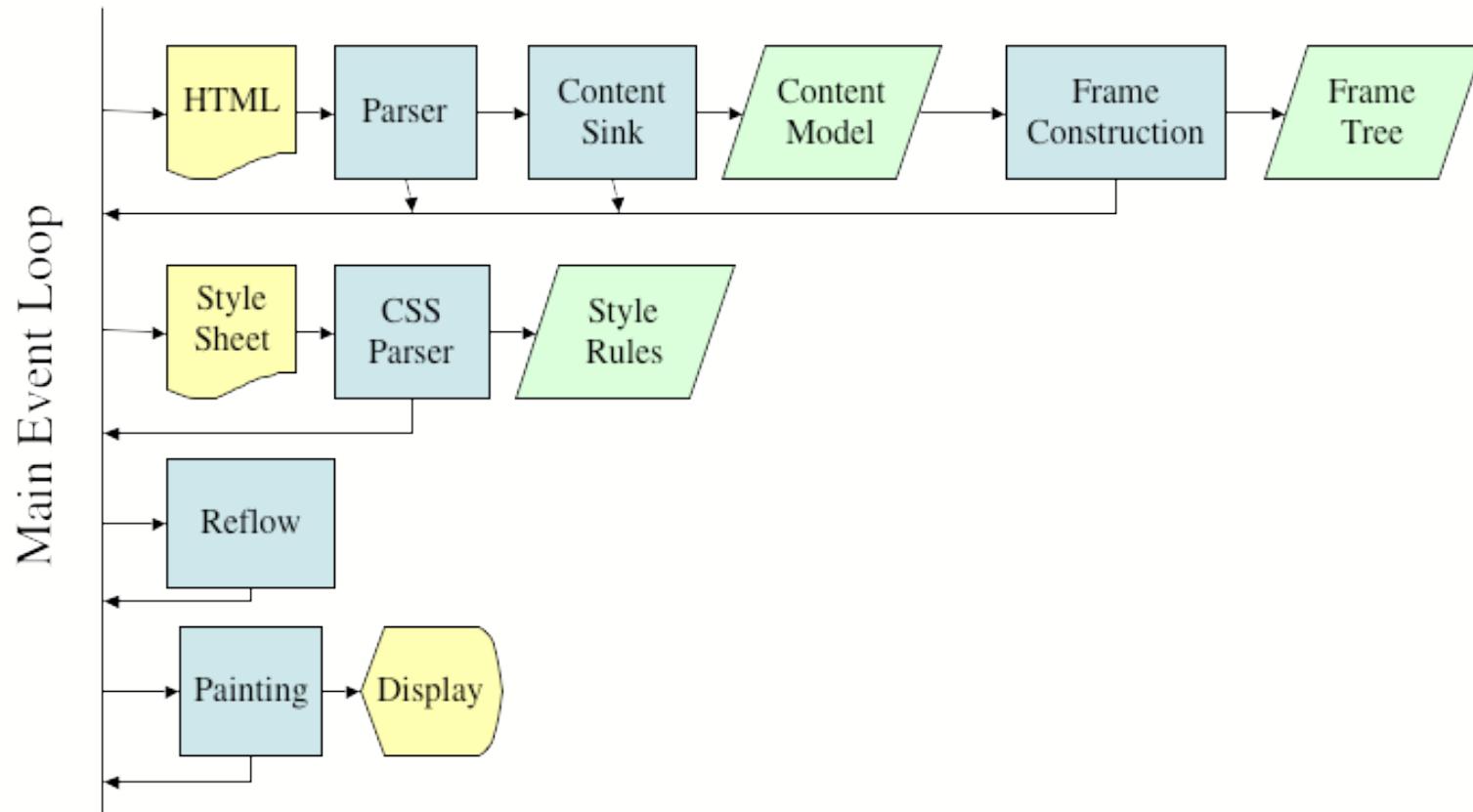




客户端技术

- 浏览器

—动态（客户端脚本技术）页面渲染





浏览器大战



IE

Firefox

Chrome

Safari

Opera

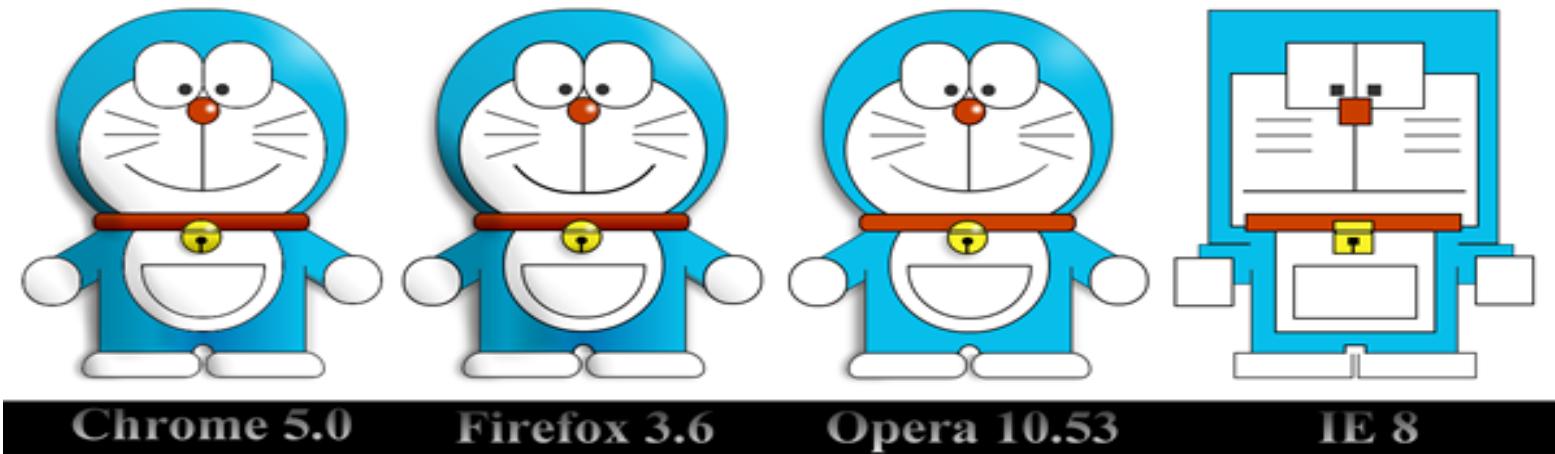
Netscape

中国传媒大学



浏览器的Web标准支持差异性

- Web标准
 - 传输协议：HTTP/HTTPS
 - HTTP响应内容的解析执行
 - HTML、JS、CSS（版本支持的差异性）
 - 图形渲染（图片、视频）





服务端技术

- Web服务器
 - 通信协议栈实现
- 应用服务器
 - 应用程序运行环境
 - PHP/Java/ASP/.NET/…
- 数据库
 - 关系型数据库： MySQL/Oracle/SQLServer/…
 - 非关系型数据库： Memcache/Redis/Mongodb/…



通信

- HTTP
- HTTPS
 - SSL
 - TLS
 - 简单策略/交互策略
 - 数字证书/PKI
- DNS
 - DNSSEC



Web软件还用到了哪些技术? (1/2)

- 用户标识与会话管理
 - 浏览器端: cookie
 - 服务端: session
- 数据存储
 - 分布式数据存储、数据分析
 - 海量数据处理技术
- 日志系统
 - 不可抵赖日志
 - 防篡改、一致性、可用性



Web软件还用到了哪些技术? (2/2)

- 负载均衡系统
 - 数据一致性
 - 故障切换
 - 资源有效利用
 - CDN、流量分配器
- 代码管理与发布
 - 版本管理
 - 代码上线发布



亲，让我们来看看淘宝购物背后的技术

- 从浏览器地址栏输入www.taobao.com开始
—DNS解析

— CDN, 让你从最近的入口访问taobao

```
huangwei@localhost:~/workspace/icontactios$ nslookup  
> www.taobao.com
```

```
Server:      192.168.1.1  
Address:    192.168.1.1#53
```

```
Non-authoritative answer:
```

```
www.taobao.com canonical name = www.gslb.taobao.com.danuoyi.tbcache.com.  
www.gslb.taobao.com.danuoyi.tbcache.com canonical name = scorpio.danuoyi.tbcache.com.  
Name: scorpio.danuovi.tbcache.com
```

```
Address: 61.55.165.251
```

```
Name: scorpio.danuoyi.tbcache.com
```

```
Address: 61.55.164.251
```

```
> server 8.8.8.8
```

```
Default server: 8.8.8.8
```

```
Address: 8.8.8.8#53
```

```
> www.taobao.com
```

```
Server:      8.8.8.8
```

```
Address:     8.8.8.8#53
```

```
Non-authoritative answer:
```

```
www.taobao.com canonical name = www.gslb.taobao.com.danuoyi.tbcache.com.  
www.gslb.taobao.com.danuoyi.tbcache.com canonical name = scorpio.danuoyi.tbcache.com.  
Name: scorpio.danuovi.tbcache.com
```

```
Address: 119.167.201.241
```

```
Name: scorpio.danuoyi.tbcache.com
```

```
Address: 101.226.178.41
```

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:61.55.164.251

- 本站主数据: 河北省邯郸市 联通
- 参考数据一: 河北省邯郸市 联通

ip138.com IP查询(搜索IP地址的地理位置)

您查询的IP:119.167.201.241

- 本站主数据: 山东省青岛市 联通
- 参考数据一: 山东省青岛市 联通



亲，让我们来看看淘宝购物背后的技术

- 一个IP == 一台服务器?

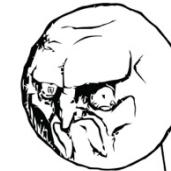
- 负载均衡

- 一拖N

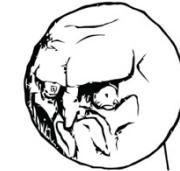
- 一个页面 == 一次请求?

The screenshot shows a Taobao search results page for '去黑头的皂'. The search bar at the top has '去黑头的皂' entered. Below the search bar, there are several product listings, each with a thumbnail image, product name, and price. The interface includes typical Taobao navigation elements like '宝贝' (Products), '评价' (Reviews), '问答' (FAQ), and '店铺' (Shop).

At the bottom of the browser window, the developer tools Network tab is open, showing a list of network requests made by the page. The requests include various files such as CSS, JS, and images, illustrating the complexity of a single page load.



NO.



NO.



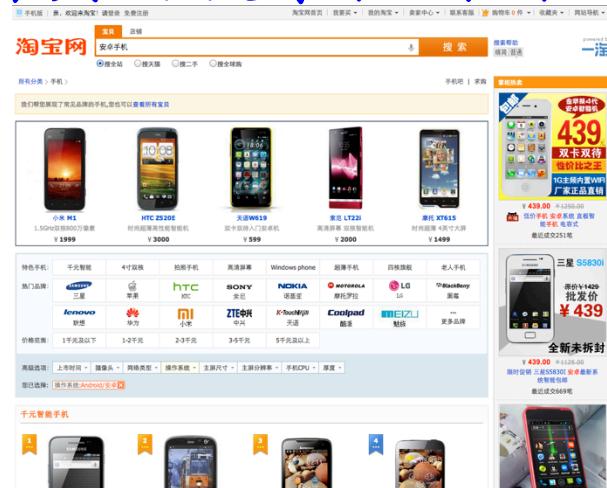
亲，让我们来看看淘宝购物背后的技术

- 为什么查看一个页面需要发出这么多请求?
 - HTML/CSS/JS/PNG/GIF/SWF...
 - 优化加载性能
 - 浏览器在同一时刻并发请求单个域名下的资源数量有限制
 - 不同资源会部署在不同的子域名下



亲，让我们来看看淘宝购物背后的技术

- 一个淘宝卖家上传修改了一件商品的图片
—后端的成千上万台图片服务器需要同步更新
 - 内容分发与同步技术
- 买家想买一个安卓手机
—在淘宝首页的搜索框内输入：安卓手机





亲，让我们来看看淘宝购物背后的技术

手机版 | 亲，欢迎来淘宝！请登录 免费注册 淘宝网首页 | 我要买 | 我的淘宝 | 卖家中心 | 联系客服 | 购物车 0 件 | 收藏夹 | 网站导航

宝贝 店铺
安卓手机
搜全站 搜天猫 搜二手 搜全球购

所有分类 > 手机 >

我们帮您展现了常见品牌的手机,您也可以[查看所有宝贝](#)

小米 M1 1.5GHz双核800万像素 ¥ 1999	HTC Z520E 时尚超薄高性能智能机 ¥ 3000	天语W619 双卡双待入门安卓机 ¥ 599	索尼 LT22i 高清屏幕 双核智能机 ¥ 2000	摩托 XT615 时尚超薄 4英寸大屏 ¥ 1499
-----------------------------------	-----------------------------------	------------------------------	----------------------------------	----------------------------------

特色手机: 千元智能 4寸双核 拍照手机 高清屏幕 Windows phone 超薄手机 四核旗舰 老人手机

热门品牌: 三星 苹果 HTC 索尼 诺基亚 摩托罗拉 LG 黑莓 联想 华为 小米 中兴 酷派 酷派 魅族 ... 更多品牌

价格范围: 1千元及以下 1-2千元 2-3千元 3-5千元 5千元及以上

高级选项: 上市时间 | 摄像头 | 网络类型 | 操作系统 | 主屏尺寸 | 主屏分辨率 | 手机CPU | 厚度 |
您已选择: 操作系统:Android/安卓

千元智能手机

- 1 SAMSUNG
- 2 ZTE
- 3 lenovo
- 4 Coolpad

- 理解用户输入
 - 搜索关键词分词
 - 猜你喜欢
 - 分词结果处理
 - 安卓
 - 手机
- 广告
 - 竞价关键词相关度计算
 - 畅销机型推荐
 - 数据挖掘与分析
- 搜索结果列表展示



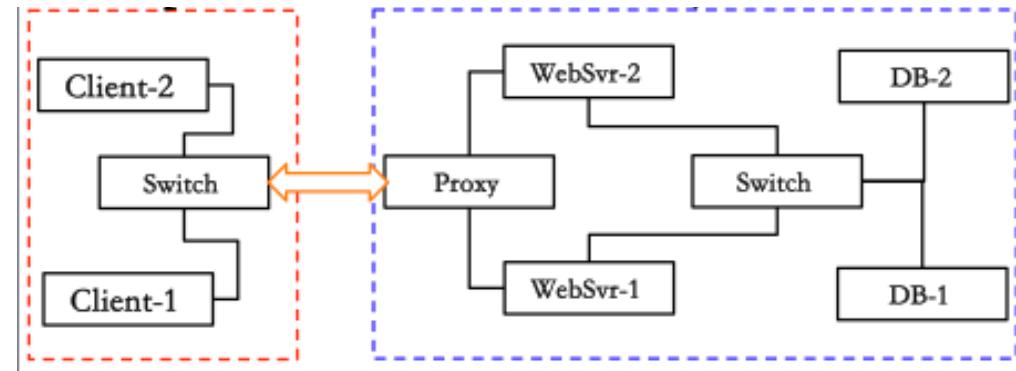
亲，让我们来看看淘宝购物背后的技术

- 查看订单详情
 - 如果卖家在你下单后恶意提高了成交价格怎么办?
 - 订单快照技术
 - 防抵赖
- 支付
 - 和银行系统的对接
 - 数据同步问题
- 上线新业务、新系统
 - 成千上万台服务器同时“安装新软件”



软件规模与软件安全

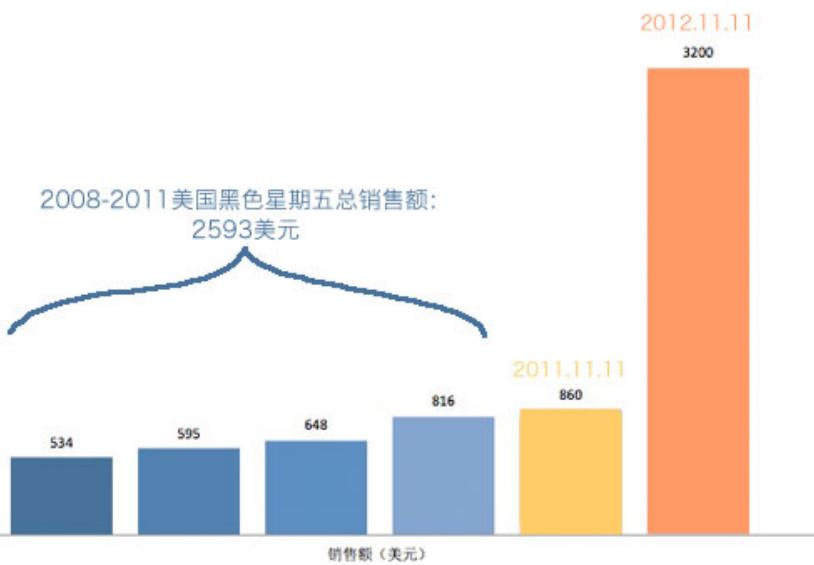
- 规模大意味着复杂度高
 - 用户数多、系统使用到的服务器多、存储和处理的数据量大、网络传输的数据多
- 复杂度提高意味着出错的概率提高
- 出错的概率提高意味着系统出现漏洞的机率增加
 - 回顾上节课内容



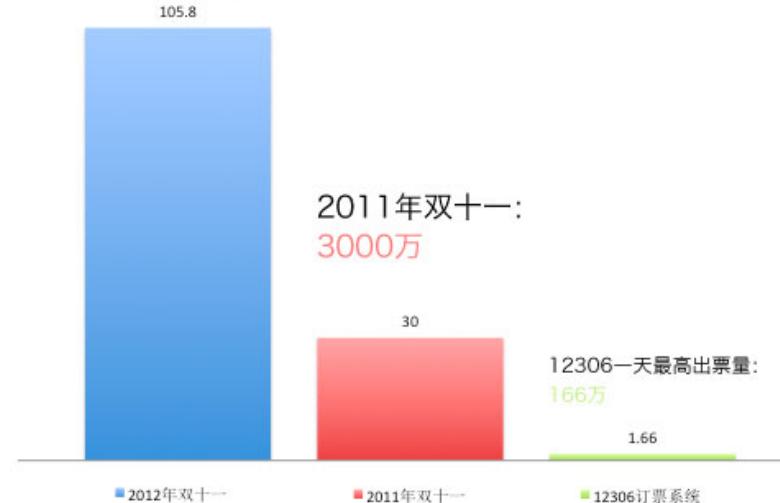


一组数据 (1/3)

2012年的双十一，支付宝总销售额超过了**191亿**。
这是2011年的3倍多，超过了美国过去4年黑色星期五的销售额总和。



支付宝在一天中处理的交易数量：
1.058亿





一组数据 (2/3)





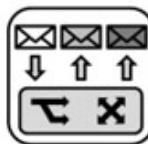
一组数据 (3/3)

OceanBase

淘宝OceanBase海量关系数据库
线上业务: 30多个
最大单表: 400亿条

APACHE
HBASE

淘宝某HBase业务
读数据流量: 10Gbps
写数据流量: 5Gbps



淘宝消息中间件notify
今年刚刚改造为TDDL
共接收消息: 50亿
共投递消息: 260亿

MySQL.

淘宝MySQL业务 某核心集群
活动连接: 超过4000
网卡: 全跑满
全天执行SQL数量: 293亿次
集群总QPS: 86万/秒
集群TPS: 11万/秒
单机QPS: 6.5万/秒



阿里云RDS关系数据库
单实例QPS: 5万6+
TPS: 5万6+
IOPS: 4.4W+



数据解读

- 大规模网站的可用性目标既是业务目标，同时也是安全目标
 - 拒绝服务攻击 VS. 大规模用户访问



知新

- Web应用及开发技术简史
- Web应用开发技术大观
- Web应用常见缺陷与加固



亲，让我们再来看看淘宝购物流程中的可能风险点

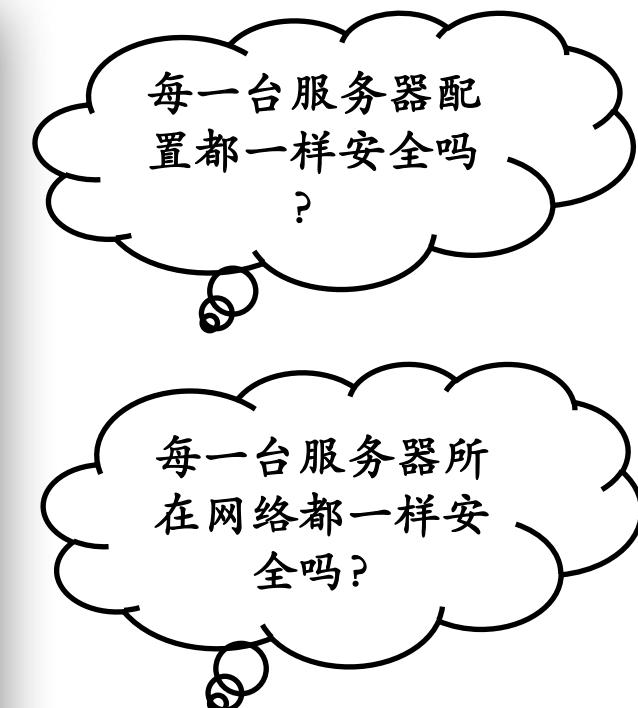
- 从浏览器地址栏输入www.taobao.com开始
—DNS解析

— CDN, 让你从最近的入口访问taobao

```
huangwei@localhost:~/workspace/icontactios$ nslookup
> www.taobao.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
www.taobao.com canonical name = www.gslb.taobao.com.danuoyi.tbcache.com.
www.gslb.taobao.com.danuoyi.tbcache.com canonical name = scorpio.danuoyi.tbcache.com.
Name: scorpio.danuovi.tbcache.com
Address: 61.55.165.251
Name: scorpio.danuoyi.tbcache.com
Address: 61.55.164.251
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> www.taobao.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.taobao.com canonical name = www.gslb.taobao.com.danuoyi.tbcache.com.
www.gslb.taobao.com.danuoyi.tbcache.com canonical name = scorpio.danuoyi.tbcache.com.
Name: scorpio.danuovi.tbcache.com
Address: 119.167.201.241
Name: scorpio.danuoyi.tbcache.com
Address: 101.226.178.41
```





亲，让我们再来看看淘宝购物流程中的可能风险点

- 一个网站包括多个子域名、多个IP、多台服务器
 - 信息安全的木桶原理
 - 整站安全性取决于最弱的一个节点

The screenshot shows a browser's developer tools Network tab with a list of requests made to various sub-domains of Taobao. The requests include:

- tao.2012.css
- mobile_charge.htm.8
- mobile_charge.htm.18
- mobile_charge.htm.18
- mobile_charge.htm.18
- mobile_charge.htm.18
- mobile_charge.htm.16
- mobile_charge.htm.24
- mobile_charge.htm.42
- mobile_charge.htm.32
- mobile_charge.htm.255
- kissym-min.js.21
- it_c.js.1
- mobile_price.htm

Each request entry includes details such as Method (e.g., GET), Status (e.g., 200 OK), Type (e.g., text/css, application/x-javascript), Initiator (e.g., Parser, Script), Size (Content Length), Latency (Time taken), and Timeline (Sequence of events).

- 站点
 - http://a.tbcdn.cn
 - http://acookie.alimama.com
 - http://acookie.tanx.com
 - http://acookie.taobao.com
 - http://cdn.tanx.com
 - http://hz.mmstat.com
 - http://i.mmcn.cn
 - http://img01.taobaocdn.com
 - http://img02.taobaocdn.com
 - http://img03.taobaocdn.com
 - http://img04.taobaocdn.com
 - http://log.mmstat.com
 - http://p.tanx.com
 - http://pcookie.taobao.com
 - http://safebrowsing.clients.google.com
 - http://textlink.simba.taobao.com
 - http://www.atpanel.com
 - http://www.taobao.com



亲，让我们再来看看淘宝购物流程中的可能风险点

- 为什么查看一个页面需要发出这么多请求?
 - HTML/CSS/JS/PNG/GIF/SWF...
 - 静态文件读取
 - 文件系统/网络文件系统
 - 动态内容读取和写入
 - 数据库
 - 第三方服务
 - 脚本执行
 - PHP/Java/.NET...



亲，让我们再来看看淘宝购物流程中的可能风险点

- 一个淘宝卖家上传修改了一件商品的图片
 - 图片内包含恶意代码
 - 非店主本人的恶意修改
 - 口令泄漏/弱口令/CSRF
- 买家想买一个安卓手机
 - 搜索框内可以构造恶意输入
 - SQL注入
 - XSS



亲，让我们再来看看淘宝购物流程中的可能风险点

- 查看订单详情

- 非授权访问TA人订单

- 支付

- 钓鱼支付

- 上线新业务、新系统

- 代码服务器漏洞导致代码泄漏
 - 臭名昭著的.svn目录

- 备份文件

- .bak/.txt等



从SDL视角看Web软件漏洞与加固

培训

需求分析

详细设计

代码实现

测试验证

产品发布

应急响应



- 杜绝弱口令
—默认口令安全



- 安全编程方法培训



从SDL视角看Web软件漏洞与加固

培训

需求分析

详细设计

代码实现

测试验证

产品发布

应急响应



- 用例建模

- 角色类型

- 匿名用户、普通注册用户、管理员、超级管理员

- 权限划分



- 业务容量规划

- 用户数、访问量、访问规律（访问洪峰）



- 系统建设成本

- 服务器/带宽/存储

- 是否计划购买外置式安全设备/软件

- 是否计划购买源代码审查工具



从SDL视角看Web软件漏洞与加固



• 域名规划

- 不同类型业务按子域名划分
 - 静态文件类服务 tcdn.tbs.com
 - 图片 img.tcdn.tbs.com
 - CSS/JS static.tcdn.tbs.com
 - 资源上传类服务 i.taobao.com



• 只读cookie

- `httpOnly`属性



• 权限规划

- 代码权限/服务器权限/数据库权限/第三方服务权限…



从SDL视角看Web软件漏洞与加固

培训

需求分析

详细设计

代码实现

测试验证

产品发布

应急响应

• 代码实现



— 前端代码安全

- XSS/CSRF/HTML注入/CSS注入



— 后端代码安全

- SQLInj/PHP LFI/PHP RFI…



从SDL视角看Web软件漏洞与加固

培训

需求分析

详细设计

代码实现

测试验证

产品发布

应急响应



- 渗透测试



- 源代码审计



- 服务器配置审计



从SDL视角看Web软件漏洞与加固

培训

需求分
析

详细设
计

代码实
现

测试验
证

产品发
布

应急响
应

- 白名单机制文件发布
 - 避免非预期文件被上线
- 配置信息独立化
 - 生产配置信息和开发环境配置信息相互独立



从SDL视角看Web软件漏洞与加固

培训

需求分析

详细设计

代码实现

测试验证

产品发布

应急响应



- 服务隔离和切换机制

- 被攻陷服务器的临时下线和重新加入

- 宕机服务器的临时屏蔽和重启后重新加入



深入Web安全和信息安全

- 计算机科学与技术专业
 - 掌握如何编写安全的软件
- 信息安全专业
 - 掌握如何编写安全的软件
 - 掌握如何发现软件中存在的漏洞并修补TA



参考文献

- Web开发技术简史 <http://webdesignergeeks.com/web-designing/web-development-history-technologies/>
- 网络的演变 <http://www.evolutionoftheweb.com/?hl=zh-cn>
- 电子邮件发送流程可视化
<http://www.google.com/green/storyofsend/desktop/>
- WebKit核心浏览器加载网页的原理
<https://www.webkit.org/blog/1188/how-webkit-loads-a-web-page/>
- 现代浏览器基本架构
<http://www.html5rocks.com/en/tutorials/internals/howbrowserswork/>



参考文献

- 解密全球最大网站Facebook背后的那些软件

<http://www.iteye.com/news/16925>