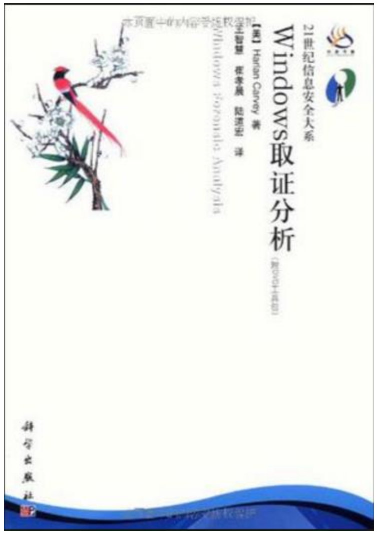
网站/服务器取证实践与挑战

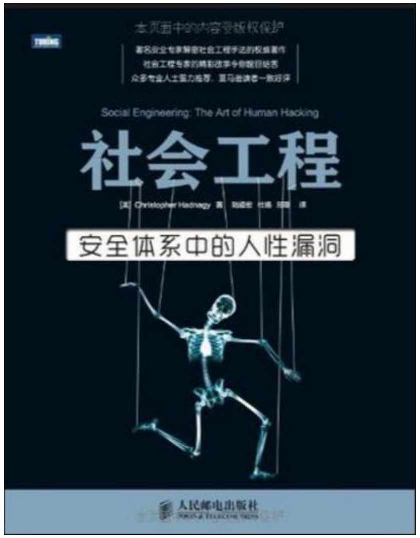
陆道宏

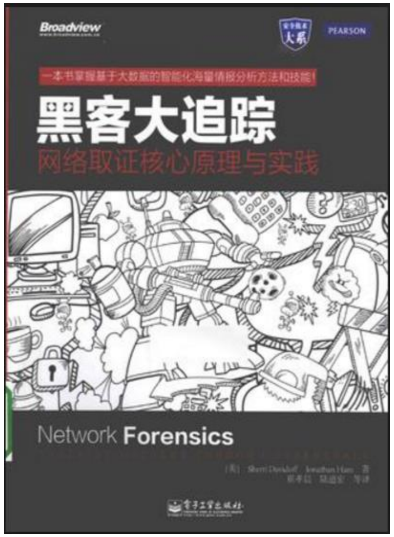
上海弘连网络科技有限公司

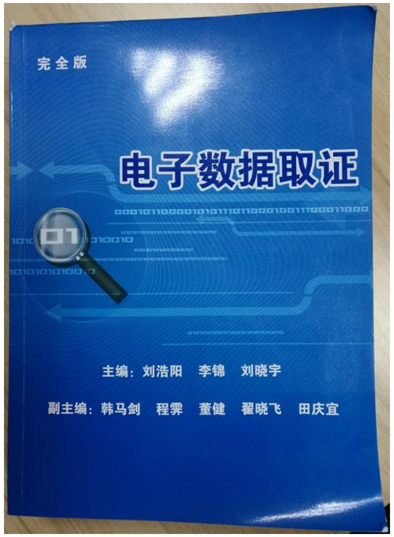
2016年7月14日

自我介绍




Social Engineering: The Art of Human Hacking
社会工程
[美] Christopher Hadnagy 著
安全体系中的人性漏洞
人民邮电出版社



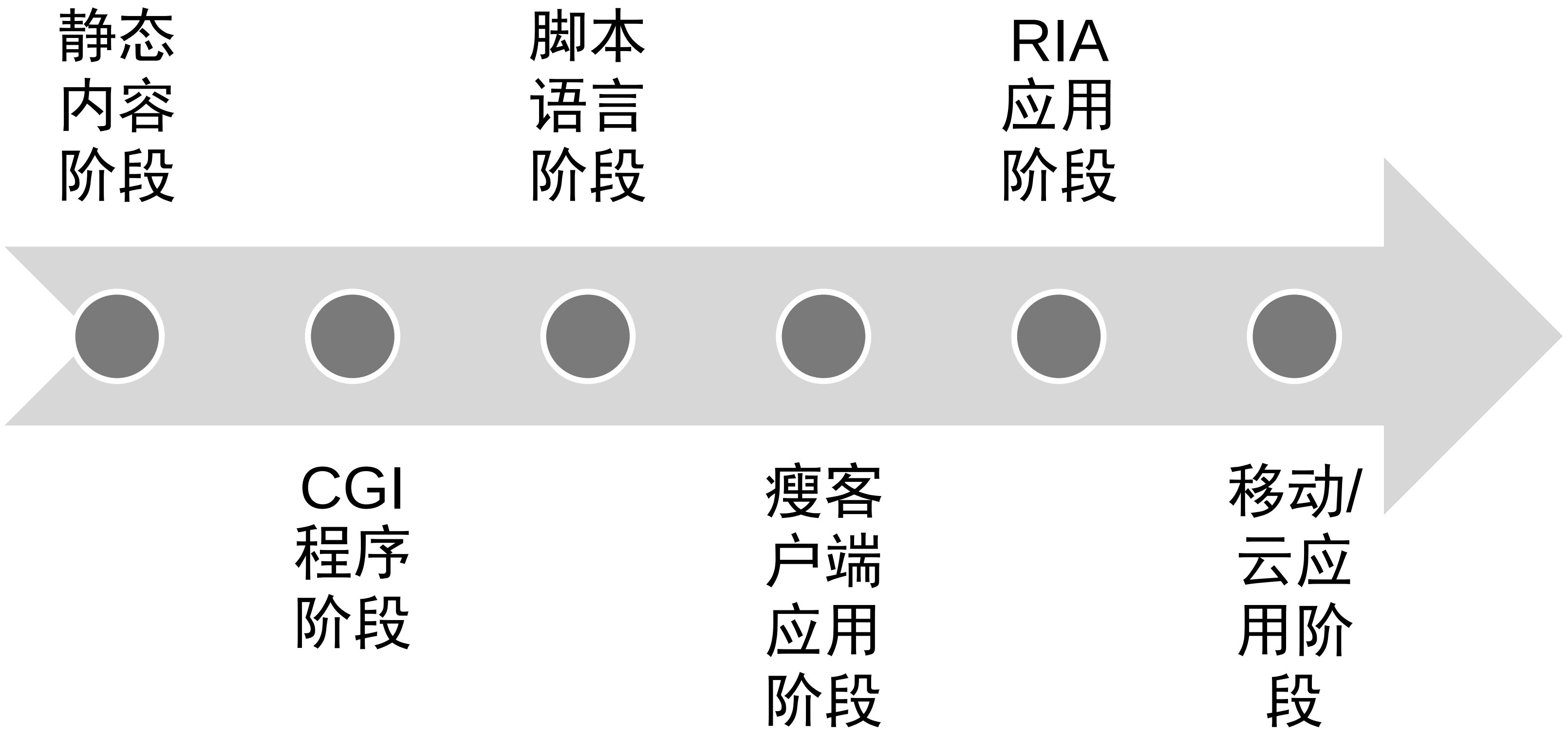


- 电子数据取证领域 15 年工作经验
- 参与设计/开发过一系列的工具产品
- ldh@forensix.cn

应用/网页取证

数据/主机取证

WEB 应用/网站的发展



静态内容阶段

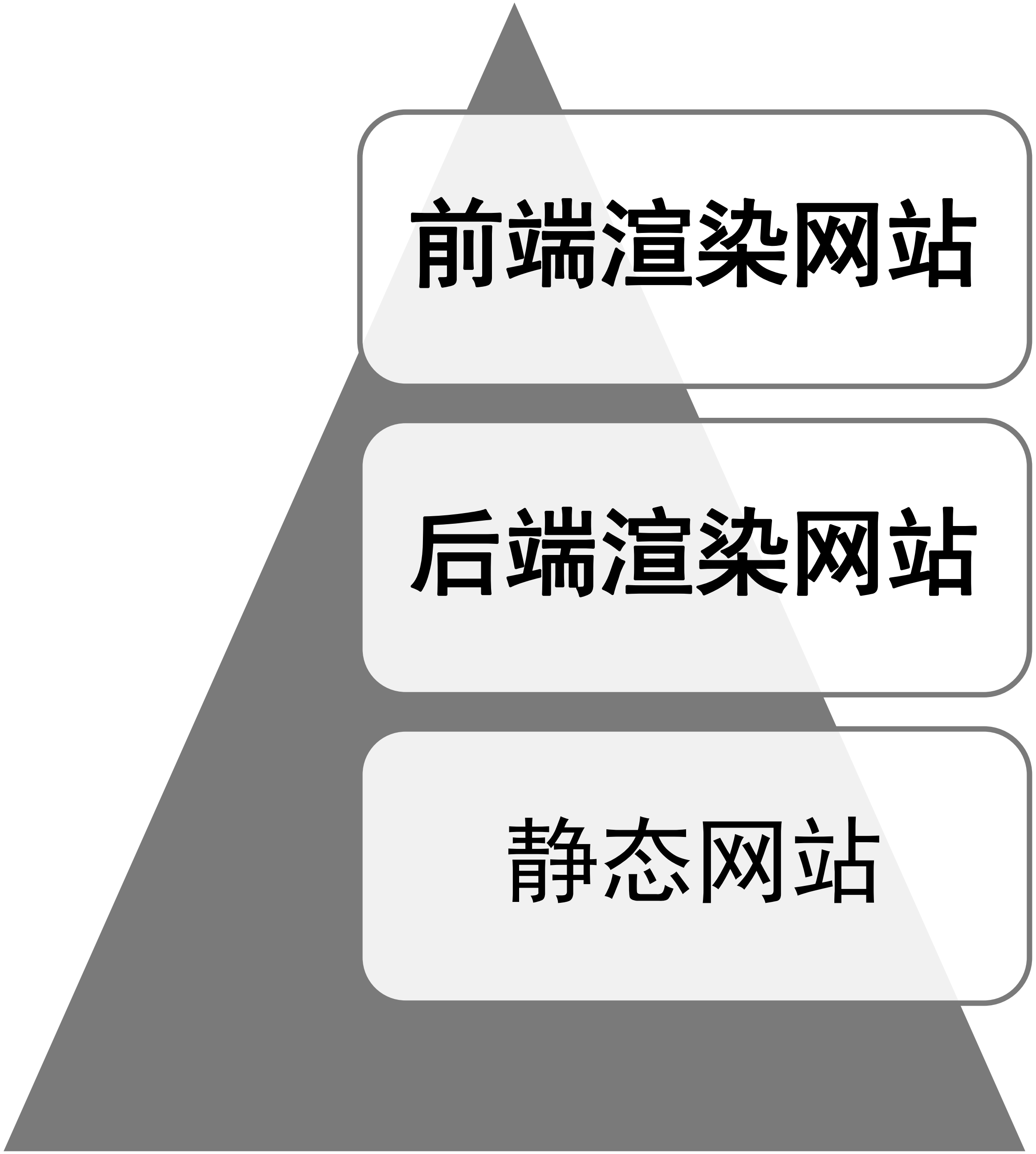
CGI程序阶段

脚本语言阶段

瘦客户端应用阶段

RIA应用阶段

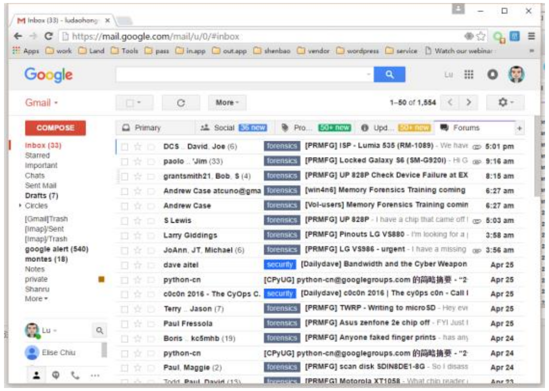
移动/云应用阶段



前端渲染网站

后端渲染网站

静态网站



DCS .. David, Joe (6)	forensics	[PRMFG] ISP - Lumia 535 (RM-1089) - We have	5:01 pm
paolo .. 'Jim (33)	forensics	[PRMFG] Locked Galaxy S6 (SM-G920I) - Hi G	9:16 am
grantsmith21, Bob, S (4)	forensics	[PRMFG] UP 828P Check Device Failure at EX	8:15 am
Andrew Case atcuno@gma	forensics	[win4n6] Memory Forensics Training coming	6:27 am
Andrew Case	forensics	[Vol-users] Memory Forensics Training comin	6:27 am
S Lewis	forensics	[PRMFG] UP 828P - I have a chip that came off	5:03 am
Larry Giddings	forensics	[PRMFG] Pinouts LG VS880 - I'm looking for a	3:58 am
JoAnn, JT, Michael (6)	forensics	[PRMFG] LG VS986 - urgent - I have a missing	3:56 am
dave aitel	security	[Dailydave] Bandwidth and the Cyber Weapon	Apr 25
python-cn		[CPyUG] python-cn@googlegroups.com 的简略摘要 - "2	Apr 25
c0c0n 2016 - The CyOps C.	security	[Dailydave] c0c0n 2016 | The cy0ps c0n - Call I	Apr 25
Terry .. Jason (7)	forensics	[PRMFG] TWRP - Writing to microSD - Hey eve	Apr 25
Paul Fressola	forensics	[PRMFG] Asus zenfone 2e chip off - FYI Just I	Apr 25
Boris .. kc5mhb (19)	forensics	[PRMFG] Anyone faked finger prints - has any	Apr 24
python-cn		[CPyUG] python-cn@googlegroups.com 的简略摘要 - "2	Apr 24
Paul, Maggie (2)	forensics	[PRMFG] scan disk SDIN8DE1-8G - So I disass	Apr 24
Todd, Paul, David (13)	forensics	[PRMFG] Motorola XT1058 - What chip reader	Apr 23

Comsenz 公司动态

Discuz! 程序发布
第一时间提供 Discuz! 论坛最新程序、升级补丁、转换程序的免费下载，请随时关注新版本动态。
版主: monkeye
76 / 2646
Comsenz 核心产品 Discuz! X3.2 ...
2016-6-1 10:36 monkeye

Discuz! 交流与讨论

Discuz!-插件
主题: 18万, 帖数: 267万
Discuz! F1.0 扩展 程序发布【R2 ... 15 分钟前 gzhxjkzx

Discuz!-模板 (3)
主题: 16万, 帖数: 302万
Discuz! F1.0 扩展 程序发布【R2 ... 15 分钟前 热血传

Discuz!-应用中心 (1)
主题: 839, 帖数: 4123
那你告诉我，我还有什么方法找回 ... 1 小时前 HAOFOB

Discuz!-开发者交流
主题: 312, 帖数: 1633
私密版块

Discuz!-安装使用 (3)
主题: 93万, 帖数: 728万
论坛数据库问题 11 分钟前 ayayaza

Discuz!-BUG反馈
主题: 6万, 帖数: 28万
点击提醒 消息 听众 管理工作 ... 昨天 17:32 2306974

关联技术专区

专用主机业务
私密版块

PHP技术讨论版
链接到外部地址

ECShop 交流与讨论
链接到外部地址

Discuz! 腾讯云
链接到外部地址

SQLAPI++ Library

SQLAPI++ is a C++ library for accessing multiple SQL databases (Oracle, SQL Server, DB2, Sybase, Informix, InterBase, SQLBase, MySQL, PostgreSQL, SQLite, SQL Anywhere and ODBC). It uses native APIs of target DBMS so applications developed with SQLAPI++ library run swiftly and efficiently. The product also provides a low-level interface that allows developers to access database-specific features. By encapsulating a vendor's API, SQLAPI++ library acts as middleware and delivers database portability. See details on supporting SQL database servers on different platforms:

Server	Windows	Linux/Unix
Oracle Database Server	Supported (OCI)	Supported (OCI)
Microsoft SQL Server	Supported (SQLNCLI/ODBC, OLE DB, DB-Library)	SQLNCLI/ODBC for Linux x86-64, otherwise ODBC driver and connection should be used (FreeTDS, Easysoft,...)
Sybase	Supported (Open Client, ASE & ASA)	Supported (Open Client, ASE & ASA)
DB2	Supported (DB2 CLI)	Supported (DB2 CLI)
Informix	Supported (Informix CLI)	Supported (Informix CLI)
InterBase/Firebird	Supported	Supported
SQLBase	Supported (CAPI)	Supported (CAPI)
MySQL, MariaDB	Supported (MySQL C API)	Supported (MySQL C API)
PostgreSQL	Supported (libpq)	Supported (libpq)
ODBC	Supported	Supported (iODBC, unixODBC)
SQLite	Supported	Supported
Sybase SQL Anywhere	Supported (SQL Anywhere C API)	Supported (SQL Anywhere C API)

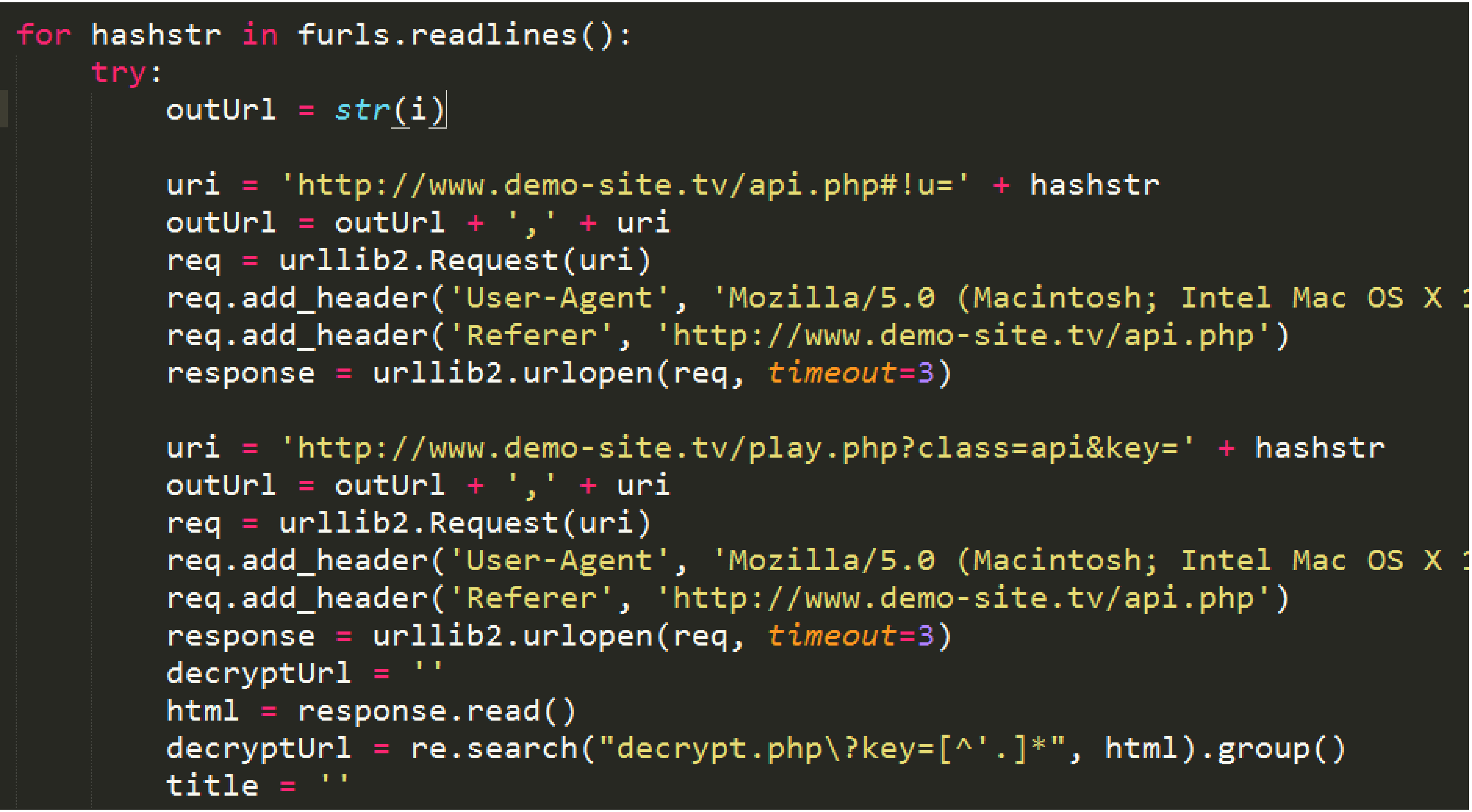
Currently SQLAPI++ library supports the following C/C++ compilers:

- Microsoft Visual C++
- Embarcadero (Borland) C++
- GNU GCC C++ compiler
- Solaris Studio C++ compiler

网页取证相关技术

- URI
- HTTP
- HTML
- MIME
- Chrome / JavaScript
- Fiddler / Charles
- IP/DNS
- Python / Node
- …

色情网站视频固定案例



```
for hashstr in furls.readlines():
    try:
        outUrl = str(i)

        uri = 'http://www.demo-site.tv/api.php#!u=' + hashstr
        outUrl = outUrl + ',' + uri
        req = urllib2.Request(uri)
        req.add_header('User-Agent', 'Mozilla/5.0 (Macintosh; Intel Mac OS X
        req.add_header('Referer', 'http://www.demo-site.tv/api.php')
        response = urllib2.urlopen(req, timeout=3)

        uri = 'http://www.demo-site.tv/play.php?class=api&key=' + hashstr
        outUrl = outUrl + ',' + uri
        req = urllib2.Request(uri)
        req.add_header('User-Agent', 'Mozilla/5.0 (Macintosh; Intel Mac OS X
        req.add_header('Referer', 'http://www.demo-site.tv/api.php')
        response = urllib2.urlopen(req, timeout=3)
        decryptUrl = ''
        html = response.read()
        decryptUrl = re.search("decrypt.php\?key=[^'.]*", html).group()
        title = ''
```

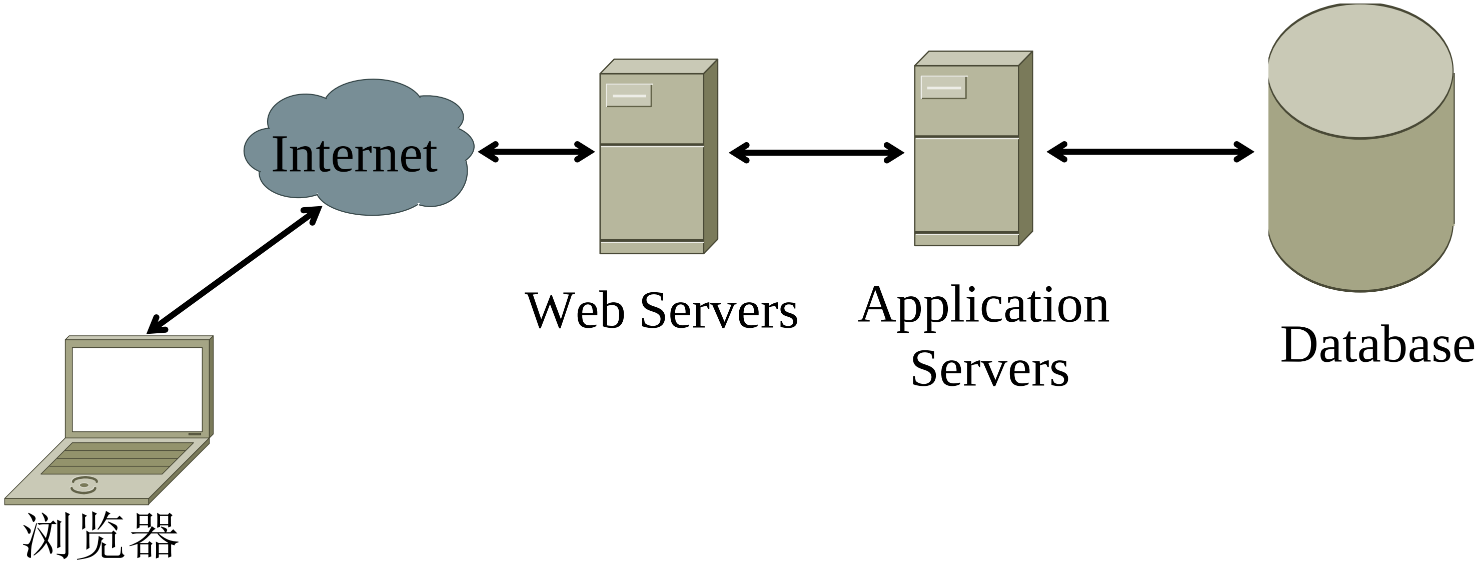
网站 / 数据库 / 日志 / 关联 / ...

配置

网站文件

日志

数据库



Internet

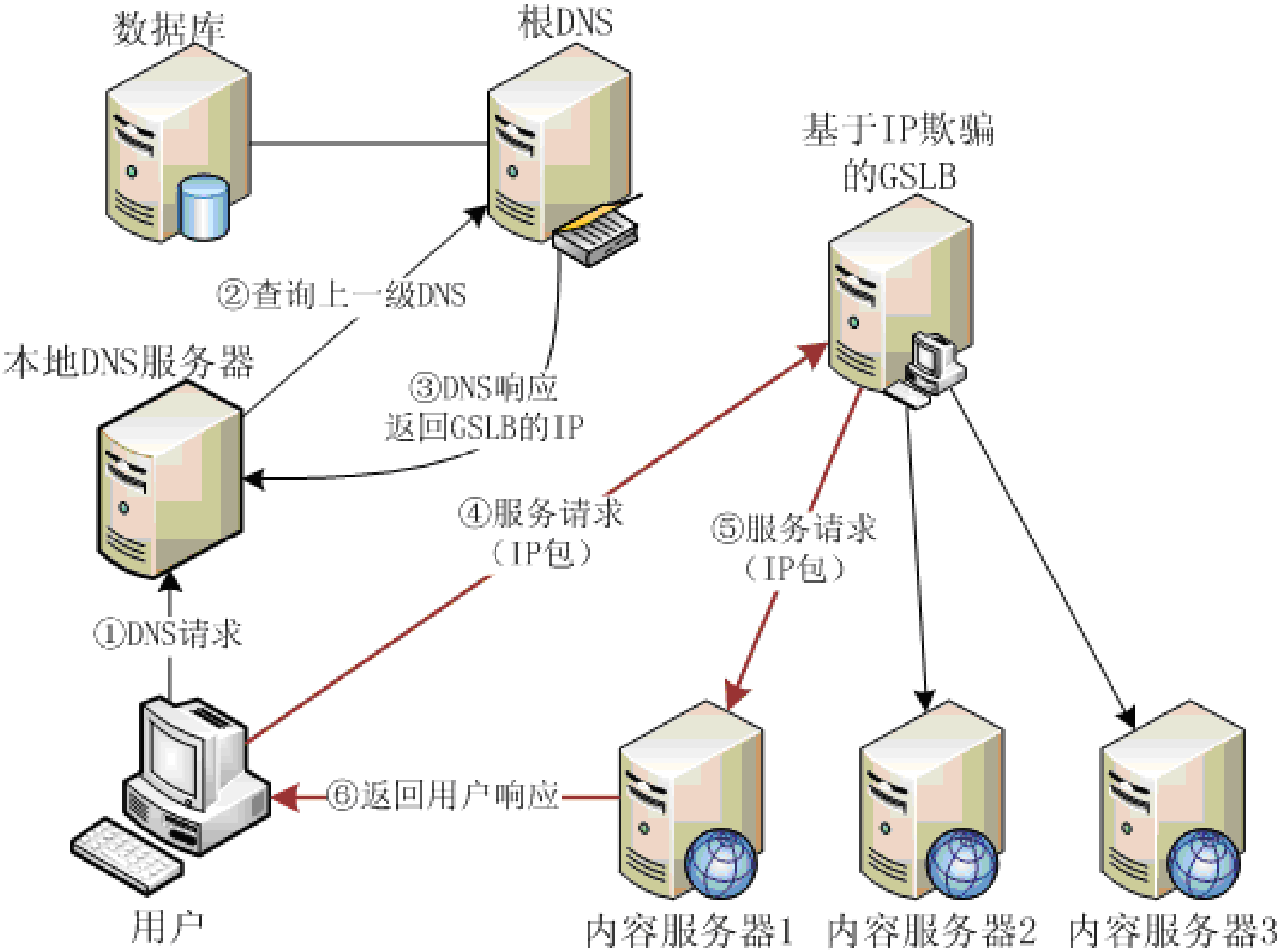
Web Servers

Application Servers

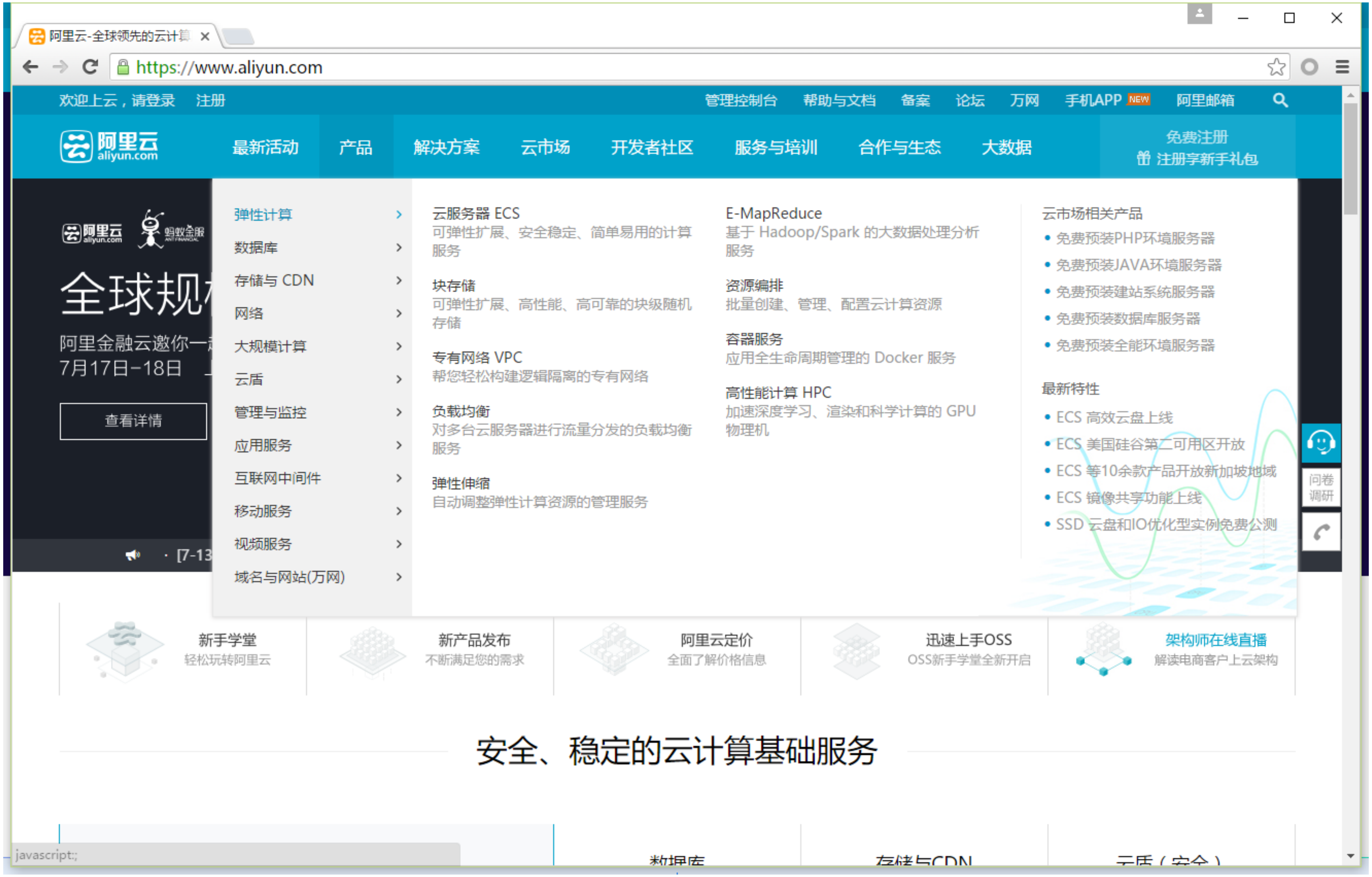
Database

浏览器

网站架构的复杂性


数据库
根DNS
基于IP欺骗
的GSLB
②查询上一级DNS
本地DNS服务器
③DNS响应
返回GSLB的IP
④服务请求
（IP包）
⑤服务请求
（IP包）
①DNS请求
⑥返回用户响应
用户
内容服务器1
内容服务器2
内容服务器3

云服务模式和挑战



阿里云-全球领先的云计算 ×

https://www.aliyun.com

欢迎上云，请登录 注册

管理控制台 帮助与文档 备案 论坛 万网 手机APP NEW 阿里邮箱

阿里云 aliyun.com

最新活动 产品 解决方案 云市场 开发者社区 服务与培训 合作与生态 大数据

免费注册
注册享新手礼包

阿里云 蚂蚁金服

全球规

阿里金融云邀你一
7月17日-18日

查看详情

[7-13

- 弹性计算 >
- 数据库 >
- 存储与 CDN >
- 网络 >
- 大规模计算 >
- 云盾 >
- 管理与监控 >
- 应用服务 >
- 互联网中间件 >
- 移动服务 >
- 视频服务 >
- 域名与网站(万网) >

云服务器 ECS
可弹性扩展、安全稳定、简单易用的计算服务

块存储
可弹性扩展、高性能、高可靠的块级随机存储

专有网络 VPC
帮您轻松构建逻辑隔离的专有网络

负载均衡
对多台云服务器进行流量分发的负载均衡服务

弹性伸缩
自动调整弹性计算资源的管理服务

E-MapReduce
基于 Hadoop/Spark 的大数据处理分析服务

资源编排
批量创建、管理、配置云计算资源

容器服务
应用全生命周期管理的 Docker 服务

高性能计算 HPC
加速深度学习、渲染和科学计算的 GPU 物理机

云市场相关产品
- 免费预装PHP环境服务器
- 免费预装JAVA环境服务器
- 免费预装建站系统服务器
- 免费预装数据库服务器
- 免费预装全能环境服务器

最新特性
- ECS 高效云盘上线
- ECS 美国硅谷第二可用区开放
- ECS 等10余款产品开放新加坡地域
- ECS 镜像共享功能上线
- SSD 云盘和IO优化型实例免费公测

问卷调研

新手学堂
轻松玩转阿里云

新产品发布
不断满足您的需求

阿里云定价
全面了解价格信息

迅速上手OSS
OSS新手学堂全新开启

架构师在线直播
解读电商客户上云架构

安全、稳定的云计算基础服务

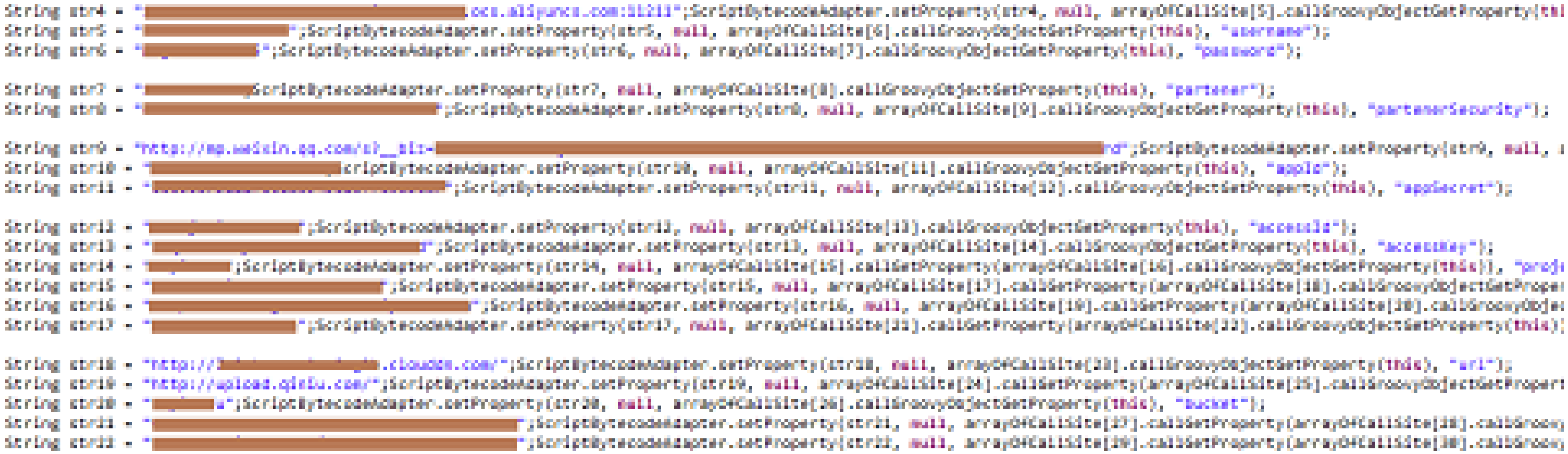
数据库 存储与CDN 云盾（安全）

javascript:;

网站/服务器取证技术

- HTTP / HTML/MIME
- JavaScript / AJAX
- PHP/ASP/…
- APACHE / IIS
- MSSQL / MySQL
- 日志分析
- Web 安全
- CDN / Cloud
- …

最近案例



```
String str4 = "[redacted].ocs.aliyuncs.com:11211";ScriptBytecodeAdapter.setProperty(str4, null, arrayOfCallSite[5].callGroovyObjectGetProperty(thi
String str5 = "[redacted]";ScriptBytecodeAdapter.setProperty(str5, null, arrayOfCallSite[6].callGroovyObjectGetProperty(this), "username");
String str6 = "[redacted]";ScriptBytecodeAdapter.setProperty(str6, null, arrayOfCallSite[7].callGroovyObjectGetProperty(this), "password");

String str7 = "[redacted]ScriptBytecodeAdapter.setProperty(str7, null, arrayOfCallSite[8].callGroovyObjectGetProperty(this), "partener");
String str8 = "[redacted]";ScriptBytecodeAdapter.setProperty(str8, null, arrayOfCallSite[9].callGroovyObjectGetProperty(this), "partenerSecurity");

String str9 = "http://mp.weixin.qq.com/s?__biz=[redacted]rd";ScriptBytecodeAdapter.setProperty(str9, null, a
String str10 = "[redacted]criptBytecodeAdapter.setProperty(str10, null, arrayOfCallSite[11].callGroovyObjectGetProperty(this), "appId");
String str11 = "[redacted]";ScriptBytecodeAdapter.setProperty(str11, null, arrayOfCallSite[12].callGroovyObjectGetProperty(this), "appSecret");

String str12 = "[redacted]";ScriptBytecodeAdapter.setProperty(str12, null, arrayOfCallSite[13].callGroovyObjectGetProperty(this), "accessId");
String str13 = "[redacted]";ScriptBytecodeAdapter.setProperty(str13, null, arrayOfCallSite[14].callGroovyObjectGetProperty(this), "accessKey");
String str14 = "[redacted];ScriptBytecodeAdapter.setProperty(str14, null, arrayOfCallSite[15].callGetProperty(arrayOfCallSite[16].callGroovyObjectGetProperty(this)), "proj
String str15 = "[redacted]";ScriptBytecodeAdapter.setProperty(str15, null, arrayOfCallSite[17].callGetProperty(arrayOfCallSite[18].callGroovyObjectGetPrope
String str16 = "[redacted]";ScriptBytecodeAdapter.setProperty(str16, null, arrayOfCallSite[19].callGetProperty(arrayOfCallSite[20].callGroovyObje
String str17 = "[redacted]";ScriptBytecodeAdapter.setProperty(str17, null, arrayOfCallSite[21].callGetProperty(arrayOfCallSite[22].callGroovyObjectGetProperty(this)

String str18 = "http://[redacted].clouddn.com/";ScriptBytecodeAdapter.setProperty(str18, null, arrayOfCallSite[23].callGroovyObjectGetProperty(this), "url");
String str19 = "http://upload.qiniu.com/";ScriptBytecodeAdapter.setProperty(str19, null, arrayOfCallSite[24].callGetProperty(arrayOfCallSite[25].callGroovyObjectGetPropert
String str20 = "[redacted]";ScriptBytecodeAdapter.setProperty(str20, null, arrayOfCallSite[26].callGroovyObjectGetProperty(this), "bucket");
String str21 = "[redacted]";ScriptBytecodeAdapter.setProperty(str21, null, arrayOfCallSite[27].callGetProperty(arrayOfCallSite[28].callGroov
String str22 = "[redacted]";ScriptBytecodeAdapter.setProperty(str22, null, arrayOfCallSite[29].callGetProperty(arrayOfCallSite[30].callGroov
```

云数据库 Memcache

云数据库 Memcache 版（ ApsaraDB for Memcache ）是一种高性能、高可靠、可平滑扩
库服务。基于淘宝分布式系统Tair和纯内存的高性能存储，为热点数据访问提供高速响应，
监控、迁移等方面的全套数据库解决方案。

参与NOSQL产品调研，赢取阿里云优惠券

云数据库 RDS

云数据库RDS（ApsaraDB for RDS，简称RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于飞天分
式系统和全SSD盘高性能存储，支持MySQL、SQL Server、PostgreSQL和PPAS（高度兼容Oracle)引擎，默
部署主备架构且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案，彻底解决数据库运维的烦恼！

购RDS享免费全量迁移服务 >>
SQL Server 2012基础版免费公测 >>
RDS独占物理机，资源专享，性能强劲，现在购买或升级即返15%代金券！ >>

陆道宏

ldh@forensix.cn