

# 本章内容安排

---

- **3.1 Web安全概述**
- **3.2 Web服务器指纹识别**
- **3.3 跨站脚本攻击及防御**
- **3.4 SQL注入攻击及防御**
- **3.5 Google Hacking**
- **3.6 防御Web攻击**
- **3.7 小结**



# 3.1 Web安全概述

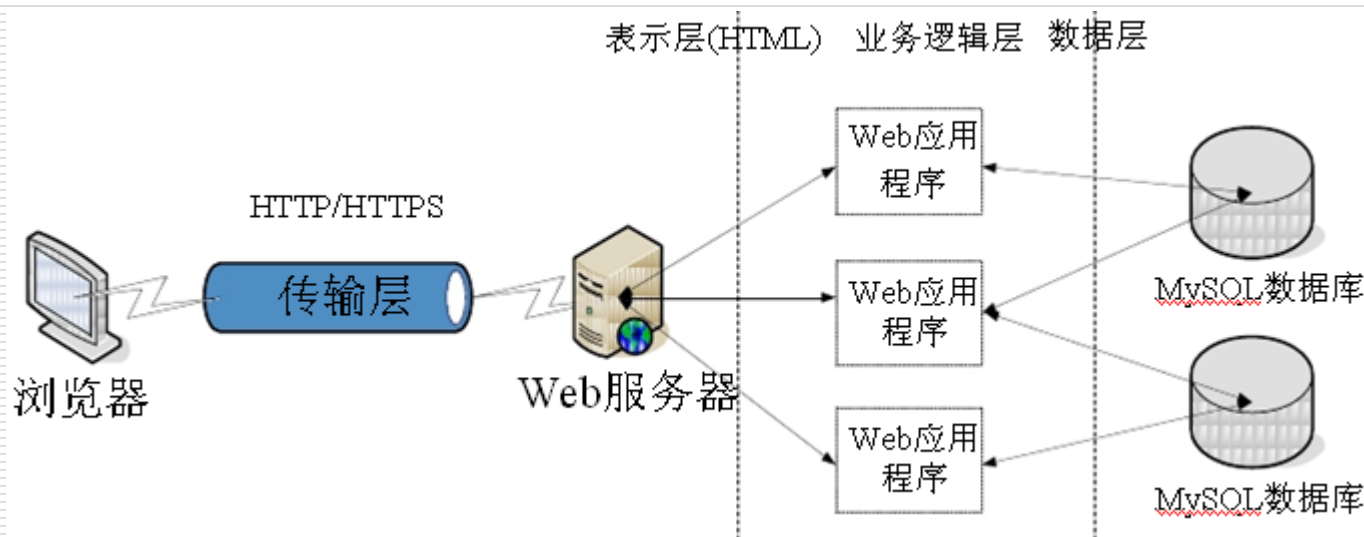
---

- **OWASP**的调查显示，对**Web**应用危害较大的安全问题分别是：
  - 未验证参数
  - 访问控制缺陷
  - 账户及会话管理缺陷
  - 跨站脚本攻击
  - 缓冲区溢出
  - 命令注入
  - 错误处理
  - 远程管理
  - **Web**服务器及应用服务器配置不当

# Web应用体系结构

## □ 传统C/S架构——B/S架构

- “瘦”客户端：**Browser (Web客户端)**
- “厚”服务器：**Web服务器、Web应用程序、数据库...**
- 通讯机制：**HTTP/HTTPS**



# Web安全

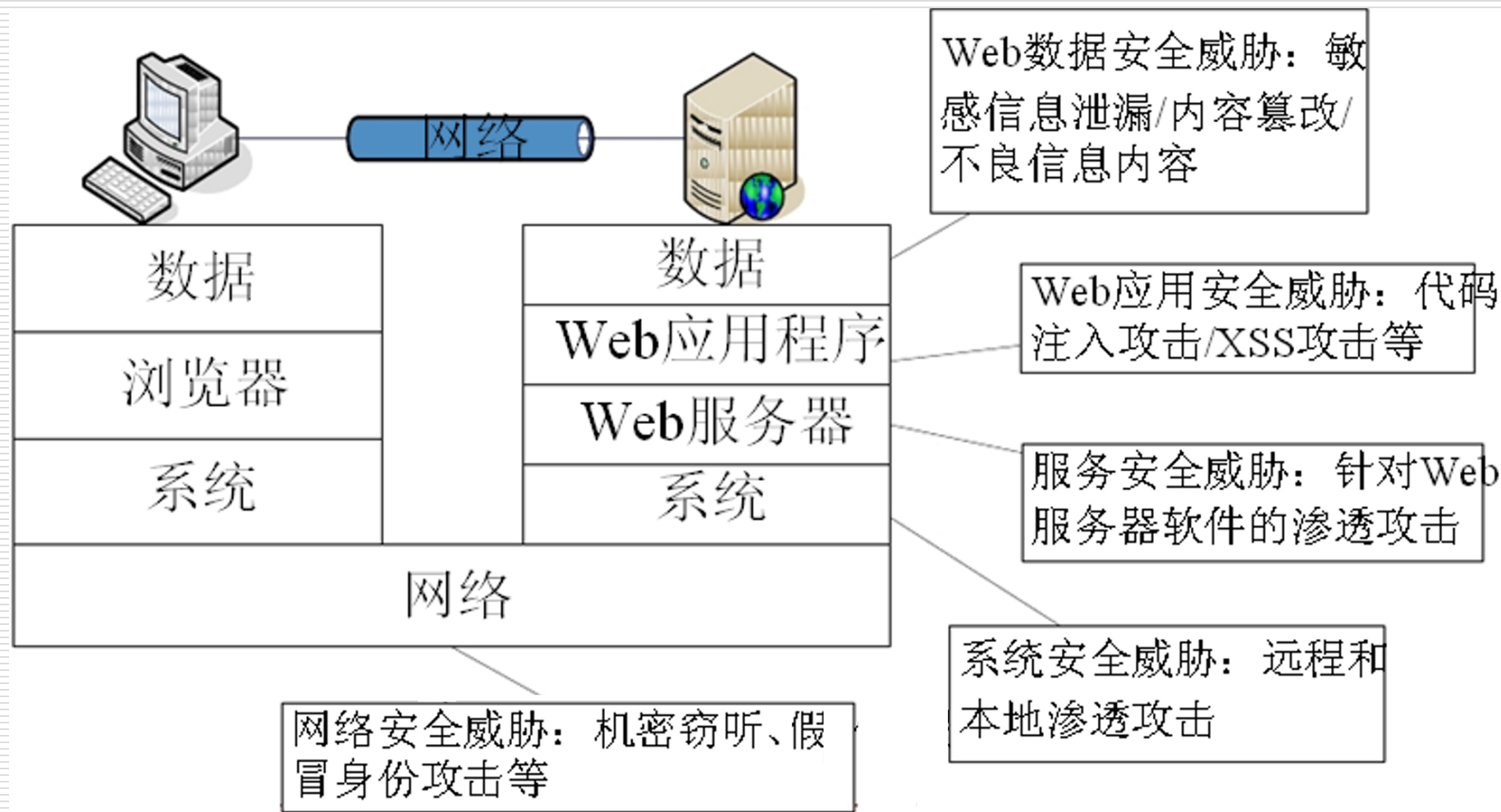
---

□ **Web安全**可以从以下三个方面进行考虑：

- Web服务器的安全
- Web客户端的安全
- Web通信信道的安全



# Web安全威胁



# Web服务器的安全

---

## □ 针对**Web**服务器的攻击可以分为三类：

- 一是利用**Web服务器的漏洞**进行攻击，如IIS缓冲区溢出漏洞利用、目录遍历漏洞利用等；
- 二是利用**Web应用程序自身的安全漏洞**进行攻击，如SQL注入，跨站脚本攻击等。
- 三是针对**Web服务器上的数据**进行攻击，如篡改数据，敏感信息泄露等。

# Web应用攻击路线图

---

- **Web**应用信息收集
- 攻击**Web**服务器软件
- 攻击**Web**应用程序
- 攻击**Web**数据内容
- 本地攻击

# (1) Web应用的信息收集

---

- 针对目标**Web**应用服务的信息收集
  - 服务器域名、**IP**地址、内网虚拟**IP**地址
  - **Web**服务器端口、其他开放服务
  - **Web**站点类型与版本
  - **Web**应用程序类型与版本
  - **Web**服务器 / **Web**应用程序中存在的安全漏洞
  
- 网络信息收集技术
  - **Whois** / **DNS**查询、**Web**搜索、端口扫描：发现目标**Web**站点
  - 类型探查技术：识别**Web**站点**OS**、服务器类型版本
  - 漏洞扫描技术：**Web**站点与服务器软件已知漏洞
  - 服务查点技术：**Web**服务器软件的“旗标”



## (2) 攻击**Web**服务器软件

---

- 流行的**Web**服务器软件
  - **MS: Win200x Server / IIS / MS SQL / ASP / ASP.NET**
  - **LAMP: Linux / Apache / MySQL / PHP**
  
- 针对**Web**服务器网络服务的远程渗透攻击
  - **IIS / MS SQL: 红色代码、尼姆达和SQL Slammer**
  - 已知漏洞渗透代码来源: **Metasploit、Exploit-db、Packetstorm、SecurityFoucs**

# Web服务器平台中的安全漏洞(1)

---

- 数据驱动的远程代码执行安全漏洞
  - 缓冲区溢出
  - **IIS HTR**数据块编码堆溢出漏洞攻击
  - **Microsoft IIS ASP**远程代码执行漏洞(**MS08-006**)
  
- 服务器功能扩展模块漏洞
  - **IIS**软件中被红色代码所利用的**IIS**检索服务缓冲区溢出漏洞
  - **WebDAV**模块**Translate:f**漏洞
  - **Apache**扩展组件模块漏洞，如**Tomcat**、**OpenSSL**、**mod\_rewrite**、**mod\_mylo**、**mod\_gzip**、**mod\_isapi**、**mod\_jk**

# Web服务器平台中的安全漏洞(2)

---

## □ 样本文件

- **Web**应用服务器包含的样板脚本和代码示例存在漏洞

- 案例: **IIS4**中的**showcode.asp**存在目录便利漏洞

- **http://SERVER/msadc/Samples/SELECTOR/showcode.asp?source=../../../boot.ini**

## □ 源代码泄露

- 能够查看到没有防护措施**Web**服务器上的应用程序源码

- 案例: **IIS**上的“**+.htr**”漏洞

- **http://SERVER/global.asa+.htr**

## □ 资源解析攻击

- 资源解析: 把同一资源的不同表示形式解析为它的标准化名称的过程.

- **C:\text.txt = ..\text.txt = \\computer\C\$\text.txt**

- 案例: **IIS**中的“**ASP::\$DATA**”漏洞

- **http://SERVER/scripts/file.asp::\$DATA**: 查看源码

# (3) 攻击Web应用程序

---

## □ Web应用程序的不安全性

- Web应用程序编码质量和测试均有限: 安全最薄弱环节
- Web应用的复杂性和灵活性进一步恶化了其安全性

## □ Web应用程序安全威胁类型

- WASC(Web Application Security Consortium)
- 针对认证机制的攻击
- 针对授权机制的攻击
- 客户端攻击
- 命令执行攻击
- 信息暴露
- 逻辑攻击

# Web应用程序安全漏洞类型列表

安全弱点	攻击技术	攻击技术 (续)
应用程序错误配置	功能滥用	空字节注入
目录列举	暴力枚举	操作系统命令注入
不恰当的文件系统权限	缓冲区溢出	路径遍历
不恰当的输入处理	内容欺骗	资源位置可预测
不恰当的输出处理	信任/会话预测	RFI 远程文件包含
信息泄露	XSS 跨站脚本	路由劫持
不安全的索引	CSRF 跨站请求伪造	会话身份窃取攻击
对抗自动程序不完善	拒绝服务	SOAP 数组滥用
认证机制不完善	指纹探测识别	SSI 注入
授权机制不完善	格式化字符串	SQL 注入
口令恢复机制不完善	HTTP 响应私运	URL 重定向机制滥用
处理验证过程不完善	HTTP 响应割裂	XPath 注入
会话失效机制不完善	HTTP 请求私运	XML 属性爆破攻击
传输层保护不完善	HTTP 请求割裂	XML 外部实体攻击
服务器误配置	整数溢出	XML 实体扩展攻击
	LDAP 注入	XML 注入
	邮件命令注入	XQuery 注入

# CGI漏洞攻击举例

---

- 某个**CGI**脚本打印**PATH\_INFO**中引用的文件

```
#!/bin/sh
#Send the header
echo "Content-type: text/html"
echo ""
echo "<HTML><HEADER><TITLE>File</TITLE><HEADER><BDOY>"
echo "Here is the file you requested:<PRE>\n"
cat $PATH_INFO
echo "</PRE></BODY></HTML>"
```

一个恶意的用户可能会输入:

`http://www.server.com/cgi-bin/foobar.sh/etc/passwd`

这样这脚本就会返回机器的口令文件

# ASP的安全性

---

## □ (1)ASP程序的安全

- ASP类似CGI，由程序代码实现，通过表单实现与用户的交互，这样一些Web服务器的内容会通过URL反映到浏览器，如果不采取相应的措施，就可能被非法利用

## □ (2) 数据库的存储

- 在Web下的数据库管理中，数据库的存储应该具有首要的安全等级。由于ASP网页访问同样通过URL，如果数据库文件存储在默认Web站点下，就有可能被客户端非法下载

## (4) 攻击**Web**数据内容

---

- 安全敏感信息泄露
- 网站内容篡改
- 不良信息内容上传



# 敏感信息泄漏

---

## □ 敏感信息类型

- **GF、BM**等科研敏感信息
- 教师、学生个人隐私信息
- 网络安全敏感信息

## □ 通常的信息泄漏途径和方式

- 未关闭**Web**服务器的目录遍历，不经意泄漏
- **Upload、Incoming**等目录中转文件时泄漏
- 缺乏安全意识，在公开的文档中包含个人隐私信息
- 在公开的个人简历、职称晋升材料、课题申请书等包含科研敏感信息

# 高校网站泄漏科研敏感信息实例

[DOC] 长春理工大学

文件格式: Microsoft Word - HTML 版

25、炮塔[REDACTED]热处理技术GF报告. 25、复杂结构件[REDACTED]熔覆技术GF报告. 26、复杂结构件[REDACTED]熔覆技术GF报告. 27、复杂结构件[REDACTED]及 ...

rsc[REDACTED].edu.cn/rsc\_new/upimages/2006[REDACTED]81.doc

长 春 理 工 大 学

2006 年评聘专业技术职务人员工作业绩表

部 门	机电工程学院	姓 名	[REDACTED]	性别	
民 族	满	出生年月	19[REDACTED]3	参加工作时间	
现工作岗位	教师	担任党政职务			
申报专业技术资格所依据学历及毕业时间	大学本科 1995年7月 硕士研究生 2002年4月				

8、复杂结构件[REDACTED]熔覆技术GF报告. 9、炮塔[REDACTED]热处理技术GF报告.

总装部、国家级、100万元 (项目编号: 41[REDACTED]2) 排第[REDACTED]  
兵器工业集团公司、部级、30万元 (项目编号: 40[REDACTED]02) 排第[REDACTED]

25、炮塔[REDACTED]熔覆技术GF报告.	2002年11月.
25、复杂结构件[REDACTED]熔覆技术GF报告.	2002年11月.
26、复杂结构件[REDACTED]熔覆技术GF报告.	2003年11月.
27、复杂结构件[REDACTED]熔覆技术GF报告.	2004年12月.
28、复杂结构件[REDACTED]熔覆技术GF报告.	2005年12月.
29、数控[REDACTED]编程与实验指导书.	2003年、2005年.
30、粉末冶金摩擦片[REDACTED]	国防专利、申请号 20041[REDACTED].9.

[DOC] 一周课程:

文件格式: Microsoft Word - HTML 版

2006.12-2008.12 主持总参通信部6904工厂“XXXX系统技术维护与升级改造”项目。 2003.7-2004.8，作为技术骨干参加总装预研“XXXX应用系统”项目。 ...

dean.pku.edu.cn/notice/upload/2009年暑期学校手册.doc

[DOC] 2007年度陕西省级精品课程申报表

文件格式: Microsoft Word - HTML 版

无人机数据链高抗干扰技术，总装十一五预研项目，编号51325040401，2007年经费8万元，将于2007.4和2007.12分两期到款，负责人。 ●2006CJ080002，超宽带无人机数据链 ...

jkpc.nwpu.edu.cn/jp2007/15/shenbaocailiao.doc

[DOC] 项目申报表 - 附件3:

文件格式: Microsoft Word - HTML 版

1) 863项目: 某型号集成处理器测试仿真系统研制, 2007.05~2008.05, 经费: 169万元, 技术负责人; 2) 总装预研: 基于SVM的智能故障诊断系统技术 ...

sy.zlgc.edu.cn/upload/20080522220916228.doc

# 网页内容篡改

## □ 2008年9月：北大/清华网站被黑，假冒校长发文

2008-09-28 06:52

### 北大网站被黑 假冒校长发文

与一个月前清华网站被黑如出一辙 怀疑出自同一“黑手” 北大方面强烈谴责

北青网 - 北京青年报：雷夏 (08/09/28 04:00)

本报报道 继一个月前清华大学网站被黑客攻击后，26日23时左右，北京大学的网站也遭到了“黑手”，网站上出现了一篇冒充北大校长许智宏名义抨击大学教育的文章，这与一个月前清华网站被黑时出现的假借清华校长顾秉林之名批评高等教育现状的文章如出一辙，不免令人怀疑出自同一“黑手”。北大新闻中心昨天发表声明，对此行为表示强烈谴责。

[](http://rec.ynet.com/adclick.php?n=ab22e4d2)

记者获悉，在26日22点半左右，北大校园网站就不能正常登录了，同学中有传言说校园网被黑客攻击了。虽然北大网站很快恢复正常，但被黑时出现在网站上的一篇文章却已经在网上流传开来。一名北大学生告诉记者，网上流传的这篇冒充北大校长许智宏名义的文章《大学教育，反思还是腐烂？》，就是黑客捏造并贴在校网上的。这篇1600多字的文章以许智宏校长的口气，评论了清华大学网站被黑客入侵事件。对所谓顾秉林校长批评高等教育现状的文章，评论说：“如果这真的是顾校长的意思，那么我佩服他。同样身为大学校长，很惭愧，我是没有勇气说这些话的。”文章对大学校园文化、高等教育现状进行了抨击，还提出三点所谓“改革建议”：“一是废除或减少政治类课程；二是加强传统道德文化教育，让学生重塑传统道德价值观；三是‘清理门户’，将一些以教授的名义长期盘踞在大学校园里的无德无能之辈清理出去……”

昨天早晨，北京大学网站已经恢复正常。网站首页上有北大新闻中心的一则声明：“9月26日晚23时09分，北京大学校园网主页遭到别有用心人的恶意攻击和篡改。假借许智宏校长名义的错误文章，混淆视听，性质恶劣。北京大学新闻中心对此表示强烈谴责！”

8月24日，清华大学网站也曾遭到黑客攻击。当时清华网站的“清华新闻”栏目中出现一篇文章：《中国大学教育就是往脑子里灌屎》，是假冒清华校长顾秉林的名义发表的。文章也对大学教育方式、学术腐败等问题进行了抨击，但由于言辞粗俗，一眼就可看出是黑客杜撰。事件发生次日，清华大学也曾发表声明，澄清所谓顾秉林校长的文章是黑客捏造，清华对此表示愤慨。

# 网页篡改站点列表

ne-h.com.cn/?key=edu.cn&mode=domain&Submit=+Search+

ZONE-H.COM.CN

China Hacked Submit

中国被黑站点统计系统

Search: edu.cn

提交者 组织名 IP 域名 精确

Search

黑页提交

中国被黑站点统计0609分析报告



黑客任务www.hacktask.com

点击这里!免费加入黑客人才库

TOP50 User	时间	提交者	页面	查看快照
NO1:23026583[4936]	2010-09-04	☆烟/nc愁☆	http://jzt.gdce.edu.cn/UplodThumbs/201093221636552.asp	快照
NO2:ev[2843]	2010-09-04	☆烟/nc愁☆	http://jiuye.nxvtu.edu.cn/admin/passt.asp	快照
NO3:用幸福耐侯...[2351]	2010-09-02	DragonEgg	http://xshe.sxnu.edu.cn/test.htm	快照
NO4:霸世永峰[1661]	2010-08-27	叨叨喵喵	http://www.jku.edu.cn/about/zywx/js/dd.txt	快照
NO5:八神[1551]	2010-08-25	DragonEgg	http://kygl.zzia.edu.cn/News/admin/admin_new.asp	快照
NO6:网络小子[1271]	2010-08-23	流浪汉	http://jiguan.gzhnc.edu.cn/1.txt	快照
NO7:寒水芊芊[1095]	2010-08-23	黑冰网络残总	http://kerx.szlg.edu.cn/cange520.asp	快照
NO8:糊涂工作室[1076]	2010-08-22	流浪汉	http://www.gxx.xcvtc.edu.cn/djtx.htm	快照
NO9:波哥VS布冯[1075]	2010-08-21	tsinghua	http://www.enr.tsinghua.edu.cn/upfile/tact.asp	快照
NO10:木鱼工作室[1039]	2010-08-19	小黑	http://www.gznc.edu.cn/uploadfile/xh.htm	快照
NO11:Timeless[1023]	2010-08-18	帅气凌云	http://jisuanji.jyu.edu.cn/shuishougailun/appic/volf.asp	快照
NO12:红领巾冲封心[875]	2010-08-17	帅气凌云	http://jkb.sut.edu.cn/add/s.html	快照
NO13:Cracker-Nr.X[858]	2010-08-16	Troten	http://www.blcu.edu.cn/hyxy/web/Lus/appic/tro.htm	快照
NO14:MacKerCe[830]	2010-08-14	icebm	http://lun.ywc.edu.cn/icebm.htm	快照
NO15:黑羽...燃[816]				
NO16:电脑迷[786]				
NO17:hackxy[709]				
NO18:黑侠[706]				
NO19:Mr.stakes[696]				

# 网页篡改站点列表(2)

www.zone-h.org/archive

英文 ▾ 网页, 是否需要翻译? 翻译 否

Home News Events Archiv

NOTIFIER

Date : ALL ▾ 01 ▾

Total notifications: 3662 of w

Legend:  
H - Homepage defacement  
M - Mass defacement (click to  
R - Redefacement (click to vie  
★ - Special defacement (spec

Mirror saved on: 2010-09-06 13:17:02

Notified by: 1923Turk  
System: Win 2003

Domain: <http://sbdllx.kmyz.edu.cn>  
Web server: IIS/6.0

IP address: 222.56.21.67  
[Notifier stats](#)

Hacked By **KADAVRA** 1923Turk Grup

Mevzu-u Bahis Vatan ise Gerisi Teferruattur.

[iletigilnicadavra.hack@hotmail.com](mailto:iletigilnicadavra.hack@hotmail.com)

\*2010 1923Turk-Grup.

Time	Notifier	H M R ★	Domain	OS	View
2010/09/08	Uxor		power.dlut.edu.cn/cn_index.php	Linux	<a href="#">mirror</a>
2010/09/08	Hmei7		www2.qnu.edu.cn/indonesia.txt	Win 2003	<a href="#">mirror</a>
2010/09/07	Kam_06	H	organic.sjtu.edu.cn	Linux	<a href="#">mirror</a>
2010/09/07	1923Turk	H M	jjxyl.kmyz.edu.cn	Win 2003	<a href="#">mirror</a>
2010/09/07	1923Turk	H M	jsjic.kmyz.edu.cn	Win 2003	<a href="#">mirror</a>
2010/09/07	1923Turk	H M	sbdllx.kmyz.edu.cn	Win 2003	<a href="#">mirror</a>
2010/09/07	1923Turk	H M	zdjjxyl.kmyz.edu.cn	Win 2003	<a href="#">mirror</a>
2010/09/07	1923Turk	M	zhyy.kmyz.edu.cn/index_.aspx	Win 2003	<a href="#">mirror</a>
2010/09/07	1923Turk	H M	wlxt.kmyz.edu.cn	Win 2003	<a href="#">mirror</a>



# 不良信息内容上传威胁

## □ 网站面临的不良信息内容威胁

- 网站被攻陷后可能成为不良信息的存储和中转仓库
- 提供用户交互的论坛/博客等网站可能涉及用户上传不良信息

### 校园网络色情泛滥海南高校积极应对

来源：海南经济报 2007-6-21 14:39:00

本报讯（实习记者 吴文霞）近日，海口警方依法开展打击网络淫秽从海南某大学网站中查出2万3千余条有害信息。记者近日走访海少高校都采取了各种积极措施抑制色情信息在校园网络中“泛滥”，

海南师范大学网络中心刘主任告诉记者，该校的网络中心员工，工俭学的学生，这些人负责管理网站病毒的“清理”、技术维护等。

海南大学的宣传部王部长说，校园网站中的信息，其来源都是通。海南广播电视大学的杨主任告诉记者，该学校的网站论坛实行学学生的学号、身份证、密码才等登陆学校的论坛。学生如果发布色情技“搜索”，将会从严处理。

海南电大杨主任说，学校的网络需要经费的支持，由于经费不多资金也少，这对管理维护不利。

### 校园警世：校园情色在沉沦之后的反省

<http://campus.soul.cn> 2009-10-30 【群组讨论】 【进入论坛】

关键词：校园情色 女生宿舍 情色小说 三级片 A片 性 色情小说

字体：大 中 小

曾经安在职业网 周末开班！

读石油大学远程教育 通过率98%

百度推广



- 2010教师资格证报名
- 师范生招聘信息库
- 师范生招聘面试指南
- 求职面试问答 面试大全
- 求职简历封面 简历模板
- 2010年大学生新春祝福

2010年  
实习生招聘

### 校园警世：性其实不过如此--校园情色在沉沦之后的反省

校园情侣的界限哦我、寝室卧谈的“荤段子”、网络资讯的泛滥在当今校园大行其道且有愈演愈烈之势，身处其境的“落单一族”正经历着青春成长期生理和心理上的双重煎熬……

# 不良信息内容上传-违法内容

千细胞讨论专区千细胞讨论专区... [大学Med\_x研究院] - Mozilla Firefox

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

大学Med\_x研究院 - 千细胞讨论专区 - 帖子列表

千细胞讨论专区

公告：当前还未有公告

[我的主题] 精华主题

状态 主题

--普通主题--

- 多美康片(原名-速眠安)订购电话 0755-61672198
- 代办发票 验证后付款,13689533292陈生
- 删除通话记录和短信内容信息 移动联通服务密码查询咨询QQ:
- 手机改号软件下载 手机改号QQ13773793
- 想了解冰毒,加QQ176701799
- 手机通话清单查询 15876919868专业查询移动联通手机通话记
- 代,开连云港发票 13528837139

Guest / 2008-08-30 08:35:53 删除 引用

高压气枪◆QQ:512736261◆气枪论  
进,LOB18,LOB57,LOB78,1000X,CP2,LOB4-1, A1000 M92,气枪子弹,工字  
气枪,气枪配件,气枪专卖, M1911 类气枪,气枪网,三箭气枪  
QQ:512736261◆KWQ沙漠之鹰,654k, cp99, GAMO COMPACT、高压  
气枪图片,出售高压气枪,高压气枪价格,高压气枪子弹,高压气枪专卖,自制高  
压气枪,高压气枪结构图◆QQ:512736261◆气枪铅弹,5.5铅弹,4.5铅弹,南  
海铅弹,气枪子弹4.5,山峰铅弹,求购气枪子弹,气枪子弹模具,气枪子弹模具  
制造,气枪铅弹◆QQ:5 1 2 7 3 6 2 6 1◆4.5mm铅弹,gamo 铅弹,4.5  
铅弹模具,铅弹制作,穿甲弹,4.5mm铅弹,进口铅弹,帆船铅弹,环球铅弹  
◆QQ 5 1 2 7 3 6 2 6 1◆5.5mm铅弹,6mm铅弹,广州三箭气枪铅弹,尖  
头铅弹,气枪铅弹销售,购买气枪铅弹,出售铅弹,4.5气枪子弹,自制铅弹,  
气枪铅弹图纸,6mm铅弹,铅弹出售,气枪铅弹模具

申江网络科技  
网址: http://com

Guest / 2008-08-08 16:10:42 删除 引用

深圳市薪峰视觉影视广告工作室拥有先进专业的制作设备以及一批高素质  
的专业工作人员,倾心致力于高品质数码影视制作。多年来所服务客户触  
及各个行业,并成功为国内外科技行业、电讯行业、医药行业、金融业、  
房地产业、娱乐行业等多种行业制作过电视广告及宣传片,现已建立一套  
从影视作品的前期策划、拍摄到后期制作高效完善的服务体系。  
唐先生  
13632503918 (谢绝无关推销)  
http://szdf188.cn

深圳市薪峰视觉影视广告  
网址: http://www.sutime.cn

Guest / 2008-07-22 11:56:25 删除 引用

# Web客户端的安全

---

- **Java Applet、ActiveX、Cookie**等技术大量被使用，如果这些程序被恶意使用，可以窃取、改变或删除客户机上的信息。
- **网页木马**。浏览器存在众多已知或者未知的漏洞，攻击者可以写一个利用某个漏洞的网页，并**挂上木马**，当用户访问了这个网页之后，就中了木马。
- **跨站脚本攻击(XSS)**对于客户端的安全威胁同样无法忽视，利用**XSS**的**Web**蠕虫已经在网络中肆虐过。



# Web通信信道的安全

---

- **Web**信道面临着网络嗅探(**Sniffer**)和以拥塞信道、耗费资源为目的的**拒绝服务**攻击(**Denial of Service**)的威胁。
- 防范措施:
  - **S-HTTP** (Secure Hyper Text Transfer Protocol) : 是一种结合 HTTP 而设计的安全通信协议。
  - **HTTPS** (HTTP over SSL, Secure Sockets Layer) : HTTP下加入SSL层
  - **SSL**加密整个通信信道, 而**S-HTTP**则分别加密每条消息。S-HTTP允许用户在每条消息上产生数字签名, 而不只是认证协议作用期间的特定消息。

## 3.2 Web服务器指纹识别(信息收集)

---

- 3.2.1 Web服务器指纹介绍
- 3.2.2 Web服务器Banner信息获取
- 3.2.3 模糊Web服务器Banner信息
- 3.2.4 Web服务器协议行为
- 3.2.5 Http指纹识别工具

## 3.2.1 Web服务器指纹介绍

---

- **Web服务器指纹**：了解远程**Web服务器**的**配置信息**，然后根据不同版本的**Web服务器**进行有目的的攻击。
- **Http指纹识别**：记录不同服务器对**Http协议**执行中的微小差别进行识别。
  - 问题：Http服务器的配置文件、增加插件或组件使得更改Http的响应信息变得很容易，这样识别变得困难

## 3.2.2 Web服务器Banner信息获取

---

- ❑ **Banner**: 旗标，或标头。这里指获取**web**服务器的版本、欢迎语或其它提示信息，以找出可能的有利于攻击的内容。
- ❑ 我们可以通过一个**TCP**客户端比如**NetCat(NC)**或者**telnet**与**web**服务器进行连接，并查看返回的应答信息。

# 获得IIS 5.0指纹信息

---

❑ C:\telnet www.longker.com 80 Get

❑ 返回结果:

HTTP/1.1 400 Bad Request

Server: Microsoft-IIS/5.0

Date: Fri, 05 Sep 2003 02:57:39 GMT

Content-Type: text/html

Content-Length: 87

<html><head><title>Error</title></head><body>  
>The parameter is incorrect. </body>  
</html>

❑ 注意到下划线标记的信息，很清楚的告诉我们运行的web服务器版本是**Microsoft-IIS/5.0**。

# 获得Apache2.0.x指纹

---

❑ **sh-2.05b# nc www.target.com 80  
OPTIONS \* HTTP/1.1**

**Host:www.target.com**

**HTTP/1.1 200 OK**

**Date: Fri, 05 Sep 2003 02:08:45 GMT**

**Server: Apache/2.0.40 (Red Hat Linux)**

**Allow: GET,HEAD,POST,OPTIONS,TRACE**

**Content-Length: 0**

**Content-Type: text/plain; charset=ISO-8859-1**

# 不同服务器的指纹比较

---

- ❑ 通过**Apache2.0.x**和**IIS5.0**指纹的比较，能够很清楚判断出不同服务器返回的信息的不同。
- ❑ 当攻击者获得了这些指纹信息后，就可以针对不同的服务器，利用它们的漏洞进行有目的的攻击了。

## 3.2.3 模糊Web服务器Banner信息

---

- 为了防范查看**Http**应答头信息来识别**Http**指纹的行为，可以选择通过下面两种方法来更改或者是模糊服务器的**Banner**信息：
  - 自定义**Http**应答头信息
  - 增加插件



# 自定义**HTTP**应答头信息

---

- 开放源代码的**Http**服务器(如**apache**), 用户可以在**源代码**里修改**Banner**信息
- 未公开源代码的**Http**服务器(如: 微软的**IIS, Netscape**), 可以在存放**Banner**信息的**DII文件**中修改。

# 自定义HTTP应答头信息—实例

---

□ **Apache**服务器被自定义成了未知服务器:  
**Http/1.1403Forbidden**  
**Date:Mon,08Sep200302:41:27GMT**  
**Server:Unknown-Webserver/1.0**  
**Connection:close**  
**Content-**  
**Type:text/html;charset=iso-8859-1**

# 使用插件

---

- ❑ 插件可以提供自定义的**Http**应答信息。
- ❑ 比如: **ServerMask**, **IIS**服务器的一个插件, **ServerMask**不仅模糊了**Banner**信息, 而且会对**Http**应答头信息里的项的序列进行重新组合, 从而来模仿**Apache**这样的服务器, 它甚至有能力和扮演成任何一个**Http**服务器来处理每一个请求。
- ❑ 这个软件可以在以下地址找到:  
**[Http://www.port80software.com/products/servermask](http://www.port80software.com/products/servermask)**

# 使用插件—实例

---

- 下面是一个使用了**ServerMask**插件的**IIS**服务器的例子：

**Http/1.1200OK**

**Server: YesweareusingServerMask**

**Date: Mon, 08 Sep 2003 02:54:17 GMT**

**Connection: Keep-Alive**

**Content-Length: 18273**

**Content-Type: text/html**

**Set-**

**Cookie: Itworksoncookies too=82.3S5.0**

**12.NT2R0RE,4147ON3P,.400.;path=/**

**Cache-control: private**

## 3.2.4 Web服务器协议行为

---

- 如果**Http**请求是合法并且规则的，**Http**服务器返回的应答信息是符合**RFC**里的描述的。
- 如果发送畸形的**Http**请求，这些服务器的响应信息就不同了，不同服务器对**Http**协议行为表现的不同就是**Http指纹识别**技术的基本根据和原理。

# 协议行为分析实例

---

□ 我们将分析**3**种不同**Http**服务对不同请求所返回的响应信息，这些请求是这样的：

- 1: HEAD / Http/1.0 发送基本的Http请求
- 2: DELETE / Http/1.0 发送不被允许的请求，如Delete请求
- 3: GET / Http/5.0 发送一个非法版本的Http协议请求
- 4: GET / JUNK/1.0 发送一个不正确规格的Http协议请求

# Exp1: 基本的Http请求

---

- 我们先发送请求**HEAD / Http/1.0**，然后分析**Http**响应头里的信息，对头信息里项的排序进行分析。发送的请求命令如下：  
**C:\>nc apache.example.com 80**  
**HEAD / Http/1.0**
- 三个服务器的响应信息参见下面三页。
- 比较结果：**Apache**头信息里的**Server**和**Date**项的排序是不同的。

# Apache1.3.23

---

□ **Http/1.1200OK**  
**Date:Mon,08Sep17:10:49GMT**  
**Server:Apache/1.3.23**  
**Last-Modified:Thu,27Feb200303:48:19GMT**  
**ETag:"32417-c4-3e5d8a83"**  
**Accept-Ranges:bytes**  
**Content-Length:196**  
**Connection:close**  
**Content-Type:text/html**



# IIS5.0

---

□ **Http/1.1200OK**  
**Server:Microsoft-IIS/5.0**  
**Content-**  
**Location:Http://iis.example.com/Default.htm**  
**Date:Mon,08Sep20:13:52GMT**  
**Content-Type:text/html**  
**Accept-Ranges:bytes**  
**Last-Modified:Mon,08Sep200310:10:50GMT**  
**ETag:W/"e0d362a4c335be1:ae1"**  
**Content-Length:133**

# NetscapeEnterprise4.1

---

□ **Http/1.1200OK**

**Server:Netscape-Enterprise/4.1**

**Date:Mon,08Sep200306:01:40GMT**

**Content-type:text/html**

**Last-modified:Mon,08Sep200301:37:56GMT**

**Content-length:57**

**Accept-ranges:bytes**

**Connection:close**

# Exp2: HttpDELETE请求

---

- 这次，我们将发送**DELETE / Http/1.0**请求，我们将分析不同**Http**服务器对非法请求的应答信息的不同。
- 发送的请求命令：  
**C:\>nc apache.example.com 80  
DELETE / Http/1.0**
- 三个服务器的响应信息参见下面三页。
- 比较结果：
  - **Apache**响应的是“**405 Method Not Allowed**”
  - **IIS**响应的是“**403 Forbidden**”
  - **Netscape**响应的是“**401 Unauthorized**”发现对**Delete**请求，响应的信息是完全不同的。

# Apache1.3.23

---

❑ **Http/1.1 405 Method Not Allowed**  
**Date:Mon,08Sep200317:11:37GMT**  
**Server:Apache/1.3.23**  
**Allow:GET,HEAD,POST,PUT,DELETE,CONNECT,OPTIONS,PATCH,PROPFIND,PROPPATCH,**  
**MKCOL,COPY,MOVE,LOCK,UNLOCK,TRACE**  
**Connection:close**  
**Content-Type:text/html;charset=iso-8859-1**

# IIS5.0

---

❑ **Http/1.1 403 Forbidden**  
**Server:Microsoft-IIS/5.0**  
**Date:Mon,08Sep200320:13:57GMT**  
**Content-Type:text/html**  
**Content-Length:3184**

# NetscapeEnterprise4.1

---

□ **Http/1.1 401 Unauthorized**  
**Server:Netscape-Enterprise/4.1**  
**Date:Mon,08Sep200306:03:18GMT**  
**WWW-**  
**authenticate:Basicrealm="WebServerServer"**  
**Content-type:text/html**  
**Connection:close**

# Exp3: 非法Http协议版本请求

---

- 这次我们将发送非法的**Http**协议版本请求，比如**GET/Http/5.0**请求，事实上**Http5.0**是不存在的，发送请求命令：
- **C:\>nc apache.example.com 80**
- **GET / Http/5.0**
- 响应信息见下面三页。
- 比较结果：
  - **Apache**响应的是"**400 Bad Request**"
  - **IIS**忽略了这个请求，响应信息是**OK**，还返回了网站根目录的**HTML**数据信息
  - **Netscape**响应的是"**505 Http Version Not Supported**"。

# Apache1.3.23

---

□ **Http/1.1400 Bad Request**  
**Date:Mon,08Sep200317:12:37GMT**  
**Server:Apache/1.3.23**  
**Connection:close**  
**Transfer-Encoding:chunked**  
**Content-Type:text/html;charset=iso-8859-1**



# IIS5.0

---

□ **Http/1.1 200 OK**  
**Server:Microsoft-IIS/5.0**  
**Content-**  
**Location:Http://iis.example.com/Default.htm**  
**Date:Mon,08Sep200320:14:02GMT**  
**Content-Type:text/html**  
**Accept-Ranges:bytes**  
**Last-Modified:Mon,08Sep200320:14:02GMT**  
**ETag:W/"e0d362a4c335be1:ae1"**  
**Content-Length:133**

# NetscapeEnterprise4.1

---

❑ **Http/1.1 505 Http Version Not Supported**  
**Server:Netscape-Enterprise/4.1**  
**Date:Mon,08Sep200306:04:04GMT**  
**Content-length:140**  
**Content-type:text/html**  
**Connection:close**

# Exp4: 不正确规则协议请求

---

- 这次测试主要是对**GET / JUNK/1.0**请求的响应，发送请求命令：

```
C:\>ncapache.example.com80  
GET / JUNK/1.0
```

- 响应信息参见下面三页。

- 比较结果：

- **Apache**忽视了不规则的协议**"JUNK"**，还返回了**200 "OK"** 和根目录的一些信息，
- **IIS**响应的是**"400 Bad Request"**
- **Netscape**几乎没有返回**Http**头信息，相反的却返回了**HTML**格式的信息来表明这是个错误请求。

# Apache1.3.23

---

□ **Http/1.1 200 OK**  
**Date:Sun,15Jun200317:17:47GMT**  
**Server:Apache/1.3.23**  
**Last-Modified:Thu,27Feb200303:48:19GMT**  
**ETag:"32417-c4-3e5d8a83"**  
**Accept-Ranges:bytes**  
**Content-Length:196**  
**Connection:close**  
**Content-Type:text/html**

# IIS5.0

---

❑ **Http/1.1 400 Bad Request**  
**Server:Microsoft-IIS/5.0**  
**Date:Fri,01Jan199920:14:34GMT**  
**Content-Type:text/html**  
**Content-Length:87**

# NetscapeEnterprise4.1

---

```
□ <HTML>  
  <HEAD><TITLE>Bad request</TITLE></HEAD>  
  <BODY>  
    <H1>Bad request</H1>  
    Your browser sent a query this server could not  
    understand.  
  </BODY>  
</HTML>
```

# 测试小结

---

- 我们下面列了一个表，我们可以很简单的辨别不同的**Http**服务器。

服务器	头信息项排序	Delete请求	非法版本	不规则协议
Apache/1.3.23	Date, Server	405	400	200
MS-IIS/5.0	Server, Date	403	200	400
Netscape4.1	Server, Date	401	505	no header

## 3.2.5 Http指纹识别工具

---

- 这里我们将介绍一个**Http**指纹识别工具**Httpprint**，它通过运用统计学原理，组合模糊的逻辑学技术，能很有效的确定**Http**服务器的类型。
- **Httpprint**收集了每种**http**服务器在交互过程中产生的特性，将它们编码成一个固定长度的**ASCII**字符串，这就是**Httpprint**签名。



# Httpprint的Http签名

---

Microsoft-IIS/5.0

CD2698FD6ED3C295E4B1653082C10D64811C9DC594DF1BD04276E4BB811C9DC5  
0D7645B5811C9DC52A200B4C9D69031D6014C217811C9DC5811C9DC52655F350  
FCCC535BE2CE6923E2CE6923F2454256E2CE69272576B769E2CE6926CD2698FD  
6ED3C295E2CE692009DB9B3E6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923  
6ED3C295

Apache/1.3.x

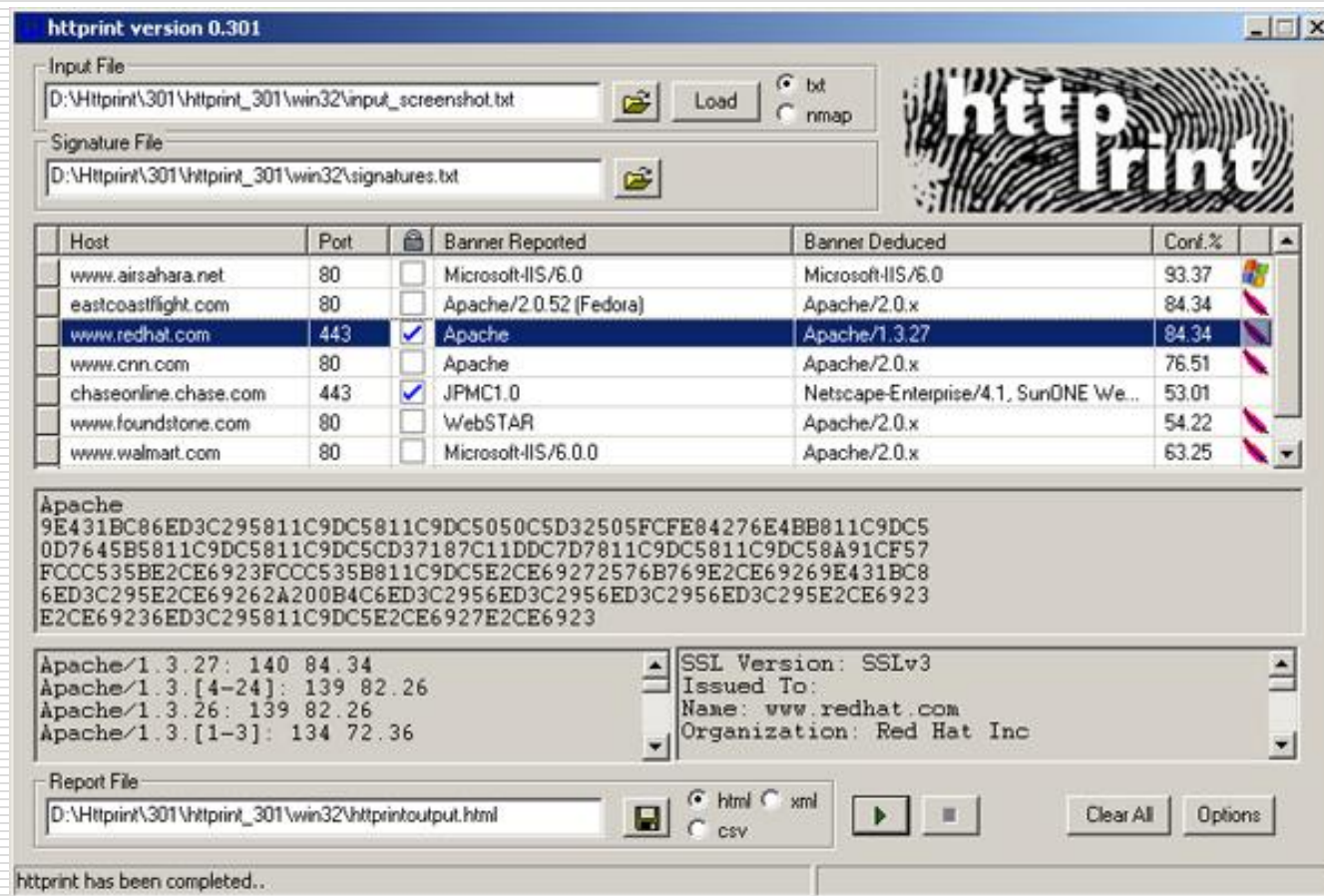
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB630A04DB  
0D7645B5970EE6BB811C9DC5CD37187C11DDC7D78398721EB06FE5D78A91CF57  
FCCC535B6ED3C295FCCC535B811C9DC5E2CE69272576B769E2CE69269E431BC8  
6ED3C295E2CE69262A200B4C811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5  
811C9DC5

# Httpprint介绍
















---

- ❑ **Httpprint**先把一些**Http**签名信息保存在一个文档里，然后分析那些由**Http**服务器产生的结果。
- ❑ 对于没有列在数据库中的签名信息时，可以利用**Httpprint**产生的报告来扩展这个签名数据库，下一次运行**Httpprint**时，这些新加的签名信息就可以使用了。
- ❑ **Httpprint**可以图形界面运行和命令行下运行，可以运行在**Windows**、**Linux**和**MacOSX**平台上。
- ❑ 下载地址：  
<http://www.net-square.com/httpprint/>







# httpprint v0.301 主界面



# 输出结果报告

httpPrint		web server fingerprinting report				
host	port	ssl	banner reported	banner deduced	icon	confidence
www.airshara.net	80		Microsoft-IIS/6.0	Microsoft-IIS/6.0		
eastcoastflight.com	80		Apache/2.0.52 (Fedora)	Apache/2.0.x		
www.redhat.com	443	✓	Apache	Apache/1.3.27		
www.cnn.com	80		Apache	Apache/2.0.x		
chaseonline.chase.com	443	✓	JPMC1.0	SunONE WebServer 6.0, Netscape-Enterprise/4.1		
www.foundstone.com	80		WebSTAR	Apache/2.0.x		
www.walmart.com	80		Microsoft-IIS/6.0.0	Apache/2.0.x		
www.port80software.com	80		Yes we are using ServerMask!	Microsoft-IIS/4.0, Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/5.1		
SSL analysis						
www.redhat.com:443						
issued to			www.redhat.com Red Hat Inc Web Operations			
serial			05:91:F9			
issued by			Equifax Equifax Secure Certificate Authority			
validity			15/11/2005 14:28:03 - 16/11/2007 15:28:03			
SSL version			SSLv3			
cipher name			DHE-RSA-AES256-SHA			
cipher version			TLSv1/SSLv3			
cipher encryption			256 bits			
chaseonline.chase.com:443						
issued to			chaseonline.chase.com JPMorgan Chase CIG			
serial			65:51:00:F6:8D:AA:7B:49:0B:10:19:16:CD:23:2D:23			
issued by			VeriSign Trust Network VeriSign, Inc.			
validity			07/03/2005 17:30:00 - 08/03/2006 18:29:59			
SSL version			SSLv3			
cipher name			RC4-MD5			
cipher version			TLSv1/SSLv3			
cipher encryption			128 bits			
 httpPrint © 2003-2005 net-square						

# 识别模糊的Banner信息

		web server fingerprinting report				
host	port	ssl	banner reported	banner deduced	icon	confidence
www.walmart.com	80		Microsoft-IIS/5.0	Apache/2.0.x		<div><div></div></div>
www.foundstone.com	80		WebSTAR	Apache/2.0.x		<div><div></div></div>
www.port80software.com	80		Yes we are using ServerMask	Microsoft-IIS/5.1, Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/4.0		<div><div></div></div>
www.ubizen.com	80		web server	Apache/2.0.x		<div><div></div></div>
www.datek.com	80		Ameritrade Web Server	Netscape-Enterprise/4.1		<div><div></div></div>
 http print © 2003 net-square						

## 3.5 Google Hacking

---

- 3.5.1 Google Hacking的原理
  - 3.5.2 Google Hacking的实际应用
-

## 3.5 Google Hacking

---

- **Google Hacking**就是利用**搜索引擎搜索**所需要的**敏感信息**的一种手段。
  - **Google Hacking**的原理非常简单，由于许多有特定漏洞的网站都有类似的标志页面，而这些页面如果被搜索引擎的数据库索引到，我们就可以通过**搜索指定的单词**来找到某些有指定漏洞的网站。
-

## 3.5.1 Google Hacking的原理

---

- **intext:** 就是把网页正文内容中的某个字符做为搜索条件
    - 例如在Google里输入“**intext:动网**”（注意：在搜索引擎中输入的字符不包括“”，本节中以下同），将返回所有在网页正文部分包含“动网”的网页。
  - **allintext:** 使用方法和**intext**类似。
  - **intitle:** 和**intext**相近，搜索网页标题中是否有所要找的字符。
    - 例如搜索“**intitle:IT安全**”，将返回所有网页标题中包含“IT安全”的网页。
  - **allintitle:** 也同**intitle**类似。
  - **cache:** 搜索Google里关于某些内容的缓存。
  - **define:** 搜索某个词语的定义。
    - 比如搜索“**define:黑客**”，将返回关于“黑客”的定义。
-



## 3.5.1 Google Hacking的原理

---

- ❑ **filetype:** 搜索指定类型的文件。这个是要重点推荐的，无论是撒网式攻击还是我们后面要说的对特定目标进行信息收集都需要用到它。
    - 例如输入“filetype:mdb”，将返回所有以“mdb”结尾的文件URL。如果对方的虚拟主机或服务器没有限制下载，那么单击这些URL就可以将对方的这些文件下载下来。
  - ❑ **info:** 查找指定站点的一些基本信息。
  - ❑ **inurl:** 搜索指定的字符是否存在于URL中。
    - 例如输入“inurl:admin”，将返回许多类似于这样的连接：  
<http://www.xxx.com/xxx/admin>，用这一搜索指令来寻找管理员登陆的URL是非常有效的一个途径。
  - ❑ **allinurl:** 也同inurl类似，可指定多个字符。
-

## 3.5.1 Google Hacking的原理

---

- **link:** 查找和指定网站做了链接的网站。
    - 例如搜索 “inurl:www.xfocus.net”可以返回所有和www.xfocus.net做了链接的URL。
  - **site:** 用来查找与指定网站有关的链接。
    - 例如输入 “site:www.xfocus.net”将返回所有和www.xfocus.net有关的URL。
  - 还有一些操作符也是很有用的：
    - + 把Google可能忽略的字列入查询范围
    - - 把某个字忽略
    - ~ 同意词
    - . 单一的通配符
    - \* 通配符，可代表多个字母
    - "" 精确查询
-

## 3.5.2 Google Hacking的实际应用

---

- 利用 “**index of**”来查找开放目录浏览的站点
    - 比如，在Google中搜索 “**intitle:“index of” passwd**”，其中一个链接打开之后，显示的内容如下页所示。
    - **passlist.txt**中存放的就是所有的账号和密码，点击即可以打开浏览。而**admin.mdb**也可以下载。
-

## 3.5.2 Google Hacking的实际应用



## 3.5.2 Google Hacking的实际应用

---

### □ 搜索指定漏洞程序

- 例如**ZeroBoard**前段时间被发现一个文件代码泄露的漏洞，可以用Google来寻找网上使用这套程序的站点。在Google中输入“`intext:ZeroBoard filetype:php`”或“`inurl:outlogin.php?_zb_path=site:.jp`”来寻找所需要的页面。
  - **phpMyAdmin**是一套功能强大的数据库操作软件，一些站点由于配置失误，导致用户可以不使用密码直接对phpMyAdmin进行建立、复制、删除等操作，我们可以用“`intitle:phpmyadmin intext:Create new database`”来搜索存在这样漏洞的程序网址。
-

## 3.5.2 Google Hacking的实际应用

---

- 查找有跨站脚本漏洞的站点:
    - allinurl:/scripts/cart32.exe
    - allinurl:/CuteNews/show\_archives.php
    - allinurl:/phpinfo.php
  - 查找有**SQL**注入漏洞的站点:
    - allinurl:/privmsg.php
-

## 3.5.2 Google Hacking的实际应用

---

- 下面以[www.xxx.com](http://www.xxx.com)站点为例，介绍如何利用**Google**进行一次完整入侵过程。
  - 首先，用**Google**查看这个站点的基本情况
    - 在Google中输入：site:xxx.com
    - 从返回的信息中，找到几个相关的域名，假设为  
http://a1.xxx.com、http://a2.xxx.com、  
http://a5.xxx.com、http://a4.xxx.com
  - 然后，使用**Ping**命令对这几个域名进行测试，查看它们是否使用的是同一个服务器。
-

## 3.5.2 Google Hacking的实际应用

---

- 接下来，在**Google**中输入**site:xxx.com filetype:doc**，看看是否有比较有用的**doc**文档资料。
  - 查找网站的管理后台地址。输入：
    - site:xxx.com intext:管理
    - site:xxx.com inurl:login
    - site:xxx.com intitle:管理
    - 假设获得2个管理后台地址：  
http://a2.xxx.com/sys/admin\_login.asp、  
http://a5.xxx.com:88/\_admin/login\_in.asp
-



## 3.5.2 Google Hacking的实际应用

---

- 得到后台地址后，来看一下服务器上运行的是什么程序。输入：
    - site:a2.xxx.com filetype:asp
    - site:a2.xxx.com filetype:php
    - site:a2.xxx.com filetype:aspx
    - site:a5.xxx.com filetype:asp
    - .....
    - 假设探测到a2服务器用的是IIS，上面用的是ASP的整站程序，还有一个PHP的论坛，a3服务器也是IIS，使用的是ASPX+ASP。
  - 既然是论坛，看看有没有公共的**FTP**帐号之类：
    - site:a2.xxx.com intext:ftp://\*:\*
-

## 3.5.2 Google Hacking的实际应用

---

- 如果没找到什么有价值的东西，再看看有没有上传的漏洞：
    - `site:a2.xxx.com inurl:file`
    - `site:a5.xxx.com inurl:load`
    - 假设在a2上发现一个上传文件的页面  
<http://a2.xxxx.com/sys/uploadfile.asp>，用IE查看一下，发现没有权限访问。
  - 接下来试试注入漏洞。输入：
    - `site:a2.xxx.com filetype:asp`
    - 得到几个ASP页面的地址，使用软件进行注入。
    - 此外，我们还可以使用`site:xxx.com intext:*@xxx.com`获取一些邮件地址，以及邮箱主人的名字；
    - 使用 `site:xxxx.com intext:电话` 来获得一些电话
  - 把搜集到的这些信息做个字典，用暴力软件进行破解，得到几个用户名和密码，即可进行登录了。剩下的其它入侵行为，在此不再赘述。
-

## 3.6 防御Web攻击

---

- 3.6.1 Web服务器安全配置
- 3.6.2 Web浏览者的安全措施
- 3.6.3 Web安全需澄清的五个误解

## 3.6.1 Web服务器安全配置

---

- **Web**服务器为互联网用户提供服务的同时，也是黑客攻击的主要对象和攻入系统主机的主要通道。
- 服务器安全配置包括主机系统的安全配置和**Web服务器的安全配置**两大部分。

# 主机系统安全配置

---

- 服务器主机系统是服务器的基础，因此显然服务器运行的安全性与其所在的主机系统安全性密切相关有关。
- 这里的主机系统安全性，指的是应用在主机上且与服务器主要服务业务不相关的配置。
  - 简单性
  - 超级用户权限
  - 本地和远程访问控制
  - 审计和可审计性
  - 恢复

# Web服务器安全配置

---

- 基于**Windows**系统**Web**服务器安全配置
- 基于**Unix**系统**Web**服务器安全配置

# 基于Windows系统Web服务器安全配置

---

- **Windows**的**IIS**的方便性和易用性，使它成为最受欢迎的**Web**服务器软件之一。但是，**IIS**的安全性却一直令人担忧。
- 下面从**IIS**的安全安装与**IIS**的安全配置两个方面进行讲解。

# IIS安全安装

---

- 要构建一个安全的**IIS**服务器，必须从安装时就充分考虑安全问题。
  - 不要将**IIS**安装在系统分区上。
  - 修改**IIS**的安装默认路径。
  - 打上Windows和**IIS**的最新补丁。



# IIS安全配置

---

- ❑ 删除不必要的虚拟目录
- ❑ 删除危险的**IIS**组件
- ❑ 为**IIS**中的文件分类设置权限
- ❑ 删除不必要的应用程序映射
- ❑ 保护日志安全

# IIS安全配置--删除不必要的虚拟目录

---

- **IIS**安装完成后在 **C:\Inetpub\wwwroot** 下默认生成了一些目录，包括**IISHelp**、**IISAdmin**、**IISSamples**、**MSADC**等，这些目录都没有什么实际的作用，可直接删除。

# IIS安全配置--删除危险的IIS组件

---

- 默认安装后的有些**IIS**组件可能会造成安全威胁，例如**SMTP Service**和**FTP Service**、样本页面和脚本，大家可以根据自己的需要决定是否删除。

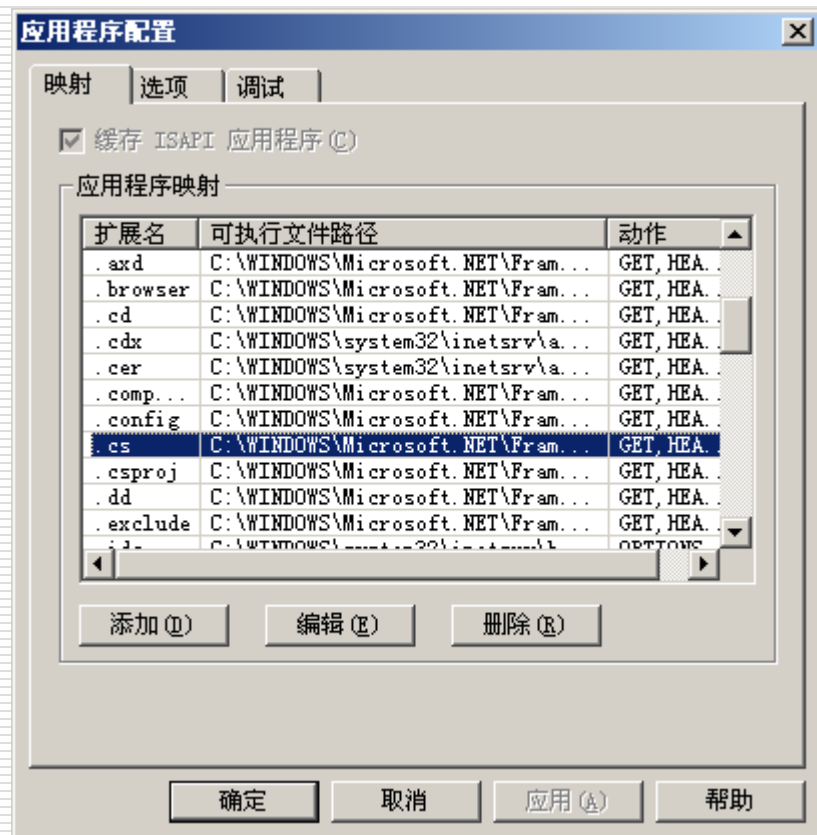
## **IIS安全配置--为IIS中的文件分类设置权限**

---

- ❑ 除了在操作系统里为**IIS**的文件设置必要的权限外，还要在**IIS**管理器中为它们设置权限。
- ❑ 一个好的设置策略是：为**Web** 站点上不同类型的文件都建立目录，然后给它们分配适当权限。例如：静态文件文件夹允许读、拒绝写，脚本文件夹允许执行、拒绝写和读取。

# IIS安全配置--删除不必要的应用程序映射

- ❑ IIS中默认存在很多种应用程序映射，可以对它进行配置，删除不必要的应用程序映射。
- ❑ 在“Internet信息服务”中，右击网站目录，选择“属性”，在网站目录属性对话框的“主目录”页面中，点击【配置】按钮，弹出“应用程序配置”对话框，在“应用程序映射”页面，删除无用的程序映射。



## IIS安全配置--删除不必要的应用程序映射(2)

- 如果需要这一类文件时，必须安装最新的系统修补补丁，并且选中相应的程序映射，再点击[编辑]按钮，在“添加/编辑应用程序扩展名映射”对话框中勾选“检查文件是否存在”选项。这样当客户请求这类文件时，**IIS**会先检查文件是否存在，文件存在后才会去调用程序映射中定义的动态链接库来解析。



# IIS安全配置--保护日志安全

---

- 日志是系统安全策略的一个重要环节，确保日志的安全能有效提高系统整体安全性。
  - **修改IIS日志的存放路径**：默认情况下，IIS的日志存放在%WinDir%\System32\LogFiles，黑客当然非常清楚，所以最好修改一下其存放路径。在“Internet信息服务”中，右击网站目录，选择“属性”，在网站目录属性对话框的“Web站点”页面中，在选中“启用日志记录”的情况下，点击旁边的[属性]按钮，在“常规属性”页面，点击[浏览]按钮或者直接在输入框中输入日志存放路径即可。
  - **修改日志访问权限**，设置只有管理员才能访问。

# 基于Unix系统Web服务器安全配置

---

- ❑ 不以**root**运行**web**服务器。
- ❑ 限制在**WEB**服务器开账户，定期删除一些用户。
- ❑ 对在**WEB**服务器上开的账户，在口令长度及定期更改方面作出要求，防止被盗用。同时注意保护用户名、组名及相应的口令。
- ❑ 尽量使**FTP**、**MAIL**等服务器与之分开，去掉**ftp**，**sendmail**，**tftp**，**NIS**，**NFS**，**finger**，**netstat**等一些无关的应用。
- ❑ 定期查看服务器中的日志**logs**文件，分析一切可疑事件。在**errorlog**中出现**rm**、**login**、**/bin/perl**、**/bin/sh**等之类记录时，你的服务器可能已经受到了一些非法用户的入侵。



## 基于Unix系统Web服务器安全配置(2)

---

- 有些WEB服务器把WEB的文档目录与FTP目录指在同一目录时，应该注意不要把FTP的目录与**CGI-BIN**指定在一个目录之下。
- 文件的访问控制：设置好WEB服务器上系统文件的权限和属性，对可让人访问的文档分配一个公用的组，如**WWW**，并只分配它只读的权利。把所有的**HTML**文件归属**WWW**组，由WEB管理员管理**WWW**组。对于WEB的配置文件仅对WEB管理员有写的权利。

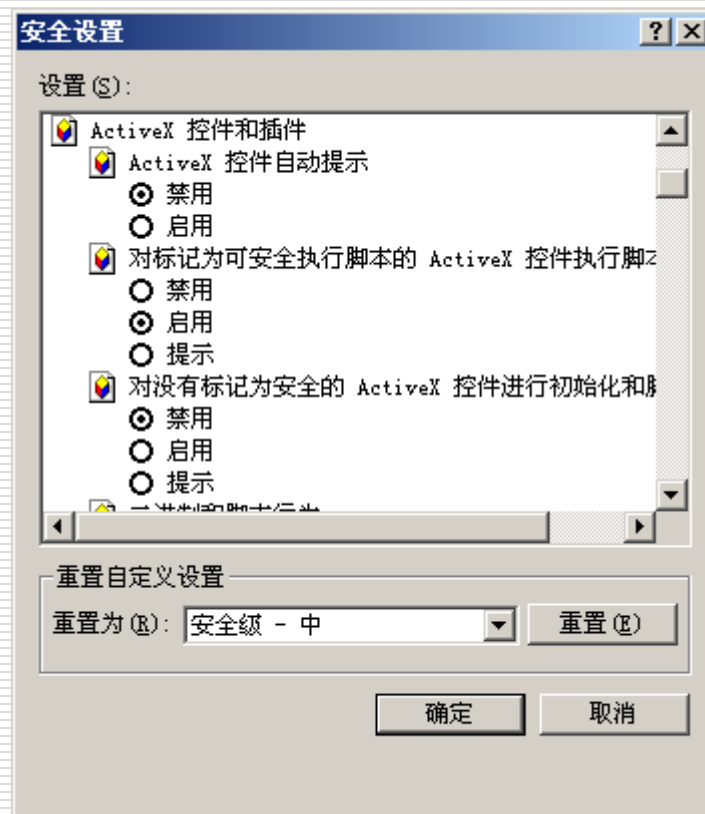
# 基于Unix系统Web服务器安全配置(3)

---

- ❑ 对不同目录设置不同的属性，如：**Read**、**Excute**、**Write**。
- ❑ 在**WEB**服务器上去掉一些不用的脚本解释器，例如：当在你的**CGI**的程序中没用到**perl**时，就尽量把**perl**在系统解释器中删除掉。

## 3.6.2 Web浏览者的安全措施

- 对浏览器的安全性进行设置，以微软**IE**为例，点击“工具”  
→**Internet**选项→安全  
→自定义级别”，打开  
如图所示的窗口，请根据  
自己的需要进行设置。



# Web浏览者的安全措施(2)

---

- ❑ 经常对操作系统打补丁、升级。
- ❑ 使用漏洞数较少的浏览器，如**Firefox**。
- ❑ 经常对浏览器进行升级。
- ❑ 不要因为好奇而打开一些不信任的网站。

## 3.6.3 Web安全需澄清的五个误解

---

- 针对**Web**安全，存在着许多误解。要增强**Web**网站的安全性，首先要澄清下面五个误解。
  - “Web网站使用了SSL加密，所以很安全”
  - “Web网站使用了防火墙，所以很安全”
  - “漏洞扫描工具没发现任何问题，所以很安全”
  - “网站应用程序的安全问题是程序员造成的”
  - “我们每年会对Web网站进行安全评估，所以很安全”

## 3.7 小结

---

- ❑ 随着互联网的发展，**Web**已经成为人们钟爱的获取信息和互相交流的方式，随之而来的**Web**安全也成为近年来安全工作者的研究重点。
- ❑ 本章主要讨论了威胁**Web**安全的常用攻击，包括**Web**页面扫描、**Google Hacking**等，并列举了相应对策。
- ❑ 应该强调的是，高质量的编程、健壮的程序设计、注重对系统的日常监控，从增强**Web**站点自身的健壮性方面来采取措施，往往更能取得显著效果。