网络攻防技术与实践课程

课程11. Web应用安全攻防技术(上)

诸葛建伟

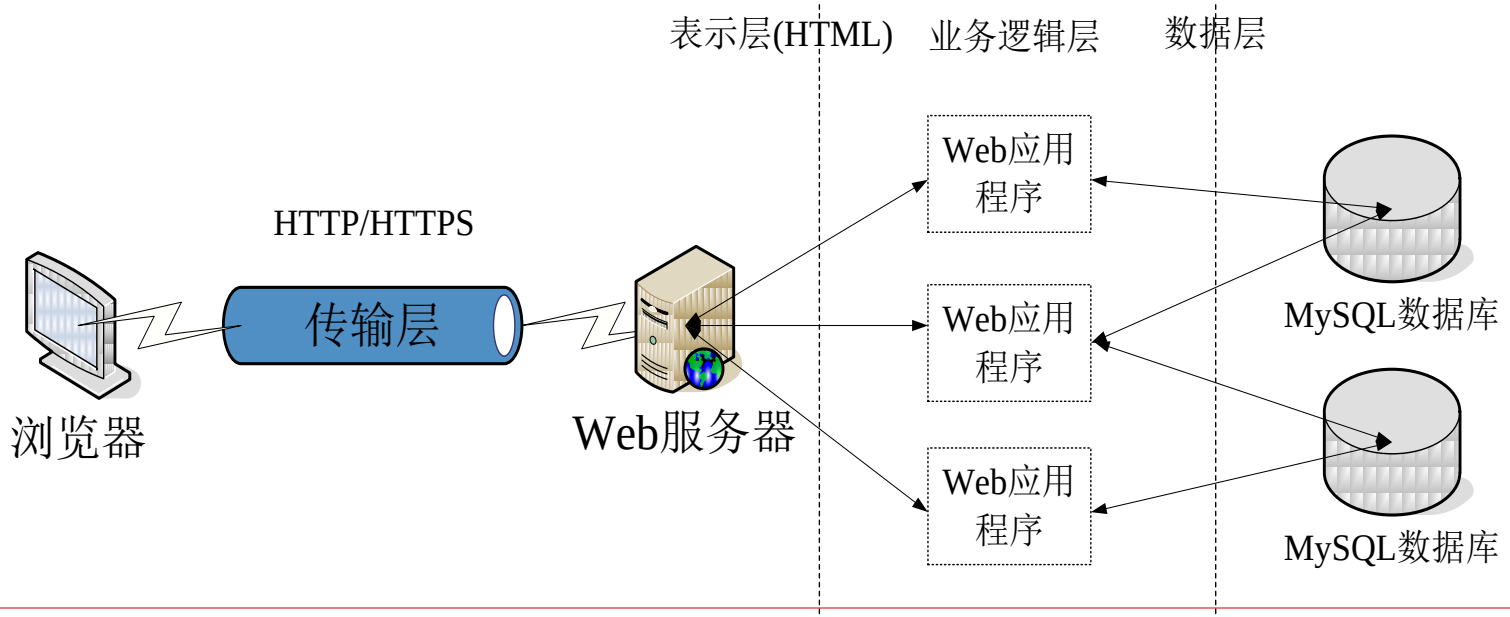
zhugejw@gmail.com

内容

1. **Web应用程序体系结构及其安全威胁**
2. **Web应用安全攻防技术概述**
3. **SQL注入**
4. **XSS跨站脚本攻击**
5. **课外实践作业：SEED SQL注入攻击实验 | SEED XSS攻击实验**

Web应用体系结构

- 传统C/S架构的计算→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



HTML静态页面和动态页面

- **HTML (HyperText Markup Language)历史**
  - **起源: 1980s, Tim Berners-Lee, ENQUIRE**
  - **1991: HTML发布，互联网进入WWW时代**
  - **1995: HTML v2.0正式称为IETF RFC 1866标准**
- **HTML: 静态标记语言**
  - **Tag标签: 表格等结构标签, 超链接, 内嵌链接, 图片, …**
  - **交互能力: 表单, 脚本→支持动态生成页面**
- **动态页面**
  - **CGI**
  - **脚本语言: ASP, JavaScript, PHP, …**
- **交互能力进一步扩展**
  - **ActiveX控件、Java Applet…**

Web客户端 — 浏览器

- 浏览器产品的商业竞争
  - “第一次浏览器大战”：**Netscape Loses to IE**
  - “第二次浏览器大战”：**IE VS. Firefox, Chrome, Safari, etc**
  - “第二次浏览器大战”：移动终端浏览器之争，**Opera, Safari, …**
- 浏览器技术的发展
  - 早期：简单的静态**HTML**页面解析与渲染
  - **1995 Netscape**引入**Javascript**，客户端脚本语言
  - **1996 Adobe(Macromedia)**引入**Flash**
  - **1999 Sun**：**Servlet**，**J2ME**
  - **2005 Ajax**

Web服务器与动态编程技术

- **Web服务器软件**
  - **HTTP守护进程**
  - 各种**Web**动态编程语言支持
  - 主流：**MS＋LAMP**

技术供应商	Web 应用服务器软件/技术
微软	IIS/ASP/ASP.NET/ISAPI/COM/...
Sun	J2EE，包括
IBM Websphere	Java Servlets
BEA Weblogic	Java Server Pages
标准化组织	HTTP/HTML/XML/CORBA/…
Apache software Foundation 等开源社区组织	Apache/PHP/ CGI/Perl/Python/…

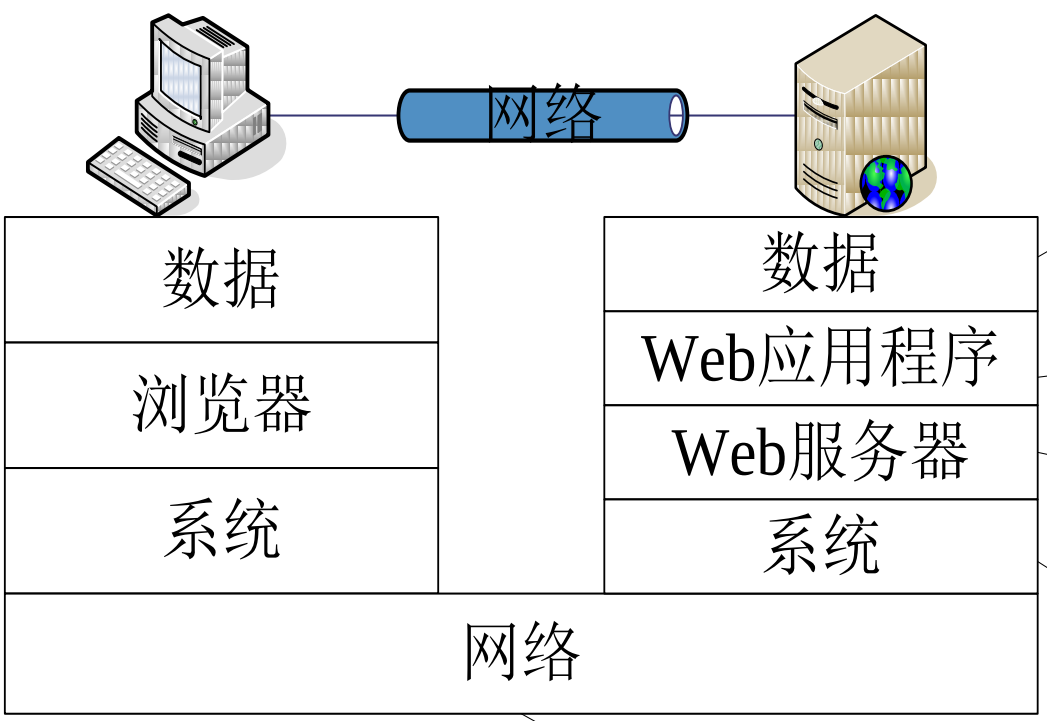
Web应用程序

- Web应用程序－Web Application
  - Web服务器端的业务逻辑
  - 现代Web应用的核心
- Web应用程序的分层模型
  - 最普遍应用：3层模型(3-tiers)
  - 表示层：接受Web客户端输入并显示结果
  - 业务逻辑层：完成Web应用业务处理，核心，实现技术－CGI、ASP、PHP等动态脚本
  - 数据层：数据库 / 本地文件；数据库连接：ODBC / OLEDB / JDBC

传输协议: HTTP/HTTPS

- HTTP
  - HTTP 1.0 (IETF RFC 1945), HTTP 1.1 (RFC 2616), 缺省TCP 80端口
  - 无状态、基于ASCII码明文传递的简单协议
  - 请求/响应模式: 请求资源标识符(URI)
  - 无状态性、明文性、简单性、流行性→易受攻击
- 状态管理－Cookies 保持连接状态
- 身份认证－基础认证等多种认证协议
- HTTPS
  - 基于SSL/TLS: 提供对传输层认证(AH)和加密(ESP)
  - HTTPS: HTTP over TLS, 缺省TCP 443端口

Web应用安全威胁



Web数据安全威胁：敏感信息泄漏/内容篡改/不良信息内容

Web应用安全威胁：代码注入攻击/XSS攻击等

服务安全威胁：针对Web服务器软件的渗透攻击

系统安全威胁：远程和本地渗透攻击

网络安全威胁：机密窃听、假冒身份攻击等

内容

1. Web应用程序体系结构及其安全威胁
2. Web应用安全攻防技术概述
3. SQL注入
4. XSS跨站脚本攻击
5. 课外实践作业：SEED SQL注入攻击实验 | SEED XSS攻击实验

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

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

- 课程3回顾：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”

Web应用程序的探测和漏洞发现

- 手工审查Web应用程序结构与源代码
- 自动下载与镜像Web站点页面
- 使用Google Hacking技术审查与探测Web应用程序

手工审查Web应用程序结构与源代码

- 静态和动态生成的页面
  - 查看源代码
  - 隐藏信息：表单隐藏字段、注释隐藏信息
  - 动态页面：脚本编程语言，页面命名规则，以及参数名称、类型与含义
- 目录结构
  - 页面存储结构
  - 目录文件枚举不安全配置
- 辅助性文件
  - **CSS**级联样式表、**XML**样式表、**Javascript**文件、**include**文件
  - 数据库字段结构、目录路径、输入参数以及数据库连接字符串

手工审查Web应用程序结构与源代码（2）

- 输入表单
  - 提交数据方法：**GET**还是**POST**
  - 表单处理行为：哪个脚本？
  - 输入字段名称、最大长度限制、隐藏字段、自动完成标记、口令字段
- 查询参数字符串
  - 复用以假冒其他用户、获取受限的数据、运行任意的系统命令，或者执行其他应用程序开发者所不希望看到的动作
  - 提供了**Web**应用程序内部工作的信息**:** 数据表字段名称，会话标识符、用户名或口令字段

通过黑客游戏提升手工分析能力

- 网页解密类黑客游戏
- ① **NotPron**解密游戏：http://deathball.net/notpron/levelone.htm，共**132**关。
- ② 路路解密破解游戏（中文）- 综合类。
- ③『中安网培』黑客游戏 （中文）- 网页过关类：**http://game.enet.org.cn/**。
- ④ **Monyer**系列（黑客游戏），**http://monyer.com/game/game1/**。
- ⑤ **sqybi** 的解谜游戏 （中文）- 网页过关类：http://sqybi.com/game/。

自动下载与镜像Web站点页面

- 在线手工审查 -> 自动下载 / 镜像，离线审查
- **Linux系统自动下载与镜像工具**
  - **Lynx / wget / …**
  - **Libcurl**
- **Windows系统**
  - **Teleport / Offline Explorer**
  - 迅雷 / **Flashget**

使用Google Hacking技术审查与探测Web应用程序

- Google已经帮我们下载并分析了几乎所有公开页面
  - Googlebot
  - Google Search Engine
- Google Hacking
  - Google的高级搜索与挖掘技巧
  - 在大范围内搜索存有漏洞的Web应用程序
  - 符合特定条件的敏感信息内容
  - 在被Google检索的目标站点中搜索特定信息

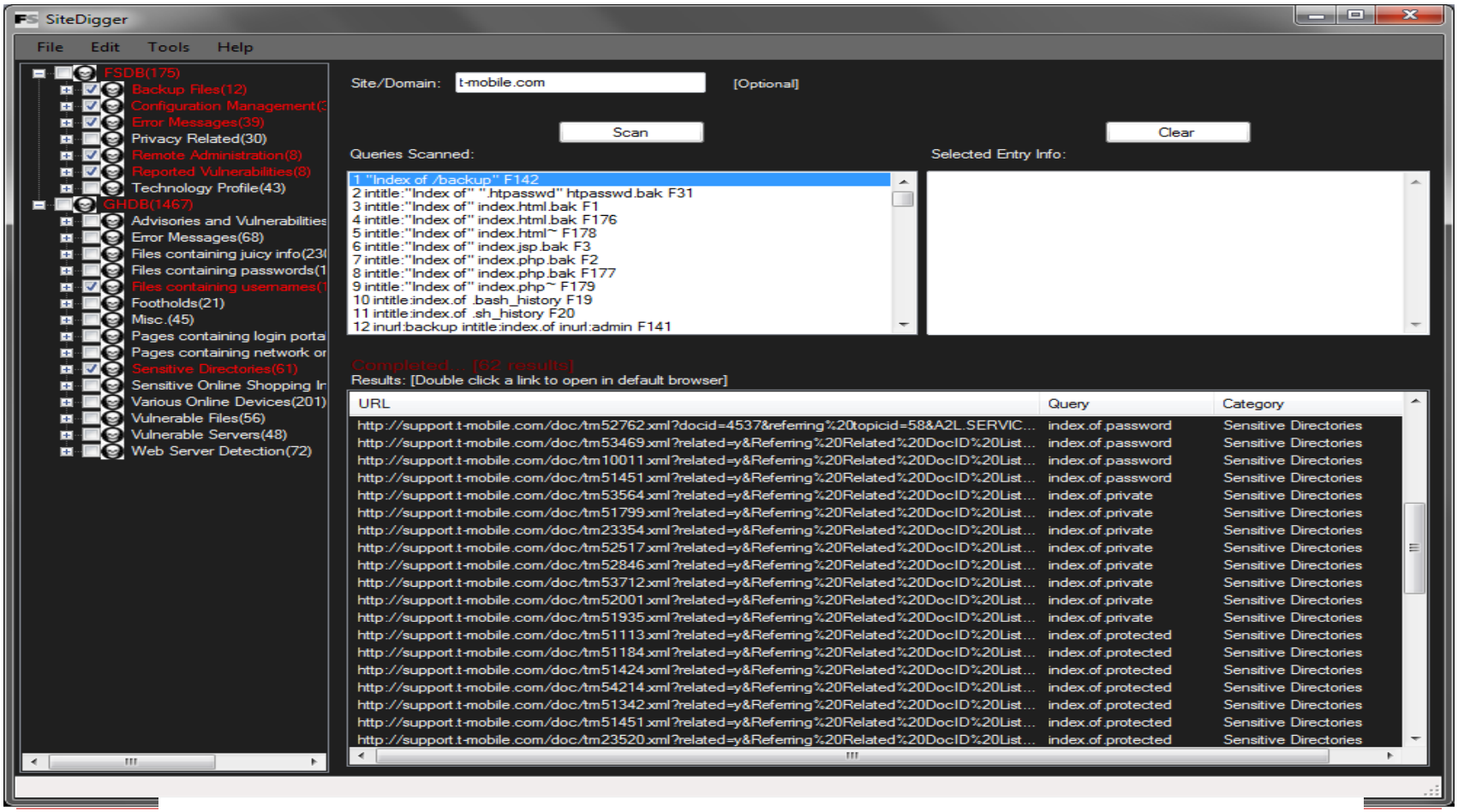
Google Hacking DataBase

- GHDB Project
  - Johnny Long, since 2004
  - 《Google Hacking for Penetration Testers》
  - 2010/11, exploit-db网站重新启动GHDB
- GHDB规模
  - 14类
  - 1,100多条查询搜索条件

Google Hacking DataBase

GHDB 大类	GHDB 类别	查询条数	备注
获取攻击入口点	立足点	21	可以帮助攻击者获得 Web 服务器立足点的查询条件。
	包含登录入口的页面	236	找出各式各样 Web 应用程序的登录入口页面。
	各种类型在线设备	203	各种 Google 能够搜索到的在线设备，如打印机、视频摄像头等
获取攻击所需信息	错误消息	69	泄露过多信息的错误消息
	包含有口令的文件	136	文件中直接包含了口令。
	包含有用户名的文件	15	文件中包含了用户名，但不包含口令。
	包含其他价值信息的文件	232	文件中包含有除用户名和口令之外其他有价值信息。
	包含网络和漏洞数据页面	59	包括如防火墙日志、蜜罐系统日志、网络信息、IDS 日志的页面。
	Web 服务器探测	72	这些查询条件验证了 Google 对 Web 服务器实施探测和轮廓获取非凡的能力。
探测安全漏洞	有漏洞的文件	57	Google 从网站上可搜索到的成千上万的有漏洞的文件
	存有漏洞的服务器	49	存在特定安全漏洞的网站服务器。
	安全威胁与漏洞	313	定位存在安全漏洞的服务，这些查询条件通常根据由各种安全威胁报告所生成的，大部分情况下针对特定产品和版本的。
获取敏感数据与信息	敏感目录	64	共享有敏感信息目录的网站。
	敏感的在线购物信息	9	能够查询在线购物信息(如客户信息、供应商、订单、信用卡号、信用卡信息)的查询条件示例。

Google Hacking工具



能够自动进行Google Hacking搜索的SiteDigger免费软件

Web应用程序安全评估与漏洞探测

- 深入的安全评估与漏洞探测
  - 透彻理解目标应用程序的体系结构和设计思路
  - 找出可能存在的薄弱环节
  - 总结出针对这个Web应用程序的详细攻击步骤
- Web应用程序的主要攻击点
  - 身份验证
  - 会话管理
  - 数据库操作
  - 输入数据合法/合理性检查

Web应用安全辅助分析工具

- 浏览器插件
  - 实时地查看和修改传递给Web服务器的数据
  - **TamperData / Live HTTP Header**
- 免费工具集
  - **Web服务器与客户端之间的代理方式运行**
    - **Fiddler，WebScarab，Burp Suite，Paros Proxy和SPIKE Proxy**
  - 结合爬虫的评估与漏洞探测工具
    - **Whisker与Libwhisker / Nikto / N-Stealth**
  - 黑客渗透测试工具：**NBSI、HDSI、Domain**
- 商业Web应用安全评估系统和漏洞扫描器
  - **IBM－Appscan、HP WebInspect、WVS、极光、Jsky**

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

- 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

- 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

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

OWASP Top ten

位次	OWASP 组织 2007 年公布的 Top 10	OWASP 组织 2010 年公布的 Top 10
1	XSS 跨站脚本	代码注入攻击
2	代码注入攻击	XSS 跨站脚本
3	恶意文件执行	不安全的身份认证和会话管理
4	不安全的直接对象引用	不安全的直接对象引用
5	CSRF 跨站请求伪造	CSRF 跨站请求伪造
6	信息泄露与不恰当的错误处理	不安全的配置
7	不安全的身份认证和会话管理	不安全的加密存储
8	不安全的加密存储	未限制 URL 访问
9	不充分的传输层保护	不充分的传输层保护
10	未限制 URL 访问	未经安全验证的重定向和前进链接

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	总装备部、国家级、100 万元（项目编号：41[redacted].2）	排名
9、炮塔[redacted]处理技术	兵器工业集团公司、部级、30 万元（项目编号：40[redacted]02）	排名

25、炮塔[redacted]处理技术 GF 报告	2002 年 11 月	第 1 作者
25、复杂结构件[redacted]熔覆技术 GF 报告	2002 年 11 月	第 1 作者
26、复杂结构件[redacted]熔覆技术 GF 报告	2003 年 11 月	第 1 作者
27、复杂结构件[redacted]熔覆技术 GF 报告	2004 年 12 月	第 1 作者
28、复杂结构件[redacted]熔覆技术 GF 报告	2005 年 12 月	第 1 作者
29、数控技术编程与实验指导书	2003 年、2005 年	参与、第
30、粉末冶金摩擦片[redacted]方法	国防专利、申请号 20041[redacted].9，2004 年 7 月 22 日	第二申请

[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 ...

jpkc.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：雷嘉 (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。

<img src='http://rec.ynet.com/adview.php?what=zone:160&n=ab22e4d2' border='0' alt=''>

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的恶意攻击和篡改。假造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。

事隔一个月，国内两所顶级学府相继遭到黑客攻击，并都冒充校长之名批评高等教育，这让众多网友和大学生怀疑，两起事件是否是同一黑客所为。

网页篡改站点列表

www.zone-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

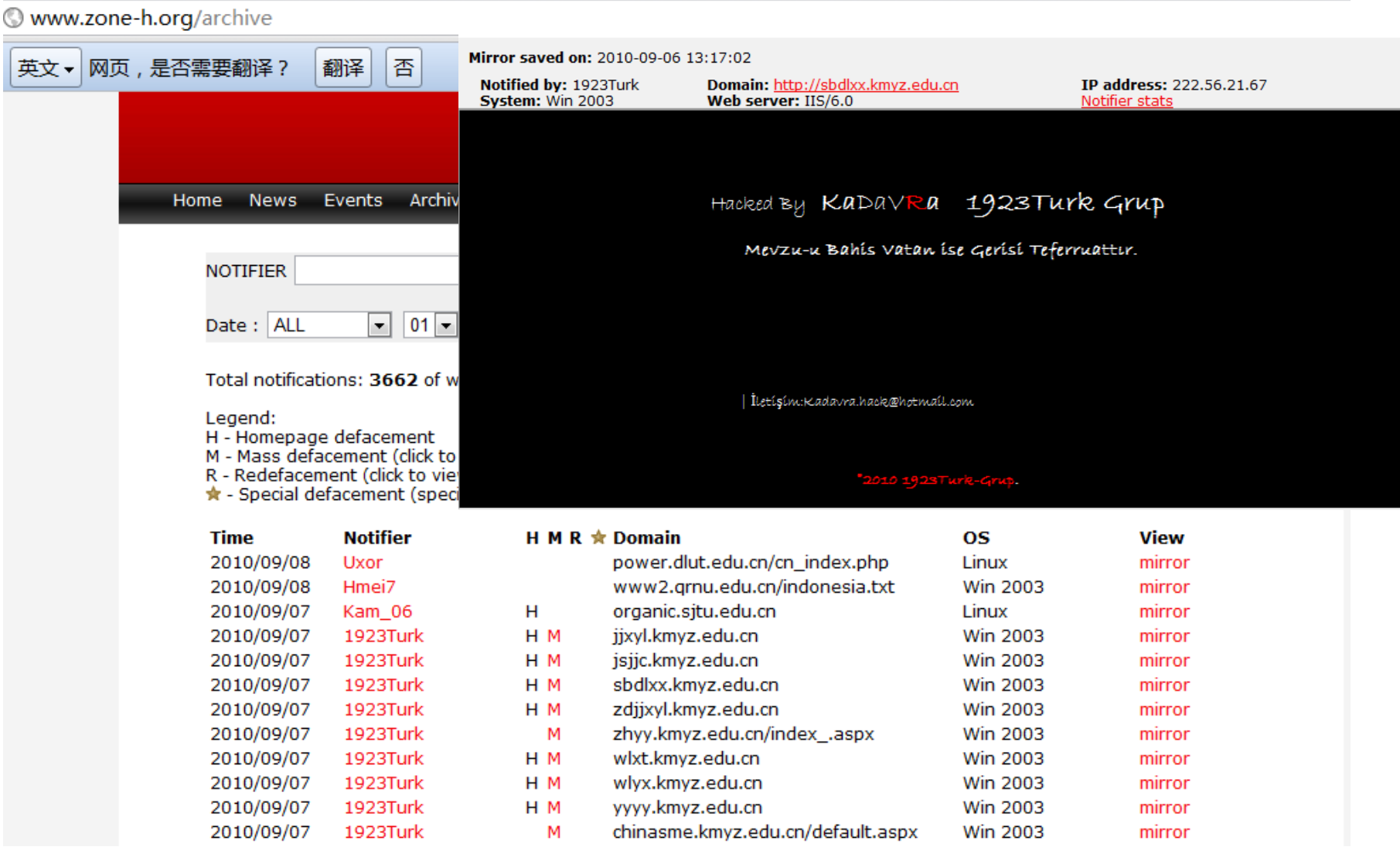
Search: edu.cn 提交者 组织名 IP 域名 精确 Search 黑 页 提 交

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[4938]	2010-09-04	☆烟/mg愁☆	http://jzt.gdcc.edu.cn/UploadThumbs/20109322183652.asp	快照
NO2:ew[2848]				
NO3:用幸福触摸 ...[2351]	2010-09-04	☆烟/mg愁☆	http://jiuye.nxtvu.edu.cn/admin/passt.asp	快照
NO4:霸业永峰[1681]	2010-09-02	DragonEgg	http://xshc.sxnu.edu.cn/test.htm	快照
NO5:八神[1551]	2010-08-27	叩叩喃喃	http://www.jku.edu.cn/about/zywx/js/dd.txt	快照
NO6:网络小子[1271]	2010-08-25	DragonEgg	http://kygl.zzia.edu.cn/News/admin/admin_new.asp	快照
NO7:寒水芊芊[1085]	2010-08-23	流浪丛	http://jiguan.gzhnc.edu.cn/1.txt	快照
NO8:糊涂工作室[1078]	2010-08-23	黑冰网络残总	http://kczx.szlg.edu.cn/cange520.asp	快照
NO9:波哥VS布冯[1075]	2010-08-22	流浪丛	http://www.gcx.xcvtc.edu.cn/djtx.htm	快照
NO10:木鱼工作室[1039]	2010-08-21	tsinghua	http://www.env.tsinghua.edu.cn/upfile/test.asp	快照
NO11:Timeless[1023]	2010-08-19	小黑	http://www.gznc.edu.cn/uploadfile/xh.htm	快照
NO12:红领巾卜封心[875]	2010-08-18	帅气凌云	http://jisuanji.jyu.edu.cn/shuishougailun/uppic/wolf.asp	快照
NO13:Cracker-Mr.X[856]				
NO14:HacKerCc[838]				
NO15:黑羽...燃[816]				
NO16:电脑迷[786]	2010-08-17	帅气凌云	http://jkb.sut.edu.cn/add/s.html	快照
NO17:hackzwy[709]	2010-08-16	Trotou	http://www.blcu.edu.cn/hyxy/web/lxs/uppic/tro.htm1	快照
NO18:黑侠[708]				
NO19:Mistakes[696]	2010-08-14	isosky	http://xsc.ruc.edu.cn/isosky.txt	快照
NO20:WebShell[692]				

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 (speci

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

Notified by: 1923Turk **Domain:** http://sbdlxx.kmyz.edu.cn **IP address:** 222.56.21.67
System: Win 2003 **Web server:** IIS/6.0 Notifier stats

Hacked By KaDaVRa 1923Turk Grup

Mevzu-u Bahis Vatan ise Gerisi Teferruattır.

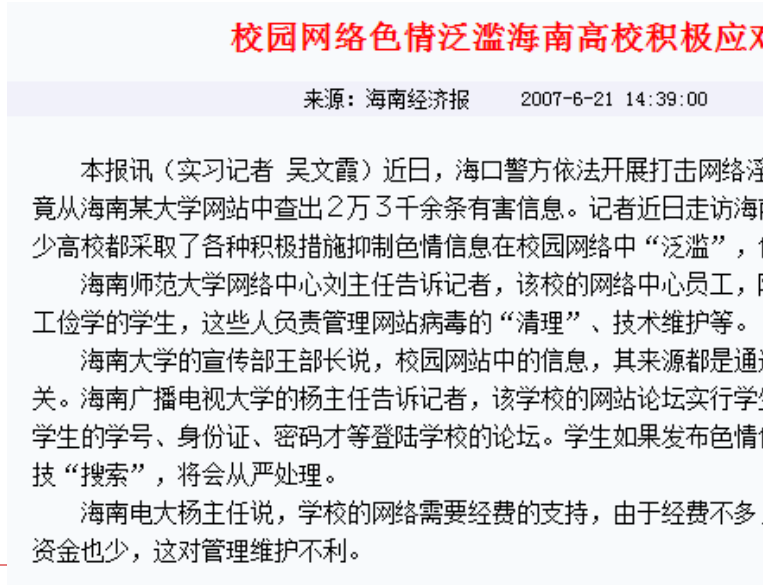
| İletişim:Kadavra.hack@hotmail.com

©2010 1923Turk-Grup.

Time	Notifier	H	M	R	★	Domain	OS	View
2010/09/08	Uxor					power.dlut.edu.cn/cn_index.php	Linux	mirror
2010/09/08	Hmei7					www2.qrnu.edu.cn/indonesia.txt	Win 2003	mirror
2010/09/07	Kam_06	H				organic.sjtu.edu.cn	Linux	mirror
2010/09/07	1923Turk	H	M			jjxyl.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk	H	M			jsjjc.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk	H	M			sbdlxx.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk	H	M			zdjjxyl.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk		M			zhyy.kmyz.edu.cn/index_.aspx	Win 2003	mirror
2010/09/07	1923Turk	H	M			wlxt.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk	H	M			wlyx.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk	H	M			yyyy.kmyz.edu.cn	Win 2003	mirror
2010/09/07	1923Turk		M			chinasme.kmyz.edu.cn/default.aspx	Win 2003	mirror

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
竟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
关。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.eol.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

首经贸在职读研 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 面经大全
- 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

校园情侣的卿卿我我、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

Thanks

诸葛建伟

zhugejw@gmail.com