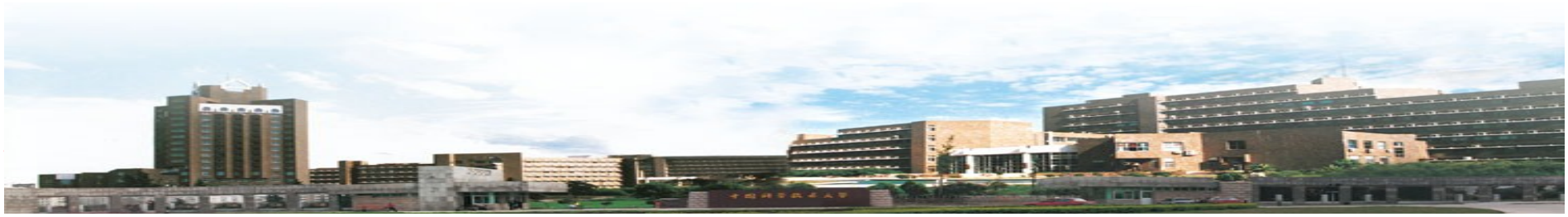
Web安全

程绍银

sycheng@ustc.edu.cn



本章内容

- Web技术简介
- Web安全需求
- Web安全面面观
- Web服务器安全策略
- Web浏览器安全策略
- Web网站入侵

本章内容

- ✓ Web技术简介
- Web安全需求
- Web安全面面观
- Web服务器安全策略
- Web浏览器安全策略
- Web网站入侵

Web技术简介

- 20世纪80年代末，Berners-Lee和他的助手创建了一个从各种各样资源中链接信息的接口。最终的结果是定义了URL、HTTP和HTML等规范，而WWW (World Wide Web)就基于此
- 今天，Web技术可使用户创建格式化的信息页面，而这些页面又可“链接”到其他信息页面并访问整个网络
- 简言之，Web是可通过Web浏览器访问的信息集合
- 第一个重要的Web浏览器是Mosaic；曾经流行的Netscape Navigator；当前，主流浏览器是IE、Firefox、Chrome等

Web技术简介

- 除文字外，Web页面还包括图像、声音、动画及其他特殊的效果。单独的页面能被链接到其他页面，以提供对附加信息的访问
- Web的发展速度是惊人的，但是Internet 和Web对于各种安全泄密非常脆弱。因此，各个机构对于Web安全的要求在逐渐增加
- WWW为用户带来世界范围的超级文本服务。此外，WWW还可以为用户提供传统的因特网服务，如Telnet、FTP、Gopher、Usernet、News等
- 基于Web的开发技术有Java、XML、Ejb、Jboss、Linux、Mysql等

Web服务器

- 从硬件上来说，服务器是指具有固定的地址，并为网络用户提供服务的节点，它是实现资源共享的重要组成部分
- 服务器是一种高性能计算机，作为网络的节点，存储、处理网络上80%的数据、信息，因此也称为网络的灵魂
- 从软件的角度上，Web服务器是驻留在服务器上的一个程序，使用超文本传输协议HTTP(hypertext transfer protocol)，它和用户方面的浏览器不断地传送各种信息
- Web服务器的作用就是管理WWW的大量信息，处理用户发来的各种请求，将满足用户要求的信息返回给用户

Web服务器的安全区域

- Web服务器是Internet上最暴露的服务器
- 如果说用于防止Internet从内部网络进行攻击的防火墙是最重要网络安全领域的话，Web服务器就可以说是第二个需要高度安全的领域了
- 服务器安全由几个安全区域组成，安全必须在每一个区域得以实现
  - 基础设施区。该区用于定义服务器在网络中的位置。这个区域必须能够防止数据窃听、网络映射和端口扫描等黑客技术的威胁

Web服务器的安全区域

- 网络协议区。该区一般指的是TCP/IP通信。操作系统内核对通信负责并保证一个透明的通信流，因此内核必须经过必要的配置
- 服务区。该区定义需要哪些服务。服务器上最好只配置完成必要操作所必须的服务
- 应用区。为安全起见，每个服务最好单独配置，否则可能被用来发送垃圾邮件
- 操作系统区。最后的保护机制是操作系统本身

Web浏览器

- Web浏览器是一个安装在硬盘上用于阅读Web信息的客户端的应用软件，是一个面向WWW的窗口
- 浏览器在很大程度上决定了能看到或不能看到什么，能做或不能做什么。浏览器在网络上与Web服务器打交道，从服务器上下载文件，把在互联网上找到的文本文档(和其他类型的文件)翻译成网页
- HTML是网络的格式化语言
- 浏览器的缓存(cache)是另一个重要的因素

HTTP协议

- HTTP(超文本传输协议)是WWW浏览器和WWW服务器之间的应用层通信协议，是用于分布式协作超文本信息系统的、通用的、面向对象的协议。它是C/S(client/server)结构的协议，允许用户接收另一台计算机上的信息。
- HTTP协议通过扩展命令，可用于类似的任务，如域名服务或分布式面向对象系统
- HTTP会话过程包括4个步骤: 连接、请求、应答和关闭
- HTTP协议是基于TCP/IP之上的协议，它不仅保证正确传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示等

HTML语言

- HTML即超文本标记语言，是用于创建Web文档)的编程语言，是WWW的描述语言
- HTML文本是由HTML命令组成的描述性文本，HTML命令可以说明文字、图形、动画、声音、表格、链接等
- HTML的结构包括头部(Head)、主体(Body)两大部分，其中头部描述浏览器所需的信息，而主体则包含所要说明的具体内容
- 设计HTML语言的目的是为了能把存放在一台计算机中的文本或图形与另一台计算机中的文本或图形方便地联系在一起，形成有机的整体

HTML语言

- HTML文档看起来与网页在浏览器上显示的不同，在屏幕上看到的网页是浏览器对HTML文档的翻译；所看到的图像被HTML文档调用，但是却是独立的文档
- 浏览器从HTML代码中读取图像的位置，然后把它们放在网页上。同样，音频或视频文件也被HTML文件调用，然后被浏览器组装
- HTML 5：下一代web开发标准

CGI公共网关接口

- CGI(common gateway interface)是一个连接外部应用程序到信息服务器(比如HTTP或者网络服务器)的标准，是连接主页和应用程序的接口
- 一般来说，CGI标准接口的功能就是在超文本文档与服务器应用程序之间传递信息。通过提供这样一个标准接口，Web服务器能够执行应用程序并将它们的输出
- 在物理上，CGI是在Web服务器端运行的一个可执行程序，提供同客户端 HTML页面的接口，由主页的一个热链接激活进行调用，并对该程序的返回结果进行处理，显示在主页上

CGI公共网关接口

- HTML语言的功能难以完成诸如访问数据库等一类的操作，CGI就是为了扩展主页的功能而设立的。随后，诸如PHP、ASP、ISAPI、NSAPI、IDC等技术也发展起来了。可以用任何一种熟悉的高级语言如C、C++、C Shell和VB编程语言来编写
- 一个简单的HTML文档是无交互的后台程序，它是静态的，处于一个不可变的状态，即文本文件不可以变化。相反地，CGI程序可以实时执行，它可以输出动态的信息
- 目前有几种信息交互式程序语言不需要在服务器上执行，而可以直接在客户机上执行并显示结果，例如: Java Applet、JavaScript、ActiveX以及VBScript

Web 2.0

- Web2.0 是相对Web1.0 的新的一类互联网应用的统称
- Web1.0 的主要特点在于用户通过浏览器获取信息。Web2.0 则更注重用户的交互作用，用户既是网站内容的浏览者，也是网站内容的制造者
- 例子
  - 博客/微博
  - 个人网站
  - 维基百科全书
  - BT/PT下载

Web 2.0特征

- 多人参与
  - Web1.0里，互联网内容是由少数编辑人员（或站长）定制的，比如sina；在Web2.0里，每个人都是内容的供稿者
  - Web2.0的内容更多元化：标签tag、多媒体、在线协作等等
  - 在Web2.0信息获取渠道里，RSS订阅扮演者一个很重要的作用
- 人是灵魂
  - 在互联网的新时代，信息是由每个人贡献出来的。各个人共同组成互联网信息源。Web2.0的灵魂是人
- 可读可写互联网
  - 在Web1.0里，互联网是“阅读式互联网”，而Web2.0是“可写可读互联网”。虽然每个人都参与信息供稿，但在大范围里看，贡献大部分内容的是小部分的人
- Web2.0的元素
  - Web2.0包含了我们经常使用到的服务，例如博客、播客、维基、P2P下载、社区、分享服务等等
- Web2.0更加重要
  - Web2.0实际上是对Web1.0的信息源进行扩展，使其多样化和个性化。
  - 博客是Web2.0里十分重要的元素，因为它打破了门户网站的信息垄断，在未来里，博客的地位将更为重要

Web 2.0七大原则

- 互联网作为平台
- 利用集体智慧
- 数据库管理是Web 2.0公司的核心竞争力
- 软件发布周期的终结
- 轻量型编程模型
- 软件超越单一设备 -- 云计算
- 丰富的用户体验

Web 3.0

- 用来概括互联网发展过程中可能出现的各种不同的方向和特征，包括
  - 将互联网本身转化为一个泛型数据库
  - 跨浏览器、超浏览器的内容投递和请求机制
  - 人工智能技术的运用
  - 语义网
  - 地理映射网
  - 运用3D技术搭建的网站甚至虚拟世界或网络公国等
  - 物联网 – IBM提出“智慧地球”

本章内容

- Web技术简介
- ✓ Web安全需求
- Web安全面面观
- Web服务器安全策略
- Web浏览器安全策略
- Web网站入侵

Web的优点与缺点

- 计算机网络技术的发展和应用，特别是Internet的出现，开创了计算机应用的崭新局面。信息的交互和共享，已经突破了国界，遍及整个世界。这种互连性和开放性给社会带来了极大的效益。同时，入侵者也得到了更多的机会，他们所造成的危害也波及到了更广泛的范围
- 一个Web站点，只要与Internet相连，就可以被所有人访问。Web的精华是交互性，这也正是它的致命弱点

Web安全风险与体系结构

- 世界上不存在没有风险的信息服务
- Web安全风险一般分为两类
  - 机密信息被窃取
  - 数据和软硬件系统被破坏
- 两类风险的危害都不可低估。尽管不可能保证绝对安全，但是应采取一些方法列出在各种情况下可能因为信息服务而带来的系统不安全性

Web安全风险

- Web服务器的信息被破译
  - Web服务器的信息(如口令、密匙等)被破译，最终导致闯入者进入服务器
  - 最常见也是最有效的保护是使用防火墙来保护Web站点，防止入侵者的袭击
- Web上的文件被未经授权的个人访问
  - Web上的文件被未经授权的个人访问，损害了文件的隐私性、机密性和完整性
  - 所以，必须采取口令、加密和防火墙等措施

Web安全风险

- 信息被截获
  - 当远程用户向服务器传输信息时，交易被截获
  - 在站点上进行交易时，可以通过数字化签名，确信该交易是可靠的
- 系统中的bug
  - 系统中的bug，使得黑客可以远程对Web服务器发出指令
  - 由此导致对系统进行修改和破坏
- 用CGI脚本编写的程序
  - 用CGI脚本编写的程序涉及远程用户从浏览器中在主机上直接操作命令时，会给Web主机系统造成危险。尽量避免CGI程序中存在漏洞

Web体系结构安全

- Web服务器软件和客户端软件是一个大系统的一小部分，这个系统大都由以下构件组成：客户端软件(就是Web浏览器)、客户端的操作系统、客户端的局域网(LAN)、Internet、服务器端的局域网(LAN)和服务器上的Web服务器软件
- 在分析和评估Web服务的安全性时要考虑所有这些成分。它们互相联系，每一个部分都会影响Web服务器的安全性，其中安全性最差的决定了给定服务的安全级别

Web的安全需求

- 服务器端/客户端是分别针对网络服务器/网络工作站(客户机)设计的，承担着对当前服务器/工作站上病毒的实时监控、检测和清除，自动向系统中心报告病毒监测情况，以及自动进行升级的任务
- 每次用户与站点建立连接，他们的客户机向服务器传送机器的数字IP地址。有时，Web站点接到的IP地址可能不是客户的地址，而是他们的请求所经过的代理服务器的地址。服务器看到的是代表客户所要文档的服务器的地址。使用HTTP协议，客户也可以向Web服务器表明发出请求的用户名

Web的安全需求

- 如果不要求服务器获得这类消息，服务器首先会将数字IP地址转换为客户的域名。为了将IP地址转化为域名，服务器与一个域名服务器联系，向它提供这个IP地址，从那里得到相应的域名
- 当Web服务器获得IP地址和客户可能的域名，它就开始一系列验证手段以决定客户是否有权访问他要求的文档
- 在这些过程中，存在着安全漏洞，应加强服务器的安全

Web的安全需求

- 作为访问网络的一扇重要窗口，浏览器安全的重要性是不言而喻的。有不少对计算机的攻击都是利用浏览器漏洞而进行的
- 客户机与站点之间建立联系，进行数据交换，称为传输。一般认为，Web由传输协议(HTTP)、数据格式(HTML)以及浏览器(IE等)组成。使用协议、数据格式或浏览器，无需任何特别要求。Web擅长交叉连接，允许使用不同的文本格式、协议及应用程序
- 信息连接不停地更新、重建与改变，有助于安全的需求。而且也有助于定义所提供服务的质量及传输更新

本章内容

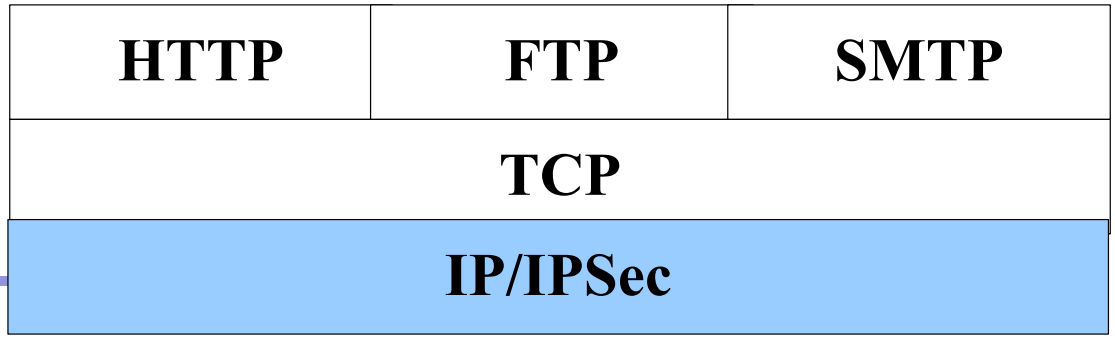
- Web技术简介
- Web安全需求
- ✓ Web安全面面观
- Web服务器安全策略
- Web浏览器安全策略
- Web网站入侵

Web安全 -- TCP/IP协议的角度

- Web是一个运行于Internet/Intranet之上的基本的Client/Server应用。Web安全性涉及前面讨论的所有计算机与网络的安全性内容。同时还具有新的挑战。Web具有双向性，Web Server易于遭受来自Internet的攻击，而且实现Web浏览、配置管理、内容发布等功能的软件异常复杂，其中隐藏许多潜在的安全隐患
- 实现Web安全的方法很多，从TCP/IP协议的角度可以分成3种：网络层安全性、传输层安全性和应用层安全性

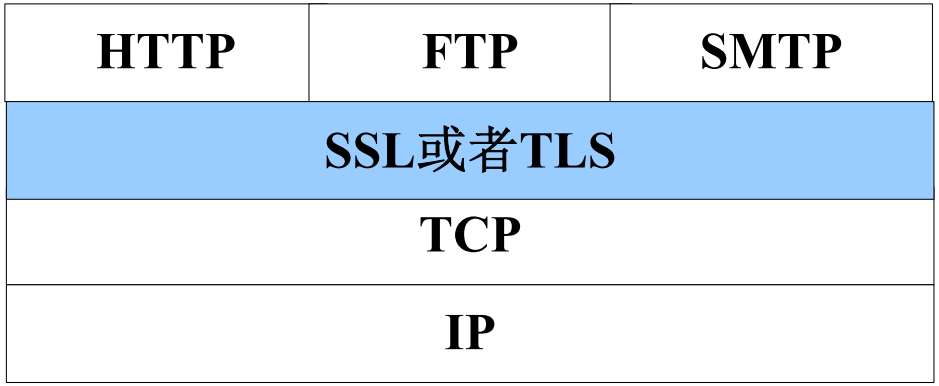
网络层安全性

- 传统的安全体系一般都建立在应用层上。这些安全体系虽然具有一定的可行性，但也存在着巨大的安全隐患，因为IP包本身不具备任何安全特性，很容易被修改、伪造、查看和重播
- IPSec可提供端到端的安全性机制，可在网络层对数据包进行安全处理。IPSec可以在路由器、防火墙、主机和通信链路上配置，实现端到端的安全、虚拟专用网络和安全隧道技术等
- 基于网络层使用IPSec来实现Web安全的模型



传输层安全性

- 在TCP传输层之上实现数据的安全传输是另一种安全解决方案，安全套接层SSL和TLS（Transport Layer Security）通常工作在TCP层之上，可以为更高层协议提供安全服务



应用层安全性

- 将安全服务直接嵌入在应用程序中，从而在应用层实现通信安全
- SET（Secure Electronic Transaction，安全电子交易）是一种安全交易协议，S/MIME、PGP是用于安全电子邮件的一种标准。它们都可以在相应的应用中提供机密性、完整性和不可抵赖性等安全服务

<table>
<tr><td></td><td>S/MIME</td><td>PGP</td><td>SET</td></tr>
<tr><td>Kerberos</td><td colspan="3" rowspan="2">SMTP, HTTP</td></tr>
<tr><td>UDP</td></tr>
<tr><td colspan="2">TCP</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">IP</td></tr>
</table>

Web安全 -- 系统安全的角度

- Web服务器端的安全
  - 服务器，如Apache
  - 数据库，如mysql
  - 解释器，如PHP/Python/Perl
- Web浏览器的安全
  - 浏览器，如IE/Firefox/Chrome等
  - 杀毒软件、木马检测软件，如Nod 32/360安全卫士等

Web安全－代码安全的角度

- 06年CWE排名前三位的漏洞类型：
  - XSS：跨站脚本攻击
  - sql-inject：sql注入
  - php-include：

Table 1: Overall Results

Rank	Flaw	TOTAL	2001	2002	2003	2004	2005	2006
Total		18809	1432	2138	1190	2546	4559	6944
[1]	XSS	13.8%	02.2% (11)	08.7% (2)	07.5% (2)	10.9% (2)	16.0% (1)	18.5% (1)
		2595	31	187	89	278	728	1282
[2]	buf	12.6%	19.5% (1)	20.4% (1)	22.5% (1)	15.4% (1)	09.8% (3)	07.8% (4)
		2361	279	436	268	392	445	541
[3]	sql-inject	09.3%	00.4% (28)	01.8% (12)	03.0% (4)	05.6% (3)	12.9% (2)	13.6% (2)
		1754	6	38	36	142	588	944
[4]	php-include	05.7%	00.1% (31)	00.3% (26)	01.0% (13)	01.4% (10)	02.1% (6)	13.1% (3)
		1065	1	7	12	36	96	913
[5]	dot	04.7%	08.9% (2)	05.1% (4)	02.9% (5)	04.2% (4)	04.3% (4)	04.5% (5)
		888	127	110	34	106	196	315
[6]	infoleak	03.4%	02.6% (9)	04.2% (5)	02.8% (6)	03.8% (5)	03.8% (5)	03.1% (6)
		646	37	89	33	98	175	214
[7]	dos-malform	02.8%	04.8% (3)	05.2% (3)	02.5% (8)	03.4% (6)	01.8% (8)	02.0% (7)
		521	69	111	30	86	83	142
[8]	link	01.8%	04.5% (4)	02.1% (9)	03.5% (3)	02.8% (7)	01.9% (7)	00.4% (16)
		341	64	45	42	72	87	31
[9]	format-string	01.7%	03.2% (7)	01.8% (10)	02.7% (7)	02.4% (8)	01.7% (9)	00.9% (11)
		317	46	39	32	62	76	62
[10]	crypt	01.5%	03.8% (5)	02.7% (6)	01.5% (9)	00.9% (16)	01.5% (10)	00.8% (13)
		278	55	58	18	22	69	56
[11]	priv	01.3%	02.5% (10)	02.2% (8)	01.1% (12)	01.3% (11)	01.5% (11)	00.8% (14)
		249	36	46	13	33	67	54
[12]	perm	01.3%	02.7% (8)	01.8% (11)	01.3% (11)	00.9% (15)	01.1% (13)	01.1% (9)
		241	39	39	15	24	48	76
[13]	metachar	01.2%	03.8% (6)	02.6% (7)	00.7% (18)	01.0% (14)	01.3% (12)	00.4% (17)
		233	55	56	8	26	59	29
[14]	int-overflow	01.0%	00.1% (32)	00.4% (25)	01.3% (10)	01.8% (9)	00.8% (14)	01.2% (8)
		190	1	8	16	47	36	82
[15]	auth	00.8%	01.5% (13)	01.3% (15)	00.5% (19)	00.7% (17)	00.5% (19)	00.9% (12)
		155	22	27	6	17	21	62
[16]	dos-flood	00.7%	02.0% (12)	01.7% (13)	00.5% (20)	01.2% (12)	00.2% (27)	00.4% (19)
		138	29	36	6	31	11	25

http://cwe.mitre.org/documents/vuln-trends/index.html

本章内容

- Web技术简介
- Web安全需求
- Web安全面面观
- ✓ Web服务器安全策略
- Web浏览器安全策略
- Web网站入侵

Web服务器上的漏洞

- 在Web服务器上，客户得不到要访问的秘密文件、目录或重要数据
- 从远程用户向服务器发送信息时，特别是信用卡之类东西时，中途遭不法分子非法拦截
- Web服务器本身存在一些漏洞，使得一些人能侵入到主机系统，破坏一些重要的数据，甚至造成系统瘫痪

Web服务器上的漏洞

- CGI安全方面的漏洞有: 有意或无意在主机系统中遗漏bug给非法黑客创造条件；用CGI脚本编写的程序当涉及远程用户从浏览器中输入表格(Form)，并进行检索(Search index)，或form-mail之类在主机上直接操作命令时，会给Web主机系统造成危险
- 还有一些简单地从网上下载的Web服务器，没有过多考虑到一些安全因素，不能用作商业应用
- 综上所述，不管是配置服务器，还是在编写CGI程序时都要注意系统的安全性。应该堵住任何存在的漏洞，创造安全的环境

Apache相关漏洞

分页 (29) < [1] 2 3 4 5 6 ... > 共 425 条记录

- 2010-12-02 Awstats Apache Tomcat配置文件远程任意命令执行漏洞
- 2010-12-01 Apache Tomcat "sort"和"orderBy"参数跨站脚本执行漏洞
- 2010-11-04 Apache Shiro URL路径目录遍历漏洞
- 2010-11-03 Apache Archiva跨站请求伪造漏洞
- 2010-10-29 Spring Security URI路径参数绕过安全限制漏洞
- 2010-10-26 SAP BusinessObjects多个远程安全漏洞
- 2010-10-20 SAP BusinessObjects Axis2组件默认口令漏洞
- 2010-10-12 Apache APR-util apr_brigade_split_line函数远程拒绝服务漏洞
- 2010-10-11 Apache QPID SSL连接拒绝服务漏洞
- 2010-10-05 Subversion mod_dav_svn模块绕过安全限制漏洞
- 2010-10-01 Apache XML-RPC信息泄露漏洞
- 2010-09-25 FreePBX系统记录菜单任意文件上传漏洞
- 2010-09-10 Apache Traffic Server远程DNS缓存投毒漏洞
- 2010-08-18 Apache CXF XML文档类型声明处理漏洞
- 2010-08-18 Apache CouchDB跨站请求伪造漏洞

定制Web服务器的安全策略和安全机制

- 安全策略是由个人或组织针对安全而制定的一整套规则和决策。每个Web站点都应有一个安全策略，这些安全策略因需而异。对Web服务提供者来说，安全策略的一个重要的组成是哪个人可以访问哪些Web文档，同时还定义获权访问Web文档的人和使用这些访问的人的有关权力和责任
- 安全机制是实现安全策略的手段或技术。必须根据需要和目标来设置安全系统，估计和分析风险。定义安全策略，选择一套安全机制

安全机制的选择

- 首先要做的是威胁分析，主要包括以下几个方面：
  - 确定安全保护的目标
  - 研究谁会对网络进行攻击
  - 分析会有什么样的威胁
  - 提出价格合理的安全机制
- 反复测试此过程，随时改变其不足之处

安全机制的选择

- 在具体服务器设置及编写CGI程序时应该注意：
  - 禁止乱用从其他网站下载的一些工具软件，并在没有详细了解之前尽量不要用root身份注册执行，以防止某些程序员在程序中设下的陷阱
  - 在选用Web服务器时，应考虑到不同服务器对安全的要求不一样
  - 在利用Web中的.htpass来管理和校验用户口令时，校验的口令和用户名不受次数限制

安全机制的选择

- 对Web服务器和Web客户来说，最重要的安全机制如下:
  - 主机和网络的配套工具和技术
  - Web应用程序的配置
  - Web服务的认证机制
  - 防火墙
  - 日志和监视
- 每个机制都涉及某种类型的系统不安全性，它们相互联系

认真组织Web服务器

- 大多数Web服务器记录它们收到的每一次连接和访问。一些浏览器和服务器一样，甚至也能提供如有关使用中的浏览器、URL、客户从哪里来以及用户的E-mail地址等信息。这些记录对于分析服务器的性能，发现和跟踪黑客袭击是很有用的
- 组织Web服务器一般包括以下几个方面的内容: 认真选择Web服务器设备和相关软件；配置Web服务器，使用它的访问和安全特性；组织和Web服务器相关的内容

认真组织Web服务器

- 组织主要包括以下步骤：
  - 连机检查。检查源程序，查看连接URL和相应的内容是否图文一致，查看URL所提供的内容是否和网页的描述一致。检查驱动器和共享的权限，系统设为只读状态
  - 将敏感文件放在基本系统中，再设二级系统，使所有的敏感数据不向Internet开放
  - 充分考虑最糟糕的情况后，配置自己的系统，即使黑客完全控制了系统，他还要面对一堵高墙
  - 检查HTTP服务器使用的Applet脚本，尤其是与客户交互作用的CGI脚本，防止非法用户恶意使用CGI程序，执行内部指令，造成破坏

安全管理Web服务器

- 安全管理Web服务器，可以从以下几个方面采取一些预防措施
  - 限制在Web服务器开账户，定期删除一些短进程的用户
  - 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
  - 尽量在不同的服务器上运行不同的服务。尽量使FTP,mail等服务器与之分开，去掉一些无关应用
  - 如不需要，尽量关闭Web服务器上的特性服务。
  - 定期查看服务器中的日志logs文件

安全管理Web服务器

- 设置好Web服务器上系统文件的权限和属性
- 有些Web服务器把Web的文档目录与FTP目录指在同一目录，应该注意不要把FTP的目录与CGI-BIN指定在一个目录之下
- 通过限制许可访问用户IP或DNS

- 另外，许多Web服务器本身都存在一些安全上的漏洞，都需要在版本升级时不断解决
- 无论多么安全的站点，都可能被破坏，都有可能遭到黑客的攻击。所以，一定要沉着冷静地处理意外事件

Web服务器的安全措施

- 从基本做起
  - 这是最保险的方式。将服务器上含有机密数据的区域都转换成NTFS格式；防毒程序也必须按时更新，建议同时在服务器和桌面计算机上安装防毒软件，这些软件可设定成每天自动下载最新的病毒定义文件。邮件服务器上也安装上防毒软件
  - 另一个保护网络的好方法是限定使用者登录网络的权限
  - 存取网络上的任何数据都必须通过密码登录。在设定密码时，混用大小写字母、数字和特殊字符。还要设定定期更新密码，密码长度不得少于8个字符

Web服务器的安全措施

- 保护备份
  - 最好利用密码保护好磁盘，若备份程序支持加密功能，还可以将数据进行加密。
- 使用RAS的回拨功能
  - 如果远端用户经常是从家里或是固定的地方上网，可以使用回拨功能
  - 另一个办法是限定远端用户只能存取单一服务器。最后就是在RAS服务器上使用“另类”网络协议
- 工作站的安全问题
  - 对于初学者，可以在所有工作站上使用Windows 2000，也可以使用Windows NT。这样就能将工作站锁定，若没有权限，将很难取得网络配置信息
  - 限制使用者只能从特定工作站登录

Web服务器的安全措施

- 执行最新修补程序
  - 在微软公司内部有一组工作人员专门检查并修补安全漏洞，这些修补程序(补丁)有时会被收集成服务包(service pack)发布
  - http://technet.microsoft.com/zh-cn/security/default.aspx
- 颁布严格的安全政策
  - 制定一个强有力的安全策略，确保每一个人都了解，并强制执行
- 7）检查防火墙
  - 仔细检查防火墙的设置
  - 不要公布非必要的IP地址
  - 要查看所有的通信端口，确定不常用的已经全部关闭

本章内容

- Web技术简介
- Web安全需求
- Web安全面面观
- Web服务器安全策略
- ✓ Web浏览器安全策略
- Web网站入侵

Web浏览器安全策略

- 随着电子商务的出现，人们开发了各种跟踪用户活动的方法，其中有两种关键方法是通过Web浏览器实现的
  - IP地址和缓冲(cache)窥探
    - 用户每次访问Web服务器时都将留下痕迹。这个痕迹在不同的服务器上以不同的方法记录下来，包括访问者的IP地址，用户主机名，甚至用户名
  - Cookie
    - Cookie可以用来定制个性化空间
    - Cookie还可以用来记录站点轨迹

浏览器自动引发的应用

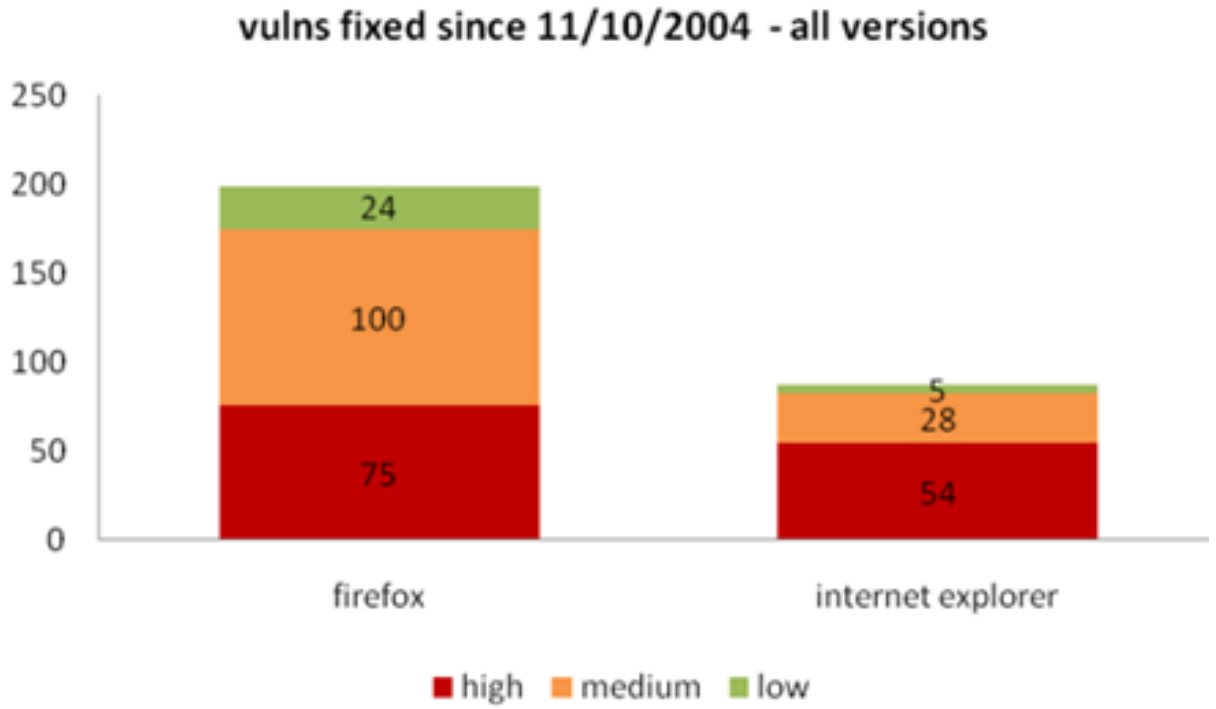
- 浏览器中使用的协议有HTTP、FTP、GOPHER、WAIS(Wide Area Information Servers)等，还包括NNTP和SMTP协议。当用户使用浏览器时，实际上是在申请HTTP等服务器。这些服务器都存在漏洞，是不安全的
- 浏览器一般只能理解一些基本的数据格式，对其他的数据格式，浏览器要通过外部程序来观察。这样，就引入了一些不安全的因素。因此可采取以下措施：
  - 不是默认的外部程序要多加注意
  - 不要允许危险的外部程序进入站点
  - 不要随便地增加外部程序
  - 不要轻信陌生人的建议而随便修改外部程序的配置

Web页面或者下载文件中内嵌的恶意代码

- 现在网络上有很多网站，只要连接到它的页面上，不是IE首页被改就是IE的某些选项被禁用了。一些网页上的恶意代码还可以格式化或删除C: 盘。它的主要行为如下
  - 肆意篡改 IE 浏览器的标题
  - 肆意篡改 IE 浏览器的默认首页
  - 禁止Internet 选项、禁止 IE 右键菜单的弹出或者右键菜单变成灰色无法使用
  - 禁止系统核心注册表的任何操作
- 对于这些恶意修改，可以用360安全卫士等工具来将IE修复到默认状态

浏览器本身的漏洞及泄露的敏感信息

- IE浏览器
  - MS09-072：5个IE漏洞
  - MS09-054：4个IE漏洞
- Firefox浏览器



浏览器本身的漏洞及泄露的敏感信息

- 为了减小危害，建议的应对措施是关闭Internet Explorer浏览器中的Active脚本。可以在Internet Explorer浏览器中执行“工具”|“选项”命令，在弹出的对话框中选取“安全”选项卡，点击“默认级别”按钮，确认IE设置安全级为“中级”及以上，最后点击“确定”按钮完成设置
- 另外，MHTML文件重定向并执行漏洞在Outlook Express中更容易被利用，可以在不打开邮件的情况下自动下载并执行网络上的恶意程序。建议将Outlook Express设置如下:
  - 执行“工具”|“选项”命令，在弹出的菜单中点击“安全”选项卡，将“选择要使用的 Internet Explorer 安全区域”设置为“受限站点区域(较安全)”

Web欺骗

- E-mail欺骗
  - E-mail欺骗表现形式有所不同，但原理相同。通常是骗用户进行一个毁坏性的操作或暴露其敏感信息
- E-mail欺骗会制造安全漏洞
  - E-mail宣称来自于系统管理员，要求用户将他们的口令改变为特定的字串。那么用户应该了解，任何MIS人员都不会用E-mail发出这样的要求。
  - 由于简单的邮件传输协议(STMP)没有验证系统，伪造E-mail十分方便。应该花一定的时间来查看E-mail错误信息，其中会经常有闯入者的线索

Web欺骗

- IP电子欺骗
  - IP电子欺骗就是伪造某台主机的IP地址的技术。即用一台机器来扮演另一台机器，以达到蒙混过关的目的。被伪造的主机往往具有某种特权或者被另外的主机所信任
- IP电子欺骗通常都要用编写的程序，发送带有假冒的IP地址的IP数据包，来达到自己的目的。在现有的网上，也有大量的可以发送伪造的IP地址的工具可以使用
- 防范IP电子欺骗可以采用以下措施
  - 在局部网络的对外路由器上加一个限制条件，只要在路由器中设置一个不允许声称来自于内部网络的外来包通过即可

Web欺骗

- 注意与外部网络相连的路由器，看它是否支持内部接口。如果路由器支持内部网络子网的两个接口，就要警惕，因为它容易收到IP欺骗
- 通过对包的监控来检查IP欺骗。用netlog或类似的包监控工具来检查外接口上包的情况，如发现包的两个地址即源地址和目的地址都是本地域地址，就意味有人试图攻击系统
- 安装一个过滤路由器来限制对外部接口的访问，禁止带有内部资源地址包通过。还要禁止(过滤)带有不同于内部资源地址的内部包通过路由器到别的网上去，这样就可以防止内部的用户对别的站点进行IP欺骗

Web浏览器的安全使用

- 浏览器及时升级
  - IE 6, IE 7 → IE8/360安全浏览器
  - Chromeplus
- 浏览器安全设置
  - 自动完成
  - Cookie安全
  - 分级审查
- 防黑于未然
  - 查毒软件：Nod 32
  - 360安全卫士

本章内容

- Web技术简介
- Web安全需求
- Web安全面面观
- Web服务器安全策略
- Web浏览器安全策略
- ✓ Web网站入侵

入侵过程：某省地震局网站

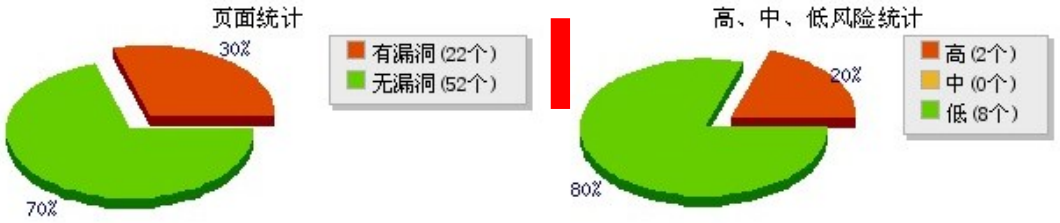
1.综述

任务名称	扫描 [eq. ' gov.cn]
扫描模板	Web应用漏洞(全部)
Web风险	风险值:8.9
域名统计	已扫描域名数：1 非常危险域名：1
信息统计	已扫描的文件：74 有漏洞的文件：22 已扫描的链接：51
时间统计	开始：2012-06-26 16:10:00 结束：2012-06-26 16:27:00 耗时：17 分
系统版本	5.0.10.28

1.1 具有最多安全性问题的文件(TOP5)

URL	漏洞数量
http://eq. .gov.cn/ny_content/	9
http://eq. .gov.cn	8
http://eq. .gov.cn/ny_content/inter.php	5
http://eq. .gov.cn/ny_content/dire.php	3
http://eq. .gov.cn/ny_content/topic_list.php	3

1.2 Web风险分布统计



3.1 域名http://eq.. gov.cn的漏洞信息

漏洞名称	出现次数	详情和解决方法
检测到目标URL存在SQL注入漏洞	5	
检测到目标URL存在跨站漏洞	8	
检测到目标URL存在内部IP地址泄露	1	
目标服务器上存在CGI默认目录	3	
检测到目标服务器上存在web应用默认目录	6	
检测到基于HTTP连接的登录请求	2	

http://eq.. .gov.cn/jingsai/admin.asp

请求方式	GET
URL	http://eq. .gov.cn/jingsai/admin.asp
参考（验证）	http://eq. .gov.cn/jingsai/admin.asp

http://eq.. .gov.cn/phpMyAdmin/

请求方式	GET
URL	http://eq .gov.cn/phpMyAdmin/
参考（验证）	http://eq.. .gov.cn/phpMyAdmin/index.php?lang=zh-gb2312&convcharset=iso-8859-1&collation_connection=utf8_unicode_ci&token=201ff21a700e7d672ac049061877d269&phpMyAdmin=c1e9bd378d6d762bec58e0aa4dfaa864

检测到管理后台登陆入口	4	
检测到flash的allowNetworking参数设置为all	8	
检测到目标网站存在无效链接	11	
检测到目标URL存在电子邮件地址模式	3	

4.漏洞列表

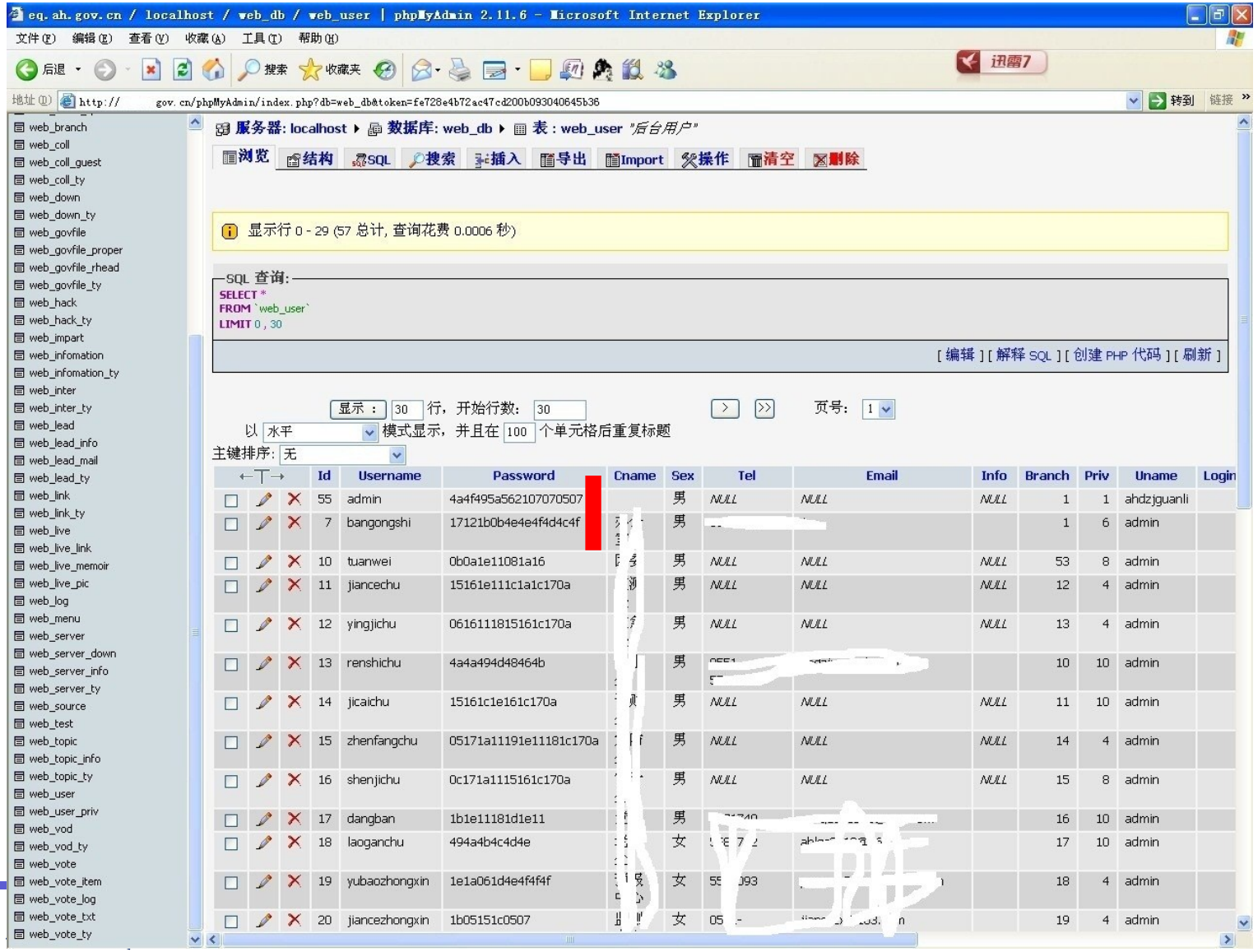
漏洞名称	总出现次数
检测到目标URL存在SQL注入漏洞	5
检测到目标URL存在跨站漏洞	8
检测到目标URL存在内部IP地址泄露	1
检测到目标网站存在无效链接	11
检测到管理后台登陆入口	4
目标服务器上存在CGI默认目录	3
检测到目标服务器上存在web应用默认目录	6
检测到基于HTTP连接的登录请求	2

PhpMyAdmin远程登录数据库

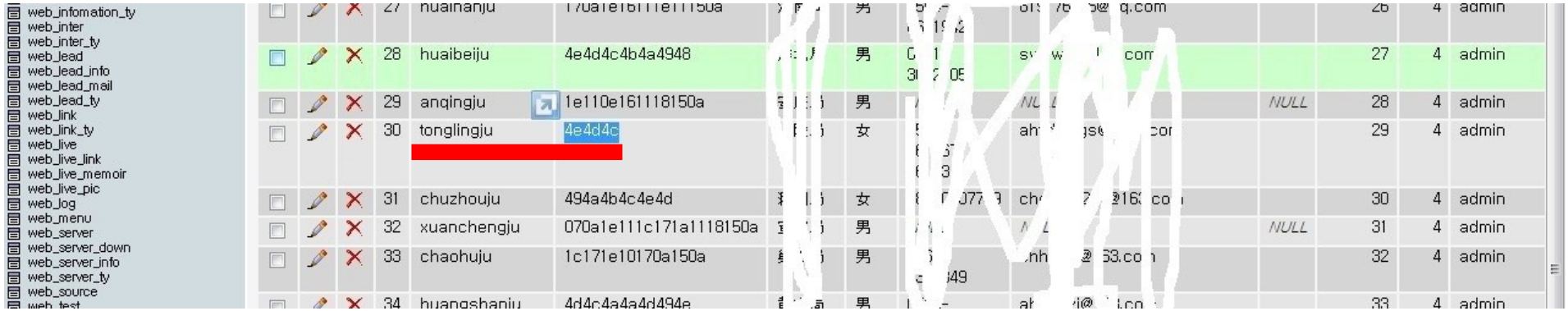
- 典型弱密码
  - 用户名和密码都是root


文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
地址(D) http:// gov.cn/phpMyAdmin/index.php?db=web_db&token=6b4ee30b87b8d1b81f1ce79b30092c69
转到 链接
phpMyAdmin
mysql (6)
test (0)
web
_db (53)
_dzyj (82)
请选择数据库
服务器: localhost
数据库 SQL 状态 变量 Engines 权限 进程 导出 Import
运行信息
刷新 Reset
此 MySQL 服务器已经运行了 0 天 9 小时，28 分 28 秒，启动时间为 2012 年 06 月 25 日 22:53。
SQL 查询 Handler Query cache Threads Temporary data Delayed inserts Key cache Joins Replication Sorting 个表
服务器流量：这些表显示了此 MySQL 服务器自启动以来的网络流量统计。
流量 ø 每小时 连接 ø 每小时 %
已收到 8,739 KB 922 KB max. concurrent connections 10 --- ---
送出 337 MB 36 MB 尝试失败 12 1.27 0.08%
统计 346 MB 37 MB 中止 0 0.00 0.00%
统计 14 k 1,519.77 100.00%
查询统计：自从启动后，服务器共收到了 142,097 次查询。
统计 ø 每小时 ø 每分钟 ø 每秒
142 k 15.00 k 249.97 4.17
查询方式 ø 每小时 % 查询方式 ø 每小时 %
admin commands 0 0.00 0.00% repair 0 0.00 0.00%
alter table 0 0.00 0.00% replace 0 0.00 0.00%
analyze 0 0.00 0.00% replace select 0 0.00 0.00%
backup table 0 0.00 0.00% reset 0 0.00 0.00%
begin 0 0.00 0.00% restore table 0 0.00 0.00%
change db 14 k 1,516.92 11.25% revoke 0 0.00 0.00%
change master 0 0.00 0.00% rollback 0 0.00 0.00%
check 0 0.00 0.00% savepoint 0 0.00 0.00%
commit 0 0.00 0.00% select 93 k 9,800.57 72.71%
create db 0 0.00 0.00% set option 0 0.00 0.00%
create function 0 0.00 0.00% show binlog events 0 0.00 0.00%
create index 0 0.00 0.00% show binlogs 18 1.90 0.01%
create table 0 0.00 0.00% show create 6 0.00 k 0.00%
delete 0 0.00 0.00% show databases 42 4.43 0.03%
delete multi 0 0.00 0.00% show fields 6 0.00 k 0.00%

查看用户名密码


eq.ah.gov.cn / localhost / web_db / web_user | phpMyAdmin 2.11.6 - Microsoft Internet Explorer
服务器: localhost ▸ 数据库: web_db ▸ 表 : web_user "后台用户"
浏览 结构 SQL 搜索 插入 导出 Import 操作 清空 删除
显示行 0 - 29 (57 总计, 查询花费 0.0006 秒)
SQL 查询:
SELECT *
FROM `web_user`
LIMIT 0 , 30
[编辑] [解释 SQL] [创建 PHP 代码] [刷新]
显示 : 30 行，开始行数: 30
以 水平 模式显示，并且在 100 个单元格后重复标题
主键排序: 无
Id Username Password Cname Sex Tel Email Info Branch Priv Uname Login
55 admin 4a4f495a562107070507 男 NULL NULL NULL 1 1 ahdzjguanli
7 bangongshi 17121b0b4e4e4f4d4c4f 男 1 6 admin
10 tuanwei 0b0a1e11081a16 男 NULL NULL NULL 53 8 admin
11 jiancechu 15161e111c1a1c170a 男 NULL NULL NULL 12 4 admin
12 yingjichu 0616111815161c170a 男 NULL NULL NULL 13 4 admin
13 renshichu 4a4a494d48464b 男 10 10 admin
14 jicaichu 15161c1e161c170a 男 NULL NULL NULL 11 10 admin
15 zhenfangchu 05171a11191e11181c170a 男 NULL NULL NULL 14 4 admin
16 shenjichu 0c171a1115161c170a 男 NULL NULL NULL 15 8 admin
17 dangban 1b1e11181d1e11 男 16 10 admin
18 laoganchu 494a4b4c4d4e 女 17 10 admin
19 yubaozhongxin 1e1a061d4e4f4f4f 女 18 4 admin
20 jiancezhongxin 1b05151c0507 女 19 4 admin
web_branch
web_coll
web_coll_guest
web_coll_ty
web_down
web_down_ty
web_govfile
web_govfile_proper
web_govfile_rhead
web_govfile_ty
web_hack
web_hack_ty
web_impart
web_infomation
web_infomation_ty
web_inter
web_inter_ty
web_lead
web_lead_info
web_lead_mail
web_lead_ty
web_link
web_link_ty
web_live
web_live_link
web_live_memoir
web_live_pic
web_log
web_menu
web_server
web_server_down
web_server_info
web_server_ty
web_source
web_test
web_topic
web_topic_info
web_topic_ty
web_user
web_user_priv
web_vod
web_vod_ty
web_vote
web_vote_item
web_vote_log
web_vote_txt
web_vote_ty

查看弱密码


web_infomation_ty
web_inter
web_inter_ty
web_lead
web_lead_info
web_lead_mail
web_lead_ty
web_link
web_link_ty
web_live
web_live_link
web_live_memoir
web_live_pic
web_log
web_menu
web_server
web_server_down
web_server_info
web_server_ty
web_source
web_test
28 huaibeiju 4e4d4c4b4a4948 男 27 4 admin
29 anqingju 1e110e161118150a 男 NULL 28 4 admin
30 tonglingju 4e4d4c 女 29 4 admin
31 chuzhouju 494a4b4c4e4d 女 30 4 admin
32 xuanchengju 070a1e111c171a1118150a 男 NULL 31 4 admin
33 chaohuju 1c171e10170a150a 男 32 4 admin

测试弱密码


http://eq. .gov.cn/admin/
MyWEB Login
VERSION 7.0
MyWEB 网站智能管理系统
用 户：
tonglingju
口 令：
验证码：
7611
登 录
© 版权所有 2001－2008 信息产业有限公司
100%

测试成功


网站智能管理平台
MyWEB V7.0 (政府版)
信息资讯
系统管理
用户:tonglingju 当前身份:信息报送员 所在部门:
网站首页 后台首页 注销
自定义快速操作
用户信息
欢迎您， 来自“ ”的 。
您总共登录 157 次此系统，最后一次登录时间是： 2012-11-05 11:05:55
您现在的身份是： 信息报送员 ！
协同工作
模糊查询:
搜索
100%

破译加解密算法

- 明文：123　　密文：4e4d4c
- 设明文是m，密文是c
  - m: 1 - 49　　2 - 50　　3 - 51
  - c : 4e - 78　　4d - 77　　4c - 76
- 猜测：ASCII码转换 + 线性算法
- 设解密算法是m = ac + b，代入值求解，计算出a = -1; b = 127，即解密算法：m = 127 – c

ASCII码对照表

下表列出了字符集中的 0 - 127。

代码	字符	代码	字符	代码	字符	代码	字符
0		32	[空格]	64	@	96	`
1		33	!	65	A	97	a
2		34	"	66	B	98	b
3		35	#	67	C	99	c
4		36	$	68	D	100	d
5		37	%	69	E	101	e
6		38	&	70	F	102	f
7		39	'	71	G	103	g
8	**	40	(	72	H	104	h
9	**	41	)	73	I	105	i
10	**	42	*	74	J	106	j
11		43	+	75	K	107	k
12		44	,	76	L	108	l
13	**	45	-	77	M	109	m
14		46	.	78	N	110	n
15		47	/	79	O	111	o
16		48	0	80	P	112	p
17		49	1	81	Q	113	q
18		50	2	82	R	114	r
19		51	3	83	S	115	s
20		52	4	84	T	116	t
21		53	5	85	U	117	u
22		54	6	86	V	118	v
23		55	7	87	W	119	w
24		56	8	88	X	120	x
25		57	9	89	Y	121	y
26		58	:	90	Z	122	z
27		59	;	91	[	123	{
28		60	<	92	\	124	|
29		61	=	93	]	125	}
30	-	62	>	94	^	126	~
31		63	?	95	_	127	

计算admin密码明文

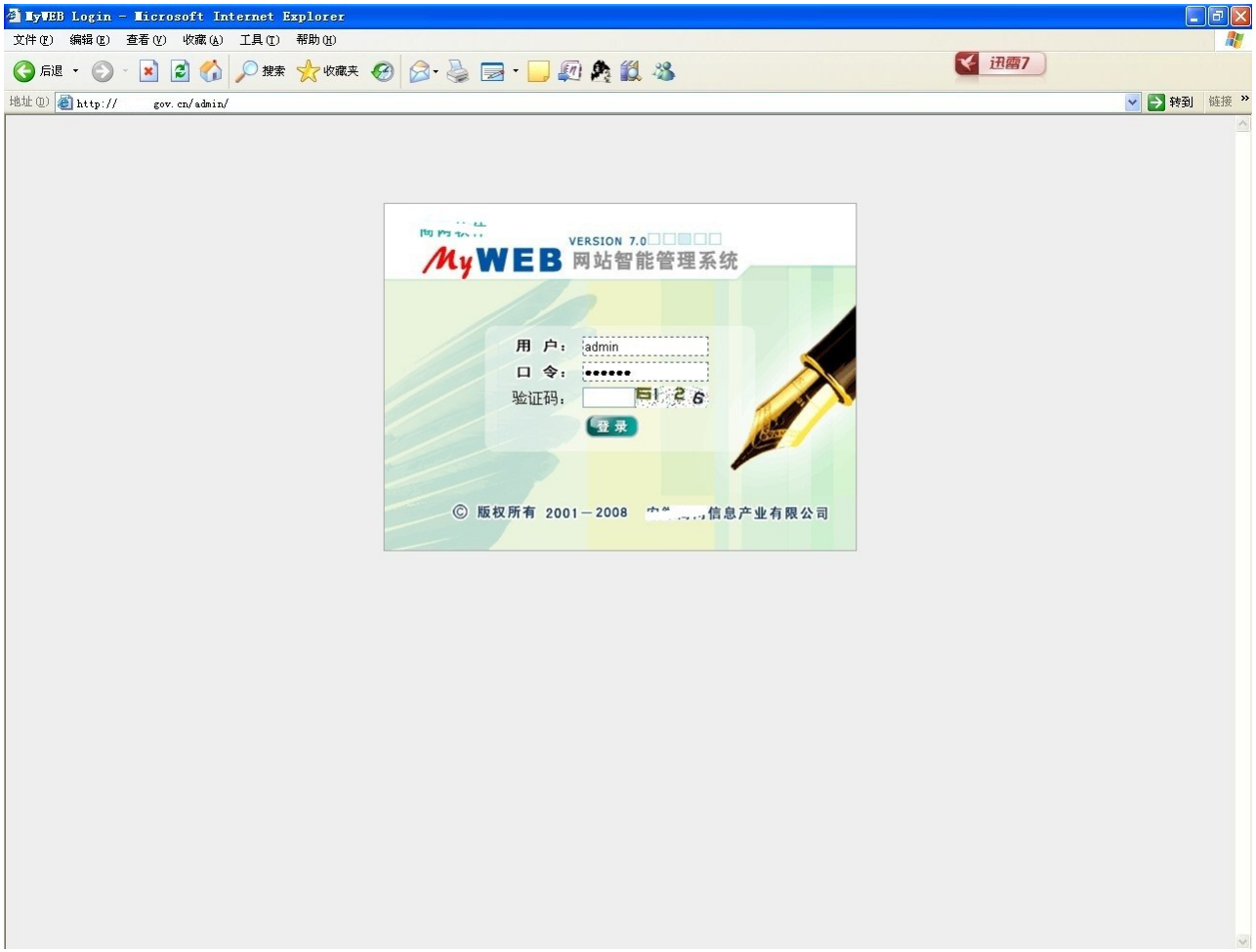
- 解密算法：m = 127 – c
- admin密码的密文：4a4f495a562107070507
- 依次进行解密
  - c: 4a - 74 4f - 79 49 - 73 5a - 90
  - m: 53 - 5 48 - 0 54 - 6 37 - %
- admin密码明文：506%)^xxzx

ASCII码对照表

下表列出了字符集中的 0 - 127。

代码	字符	代码	字符	代码	字符	代码	字符
0		32	[空格]	64	@	96	`
1		33	!	65	A	97	a
2		34	"	66	B	98	b
3		35	#	67	C	99	c
4		36	$	68	D	100	d
5		37	%	69	E	101	e
6		38	&	70	F	102	f
7		39	'	71	G	103	g
8	**	40	(	72	H	104	h
9	**	41	)	73	I	105	i
10	**	42	*	74	J	106	j
11		43	+	75	K	107	k
12		44	,	76	L	108	l
13	**	45	-	77	M	109	m
14		46	.	78	N	110	n
15		47	/	79	O	111	o
16		48	0	80	P	112	p
17		49	1	81	Q	113	q
18		50	2	82	R	114	r
19		51	3	83	S	115	s
20		52	4	84	T	116	t
21		53	5	85	U	117	u
22		54	6	86	V	118	v
23		55	7	87	W	119	w
24		56	8	88	X	120	x
25		57	9	89	Y	121	y
26		58	:	90	Z	122	z
27		59	;	91	[	123	{
28		60	<	92	\	124	|
29		61	=	93	]	125	}
30	-	62	>	94	^	126	~
31		63	?	95	_	127	

用系统管理员帐号登陆后台




网站智能管理平台 - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
后退 搜索 收藏夹
迅雷7
地址(D) http://. gov.cn/admin/myweb.php
转到 链接
MyWEB V7.0 (政府版)
信息资讯 互动管理 多媒体管理 地震目录 其他功能 系统管理
用户:admin 当前身份:系统管理员 所在部门:防震减灾信息网 | 网站首页 后台首页 注销
信息资讯
新闻管理
新闻添加
新闻浏览
新闻审核
分类管理
信息报送
专题报道
相关设置
新闻类型管理
增加栏目
排列顺序 栏目名称 添加人 操 作
100 主站栏目 （14 个子项目） 修改 | 清空 | 删除
10 灾害防御协会 （6 个子项目） 修改 | 清空 | 删除
10 地震学会 （4 个子项目） 修改 | 清空 | 删除
10 地震局团委 （8 个子项目） 修改 | 清空 | 删除
10 廉政之窗 （8 个子项目） 修改 | 清空 | 删除

网站入侵反思

- 网页设计和编码要考虑安全性
- 不需要暴露的页面坚决不暴露
- **坚决杜绝弱密码**！！！

最多使用的密码

rank	密码	次数	rank	密码	次数
1	123456	4,138,464	11	123321	183,741
2	123456789	1,070,028	12	666666	134,599
3	111111	1,033,040	13	1234567	127,268
4	123123	471,036	14	111222tianya	116,015
5	000000	428,307	15	7758521	115,560
6	12345678	409,722	16	1314520	115,227
7	wodima123	392,869	17	888888	110,647
8	5201314	298,458	18	a321654	106,441
9	a123456	195,049	19	654321	100,137
10	11111111	186,429	20	woaini	99,977

小结

- 掌握web服务器和浏览器的安全策略
- 掌握XSS和sql-inject的基础原理