甘肃政法学院

本科生实验报告

（五）

姓名:米小莉

学院:计算机科学学院

专业:计算机科学与技术

班级:09 计本班

实验课程名称:网络攻击与防御技术

实验日期:2012 年 6 月 14 日

指导教师及职称:武光利

实验成绩:

开课时间：2011-2012 学年 第二 学期

甘肃政法学院实验管理中心印制

实验题目	Snort系统的安装与配置			小组合作	否
姓名	米小莉	班级	09 计本班	学　　号	200981010123

一、实验目的

熟悉入侵检测工具 snort在 Windows 操作系统中的安装和配置方法

二．实验环境

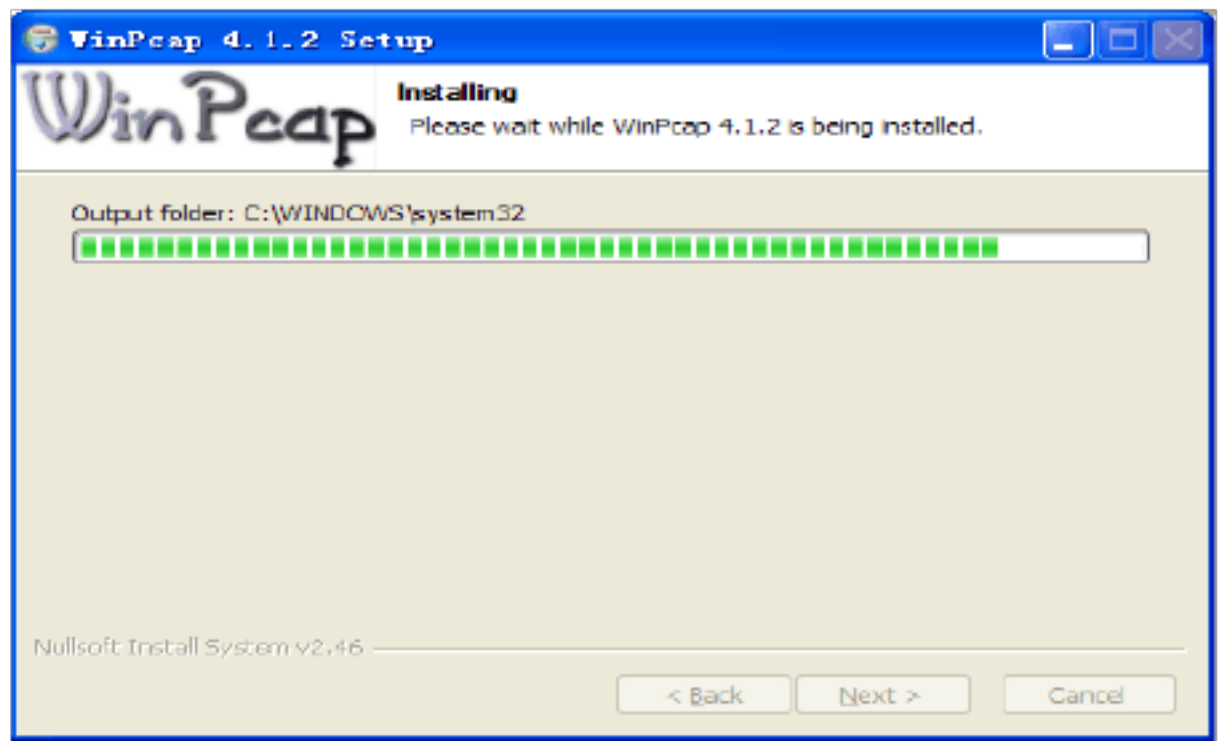
操作系统：windows xp

软件：winpcap$_{AppServ}$

三、实验内容与步骤

Windows 环境下安装和配置 snort

（1)、安装 Snort和 Wincap 包



2.AppServ

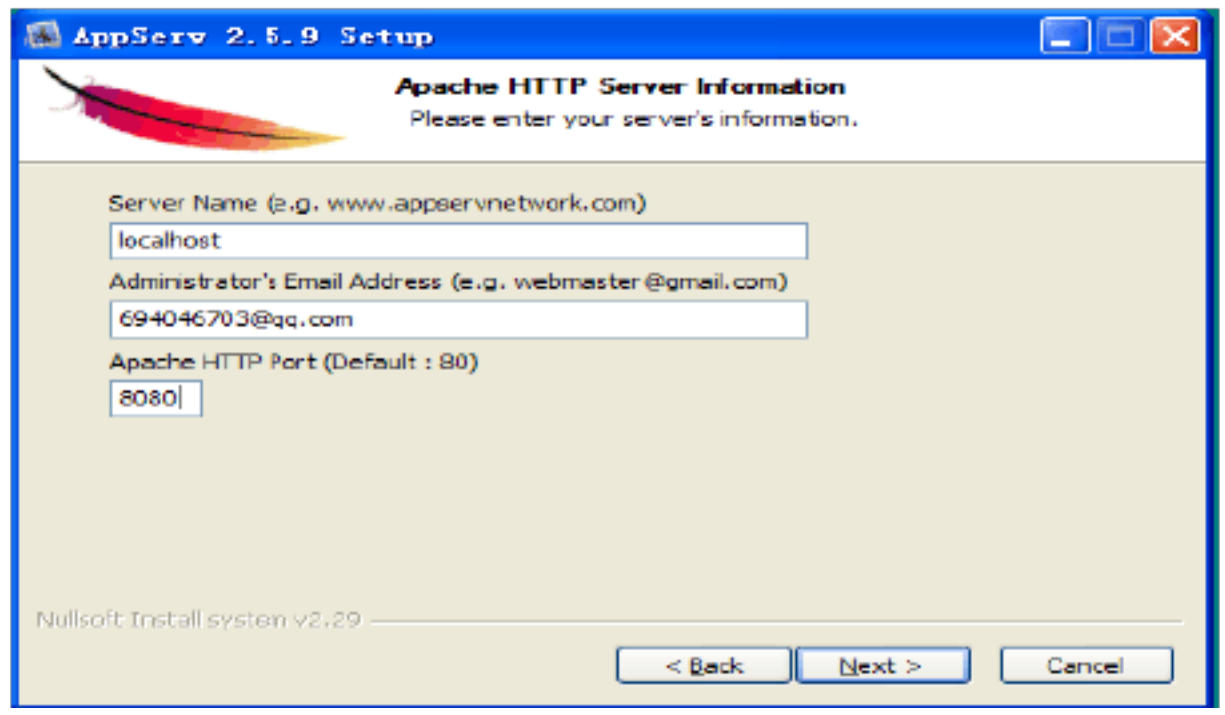
（1）安装 AppServ

启动 AppServ 安装文件后，出现如图所示的设置服务器信息界面：

在 Server Name中输入域名 localhost

Administrator’sEmail Address中输入邮箱地址：694046703@qq.com

监听端口设为 8080

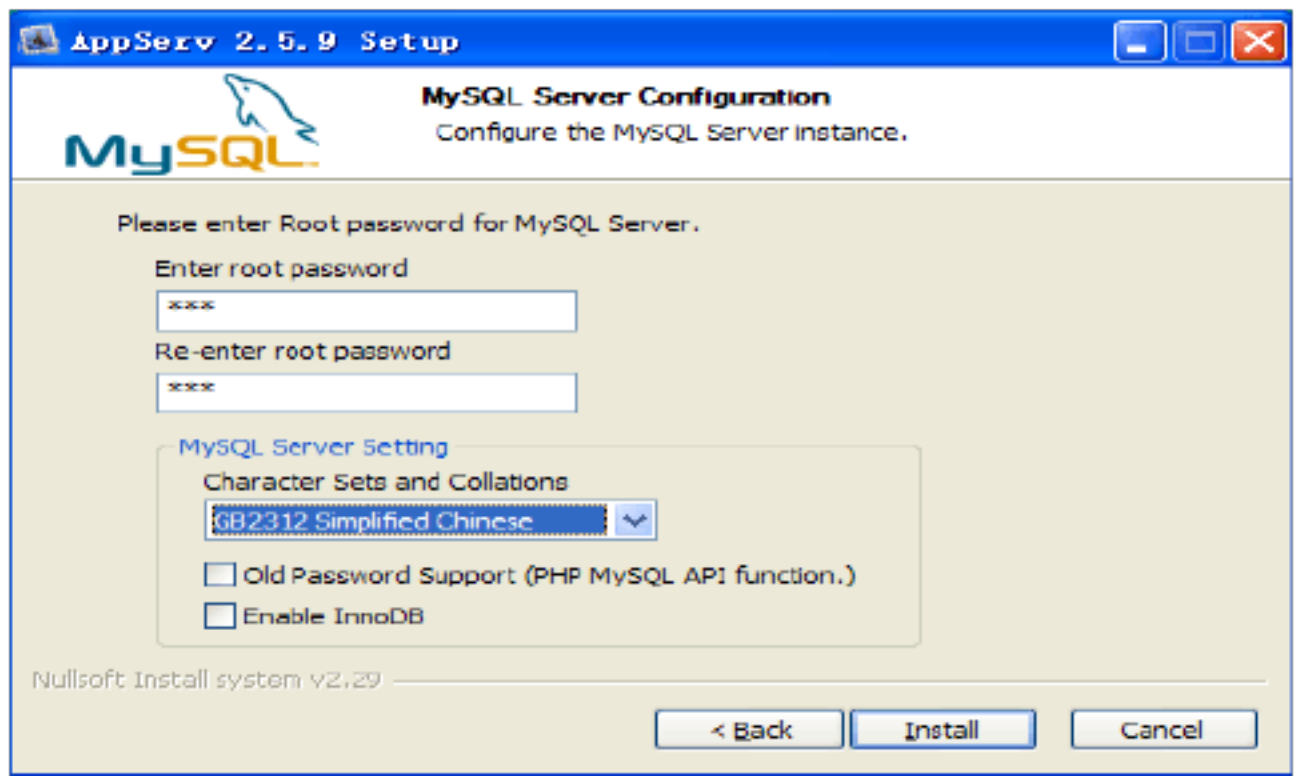


点击 next，进入下一界面：

在出现的界面中输入密码（123）：

"Character Sets and Collations"选择"GB 2312Simplified Chinese"，

下图所示：



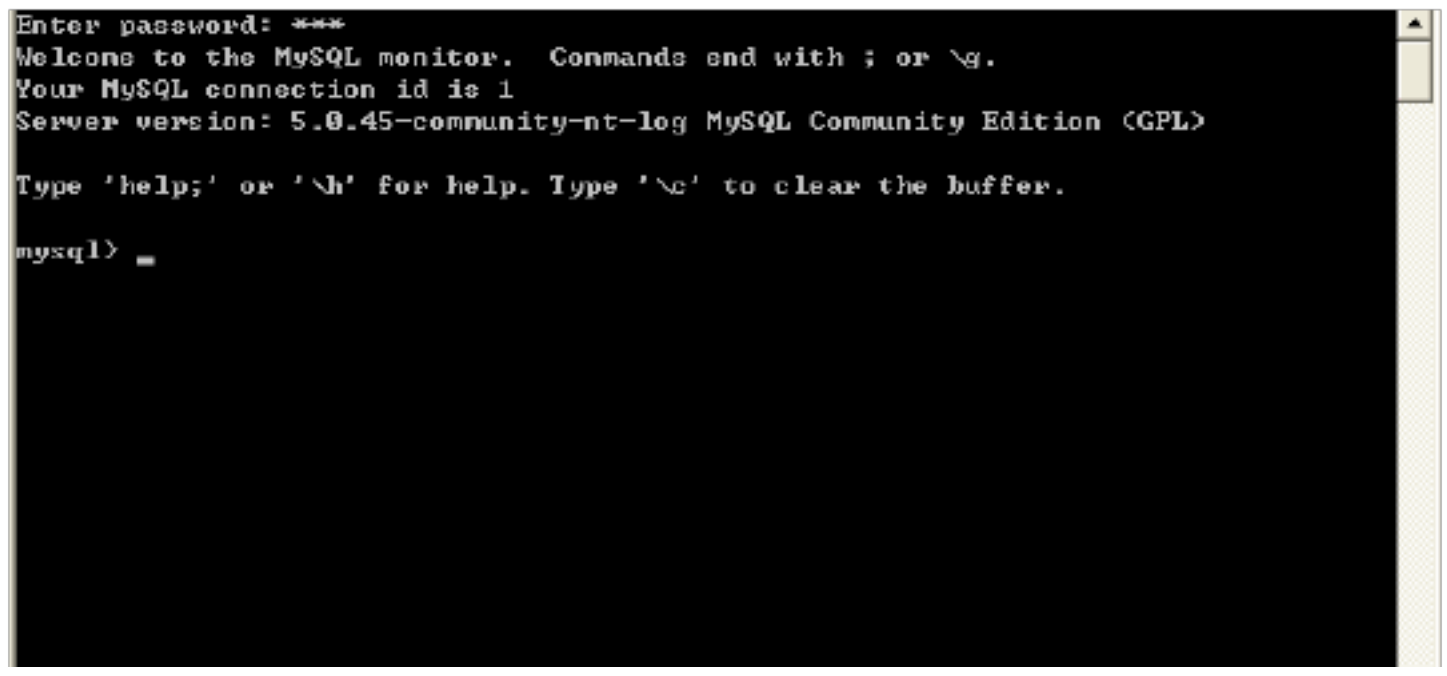
然后单击"Instal进入安装过程，出现下图：

安装完成后将 C:\Appserv\php5目录下的 php.ini-dist文件改名为 php.Ini 并启动 Apache 和

MySql 。

（控制面板—管理—服务　确保 Apache 和 MySql 已启动）

安装完成后可以查看（MySQL　启动如下图）

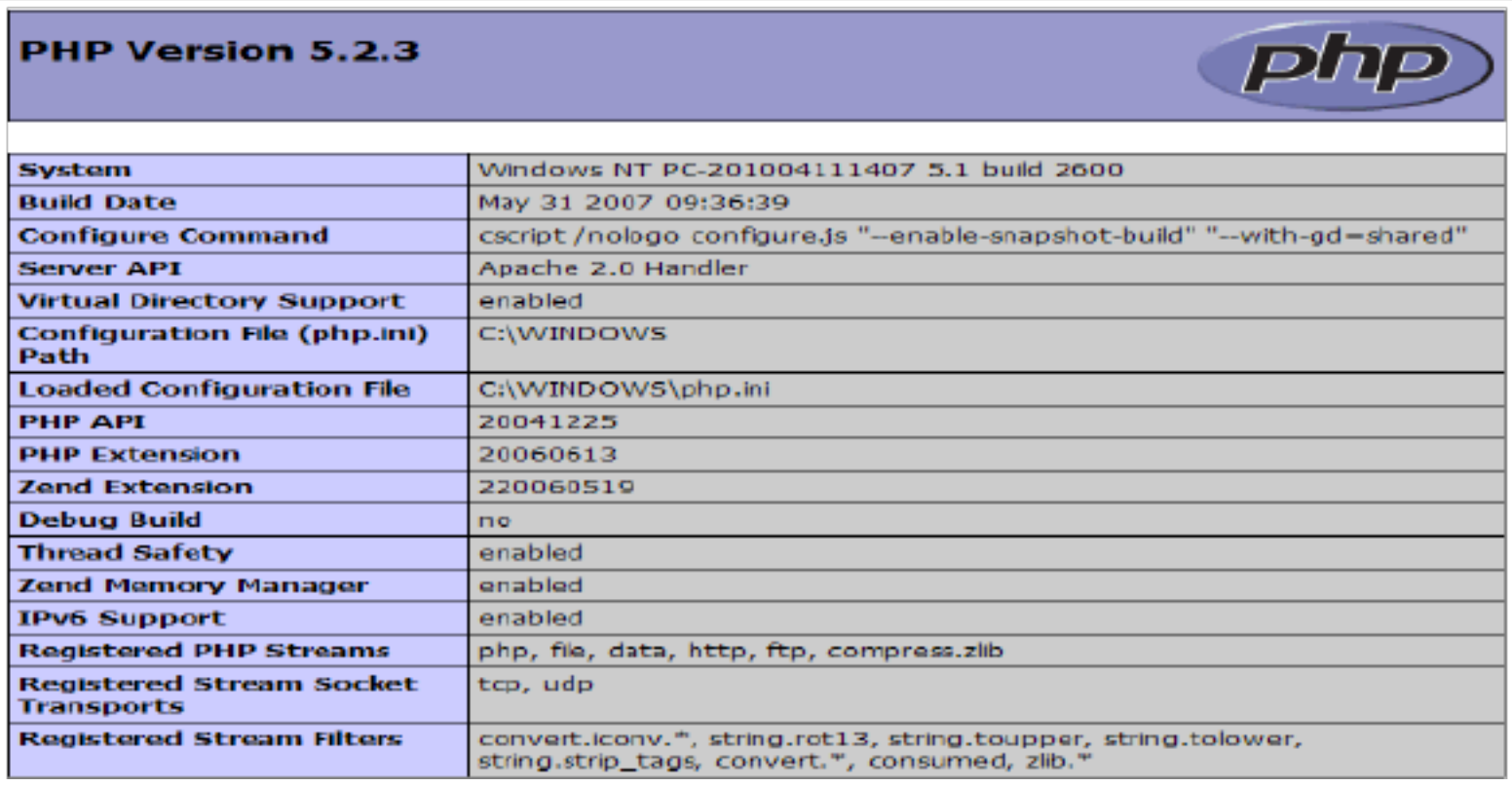


在浏览器中输入　:8080　　出现：

表示安装成功！

（2）测试 AppServ

首先查看"控制面板"/"管理"/"服务",确保 Apache 和 MySQL　已经启动，然后，在浏览器中输入　:8080/phpinfo.php,　　（下图）



PHP Version 5.2.3

System	Windows NT PC-201004111407 5.1 build 2600
Build Date	May 31 2007 09:36:39
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\WINDOWS\php.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*

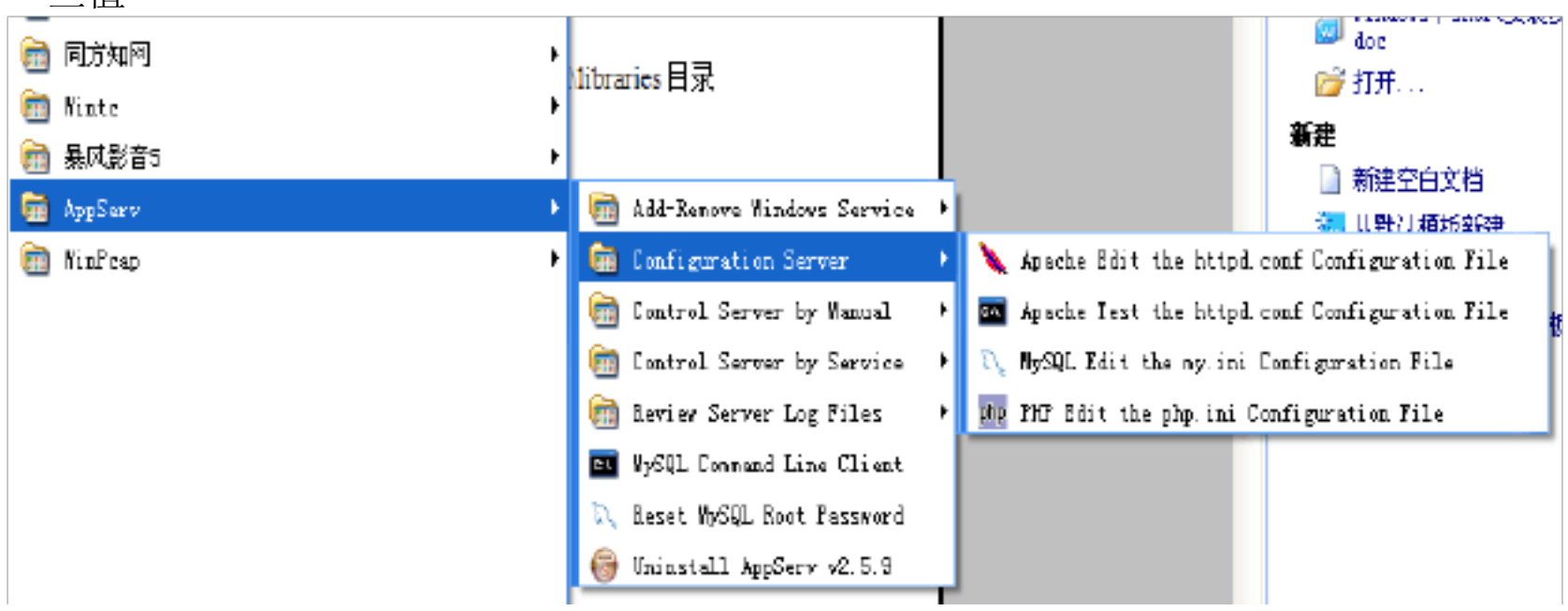
可以了解 php 的一些信息。

最后打开浏览器，输入 :8080/phpMyAdmin/index.php,

下图）输入用户名 root和密码，可以浏览数据库内容

（3）配置 AppServ

第一步，编辑 Apache 服务器配置文件。打开 Apache2.2\con文件中的 httpd.conf检查相应的一些值



进入 Apache 服务器配置文件

需要检查一下一些值：

```
LoadModule php5_module C:/AppServ\php5\php5apache2_2.dll
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
# If your host doesn't have a registered DNS name, enter its IP address here.
ServerName localhost:8080
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
DocumentRoot "C:/AppServ/
```

第二步，编辑 phpMyAdmin 中的关键文件。打开 C:\AppServ\ 目录下的 config.default.php 文件

设置 phpMyadmin 的 URL ，$cfg['PmaAbsoluteUri'] = '

```
 */
$cfg['PmaAbsoluteUri'] = 'http://localhost:8080/phpmyadmin/';

/**
```

$cfg['blowfish_secret'] = '123'

```
 */
$cfg['blowfish_secret'] = '123';

/**
```

$cfg['DefaultLang'] = 'zh-gb2312'

```
// Default language to use, if not browser-defined or user-defined
$cfg['DefaultLang'] = 'zh-gb2312';

// Default connection collation (used for MySQL >= 4.1)
```

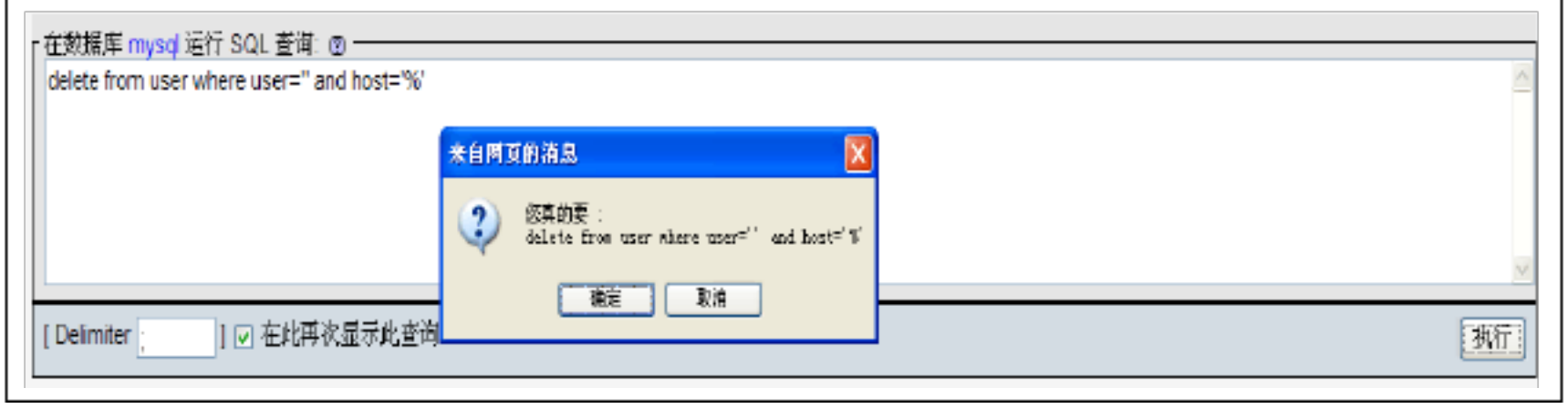
$cfg['DefaultCharset'] = 'gb2312'

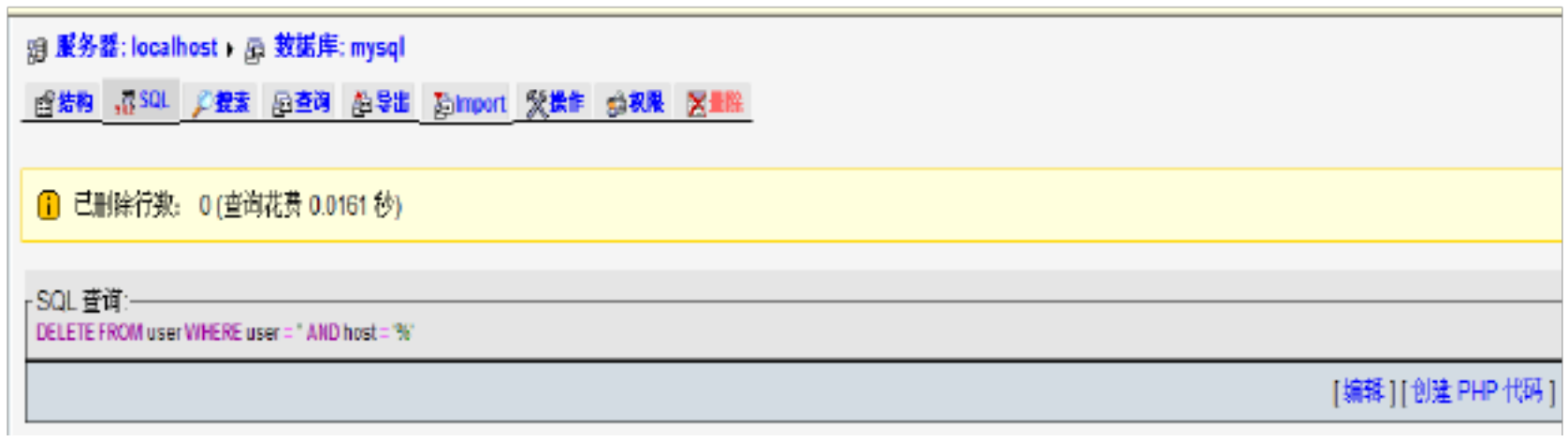
```
// (see $cfg['AvailableCharsets'] to possible choices, you can add your own)
$cfg['DefaultCharset'] = 'gb2312';

// Allow charset recoding of MySQL queries, must be also enabled in language
```

$cfg['Servers'][$i]['auth_type'] cookie'

```
                                    // features (pmadb)
$cfg['Servers'][$i]['auth_type']    = 'cookie'; // Authentication method (valid choices: config, http, HTTP, signon or cookie)
$cfg['Servers'][$i]['user']         = 'root';   // MySQL user
$cfg['Servers'][$i]['password']     = '';       // MySQL password (only needed
                                    // with 'config' auth type)
```

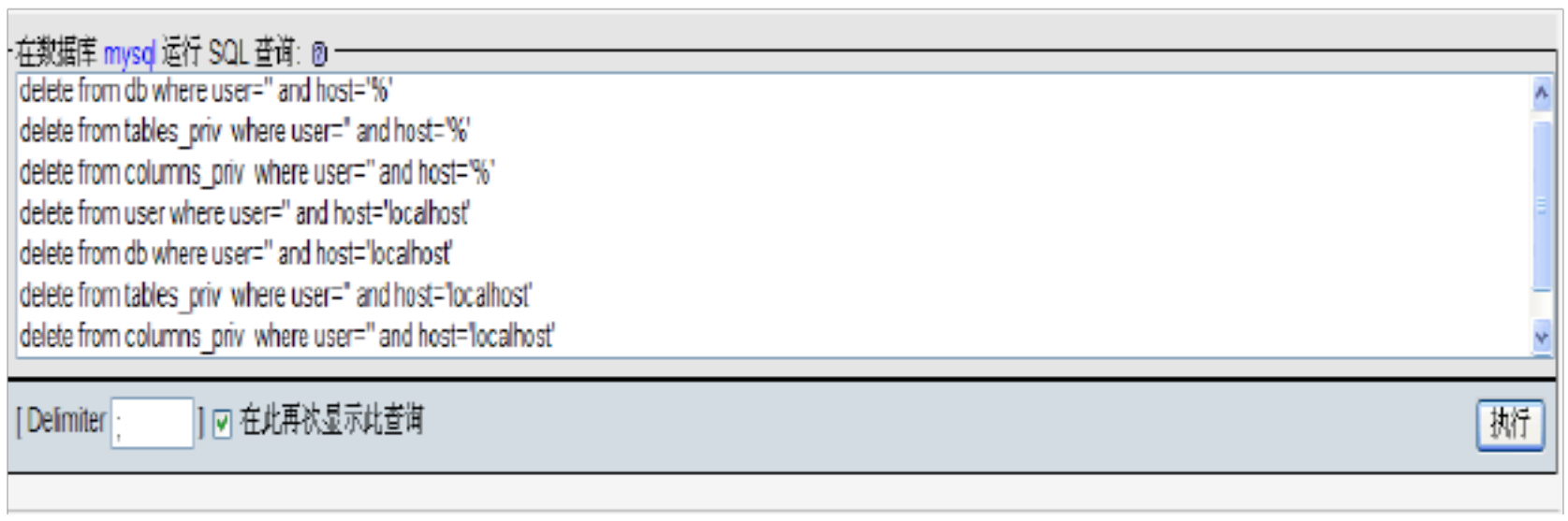
第三步，为安全起见，还必须删除 Mysql 安装后默认的 any@% 、any@localhos和 root@% 帐号。






```
delete from db where user='' and host='%'
delete from tables_priv where user='' and host='%'
delete from columns_priv where user='' and host='%'
delete from user where user='' and host='localhost'
delete from db where user='' and host='localhost'
delete from tables_priv where user='' and host='localhost'
delete from columns_priv where user='' and host='localhost'
delete from user where user='root' and host='%'
delete from db where user='root' and 'host'='%'
delete from tables_priv where user='root' and host='%'
delete from columns_priv where user='root' and 'host'='%'
```

注意，上面的'是两个单引号而不是一个双引号。这样只允许 root从 localhost连接。



第四步，配置 php.ini 打开 C:\WINDOWS|php.ini 文件。修改后的值如下图：

第五步，对 Mysql 进行修改。首先需要建立 Snort运行必需的 Snort 库和 Snort_archiv库：

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> create database snort;
Query OK, 1 row affected (0.73 sec)

mysql> create database snort_archive;
Query OK, 1 row affected (0.34 sec)

mysql>
```


```
CREATE TABLE signature ( sig_id      INT      UNSIGNED NOT NULL AUTO_INCREMENT,
                         sig_name    VARCHAR(255) NOT NULL,
                         sig_class_id INT     UNSIGNED NOT NULL,
                         sig_priority INT     UNSIGNED,
                         sig_rev     INT      UNSIGNED,
                         sig_sid     INT      UNSIGNED,
                         sig_gid     INT      UNSIGNED,
                         PRIMARY KEY (sig_id),
                         INDEX       sign_idx (sig_name(20)),
                         INDEX       sig_class_id_idx (sig_class_id));
```

修改前

```
CREATE TABLE signature ( sig_id      INT      UNSIGNED NOT NULL AUTO_INCREMENT,
                         sig_name    VARCHAR(255) NOT NULL,
                         sig_class_id INT     UNSIGNED NOT NULL,
                         sig_priority INT     UNSIGNED,
                         sig_rev     INT      UNSIGNED,
                         sig_sid     INT      UNSIGNED,
                         sig_gid     INT      UNSIGNED,
                         PRIMARY KEY (sig_id),
                         INDEX       sign_idx (sig_name(20)),
                         #，INDEX     sig_class_id_idx (sig_class_id)
                         );
```

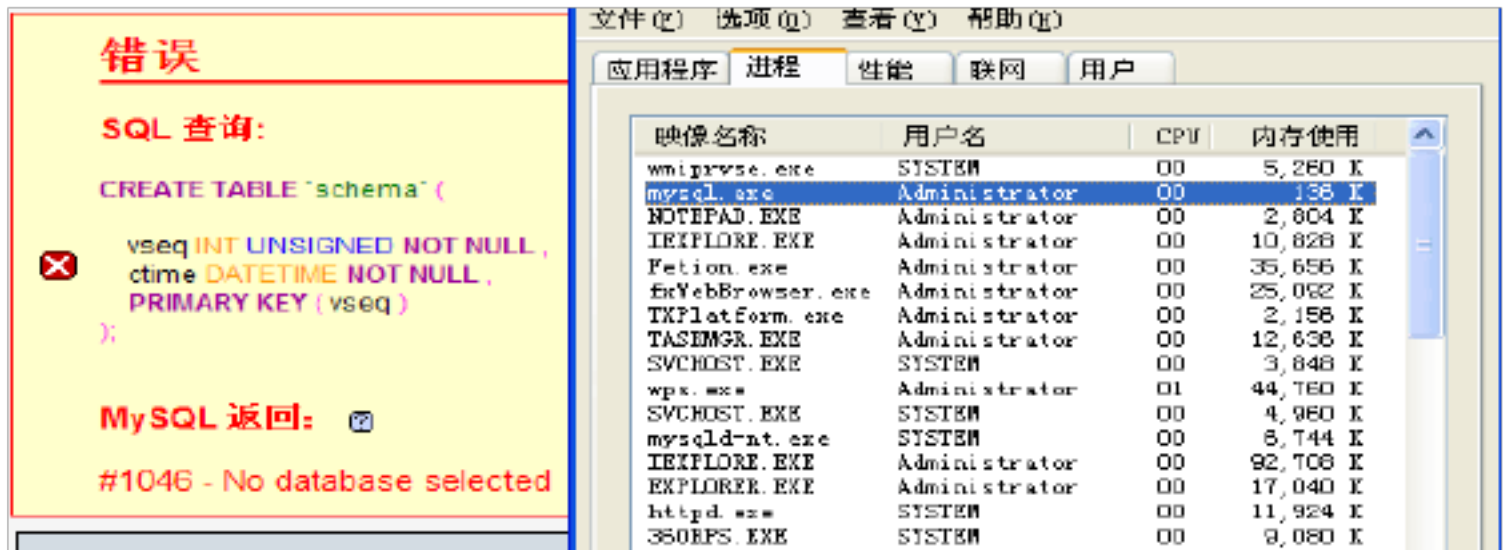
修改后

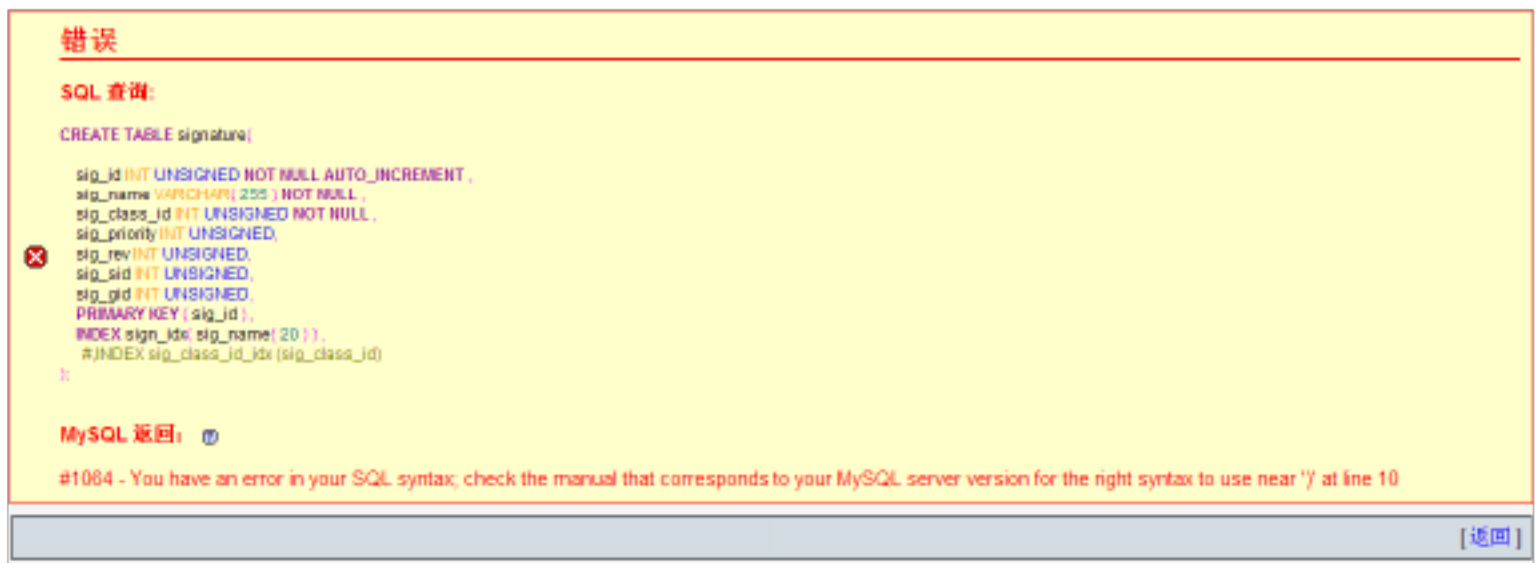
Run SQL query\queries on server localhost:

```
CREATE TABLE `schema` ( vseq      INT     UNSIGNED NOT NULL,
                        ctime     DATETIME NOT NULL,
                        PRIMARY KEY (vseq));
INSERT INTO `schema` (vseq, ctime) VALUES ('107', now());

CREATE TABLE event ( sid   INT       UNSIGNED NOT NULL,
                     cid   INT       UNSIGNED NOT NULL,
```

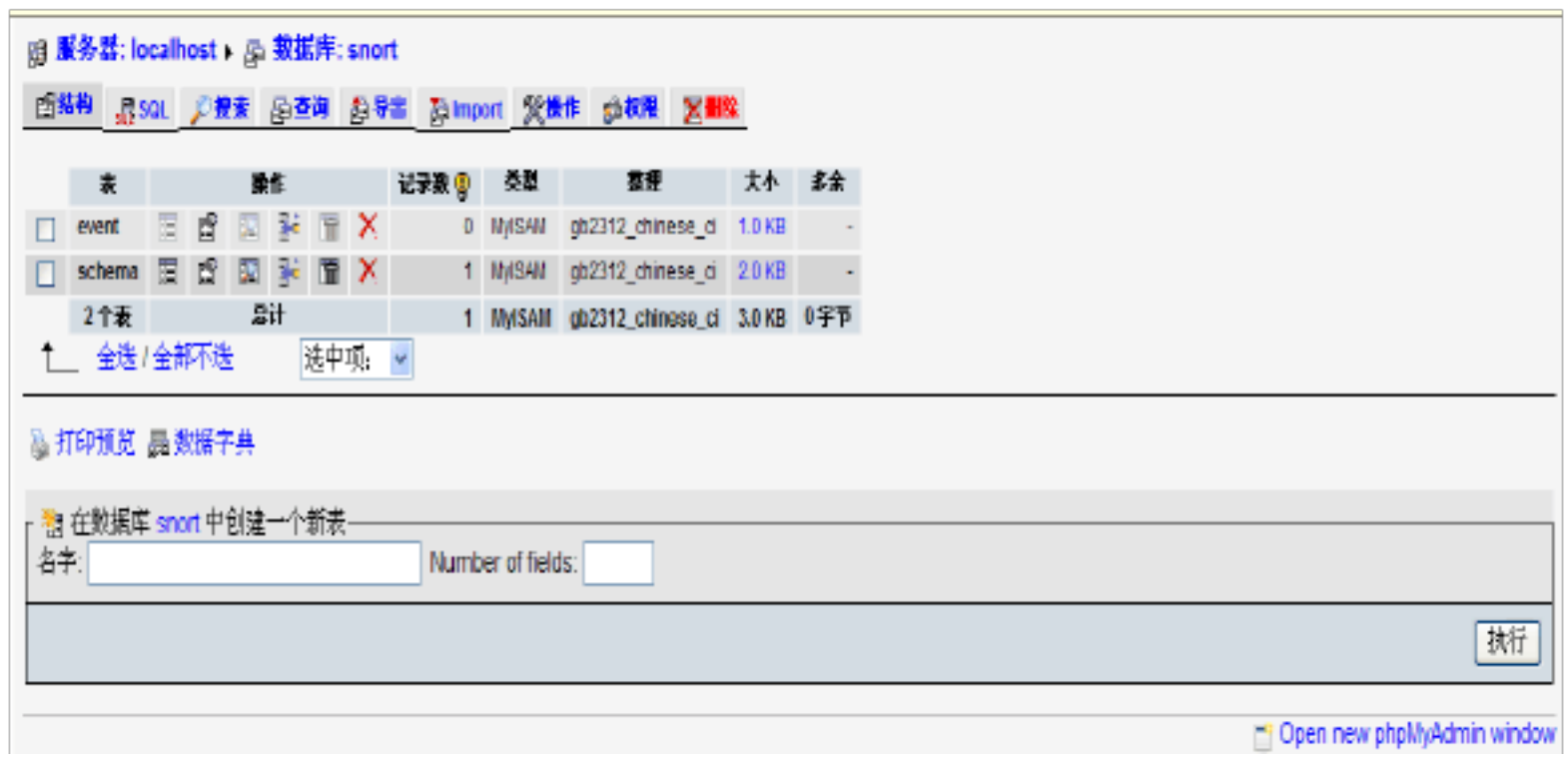
[Delimiter ;] 在此再次显示此查询 执行

错误是因为没有启动 mysql,第二次是因为)；被#，屏蔽了，修改后如下图：



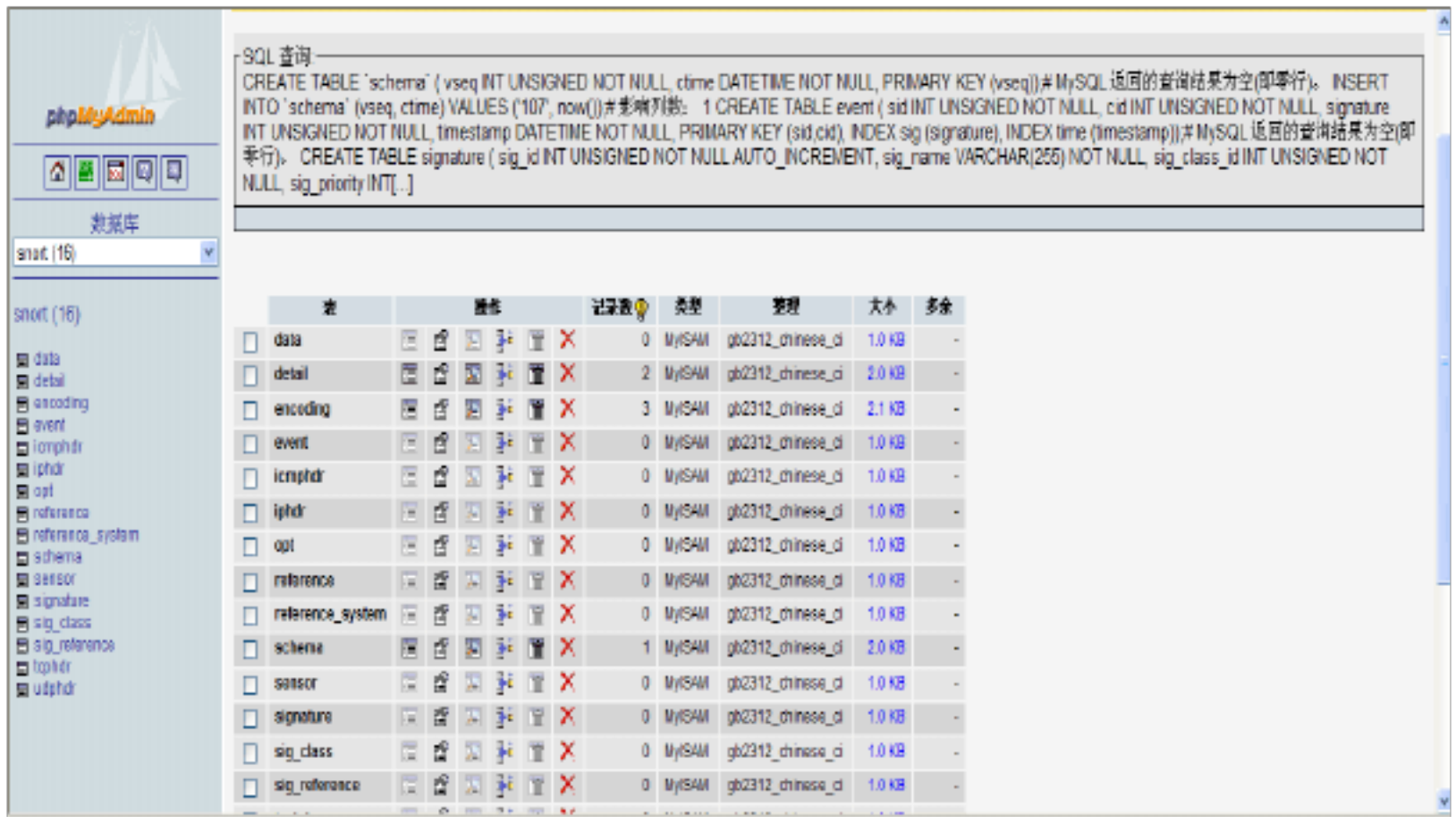


程序第一次运行就生成了 event表和 schema 表，需要删除错误的表后才能重新创建表。



```
CREATE TABLE signature ( sig_id          INT             UNSIGNED NOT NULL
AUTO_INCREMENT,
                        sig_name        VARCHAR(255) NOT NULL,
                        sig_class_id INT            UNSIGNED NOT NULL,
                        sig_priority INT            UNSIGNED,
                        sig_rev         INT             UNSIGNED,
                        sig_sid         INT             UNSIGNED,
                        sig_gid         INT             UNSIGNED,
                        PRIMARY KEY (sig_id),
                        INDEX     sign_idx (sig_name(20)));
                        #,INDEX     sig_class_id_idx (sig_class_id)
```

经过多次排错，终于运行成功：



第六步，使用 C:\Snort\schemas目录下的 create_MySQL 脚本建立 Snort运行必需的数据表。在此，可以通过 MySQL 提示符下运行 SQL 语句 show tables来检验配置的正确性

其中 c:\Snor为 Snort的安装目录，打开命令提示符，运行以下命令：

```
mysql -D Snort -u root -p < c:\Snort\schemas\create_mysql
mysql -D Snort_archive -u root -p < c:\Snort\schemas\create_Mysql
```

每次提示输入 root的密码，输入密码即可建立所需要的表。