# 十大措施保证系统安全

## 一、 MD5 加密用户密码

本系统用户密码采用 MD5 加密，这是一种安全性非常高的加密算法，是普遍使用广泛应用于文件验证，银行密码加密等领域，由于这种加密的不可逆性，在使用 10 位以上字母加数字组成的随机密码时，几乎没有破解的可能性。

## 二、 COOKIES 加密

本系统保存 COOKIES 时，对保存于 COOKIES 中的数据采用了以 MD5 加密为基础，加入随机加密因子的改进型专用加密算法。由于使用的不是标准 MD5 加密，因此本系统 COOKIES 中保存的数据不可能被解密。因此，黑客试图用伪造 COOKIES 攻击系统变得完全不可能，系统用户资料变得非常安全。

## 三、 SQL 注入防护

系统在防 SQL 注入方面，设置了四道安全防护：

第一、系统级 SQL 防注入检测，系统会遍历检测所有用 GET、POST、COOKIES 提交到服务器上的数据，如发现有可能用于构造可注入 SQL 的异常 代码，系统将终止程序运行，并记录日志。这一道安全防护加在连接数据库之前，能在连接数据库前挡处几乎所有的 SQL 注入和危害网站安全的数据提交。

第二、 程序级安全仿 SQL 注入系统，在应用程序中，在构建 SQL 查询语句前，系统将对由外部获取数据，并带入组装为 SQL 的变量进行安全性合法性验证，过滤可能构成注入的字符。

第三、 禁止外部提交表单，系统禁止从本域名之外的其它域名提交表单，防止从外部跳转传输攻击性代码。

第四、数据库操作使用存储过程 系统所有的重要数据操作，均使用存储过程作参数查询，避免组装 SQL 字符串，令即使通过了层层 SQL 注入过滤的攻击性字符仍然无法发挥作用。

## 四、 木马和病毒防护

针对可能的木马和病毒问题，系统认为，在服务器设置安全的情况下，外部带来的安全问题，主要是用户可能上传病毒和木马，本系统作了如下四层的防护

第一、 客户端文件检测，在上传之前，对准备上传的文件进行检测，如果发现不是服务器设置的允许上传的文件类型，系统拒绝进行上传。如果客户端屏蔽了检测语句，则上传程序同时被屏蔽，系统无法上传任何文件。

第二、 服务器端文件安全性检测，对上传到服务器的文件，程序在将文件写入磁盘前，检测文件的类型，如发现是可能构成服务器安全问题的文件类型，即所有可以在服务器上执行的程序，系统都拒绝写入磁盘。以此保证不被上传可能在服务器上传播的病毒和木马程序。

第三、对有权限的服务器，系统采用即上传即压缩策略，所有上传的除图片文件、视频文件外，其它各种类型的文件一但上传，立即压缩为 RAR，因此，即使包含木马也无法运行。不能对网站安全带来威胁。

第四、底层的文件类型检测 系统对文件类型作了底层级检测，由于不仅检测扩展名，而是对文件的实际类型进行检测，所以无法通过改扩展名方式逃过安全性验证。

## 五、 权限控制系统

系统设置了严格有效的权限控制系统，何人可以发信息，何人能删除信息等权限设置系统一共有数十项详细设置，并且网站不同栏目可以设置完全不同的权

限，所有权限均在多个层次上严格控制权限。

## 六、IP 记录

IP 地址库 除记录所有重要操作的 IP 外，还记录了 IP 所在地区，系统中内置约了 17 万条 IP 特征记录。

详细的 IP 记录 所有的创建记录、编辑记录行为（如发文章，发评论，发站内信等），均记录此操作发生的 IP，IP 所在地区，操作时间，以便日后备查。在发现安全问题时，这些数据会非常关键和必要。

## 七、隐藏的程序入口

本系统具有全站生成静态页 系统可以全站生成 HTML 静态文件，使网站的执行程序不暴露在 WEB 服务中，HTML 页不和服务器端程序交互，黑客很难对 HTML 页进行攻击，很难找到攻击目标。

## 八、有限的写文件

系统所有的写文件操作只发生于一个 UPFILE 目录，而此目录下的文件均为只需读写即可，可通过 WINDOWS 安全性设置， 设置此目录下的文件只读写，不执行，而程序所在的其它文件夹只要执行和读权限，从而使破坏性文件无法破坏所有程序执行文件，保证这些文件不被修改。

## 九、作了 MD5 校验的订单数据

在商城订单处理中，对提交的订单信息作了 MD5 校验，从而保证数据不被非法修改。

## 十、编译执行的代码

由于基于.net 开发， 代码编译执行，不但更快，也更安全