## 项目安全性怎么解决？

是指攻击安全还是访问量过大安全还是数据安全？

如果是攻击性的话，input框都采用了js验证，用java代替重复效验，避免输入不必要的空格或者sql注入。

如果是访问的安全的话，页面做了大量的页面静态化，缓存，通常访问量不会增加服务器造成负担。

如果是数据安全这一块的话，系统用的是linux，数据库的账号密码都做了加密处理。

如果是数据遗失或是自然灾害，数据库做了读写分离，而且一个主库，两个从库，其中一个从库做了备份，而且是定时备份。

在登录过程中，为了防止程序直接登录，也做了一些验证码，包括支付的资金账户安全，我们的系统没有钱，主要是通过超链接将钱存储到网络支付宝qq账号，最主要还是支付宝的安全和网民的安全,而且这个账号只能出不能进。

## 防sql注入

针对防sql注入，我们通常是这样做的：

首先在前台页面对用户输入信息进行js验证，对一些特殊字符进行屏蔽， 比如：or ,单引号，--，= ，还有就是限制用户名输入的长度，我们一般将其限制在6---13位。另外，对于用户的敏感信息我们进行Md5加密，还有，为了增加用户体验度和用户友好度，为了不使用户看到一些详细的异常信息我们会进行错误信息页面的定制，像404,500错误。另一个我层面讲，这样做也是为了保护我们的一些重要信息。此外，我们会给特定的人分配定定的权限，而不是给其分配管理员权限！