我又来水一帖的，关于服务端验权的问题

作者：cykcyk123
原文链接：https://ld246.com/article/1484660634386
来源网站：链滴

2016年下半年我们公司开启了一个商城的项目。

其实我们每个人都想把整个项目做到最精细，但是我们公司的理念是现有房子，大小是另外一回事。

我们公司的项目是JAVA 框架是SSH，重点使用struts2。

我是前端出身的，自然负责前端页面和与后端的对接。

一开始时间充裕，所以登录页面我画了1天时间，包括对帐号密码输入的验证和扫码登录的接口。

虽然时间长，但是基本完美。

但是随着项目的推进，我发现越来越不对劲，负责后端的同事每逢提交表单的时候都需要我对表单项行验证。

在我真正感觉到蹊跷，是又一次我需要知道表单对应的name的时候，我打开了对应action的代码，果发现。这个接口仅仅是一个存入的数据库的接口，而没有进行登录验证和对应的权限验证。

于是我有很调皮的点开了其他包括接口，发现果真如此。

也就是说，在我没有登录或者当前登录账户没有修改权限的情况下是可以使用相应的接口进行修改插甚至删除的操作的。

难道仅仅需要前端验权而后端不需要么。

另外，我们的接口无论网页或者app都采用如同https://hacpai.com/post?type=0 这样的接口进行单提交，网页的表单提交没有做表单令牌，而在app上甚至参数是最简单的明文的userid作为参数提。总感觉会出问题

虽然我是一个前端，在php上虽然不算过多精通，但是在我写过的wechat对接的项目中使用到了表单牌，在我目前的项目中，与webapp对接都是用的是自己编写的加密token，app需要保存并使用toke才可以换取所需要的数据甚至添加好友聊天等功能。这些都是我自己做的项目。

就像我回复的一篇帖子一样，在创业性公司，永远缺少大牛，大家也是身位平等，毕竟我是前端，我可能也不必要甚至不方便跟后端商量或提出这样的事情。而且人家是我的主管，而我仅仅是一个没有何实权的副经理。

写在接口的时候偶然想起这么糟心的一件事情，就来吐槽一下。

各位对前端与后端对接所发送的数据接口有什么建议，如何安全的提交表单，如何更加方便的验权，时的经验，如果方便，麻烦教导下。

一个迷茫的前端