页面添加/删除等功能的js，在页面功能性隐藏按钮后(有些状态需要，有些不需要，所以js是据需要显示/隐藏)，

通过浏览器可以执行，

使得用户超出了网站的意图进行操作；

解决：

后台增删改查等操作时，也必须加上需要的条件判断；

·针对于不同状态的不同操作；使代码不能绕过状态；

·登录判断，只能操作本人的记录；

进一步：

页面的所有js功能，必须进行分析，需要的都在后台进行防范处理；

////////////////////////////////////////////////////////////////

通过js中的删除代码，进行超出操作：

示例，页面中有如下js

function toRemoveBankCard(id) {

layer.confirm("确定删除？", function() {

$.ajax({

url : "${path}/bankinfo/removeBankCard.do",

data : {'id' : id},

Path/bankinfo/removeBankCard.do?id=14279 ---可以实现删除；

如此，恶意用户，可以删除掉网站所有的银行卡，挂了就；

解决：

1，网站前台用户操作中，不能有删除银行卡的功能；

删除银行卡功能必须是后台特定用户拥有，并进行用户、角色等验证；

2，简单的，必须有的类似删除功能的，

删除时，判断登录，用户，只能删除本用户的；