#  Js跟踪之未授权访问

本漏洞来自（安全研究-小秘圈），作者：winway，请勿泄漏圈内任何文件

一个正常登陆框，然后啥都没了，正常的可能会有个人的攻击思路，这个是自己一个项目的招生系统，其实这个漏洞挺有意思的，通过js找到一处登陆接口，其中带了主要的逻辑其实逻辑漏洞这个玩意真的只有思想不到位，按照个人的思维来攻击脑洞真的需要很大，如果大家有什么奇葩的逻辑漏洞可以分享出来一起学习成长。



在js中跟踪到一块登陆到js，看看具体到内容情况，在继续跟踪



跟踪到js



post(baseUrl\_+"/framework/login\_login.do",{loginId:a,password:b,verifycode:c,abc:Math.random()},

function(a){"true"==a?window.location=baseUrl\_+"/framework/login\_toManage.do":" code Faild" ==a?

出问题的可能是这几条，其次出现的是逻辑问题可能从js中不好判断，但是跟踪到这个位置确实访问了其中几处url，第一处是一个登陆效验，第二处是直接访问到一个空白到后台页面，这里就有问题了



为何能访问到该后台框架，肯定存在问题，我到理解可能有误但是其中js有三处主要登陆参数处，1，userid=a，password=b，code=c 那么很正常但是他仿佛只效验了userid



其实其中根据js来判断可能会出错毕竟得不到一个真正到白盒测试，但是js中确实只对a进行判断然后直接得到后台url那么我在对根据跟踪拿到对信息进行一个测试



用户名正确，密码错误会直接显示密码错误，如果用户名错误直接显示用户错误，但是在输入正确的用户名，也就是刚刚说到的a，再去手工访问刚刚的空白后台地址时它是直接得到了admin这个用户的所有权限说明了它确实只效验了参数a

