#### 第四更:

Ps:此次是对一个系统的具体挖掘方法，在我们挖掘漏洞的时候，遇见困难的，在自己技术和知识积累的情况达不够的时候，就可以放弃换简单的系统挖掘，一般脆弱系统为弱口令能进去的系统，之后在对后台挖掘，edusrc平台的某位核心白帽子都是靠弱口令上去的！！！

###  对Js接口的继续探讨

目标站点：[http://202.197.xx.xxx/（学校常用的视频点播平台）](http://202.197.xx.xxx/%EF%BC%88%E5%9B%A0%E4%B8%BA%E4%B8%8A%E6%AC%A1%E7%9A%84%E5%8E%9F%E5%9B%A0%EF%BC%8C%E6%89%80%E4%BB%A5%E4%BB%A5%E5%90%8E%E7%9A%84%E6%96%87%E7%AB%A0%E9%83%BD%E7%9A%84%E6%89%93%E7%A0%81%E4%BA%86%EF%BC%89)



开局也是这样的一个登录框，当然首先测试就是弱口令admin/admin (admin/123456) 等常规的密码， （可以进行小量字典爆破一下），但是都没有办法进入，于是尝试寻找操作手册或者初始密码看是否能进入后台。

谷歌寻找操作手册：



操作手册能寻找到很多,但是点进去观看一看翻后，只提示了管理员账号为admin/初始密码需要自己设置，这种情况下，我们就不要继续在死磕查找弱口令，因为管理员一般在这种情况下是不可能继续设置简单的密码的。



操作手册没有任何帮助后，我又再次返回登录页面，这时候我们就可以查看js文件，或者网页源代码来帮助我们挖掘漏洞：



在翻阅后看到这个接口：

（get方法构造请求，post传输参数）能看懂ajax吧，看不懂的就需要去弥补js的知识，随手构造接口访问试试：



没想到报错爆出另一个参数，然后构造语法开始对管理员密码重置：



success出现，更改管理员密码的逻辑漏洞到手，但是我的习惯一般都是先改弱口令然后在提交逻辑漏洞：



成功重置密码进入后台，后台可以上传文件到达getshell，由于上传没有难度，无waf，我就不记录了，

站点大约有38个全是edu的：



js接口需要熟练的使用，那么逻辑的0day唾手可得，下面这个系统也是同样的方法：我就直接上报告分析了：此系统大约50 个站点全部以修复



总结：其实挖洞还是细心和个人思维，黑盒测试玩的就是思路，想法有多大，漏洞就有多大，别以为不可

能，或者一直和waf死磕。