**记录授权系统的测试**

**前言**

此系统只是浅度测试，领导让我随便测测就行，各位大哥勿喷。目的主要还是用实际系统告诉还未工作的哥哥们，可能工作的系统有些比你挖的src叼，但肯定也有很low的，加油！

**正文部分**

既然是授权了，一般情况下确定了这个ip，当时客户给我了一个前台810端口下的，IP访问，也不用想什么域名，测一下目录找找后台，或者nmap扫一下端口，看看后台是不是在其他端口就可以了，这里很简单，后台很好找，就在admin目录下，如下图



其他用于写报告的漏洞这里就不写了

先看以下前台

**1、SQL注入漏洞**

一般情况下还是想看看新闻详情页面，总觉得此页面会存在漏洞，但是很不友好，此页面测试了以下，过滤的相当全面



只能换个页面，新闻列表，此页面是存在注入的



但是测试了之后会发现输入and 1和and 0都是错误页面，换&&或者%26都不行，or和xor也都不行，order by也返回错误，注释符号也返回错误，那现在只希望这个传参是整形的了





事实证名id=2-1返回了和id=1一样的数据



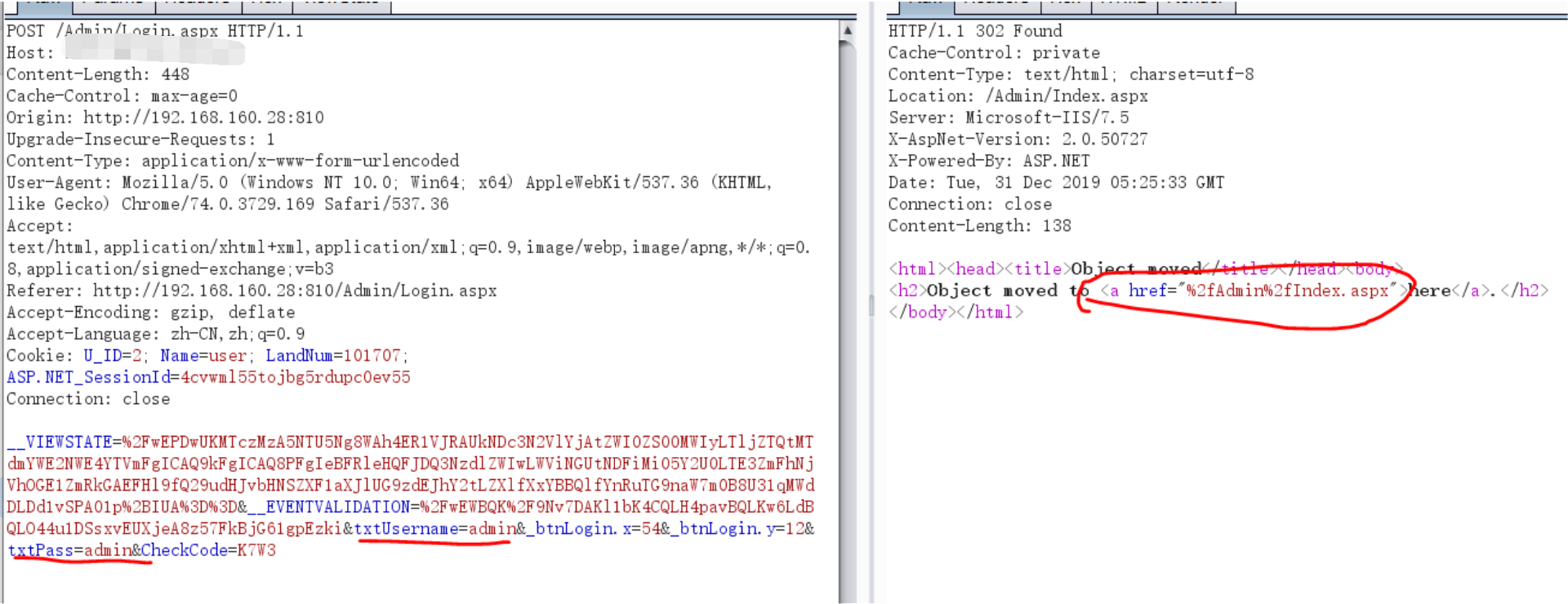
哪里用就很简单了直接在1的位置输入payload就可以

比如：id=105-ascii(substring((DB\_NAME()),1,1))，说明第一个字符的ascii值为104

过，我不想注入拿密码，后来事实证明真的解不出来

**2、弱口令？**

是弱口令吗，我反正admin/admin进了后台

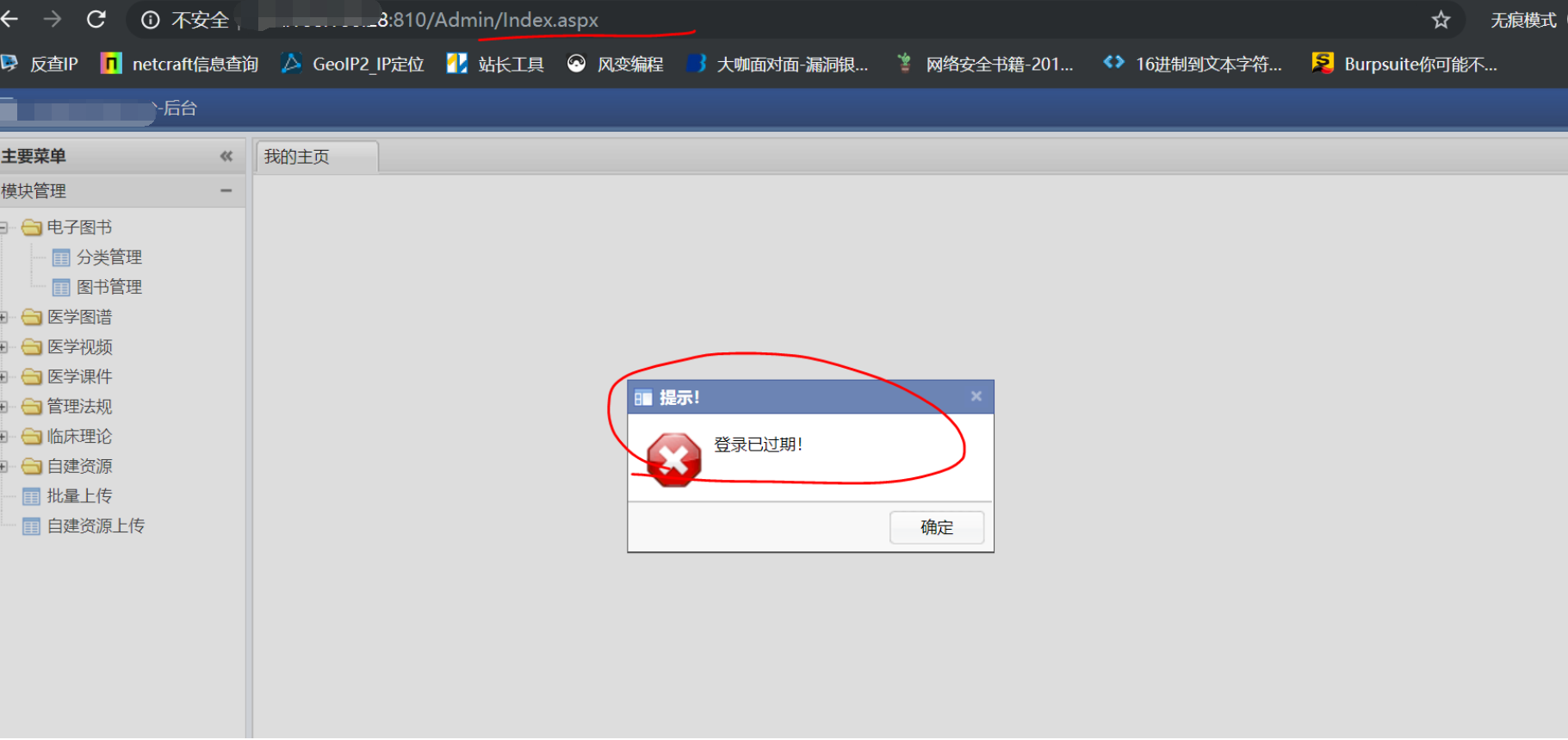


成功跳转了index，但是这个cookie相当可疑啊！我用的admin登录的。U\_ID=2就忍了，Name怎么还成user了，莫不是。。。但这里依然不能确定，但是这cookie的样子不是未授权就是越权啊

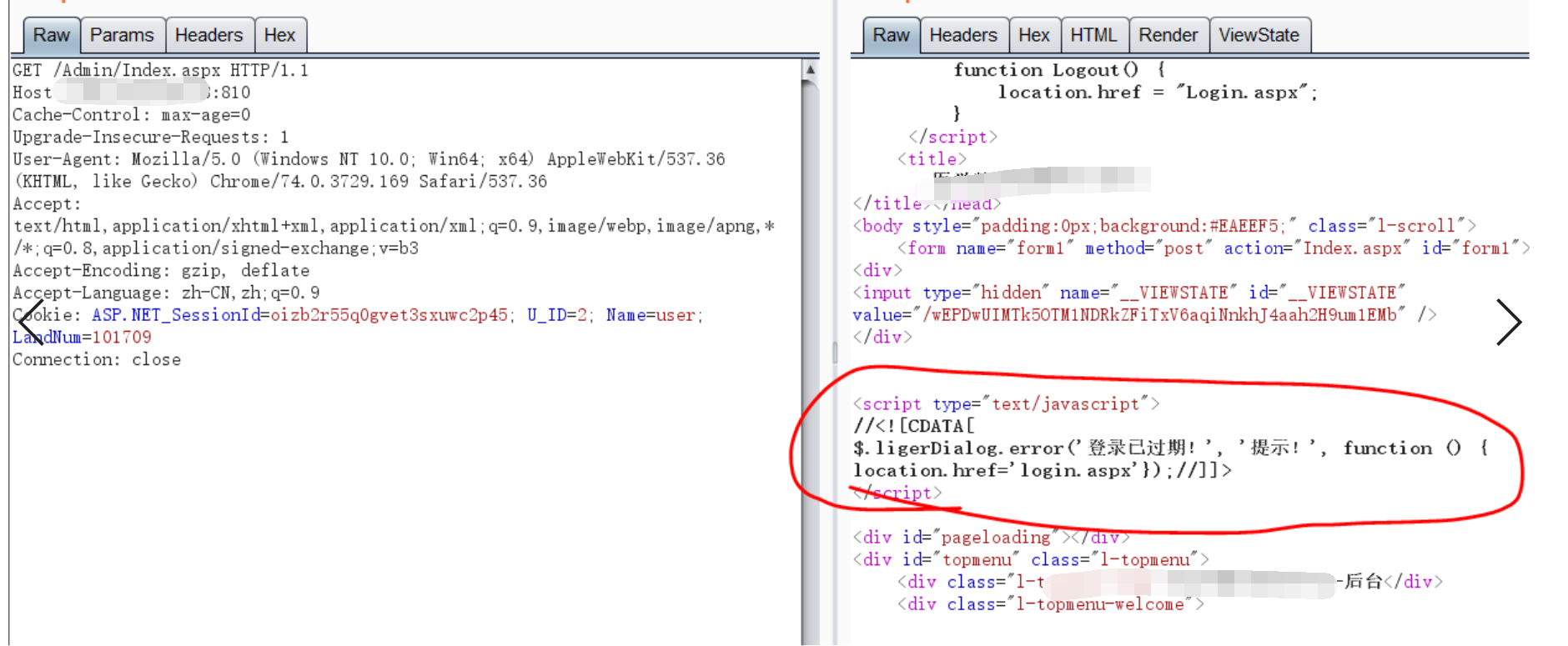
**3、未授权访问**

于是乎尝试一波未授权，毕竟还是要写报告的

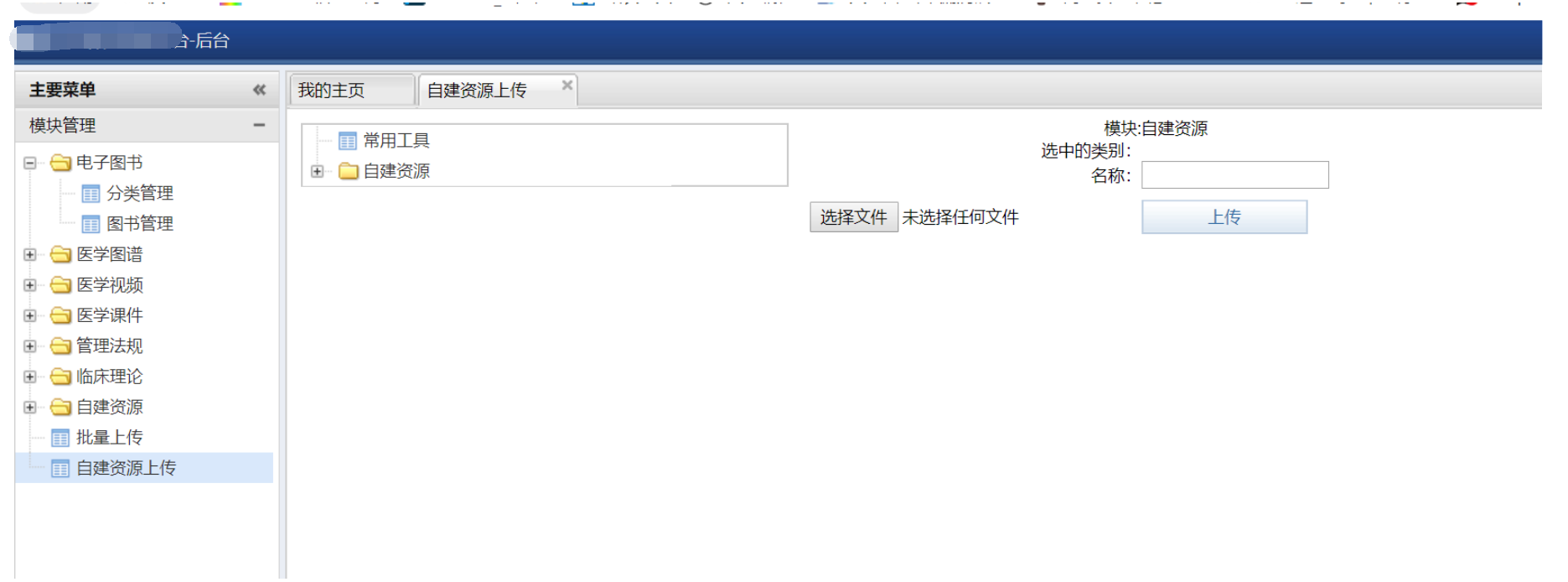
直接访问index页面，会有弹窗，身份过期，但是是在你点击确定之后才跳转登陆页面，这就已经是漏洞了，如果能访问到东西，那就未授权无疑了



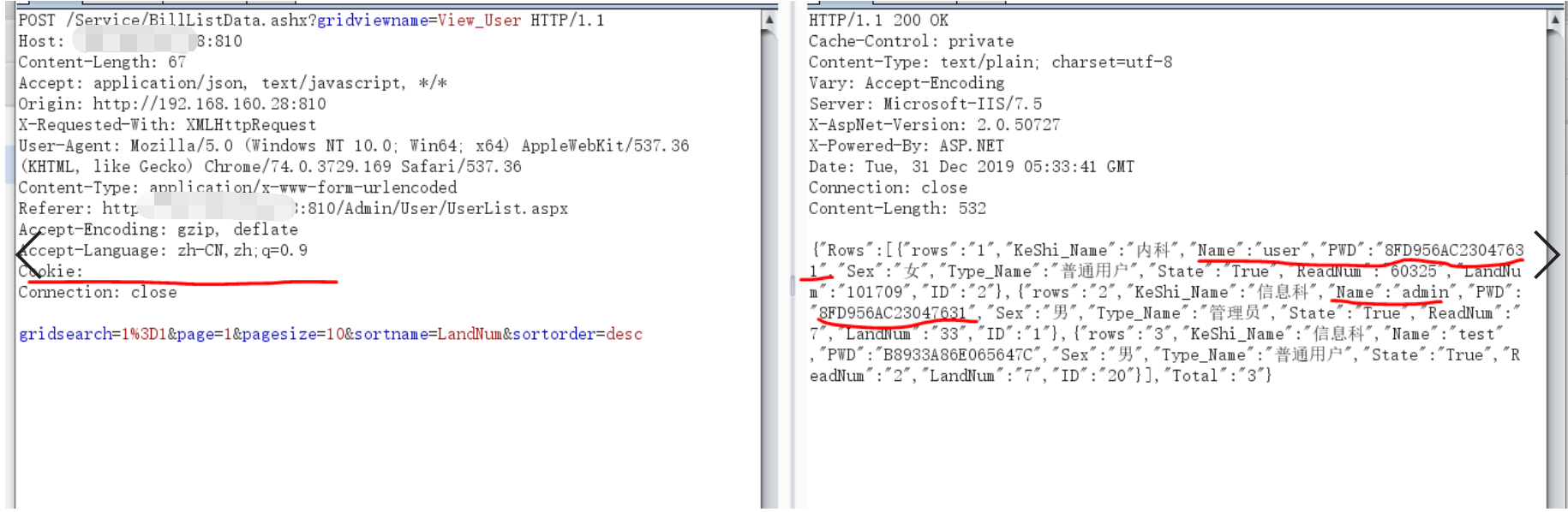
而这种弹窗，非常好过的，返回包的js代码删了就行，如下图



页面停留在了，后台页面



但是测试了以下，不是全部都存在未授权，只能说某些接口吧，比如上面的上传，就是只能看，上传提交的页面会对身份信息进行验证，但是查看用户页面就不存在，直接查看，所有用户名和密码，如下图



从返回信息的密码里面我尝试解码一波，16位应该是md5，但是没有解出来，admin这种口令按说肯定可疑撞出来啊，为了进一步确定猜想，我看到user的密码和admin的密码是一样的

尝试admin登录user，登录失败，wtf？

应该就是了不是弱口令，可能是某程序员镶嵌在代码里的万能账户，无论修改密码与否，admin/admin是都能登录的，不知道算个啥洞

**4、文件上传之zip**

为什么要把这个东西提一嘴，因为真的发现了，漏洞不一定上传脚本语言才是危害大，你可以上传html，有人可能会问html能干嘛，首先钓鱼，哥哥们都知道，s2里面存在可利用webconsole的页面，你可以上个html的前置跳转页完成利用，甚至对于这种国家单位来说，你传个某些方向言论的html，简直是灭顶之灾，妥妥的高危，而我今天选择了上传zip，哈哈哈

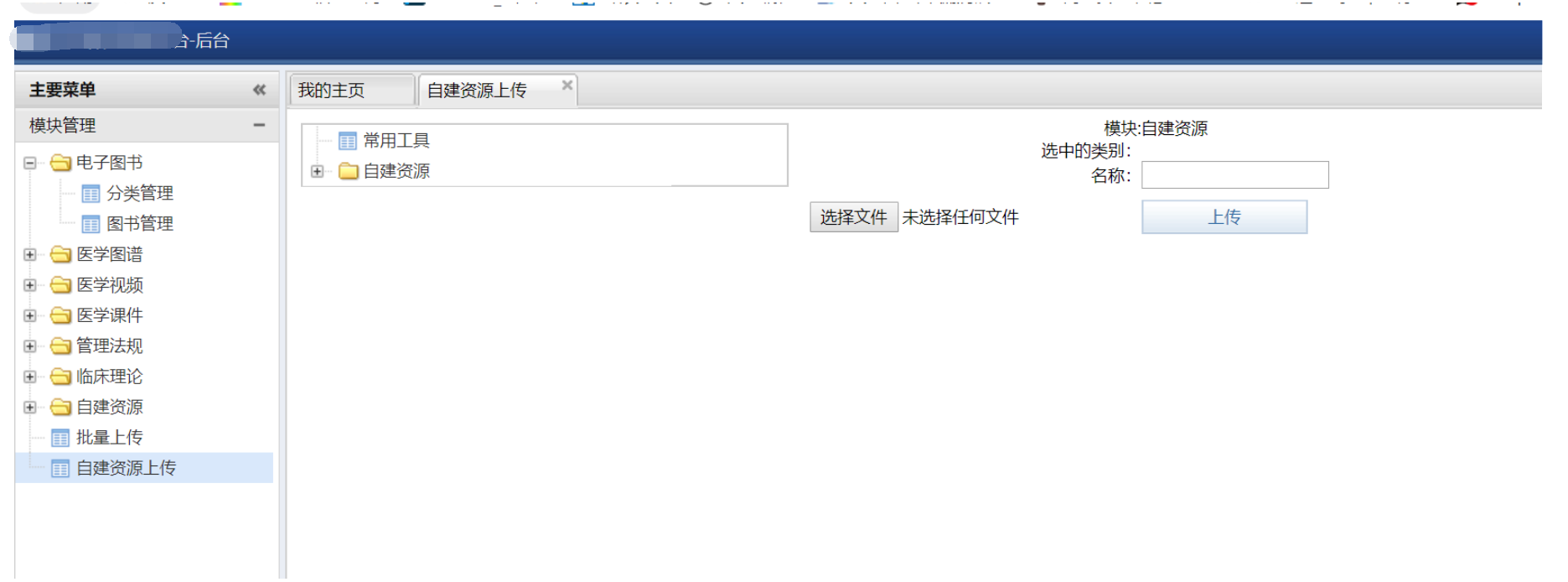
其实因为上传shell的方式我实在没绕过去，白名单加重命名一般就不想了，巧了zip是白名单

为什么说这个传zip是个洞呢，但是我没给客户提，先来看看前台某页面

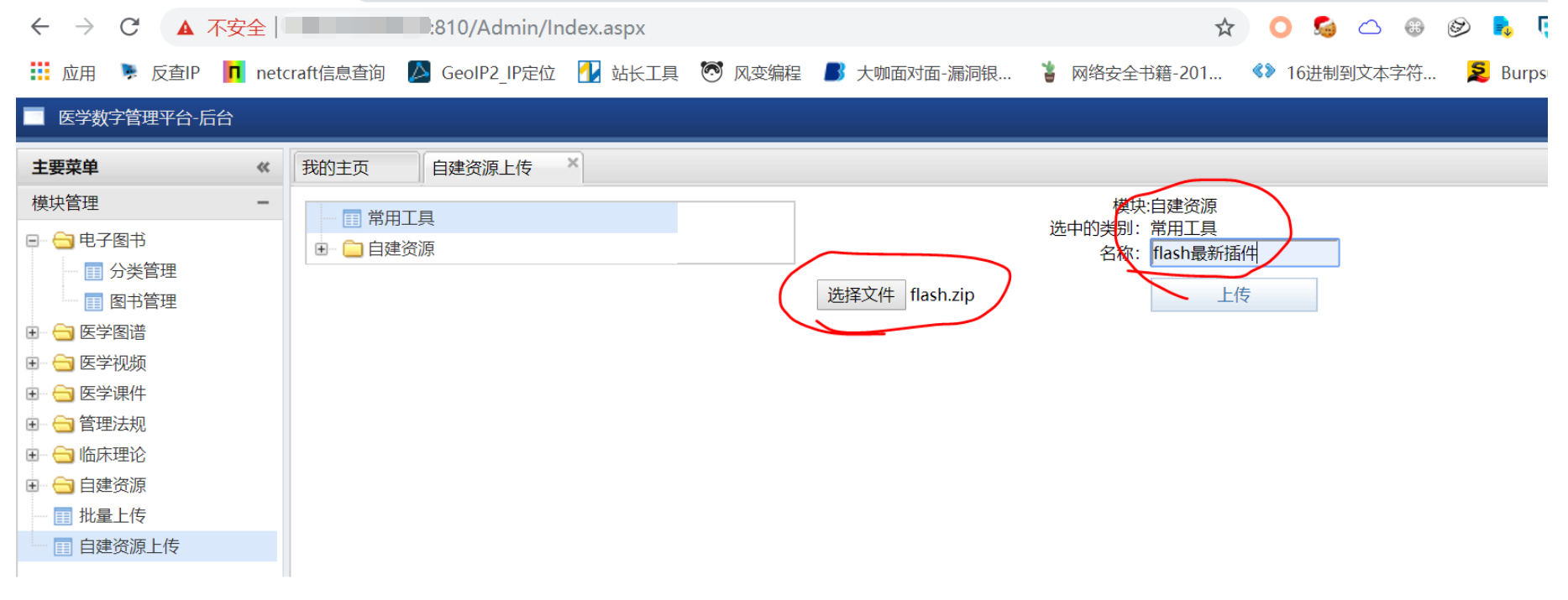


这里的文件基本都是zip和rar的，共系统用户下载，而且比如flash是必须装的，不然不能正常访问，那么问题就来了，如果这个上传点可控，我还特么上传什么shell

然后我找到了就是下面这个页面，自建资源



接下来，我们就可以用msf生成一个exe的反弹shell的木马文件，改个名，压缩一下，免杀的话这里不提，只是思路，如下图flash.zip



成功上传，如图



看看前台效果，如下



还嫌不够的话，你甚至还可以发个公告，告诉大家，flash插件改更新了，反正你有万能账户。端起茶叶水，等着shell回弹

**总结**

觉得这种有点意思，分享下，此系统其他写报告的洞就不说了，都是凑数，而这个没写报告。。。。