使用2003系统搭建ASP网站BBSXP



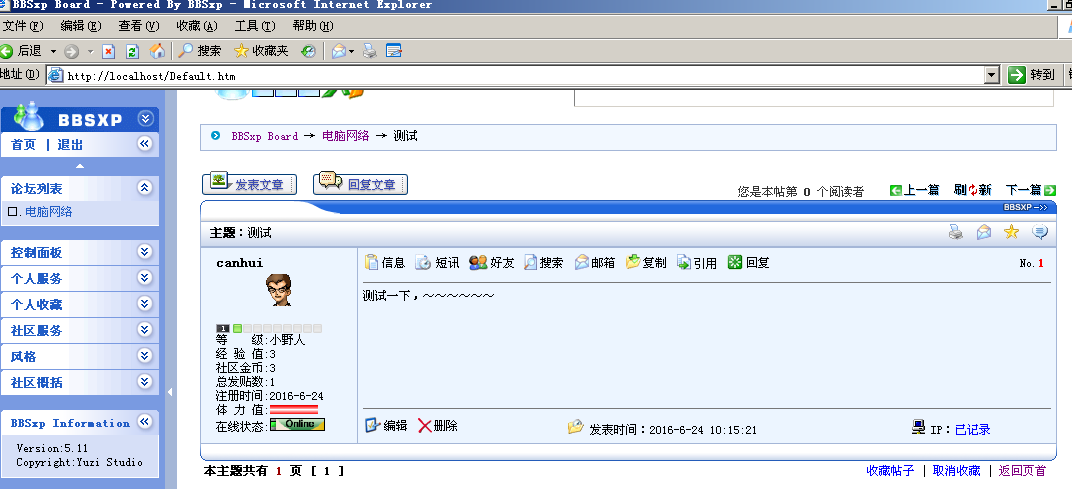
设置论坛电脑网络



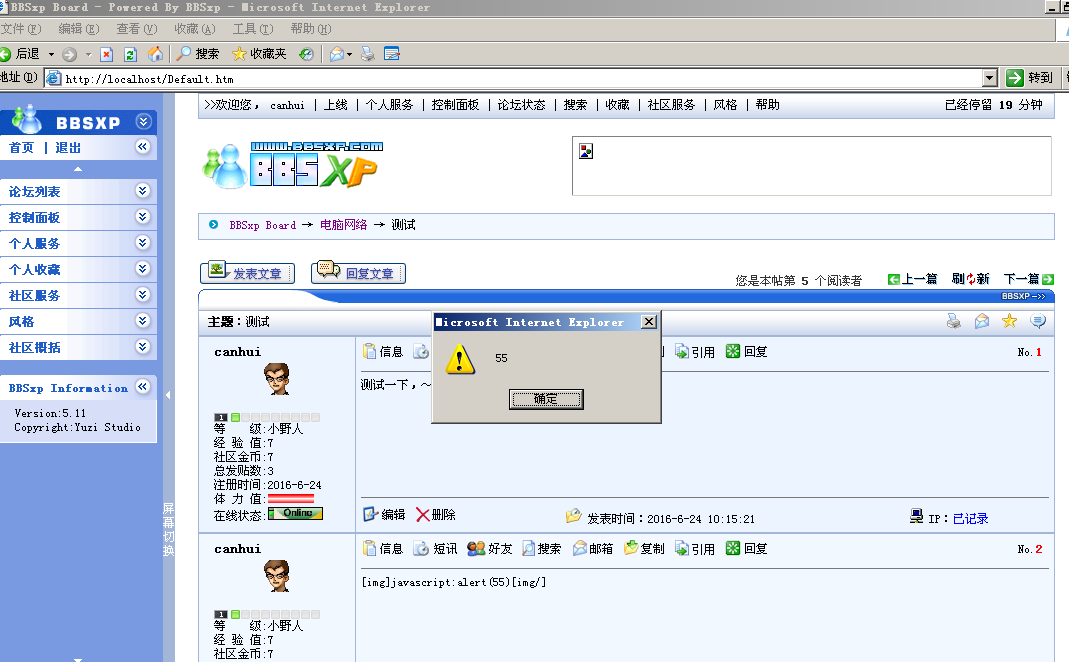
注册普通用户canhui



在电脑网络发表文章



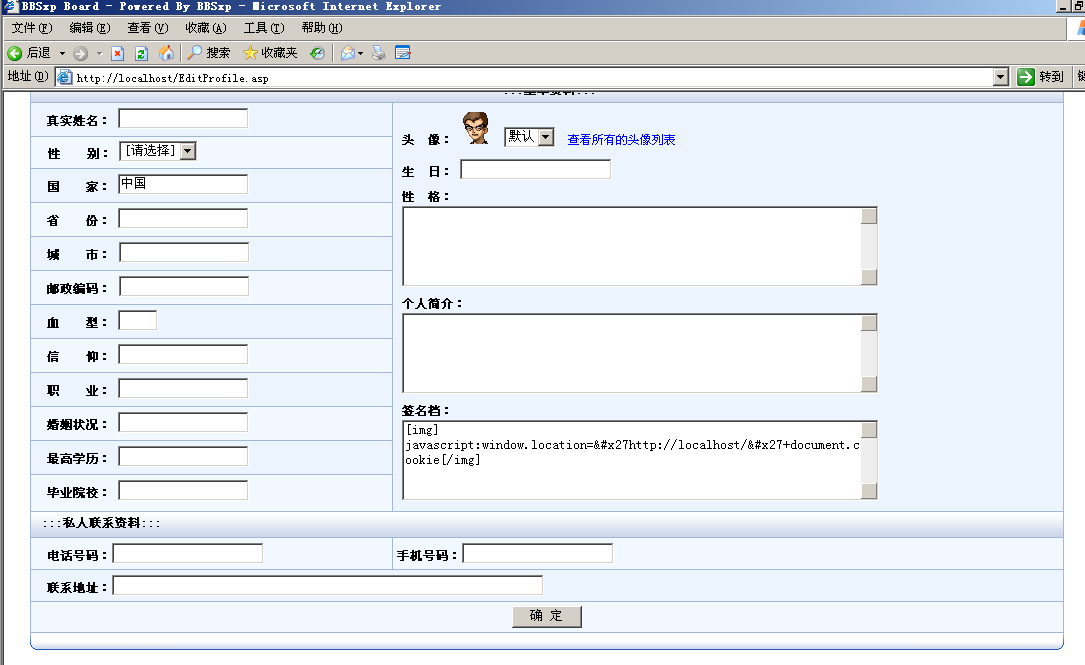
在回复帖子栏输入信息判断是否存在XSS漏洞



**弹窗发现存在XSS漏洞，存在XSS漏洞**

**利用XSS漏洞盗取cookie信息**

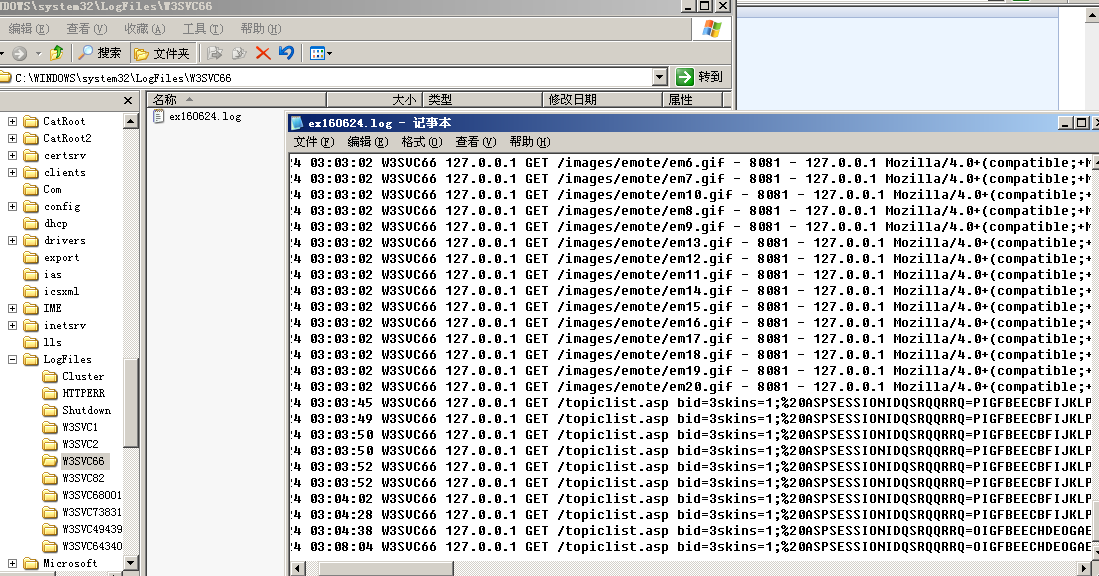
把签名档设置为，当其他用户浏览了帖子发送cookie到定义的网站上



用管理员访问canhui的帖子，跳转到设置的地址上，并发送了cookie



找到IIS服务器的日志文件



Admin的cookie值为

skins=1;%20ASPSESSIONIDQSRQQRRQ=OIGFBEECHDEOGAEPNPDLDIME;%20userpass=592742EF7B3263F3F5072C03935026C3;%20username=canhui;%20addmin=40;%20onlinetime=2016%2D6%2D24+11%3A03%3A39;%20posttime=2016%2D6%2D24+10%3A21%3A36;%20CNZZDATA1254308410=1544461098-1466726524-%7C1466732072;%20bbs=Mymark=551&Mycook=30&Myhide=1&Mytopic=50&Mypass=7a57a5a743894a0e&Myname=admin&Mymoney=476&Myface=images%2Fheadpic%2F1%2Egif