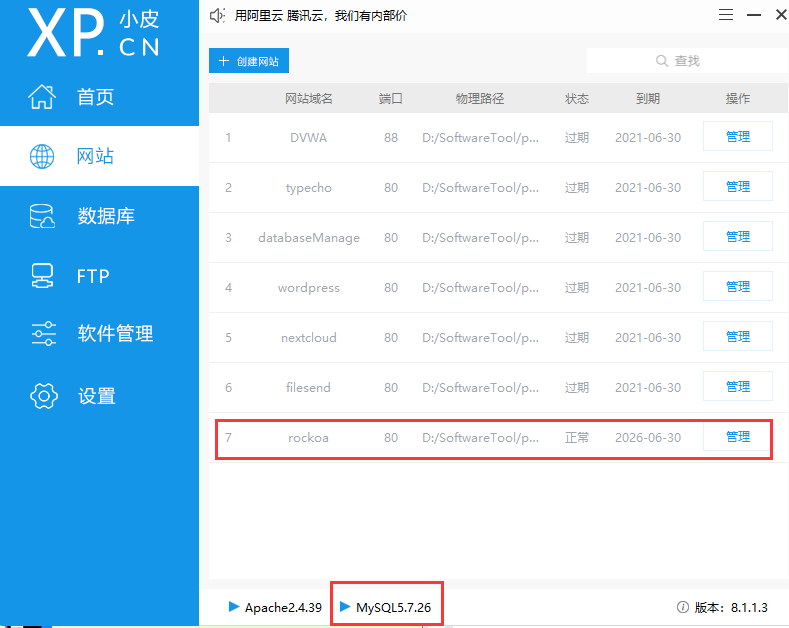
**1.安装PHPStudy，然后安装rockoa站点（所用php版本为5.4，数据库版本为5.7）**



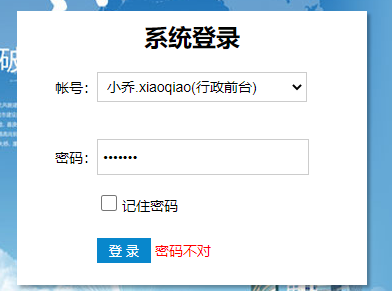
然后访问对应站点，根据提示进行安装即可

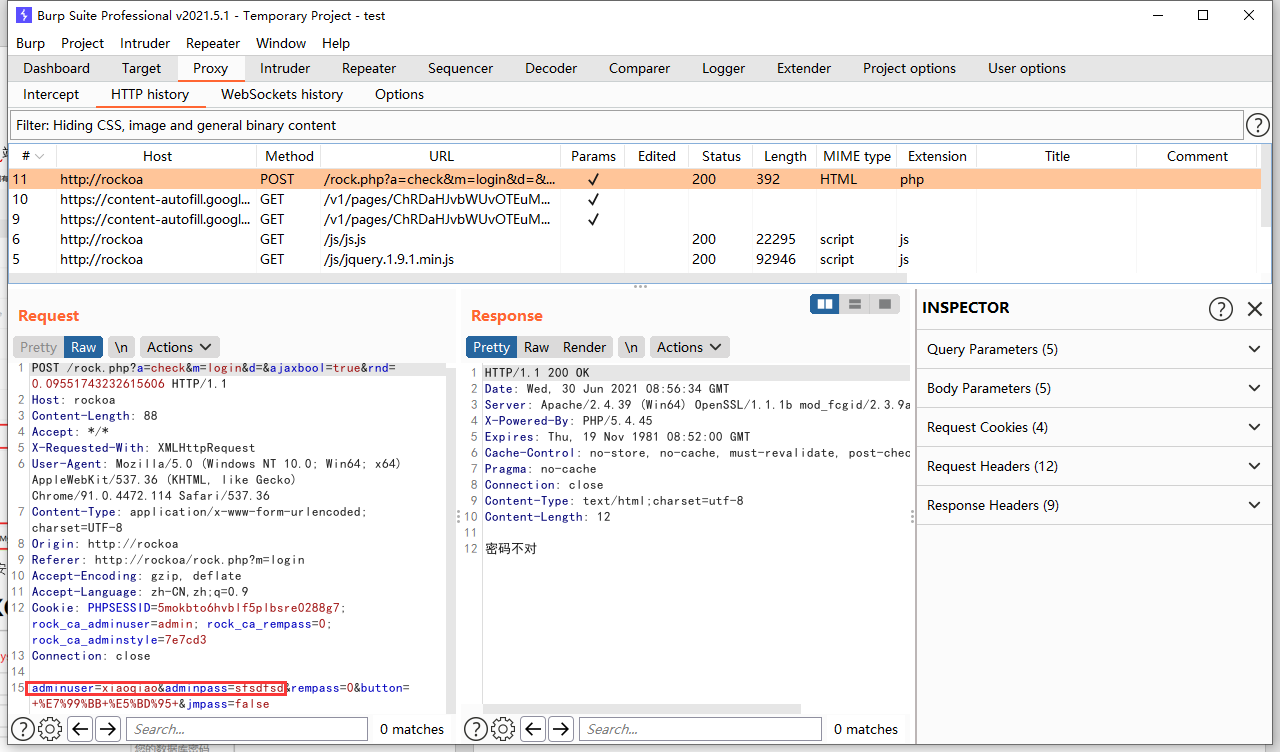




**2.使用burp suite对网站登录进行暴力破解**

利用burp抓取登录界面产生的请求包

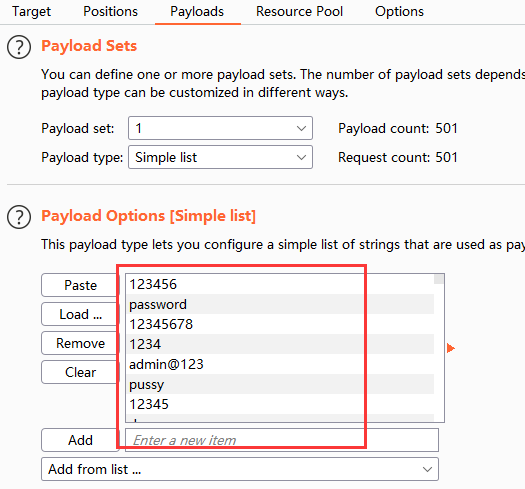




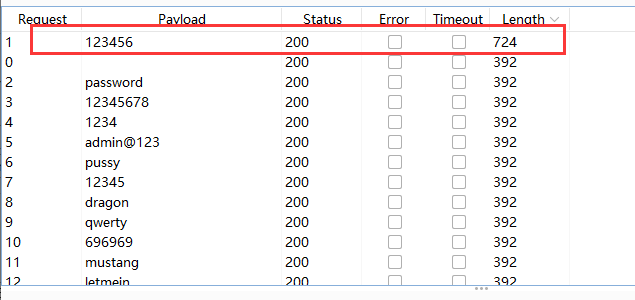
在intruder中设定爆破字段



设置字典



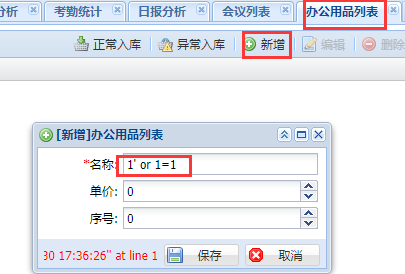
进行爆破



该请求包的长度明显和其他不一样，很可能就是登录成功的返回，查看返回内容，确实是登录成功

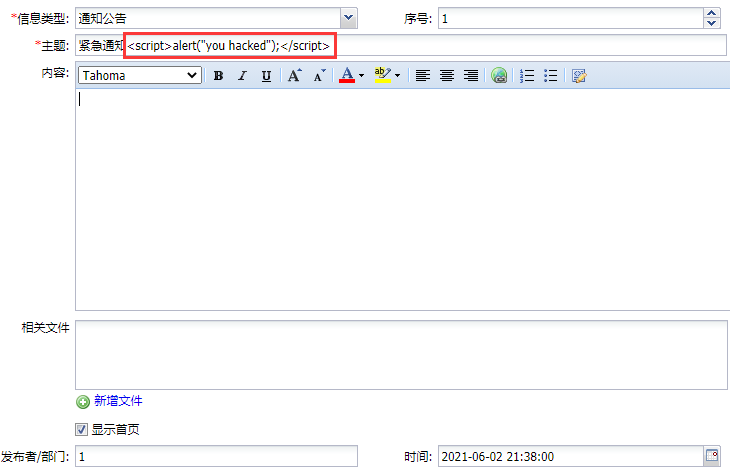
**3.SQL注入检测**

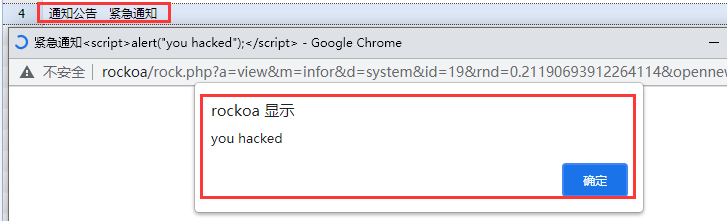
经过检测，发现这里存在sql注入漏洞



**4.XSS攻击**

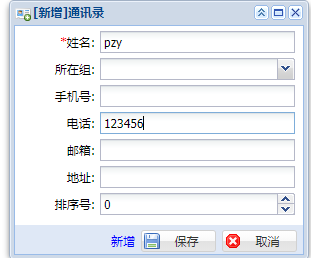
在主题中注入js代码，能够在查看该通告的时候，触发js代码执行

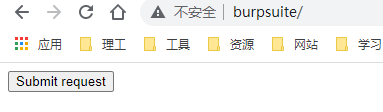


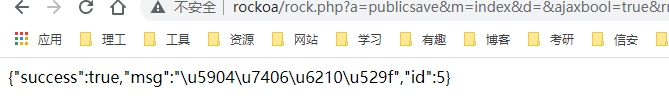


**5.CSRF**

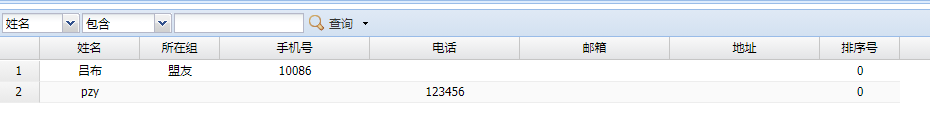
通讯录处，使用burp截获添加通讯录的数据包，然后生成钓鱼网页，诱惑受害者点击







（成功执行钓鱼网页）



（此时通讯录中已多出一条记录）