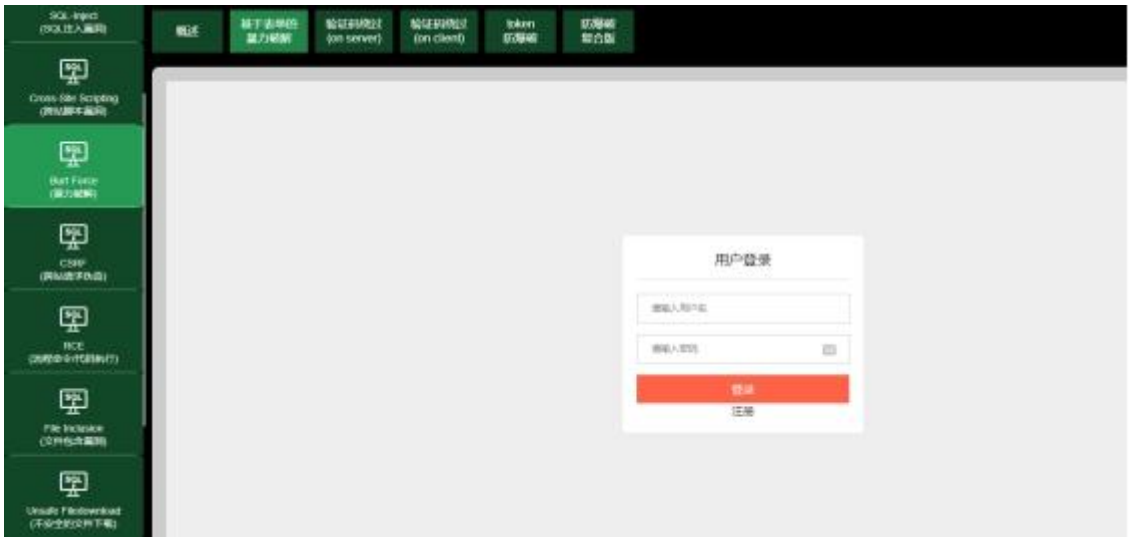
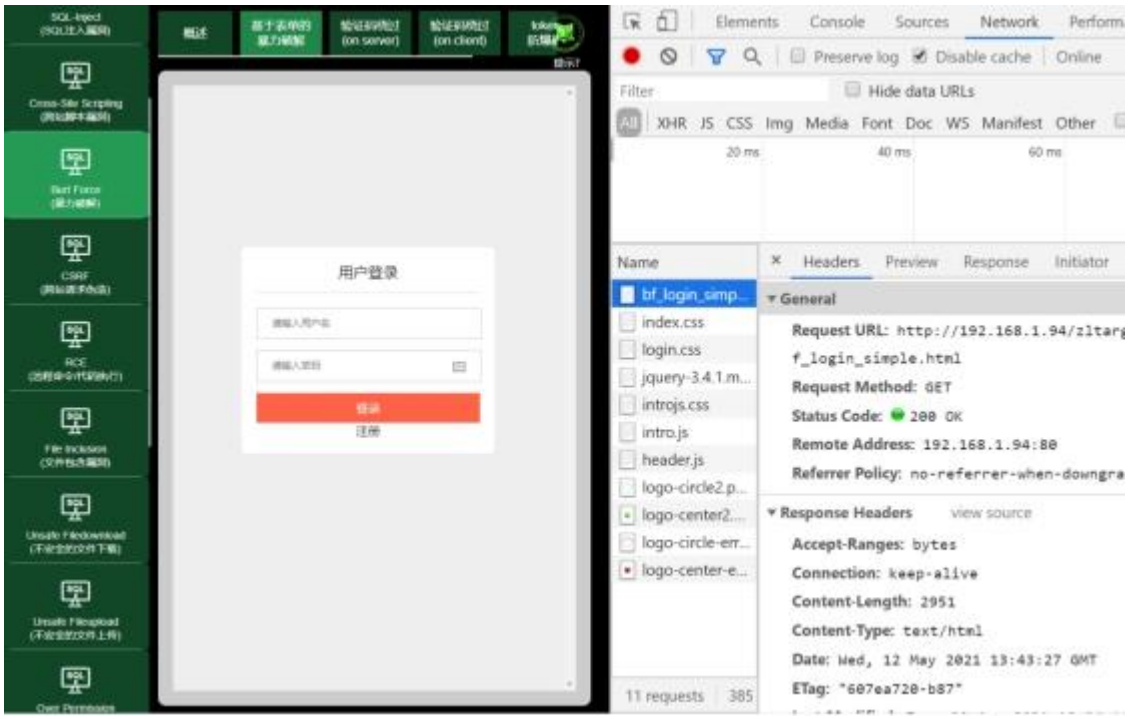
暴力破解的实验

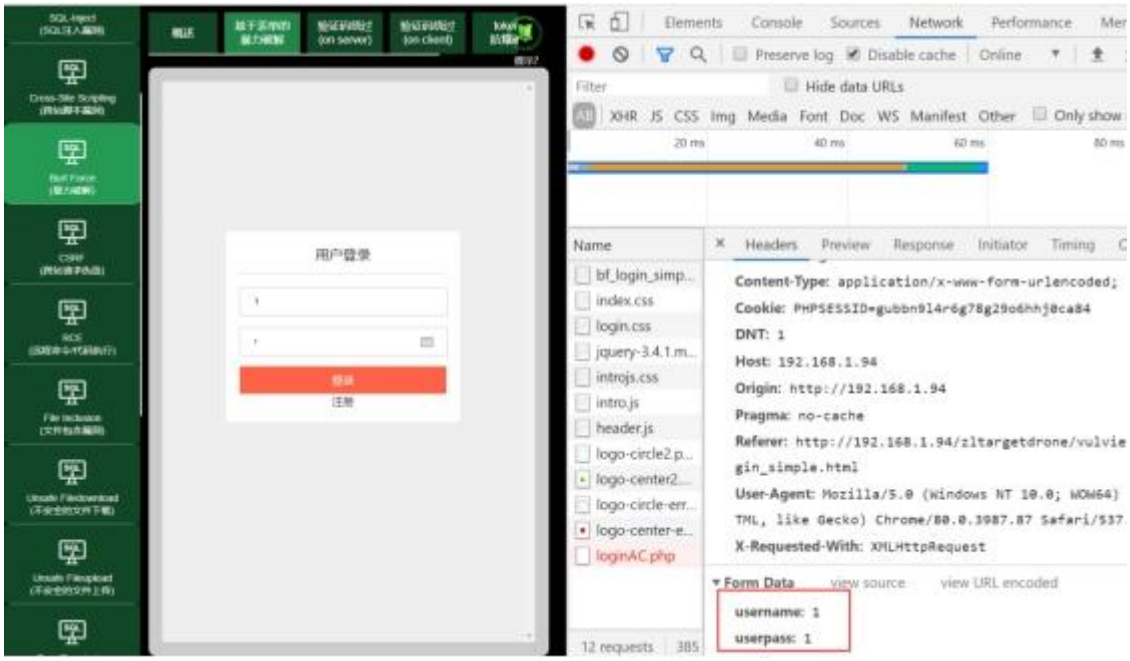
1、暴力破解的实验原理

暴力破解”是一攻击具手段，在 web 攻击中，一般会使用这种手段对应用系统的认证信息进行获取。 其过程就是使用大量的认证信息在认证接口进行尝试登录，直到得到正确的结果。 为了提高效率，暴力破解一般会使用带有字典的工具来进行自动化操作。 理论上来说，大多数系统都是可以被暴力破解的，只要攻击者有足够强大的计算能力和时间，所以断定一个系统是否存在暴力破解漏洞，其条件也不是绝对的。 我们说一个 web 应用系统存在暴力破解漏洞，一般是指该 web 应用系统没有采用或者采用了比较弱的认证安全策略，导致其被暴力破解的“可能性”变的比较高。 这里的认证安全策略，包括： 1.是否要求用户设置复杂的密码； 2.是否每次认证都使用安全的验证码或者手机 otp； 3.是否对尝试登录的行为进行判断和限制（如：连续 5 次错误登录，进行账号锁定或 IP 地址锁定等）； 4.是否采用了双因素认证等等。

1.1、如何进行暴力破解之基于表单的暴力破解？





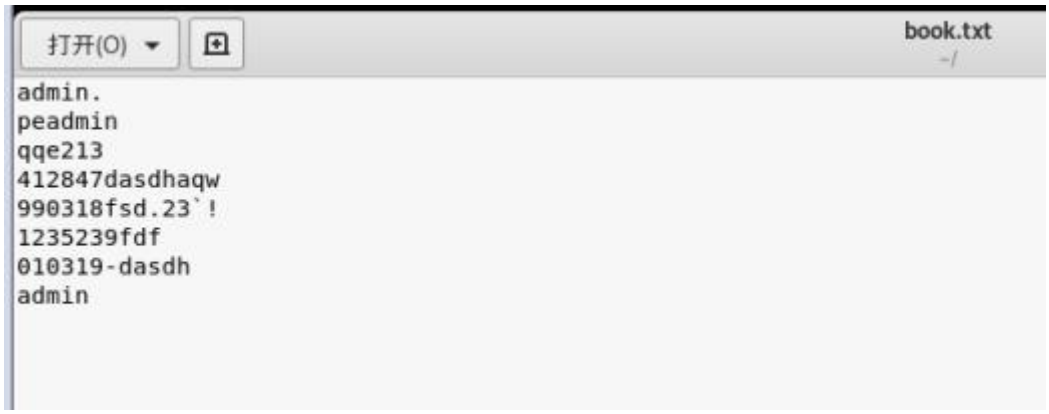


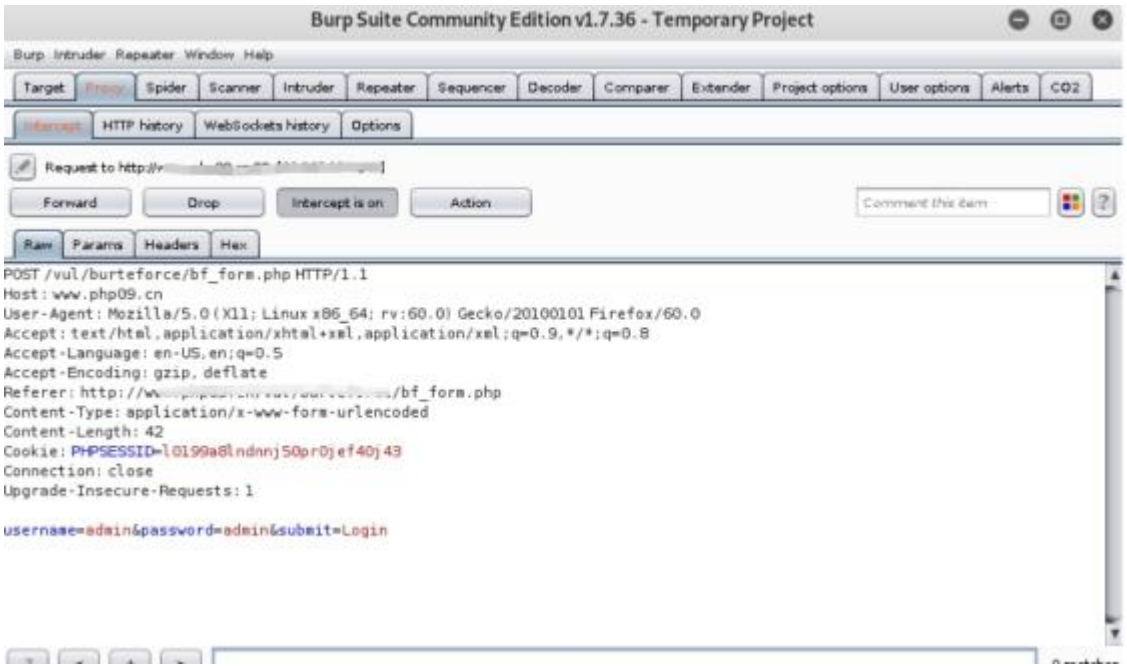
一般情况下，可以直接通过浏览器查看请求的路径的提交的数据，以判断是否可以进行一步的渗透操作，如果存在可以提交的数据，且数据为明文形式，可以通过伪造数据字典通过工具进一步进行爆破处理。

1.2、通过字典进行暴力破解

工具：burp suite

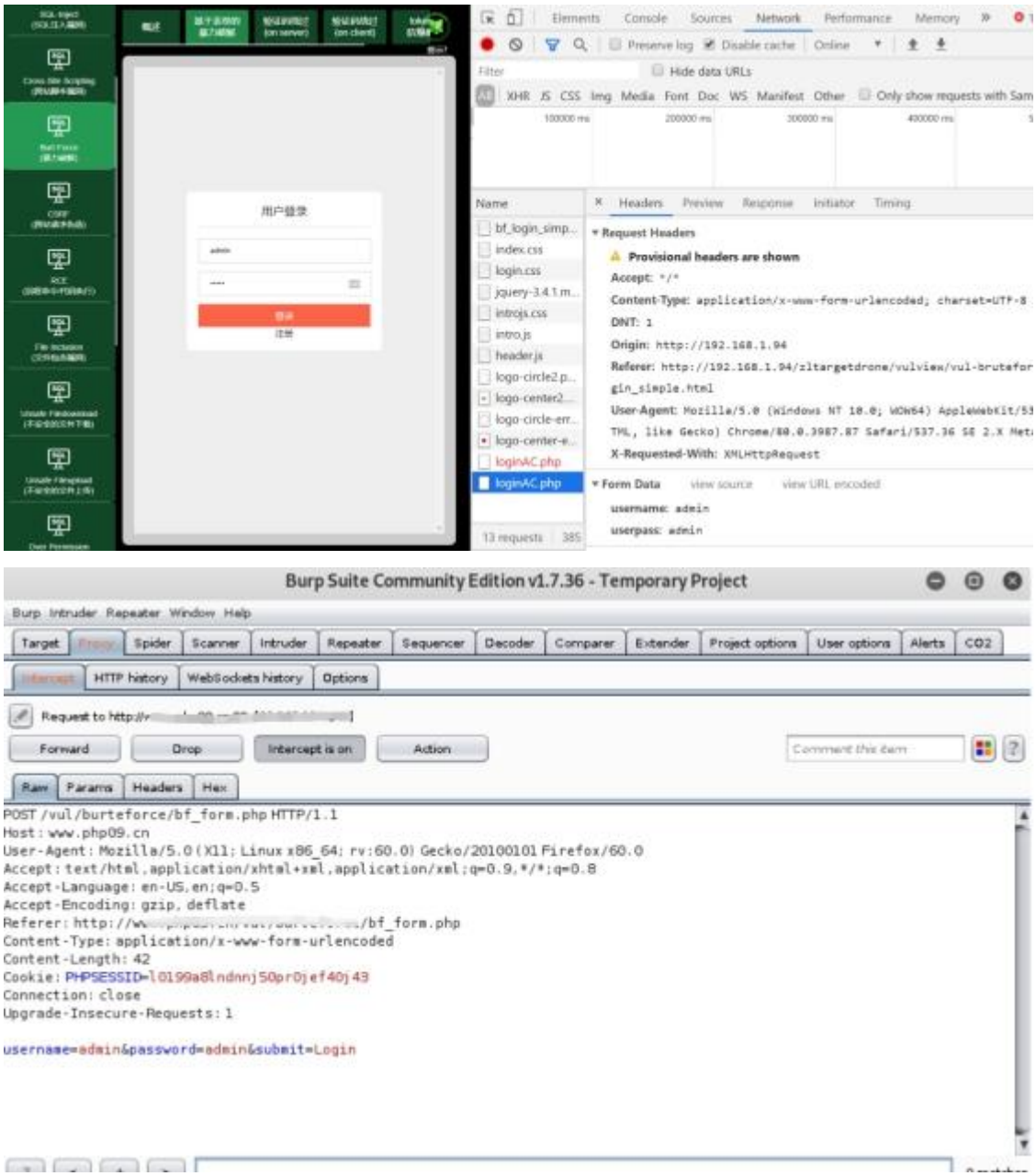
字典：





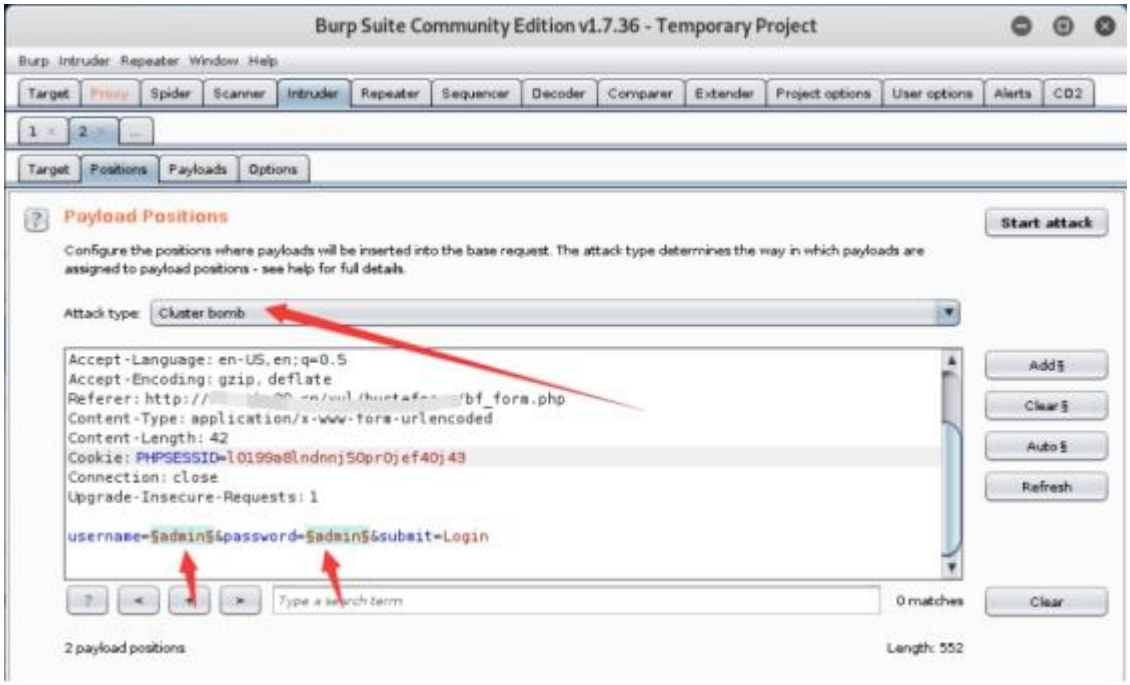
通过 BS 工具，直接对可提交数据的接口进行字典注入，通过注入的数据，观察返回结果。我们随便键入用户名和密码，可以看到发送的为 POST 请求，username 对应的用户名.password 处对应的密码。当然,我们此处登录失败。

1.3、通过工具注入推测接口进行暴力破解



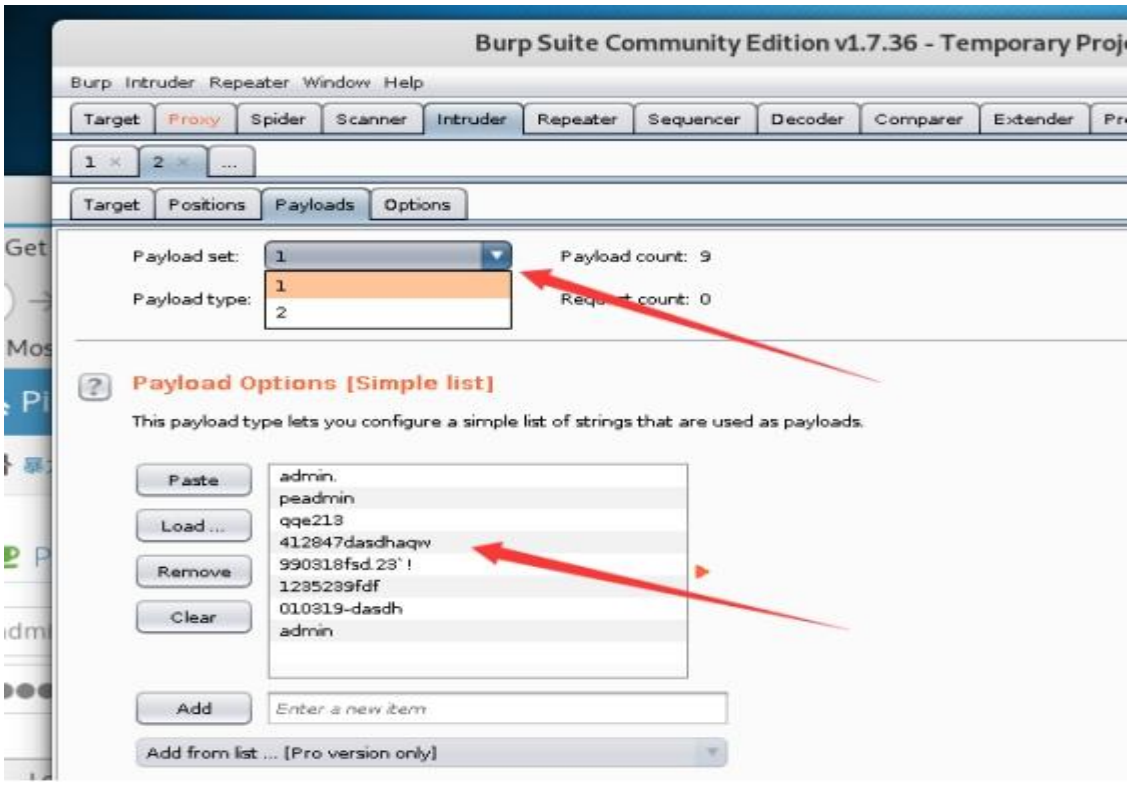
我们抓到这次请求之后,使用 burp 的 intruder 进行爆破。我们首先选择 bomb 模式, 因为这个模式会穷举字典的一切组合,来尝试所有可能出现的用户名,密码。我们在 username 和 password 处进行标记,标记的意思就是等会要替换的位置。

1.4、载入字典文件并设置爆破规则



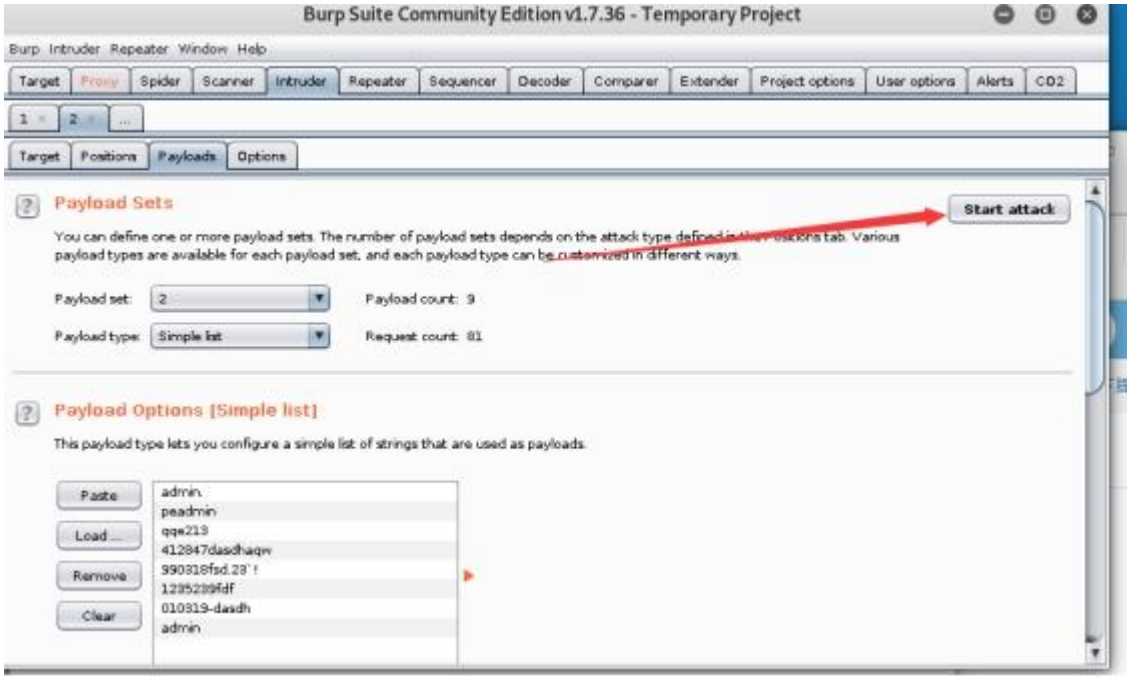
接下来我们载入字典文件.一般来说,前面设置了几个变量,后面就需要载入几个字典(跟爆破模式相关)，字典可以一直,载入完字典也可以再次进行手动添加,字典也可以根据特定的规则进行自动生成.替换等。

1.5、加载暴力破解的字典进行爆破。



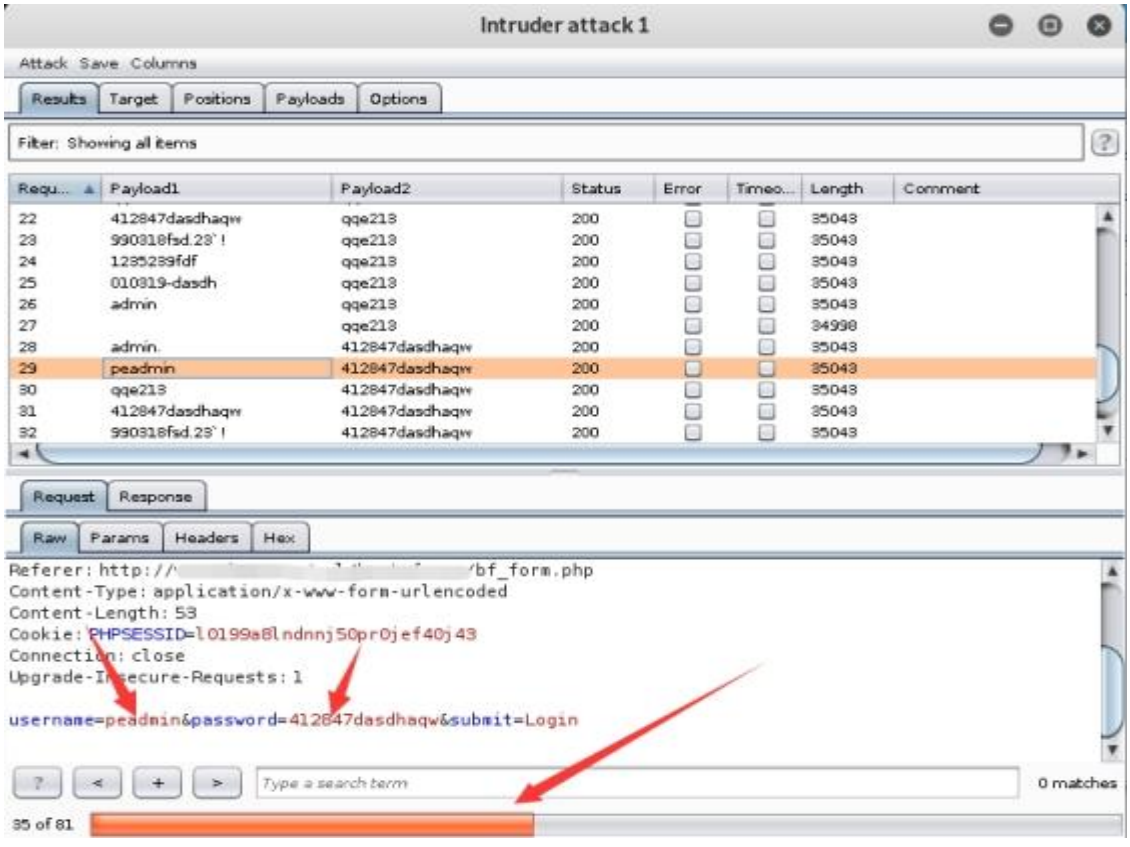
加载在第一步时生成的字典，列表中显示预设的字典数据。

1.6、开始暴力破解



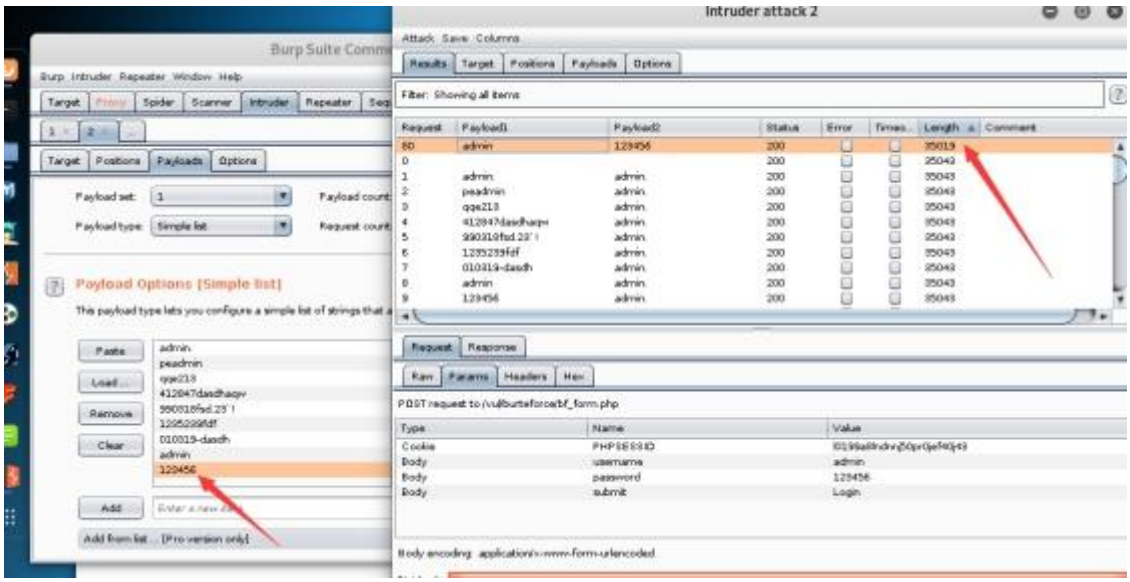
点击开始破解按钮，执行字典中的数据，数据将根据第二步中得到的请求地址来替换数据，实现自动化破解。

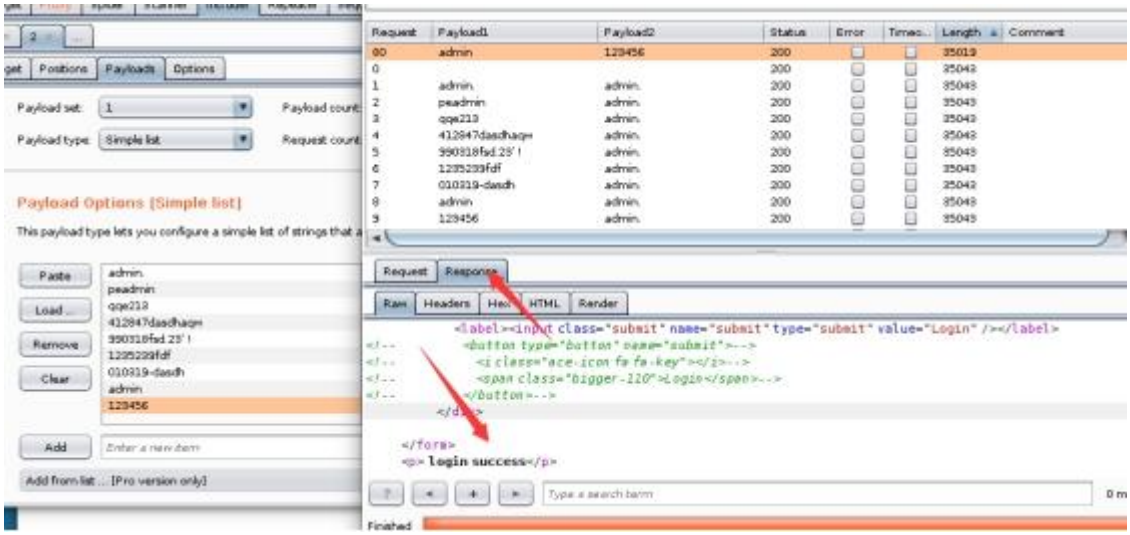
1.7、查看破解提交情况并判断下一步破解步骤



破解的时候 我们可以点击某一次请求 来查看具体发送的内容. 下方则显示整体进度条。

1.8、手动干预爆破数据，提高成功率

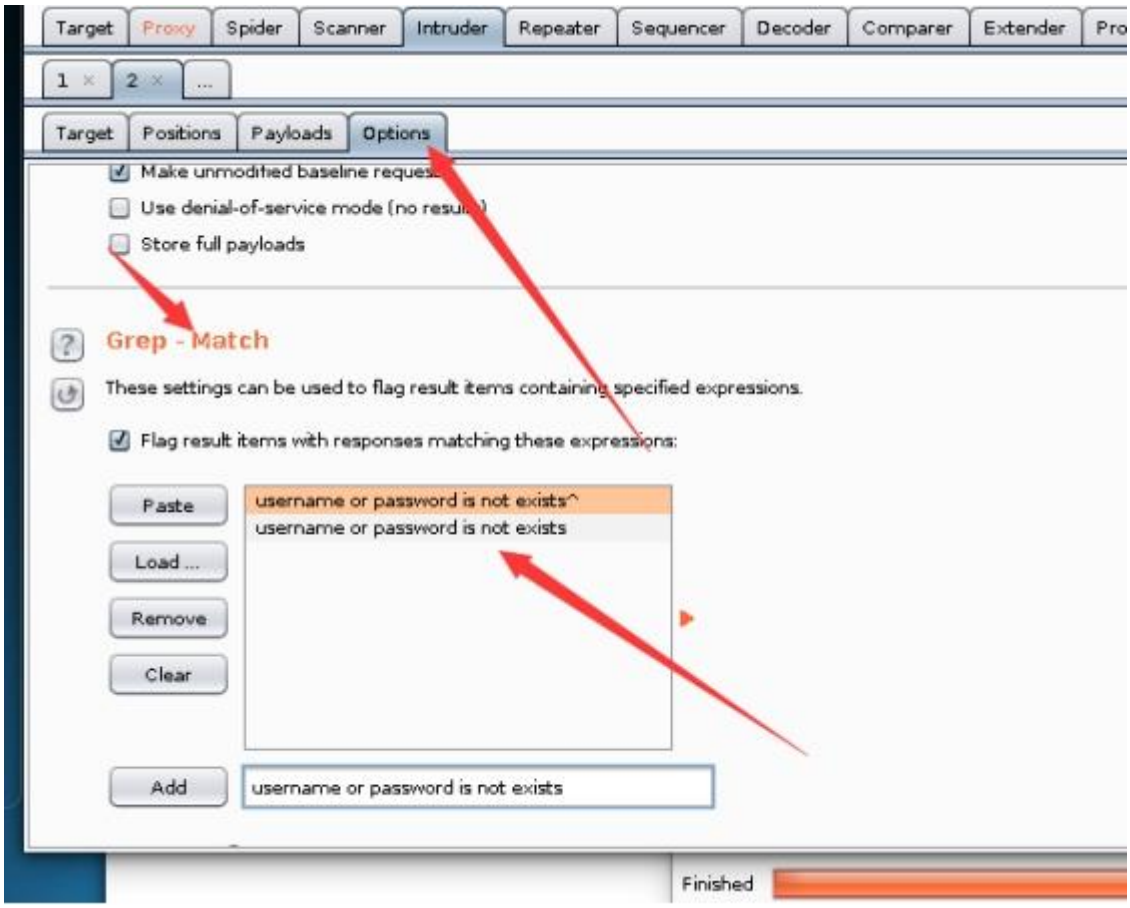


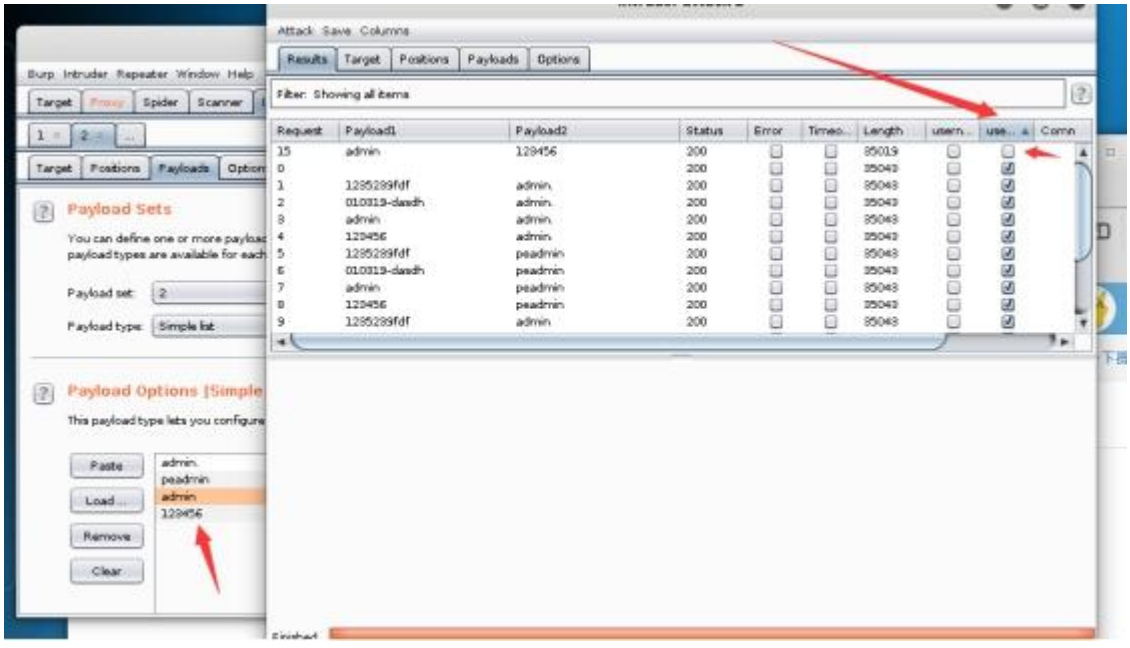


刚才由于我的字典文件里面没有正确的密码(123456),导致破解不成功，我手动添加了 123456 之后,破解完成之后可以看到,响应的长度和众多响应不一样,我们可以点开查看响应。

1.9 设置 burp 添加规则爆破

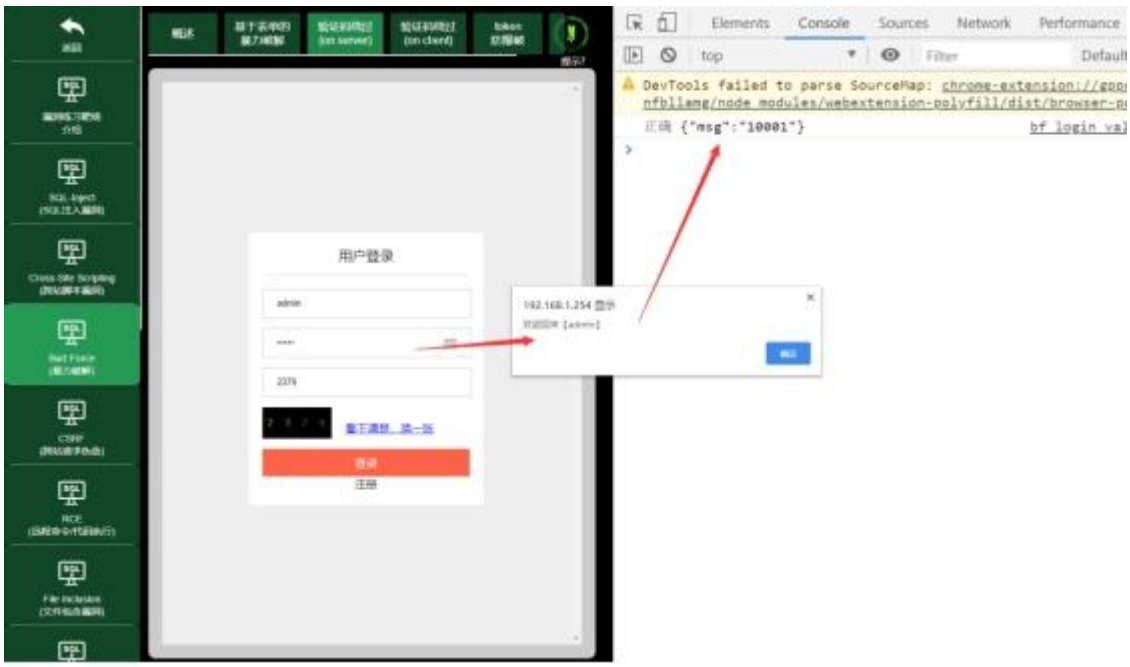
设置 burp 添加规则,从新尝试，从上次我们已经得知账户为 admin,密码为 123456,这次我们节省时间,字典少一点.





添加完之后,我们开始爆破. 完了点击排序. 我们很快的发现有一个请求没有打钩,没有打钩就证明没有出现特别的提示情况,我们点开请求查看,可看到对应的正确的账号密码.这到里破解到完成了。

1.10 验证爆破的用户名密码是否有效和正确



利用刚才爆破出来的用户名和密码进行登录，系统提示登录成功，则说明爆破成功。