短信验证码系列（二）

0X01（四位数验证码爆破）：

原理：在我们收到验证码的时候会有一个时间限制，比如 60s、五分钟内、24 小时内失效，但是往往这些验证码都不会在这个时间内失效，此时我们就可以考虑爆破验证码来获取认证。

（其实此处还有一个漏洞就是如果验证码在规定时间内没有失去效果，也是可以提交的）

常见存在漏洞的功能点：

1、修改密码功能点：修改密码时不需要输入原密码，网站通过验证码决定是否是本用户修改，并且网站的验证码机制没有时间（或者时间在一分钟以外最好，方便爆破）和次数限制，

2、用户注册点：如果可以爆破验证码，此时我们就可以获取任意用户注册漏洞，等级在中 高危 赏金可以达到四位数

3、支付功能点：如果支付时是通过短信验证，而且还是四位数的验证码，也可以尝试爆破

总而言之只要遇见短信验证的地方都可以尝试

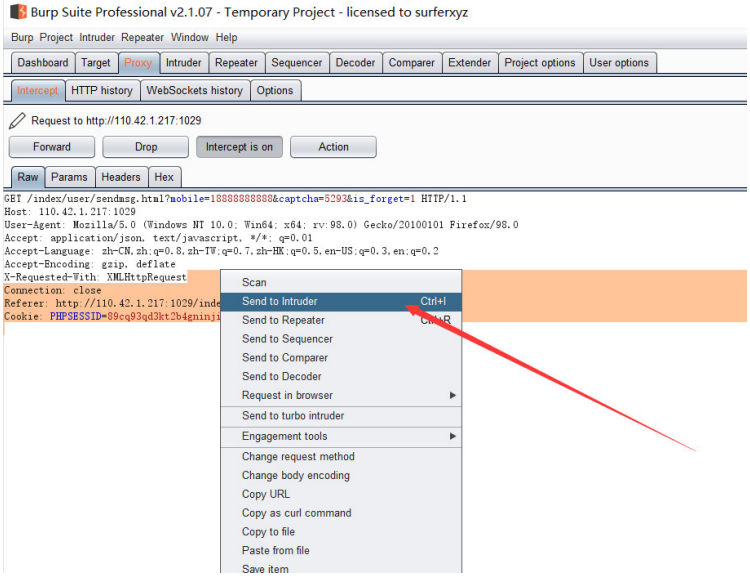
爆破验证码最好是爆破四位的，六位的话可能需要更多时间。

0X02（操作）：

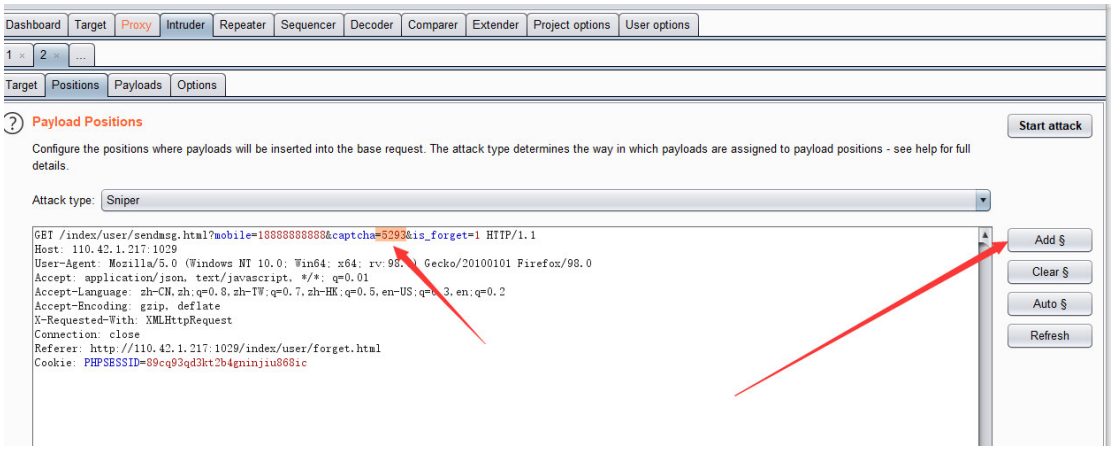
1、 工具：BURP

2、 操作：

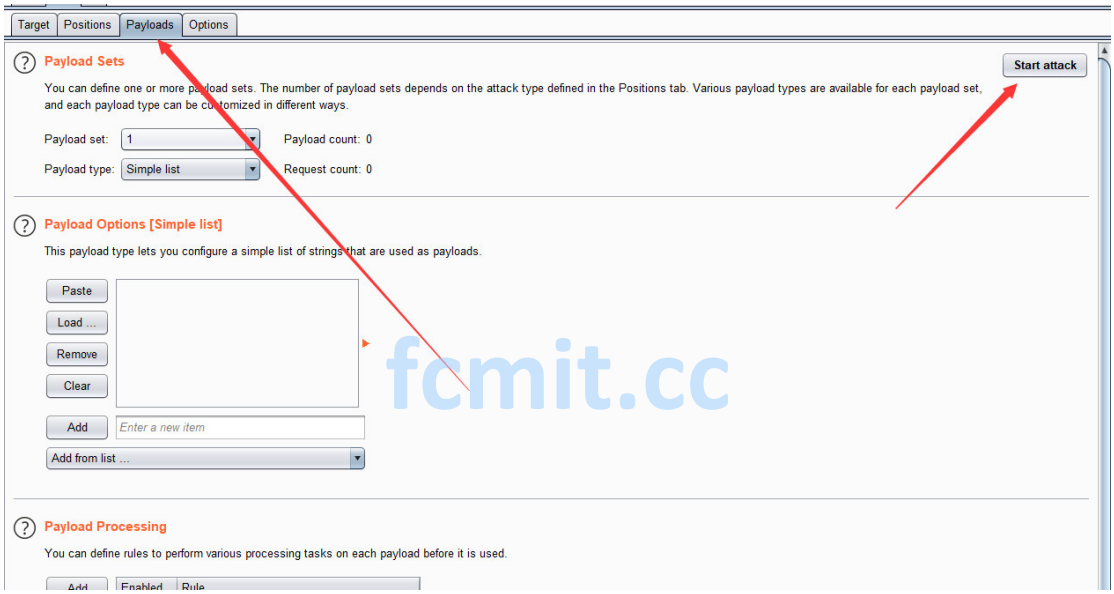
在短信验证码处抓包，发送到 intrudre 进行爆破



鼠标左键选择要爆破的位置，然后点击 add 即可



接下来在第三个模块选择爆破方法：（各种爆破方法去 b 站学习），最后点攻击即可。



0X03（案例）：

参与活动

漏洞类型 应用漏洞 >> 设计缺陷/逻辑错误

提交时间 2021-11-15 11:52:32

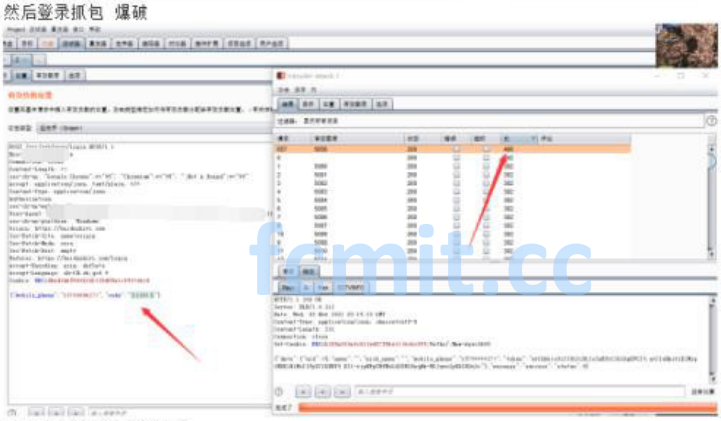
危害自评 低危

奖励安全币 5

附件 --

描述 在登录框任意输入账号获取验证码：

然后登录抓包 爆破



可以看出能成功爆破成功