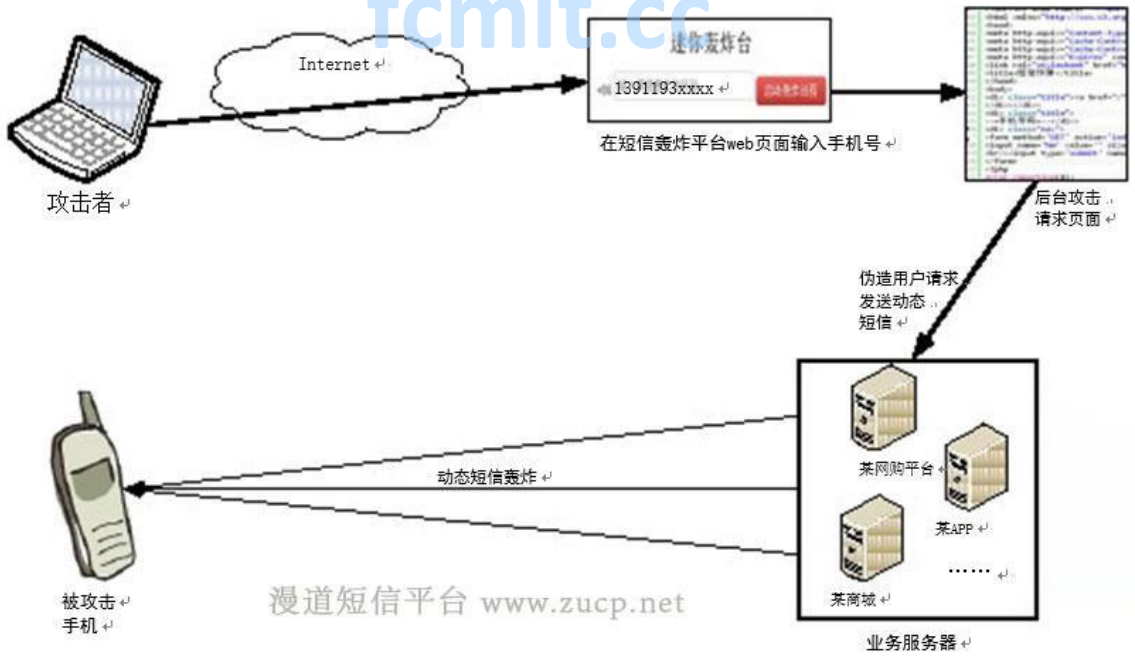
短信轰炸

0x01 原理：

短信轰炸原理

短信轰炸一般基于 WEB 方式，其由两个模块组成，包括：一个前端 Web 网页，提供输入被攻击者手机号码的输入窗口；一个后台攻击页面(如 PHP)，利用从各个网站上找到的短信验证码 URL 和前端输入的被攻击者手机号码，发送 HTTP 请求，每次请求给用户发送一条短信验证码。利用这两个模块实施“短信轰炸”攻击，原理具体分析如下：

1. 恶意攻击者在前端页面（下图所示 ）中输入被攻击者的手机号；
2. 短信轰炸后台服务器，将该手机号与互联网收集的可不需要经过认证即可发送短信的 URL 进行组合，形成可发送验证码短信的 URL 请求；
3. 通过后台请求页面，伪造用户的请求发给不同的业务服务器；
4. 业务服务器收到该请求后，发送短信验证码到被攻击用户的手机上。



0x02：测试工具

使用 burp 抓包然后发送到 re 模块或者使用并发插件即可

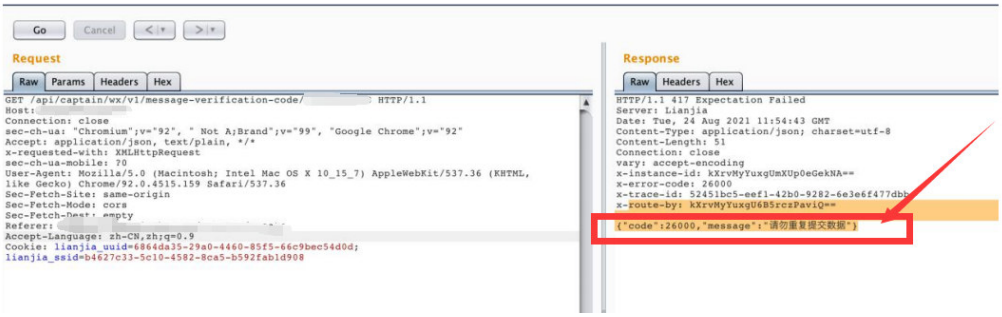
0x03：案例及绕过方式：

在测试过程发现有接收验证码的地方都可以进行测试，列入下方为某项目中的一点：

抓包

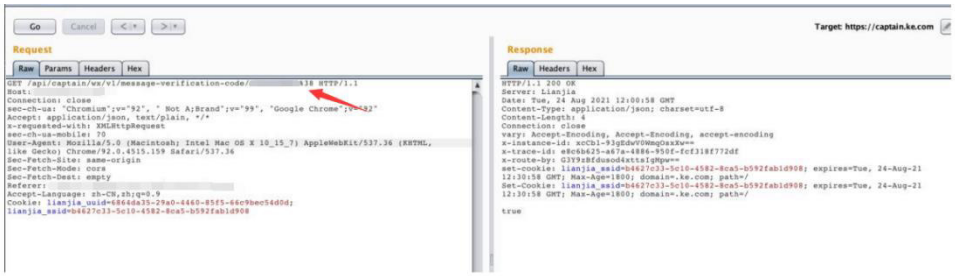
获取数据包后进行 re 模块重发，看看是否有防护，如果没有防护，直接并发测试完成轰炸即可：

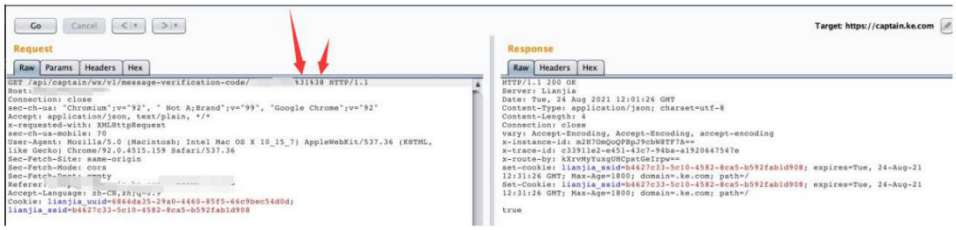
其实他这个是做了限制的，如果重复发送数据包的话会提示



如上图所示，此处是做了限制，这时候我们就要去思考如何绕过（当然这里可以去了解编码获取查看开发原理来进行绕过）

经过测试后，发现此处可以通过 url 编码来突破：





比如我的号码是 17699999999
我把 17 url 编码为%31%37699999999 就可以发送短信到我的手机号上面来
按照这个思路我把 176 编码也是可以的、把 1769 编码也是可以的、把电话号第一位和电话号第三位 url 编码也是可以的
就可以无限制发送短信到我的手机号上，当然也可以轰炸别人

总结：

手机号码前后加空格，86，086，0086，+86，0，00，/r,/n, 以及特殊符号等
修改 cookie，变量，返回
138888888889 12 位经过短信网关取前 11 位，导致短信轰炸
进行能解析的编码。