短信验证系列（四）

0x01:原理：

验证码与手机号未绑定

一般来说短信验证码仅能使用一次，验证码和手机号未绑定，验证码一段时期内有效，那么就可能出现如下情况：

1、A 手机的验证码，B 可以拿来用

2、A 手机在一定时间间隔内接到两个验证码，都可以用。

3、A 的手机号码，可以替换为 B 来接收验证码

0x02 测试

1、准备工具：

Burp 或者 f12 浏览器控制台。

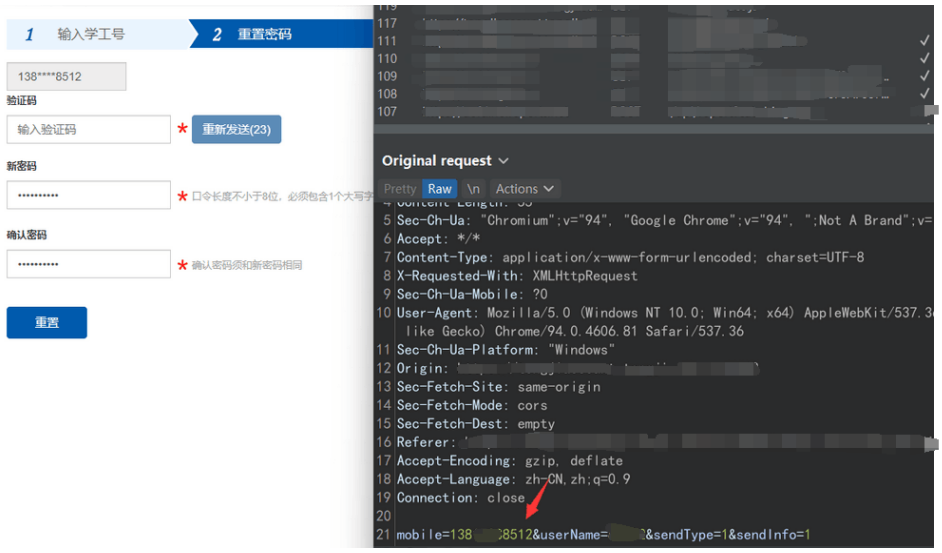
2、测试功能点：

短信验证码处

0x03 案例：

下面案例是某天的一个的项目，在学工主页的时候发现输入学生姓名和 xh 既可以重置密码，但是此时需要向学生用户发送一条短信，于是在发送后短信验证码后，在工作台查看

数据包可以发现我们能修改发送验证码的手机号：



可以发现 mobile 这个参数是我们可以控制的，于是我们将这个参数后面的手机号修改为自己的手机号：然后我的手机就出现下面的这张图

这样任意密码重置就到手了。

注：此类漏洞的挖掘可以多关注众测 补天 漏洞盒子这一类厂商。