### 短信验证码绕过漏洞

#### 0x01原理：

服务器端返回的相关[参数](https://so.csdn.net/so/search?q=%E5%8F%82%E6%95%B0&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/weixin_33778778/article/details/_blank)作为最终登录凭证，导致可绕过登录限制。

危害：在相关业务中危害也不同，如找回密码，注册，电话换绑等地方即可形成高危漏洞，如果是一些普通信息，个人信息修改的绕过就是中低危。

#### 0x02操作：

利用burp获取返回包（右键找到DO intercept) 修改即可：



测试方法：

先获取正确的验证码然后看看成功的返回包将其保存，然后再去输入错入的信息获取返回包，将正确的替换

#### 0x03案例

如下信息修改框，先获取正确的返回包。



然后输入错误的返回包，将正确的替换：



这里修改后，信息就自动保存成功。

最终获取赏金：50R

