短信验证码绕过漏洞

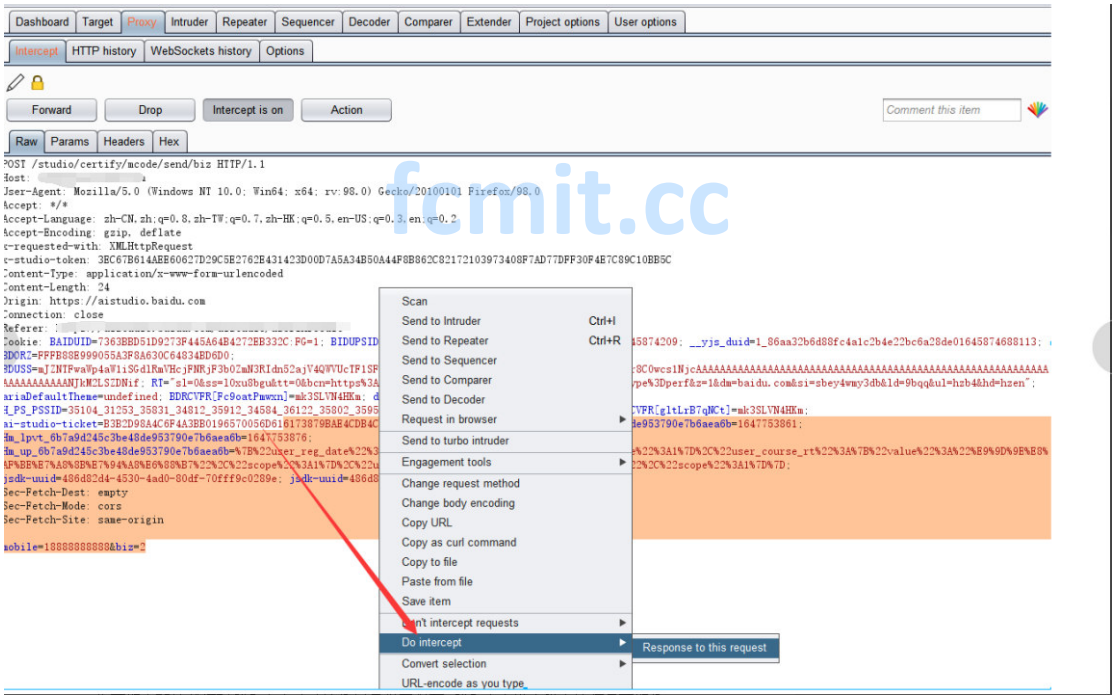
0x01 原理：

服务器端返回的相关参数作为最终登录凭证，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

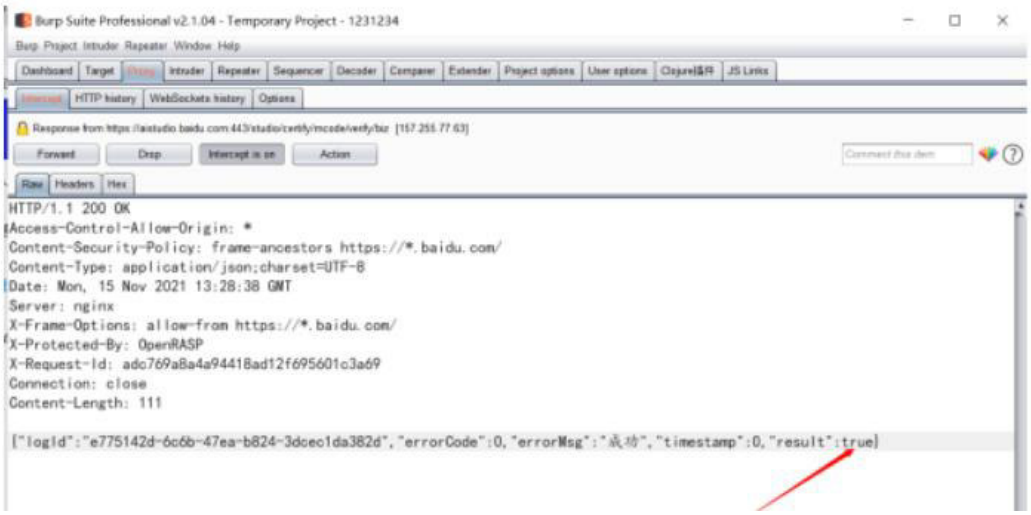
0x03 案例

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：

fcmit.cc

修改result的false为true



这里修改后，信息就自动保存成功。

最终获取赏金：50R


漏洞状态 待用户复查
漏洞ID
漏洞名称 信验证码绕过
参与活动
提交时间
危害自评 低危
审核等级 低危
励安全币 10
附件 --

fcmit.cc