### 账户管理类业务

#### 注册场景业务逻辑测试

**测试描述：**通过抓包工具分析注册场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**注册场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）username（可能为username、手机号、邮箱等）字段。

**用例一：**使用抓包工具代理模块拦截含有待注册用户名的报文，利用intruder模块结合用户名规则，对用户名进行枚举，查看能否枚举出其他用户的注册信息。

**测试预期：**如能通过报文返回内容判断出用户存在与否，则存在枚举用户名漏洞。

**用例二：**使用抓包工具代理模块拦截含有待注册用户名的报文，利用intruder模块对用户名进行枚举，查看能都否批量注册用户。

**测试预期：**如能成功批量注册用户，则存在批量注册漏洞。

**测试前置：**涉及的业务场景注册执行报文。

**用例一：**使用抓包工具代理模块获取执行注册的报文或流程，利用重放模块再次发送报文，查看能否重复注册同一个用户。

**测试预期：**如能重复注册一个用户，则存在重复注册漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成注册，则存在工作流程逃逸漏洞。

#### 注销场景业务逻辑测试

**测试描述：**通过抓包工具分析注销场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**注销场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证账户状态。

**测试预期：**如可注销受害人账户，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成注销，则存在工作流程逃逸漏洞。

#### 账户权限变更场景业务逻辑测试

**测试描述：**通过抓包工具分析账户权限变更场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**账户权限变更场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证账户权限。

**测试预期：**如可变更受害人账户权限，则存在水平越权漏洞。

测试前置：涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成账户权限变更，则存在工作流程逃逸漏洞。

#### 账户暂停/恢复场景业务逻辑测试

**测试描述：**通过抓包工具分析账户暂停/恢复场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**账户暂停/恢复场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证账户状态。

**测试预期：**如可暂停或恢复受害人账户，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**：如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成还在账户暂停/恢复业务，则存在工作流程逃逸漏洞。

### 密码管理类业务

#### 密码修改场景业务逻辑测试

**测试描述：**通过抓包工具分析密码修改场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**密码修改场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及涉及的业务场景，获取from表单中，input标签为password属性的字段

**用例一：**通过抓包工具的代理模块抓包，查看密码字段信息是否为明文，如果加密，则验证是否为常见弱加密方式（如base64编码、URL编码等）。

**测试预期：**如上送报文中密码字段为明文，则存在密码字段未使用字段级加密漏洞；若上送报文中密码字段为常见弱加密方式，则存在密码字段加密强度不足漏洞。

**用例二：**若原密码字段未限制错误次数，同在存在密码字段未使用字段级加密漏洞/加密强度不足漏洞，或可以使用其他方式构造自动化脚本破解密码字段加密内容的情况，测试人员使用抓包工具的intruder模块或定制脚本利用标准弱密码字典进行爆破。对于内网测试环境，应调整表标准弱密码的顺序，将正确的密码置于爆破次序的后50%

**测试预期：**如可执行爆破流程且获取正确的密码，则存在弱密码爆破漏洞

**用例三：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成密码修改业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证密码修改情况。

**测试预期：**如可修改受害人密码，则存在水平越权漏洞。

#### 密码找回场景业务逻辑测试

**测试描述：**通过抓包工具分析密码找回场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及认证要素，则参考对应的认证要素测试方式。

**测试标签：**WEB应用安全测试

**业务场景：**密码找回场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，涉及涉及的业务场景，获取from表单中，input标签为password属性的字段。

**用例一：**通过抓包工具的代理模块抓包，查看密码字段信息是否为明文，如果加密，则验证是否为常见弱加密方式（如base64编码、URL编码等）。

**测试预期：**如上送报文中密码字段为明文，则存在密码字段未使用字段级加密漏洞；若上送报文中密码字段为常见弱加密方式，则存在密码字段加密强度不足漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证密码修改情况。

**测试预期：**如可修改受害人密码，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**：如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成密码找回业务，则存在工作流程逃逸漏洞。

### 信息查询及维护类业务

#### 信息查询场景业务逻辑测试

**测试描述：**通过抓包工具分析信息查询场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞

**测试标签：**WEB应用安全测试

**业务场景：**信息查询场景（包括但不限于客户信息查询和金融交易信息查询）

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、卡号、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证能否查询受害人交易信息。

**测试预期：**如可查询查询受害人的信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为高权限受害人的身份标识，验证能否查询受害人交易信息。

**测试预期：**如可查询查询受害人的信息，则存在垂直越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证能否查询受害人业务信息。

**测试预期：**如可查询受害人的业务信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为高权限受害人的业务标识，验证能否查询受害人交易信息。

**测试预期：**如可查询受害人的业务信息，则存在垂直越权漏洞。

#### 信息修改场景业务逻辑测试

**测试描述：**通过抓包工具分析信息修改场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞

**测试标签：**WEB应用安全测试

**业务场景：**涉及客户信息修改和金融交易修改的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证查询/修改的信息归属。

**测试预期：**如可查询/修改归属受害人的信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为高权限受害人的身份标识，验证查询/修改的信息归属。

**测试预期：**如可查询/修改归属受害人的信息，则存在垂直越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证能否查询/修改受害人业务信息。

**测试预期：**如可查询/修改受害人的业务信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为高权限受害人的业务标识，验证能否查询/修改受害人交易信息。

**测试预期：**如可查询/修改受害人的业务信息，则存在垂直越权漏洞。

#### 信息导出/下载场景业务逻辑测试

**测试描述：**通过抓包工具分析信息导出/下载场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞

**测试标签：**WEB应用安全测试

**业务场景：**涉及客户信息修改和金融交易信息导出/下载的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、卡号、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证查询/导出/下载的信息归属。

**测试预期：**如可查询/导出/下载归属受害人的信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为高权限受害人的身份标识，验证查询/导出/下载的信息归属。

**测试预期：**如可查询/导出/下载归属受害人的信息，则存在垂直越权漏洞。

**用例三：**通过抓包工具的代理模块抓包，查看有关文件名、文件编号的字段是否为明文，如果是明文，则将其修改为其他平行用户的文件名、文件编号的信息；如果加密，则验证是否为常见弱加密方式（如base64编码、URL编码等），如果是，则解密后再次进行如上操作替换字段。

**测试预期：**如上替换文件名、文件编号的信息后，可导出/下载其他用户的用户信息文件，则存在任意文件下载漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证能否查询/导出/下载受害人业务信息。

**测试预期：**如可查询/导出/下载受害人的业务信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为高权限受害人的业务标识，验证能否查询/导出/下载受害人交易信息。

**测试预期：**如可查询/导出/下载受害人的业务信息，则存在垂直越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）下载路径字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改下载路径字段为系统敏感文件路径（如/etc/passwd），验证能否下载目标文件。

**测试预期：**如可下载目标文件，则存在任意文件下载漏洞

#### 信息删除场景业务逻辑测试

**测试描述：**通过抓包工具分析信息删除场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞

**测试标签：**WEB应用安全测试

**业务场景：**涉及客户信息修改和金融交易删除的业务场景

**测试工具**：抓包工具

**测试用例**：

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证查询/删除的信息归属。

测试预期：如可查询/删除归属受害人的信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为高权限受害人的身份标识，验证查询/删除的信息归属。

**测试预期：**如可查询/删除归属受害人的信息，则存在垂直越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证能否查询/删除受害人业务信息。

**测试预期：**如可查询/删除受害人的业务信息，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为高权限受害人的业务标识，验证能否查询/删除受害人交易信息。

**测试预期：**如可查询/删除受害人的业务信息，则存在垂直越权漏洞

### 金融交易类业务

#### 支付场景业务逻辑测试

**测试描述：**通过抓包工具分析支付场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节。

**测试标签：**WEB应用安全测试

**业务场景：**涉及支付的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关cardid、电子账户等支付来源或支付接收字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改支付来源卡号、电子账户为受害人信息，验证能否支付成功。

**测试预期：**如可用受害人的卡号、电子账号支付成功，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改支付接收卡号、电子账户为攻击人信息，验证能否成功接受

**测试预期：**如可支付成功，则存在参数篡改漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成支付流程。

**测试预期**：如可用篡改后的数据完成业务流程支付成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成支付流程。

**测试预期：**如可用篡改后的数据完成业务流程支付成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关支付结果的标志位字段。

**用例一：**支付失败的情况下，通过抓包工具的代理模块拦截报文，篡改支付结果为成功，验证能否完成支付流程。

**测试预期：**如可支付成功，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成支付业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，执行支付的报文。

**用例一：**通过抓包工具的代理模块获取流程中执行支付的报文，使用抓包工具的重放模块重复发送报文，验证重放报文实现支付成功。

**测试预期：**如重放报文能完成支付业务，则存在重放漏洞。

#### 转账场景业务逻辑测试

**测试描述：**通过抓包工具分析转账场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节。

**测试标签：**WEB应用安全测试

**业务场景：**涉及转账的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关转账金额等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成支付流程。

测试预期：如可用篡改后的数据完成业务流程支付成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关cardid、电子账户等转账来源或转账接收字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改转账来源卡号、电子账户为受害人信息，验证能否转账成功。

**测试预期：**如可用受害人的卡号、电子账号转账成功，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改支付接收卡号、电子账户为攻击人信息，验证能否转账接受。

**测试预期：**如可转账成功，则存在参数篡改漏洞。

**测试前置：**涉及的业务场景，执行转账的报文。

**用例一：**通过抓包工具的代理模块获取流程中执行转账的报文，使用抓包工具的重放模块重复发送报文，验证重放报文实现转账成功。

**测试预期：**如重放报文能完成转账业务，则存在重放漏洞。

**用例二：**通过抓包工具的代理模块拦截流程中执行转账的报文，使用抓包工具的intruder模块多线程发送报文，验证转账是否成功。

**测试预期：**如执行多笔转账但只扣款一次，则存在多线程竞争漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

#### 充值缴费场景业务逻辑测试

**测试描述：**通过抓包工具分析充值缴费场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节。

**测试标签：**WEB应用安全测试

**业务场景：**涉及充值缴费类交易的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关充值金额等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成充值缴费流程。

**测试预期：**如可用篡改后的数据完成业务流程充值缴费成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、卡号、手机号等标识缴费资金来源的字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改标识缴费资金来源的字段为受害人信息，验证能否充值/缴费成功。

**测试预期：**如可用受害人账户充值缴费成功，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

测试前置：涉及的业务场景，执行充值/缴费的报文。

**用例一：**通过抓包工具的代理模块获取流程中执行转账的报文，使用抓包工具的重放模块重复发送报文，验证重放报文能否充值/缴费成功。

**测试预期：**如重放报文能完成充值缴费业务，则存在重放漏洞。

**用例二：**通过抓包工具的代理模块拦截流程中执行转账的报文，使用抓包工具的intruder模块多线程发送报文，验证充值缴费是否成功。

**测试预期：**如执行此充值缴费转账但只扣款一次，则存在多线程竞争漏洞。

#### 非金融产品购买场景业务逻辑测试

**测试描述：**通过抓包工具分析非金融产品购买场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。

若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试。

若场景涉及优惠活动/券/积分使用，对应功能部分请参考x.x.x.x章节逐条进行测试。

若场景涉及支付功能，对应功能部分请参考x.x.x.x章节逐条进行测试。

**测试标签：**WEB应用安全测试

**业务场景：**主要是在购买限量商品、领取优惠卷、积分进行购买支付的业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量、运费等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成购买流程。

测试预期：如可用篡改后的数据完成业务流程购买成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关购买结果的标志位字段。

**用例一：**购买失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文的响应结果为成功，验证能否完成购买业务或生成购买订单。

**测试预期：**如可完成购买业务或生成购买订单，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，执行购买的报文。

**用例一：**通过抓包工具的代理模块获取流程中执行购买的报文，使用抓包工具的重放模块重复发送报文，验证重放报文能否购买成功。

**测试预期：**如重放报文能完成购买业务，则存在重放漏洞。

#### 非金融订单取消场景业务逻辑测试

**测试描述：**通过抓包工具分析非金融订单取消业务场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节。

**测试标签：**WEB应用安全测试

**业务场景：**涉及订单取消业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单号、username、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为受害人信息，验证查询/取消受害人订单。

**测试预期：**如可查询/取消受害人订单，则存在水平越权漏洞

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单取消结果的标志位字段**。**

**用例一：**取消订单失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文的响应结果为成功，验证能否完成订单取消。

**测试预期：**如可完成订单取消，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一**：通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、积分、运费、优惠券等购买时消耗的资源的字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改金额、积分、运费优惠券等购买时消耗的资源的字段为任意其他数值（包括合法数值与非法数值）并提交，验证订单取消后能否返还篡改后的金额、积分、运费、优惠券等。

**测试预期：**如订单取消后能返还篡改后的金额、积分、运费、优惠券等，则存在参数篡改类漏洞

#### 非金融产品退货/退款场景业务逻辑测试

**测试描述：**通过抓包工具分析非金融产品退货/退款场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及非金融产品退货/退款场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单号、用户名、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为受害人信息，验证能否查询或对受害人订单发起退货/退款。

**测试预期：**如能查询到受害人订单或对受害人订单发起退货/退款，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关退货/退款结果的标志位字段。

**用例一：**退货退款失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文的响应结果为成功，验证能否完成退货退款。

**测试预期：**如可完成退货退款，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、积分、运费、优惠券等购买时消耗的资源的字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改金额、积分、运费优惠券等购买时消耗的资源的字段为任意其他数值（包括合法数值与非法数值）并提交，验证退货退款后能否返还篡改后的金额、积分、运费、优惠券等。

**测试预期：**如退货退款后能返还篡改后的金额、积分、运费、优惠券等，则存在参数篡改类漏洞。

#### 金融产品购买场景业务逻辑测试

**测试描述：**通过抓包工具分析金融产品购买场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融产品购买业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量、利率、汇率等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成购买流程。

**测试预期：**如可用篡改后的数据完成业务流程购买成功，则存在参数篡改类漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关购买结果的标志位字段。

**用例一：**购买失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文的响应结果为成功，验证能否完成购买业务或生成购买订单。

**测试预期：**如可完成购买业务或生成购买订单，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，执行购买的报文。

**用例一：**通过抓包工具的代理模块获取流程中执行购买的报文，使用抓包工具的重放模块重复发送报文，验证重放报文能否购买成功。

**测试预期：**如重放报文能完成购买业务，则存在重放漏洞。

#### 金融产品赎回场景业务逻辑测试

**测试描述：**通过抓包工具分析金融产品赎回场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融产品赎回场景业务

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及金融产品赎回场景业务场景

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为受害人信息，验证能否查询或对受害人金融产品发起赎回。

**测试预期：**如能查询到受害人订单或对受害人订单发起退货/退款，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改表面赎回渠道的业务标识字段为攻击人信息，验证能否赎回金融产品至攻击人账户。

**测试预期：**如能赎回金融产品至攻击人账户，则存在水平越权漏洞。

**用例三：**赎回失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文有关赎回结果的标志位字段响结果为成功，验证能否完成赎回业务。

**测试预期：**如可完成赎回，则存在工作流程逃逸漏洞。

**用例四：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量、利率、汇率等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成赎回流程。

**测试预期：**如可用篡改后的数据完成赎回，则存在参数篡改类漏洞。

#### 金融产品订单取消场景业务逻辑测试

**测试描述：**通过抓包工具分析金金融产品订单取消场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试对应的测试前置逐条进行测试，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融产品订单取消业务场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单号、交易号、cardid号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为受害人信息，验证能否查询或对受害人金融产品发起赎回。

**测试预期：**如能查询到受害人订单或对受害人订单发起取消，则存在水平越权漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，篡改表明资金退回渠道的业务标识字段为攻击人信息，验证能否取消的金融产品资金返还至攻击人账户。

**测试预期：**如能将取消的金融产品资金返还至攻击人账户，则存在水平越权漏洞

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单号、username、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为受害人信息，验证查询/取消受害人订单。

**测试预期：**如可查询/取消受害人订单，则存在水平越权漏洞

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关订单取消结果的标志位字段。

**用例一：**取消订单失败的情况下，通过抓包工具的代理模块拦截报文，篡改报文的响应结果为成功，验证能否完成订单取消。

**测试预期：**如可完成订单取消，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成转账业务，则存在工作流程逃逸漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关金额、商品数量、利率、汇率等数值型字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改数值型字段为任意其他数值（包括合法数值与非法数值）并提交，验证能否以篡改后数值完成取消流程。

**测试预期：**如可用篡改后的数据完成取消，则存在参数篡改类漏洞。

### 金融交易关联类业务

#### 业务开立场景业务逻辑测试

**测试描述：**通过抓包工具分析业务开立场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若该场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试方式，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融业务开立场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、身份证号、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证业务开立情况。

**测试预期：**如可执行受害人的开立业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成业务开立，则存在工作流程逃逸漏洞。

#### 业务变更场景业务逻辑测试

**测试描述：**通过抓包工具分析业务变更场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若该场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试方式，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融业务变更场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证业务变更情况。

**测试预期：**如可变更受害人业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、身份证号、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证业务变更情况。

**测试预期：**如可变更受害人业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成业务变更，则存在工作流程逃逸漏洞。

#### 业务解约/中止场景业务逻辑测试

**测试描述：**通过抓包工具分析业务解约/中止场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若该场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试方式，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融业解约/中止务变更场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证业务解约/中止情况。

**测试预期：**如可解约/中止受害人业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、身份证号、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证业务解约/中止情况。

**测试预期：**如可解约/中止受害人业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段**。**

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成业务解约/中止，则存在工作流程逃逸漏洞。

#### 审批审核场景业务逻辑测试

**测试描述：**通过抓包工具分析业务审批/审核场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。若该场景涉及人脸、证书、短信验证码等认证要素，请参考对应的认证要素测试方式，详见x.x.x章节

**测试标签：**WEB应用安全测试

**业务场景：**涉及金融业务审批/审核场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关交易号、流水号、商品编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为同权限受害人的业务标识，验证业务解约/中止情况。

**测试预期：**如可审批/审核受害人业务，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关username、cardid、phone等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证业务解约/中止情况。

**测试预期：**如可审批/审核受害人业务，则存在水平越权漏洞。

测试前置：涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终完成审批/审核业务，则存在工作流程逃逸漏洞。

#### 优惠活动/券/积分获取场景业务逻辑测试

**测试描述：**通过抓包工具分析优惠活动/券/积分获取场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。

**测试标签：**WEB应用安全测试

**业务场景：**涉及优惠活动/券/积分获取场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关地区编号、数量、时间、参与次数等限制字段。

**用例一：**通过抓包工具的代理模块抓包，修改有关地区编号的字段为其他地区编号，如将010（北京）修改022（天津），验证能否绕过区域限制参与优惠活动/券/积分获取。

**测试预期：**如可参加其他地区的优惠活动/券/积分获取，则存在工作流逃逸漏洞。

**用例二：**通过抓包工具的代理模块拦截报文，修改有关获取数量或数量限制字段，验证能否超额领取券/积分。

**测试预期：**如可超额领取券/积分，则存在工作流逃逸漏洞。

**用例三：**参与不在有效期内的活动/券/积分获取，通过抓包工具的代理模块拦截报文，修改有关活动时间或当前时间的字段，验证能否参加活动/券/积分获取。

**测试预期：**如可参加本来不能参加的优惠活动/券/积分获取，则存在工作流逃逸漏洞。

**用例四：**参与已超出参与次数的活动/券/积分获取，通过抓包工具的代理模块拦截报文，篡改已参加过活动的标志或参与次数字段，验证能否参与活动/券/积分获取。

**测试预期：**如可成功参加优惠活动/券/积分获取，则存在工作流逃逸漏洞。

**测试前置：**涉及的业务场景中，获取券/积分的报文。

**用例一：**通过抓包工具代理模块拦截获取券/积分的报文，利用抓包工具重放模块重复多次发送报文，验证券/积分领取情况。

**测试预期：**如可突破业务限制多次领取券/积分，则存在重放漏洞。

#### 优惠活动/券/积分使用场景业务逻辑测试

**测试描述：**通过抓包工具分析优惠活动/券/积分使用场景的接口内容及工作流程，逐条实施案例验证是否存在业务逻辑漏洞。

**测试标签：**WEB应用安全测试

**业务场景：**涉及优惠活动/券/积分使用场景

**测试工具：**抓包工具

**测试用例：**

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关用户名、卡号、手机号等用户身份标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改用户身份标识字段为同权限受害人的身份标识，验证能否查询或使用他人优惠活动/券/积分。

**测试预期：**如可查询/使用受害人的优惠活动/券/积分，则存在水平越权漏洞

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关活动号、券编号等业务标识字段。

**用例一：**通过抓包工具的代理模块拦截报文，篡改业务标识字段为不具有业务权限的业务标识，验证能否正常使用活动/券。

**测试预期：**如可正常使用活动/券，则存在水平越权漏洞。

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）有关有关地区编号、数量、时间、参与次数等使用限制字段。

**用例一：**通过抓包工具的代理模块抓包，修改有关地区编号的字段为其他地区编号，如将010（北京）修改022（天津），验证能否绕过区域限制使用优惠活动/券/积分。

**测试预期：**如可绕过地区限制，使用优惠活动/券/积分，则存在工作流逃逸漏洞。

**用例二：**使用不在有效期内的活动/券/积分，通过抓包工具的代理模块拦截报文，修改有关活动时间或当前时间的字段，验证能否使用活动/券/积分。

**测试预期：**如可使用超期的优惠活动/券/积分，则存在工作流逃逸漏洞。

**用例三：**通过抓包工具的代理模块拦截报文，修改有关剩余数量（如优惠券剩余数量，积分剩余数量）或使用数量（如使用的优惠券数量，积分数量，积分抵扣百分比限制等）字段，验证能否超额使用优惠活动/券/积分。

**测试预期：**如可超额使用优惠活动/券/积分，则存在工作流逃逸漏洞

**测试前置：**涉及的业务场景，包括但不限于HTTP或https数据包中（header、get、post body等区域）控制流程分支的字段。

**用例一：**通过抓包工具的代理模块截断流程中的上送报文或响应报文，篡改报文中控制流程分支的字段，或直接构造业务最终执行的报文，提交报文并验证业务流程。

**测试预期：**：如可略过业务设置中不允许略过的业务流程或进入与用户权限不相符的业务流程，并最终优惠活动/券/积分使用，则存在工作流程逃逸漏洞。