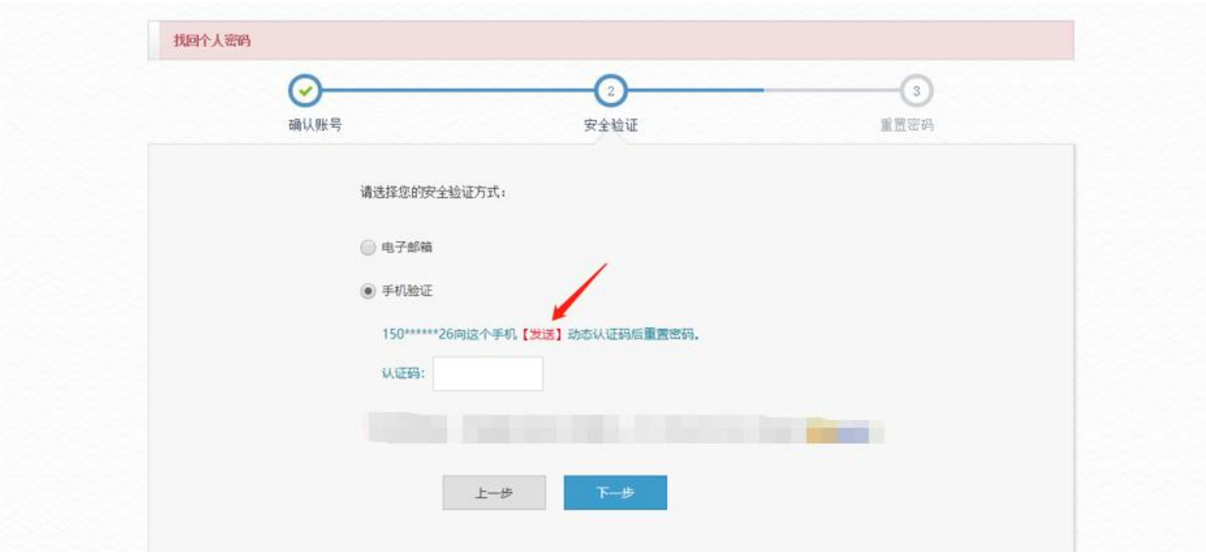
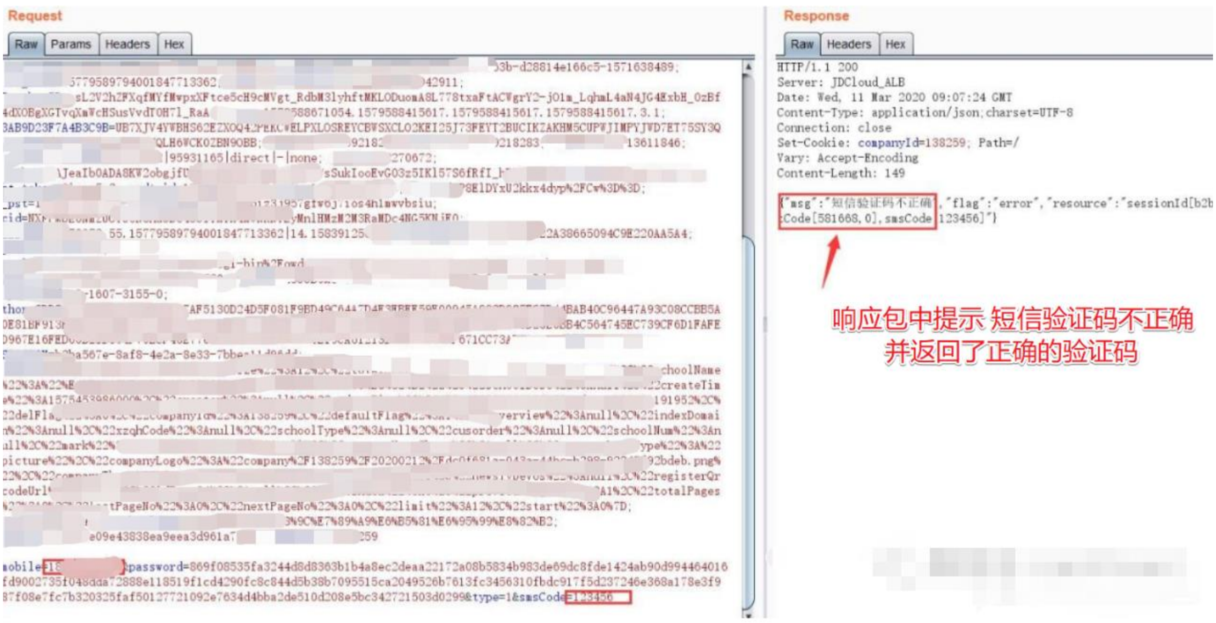
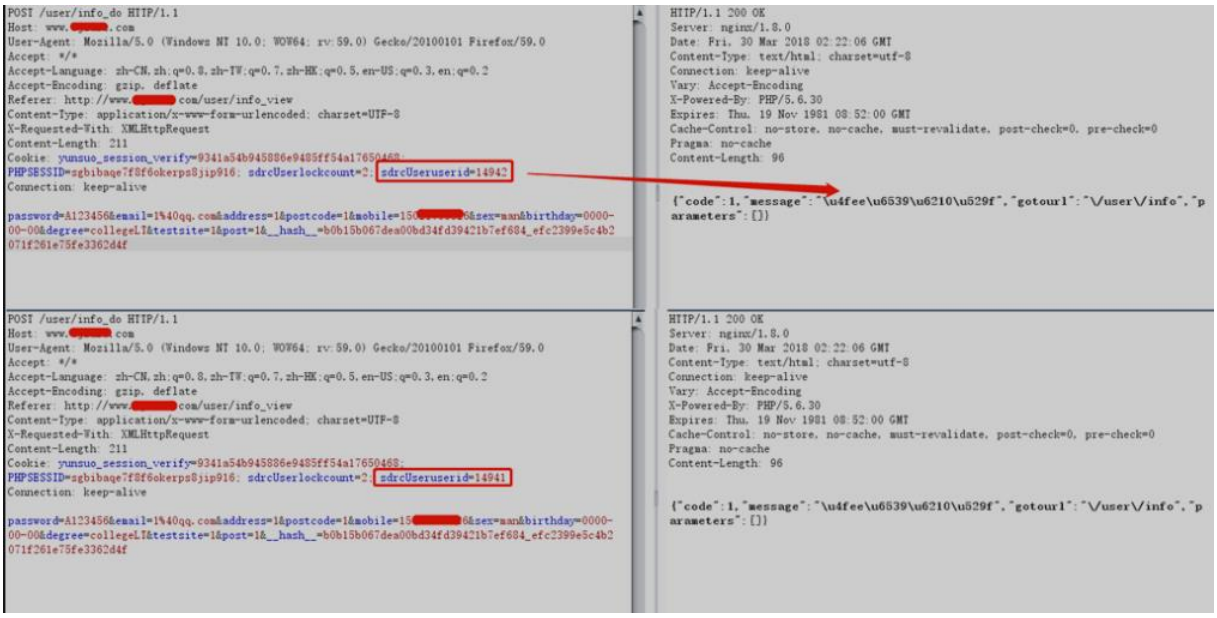
短信验证码回传显示


找回个人密码
确认账号
安全验证
重置密码
请选择您的安全验证方式：
电子邮箱
手机验证
150******26向这个手机【发送】动态认证码后重置密码。
认证码：
上一步
下一步

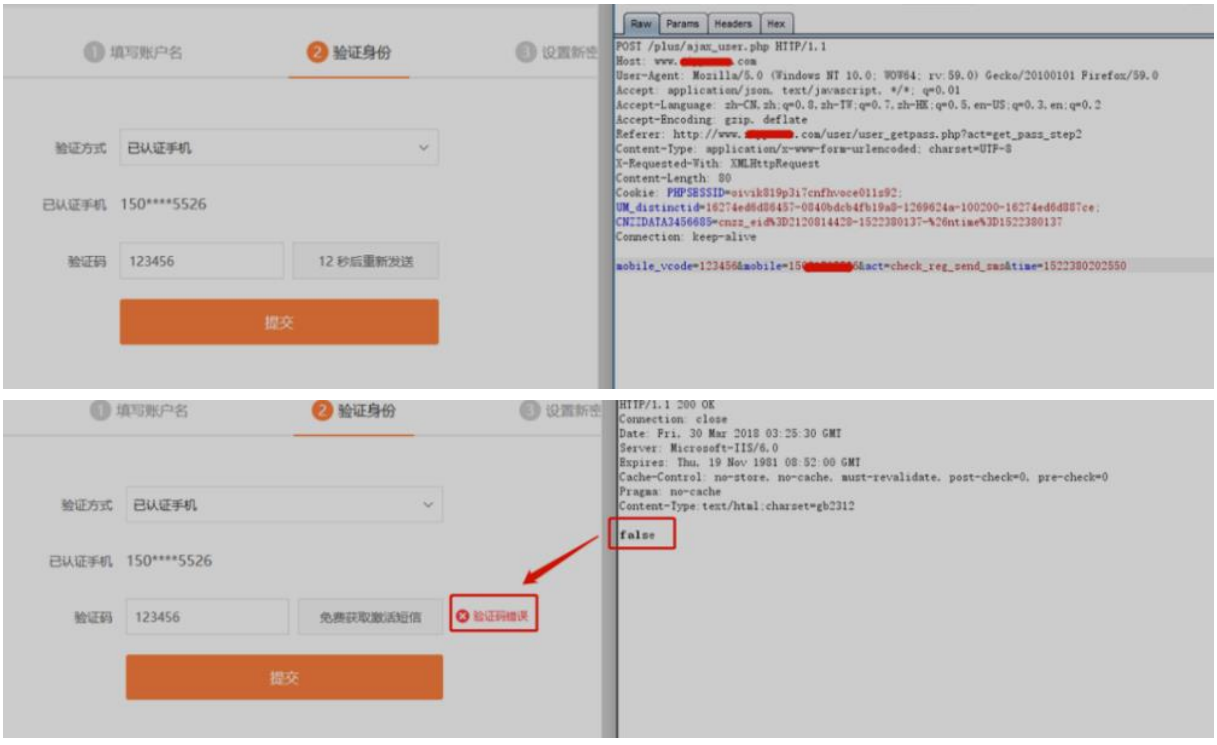

HTTP/1.1 200 OK
DrivedBy: RaySrv RayEng/1.5.0
Date: Thu, 05 Apr 2018 06:26:12 GMT
Content-Type: application/json
Connection: keep-alive
X-Powered-By: Servlet/2.5 JSP/2.1
Content-Length: 816

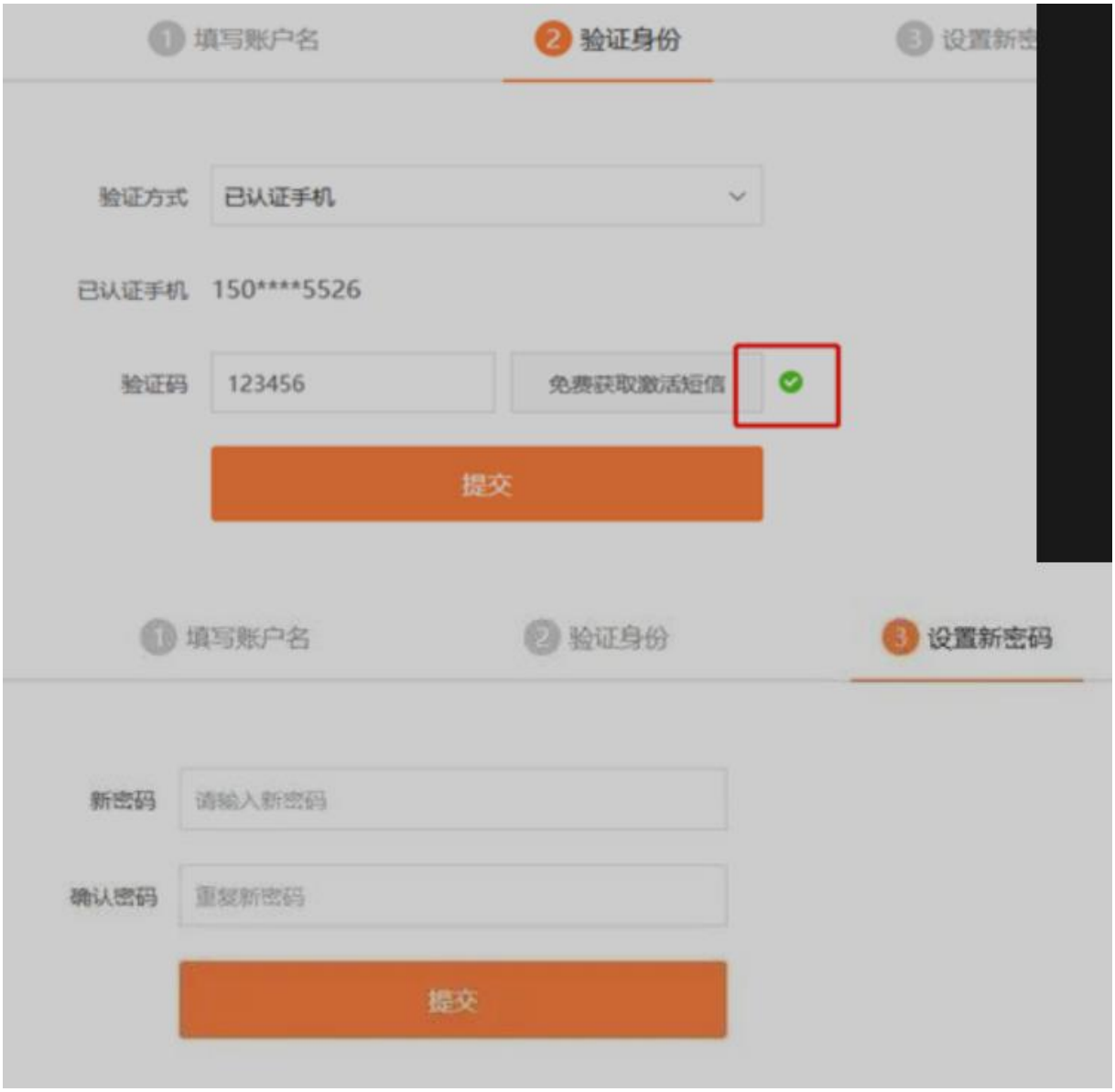

Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex
HTTP/1.1 200
Server: JDCloud_ALB
Date: Wed, 11 Mar 2020 09:07:24 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 149
响应包中提示 短信验证码不正确
并返回了正确的验证码

修改用户对象重置任意用户



修改响应包重置任意用户





未验证导致重置任意用户

最终只需要修改 r 为其他用户 ID，即可重置其他用户密码。

某 SRC 重定向验证邮箱绕过

https://mp.weixin.qq.com/s/zsHHSXZHaLmiJFkgsjoHKg

某 SRC 配合信息泄漏重置绕过

记一次简单的 src 挖掘 - 先知社区 (aliyun.com)