

短信验证码回传显示

找回密码

1

2

3

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

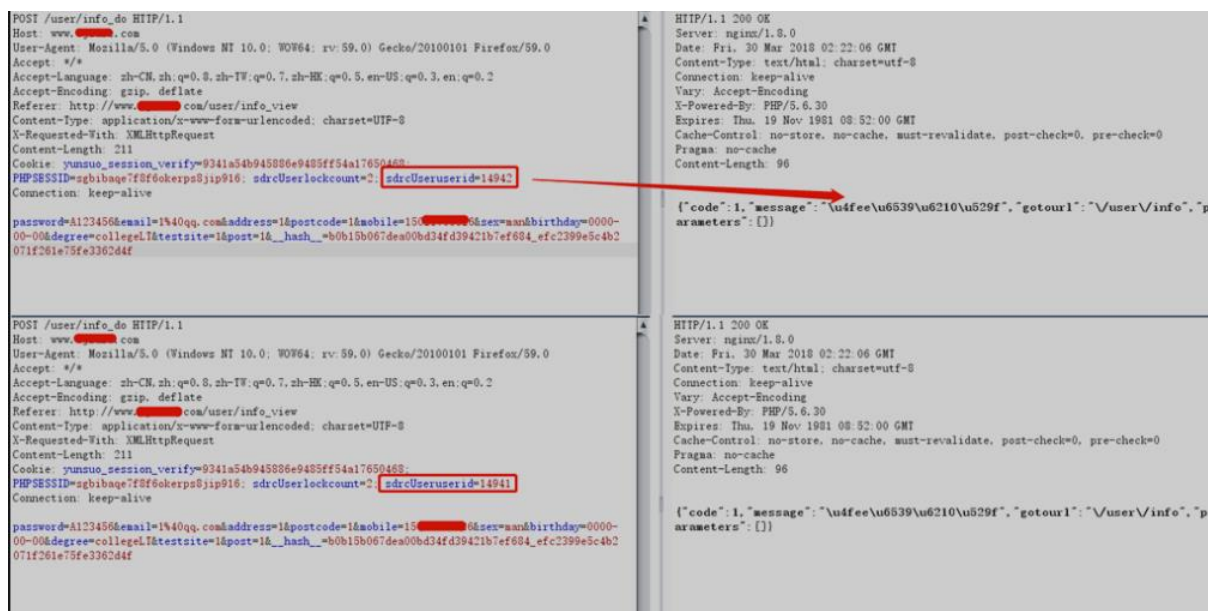
```

HTTP/1.1 200 OK
DrivenBy: 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

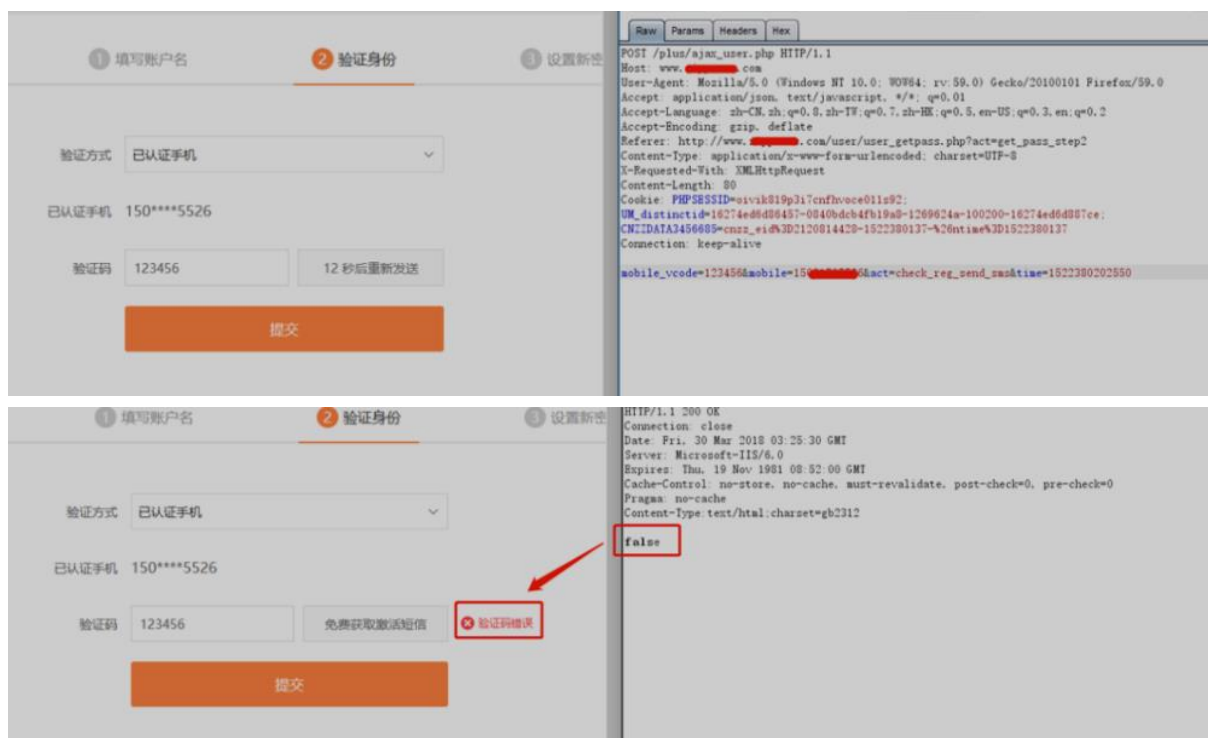
{"view":null,"model":{"id":"1","process":"pd":{"createTime":"2018-04-05
14:35:45","phone":"[REDACTED]","SYSNAME":"錫瑋偉派烘埤鐫鈔金錫康約便$想維萃犖","username":"[REDACTED]","SENDTIME":"20180405143544","
op":"gr","smsCode":"650302","UUID":"e556de5596de4ec095242679c8926b3e","LOGINNAME":"[REDACTED]","returnmsg":"0.201804051427342516977
0663.0.1.0.錫悒氣鎧週姍","type":"1","mobile":"[REDACTED]","viewName":null,"modelmap":{"msg":{"success":"2018
-04-05
14:35:45","phone":"[REDACTED]","SYSNAME":"錫瑋偉派烘埤鐫鈔金錫康約便$想維萃犖","username":"[REDACTED]","SENDTIME":"20180405143544","
op":"gr","smsCode":"650302","UUID":"e556de5596de4ec095242679c8926b3e","LOGINNAME":"[REDACTED]","returnmsg":"0.201804051427342516977
0663.0.1.0.錫悒氣鎧週姍","type":"1","mobile":"[REDACTED]"},"empty":false,"reference":false}}}}

```

修改用户对象重置任意用户



修改响应包重置任意用户



1 填写账户名 2 验证身份 3 设置新密码

验证方式 已认证手机

已认证手机 150****5526

验证码 123456 免费获取激活短信

提交

1 填写账户名 2 验证身份 3 设置新密码

新密码 请输入新密码

确认密码 重复新密码

提交

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 \(aliyun.com\)](#)