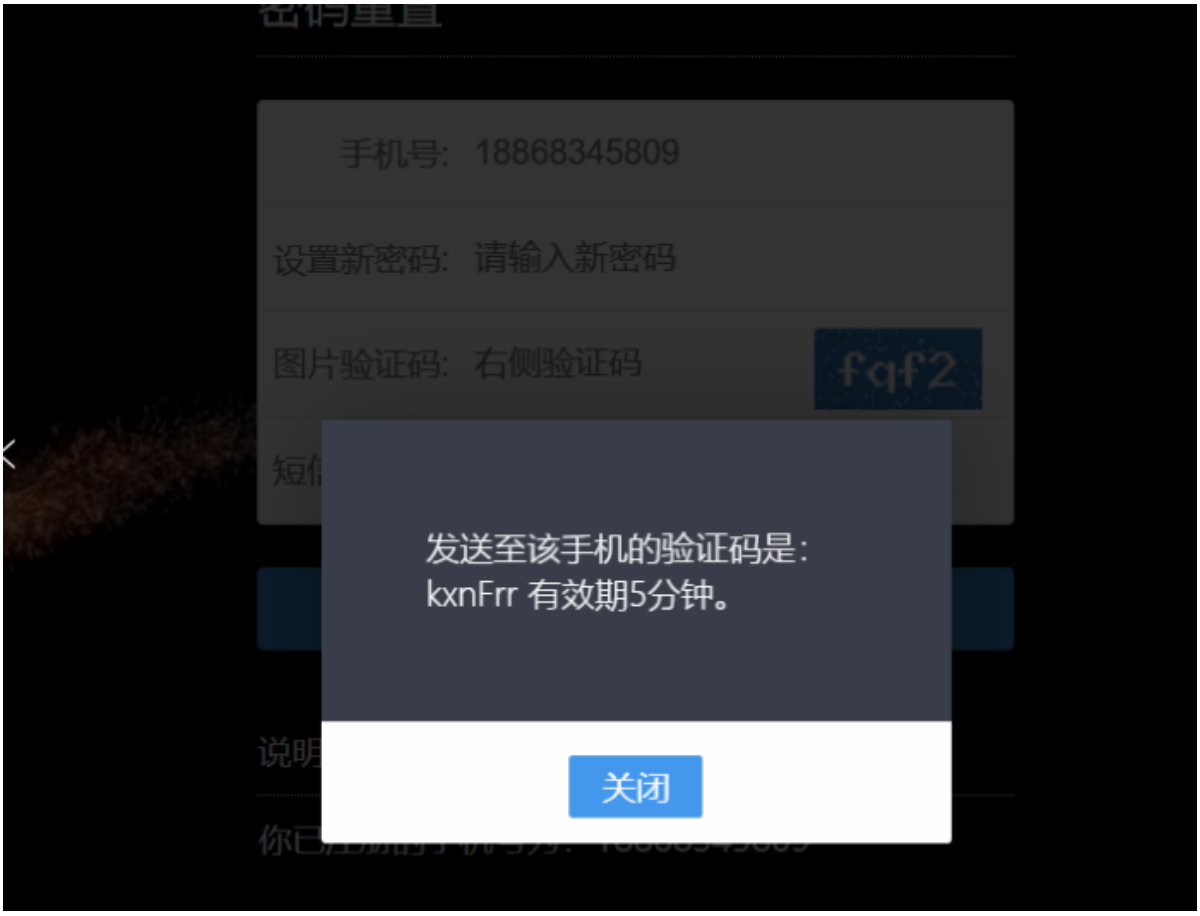
Day35　WEB漏洞–逻辑越权之找回机制及接口爆破

35.1 密码重置-验证码套用

```
https://www.mozhe.cn/bug/detail/K2sxTTVYaWNncUE1cTdyNXIyTklHdz09bW96aGUmozhe
```

正常情况下，手机验证是第一个页面输入手机号，验证码，第二个页面重置密码，而该题目中，手机验证码和重置密码在同一个地方，步骤：先用要重置密码的手机获取验证码（验证码得不到，不用管）

然后用已经注册的且在身边的手机号获得验证码输入:

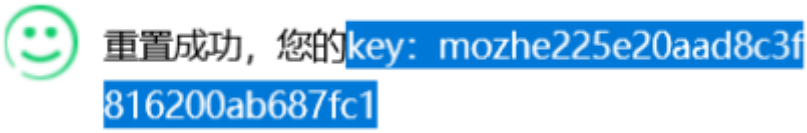


然后抓包，将之前那个号码换成要重置密码的手机号:

```
Connection: close
Referer: http://219.153.49.228:49081/password_reset.php
Cookie: PHPSESSID=la682nl2rpq9be37rk54isn167

mobile=17101304128&pwd=123456&v_code=gvkv&s_code=a
```

成功获得flag:




```
1  原理分析
2  *其短信验证码5分钟内有效，只验证验证码的有效性，而没有验证验证码和手机号的一致性。所以可以越权重置。未验证短信验证码与手机的匹配关系（却验证了短信验证码与图片验证码）。
3  *服务器端应该是只检查是否发送过验证码，但未验证验证码与手机号的匹配关系，导致任意账号重置
4  *正常的验证
5  ---界面1：输入手机号码，验证码（验证手机和验证码匹配）；界面2：重置密码
6  ---这里是2步连在一起，就没考虑操作对象更改的问题
```

35.2 找回重置机制

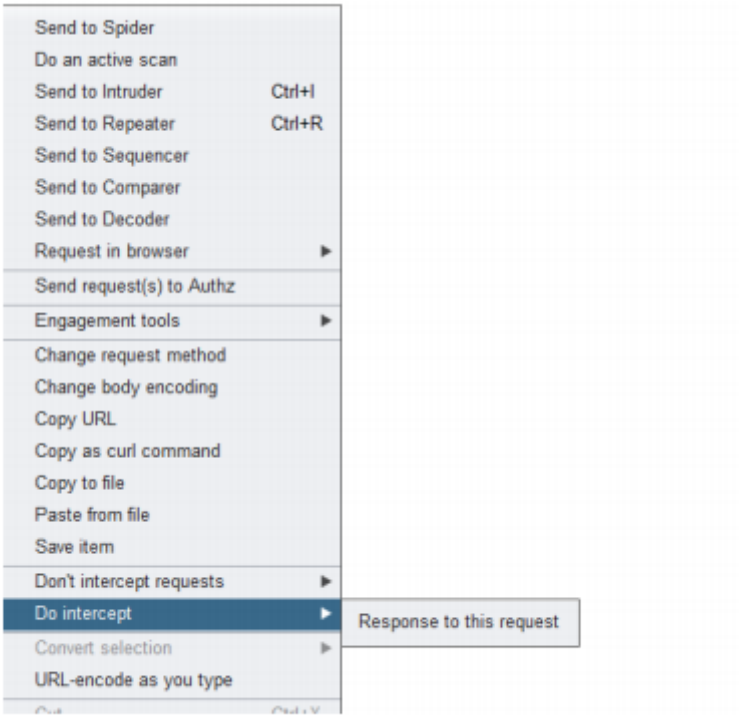
35.2.1客户端回显

在发送验证码的过程中，验证码直接在数据包中显示。验证码在客户端的浏览器或数据包中可以看到。

35.2.2 Response状态值

手机邮箱验证码逻辑-客户端回显-实例抓包，在数据包里面，直接可以看到验证码随便输一个验证码，抓包，之后全程接管，将状态码进行更改，例如将3改为1，以当前的回复值修改就有意义，若是以服务器来验证的话，就不行。

页面通过该值返回输入的验证码的对错，可以修改数据包中的值，有回复的状态值如0/1，我们可以更改状态值来实现绕过



35.2.3 验证码爆破

如果验证码范围不大，验证码有效时间足够，没有次数限制，则可以尝试（下一章介绍）

35.2.4 找回流程绕过

发送验证码-验证-重置密码，绕过验证码验证，直接请求下一步（找回成功后会跳转到另外一个页面，先通过一个正常用户去获取跳转的URL和数据包，再换一个用户去访问第三步（跳过验证 ）

35.3 接口调用乱用

原理：网站注册等等会有验证码，就有一个专门发验证码的接口，恶意的将这些网站的接口收集到一起，用程序批量的循环发送

资源：

```
1  http://downcode.com/downcode/j_16621.shtml
   https://pan.baidu.com/s/1P73QFmEhY6f350CvmnOJNg 提取码：xiao
   https://pan.baidu.com/s/1N963jFjTefNc6Gnso-RHmw 提取码：xiao
   https://www.mozhe.cn/bug/detail/K2sxTTVYaWNncUE1cTdyNXIyTklHdz09bW96aGUmozhe
```