Hillstone
山 石 网 科

山石网科安全服务事业部

健康管理中心

渗透测试报告

山石安服 以人为本
36.7℃贴心安全服务

目录

■ **版本编号** V1.0　　■ **密级** 商业机密

■ **版本变更记录**

时间	版本	说明	修改人
2025.03.05	V0.1	报告起稿	张炜
2025.03.05	V0.2	报告填充	张炜
2025.03.05	V1.0	报告审核	戴恩军

■ **版权声明**

■ **适用性声明**

本文档为北京山石网科信息技术有限公司（以下简称“山石网科”）在日照市人民医院实施渗透测试服务后提供的报告，适用于相关技术人员在对发现的漏洞进行安全修复时作参考。

一. 渗透测试基础信息

1.1 发起测试的设备

测试设备	操作系统	IP 地址
电脑	Windows、kali	117.73.9.61

1.2 测试目标信息

测试时间	系统名称	域名/IP	测试账号
3.5-3.5	健康管理中心	https://tj.rzrmyy.cn:8001/	

1.3 测试人员

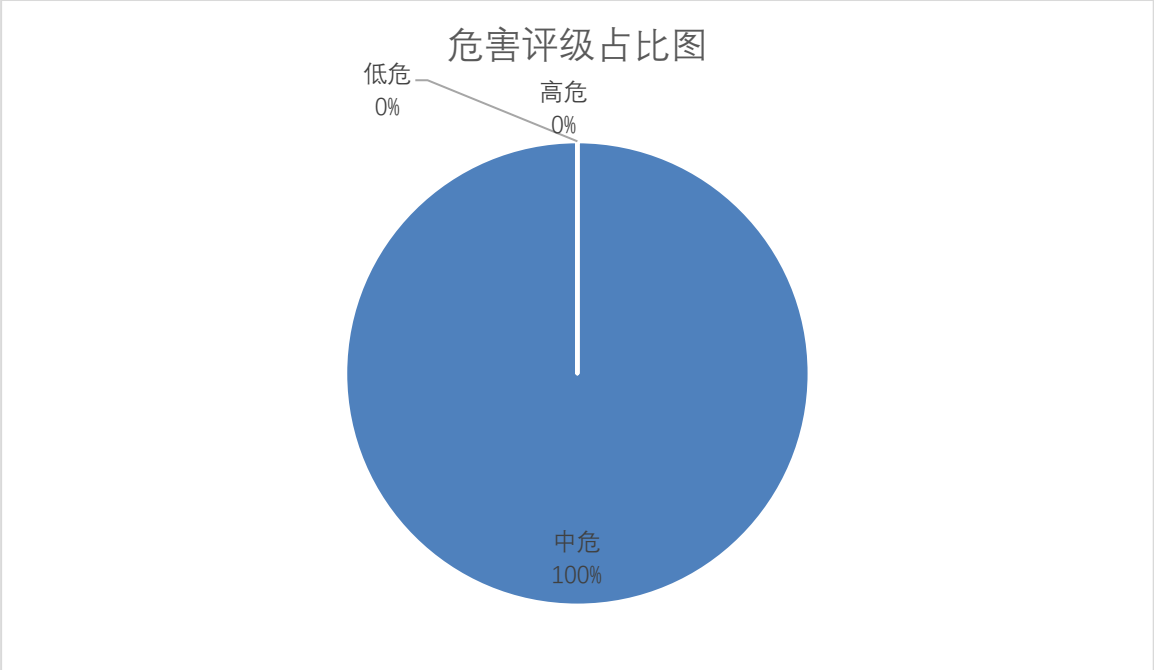
姓名	职务	项目角色
张炜	高级安全服务工程师	WEB 安全测试工程师

二. 渗透测试结果综述

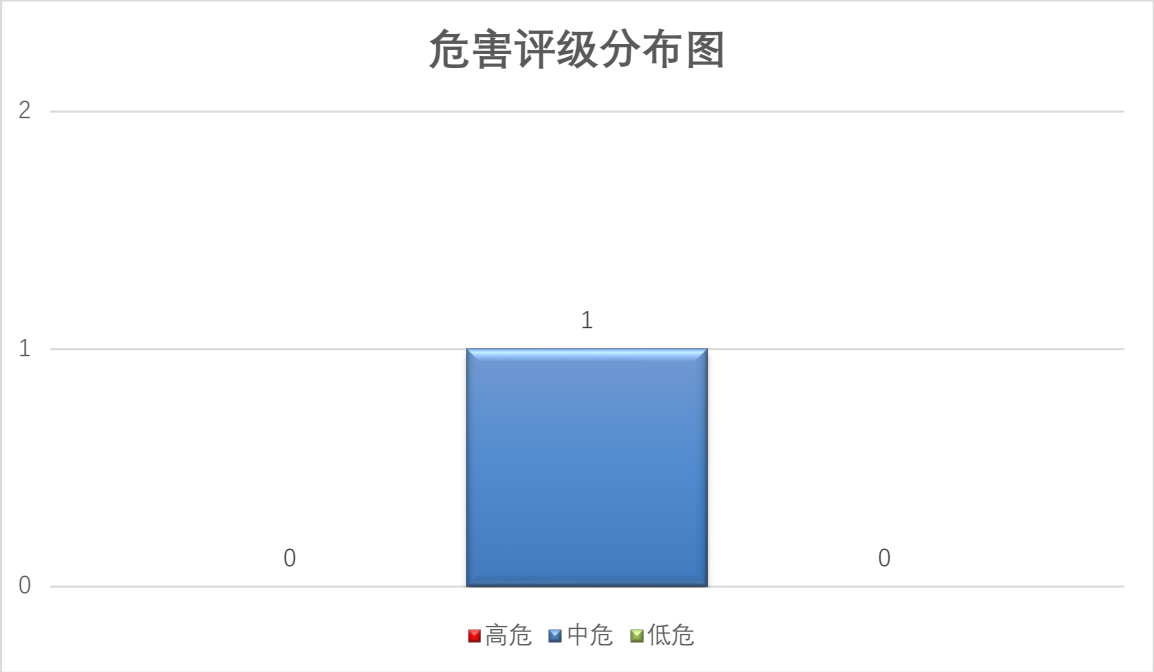
本次渗透测试站点的“健康管理中心”共发现高危漏洞 0 个，中危漏洞 1 个，低危漏洞 0 个，共计 1 个漏洞。

系统名称	高危	中危	低危	汇总
健康管理中心	0	1	0	1

2.1 危害评级占比图



2.2 危害评级分布图



2.3 危害评级汇总表

各危害评级漏洞信息如下：

序号	漏洞名称	危害评级	漏洞描述	所属资产
1	短信轰炸漏洞	中危	站点登录接口通过短信验证码登录，攻击者可以通过重发包进行短信验证码轰炸	健康管理中心

2.4 危害评级标准表

危害评级标准如下：

危害评级	描述
高危	可直接威胁到网络、操作系统、业务系统的安全性，可导致业务中断或敏感信息泄漏的漏洞。 此类风险如远程缓冲区溢出、命令执行、SQL 注入、关键业务弱口令、未授权访问、重要接口越权、重大敏感信息泄漏等。
中危	存在一定的危害性，一经利用即可威胁到操作系统、业务系统的安全性，进而威胁到网络的安全性的漏洞。

危害评级	描述
	此类风险如远程缓冲区溢出、非关键业务弱口令、XSS 跨站、普通敏感信息泄漏、跨站请求伪造等。
低危	存在相对较小的危害性，并不直接对系统或应用造成危害。一旦被利用时影响相对较小，在测试中通常会为进一步的渗透产生辅助性作用。 此类风险如信息泄漏、非关键业务拒绝服务漏洞等。

三. 渗透测试方法、依据及准备

3.1 测试方法

渗透测试是对用户信息安全措施积极评估的过程，通过系统化的操作和分析，积极发现系统和网络中存在的各种缺陷和弱点，如设计缺陷和技术缺陷。

图 2.1.2 测试流程

渗透测试服务流程定义为如下阶段：

信息收集

此阶段中，测试人员会对网站的 IP 地址、DNS 记录、服务器版本等信息进行收集和归纳。

渗透测试

此阶段中，测试人员结合信息收集阶段获得的信息以及渗透测试标准对目标发起测试。

权限提升

此阶段中，测试人员尝试将渗透测试阶段获得的权限提升至管理员权限以获得对系统的完全控制权。

威胁分析

此阶段中，测试人员对上述发现的漏洞进行分类并分析其产生的原因及造成的影响。

输出报告

此阶段中，测试人员根据测试和威胁分析的结果编写渗透测试报告。

3.2 测试工具

信息收集工具：Hping、搜索引擎、nmap、nslookup、dnsenum

WEB 手工分析工具：burp suite、OWASP ZAP

数据库注入测试工具：Havij、sqlmap、pangolin

应用软件：Ftp、远程桌面连接工具等

浏览器：IE、Firefox

WEB 漏洞扫描器：IBM appscan 最新版、HP webinspect 最新版、WVS 最新版、Netsparker

综合扫描器：Nessus（可扫数据库、服务器、中间件等）、山石网科远程安全评估系统

漏洞利用平台：Metasploit

3.3 参考依据

为了保证此次渗透测试的先进性、完备性、规范性，渗透测试工程师将参考行业内有关的标准进行操作。

国内部分标准

- GB/T 20984-2022 信息安全技术 信息安全风险评估方法
- GB/T 31506-2022 信息安全技术 政务网站系统安全指南
- GB/T 35273-2020 信息安全技术 个人信息安全规范
- GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
- GB/T 28450-2020 信息技术 安全技术 信息安全管理体系审核指南
- GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南
- GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
- GB/T 38645-2020 信息安全技术 网络安全事件应急演练指南
- GB/T 37964-2019 信息安全技术 个人信息去标识化指南
- GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求
- GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求
- GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南
- GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南
- GB／T 36958-2018 信息安全技术 网络安全等级保护安全管理中心技术要求
- GB/T 36959-2018 信息安全技术 网络安全等级保护测评机构能力要求和评估规范
- GB/T 37094-2018 信息安全技术 办公信息系统安全管理要求
- GB/T 37095-2018 信息安全技术 办公信息系统安全基本技术要求
- GB/T 37096-2018 信息安全技术 办公信息系统安全测试规范
- GB/T 36957-2018 信息安全技术 灾难恢复服务要求
- GB/T 37046-2018 信息安全技术 灾难恢复服务能力评估准则
- GB/T 35278-2017 信息安全技术 移动终端安全保护技术要求
- GB/T 32923-2016 信息安全技术 信息安全治理
- GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南
- GB/T 33132-2016 信息安全技术 信息安全风险处理实施指南
- GB/T 30270-2013 信息技术 安全技术 信息技术安全性评估方法
- GB/T 30279-2013 信息安全技术 安全漏洞等级划分指南
- GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范
- GB/T 20984-2007 信息安全技术 信息安全风险评估规范
- GB/Z 20986-2007 信息安全事件分类分级指南
- ISO/IEC 27001:2005 信息技术 安全技术 信息系统规范与使用指南
- ISO/IEC 13335-1: 2004 信息技术 安全技术 信息技术安全管理指南
- ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
- ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
- ……

国际部分标准

- 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
- 信息系统审计标准（ISACA）G7 应有的职业谨慎
- 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
- 信息系统审计标准（ISACA）G18 信息系统管理
- 信息系统审计标准（ISACA）G19 不正当及非法行为
- 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
- CESG (CHECK) IT Health Check 方法
- OWASP OWASP_Testing_Guide_v3
- OWASP OWASP_Development_Guide_2005
- OWASP OWASP_Top_10_2010_Chinese_V1.0
- OWASP OWASP_Top_10_2013-Chinese-V1.2
- OWASP OWASP_Top_10_2017_RC1_V1.0
- OWASP OWASP_Testing_Guide_v4
- OWASP API Security TOP 10
- OSSTMM OSSTMM_Web_App_Alpha
- Web 应用安全委员会（WASC）WASC Threat Classification v2
- ……

测试项部分标准

测试分类	测试子项
信息收集	搜索引擎信息发现和侦察
	识别 web 服务器
	web 服务器元文件信息发现
	服务器应用应用枚举
	评论信息发现
	识别 web 应用框架
配置以及部署管理测试	网络基础设施配置测试
	应用平台配置管理测试
	文件扩展名处理测试
	备份和未链接文件测试
	枚举管理接口测试
	应用跨域策略测试
身份鉴别管理测试	角色定义测试
	用户注册过程测试
	帐户权限变化测试
	帐户枚举测试
	弱用户名策略测试
认证测试	口令信息加密传输测试
	默认口令测试
	认证绕过测试
	密码策略测试

	安全问答测试
	密码重置测试
授权测试	目录遍历/文件包含测试
	授权绕过测试
	权限提升测试
	不安全对象直接引用测试
会话管理测试	会话管理绕过测试
	会话固定测试
	会话令牌泄露测试
	跨站点请求伪造（CSRF）测试
	登出功能测试
输入验证测试	跨站脚本测试
	HTTP 参数污染测试
	SQL 注入测试
	LDAP 注入测试
	代码注入测试
	命令执行注入测试
	缓冲区溢出测试
错误处理测试	错误码分析
	栈追踪分析
密码学测试	弱 SSL/TLS 加密
	不安全的传输层防护测试
	Padding Oracle 测试
	非加密信道传输敏感数据测试
	加密密钥强度测试
业务逻辑测试	业务逻辑数据验证测试
	功能使用次数限制测试
	非预期文件类型上传测试
	恶意文件上传测试
客户端测试	HTML 注入测试
	客户端 URL 重定向测试
	CSS 注入测试
	点击劫持测试
	跨源资源分享测试（CORS）
	Flash 跨站测试
……	……

四. 渗透测试漏洞详细信息

4.1 短信轰炸漏洞（中危）

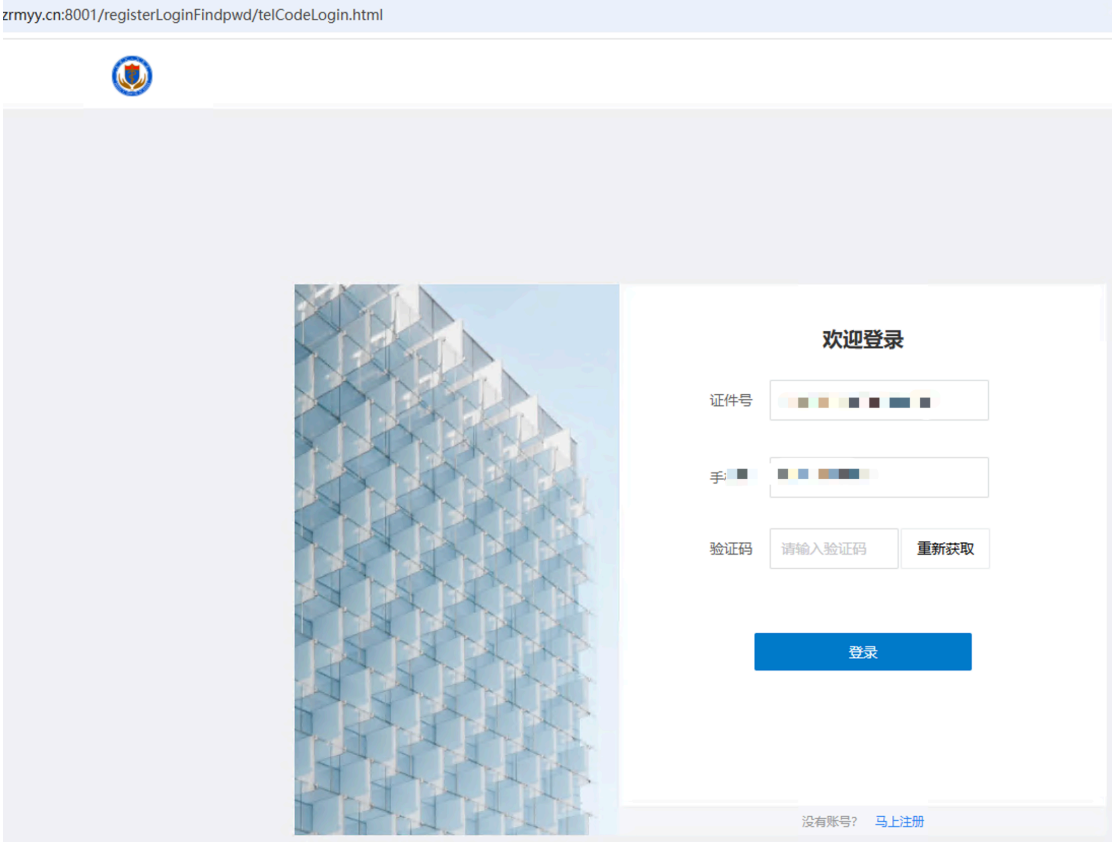
漏洞危害描述：站点登录接口通过短信验证码登录，攻击者可以通过重发包进行短信验证码轰炸

漏洞评级：中危

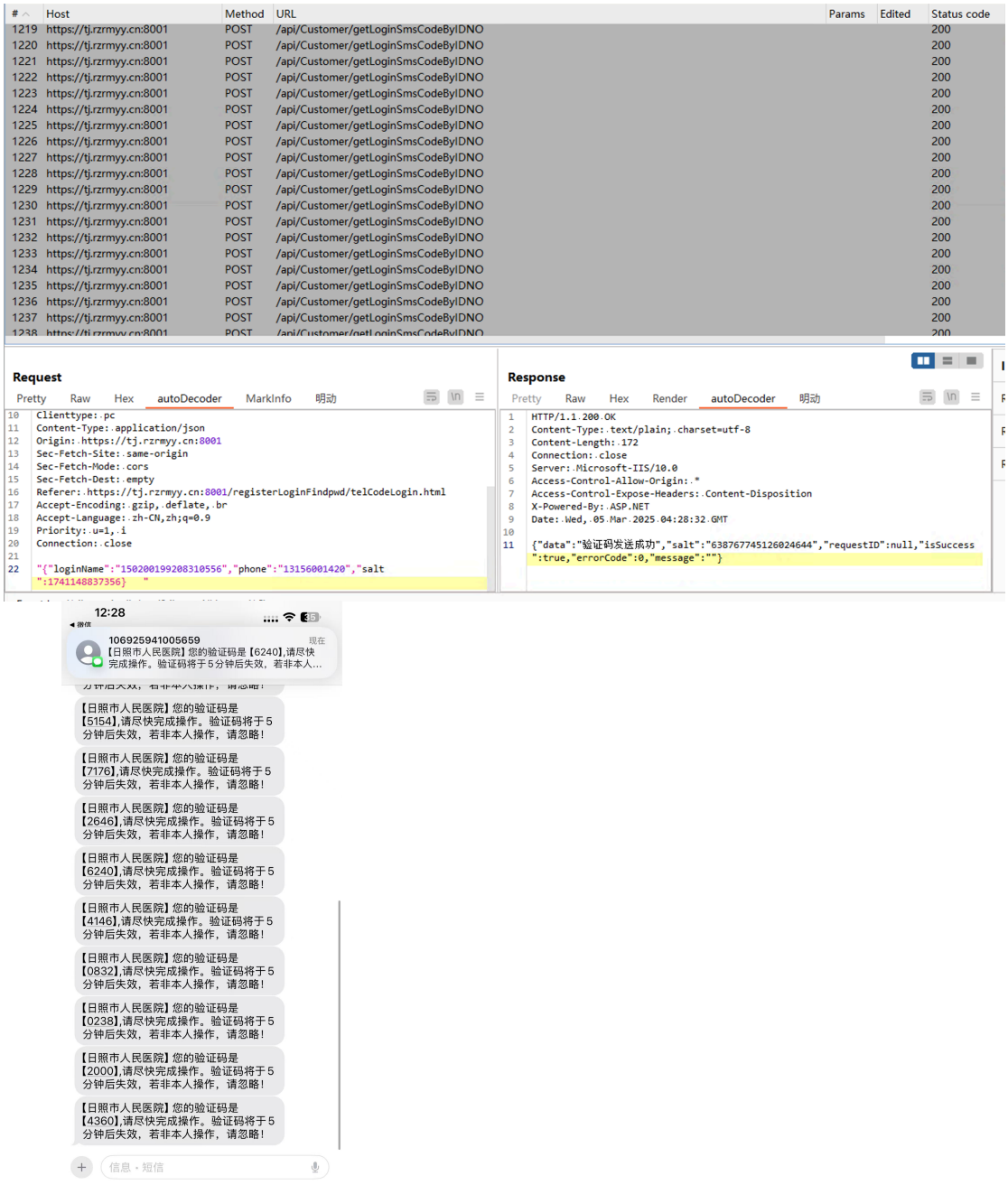
漏洞分析与验证：

打开登录页面，输入注册的身份证和手机号：

https://tj.rzrmyy.cn:8001/registerLoginFindpwd/telCodeLogin.html



输入后点击“获取验证码”，在首个申请验证码的数据包未产生汇报时重发数据包，可以进行短信轰炸。



#	Host	Method	URL	Params	Edited	Status code
1219	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1220	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1221	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1222	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1223	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1224	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1225	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1226	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1227	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1228	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1229	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1230	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1231	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1232	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1233	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1234	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1235	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1236	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1237	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200
1238	https://tj.rzrmyy.cn:8001	POST	/api/Customer/getLoginSmsCodeByIDNO			200

Request

Pretty Raw Hex autoDecoder MarkInfo 明动

```
Clienttype:pc
Content-Type:application/json
Origin:https://tj.rzrmyy.cn:8001
Sec-Fetch-Site:same-origin
Sec-Fetch-Mode:cors
Sec-Fetch-Dest:empty
Referer:https://tj.rzrmyy.cn:8001/registerLoginFindpwd/telCodeLogin.html
Accept-Encoding:gzip,deflate,br
Accept-Language:zh-CN,zh;q=0.9
Priority:u=1,i
Connection:close

"{"loginName":"150200199208310556","phone":"13156001420","salt
":1741148837356}  "
```

Response

Pretty Raw Hex Render autoDecoder 明动

```
HTTP/1.1 200 OK
Content-Type:text/plain;charset=utf-8
Content-Length:172
Connection:close
Server:Microsoft-IIS/10.0
Access-Control-Allow-Origin:*
Access-Control-Expose-Headers:Content-Disposition
X-Powered-By:ASP.NET
Date:Wed,05 Mar 2025 04:28:32 GMT

{"data":"验证码发送成功","salt":"638767745126024644","requestID":null,"isSuccess
":true,"errorCode":0,"message":""}
```


漏洞修复建议：限制用户同一 IP 在一分钟内提交 POST 的次数和频率，或者对同一手机号进行一分钟内获取一次短信的限制。

Hillstone AF

HS-AF@hillstonenet.com

www.hillstonenet.com.cn