

**海门区网信办**

**渗透测试报告**

**江苏晟晖信息科技有限公司**

**2025年04月24日**

1. 验证综述
   1. 目标信息

**漏洞来源IP地址段/域名：**

|  |  |
| --- | --- |
| **目标** | **备注** |
| https://tjzx.hmph120.com:10300/ |  |

* 1. 已发现漏洞类型

|  |  |
| --- | --- |
| **高危漏洞** | **1.南通市海门区人民医院-海门区人民医院健康管理中心小程序-信息泄露**  **2.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人报告**  **3.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人个人信息**  **4.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人体检报告单**  **5.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人订单**  **6.南通市海门区人民医院-海门区人民医院健康管理中心小程序-订单处未授权访问**  **7.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权修改我的体检人信息**  **8.南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权进行套餐预约**  **9.南通市海门区人民医院-海门区人民医院健康管理中心小程序-登录验证码爆破导致任意用户登录** |
| **中危漏洞** | **无** |
| **低危漏洞、信息泄露** | **无** |
| **测试项** | **无** |

* 1. 测试遗留问题

渗透测试过程中未遗留任何威胁信息，未在目标系统遗留任何文件（如木马、后门）。

* 1. 验证结果详情
     1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-信息泄露

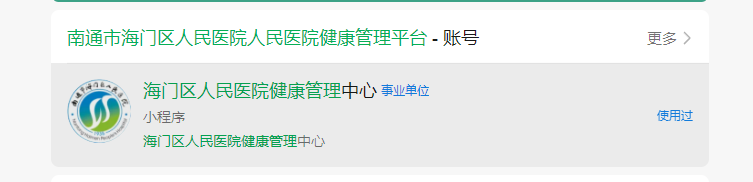
**漏洞类型：信息泄露**

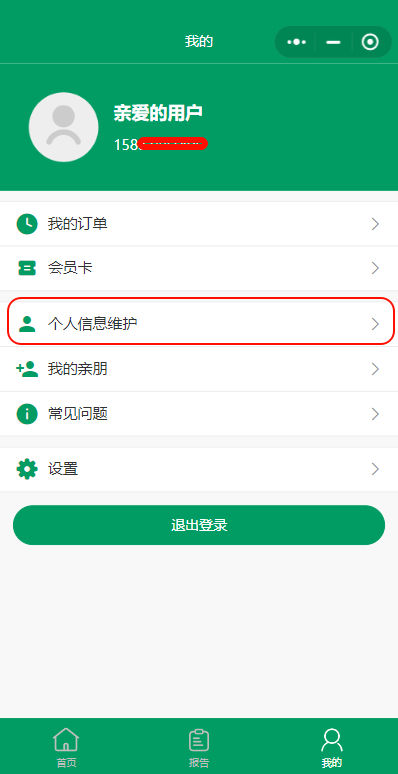
**漏洞评级：高**

**漏洞地址：**

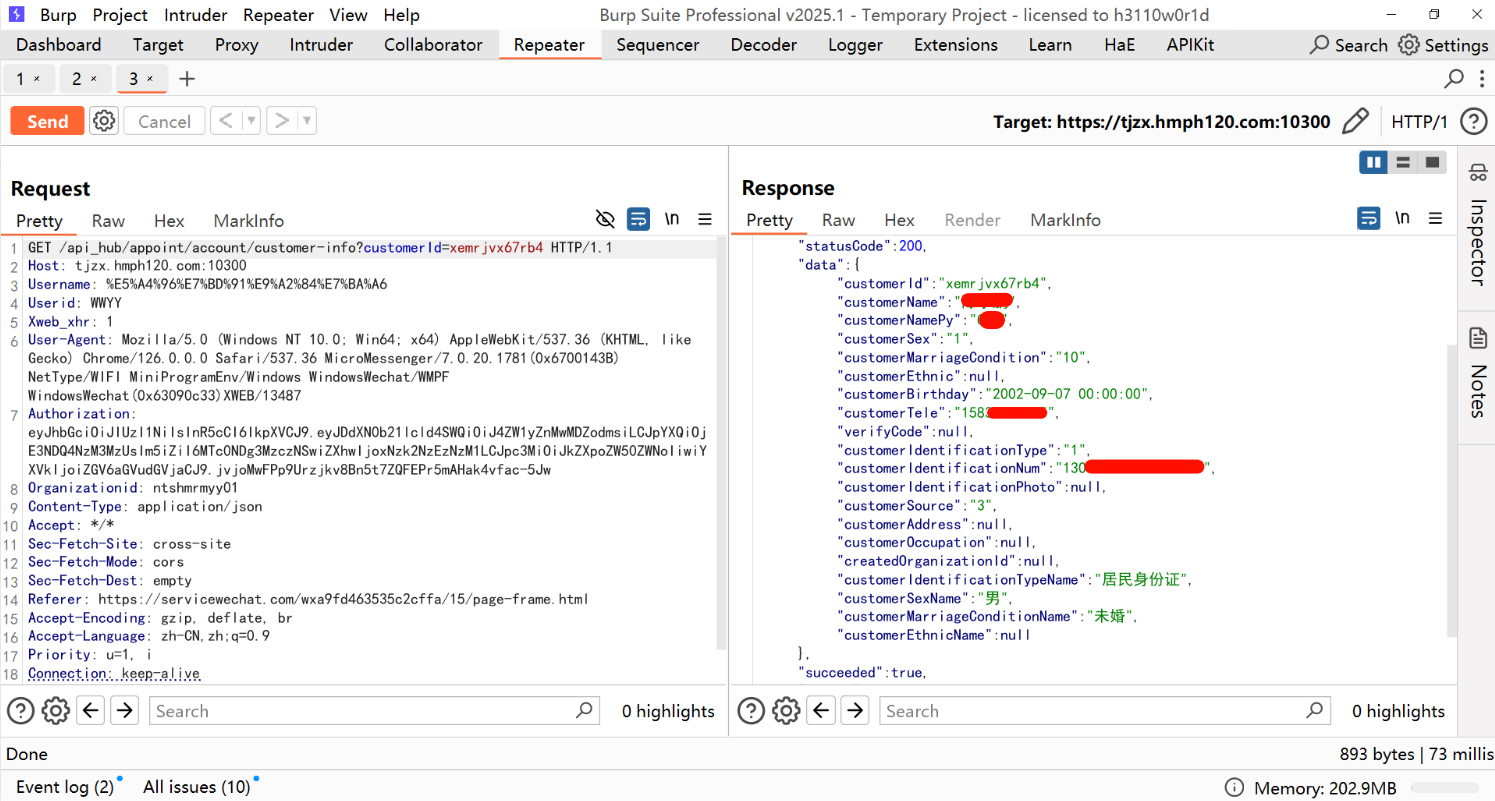
https://tjzx.hmph120.com:10300/api\_hub/appoint/account/customer-info?customerId=

**漏洞详情：**

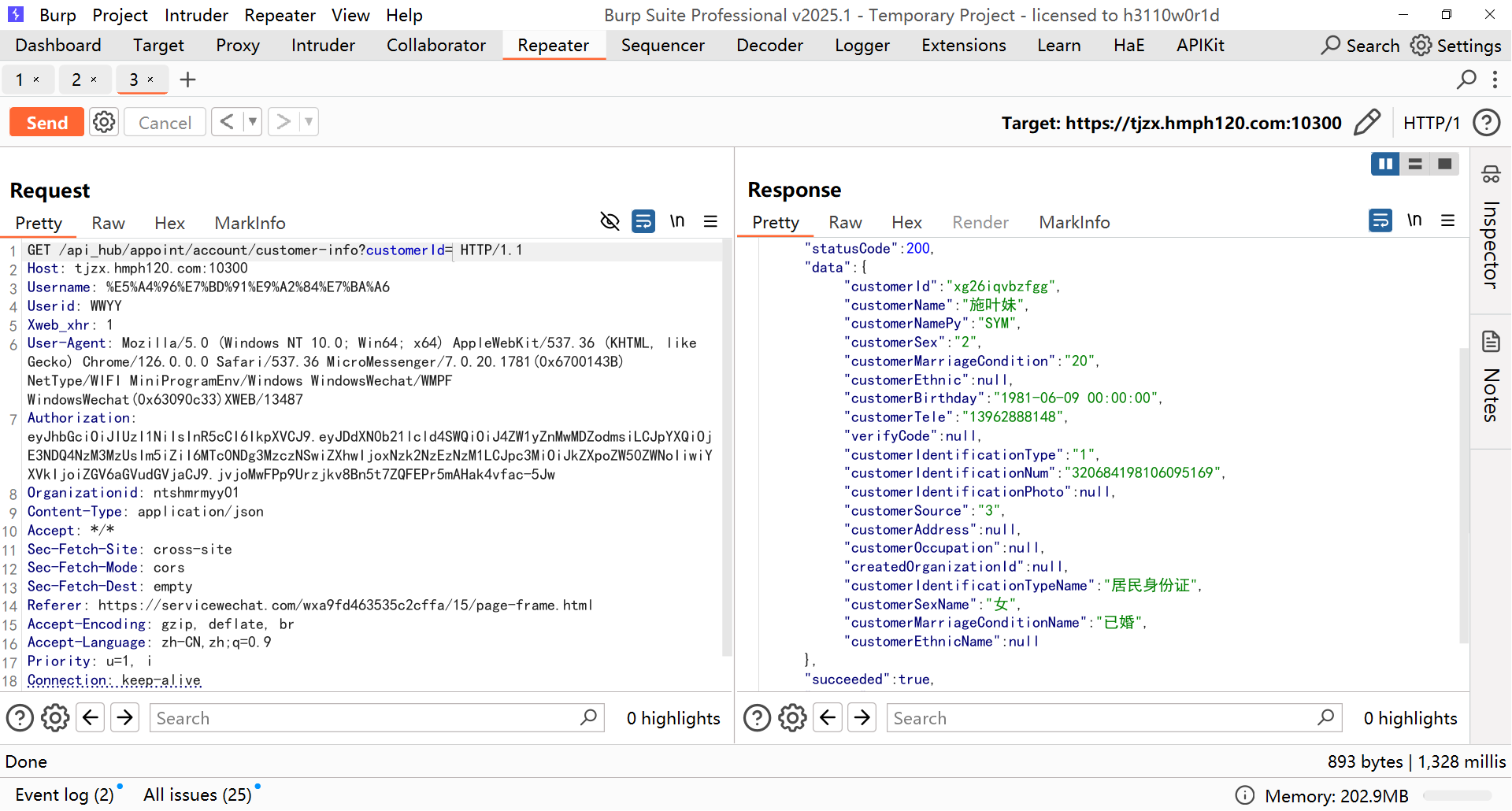




下面是自己信息



将customerId删除得到他人信息



**造成的危害：**

恶意分子通过批量查询用户信息，导致用户 xxxx 信息泄漏，可以对用户实施钓鱼、诈骗等。甚至用于黑产。

**修复建议：**

1. 对查询请求做好检查和限制。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人报告

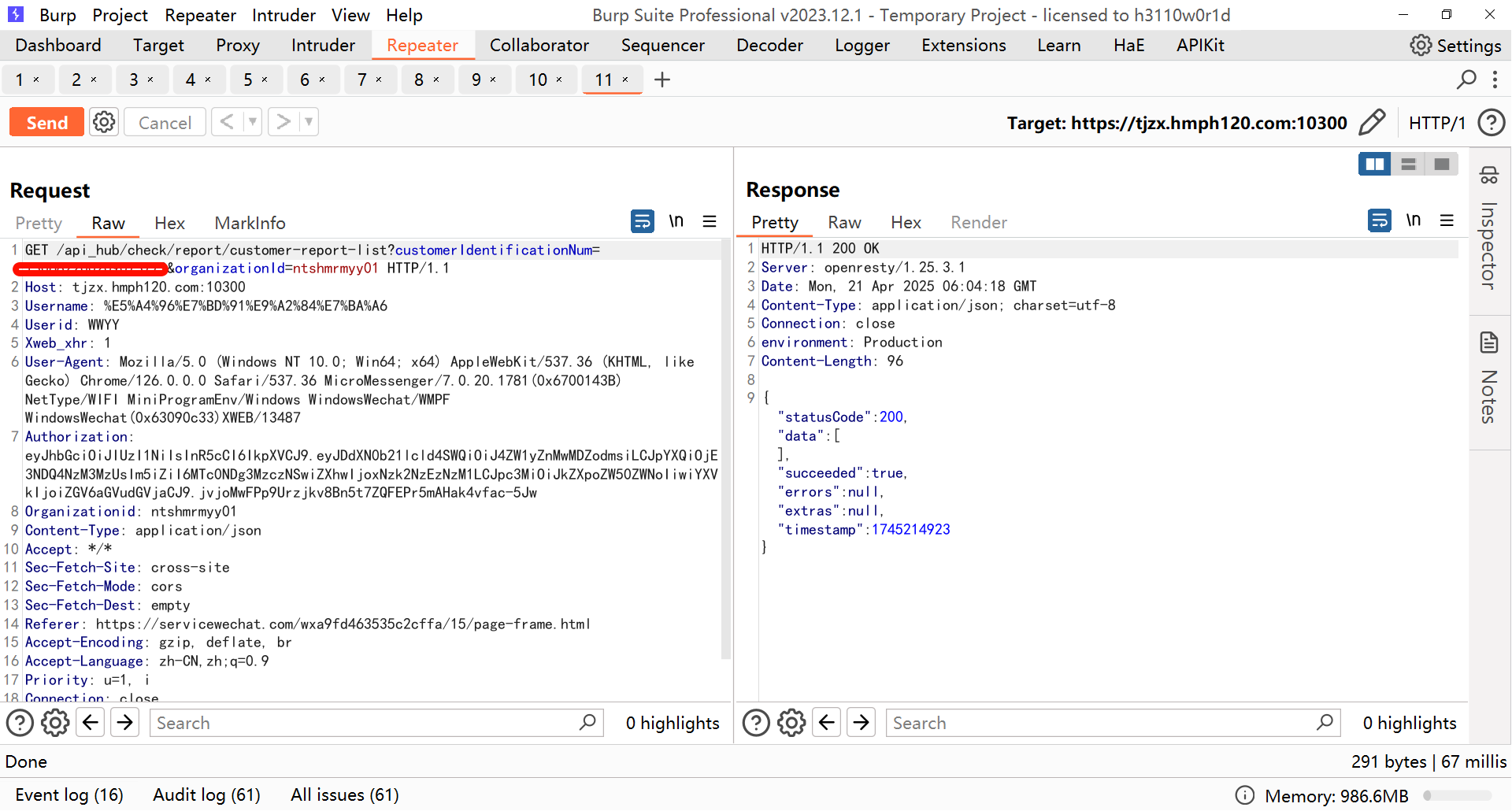
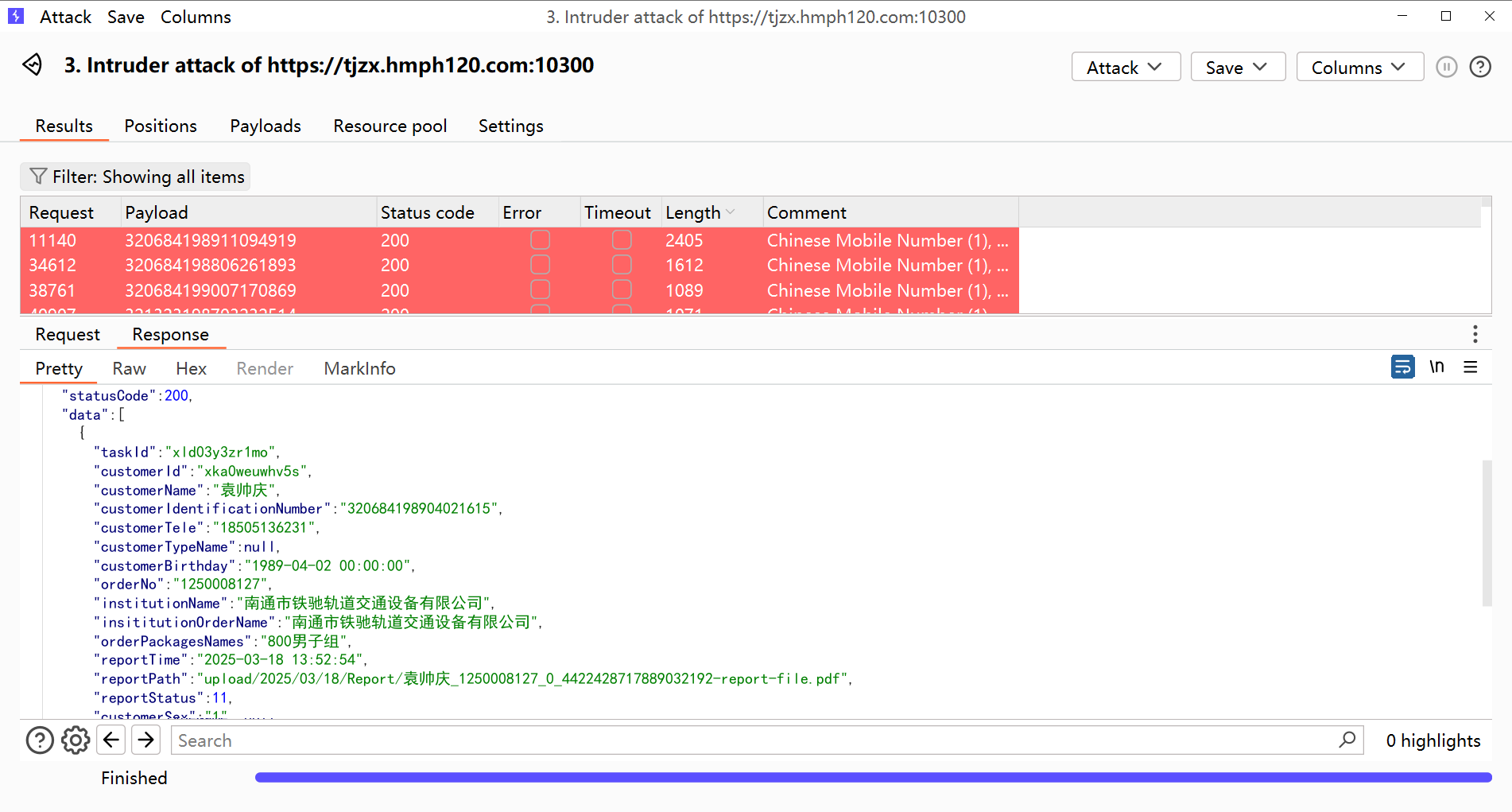
**漏洞类型：访问控制缺陷**

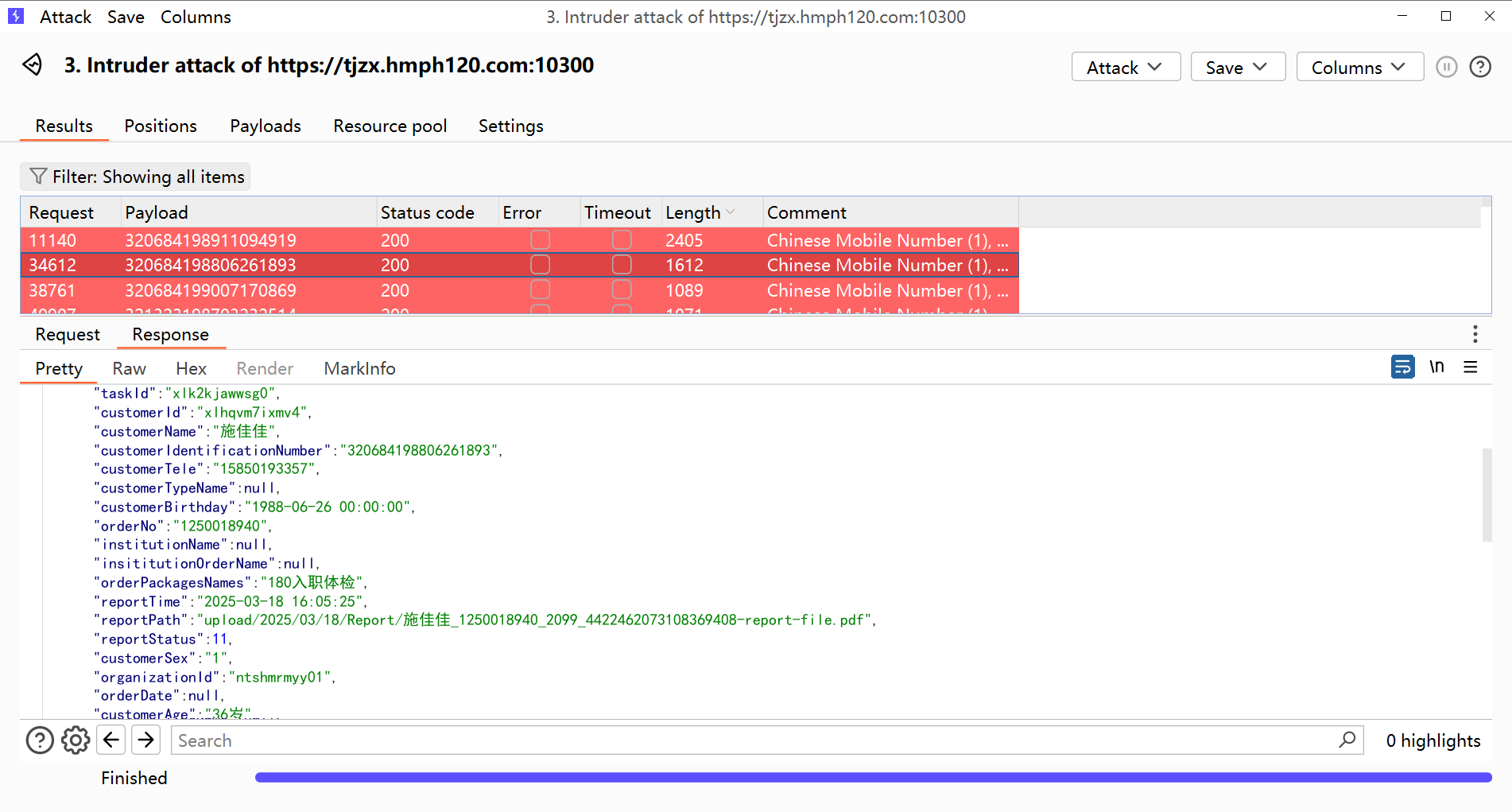
**漏洞评级：高**

**漏洞地址：**

https://tjzx.hmph120.com:10300/api\_hub/check/report/customer-report-list?customerIdentificationNum=320684198904021615=ntshmrmyy01

**漏洞详情：**

  
遍历customerIdentificationNum值  




**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人个人信息

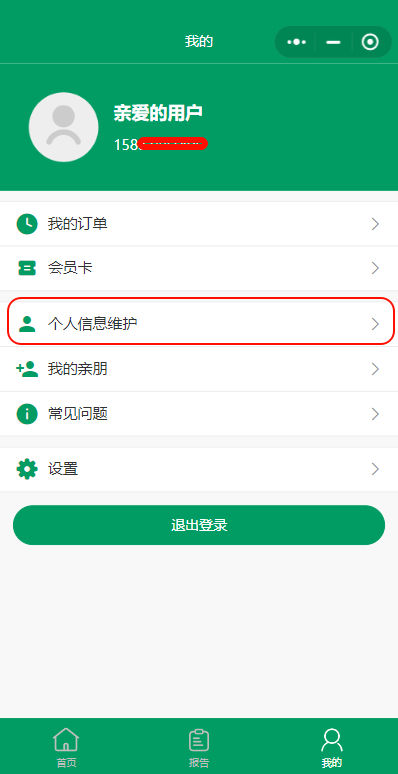
**漏洞类型：访问控制缺陷**

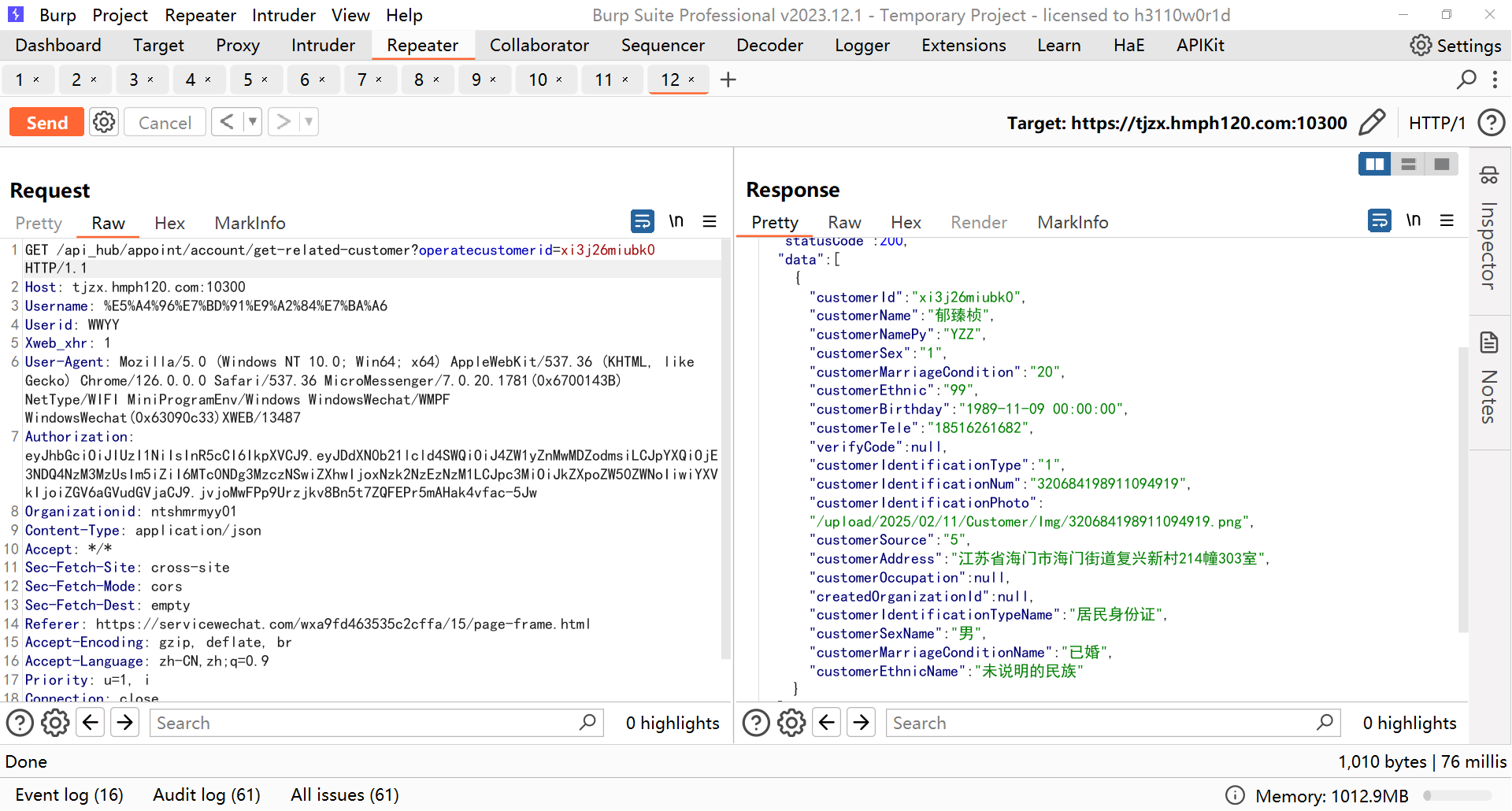
**漏洞评级：高**

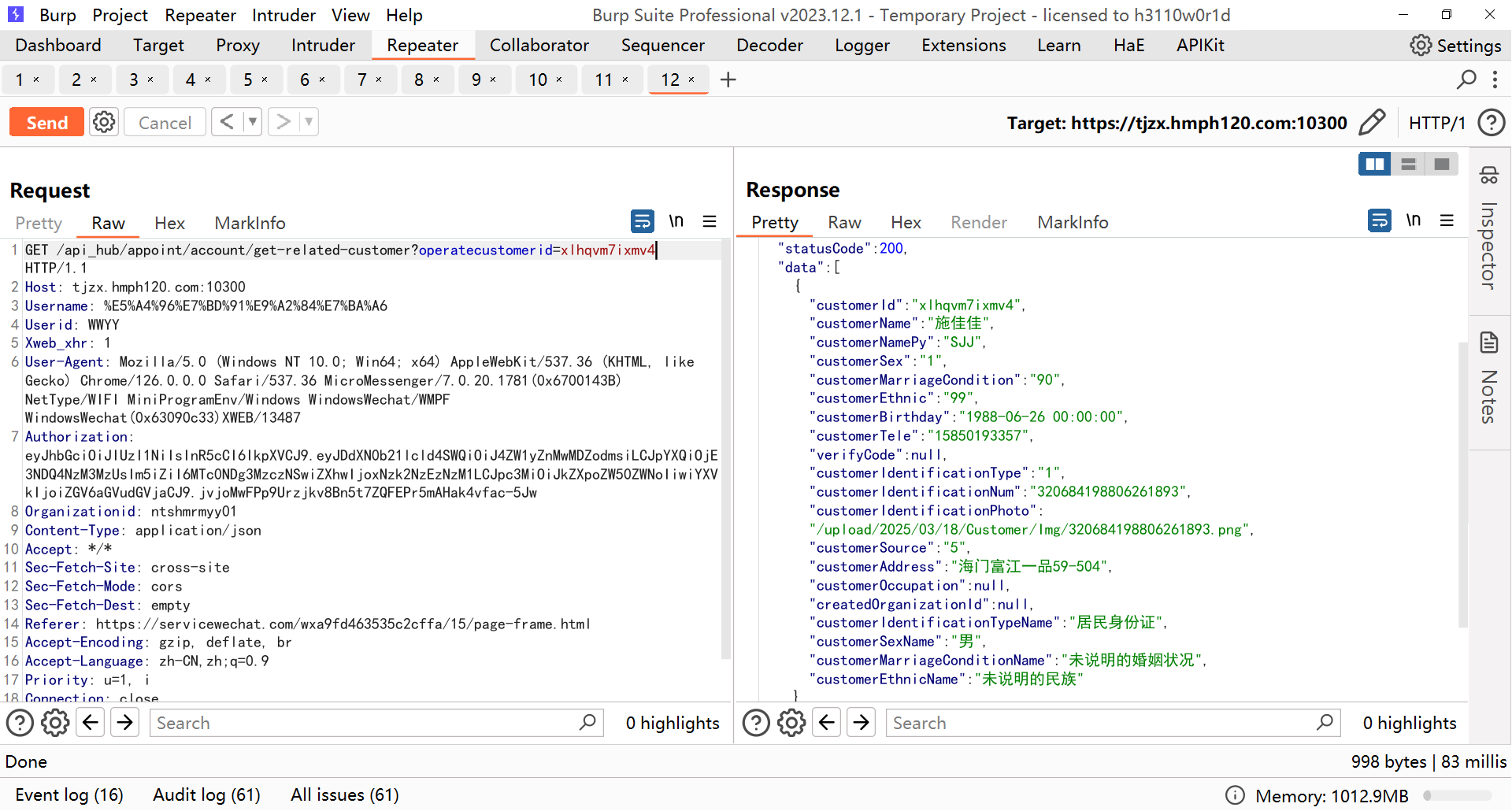
**漏洞地址：**

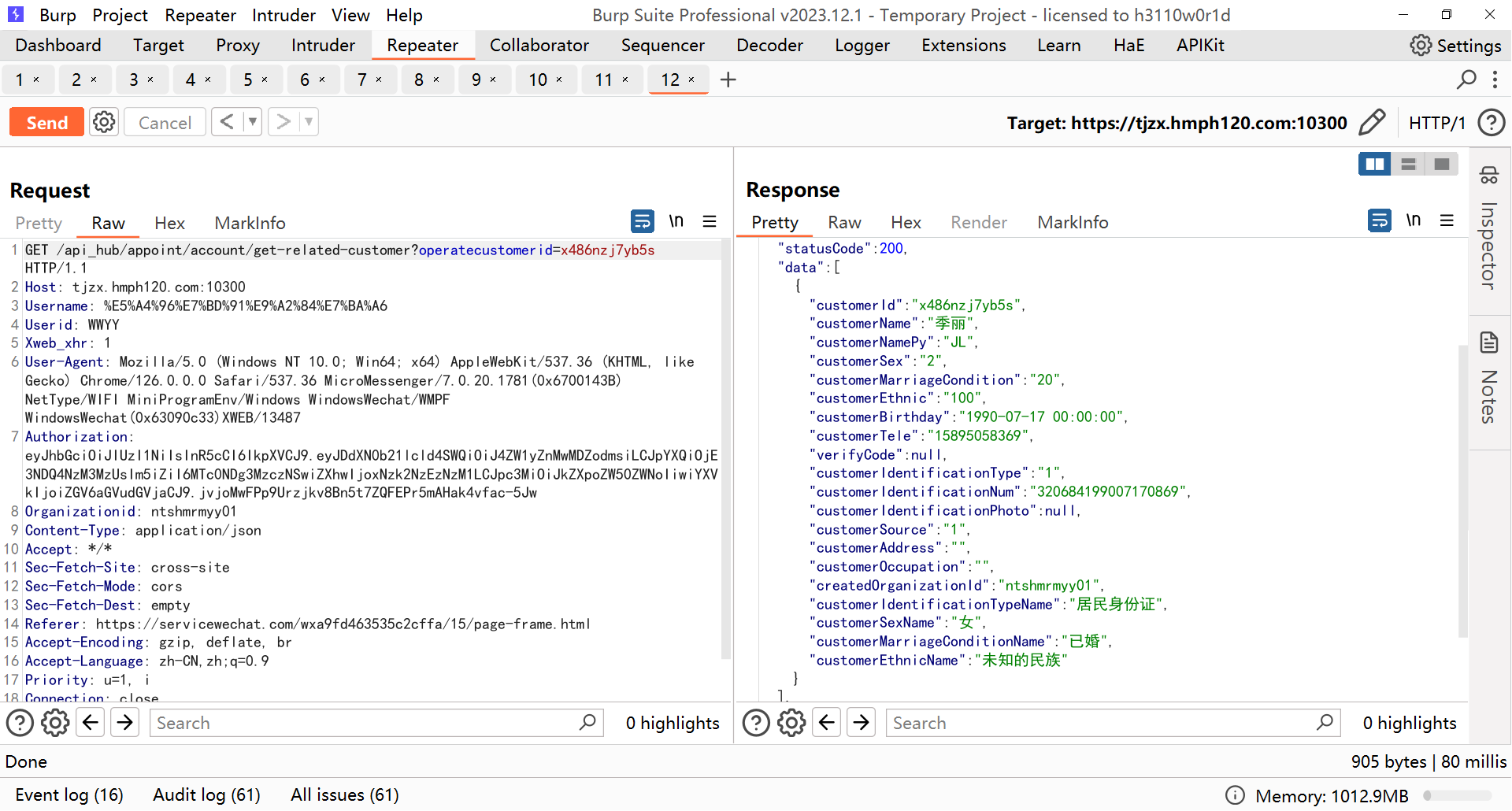
https://tjzx.hmph120.com:10300/api\_hub/appoint/account/get-related-customer?operatecustomerid=xi3j26miubk0

**漏洞详情：**



通过南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人报告得到customerId值，将customerId进行遍历  






**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人体检报告单

**漏洞类型：访问控制缺陷**

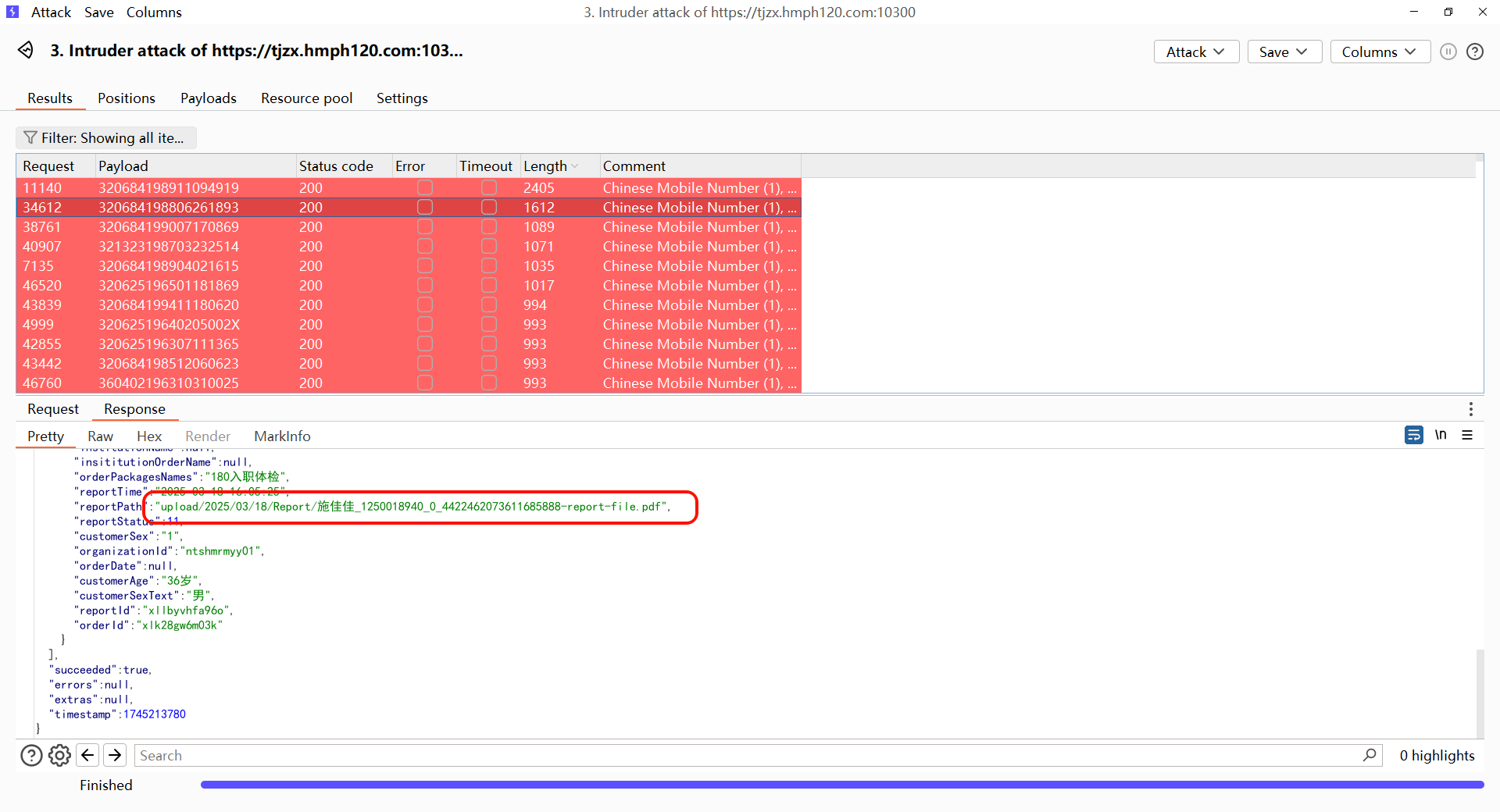
**漏洞评级：高**

**漏洞地址：**

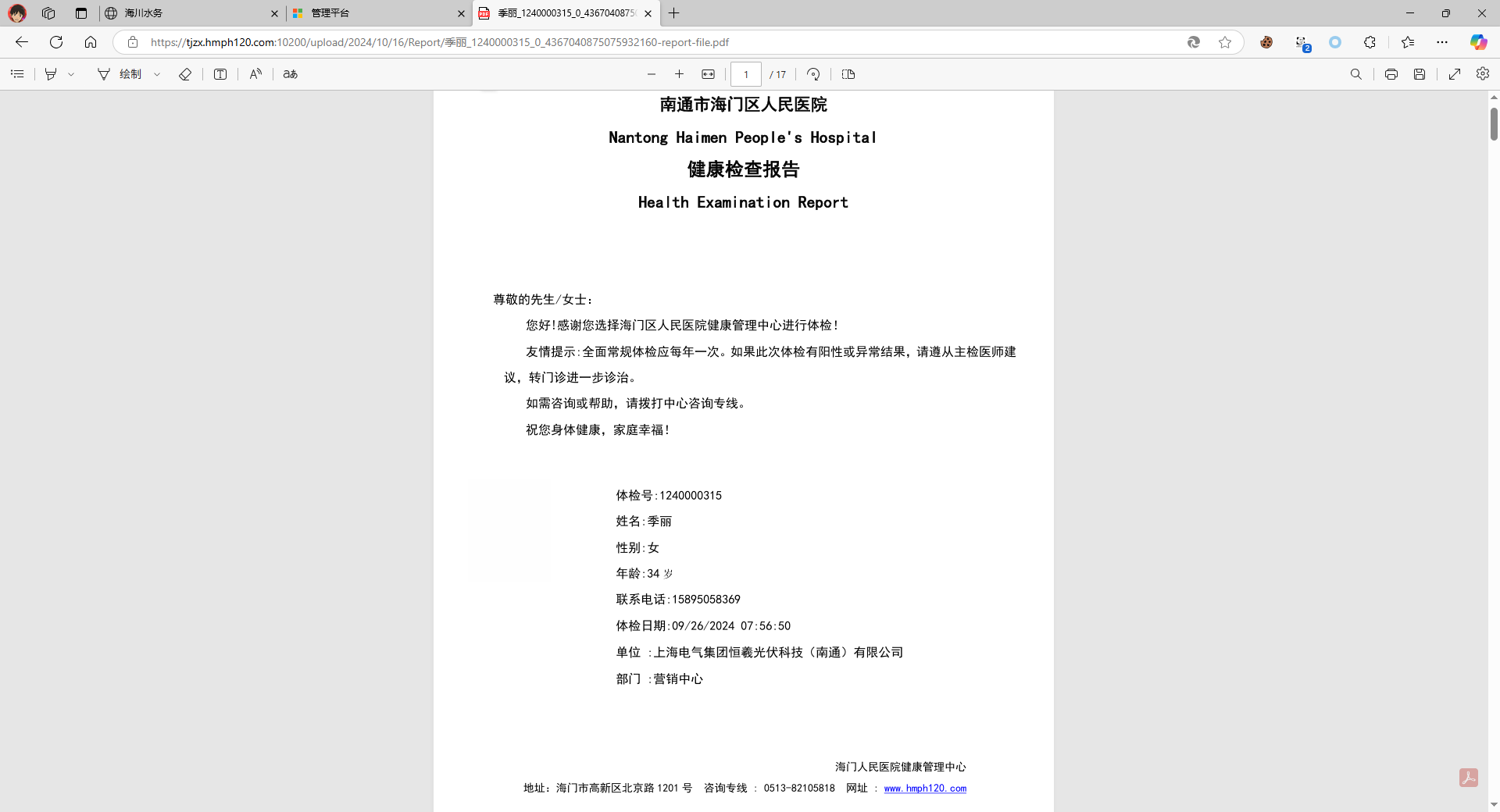
https://tjzx.hmph120.com:10300/api\_hub/check/report/customer-report-list?customerIdentificationNum=320684198806261893=ntshmrmyy01

**漏洞详情：**

通过南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人报告得到体检报告部分地址



将地址拼接到https://tjzx.hmph120.com:10200/后面



**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人订单

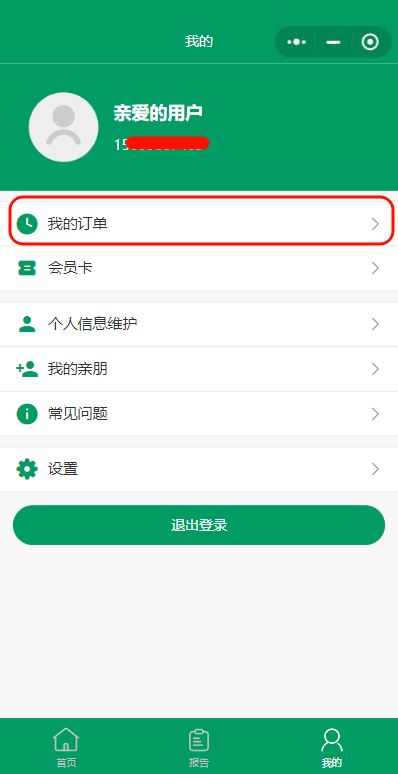
**漏洞类型：访问控制缺陷**

**漏洞评级：高**

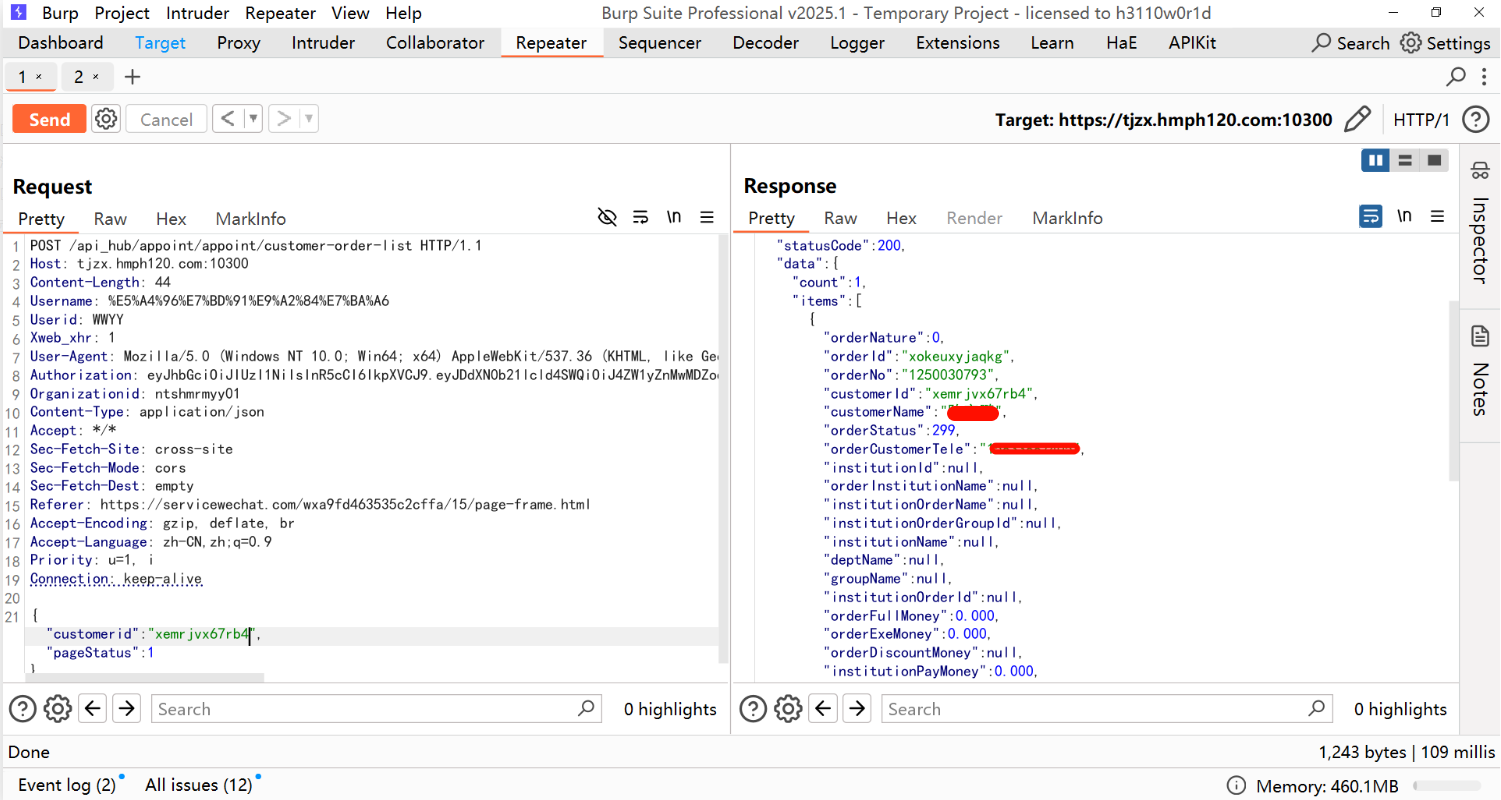
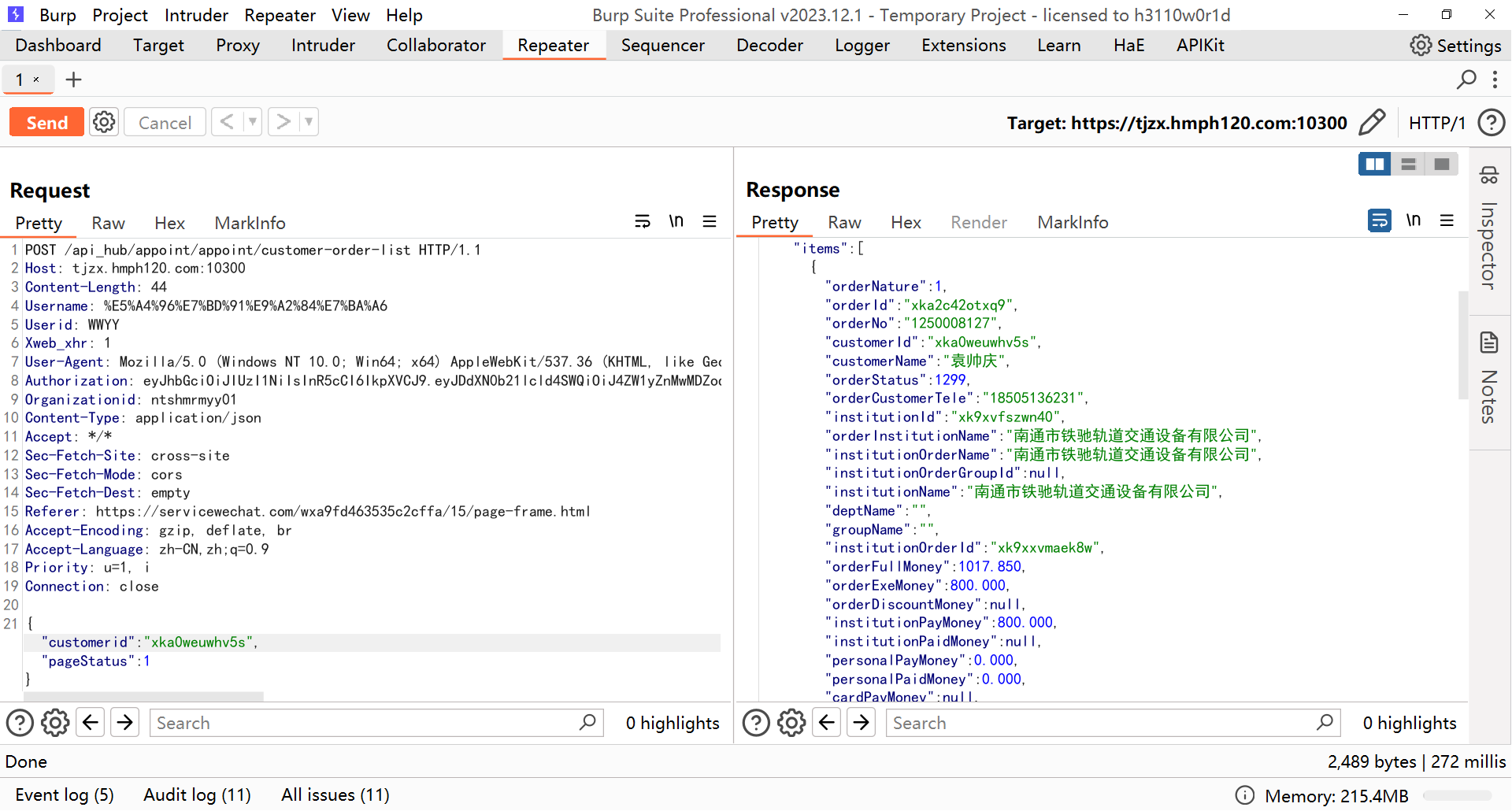
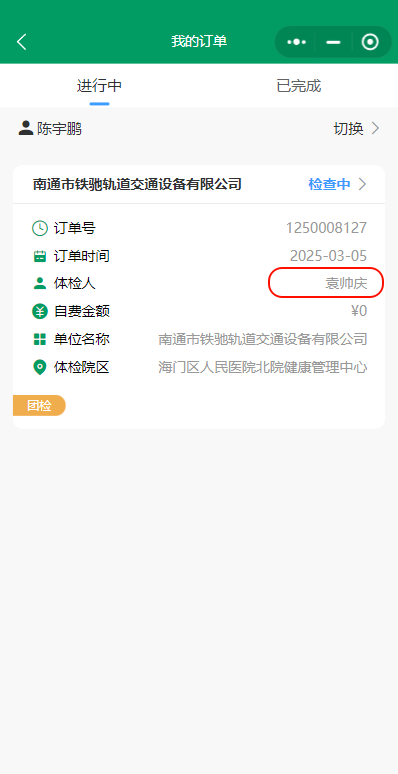
**漏洞地址：**

https://tjzx.hmph120.com:10300/api\_hub/appoint/appoint/customer-order-list

**漏洞详情：**



本人订单信息

  
通过南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权查看他人报告 获得，修改customerid值  
  


**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-订单处未授权访问

**漏洞类型：访问控制缺陷**

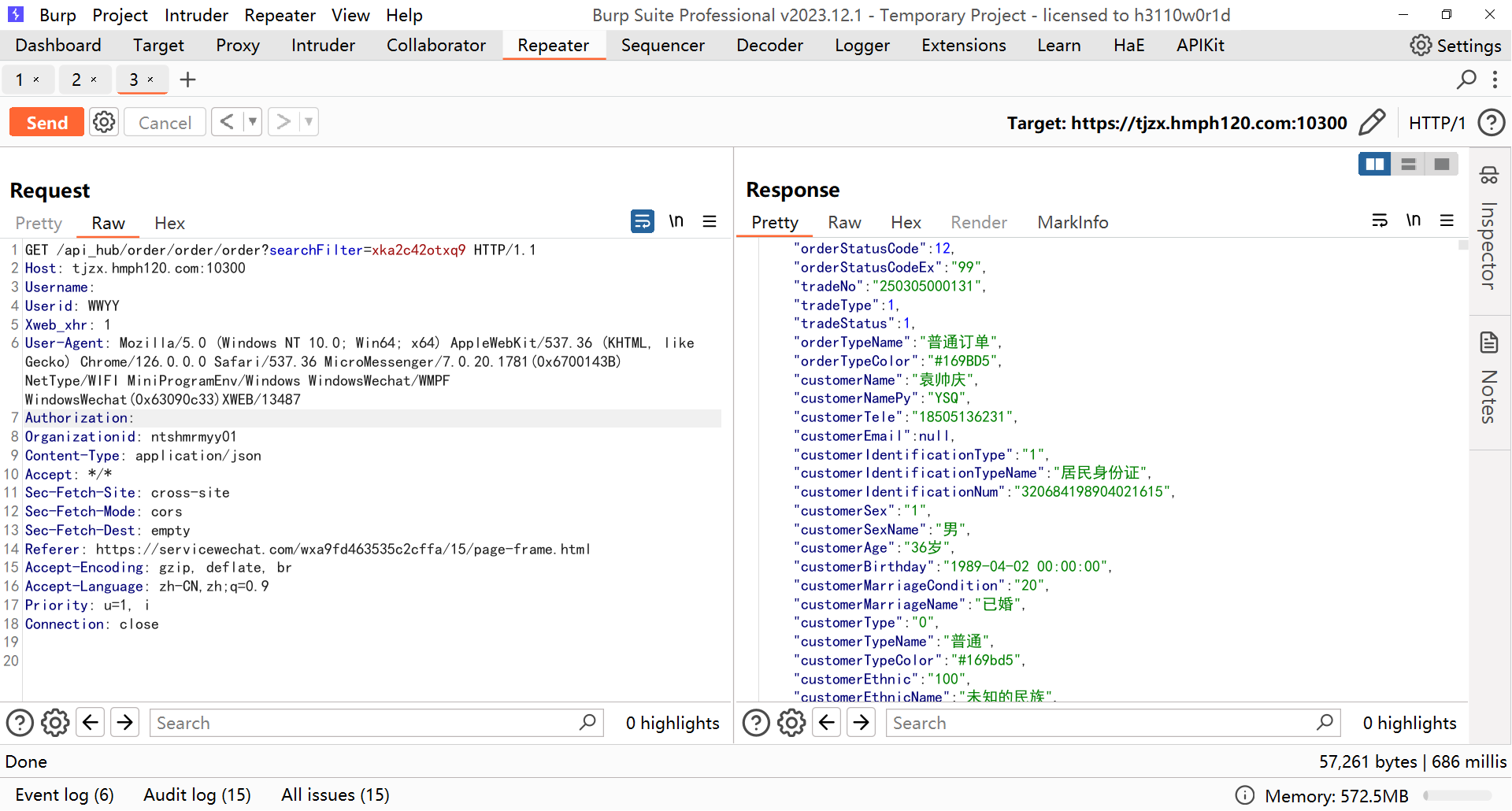
**漏洞评级：高**

**漏洞地址：**

https://tjzx.hmph120.com:10300/api\_hub/order/order/order?searchFilter=xka2c42otxq9

**漏洞详情：**

将Authorization删除也可以看到



**造成的危害：**

攻击者可在没有认证的情况下直接操作对应的 API 接口，可直接被非法增删改次数据。且因为攻击是在未认证下进行的，所以后续无法通过定位用户进行异常排查。

**修复建议：**

1. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 2. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 3. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 4. 在验证用户身份权限前不进行任何数据的交互。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权修改我的体检人信息

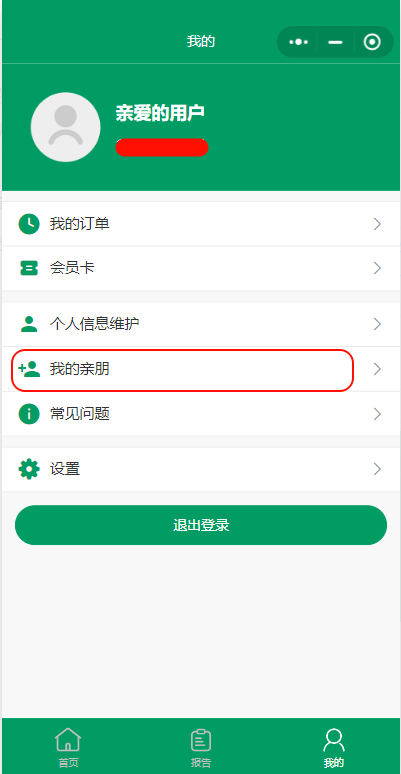
**漏洞类型：访问控制缺陷**

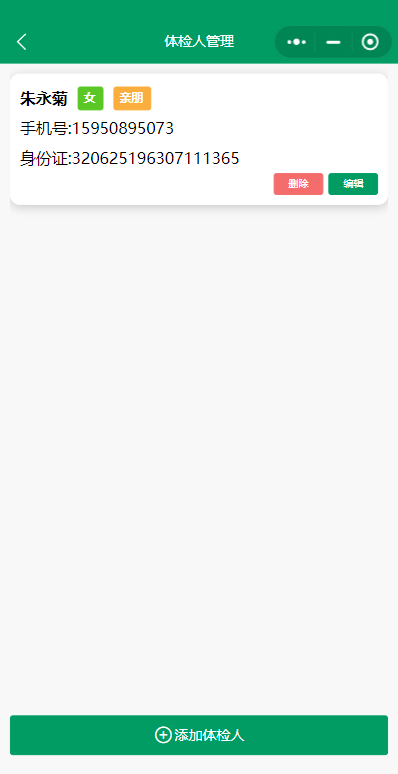
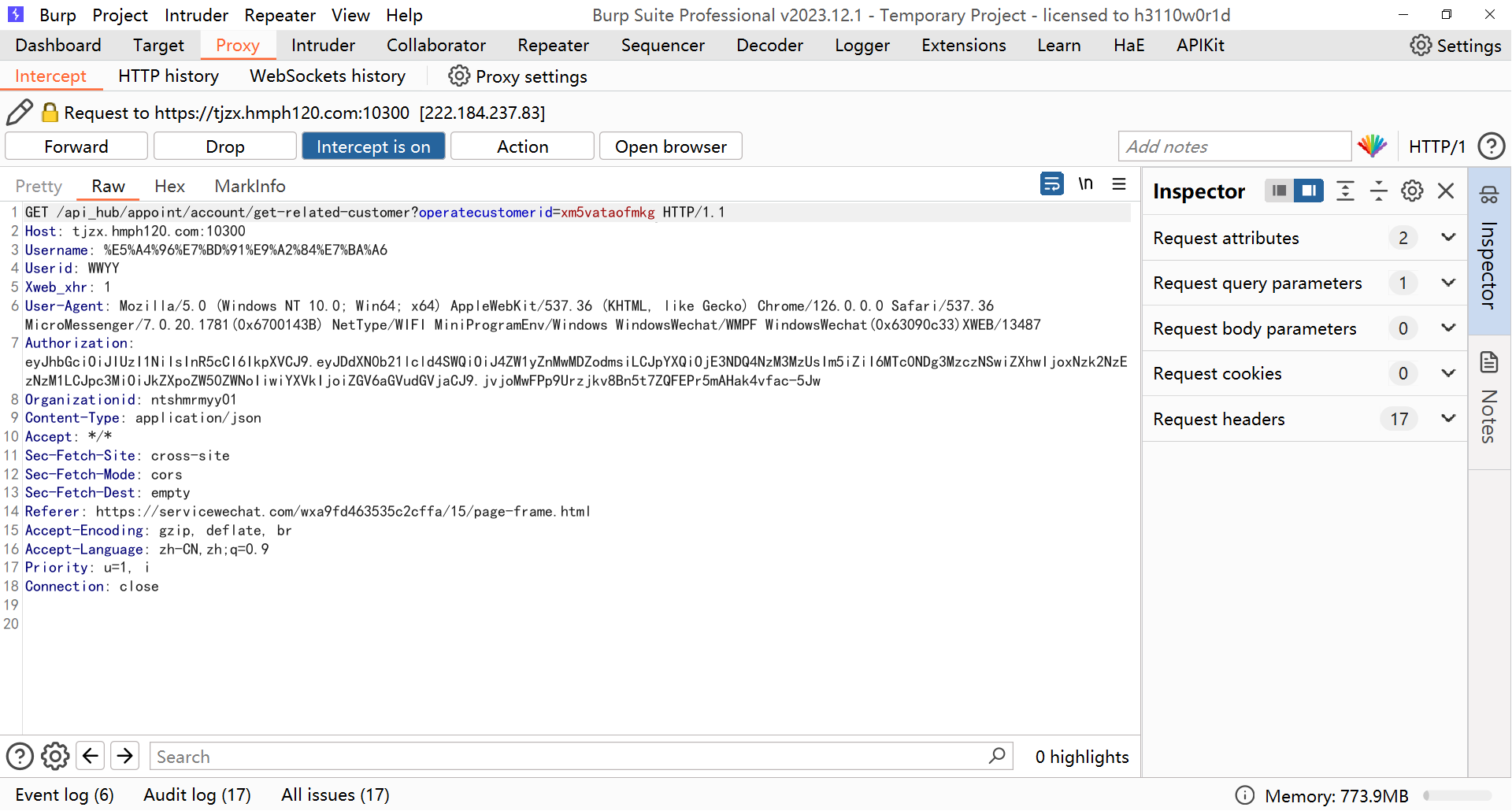
**漏洞评级：高**

**漏洞地址：**

https://tjzx.hmph120.com:10300/api\_hub/appoint/account/get-related-customer?operatecustomerid=xm5vataofmkg

**漏洞详情：**



修改operatecustomerid值可直接进入他人体检人管理  


进入编辑可直接进行修改



**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-越权进行套餐预约

**漏洞类型：访问控制缺陷**

**漏洞评级：高**

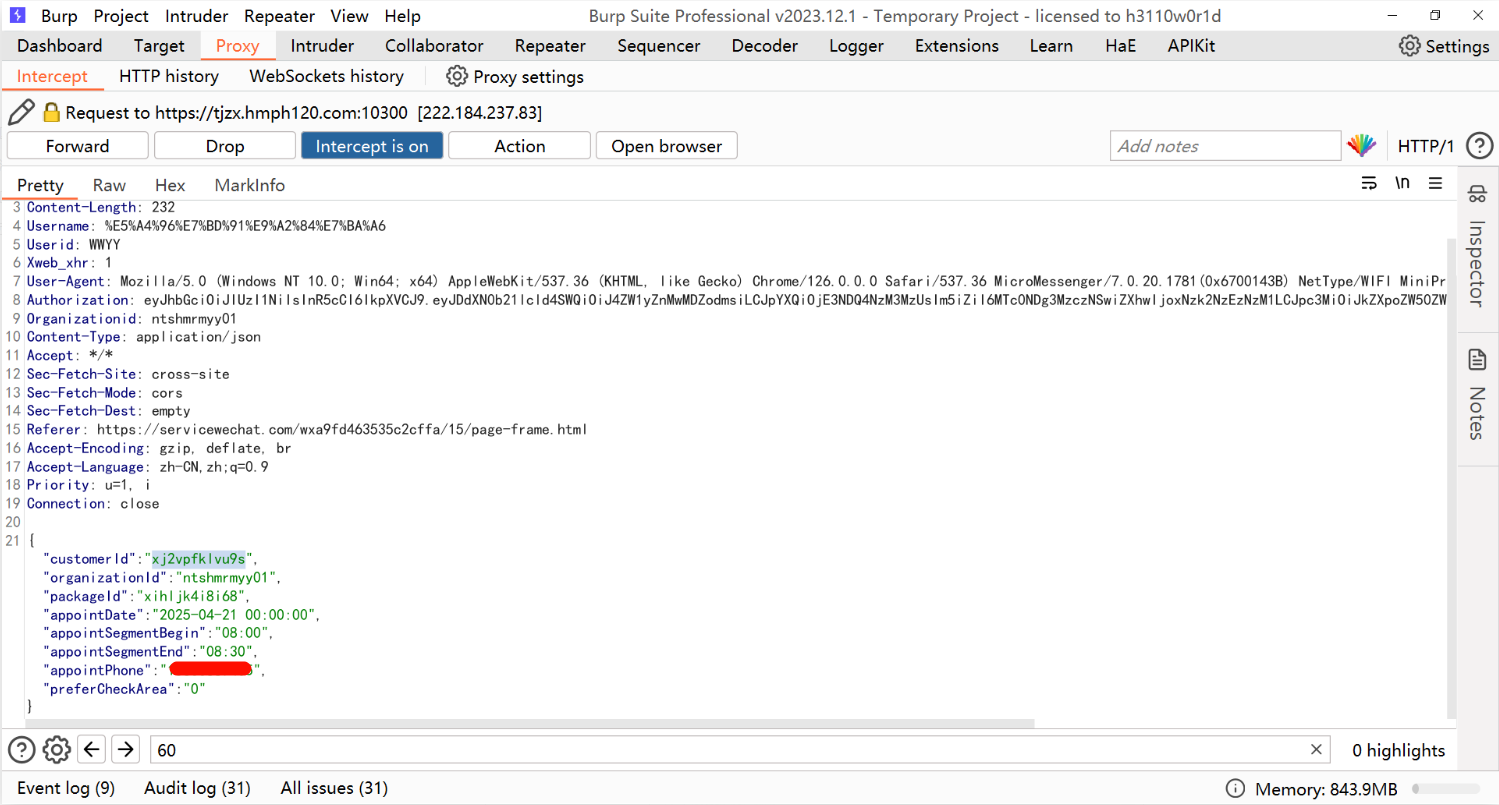
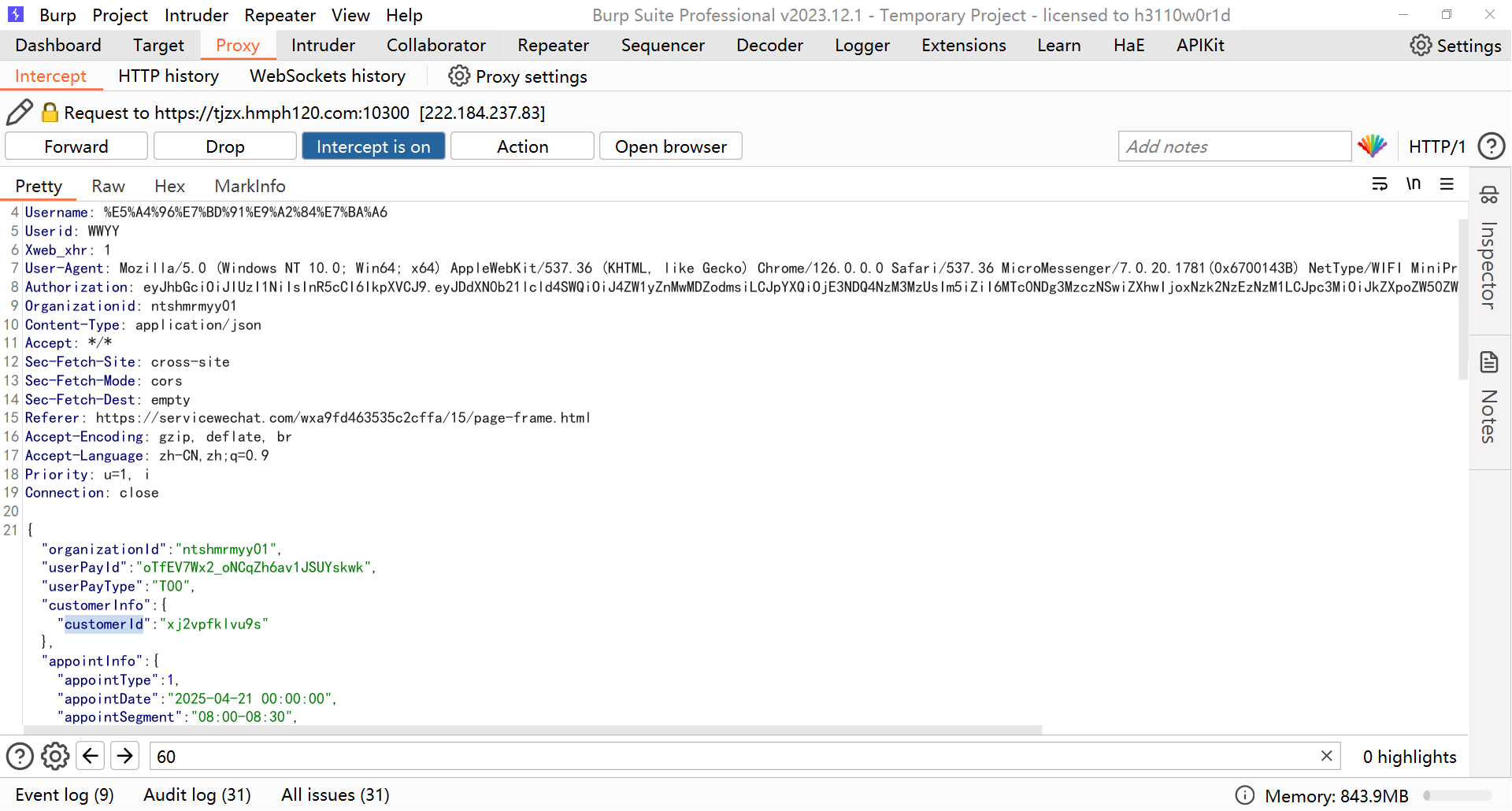
**漏洞地址：**

https://tjzx.hmph120.com:10300/api\_hub/appoint/appoint/save-package-appoint

**漏洞详情：**

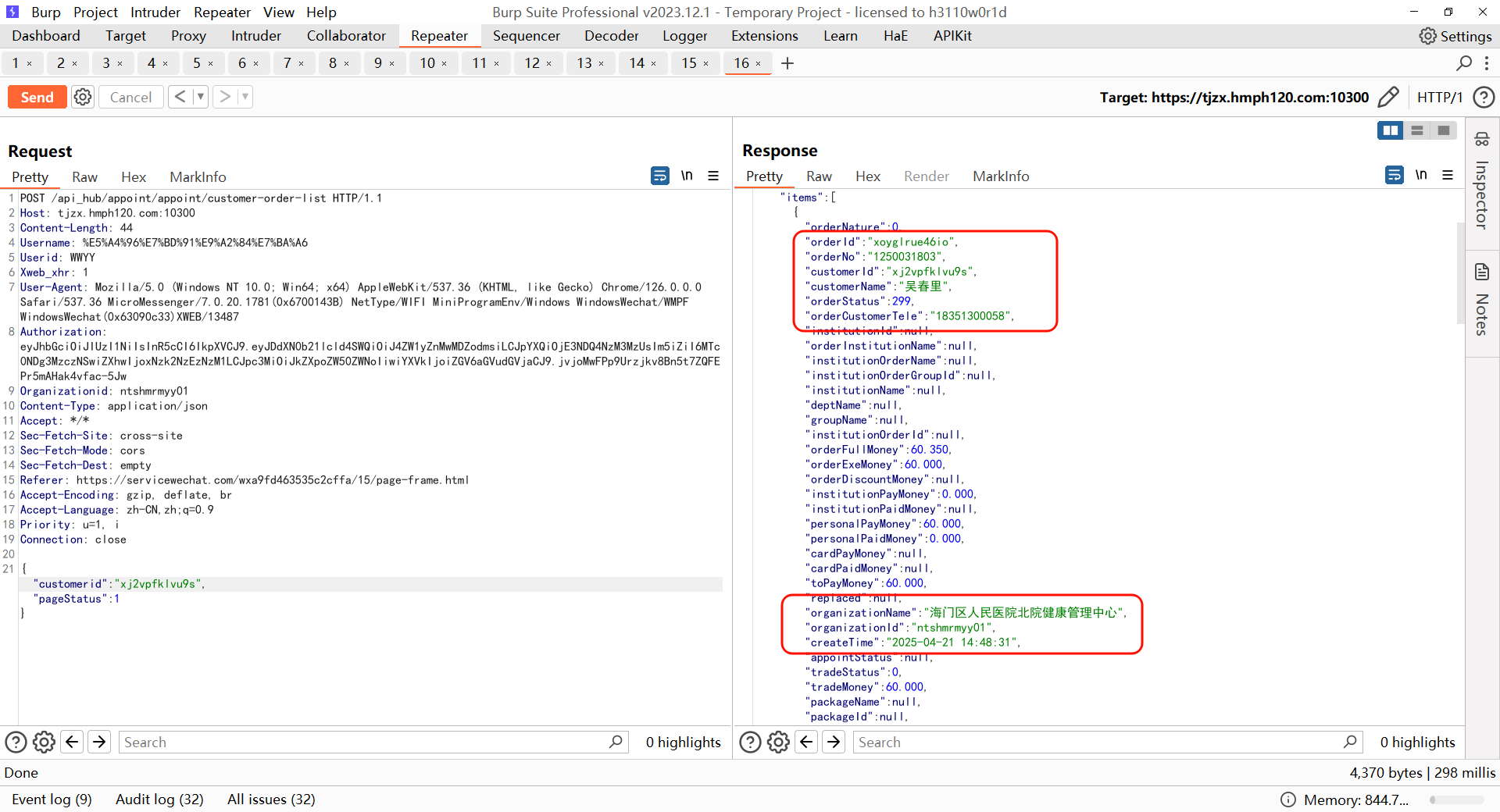


提交订单 修改customerId值



使用越权查看他人订单漏洞查看是否预约成功



**造成的危害：**

垂直越权漏洞会导致低权限用户用来执行高权限用户的功能，获取高权限用户的账号信息，执行高权限用户的操作功能。

**修复建议：**

1. 设置目录访问权限。  
 2. 日常开发中要多留意业务逻辑可能出现的漏洞和水平权限漏洞或者其它未发现的漏洞。  
 3. 鉴权，服务端对请求的数据和当前用户身份做校验;完善基础安全架构，完善用户权限体系。  
 4. 通过修改配置文件，禁止中间件（如IIS、apache、tomcat）的文件目录索引功能。  
 5. 对于后台接口，确保所有 API 接口先经过登录控制器。  
 6. 在验证用户身份权限前不进行任何数据的交互。  
 7. 严格校验当前用户操作与当前登录用户身份权限是否匹配。

* + 1. 南通市海门区人民医院-海门区人民医院健康管理中心小程序-登录验证码爆破导致任意用户登录

**漏洞类型：参数控制缺陷**

**漏洞评级：高**

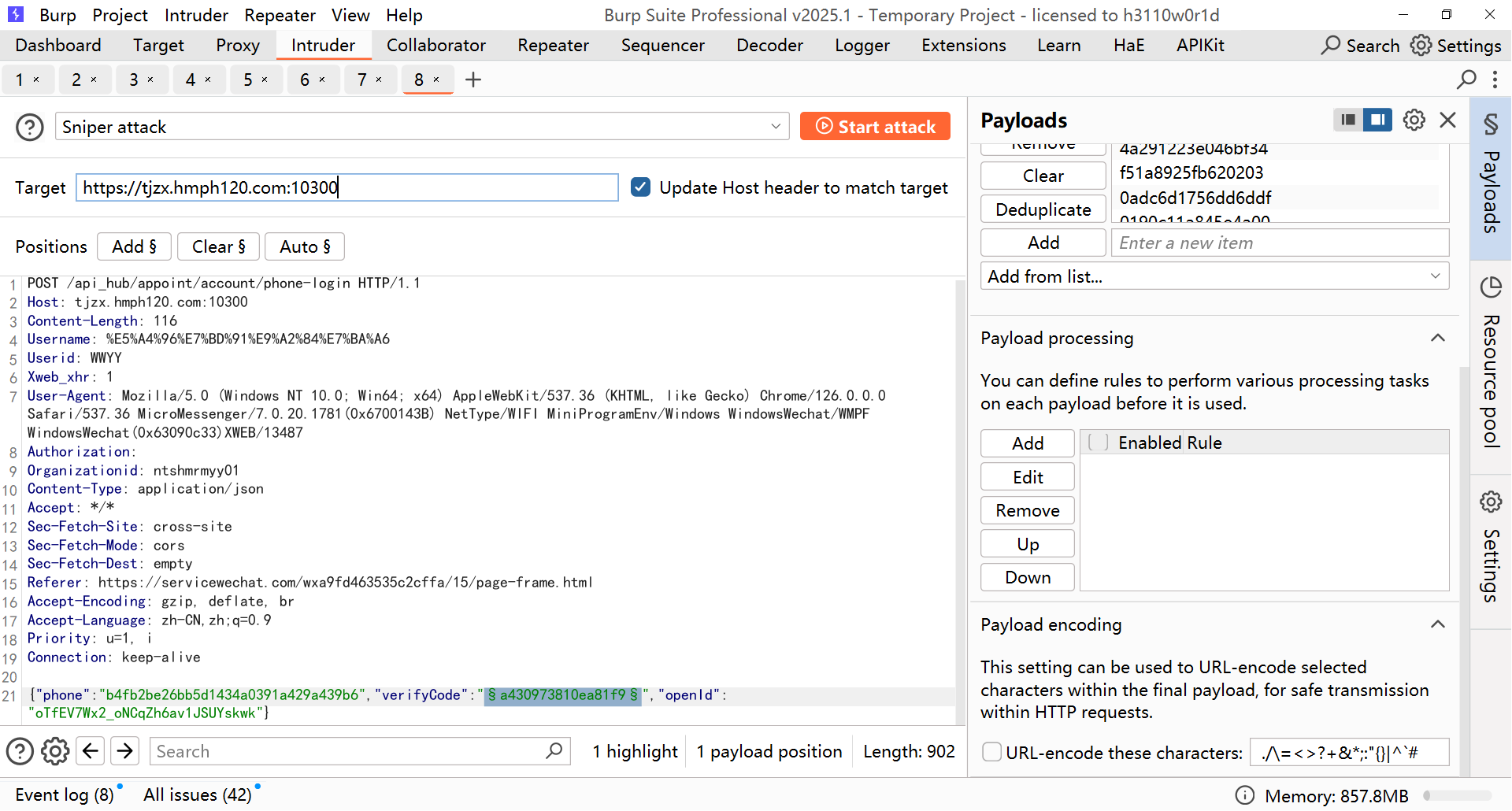
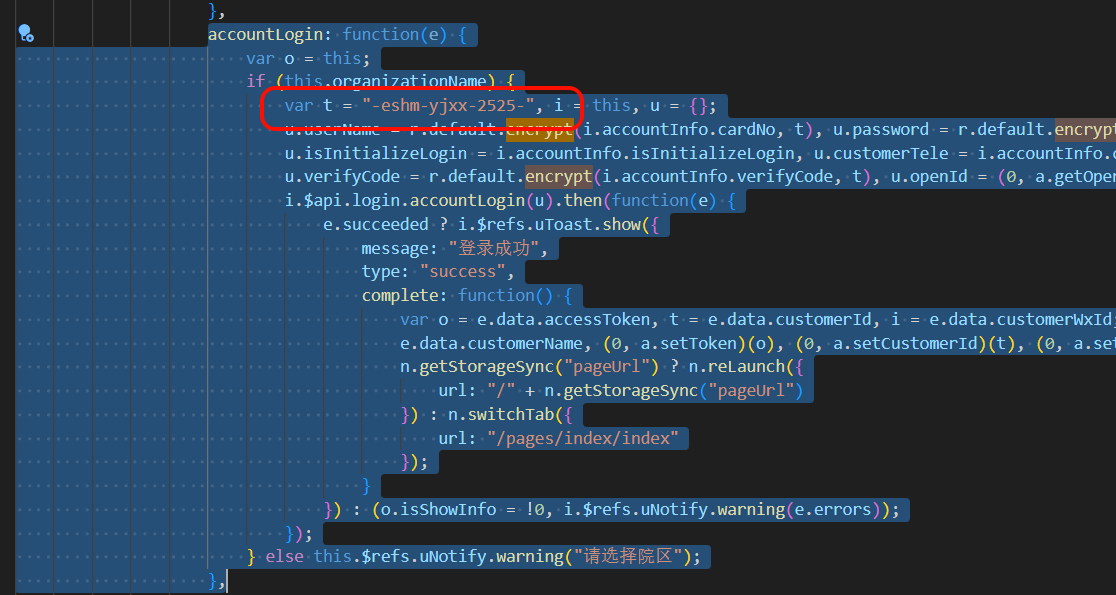
**漏洞地址：**

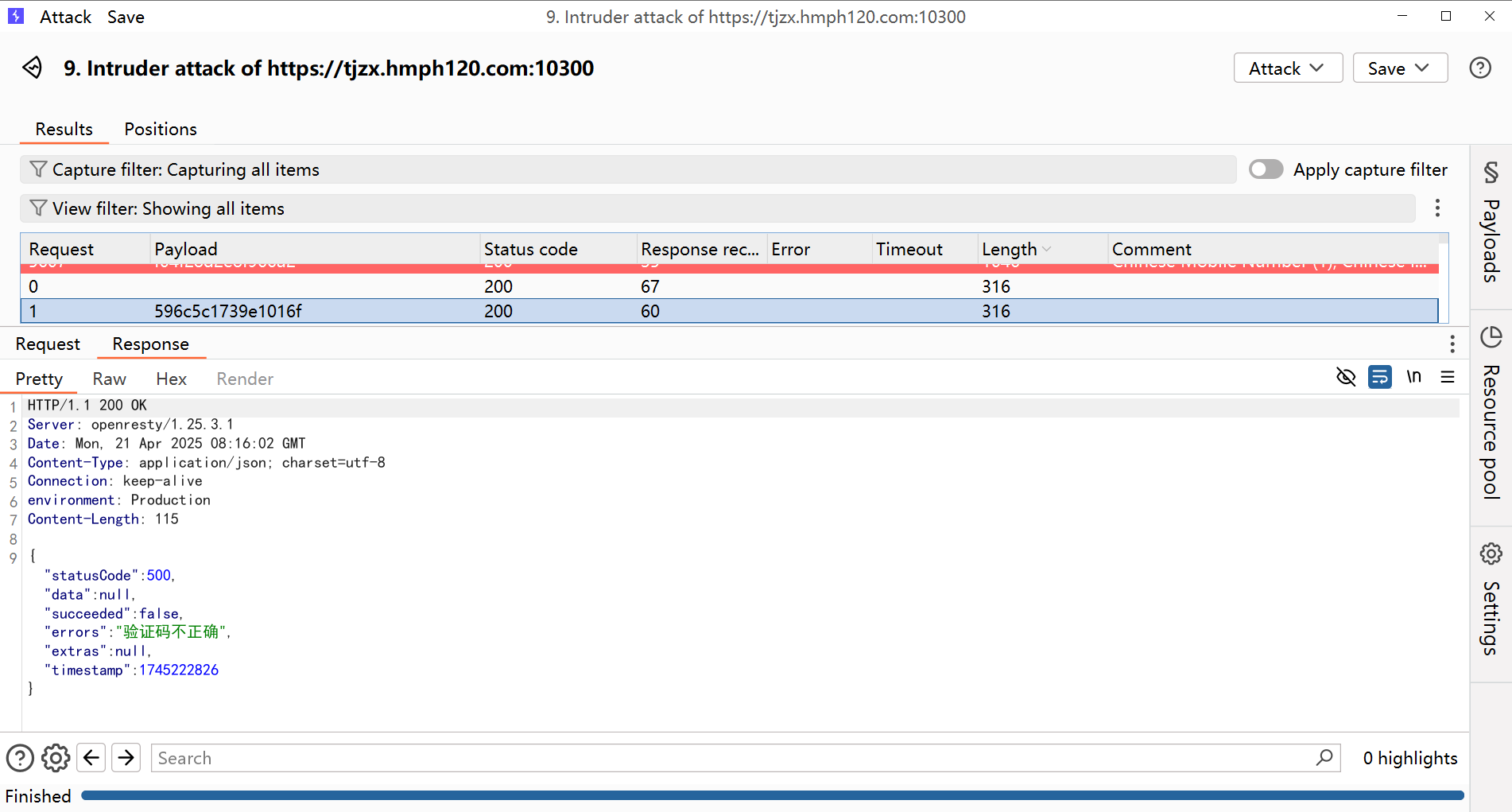
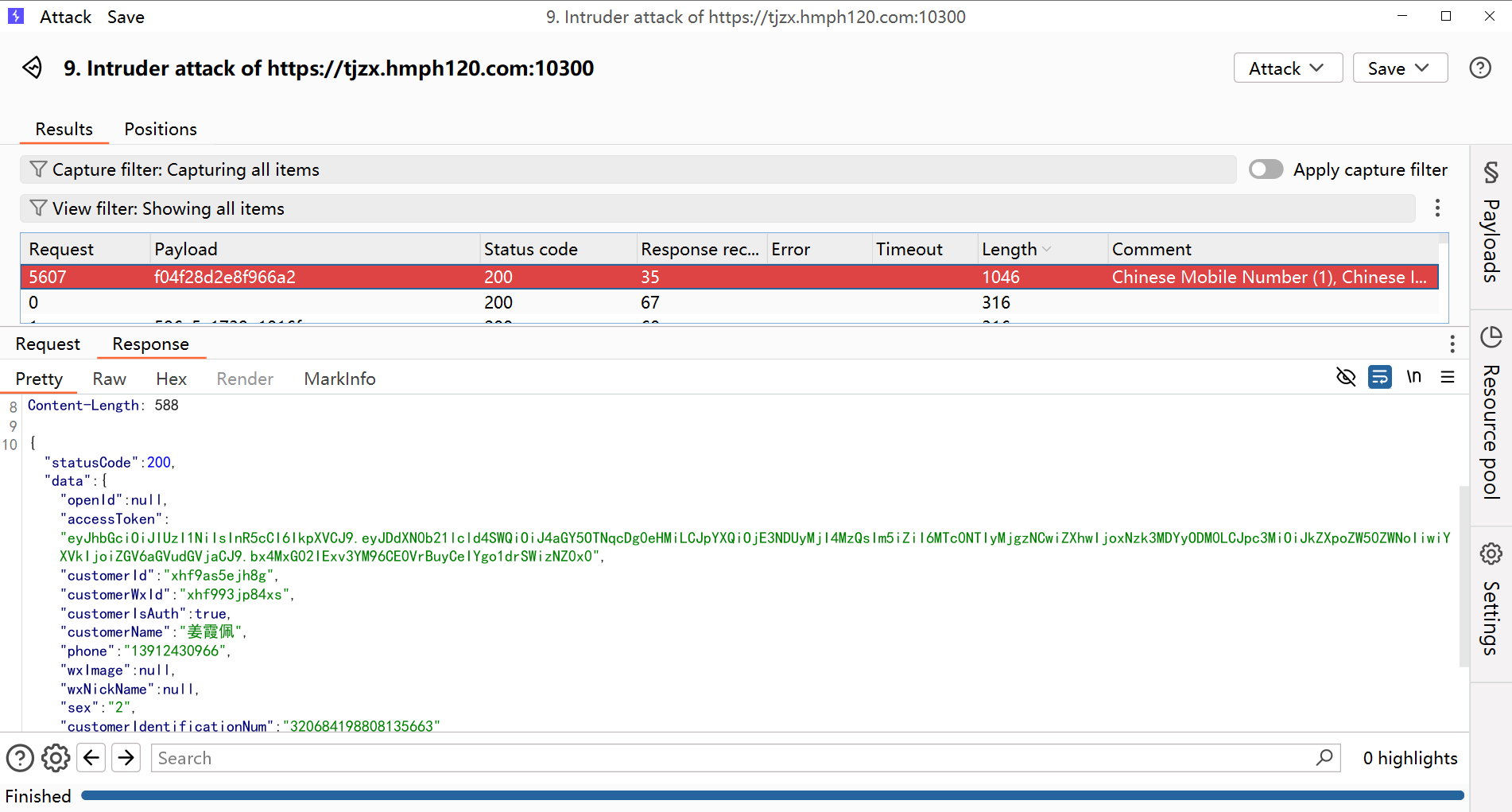
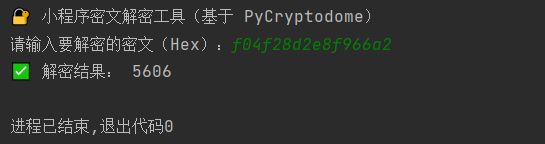
https://tjzx.hmph120.com:10300/api\_hub/appoint/account/phone-login

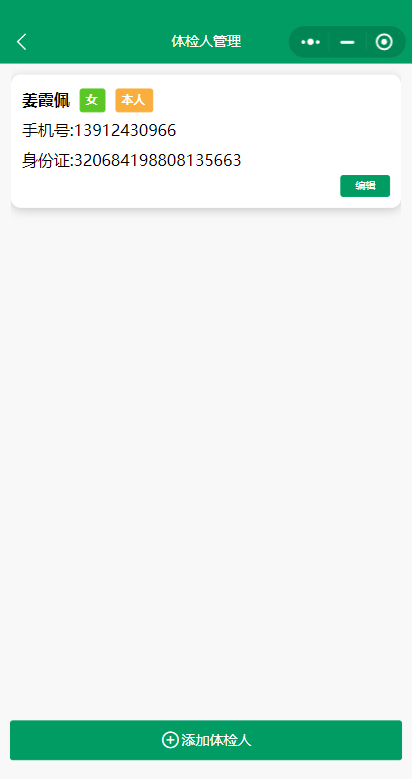
**漏洞详情：**



通过逆向得到加密解密方式，密钥如下

  
将verifyCode值进行遍历

  
  
验证码成功只验证一次  
我们将返回包内容替换为上传成功登录后的可直接登录



**造成的危害：**

攻击者可以重复 post 请求，针对某手机号进行短信轰炸。

**修复建议：**

1. 将短信验证码时间限制判断放在后端进行。  
 2. 同一手机号，60秒内不能重复发送，24小时内总共发送不超过5次。  
 3. 加上 IP 限制，例如某 IP 一小时内连续登录发送 3 次，6 个小时内禁止该 ip 发送。

1. 安全控制建议
   1. 应用控制建议
2. 对网站的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。
3. 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，特别是影响到Web站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。
   1. 主机控制建议
4. 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞。
5. 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
   1. 认证控制建议
6. 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
7. 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的，或者限制为指定范围内 IP 访问。