|  |
| --- |
|  |
| 驻马店市中心医院 |
| 应用系统渗透测试报告 |
|  |
|  |
|  |
|  |
|  |
| 安可信信息技术有限公司 |
| 2023年8月 |

**目 录**

[一 健康管理中心 2](#_Toc144309821)

[1.1 健康管理中心体检预约模块存在逻辑越权漏洞 2](#_Toc144309822)

[二 远秋医学在线考试系统 3](#_Toc144309823)

[2.1 远秋医学在线考试系统考核试卷模块存在逻辑越权漏洞 3](#_Toc144309824)

# 健康管理中心

## 健康管理中心体检预约模块存在逻辑越权漏洞

**漏洞位置：**

http://jktj.zmdszxyy.cn/api/Order/OrderDetail?orderCode=3ccd4bca-9caf-4339-9155-854bf0ddab06

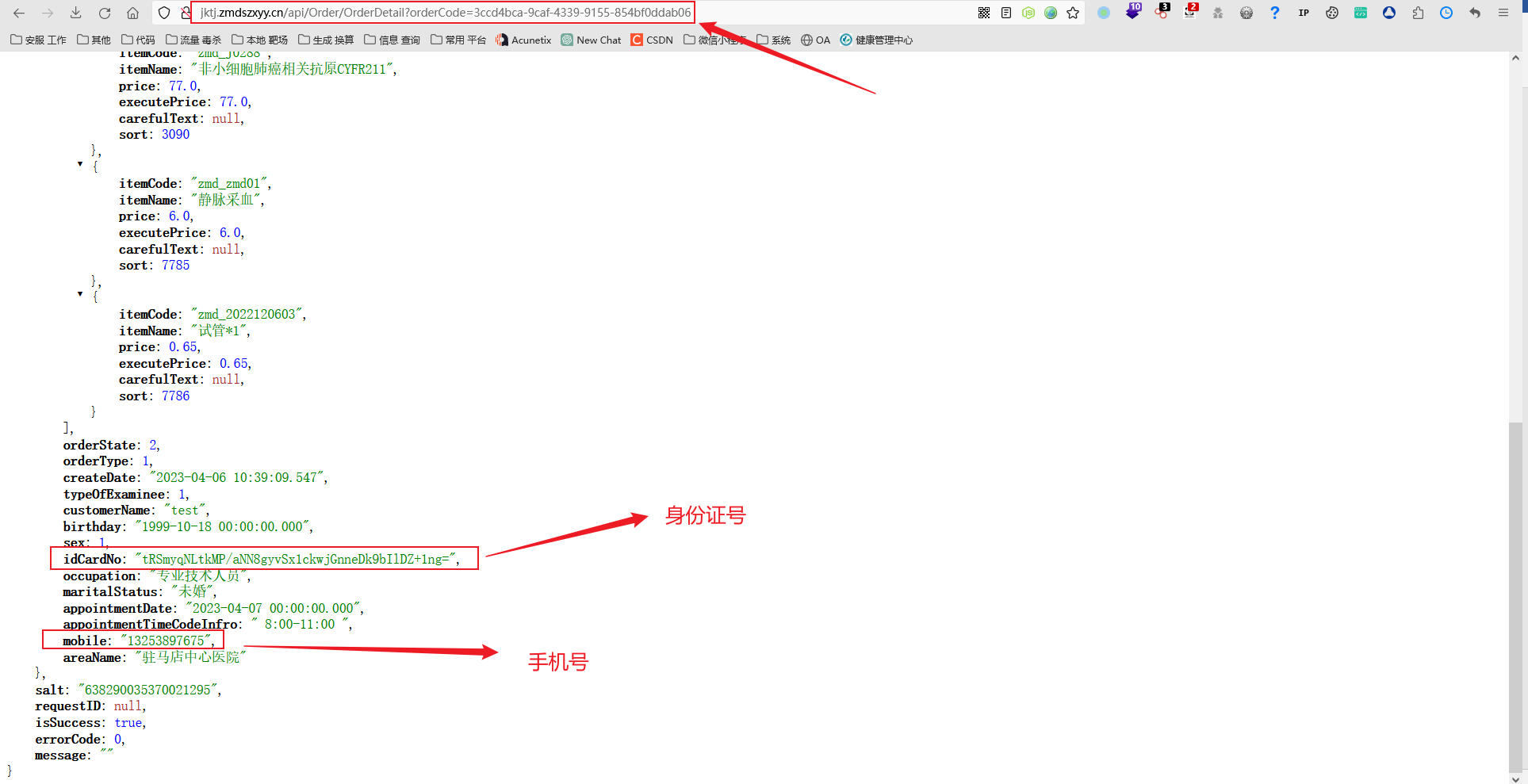
**漏洞等级：**高危

**漏洞描述：**

一个用户一般只能够对自己本身的信息进行增删改查，然而由于后台开发人员的疏忽，没有在信息进行增删改查时候进行用户判断，从而导致可以对其他用户进行增删改查等等操作，利用业务的设计缺陷，获取敏感信息或破坏业务的完整性，攻击者可利用该漏洞获取到任意患者的个人信息和体检信息。

**漏洞复现：**

浏览器直接访问上述URL地址，患者个人敏感信息页面不经过身份识别验证就可在浏览器页面查看，导致患者敏感信息泄露。操作界面如下：



在浏览器页面按F12进入控制台，执行Decrypt命令，解密出患者的身份证号，从而造成患者信息泄露。操作界面如下：



经过以上测试可以证明患者敏感个人信息被泄露，验证健康管理中心系统体检预约功能模块存在逻辑越权漏洞。

**修复建议：**

1、不能只根据用户ID参数去搜索，应进行二次身份验证防止水平越权。

2、可以从用户的加密认证 Cookie 中获取当前用户ID，防止攻击者对其修改。或在Session、Cookie中加入不可预测、不可猜解的User信息。

3、在每个页面加载前进行权限认证，防止垂直越权。

4、对有多步验证的功能模块，需要准确验证上一步是否通过。

# 远秋医学在线考试系统

## 远秋医学在线考试系统考核试卷模块存在逻辑越权漏洞

**漏洞位置：**

http://218.28.245.74:8004/Manage/BrowsePaper.aspx?type=ScaleAnlyer&dfsad=11&id=4492

http://218.28.245.74:8004/Manage/BrowsePaper.aspx?type=PaperBrowser&id=4490

**漏洞等级：**高危

**漏洞描述：**

远秋医学在线考试系统存在越权漏洞，攻击者可以在不登录系统的情况下，任意查看系统中试卷的相关信息，包括试卷查分、成绩分析等两个模块的敏感信息，这将导致敏感信息泄露，甚至当攻击者拥有该权限的用户，可以任意执行操作。

**漏洞复现：**

直接在浏览器中访问以下URL，注意URL中的id参数为本次查询id, 修改这个值即可查看任意用户的试卷与分数信息。

|  |
| --- |
| http://218.28.245.74:8004/Manage/BrowsePaper.aspx?type=ScaleAnlyer&dfsad=11&id=4492 |

访问上述URL，越权获取此用户的试卷信息，可以看到考生姓名、考试时间、考生总分、考试类型、试卷答案与详解等信息。信息界面如下：



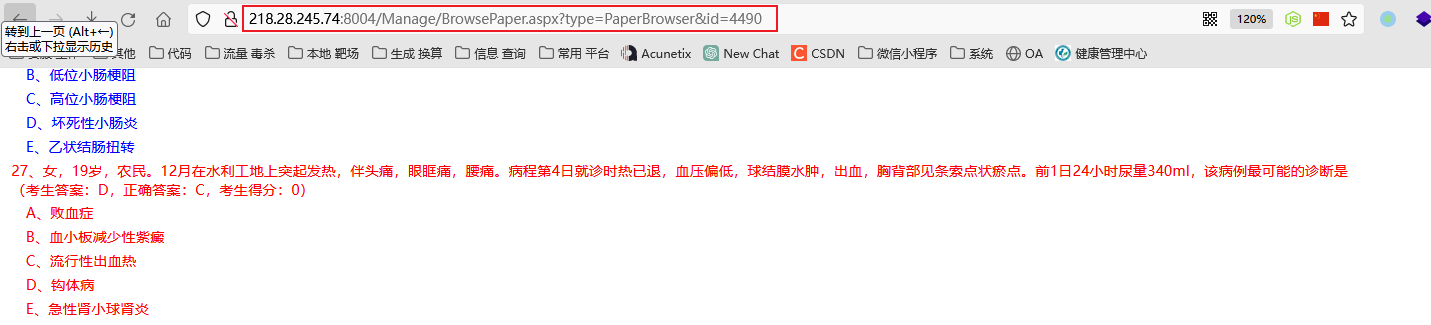


直接在浏览器中访问以下URL，注意URL中的id参数为本次查询id, 修改这个值即可查看任意用户的试卷与分数信息。

|  |
| --- |
| http://192.168.16.106:8002/Manage/BrowsePaper.aspx?type=PaperBrowser&id=4490 |

访问上述URL，越权获取此用户的试卷信息，可以看到考生姓名、考试时间、考生总分、考试类型、试卷答案与详解等信息。信息界面如下：





发现管理员后台界面在线考试功能的试卷差分与成绩分析模块都可以进行越权，经过以上测试验证远秋医学在线考试系统存在逻辑越权漏洞。

**修复建议：**

敏感操作必须先验证操作者的权限，如果操作者权限不足则拒绝操作或重定向至登录页面。