**郑州市中心医院**

**颐健体检导检**

**渗透测试报告**

河南天祺信息安全技术有限公司

1、测试对象与环境

本次渗透测试按约定的测试范围展开测试工作，测试对象如下表所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **测试对象** | **相关资产信息** | **账号** | **密码** |
| 颐健体检导检 | |  | | --- | | 10.20.6.33 | | 10.20.6.35 | | 10.20.6.34 | | 无 | 无 |

2、测试结果综述

### 2.1 渗透测试情况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统名称** | **高危风险** | **中危风险** | **低危风险** | **合计** |
| 颐健体检导检 | 0 | 1 | 0 | 1 |

### 2.2 漏洞统计列表

|  |  |  |
| --- | --- | --- |
| **序号** | **漏洞名称** | **风险级别** |
| 1 | 未授权访问漏洞 | 中危 |

3、测试过程详述

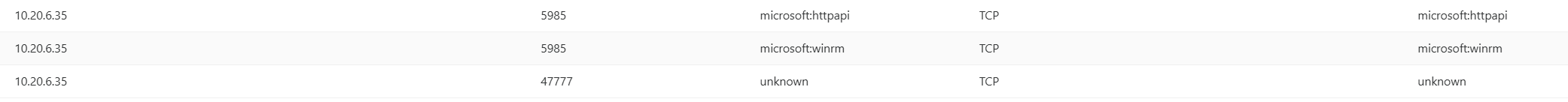
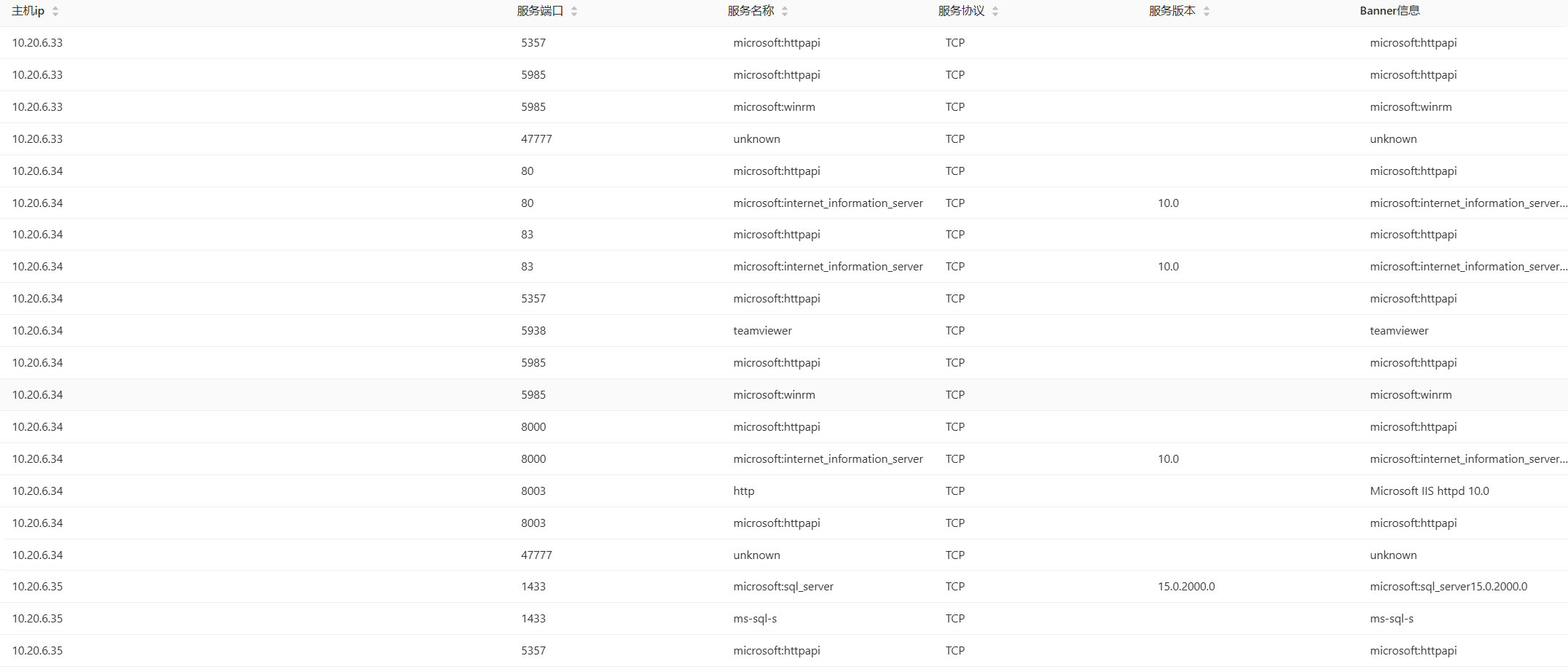


## 基础信息探测

### 开放端口与服务探测

通过使用端口扫描工具对主机在Internet上的端口开放情况进行检查

结果如下图所示：



根据扫描结果，在不影响业务的情况下，建议关闭不必要的端口。

## 测试结果详述

## 3.2.1未授权访问漏洞

**问题描述：**

未授权访问到后台信息。

**风险等级：中危**

**漏洞危害：**

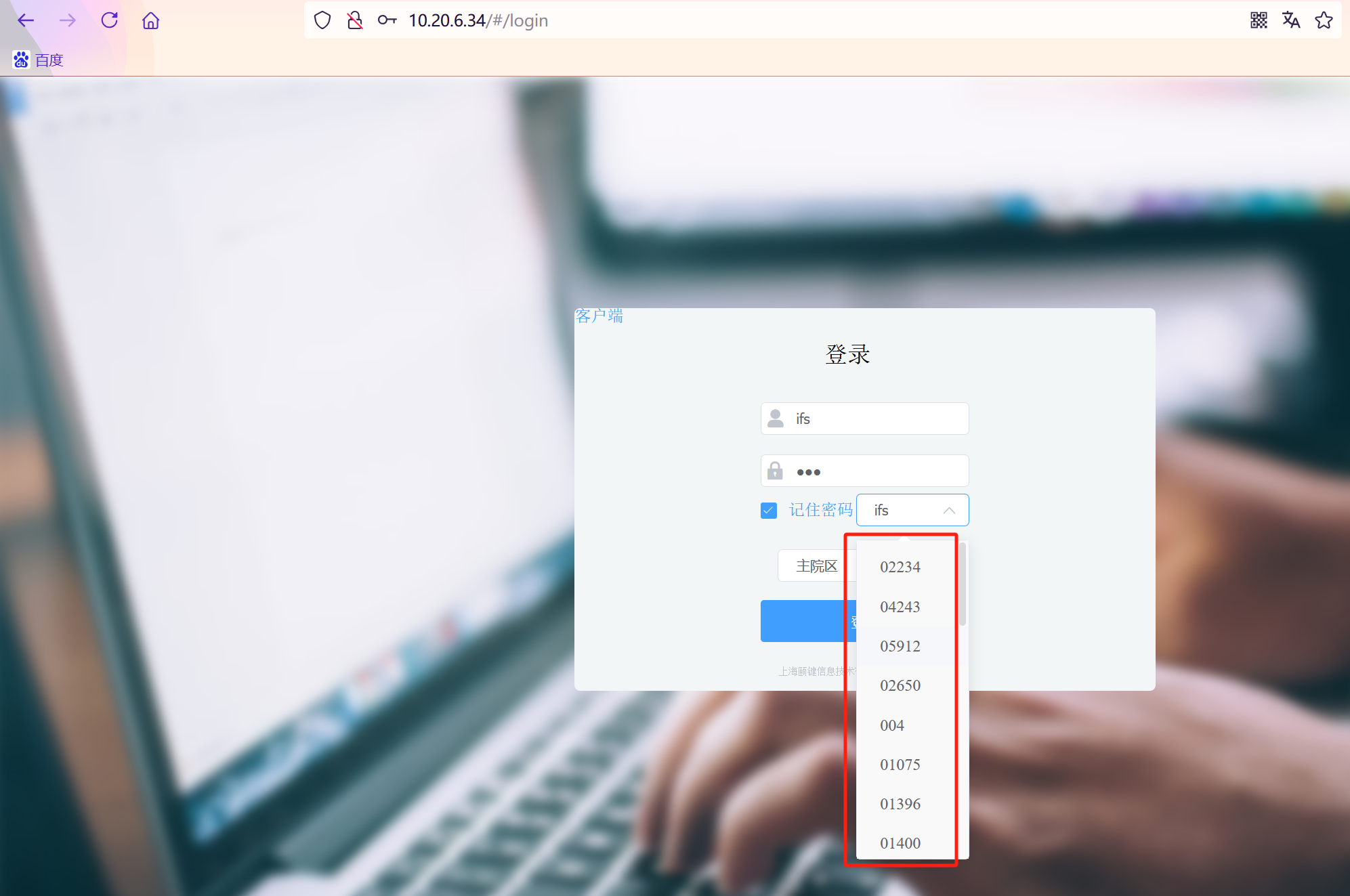
攻击者可未授权获取后台的配置等敏感信息。

**漏洞影响：**

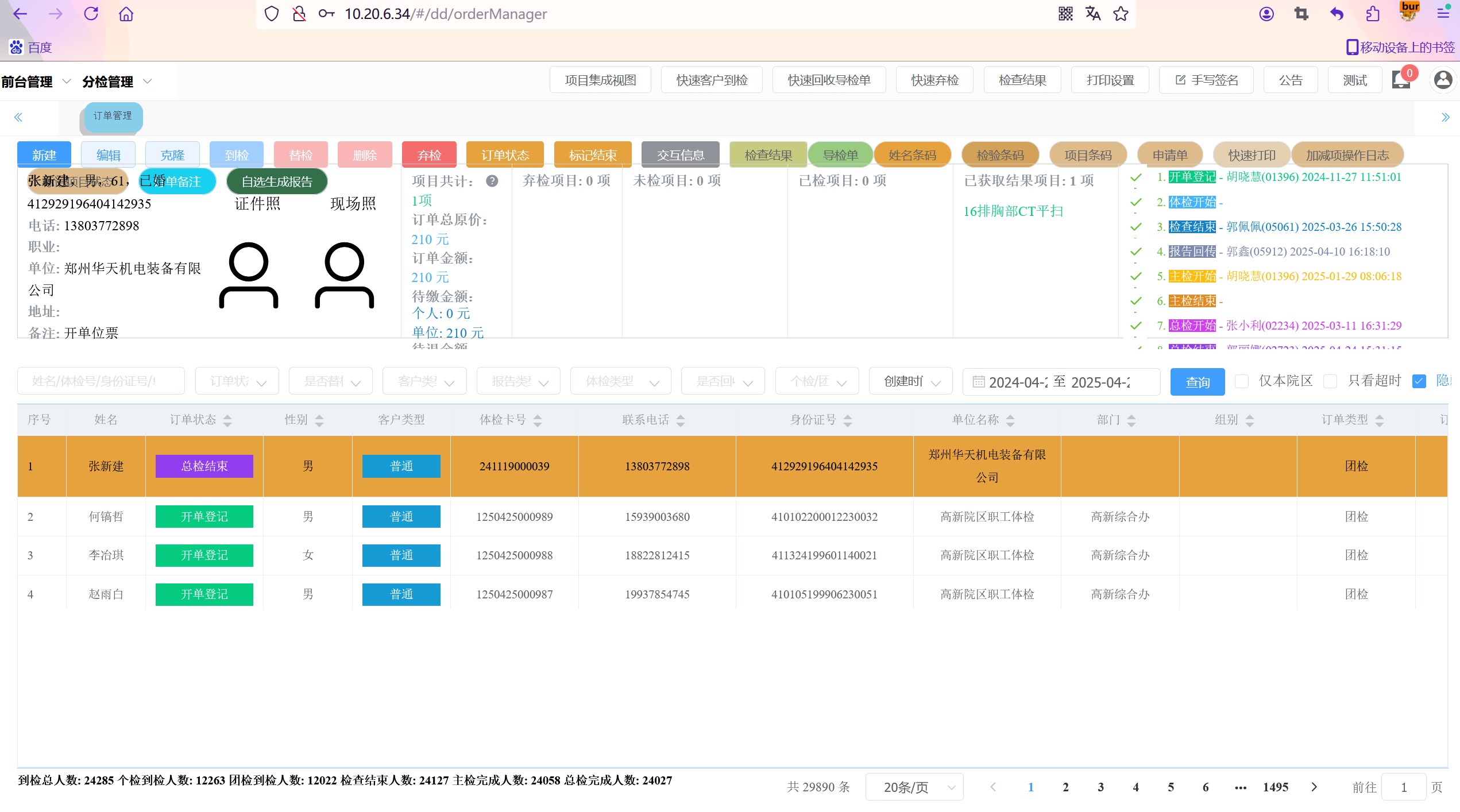
http://10.20.6.34

**漏洞验证：**

http://10.20.6.34/#/login



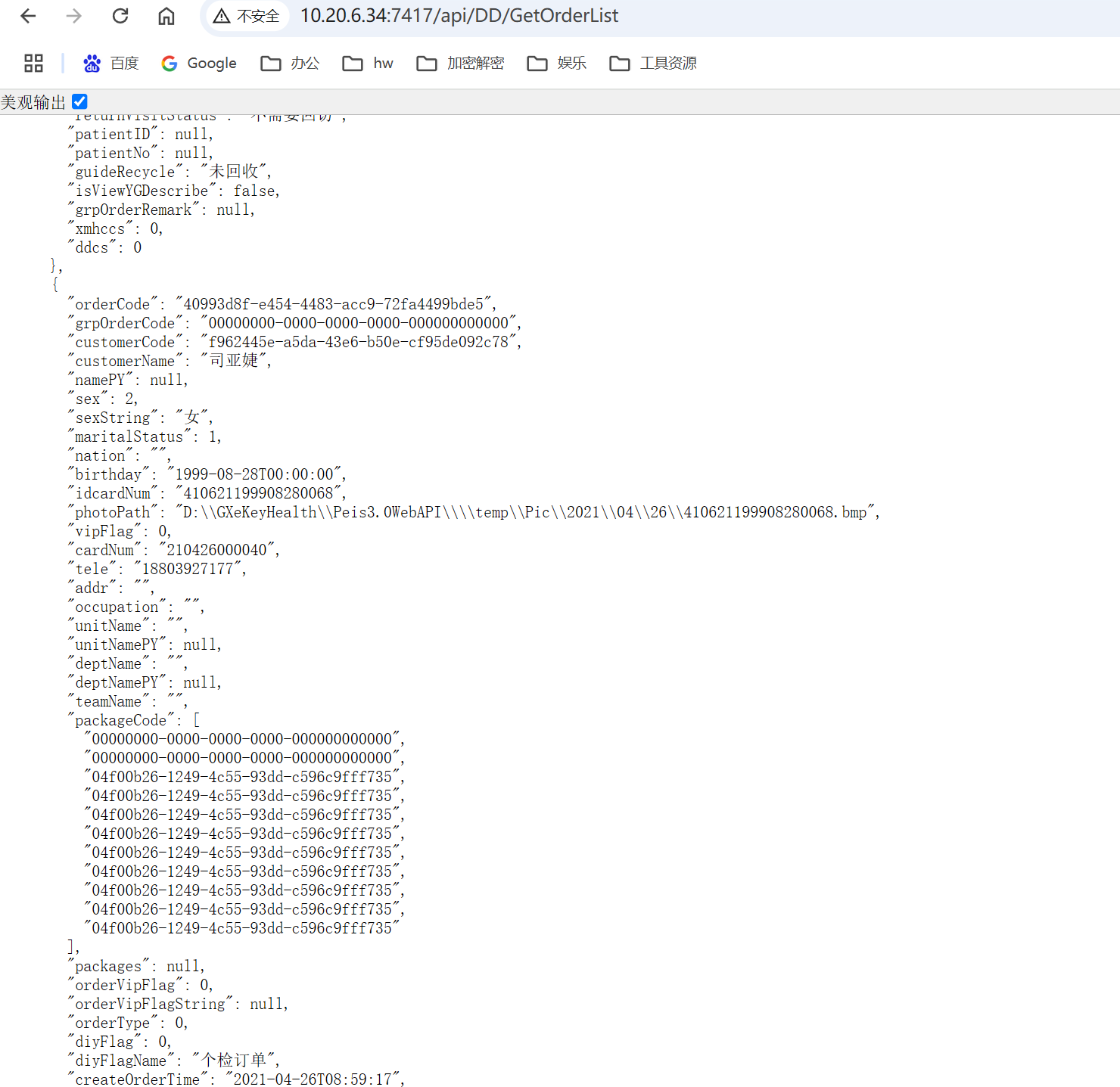
只要点击此处，账号密码会自动输入，点击即可登录



未授权访问

http://10.20.6.34:7417/api/DD/GetOrderList

病人信息泄露



**修复建议：**

增加权限校验机制，升级相关系统版本。

附件、风险程度分级

|  |  |
| --- | --- |
| **漏洞等级** | **漏洞描述** |
| **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。此类风险如高危性质远程缓冲区溢出、SQL注入、关键业务弱口令、验证绕过、未授权的访问、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。此类风险如远程缓冲区溢出、非关键业务弱口令、XSS跨站、敏感信息泄漏等。 |
| **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。 |