

CA - 04月24日

渗透测试报告

报告编号：YJ-SCAN-20250424

2025年04月24日

# 基本信息表

|  |  |
| --- | --- |
| **测试单位** | **上海视岳计算机科技有限公司** |
| **测试对象** | **CA - 04月24日** |
| **测试地址** | **https://tijian.shtrhospital.com/** |
| **测试日期** | **2025-04-23** |
| **审核人员** | **龙宇博** |
| **报告版本** | **V1.0** |
| **报告编号** | **YJ-SCAN-20250424** |
| **编制日期** | **2025.04.24** |

**目录**

[基本信息表 2](#_Toc129680808)

[一、 任务信息 5](#_Toc129680809)

[二、 目标信息 6](#_Toc129680810)

[1. 目标首页 6](#_Toc129680811)

[2. 开放端口 6](#_Toc129680812)

[三、 漏洞综述 7](#_Toc129680813)

[1. 漏洞统计 7](#_Toc129680814)

[2. 测试项目 8](#_Toc129680815)

[3. 漏洞列表 8](#_Toc129680816)

[四、 漏洞详情 8](#_Toc129680817)

[五、 附录 9](#_Toc129680819)

[1. 原理说明 9](#_Toc129680821)

[2. 工具说明 9](#_Toc129680822)

[3. 流程说明 10](#_Toc129680823)

[4. 风险规避 11](#_Toc129680824)

[5. 版权声明 12](#_Toc129680825)

[6. 标准规范 13](#_Toc129680826)

[7. 等级标准 13](#_Toc129680827)

[8. CCRC资质 15](#_Toc129680828)

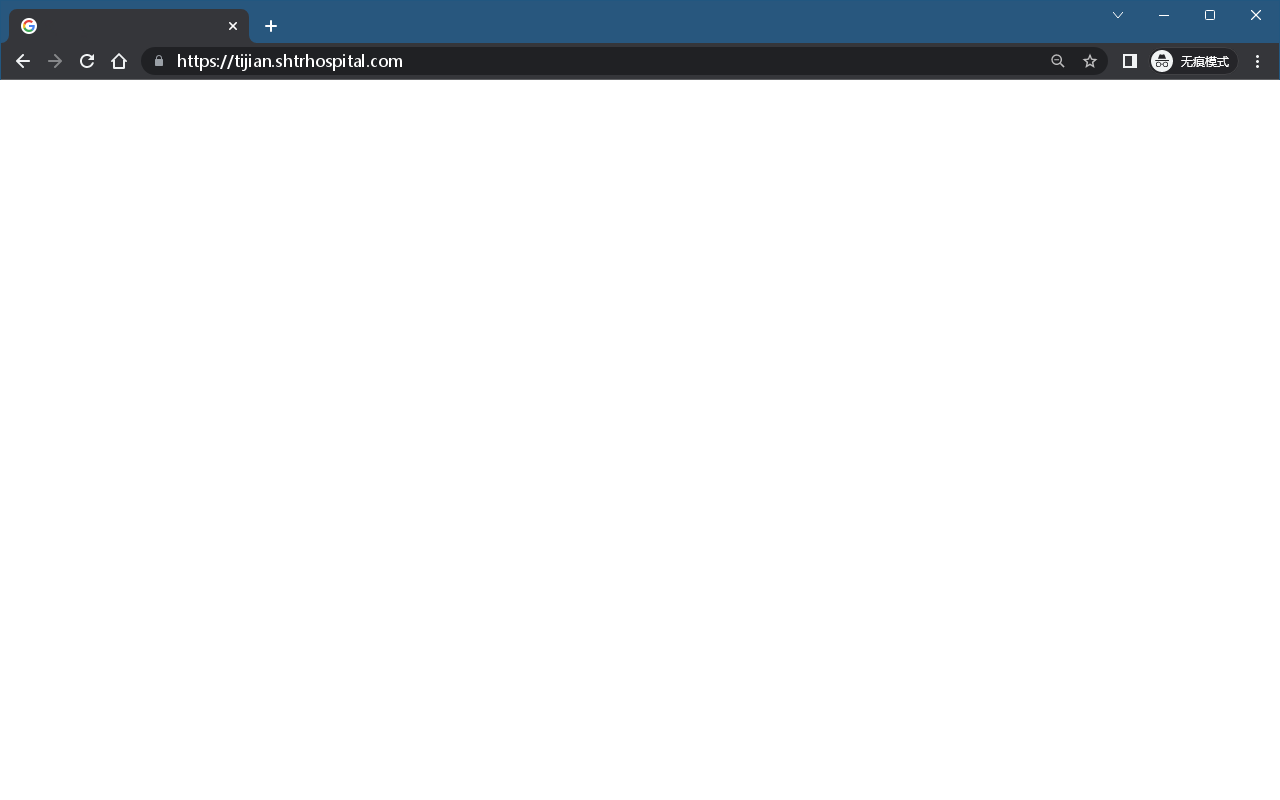
[9. ISO27001 16](#_Toc129680829)

# 任务信息

|  |  |
| --- | --- |
| **任务编号** | 23 |
| **任务名称** | CA - 04月24日 |
| **渗透目标** | https://tijian.shtrhospital.com/ |
| **自动登录** | 不需要 |
| **渗透模板** | ALL |
| **端口模式** | 默认端口 |
| **代理设置** | 关闭 |
| **开始时间** | 2025-04-23 14:07:21 |
| **结束时间** | 2025-04-23 16:13:39 |
| **渗透时长** | 2小时7分钟 |
| **完成进度** | 100% |

# 目标信息

## 目标首页



**系统信息**

|  |  |
| --- | --- |
| **IP类型** |  |
| **操作系统** |  |

## 开放端口

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP** | **协议** | **端口** | **服务** | **建议** |
| 101.231.113.13 | https | 443 | https | / |

# 漏洞综述

## 漏洞统计

本网站风险级别：高危。

本次渗透测试共发现4个漏洞，其中高危漏洞1个，中危漏洞1个，低危漏洞2个，信息0个。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **风险级别** | 高危 | 中危 | 低危 | 信息 |
| **漏洞数量** | 1 | 1 | 2 | 0 |



## 测试项目

|  |  |  |  |
| --- | --- | --- | --- |
| **测试项目** | **测试内容** | **测试记录** | **测试结果** |
| **Platform** | 远程命令执行 | 已测试 | / |
| 系统脆弱性 | 已测试 | / |
| 中间件 | 已测试 | 存在脆弱性 |
| 端口扫描 | 已测试 | 存在脆弱性 |
| 反序列化漏洞 | / | / |
| **Web** | 注入攻击 | 已测试 | / |
| XSS | 已测试 | / |
| 证书类 | 已测试 | 存在脆弱性 |
| 常规脆弱性 | 已测试 | 存在脆弱性 |
| **其他** | 弱口令 | 已测试 | / |
| 拒绝服务 | 已测试 | / |
| 信息泄露 | 已测试 | 存在脆弱性 |
| 逻辑漏洞 | 已测试 | / |
| 权限控制 | 已测试 | / |
| 管理后台泄露 | 已测试 | / |
| 子域名 | 已测试 | / |

## 漏洞列表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **漏洞名称** | **漏洞级别** | **整改结果** |
| **1** | 信息泄露之备份文件泄露（1个） | 高危 | / |
| **2** | 检查Apache Tomcat默认文件（1个） | 中危 | / |
| **3** | Apache Tomcat SEoL (8.5.x)（1个） | 低危 | / |
| **4** | 发现不必要的http响应头（1个） | 低危 | / |

# 漏洞详情



## 1 信息泄露之备份文件泄露一高危（1个）

|  |  |
| --- | --- |
| **漏洞名称** | 信息泄露之备份文件泄露 |
| **漏洞等级** | **高危** |
| **漏洞影响** | 1. 漏洞URL: https://tijian.shtrhospital.com/1.rar  漏洞参数: <无> |
| **漏洞说明** | 请求可能存在的备份文件，一般网站备份文件可能会包含敏感信息，程序源代码等，存在一定危害! |
| **解决方案** | [1] 删除不必要的备份文件 [2] 备份网站数据后应当转移到非web目录的地方 |
| **测试信息** | https://tijian.shtrhospital.com/1.rar |

## 2 检查Apache Tomcat默认文件一中危（1个）

|  |  |
| --- | --- |
| **漏洞名称** | 检查Apache Tomcat默认文件 |
| **漏洞等级** | **中危** |
| **漏洞影响** | 1. 漏洞URL: 101.231.113.13  漏洞参数: max\_attachments\_exceeded: True ports:  8088 / tcp / www:  hostname: 101.231.113.13 severity: 2 plugin\_output:  The server is not configured to return a custom page in the event of a client requesting a non-existent resource. This may result in a potential disclosure of sensitive information about the server to attackers. |
| **漏洞说明** | 检查 Apache Tomcat 的默认文件。 |
| **解决方案** | 在远程 Apache Tomcat 服务器上安装了默认错误页面、默认索引页面、示例 jsp 和/或示例 servlet。应该删除这些文件，因为它们可能帮助攻击者发现有关远程 Tomcat 安装或主机本身的信息。 |
| **测试信息** | max\_attachments\_exceeded: True ports:  8088 / tcp / www:  hostname: 101.231.113.13 severity: 2 plugin\_output:  The server is not configured to return a custom page in the event of a client requesting a non-existent resource. This may result in a potential disclosure of sensitive information about the server to attackers. |

## 3 Apache Tomcat SEoL (8.5.x)一低危（1个）

|  |  |
| --- | --- |
| **漏洞名称** | Apache Tomcat SEoL (8.5.x) |
| **漏洞等级** | **低危** |
| **漏洞影响** | 1. 漏洞URL: 101.231.113.13  漏洞参数: max\_attachments\_exceeded: True ports:  8088 / tcp / www:  hostname: 101.231.113.13 severity: 1 plugin\_output:   URL : http://101.231.113.13:8088/  Installed version : 8.5.100  Security End of Life : March 31, 2024  Time since Security End of Life (Est.) : >= 1 month |
| **漏洞说明** | According to its version, Apache Tomcat is 8.5.x. It is, therefore, no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. |
| **解决方案** | Upgrade to a version of Apache Tomcat that is currently supported. |
| **测试信息** | max\_attachments\_exceeded: True ports:  8088 / tcp / www:  hostname: 101.231.113.13 severity: 1 plugin\_output:   URL : http://101.231.113.13:8088/  Installed version : 8.5.100  Security End of Life : March 31, 2024  Time since Security End of Life (Est.) : >= 1 month |

## 4 发现不必要的http响应头一低危（1个）

|  |  |
| --- | --- |
| **漏洞名称** | 发现不必要的http响应头 |
| **漏洞等级** | **低危** |
| **漏洞影响** | 1. 漏洞URL: https://tijian.shtrhospital.com  漏洞参数: Server or X-Powered-By |
| **漏洞说明** | 出于安全和隐私考虑，Web 页面中不应出现 Http 响应头，例如“Server”、“X-Powered-By”、“X-AspNetMvc-Version”和“X-AspNet-Version”。 “Server”头是通常在服务器每次将响应发送到客户端时缺省添加的头。 “X-Powered-By”头是在服务器每次将响应发送到客户端时可能缺省添加的头。 这些添加的头可能会泄露有关内部服务器软件版本和类型的敏感信息，从而使攻击者可以对其进行指纹识别并使用有针对性的漏洞进行攻击。此外，在公布新的漏洞后，服务器很可能会受到该漏洞的攻击。 |
| **解决方案** | 配置服务器，从要发送给所有传出请求的内容中删除缺省“服务器”头. |
| **测试信息** |  |

# 附录



## 原理说明

1. 渗透测试过程主要依据现今已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行可控制、非破坏性质的攻击性测试。
2. 本次渗透测试基于线上环境，考虑到对业务的影响以及测试代码对数据库造成垃圾数据的可能性，选用测试代码为保守基础代码与人工智能AI测试。
3. 本次渗透测试模式属于黑盒测试，即测试工具在主动探索目标网络环境的情况下，以某一URL或IP地址为目标，尝试突破其网站/网络的测试。类似于一次真实的黑客攻击。

## 工具说明

|  |  |
| --- | --- |
| **工具名称** | **岳戟** |
| **工具用途** | **AI自动化渗透测试漏洞检测** |
| **相关信息** | **https://chinashiyue.cn/** |

## 流程说明

* **方案制定：**

在获取到甲方单位的授权许可后，才进行渗透测试的实施。并且将实施范围、方法、时间、人员等具体的方案与甲方单位进行交流，并得到甲方单位的认同。在测试实施之前，会做到让甲方单位对渗透测试过程和风险的知晓， 使随后的正式测试流程都在甲方单位的控制下。

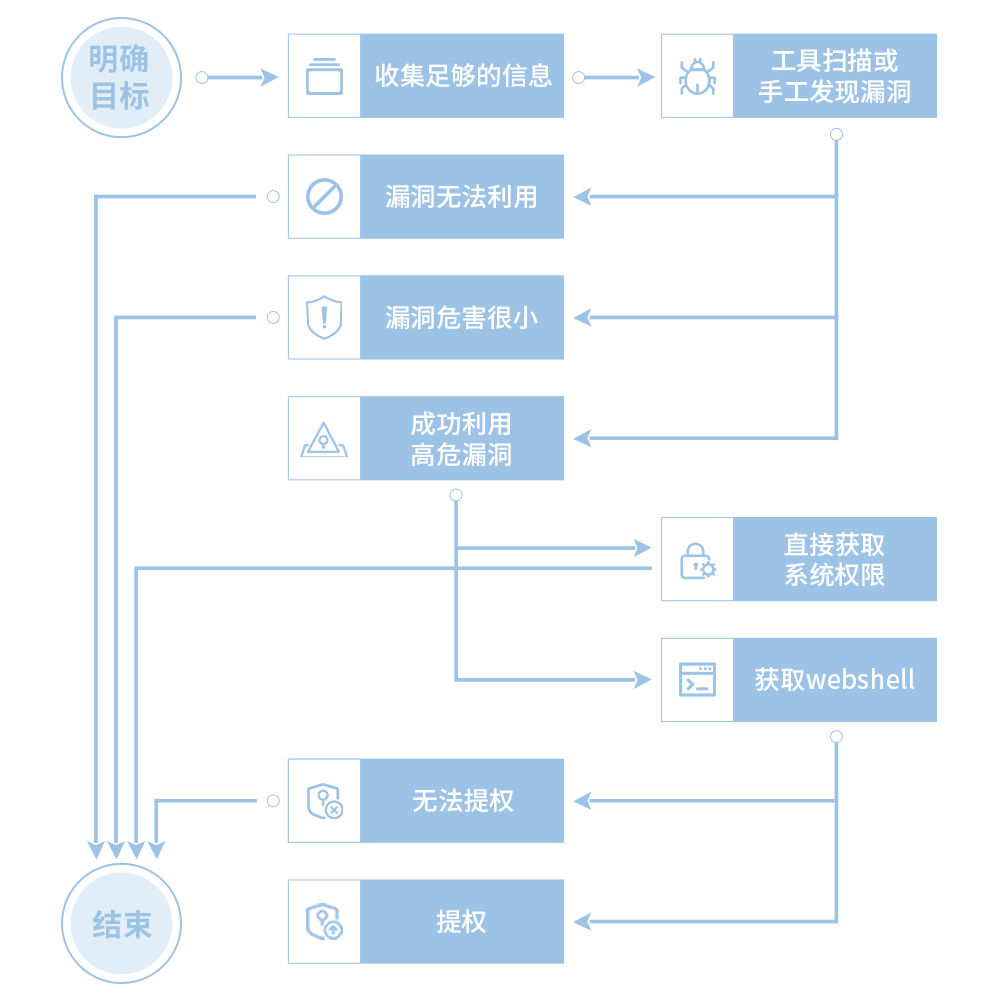
* **信息收集：**

包括：操作系统类型指纹收集；网络拓扑结构分析；端口扫描和目标系统提供的服务识别等。

* **测试实施：**

模拟攻击者利用服务器配置不当或应用程序脆弱性进行的模拟攻击行为。我司采用一套强大的专业工具及有效的安全评估测试方法来发现将会导致信息泄露、数据篡改等问题的脆弱性。

具体测试流程如下图所示：



## 风险规避

在渗透测试过程中，尽管测试人员会尽量避免做影响正常业务运行的操作，也会实施风险规避的计策，但是由于测试过程变化多端，渗透测试服务仍然有可能对网络、系统运行造成一定不同程度的影响，严重的后果是可能造成服务停止， 甚至是宕机。比如渗透人员实施系统权限提升操作时，突遇系统停电，再次重启时可能会出现系统无法启动的故障等。因此，我们会在渗透测试前与甲方单位详细讨论渗透方案，并采取如下多条策略来规避渗透测试带来的风险。

* **时间策略：**

为减轻渗透测试造成的压力和预备风险排除时间，一般的安排测试时间在业务量不高的时间段。

* **测试策略：**

 为了防范测试导致业务的中断，可以不做一些拒绝服务类的测试。非常重要的系统不建议做深入的测试，避免意外崩溃而造成不可挽回的损失；具体测试过程中，最终结果可以由测试人员做推测，而不实施危险的操作步骤加以验证等。

* **备份策略：**

为防范渗透过程中的异常问题，测试的目标系统需要事先做一个完整的数据备份，以便在问题发生后能及时恢复工作。对于核心业务系统等不可接受可能风险的系统的测试，可以采取对目标副本进行渗透的方式加以实施。这样就需要完整的复制目标系统的环境：硬件平台、操作系统、应用服务、程序软件、业务访问等；然后对该副本再进行渗透测试。

* **应急策略：**

测试过程中，如果目标系统出现无响应、中断或者崩溃等情况，我们会立即中止渗透测试，并配合系统管理员进行修复处理等。 在确认问题、修复系统、 防范此故障再重演后，经甲方单位方同意才能继续进行其余的测试。

* **沟通策略：**

测试过程中，确定系统管理员的联系方式，便于及时沟通并解决工程中的难点。

## 版权声明

1. 本文中出现的截图、测试内容信息等内容，除另有特别注明，版权均属上海市同仁医院所有，受到有关产权及版权法保护。任何个人、机构未经该公司的书面授权许可，不得以任何方式复制或引用本文的任何片断。
2. 本文档为系统渗透测试服务工作所提供的报告，用于说明在渗透测试工作过程中发现的问题。
3. 信息安全是一个动态过程，以上结论只适用于截止此报告生成的渗透测试阶段之内。随时间迁移，有可能会产生、发现新的安全问题，本报告结论可能不再适用。
4. 本次安全评估测试系通过internet链路进行，在非相同的防护措施下可能存在测试结论不同的情况，但漏洞仍真实存在。故本次报告的安全性评估仅在同样的防护措施和同样的入侵环境生效。

## 标准规范

本次渗透测试主要参考以下标准和规范：

GB/T 30279-2020 《信息安全技术 网络安全漏洞分类分级指南》

GB/T 28458-2020 《信息安全技术 网络安全漏洞标识与描述规范》

OWASP Top 10-2021

## 等级标准

|  |  |
| --- | --- |
| **风险等级** | **描述** |
| **高危** | 风险可直接威胁到网络、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露。此类风险如高危性质远程缓冲区溢出、SQL注入、XSS跨站、关键业务弱口令、验证绕过、未授权的访问、源代码泄露、文件包含等漏洞。 |
| **中危** | 风险存在一定的危害性，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HTML未受CSRF保护、网站目录存在备份文件、文件上传过滤不严、路径遍历、配置缺陷等漏洞。 |
| **低危** | 风险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，在渗透测试中通常会为进一步的渗透产生辅助性作用。例如IIS开启了Webdav支持、登录页面可以暴力破解等漏洞。 |
| **信息** | 风险存在最低的危害性，通常并不能被直接利用以入侵系统，黑客往往会利用信息类的漏洞来获取系统相关信息，为进一步入侵提供便利。 |

## CCRC资质



## ISO27001

