

**网站漏洞**

**扫描报告**

Website Security Vulnerability Scanning Report

**山东大学齐鲁医院健康管理中心网站**

**风险等级：中危**

杭州安恒信息技术股份有限公司

2024年01月01日

# 概要信息

## 扫描对象

|  |  |
| --- | --- |
| **网站名称** | **山东大学齐鲁医院健康管理中心网站** |
| **网站URL** | https://ctzx.qiluhospital.com |
| **监测域名** | ctzx.qiluhospital.com |
| **结束状态（最近一次)** | **正常结束** |
| **域名注册有效期** | 2003-04-22 - 2022-04-22 |
| **主办单位名称（性质）** | **山东大学齐鲁医院** |
| **主办单位性质** | **事业单位** |
| **ICP备案号** | **鲁ICP备10007518号-1** |

## 扫描概要

本报告由SaaS云监测平台制作，采用web安全检查后得出的扫描报告，属于内部资料，请进行妥善管理。

本报告共扫描1个网站，共发现web安全漏洞14个，其中0个紧急，0个高危，1个中危，13个低危。

## 网站风险分布

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞风险总数14 | | | |
| **紧急** | **高危** | **中危** | **低危** |
| 0 | 0 | 1 | 13 |

|  |  |  |
| --- | --- | --- |
| **漏洞等级** | **漏洞类型** | **漏洞数量** |
| 中危 | **SSL 3.0协议** | 1 |
| 低危 | **Html form表单没有CSRF防护** | 3 |
| 低危 | **https页面上的混合内容** | 1 |
| 低危 | **测试文件** | 1 |
| 低危 | **启用TLS 1.1** | 1 |
| 低危 | **Microsoft IIS 版本信息泄露** | 1 |
| 低危 | **jQuery跨站脚本** | 1 |
| 低危 | **Web应用程序错误** | 1 |
| 低危 | **HTTP Content-Security-Policy缺失** | 1 |
| 低危 | **POODLE攻击(带有CBC密码套件的SSLv3)** | 1 |
| 低危 | **HTTP X-Download-Options缺失** | 1 |

# 2网站漏洞详情

网站漏洞详情仅展示漏洞基本信息，更多漏洞详情可登录您的saas租户端平台，

『云监测』→『漏洞/安全事件/内容查询』操作栏中点击查看。

## 2.1紧急漏洞

暂无数据

## 2.2高危漏洞

暂无数据

## 2.3中危漏洞

**2.3.1.SSL 3.0协议** **【中危】**

|  |  |
| --- | --- |
| **漏洞名称** | **SSL 3.0协议** |
| **风险等级** | 中危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | {VUL\_PORT}: 443 |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **远程服务使用SSL 3.0加密流量，这是不安全且已弃用的协议，具有众所周知的漏洞。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 禁用 SSL 3.0 并改用 TLS 1.2（或更高版本）。 |

## 2.4低危漏洞

**2.4.1.Html form表单没有CSRF防护** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **Html form表单没有CSRF防护** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/personalSettings/personalSetting.html?completeCustomerInfoFlag=1 |
| **漏洞POC** | {ID\_DB\_FORM\_NAME}: undefined, {ID\_DB\_FORM\_ACTION}: |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **CSRF（Cross-site request forgery跨站请求伪造，也被称成为“one click attack”或者session riding，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。WebScan发现一个HTML表单没有明显的反CSRF保护。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 验证此表格是否需要防CSRF保护，必要时实施CSRF对策。 |

**存有该漏洞的其他URL【低危】（部分举例）**

|  |  |
| --- | --- |
| **漏洞URL** | **漏洞POC** |
| https://ctzx.qiluhospital.com/report/MEReport.html?name=1 | {ID\_DB\_FORM\_NAME}: undefined, {ID\_DB\_FORM\_ACTION}: |
| https://ctzx.qiluhospital.com/personalSettings/personalSetting.html?completeCustomerInfoFlag=1 | {ID\_DB\_FORM\_NAME}: undefined, {ID\_DB\_FORM\_ACTION}: |

**2.4.2.https页面上的混合内容** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **https页面上的混合内容** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/questionnaire/comQuestionnaire.html |
| **漏洞POC** | [{"mixedType":"active","tagName":"script","location":"http://iconfont.eeejian.com/v30/iconfont.js","attribute":"src"}] |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **通过安全 HTTPS 连接加载初始 HTML，但通过不安全的 HTTP 连接加载其他资源（如图像、视频、样式表、脚本）时，就会出现混合内容。使用不安全的 HTTP 协议请求子资源会降低整个页面的安全性，因为这些请求容易遭受中间人攻击，攻击者会窃听网络连接并查看或修改两方之间的通信。利用这些资源，攻击者可以跟踪用户并替换网站上的内容，而对于主动混合内容的情况，他们可以完全控制页面，而不仅仅是导致资源不安全。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 将包含HTTP链接属性的标签替换为HTTPS链接 |

**2.4.3.测试文件** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **测试文件** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/test.html |
| **漏洞POC** | test.html |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **弱点描述：Web应用程序在开发过程中，程序员为了测试代码功能，在Web目录下放置测试文件，可能包含敏感信息。攻击者读取上述文件的内容，以便进一步攻击目标站点。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 一般性的建议：[1]删除或者限制访问测试文件。 |

**2.4.4.启用TLS 1.1** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **启用TLS 1.1** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | {VUL\_PORT}: 443 |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **Web 服务器支持通过 TLS 1.1 进行加密。在针对支付卡行业 (PCI) 数据安全标准 (DSS) 合规性时，建议改用 TLS 1.2 或更高版本。根据 PCI 的说法，2018 年 6 月 30 日是禁用 SSL/早期 TLS 并实施更安全的加密协议 - TLS 1.1 或更高版本（强烈建议使用 TLS v1.2）以满足 PCI 数据安全标准 (PCI DSS) 的截止日期) 以保护支付数据。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 建议禁用 TLS 1.1 并将其替换为 TLS 1.2 或更高版本。 |

**2.4.5.Microsoft IIS 版本信息泄露** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **Microsoft IIS 版本信息泄露** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | {IIS\_VERSION}:8.5 |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **此 Web 应用程序返回的 HTTP 响应包括名为 Server 的响应头。响应头的值包含Microsoft IIS服务器的版本信息。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | Microsoft IIS 应配置为从响应中删除不需要的 HTTP 响应头。 |

**2.4.6.jQuery跨站脚本** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **jQuery跨站脚本** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/assets/js/jquery.cookie.js |
| **漏洞POC** | jQuery Ver : 1.4.1 |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **弱点描述：低于1.6.3版本的jQuery组件存在$(location.hash) 和 $(#)的跨站脚本漏洞，详情：http://bugs.jquery.com/ticket/9521。该警告有可能是误报，扫描器只是判断了jquery的版本，并没有模拟执行。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:3.7 |
| 修复建议 | 一般性的建议：建议更新使用新版本的jQuery组件：http://jquery.com。 |

**2.4.7.Web应用程序错误** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **Web应用程序错误** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/api/Article/GetPhoneList |
| **漏洞POC** | HTTP CODE : 500 |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **弱点描述：Web应用程序在处理访问者的请求时，如果符合Web应用程序的逻辑或者Web应用程序本身没有异常，那么将结果直接反馈给访问者。如果提交不符合Web应用程序逻辑的数据，Web应用程序在处理这些请求的时候未做相应的处理，直接把Web服务器的错误反馈给访问者。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 一般性的建议：过滤客户端提交的危险字符，客户端提交方式包含GET、POST、COOKIE、User-Agent、Referer、Accept-Language等，其中危险字符如下：[1] |[2] &[3] ;[4] $[5] %[6] @[7] '[8] "[9] [10] ()[11] +[12] CR[13] LF[14] ,[15] .开发语言的建议:[1] 检查入局请求，以了解所有预期的参数和值是否存在。 当参数缺失时，发出适当的错误消息，或使用缺省值。[2] 应用程序应验证其输入是否由有效字符组成（解码后）。 例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。[3] 确保值符合预期范围和类型。 如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。 例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。[4] 验证数据属于提供给客户端的集合。[5] 请勿在生产环境中输出调试错误消息和异常。 |

**2.4.8.HTTP Content-Security-Policy缺失** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **HTTP Content-Security-Policy缺失** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | https://ctzx.qiluhospital.com/ |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **内容安全策略 (CSP) 是一个额外的安全层，用于检测并削弱某些特定类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击等。无论是数据盗取、网站内容污染还是散发恶意软件，这些攻击都是主要的手段。CSP 的实质就是白名单制度，开发者明确告诉客户端，哪些外部资源可以加载和执行，等同于提供白名单。它的实现和执行全部由浏览器完成，开发者只需提供配置。CSP 大大增强了网页的安全性。攻击者即使发现了漏洞，也没法注入脚本，除非还控制了一台列入了白名单的可信主机。CSP开启可能会导致js、css出现报错。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 启用 CSP方法：一种是通过 HTTP 头信息的Content-Security-Policy的字段，另一种是通过网页的meta标签。 |

**2.4.9.POODLE攻击(带有CBC密码套件的SSLv3)** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **POODLE攻击(带有CBC密码套件的SSLv3)** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | {VUL\_PORT}:443, {PROTOCOL}:SSL3, {CBC\_CIPHERS}:TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **SSL protocol是美国网景（Netscape）公司研发的安全套接层协议（Secure Socket Layer）的缩写，为互联网通信提供安全及数据完整性保障。 OpenSSL 1.0.1i及之前版本中使用的SSL protocol 3.0版本中存在加密问题漏洞，该漏洞源于程序使用非确定性的CBC填充。攻击者可借助padding-oracle攻击利用该漏洞实施中间人攻击，获取明文数据。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 建议禁用 SSLv3 并将其替换为 TLS 1.2 或更高版本 要禁用 SSLv2 和 SSLv3： 对于Apache： SSLProtocol 所有 -SSLv2 -SSLv3 对于 Nginx： ssl\_protocols TLSv1.2； |

**2.4.10.HTTP X-Download-Options缺失** **【低危】**

|  |  |
| --- | --- |
| **漏洞名称** | **HTTP X-Download-Options缺失** |
| **风险等级** | 低危 |
| **漏洞URL** | https://ctzx.qiluhospital.com/ |
| **漏洞POC** | https://ctzx.qiluhospital.com/ |
| **取证截图** | **无取证截图** |
| **漏洞描述** | **Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效。Web 服务器对于 HTTP 请求的响应头中缺少 X-Download-Options，这将导致浏览器提供的安全特性失效，更容易遭受 Web 前端黑客攻击的影响。** |
| **漏洞编号** | CVE:--  CNVD:--  CVSS:-- |
| 修复建议 | 1）修改服务端程序，给 HTTP 响应头加上 X-Download-Options 如果是 java 服务端，可以使用如下方式添加 HTTP 响应头 response.setHeader("X-Download-Options", "value") 如果是 php 服务端，可以使用如下方式添加 HTTP 响应头 header("X-Download-Options: value") 如果是 asp 服务端，可以使用如下方式添加 HTTP 响应头 Response.AddHeader "X-Download-Options", "value" 如果是 python django 服务端，可以使用如下方式添加 HTTP 响应头 response = HttpResponse() response["X-Download-Options"] = "value" 如果是 python flask 服务端，可以使用如下方式添加 HTTP 响应头 response = make\_response() response.headers["X-Download-Options"] = "value"；2）修改负载均衡或反向代理服务器，给 HTTP 响应头加上 X-Download-Options 如果使用 Nginx、Tengine、Openresty 等作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： add\_header X-Download-Options value; 如果使用 Apache 作为代理服务器，在配置文件中写入如下内容即可添加 HTTP 响应头： Header add X-Download-Options "value"。 |