**保健体检信息管理系统**

**渗透测试报告**



杭州安恒信息技术股份有限公司

二〇二五年四月

**声明**

* 本报告仅适用于保健体检信息管理系统在安全评估时的系统状况。系统的安全评估周期和系统安全评估时的基本状况将在下列的章节中给出。
* 在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自增加、修改、伪造或掩盖事实。
* 为保证系统所属方的利益，本评估报告仅提供给被测系统所属方，杭州安恒信息技术股份有限公司不向第三方提供，并为其保密。被评估方不能将此报告或报告中的某一部分拷贝或复制，作为广告宣传材料。

单位名称：杭州安恒信息技术股份有限公司

联系地址：浙江省杭州市滨江区西兴街道联慧街188号

联系电话：0571--28860999

传 真：0571--28863666

目录

[1. 评估计划 4](#_Toc130605472)

[1.1. 测试对象 4](#_Toc357880670)

[1.2. 测试人员 4](#_Toc1946209090)

[1.3. 测试IP 4](#_Toc1612748173)

[1.4. 风险等级 4](#_Toc2067434824)

[2. 检测结果 5](#_Toc1091678508)

[2.1. 未授权访问1【高风险】 5](#_Toc1887887635)

[2.2. 未授权访问2【高风险】 5](#_Toc656597020)

[2.3. 任意文件上传【高风险】 8](#_Toc1655136854)

[2.4. 未授权访问3【中风险】 11](#_Toc1529425587)

[2.5. 密码明文传输【中风险】 12](#_Toc1824069766)

* **文档说明**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 保健体检信息管理系统渗透测试报告 | | |
| **评估人员** | 李淑鹏 | **评估日期** | 2025/4/17 – 2025/7/21 |
| **制作人员** | 李淑鹏 | **制作日期** | 2025/4/21 |
| **扩散范围** | 限“安恒信息”、“山东大学齐鲁医院”内部传阅 | | |

* **适用范围**

本文档是经山东大学齐鲁医院授权，由杭州安恒信息技术股份有限公司（以下简称“安恒信息”）对保健体检信息管理系统相关站点进行渗透测试，根据评估结果所提交的技术报告，用于对该网站的安全状况做出安全评估和加固建议，仅限于“安恒信息”、山东大学齐鲁医院内部人员传阅。

# 评估计划

## 测试对象

评估系统列表：

|  |  |
| --- | --- |
| **系统名称：** | 保健体检信息管理系统 |
| **系统地址：** | http://172.18.3.195/ |
| **防护情况：** | 无WAF |
| **测试账号：** | 测试管理员账户密码qlyy/123456  测试普通用户密码testuser/123456 |

## 测试人员

由“安恒信息”资深安全研究工程师主要参与。人员如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目角色** | **姓名** | **联系方式** | **项目职责** | **经历** |
| 项目成员 | 李淑鹏 | 17854401189 | 漏洞挖掘 | 多年信息安全攻防经验 |

## 测试IP

主要使用以下IP对目标系统进行了测试：

|  |
| --- |
| **测试IP** |
| 172.31.134.61 |

## 风险等级

|  |  |  |
| --- | --- | --- |
| **编号** | **风险等级** | **风险描述** |
| 1 | 高风险 | 可对目标网站造成重大损失，如信息篡改、数据损坏以及远程控制 |
| 2 | 中风险 | 可获取目标网站敏感信息，并结合其他安全漏洞可能影响目标网站的正常运营 |
| 3 | 低风险 | 可获取目标网站少量敏感信息，一般不会导致严重的安全事件 |

# 检测结果

管理员账号测试和普通测试账号密码为123456，需要改成强口令。注意：强口令要求至少包含大小写字母、数字和特殊字符中的三种组合，且长度不少于10位。同时，避免使用如“ASDqwe!@#”这类简单组合，数字不得连续出现三位以上。

## 未授权访问1【高风险】

|  |  |
| --- | --- |
| **漏洞名称：** | 未授权访问 |
| **漏洞描述：** | 未授权访问漏洞，是在攻击者没有获取到登录权限或未授权的情况下，即可通过直接输入网站控制台主页面地址或不允许查看的链接便可进行访问，同时进行操作。 |
| **风险程度：** | **高风险** |
| **漏洞位置：** | <http://172.18.3.195:10000/api_hub/crm/customer/customer-list?searchFilter=1&customerType=0&organizationId=qlyybj01&startTime=&endTime=&pageIndex=1&pageSize=20> |
| **漏洞证明：** | 直接访问URL可获取到数据，数据包括姓名、手机号、身份证号等个人敏感信息。 |
| **修复建议：** | 进行鉴权。 |

## 未授权访问2【高风险】

|  |  |
| --- | --- |
| **漏洞名称：** | 未授权访问 |
| **漏洞描述：** | 未授权访问漏洞，是在攻击者没有获取到登录权限或未授权的情况下，即可通过直接输入网站控制台主页面地址或不允许查看的链接便可进行访问，同时进行操作。 |
| **风险程度：** | **高风险** |
| **漏洞位置：** | http://172.18.3.195:10000/api\_hub/check/task/task-progress?orderType[]=aaa000000001&guideReturned=0&ignoreCompleted=0&pageIndex=1&pageSize=20&\_t=1745221204148  <http://172.18.3.195:10000/api_hub/check/task/task-progress?orderType[]=aaa000000001&pageIndex=1&pageSize=20&_t=1745221204139>  <http://172.18.3.195:10000/api_hub/check/task/task-progress?orderType[]=aaa000000001&guideReturned=0&ignoreCompleted=0&searchFilter=11&timeRange[]=2025-04-14&timeRange[]=2025-04-21&pageIndex=1&pageSize=20&_t=1745221207437>  <http://172.18.3.195:10000/api_hub/order/bj/bj-order-list?pageIndex=1&pageSize=20&searchFilter=&orderDate=&timeType=1&statusFilter=0&sortType=&sortField=&_t=1745221971487> |
| **漏洞证明：** | 1.先通过接口获取组织号  <http://172.18.3.195:10000/api_hub/base/organization/organization-tree?orgKey=&_t=1745220708024>    2.填写组织号，未做鉴权操作，可随意获取数据 |
| **修复建议：** | 进行鉴权。 |

## 任意文件上传【高风险】

|  |  |
| --- | --- |
| **漏洞名称：** | 任意文件上传 |
| **漏洞描述：** | 一般情况下，文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。文件上传本身是web中最为常见的一种功能需求，关键是文件上传之后服务器端的处理、解释文件的过程是否安全。一般的情况有：  1. 上传文件WEB脚本语言，服务器的WEB容器解释并执行了用户上传的脚本，导致代码执行；  2. 上传文件FLASH策略文件crossdomain.xml，以此来控制Flash在该域下的行为；  3. 上传文件是病毒、木马文件，攻击者用以诱骗用户或管理员下载执行；  4. 上传文件是钓鱼图片或为包含了脚本的图片，某些浏览器会作为脚本执行，实施钓鱼或欺诈； |
| **风险程度：** | **高风险** |
| **漏洞位置：** | http://172.18.3.195:10200/api/static-file/upload-file |
| **漏洞证明：** | 地址：http://172.18.3.195:10200/upload/2025/04/21/Base/Img/1.html    数据报文如下：   |  | | --- | | POST /api/static-file/upload-file HTTP/1.1  Host: 172.18.3.195:10200  Content-Length: 313  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.95 Safari/537.36  Content-Type: multipart/form-data; boundary=----WebKitFormBoundary0OVph8fL4al0XEEu  Accept: \*/\*  Origin: http://172.18.3.195  Referer: http://172.18.3.195/system/appointManage/appoint\_app\_banner  Accept-Language: zh-CN,zh;q=0.9  Connection: close  ------WebKitFormBoundary0OVph8fL4al0XEEu  Content-Disposition: form-data; name="addtionPath"  Base/Img  ------WebKitFormBoundary0OVph8fL4al0XEEu  Content-Disposition: form-data; name="content"; filename="1.html"  Content-Type: image/png  <script>alert(1)</script>  ------WebKitFormBoundary0OVph8fL4al0XEEu-- | |
| **修复建议：** | 1. 对上传文件做有效文件类型判断，采用白名单控制的方法，开放只允许上传的文件格式，其中文件类型判断应对上传文件的后缀、文件头、图片类的预览图等做检测来判断文件类型，同时注意重命名上传文件的文件名避免攻击者利用WEB服务的缺陷构造畸形文件名实现攻击目的； 2. 禁止上传目录有执行权限，强烈建议上传后的文件不要保存在网站目录下； 3. 使用随机数改写文件名和文件路径，使得用户不能轻易访问自己上传的文件。 |

## 未授权访问3【中风险】

|  |  |
| --- | --- |
| **漏洞名称：** | 未授权访问 |
| **漏洞描述：** | 未授权访问漏洞，是在攻击者没有获取到登录权限或未授权的情况下，即可通过直接输入网站控制台主页面地址或不允许查看的链接便可进行访问，同时进行操作。 |
| **风险程度：** | **中风险** |
| **漏洞位置：** | <http://172.18.3.195:8500/v1/catalog/nodes>  http://172.18.3.195:8500/v1/agent/self |
| **漏洞证明：** |  |
| **修复建议：** | 请做页面限制访问。 |

## 密码明文传输【中风险】

|  |  |
| --- | --- |
| **漏洞名称：** | 密码明文传输 |
| **漏洞描述：** | 密码明文传输一般存在于web网站登录页面，用户名或者密码采用了明文传输，容易被嗅探软件截取。攻击者可能结合中间人攻击，窃取明文传输的密码，从而非授权登录系统，执行破坏性操作。 |
| **风险程度：** | **中风险** |
| **漏洞位置：** | http://172.18.3.195:10000/api\_hub/base/user/login |
| **漏洞证明：** |  |
| **修复建议：** | 建议在网站前端用 Javascript 做密码加密，加密后再进行传输。 |

报告完结