

|  |  |
| --- | --- |
| 文档编号 |  |
| 版本编号 | Ver 1.0 |
| 密级 | 商密 |
| 日期 | 2025-04-24 |

|  |
| --- |
| 保健体检信息管理系统 |
| 源代码安全审计报告 |

|  |
| --- |
| **©2025安恒信息** |
| **版权所有，未经授权，严禁复制、编辑和传播！** |

**声明**

* **适用性声明**

本报告仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）开展安全评估时的状况。评估结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响评估结论的有效性。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。

* **版权声明**

本文中的所有信息均为山东大学齐鲁医院内部信息，务请妥善保管，未经山东大学齐鲁医院和安恒信息明确作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

* **版本变更记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **拟制／修改日期** | **拟制／修改人** | **修改记录** | **批准人** |
| 1.0 | 2025-04-24 | 李扬 | 创建文档 |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[一、 报告摘要 1](#_Toc18474)

[二、 源代码安全审计工作简介 1](#_Toc15075)

[2.1 审计概述 1](#_Toc21993)

[2.2 审计方式 1](#_Toc20146)

[2.3 审计流程 1](#_Toc23673)

[2.3.1 信息收集阶段 1](#_Toc2475)

[2.3.2 编码脆弱性和缺陷分析阶段 1](#_Toc432)

[2.3.3 逻辑结构缺陷分析阶段 2](#_Toc20801)

[2.3.4 报告编制阶段 2](#_Toc22623)

[2.4 审计人员 2](#_Toc19329)

[2.5 风险等级对照表 2](#_Toc23257)

[三、 审计对象 3](#_Toc11267)

[四、 源代码安全审计结果 4](#_Toc20131)

[4.1 中级风险（2个） 4](#_Toc10590)

[4.1.1 密钥硬编码 4](#_Toc654)

[4.1.2 JWT认证无效 4](#_Toc26444)

1. 报告摘要

杭州安恒信息技术股份有限公司（以下简称：“安恒信息”）在本次山东大学齐鲁医院源代码安全审计工作中，共分析源代码文件约327个，代码总量约265,033行，**总共发现2个安全风险，高危风险0个，中危风险2个，低危风险0个**；

安全风险主要表现为：密钥硬编码、JWT认证无效。

安全风险所对应的漏洞详情，请详见下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **漏洞来源** | **序号** | **风险等级** | **漏洞类型** | **数量（个）** |
| **源代码漏洞** | 1 | 中风险 | 密钥硬编码 | 1 |
| **源代码漏洞** | 2 | 中风险 | JWT认证无效 | 1 |
| **合计** | | | | **2** |

1. 源代码安全审计工作简介

审计概述

源代码安全审计工作是以OWASP十大Web漏洞为主要检查依据，针对应用系统的源代码，通过了解其业务系统，从应用系统结构方面，检查其各模块和功能之间的功能实现、权限验证等内容；从安全性方面，检查其存在的脆弱性和缺陷的一项审查工作。在明确当前安全现状和需求的情况下，此项工作对于下一步安全编码规范性建设具有重大意义。

审计方式

源代码安全审计工作是采用人工结合专业源代码扫描工具的审查方式，对源代码进行安全审计。

审计流程

源代码安全审计流程定义为如下四个阶段：

信息收集阶段

在此阶段中，审计人员需要对目标应用系统进行必要的信息收集，例如源代码、web服务器应用系统信息、业务流、开发文档以及必要的测试帐号等。

编码脆弱性和缺陷分析阶段

在此阶段中，审计人员重点审查源代码的缺陷和脆弱性问题，审查内容主要包含以下几方面：

* API滥用：例如调用非本单位直接控制的资源、对象过于频繁调用、直接调用空对象导致系统资源消耗过大或是程序执行效率低下等。
* 代码质量：例如对象错误或不适合调用导致程序未能按预期的方式执行，功能缺失；类成员与其封装类同名，变量赋值后不使用等。
* 封装：多余的注释信息、调试信息问题导致应用系统信息暴露、错误的变量声明。
* 程序异常处理：忽略处理的异常、异常处理不恰当造成的信息泄露或是不便于进行错误定位等。
* 输入验证：SQL注入、跨站脚本、拒绝服务攻击、对上传文件的控制等，因为未能较好的控制用户提交的内容所造成的问题。
* 安全功能：请求的参数没有限制范围导致的信息泄露、cookie超时和域范围等配置方面的内容。

逻辑结构缺陷分析阶段

在此阶段中，审计人员针对目标应用系统的源代码进行必要的逻辑结构分析，审查应用系统在对业务流处理的过程中，是否存在权限控制不严格、表单逻辑处理的错误、功能缺失等因为结构控制不严所造成的问题。

报告编制阶段

最后，审计人员对漏洞风险进行定级，并依据漏洞类型给出相应修改建议，编制审计报告。

审计人员

审计人员如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目角色** | **姓名** | **联系方式** | **职务** | **项目职责** |
| 项目成员 | 李扬 | 17621777361 | 源代码安全审计工程师 | 对源代码进行审计并编写系统源代码安全审计报告。 |

风险等级对照表

|  |  |  |
| --- | --- | --- |
| **序号** | **风险等级** | **风险描述** |
| 1 | 高风险 | 可对直接对目标网站/系统造成重大损失，如信息篡改、数据损坏以及远程控制等操作。 |
| 2 | 中风险 | 可获取目标网站/系统敏感信息，并结合其它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/系统少量敏感信息，一般不会导致严重的安全事件。 |

1. 审计对象

本次项目的审计对象为保健体检信息管理系统源代码，基本信息如下所示：

|  |  |
| --- | --- |
| **基本信息** | |
| 应用系统名称 | 保健体检信息管理系统 |
| 开发语言类型 | .net |

1. 源代码安全审计结果

中级风险（2个）

密钥硬编码

问题列表

漏洞汇总

|  |  |
| --- | --- |
| **已发现问题数（个）** | 1 |
| **问题位置** | V6Peis.LocalData.Web.Entry\Controllers\MaintenanceController.cs |

MaintenanceController.cs 29行

if (!string.IsNullOrEmpty(model.ResultDBStr))

{

if (model.DecryptPassword == "YJXX2525")

//省略后续代码

问题描述

在软件研发实践中，采用静态硬编码方式存储敏感凭证（如数据库连接字符串、API密钥或认证令牌）属于高危风险。此类实现方式存在严重安全隐患：

1. 权限管控失效：项目源码中的明文密码对开发团队全员可见，违背最小授权原则。
2. 运维弹性丧失：生产系统投产运行后，若遭遇密钥泄露事件，需通过发版更新强制修复，无法在维护阶段实现动态凭证更新。
3. 修改密钥时将导致业务中断（需停机修改所有硬编码节点）。
4. 合规性缺失：违反等保2.0第8.1.4条关于"不应在代码中明文存储鉴别信息"的要求。

解决方案

加密存储方案：对敏感凭证进行加密处理。

JWT认证无效

问题列表

漏洞汇总

|  |  |
| --- | --- |
| **已发现问题数（个）** | 1 |
| **问题位置** | V6Peis.LocalData\V6Peis.LocalData.Web.Core\Handlers\JwtHandler.cs |

JwtHandler.cs 14行

public override Task<bool> PipelineAsync(AuthorizationHandlerContext context, DefaultHttpContext httpContext)

{

// 这里写您的授权判断逻辑，授权通过返回 true，否则返回 false

return Task.FromResult(true);

}

问题描述

在JwtHandler.cs中，发现授权处理逻辑直接返回true，这意味着所有JWT认证请求都会被自动通过，不进行任何实际的验证。

解决方案

添加有效的授权判断逻辑。