产品研发部网络安全自查报告

1. **系统概况（一句话）**

（1）系统名称 ：生产资源管理系统

（2）系统主要功能：人员、车辆、异常驾驶行为管理

（3）系统开发、上线时间节点：2025年6月

（4）用户对象，用户数量等：生产资源相关管理人员，目前用户数量34

1. **系统部署情况**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **部署环境** | **服务器名** | **主机名** | **内网IP** | **公网IP** | **CPU分配(核)** | **内存分配（GB）** | **磁盘分配（GB/TB）** |
| 1 | 正式环境 | 生产资源管理平台应用服务器 | suog-PRMP-web |  |  | 8 | 8 | 500 |
| 2 | 正式环境 | 生产资源管理平台数据库服务器 | suog-PRMP-db |  |  | 8 | 16 | 300 |
| 3 | 测试环境 | 生产资源管理平台测试服务器 | suog-PRMP-test |  |  | 8 | 16 | 400 |

1. **系统外网端口配置清单自查**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务器内网IP | 服务器公网IP | 服务器用途 | 部署环境 | 端口号 | 协议 | 内网/外网 | 端口用途 | 启用状态 |
| 1 | 172.16.193.125 | - | 应用服务器 | 生产环境 | 13000 | https | 内网 |  | 启用 |
| 3 | 172.16.193.126 | - | 数据库服务器 | 生产环境 |  |  |  |  |  |
| 4 | 172.16.216.40 | - | 测试服务器 | 测试环境 | 14000 | https | 内网 |  | 启用 |

1. **重大网络安全风险项资产**

|  |  |  |
| --- | --- | --- |
| **序号** | **问题** | **核查项点（每项均需截图证明）** |
| 1 | 外网页面访问 | 1. 除小程序、APP之外，不应存在公网可访问的页面   截图：本系统无公网地址，未对公网开放 |
| 2 | 弱身份验证 | 1. 不应存在前端框架硬编码写入账号密码问题   截图： |
| 3 | 登录功能可暴力破解 | 1. 是否部署了登录验证（验证码/短信验证）      1. 是否部署了登录失败限制（登录失败超过5次锁定账号） 2. 登录失败提示信息不得为“用户名错误、密码错误”等指向明确的描述，需改为“用户名或密码错误”   截图： |
| 4 | 敏感信息泄露 | 1. 公网可访问的URL路径下，不应存在config.js等包含敏感ID、密码信息的文件   截图： |
| 5 | 前端代码硬编码泄露敏感信息 | 1. 前端代码不应存在明文形式代码写入的用户密码、API密钥、IP地址、手机号码、车牌号码、OAuth令牌等其他敏感信息；   截图：（开发工具抓包截图） |
| 6 | 明文传输用户名密码 | 1. 用户登录请求中的用户名、用户密码登敏感字段均需要本地JS加密后传输   截图：  前端密码加密 |
| 8 | 未启用HTTPS | 1. 公网端口启用https协议通信   截图 |
| 9 | 为对系统管理员权限进行拆分 | 1. 三级等保要求，需要将超级管理权限拆分为系统管理员、安全管理员、审计管理员；   截图 可以自定义权限组 |