面向人脸分析的 AI 攻防靶场平台前端网页设计产品需求分析

本产品需求分析围绕面向人脸分析的 AI 攻防靶场平台展开，旨在构建一个能为模型提供攻击检测与评估的平台，以下从用户角色、功能需求、交互需求、视觉设计需求等方面进行简要分析。

## 一、用户角色

攻击方：试图对人脸分析模型发起攻击，以探索模型漏洞和弱点的人员。

防御方：负责保护人脸分析模型，对攻击进行检测和防御的人员。

管理员：管理平台整体运行，包括用户管理、靶场设置、数据统计等工作。

## 二、功能需求

登录注册：支持用户名 + 密码登录，同时提供手机号或邮箱注册功能，数据传输采用加密技术保障安全。

### 攻击方功能

主控制台：查看得分排行榜。

靶场查看：展示可供攻击的人脸分析模型相关信息，如模型类型、应用场景、安全防护等级等。

成果查看：呈现攻击方发起的攻击记录，包括攻击方式、攻击结果（成功 / 失败）、影响程度等，可查看详细报告及审批情况。

成果提交：提供标准化的攻击报告模板，方便攻击方填写。攻击方提交攻击报告，包括攻击过程、使用工具、发现的漏洞等内容，可上传相关附件。

### 防御方功能

防御任务：展示需要防御的攻击任务及对应模型，可查看攻击方的攻击记录。

防御成果：呈现防御方采取的防御措施及效果，如漏洞修复情况、模型加固效果等。

报告提交：提交防御报告，说明防御策略、遇到的问题及解决方案。

### 管理员功能

用户管理：管理攻击方、防御方和其他管理员的账号信息，包括添加、删除、权限设置等。

靶场管理：配置和管理人脸分析模型靶场，如添加新模型、设置模型参数、启用 / 禁用模型等。

报告审批：对攻击方和防御方提交的报告进行审批，可下载附件查看详细内容。

数据统计：统计平台的相关数据，如攻击次数、成功攻击次数、防御成功率等，生成可视化报表。

## 三、交互需求

界面导航：采用简洁明了的导航栏，方便用户快速找到所需功能模块。

操作反馈：对用户的操作及时给予反馈，如提交报告后的提示信息、审批结果通知等。

数据展示：以直观易懂的方式展示数据，如表格、图表等形式。

## 四、视觉设计需求

整体风格：保持简洁、专业的设计风格，色彩搭配协调，符合科技感主题。

页面布局：合理规划页面布局，保证信息展示清晰有序，避免内容过于拥挤。

## 五、性能需求

响应速度：页面加载和操作响应时间应控制在合理范围内，确保用户体验流畅。

兼容性：兼容主流浏览器和不同设备屏幕尺寸，保证在各种环境下正常使用

