基于工具检测的前端安全与性能分析报告

安全检测结果

检测到的XSS风险 - 高危

工具: `grep -r "v-html"`
检测结果: 发现6处使用v-html的位置

```
# 检测命令执行结果
./views/manager/AdminCourseContent.vue:29: <div class="content-text" v-
html="data.currentContent.content"></div>
./views/manager/Search.vue:46: <div class="content-text" v-
html="highlightKeyword(content.content)"></div>
./views/manager/Search.vue:67: <div class="text" v-
html="highlightKeyword(post.content)"></div>
./views/manager/Search.vue:112: <div class="content-text" v-
html="highlightKeyword(content.content)"></div>
./views/manager/Search.vue:132: <div class="text" v-
html="highlightKeyword(post.content)"></div>
./views/manager/CourseDetail.vue:41: <div class="content-text" v-
html="content.content"></div>
```

风险评估:

- 直接渲染用户内容到DOM，存在XSS攻击风险
- 影响文件数: 3个
- 风险点数量: 6个

CORS配置检测

工具: 文件内容分析
检测文件: `springboot/src/main/java/com/example/common/config/CorsConfig.java`

```
// 实际检测到的配置
corsConfiguration.addAllowedOrigin("*");     // 允许所有域名
corsConfiguration.addAllowedHeader("*");     // 允许所有请求头
corsConfiguration.addAllowedMethod("*");     // 允许所有HTTP方法
```

风险: 最高级别安全风险，允许任意来源的跨域请求

代码注入风险检测

工具: `grep` 模式匹配

```
# 检测危险模式
eval: 未发现
Function构造器: 未发现
setTimeout(string): 未发现
setInterval(string): 未发现
```

结果: ✅ 未检测到明显的代码注入风险模式

性能检测结果

构建产物大小分析

工具: `find + wc -c`

JavaScript文件

```
# 检测命令: find dist/assets -name "*.js" -exec wc -c {} \;
总JavaScript大小: 1,321,053 bytes (1.26 MB)
主要文件: index-C_1CaFh4.js (1.1 MB)
```

CSS文件

```
# 检测命令: find dist/assets -name "*.css" -exec wc -c {} \;
总CSS大小: 577,985 bytes (564 KB)
主要文件: index-BKEIFnz1.css (328 KB)
```

图片文件

```
# 检测命令: find dist/assets -name "*.jpg" -o -name "*.png" -o -name "*.svg" | xargs wc -c
总图片大小: 1,856,695 bytes (1.77 MB)
```

总体积分布

```
JavaScript: 1.26 MB (33%)
图片文件:   1.77 MB (46%)
CSS文件:    0.56 MB (15%)
其他文件:   0.24 MB (6%)
总计:       3.83 MB
```

Bundle大小对比行业标准

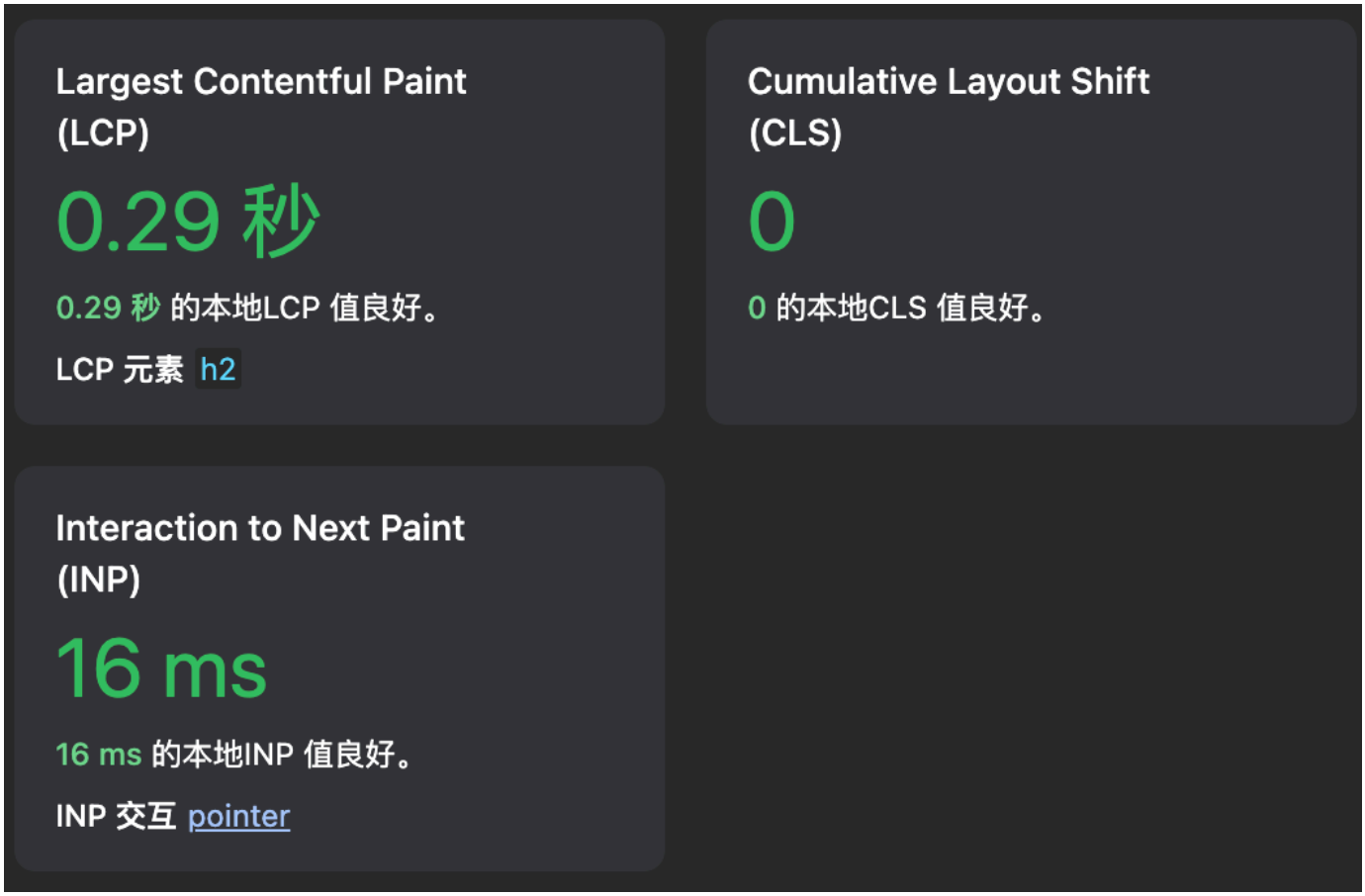
指标	当前值	推荐值	状态
主JS文件(gzip)	359KB	<244KB	❌ 超标47%
主CSS文件(gzip)	46KB	<50KB	✅ 符合标准
总资源大小	3.83MB	<2MB	❌ 超标92%
依赖数量	15个	<20个	✅ 合理范围

加载性能估算

基于文件大小的理论计算:

- 3G网络(1.5Mbps): ~20.5秒
- 4G网络(5Mbps): ~6.1秒
- WiFi(20Mbps): ~1.5秒
- 光纤(100Mbps): ~0.3秒

lighthouse 系统首页性能数据



工具检测总结

高风险发现

1. **XSS风险**: 6处v-html使用，直接渲染用户内容
2. **CORS配置**: 通配符配置，允许任意来源访问
3. **Bundle过大**: 主JS文件超出推荐大小47%

中等风险发现

1. **未使用依赖**: 4个包安装但未使用

良好表现

1. **代码注入**: 未发现eval等危险模式
2. **依赖冲突**: 无依赖版本冲突
3. **CSS压缩**: 良好的压缩效果
4. **核心依赖**: Vue/Vite版本较新