# Shelter 访问日志分析总结

## 📊 基本概况

- **总请求数**: 11,844 条
- **分析时间**: 2025年12月21日
- **日志文件**: shelter_access.log.1

## 🔍 关键发现

### 1. HTTP 状态码分布

- ✅ **成功请求 (2xx)**: 7,236 条 (61.09%)
- 🔄 **重定向 (3xx)**: 3,838 条 (32.40%) - 主要是301永久重定向
- ⚠️ **客户端错误 (4xx)**: 546 条 (4.61%)
- ❌ **服务器错误 (5xx)**: 204 条 (1.72%)

**主要状态码**:

- `200 OK`: 7,072 (59.71%)
- `301 永久重定向`: 3,838 (32.40%)
- `401 未授权`: 453 (3.82%)
- `503 服务不可用`: 149 (1.26%)
- `500 内部服务器错误`: 55 (0.46%)

### 2. 访问量 Top 5 IP 地址

| IP地址 | 请求数 | 占比 | 备注 |
|---|---|---|---|
| 66.90.99.250 | 1,379 | 11.64% | 最高访问量 |
| 39.144.137.202 | 879 | 7.42% | 包含50次错误请求 |
| 213.165.255.135 | 836 | 7.06% | ⚠️ **604次扫描尝试** |
| 61.158.27.197 | 686 | 5.79% | 正常用户 |
| 223.104.159.19 | 588 | 4.96% | 包含48次错误请求 |

### 3. 最热门的API端点

1. `/api/articles/` - 1,523 次 (12.86%)
2. `/api/notifications/unread_count/` - 1,441 次 (12.17%)
3. `/api/conversations/summary/` - 1,395 次 (11.78%)
4. `/api/articles/tags/` - 1,162 次 (9.81%)
5. `/api/conversations/` - 582 次 (4.91%)

### 4. ⚠️ 安全威胁分析

#### 可疑扫描活动

- **检测到 656 次可疑扫描尝试**
- **主要攻击源**: `213.165.255.135` (604次扫描，占所有扫描的92%)

**扫描目标路径包括**:

- `/admin/`
- `/phpMyAdmin/`
- `/phpmyadmin/`
- `/nacos/`
- `/.env`
- `/config.json`
- 各种已知漏洞路径

**建议措施**:

1. 将 213.165.255.135 加入黑名单
2. 检查其他扫描IP: 47.102.184.31 (10次), 4.189.104.41 (8次)
3. 加强路径访问控制

### 错误请求分析

- **总错误请求**: 770 次 (4xx/5xx)
- **主要错误类型**:
  - 401 未授权: 453 次 - 可能为未认证访问或认证失效
  - 503 服务不可用: 149 次 - 服务过载或维护
  - 500 内部服务器错误: 55 次 - 需要检查服务器日志

**产生错误最多的IP**:

1. 39.144.137.202 - 50次错误 (503, 401, 500)
2. 223.104.159.19 - 48次错误 (503, 401)
3. 183.157.163.101 - 45次错误 (全部401)

## 5. 流量时间分布

**高峰期**:

- **10:00** - 3,751 次请求 (峰值，31.67%)
- **16:00** - 1,154 次请求 (9.74%)
- **22:00** - 711 次请求
- **20:00** - 716 次请求
- **02:00** - 770 次请求

**低峰期**:

- 03:00 - 67 次
- 04:00 - 7 次
- 07:00 - 4 次

**建议**: 在10:00高峰期需要确保服务器有足够的处理能力。

## 6. User-Agent 分析

**主要客户端类型**:

- Windows 10 + Chrome: ~4,000+ 次 (33%+)
- Linux/Android: ~2,700+ 次 (23%+)
- 其他浏览器: ~5,000+ 次

# 🎯 建议与优化

## 安全性建议

1. ✅ **立即封禁扫描IP**: 213.165.255.135
2. ✅ **加强访问控制**: 对敏感路径（/admin, /api等）实施更严格的认证
3. ✅ **监控异常行为**: 关注高频401错误，可能是暴力破解
4. ✅ **检查日志**: 分析503和500错误，可能是服务器性能问题

## 性能优化建议

1. ⚡ **高峰期扩容**: 10:00时段请求量是平均值的3-4倍
2. ⚡ **缓存优化**: /api/notifications/unread_count/ 和 /api/conversations/summary/ 访问频繁，建议增加缓存
3. ⚡ **CDN使用**: 考虑将静态资源（头像、封面图）放到CDN

## 监控建议

1. 📊 持续监控 213.165.255.135 的访问
2. 📊 设置错误率告警（当前4xx+5xx占6.22%，可设置阈值）

2. 📊 设置错误率告警（当前4xx+5xx占6.55%，可设置阈值）
3. 📊 监控高频API的性能指标

## 📈 数据统计摘要

- **正常请求率**: 93.49% (200, 201, 206, 304)
- **错误率**: 6.51% (4xx + 5xx)
- **扫描尝试率**: 5.54% (656/11844)
- **API请求占比**: ~70% (估算)
- **平均每小时请求**: ~494 次

*分析生成时间: 2025年12月21日*
*分析工具: analyze_log.py*