Baseado no relatório ZAP fornecido, segue uma **análise de segurança com pontuação de 0 a 10**, levando em consideração a gravidade dos alertas, a quantidade, e a natureza das vulnerabilidades encontradas.

🔍 **Resumo dos Alertas:**

- **Total de alertas:** 10
    - **Médio:** 4 (40%)
    - **Baixo:** 3 (30%)
    - **Informativo:** 3 (30%)
    - **Alto: 0 (nenhum alerta crítico)**

⚠️ **Principais Vulnerabilidades (com Risco Médio):**

1. **CSP: Falha na definição de diretiva sem fallback**
    - Pode permitir a execução de scripts maliciosos.
    - Sugestão: Configurar uma política CSP robusta com diretrizes de fallback.
2. **Cabeçalho de Política de Segurança de Conteúdo (CSP) não definido**
    - Deixa a aplicação vulnerável a ataques XSS.
    - Sugestão: Adicionar o cabeçalho Content-Security-Policy.
3. **Configuração incorreta entre domínios (CORS)**
    - Pode permitir requisições não autorizadas entre domínios.
    - Sugestão: Restringir origens confiáveis via configuração de CORS.
4. **Cabeçalho anti-clickjacking ausente**
    - Pode permitir que a aplicação seja incorporada em iframes, facilitando ataques de clickjacking.
    - Sugestão: Incluir o cabeçalho X-Frame-Options: DENY ou SAMEORIGIN.

⚠️ **Riscos Baixos Comuns:**

- **Cabeçalhos de segurança ausentes:**
    - Strict-Transport-Security e X-Content-Type-Options.
    - Apesar de baixo risco, são importantes para hardening.
- **Inclusão de arquivos JS de fontes externas**
    - Pode ser um vetor para scripts maliciosos se não verificados.

ℹ️ **Informativos:**

- Comentários suspeitos no código.
- Recursos cacheados.
- Detecção de aplicação web moderna (sem risco direto, apenas observação técnica).

✅ **Pontos Positivos:**

- Nenhum alerta de **risco alto**.
- A maioria dos problemas são **relacionados a headers de segurança**, facilmente solucionáveis.
- Aplicação parece **estar em ambiente local (127.0.0.1)**, o que sugere ambiente de desenvolvimento (sem exposição externa direta ainda).

🔐 **Pontuação de Segurança:**

Com base na análise, dou à aplicação a seguinte **pontuação de segurança:**
📊 **Nota: 6.5 / 10**

🔧 **Recomendações para melhorar para 9+ / 10:**

1. **Adicionar todos os headers de segurança recomendados:**
    - Content-Security-Policy
    - X-Frame-Options
    - Strict-Transport-Security
    - X-Content-Type-Options
2. **Corrigir configuração CORS** se a aplicação aceitar requisições externas.
3. **Evitar dependências externas sem verificação**, especialmente JS.
4. **Remover comentários suspeitos em produção.**
5. **Rodar novos testes após as correções.**
