Com base na análise do relatório do ZAP, podemos atribuir uma pontuação geral de segurança considerando a quantidade e a gravidade dos alertas.

Critérios de Avaliação

- **Risco Alto**: 0 alertas (ótimo)
- **Risco Médio**: 6 alertas (preocupante, mas não crítico)
- **Risco Baixo**: 5 alertas (indicam melhorias necessárias)
- **Informativos**: 3 alertas (não são falhas diretas, mas boas práticas ausentes)

Principais Problemas Encontrados

1. **Política de Segurança de Conteúdo (CSP) fraca ou ausente**
    - Falta de CSP apropriado pode permitir ataques como **Cross-Site Scripting (XSS)**.
2. **Vazamento de informações do servidor**
    - Cabeçalhos como "X-Powered-By" e "Server" expõem informações que podem ser exploradas.
3. **Configuração inadequada de cookies**
    - Falta de HttpOnly e SameSite pode levar a ataques de **sequestro de sessão e CSRF**.
4. **Parâmetros passíveis de adulteração**
    - Indica possíveis problemas de **injeção ou manipulação de requisições**.
5. **Arquivos ocultos expostos**
    - Pode permitir acesso a informações sensíveis.

Pontuação de Segurança (0 a 10)

Com base nesses fatores, atribuo uma pontuação de **6.5/10**.

- **Pontos positivos**:
  ✅ Nenhum alerta de risco alto.
  ✅ Poucos problemas críticos.
- **Pontos negativos**:
  ⚠️ Falta de boas práticas de segurança (CSP, cookies, vazamento de informações).
  ⚠️ Possibilidade de exploração de vulnerabilidades de nível médio.

Se os problemas de **CSP, cookies e vazamento de informações** forem corrigidos, a pontuação pode subir para **8 ou 9/10**. 🚀