Com base no relatório do ZAP, podemos calcular uma pontuação de segurança considerando a quantidade e severidade dos alertas. Vamos adotar uma métrica ponderada:

- **Alto risco:** 0 alertas → 0 pontos
- **Médio risco:** 3 alertas → -15 pontos (5 pontos cada)
- **Baixo risco:** 3 alertas → -6 pontos (2 pontos cada)
- **Informativo:** 2 alertas → -2 pontos (1 ponto cada)

Pontuação final: (100 - (15 + 6 + 2)) = 77/100

Análise:

- O sistema tem um nível de segurança **razoável**, mas com várias melhorias necessárias.
- Principais problemas:
    - **Falta de CSP e headers de segurança**: Torna o sistema vulnerável a ataques como **clickjacking e XSS**.
    - **Ausência de tokens Anti-CSRF**: Pode permitir ataques de falsificação de requisição.
    - **Exposição de informações do servidor**: Pode facilitar ataques de reconhecimento e exploração de vulnerabilidades conhecidas.

Recomendações:

1. **Implementar Content Security Policy (CSP)** para evitar XSS.
2. **Adicionar cabeçalhos de segurança**, como X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security e Referrer-Policy.
3. **Corrigir CSRF** implementando tokens em formulários.
4. **Esconder informações do servidor** removendo o cabeçalho Server.
5. **Definir atributo SameSite nos cookies** para mitigar ataques CSRF.