# Vulnerabilidades de Segurança Encontradas

## **Website Analisado** AE Carlos Amarante (<https://aecarlosamarante.pt/>)

## **Ferramenta Utilizada** OWASP ZAP (scanner automático de segurança web)

## **Vulnerabilidades Encontradas - 9 Total**

|  |  |  |
| --- | --- | --- |
| Nível de Risco | Quantidade | Percentagem |
| **Médio** | 4 | 44% |
| **Baixo** | 3 | 33% |
| **Informativo** | 2 | 23% |
| **Alto** | 0 | 0% | |

## **Distribuição por Nível de Risco**

### **CATEGORIA 1: PROBLEMAS DE CONFIGURAÇÃO DE SEGURANÇA (4 vulnerabilidades)**

**1. Content Security Policy (CSP) não configurado**

* **O que é:** Falta de proteção contra scripts maliciosos
* **Risco:** Ataques de XSS (Cross-Site Scripting)
* **Solução:** Configurar política de segurança de conteúdo

**2. Proteção Anti-Clickjacking em falta**

* **O que é:** Sem proteção contra incorporação maliciosa da página
* **Risco:** Página pode ser usada em ataques de clickjacking
* **Solução:** Adicionar cabeçalho X-Frame-Options

**3. HSTS (Strict-Transport-Security) não ativo**

* **O que é:** Não força conexões seguras HTTPS
* **Risco:** Possíveis ataques man-in-the-middle
* **Solução:** Ativar HSTS no servidor

**4. X-Content-Type-Options em falta**

* **O que é:** Permite interpretação incorreta de tipos de ficheiro
* **Risco:** Execução de conteúdo malicioso
* **Solução:** Adicionar cabeçalho "nosniff"

### **CATEGORIA 2: VAZAMENTO DE INFORMAÇÕES (3 vulnerabilidades)**

**5. Servidor revela informações técnicas**

* **O que é:** Cabeçalho X-Powered-By expõe tecnologia usada
* **Risco:** Facilita ataques direcionados
* **Solução:** Remover cabeçalhos informativos

**6. Timestamps Unix expostos**

* **O que é:** Informações de tempo do servidor visíveis
* **Risco:** Revelação de detalhes internos
* **Solução:** Ocultar timestamps desnecessários

**7. Comentários suspeitos no código**

* **O que é:** Comentários no código fonte podem revelar informações
* **Risco:** Exposição de estruturas internas
* **Solução:** Limpar comentários do código de produção

### **CATEGORIA 3: CONFIGURAÇÃO DE CACHE (1 item)**

**8. Diretivas de cache a rever**

* **O que é:** Configurações de cache podem não estar otimizadas
* **Risco:** Possível cache inadequado de conteúdo sensível
* **Solução:** Revisar políticas de cache

### **CATEGORIA 4: APLICAÇÃO MODERNA (1 item)**

**9. Aplicação web moderna identificada**

* **O que é:** Website usa tecnologias modernas
* **Risco:** Requer testes específicos adicionais
* **Solução:** Implementar testes para aplicações modernas