

Relatório - Configuração de Headers e CSP

1. Configuração dos Headers de Segurança no Servidor Web

Os headers de segurança foram configurados no servidor web (Apache - XAMPP) para aumentar a proteção contra vulnerabilidades comuns em aplicações web. Abaixo está a descrição de cada header configurado:

X-XSS-Protection: Ativado para prevenir ataques de Cross-Site Scripting (XSS):

```
Header set X-XSS-Protection "1; mode=block"
```

X-Frame-Options: Configurado como **"SAMEORIGIN"** para evitar ataques de clickjacking, permitindo que a página seja incorporada apenas por frames do mesmo domínio:

```
Header always set X-Frame-Options "SAMEORIGIN"
```

Strict-Transport-Security (HSTS): Força conexões HTTPS e protege contra ataques de downgrade:

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

X-Content-Type-Options: Configurado como **"nosniff"** para evitar que navegadores interpretem tipos MIME incorretos:

```
Header set X-Content-Type-Options "nosniff"
```

Referrer-Policy: Configurado como **"no-referrer"** para evitar que informações de referência sejam enviadas ao site de destino:

```
Header set Referrer-Policy "no-referrer"
```

- **Content-Security-Policy (CSP):** Define regras para carregamento de conteúdo, descritas em mais detalhes no próximo item.

2. Código da CSP Implementada

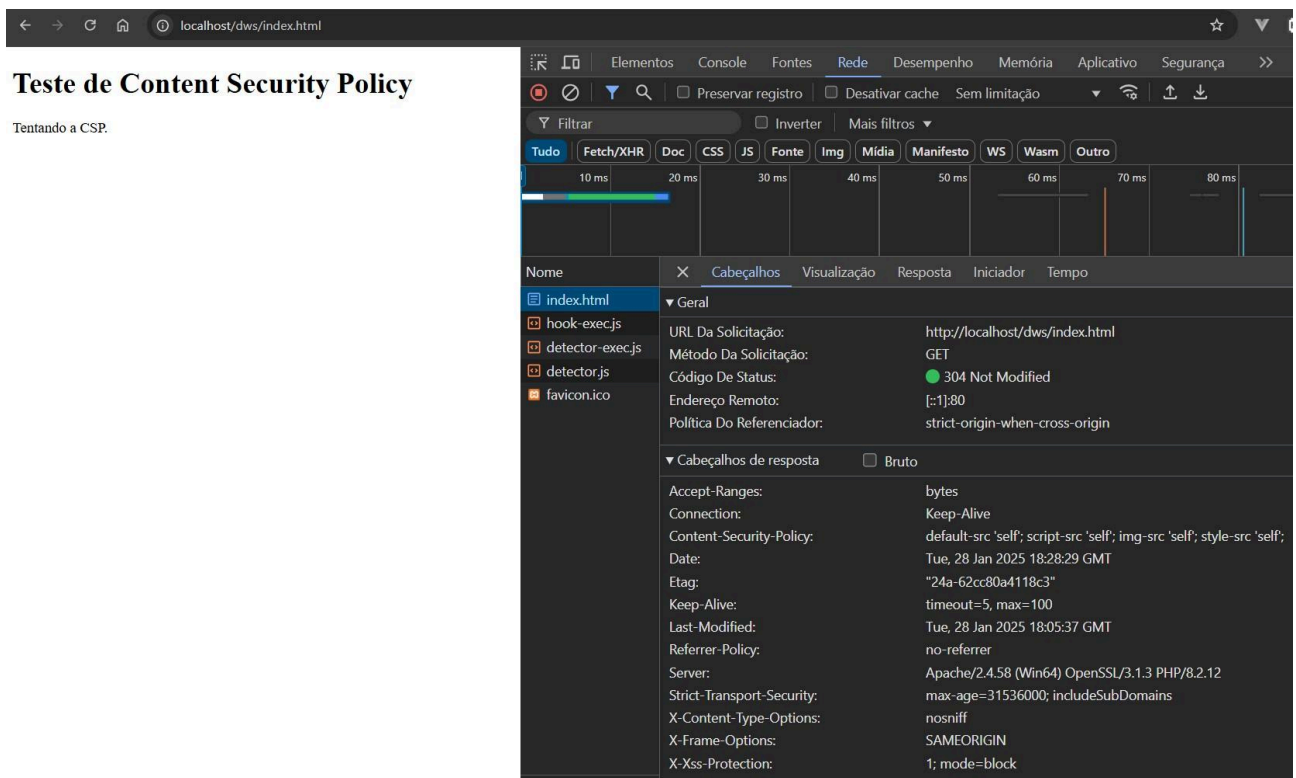
A seguinte **Content-Security-Policy (CSP)** foi implementada para restringir o carregamento de recursos no site simples:

```
default-src 'self';  
script-src 'self';  
img-src 'self';  
style-src 'self';  
object-src 'none';  
require-trusted-types-for 'script';
```

3. Análise dos Resultados dos Testes

Resultados no Console do Navegador

- Os headers configurados foram verificados usando as ferramentas do desenvolvedor do navegador.




Resultados do CSP Evaluator

- A política CSP foi avaliada no Google CSP Evaluator, que identificou as seguintes melhorias implementadas:
 - O bloqueio de recursos não confiáveis foi configurado com sucesso.
 - A diretiva `require-trusted-types-for 'script'` foi adicionada para maior proteção contra XSS.

Content Security Policy

[Sample unsafe policy](#)[Sample safe policy](#)

```
default-src 'self'; script-src 'self'; img-src 'self'; style-src 'self';
```

CSP Version 3 (nonce based + backward compatibility checks) 

CHECK CSP

Evaluated CSP as seen by a browser supporting CSP Version 3

[expand/collapse all](#)

✓	default-src	
⚠	script-src	
✓	img-src	
✓	style-src	
ⓘ	require-trusted-types-for [missing]	Consider requiring Trusted Types for scripts to lock down DOM XSS injection sinks. You can do this by adding "require-trusted-types-for 'script'" to your policy.

Legend

- ❗ High severity finding
- ⚠ Medium severity finding
- ⚠ Possible high severity finding
- Directive/value is ignored in this version of CSP
- ⚠ Possible medium severity finding
- ✗ Syntax error
- ⓘ Information
- ✓ All good

4. Reflexão

A implementação de headers de segurança e de uma CSP robusta é crucial para proteger aplicações web contra ataques comuns, como:

- Cross-Site Scripting (XSS): Mitigado pelo uso de
 - **Content-Security-Policy, X-XSS-Protection**
 - **require-trusted-types-for 'script'**.
- Clickjacking: Prevenido pelo header **X-Frame-Options**.
- Ataques de downgrade e exposição de dados: Evitados pelo uso de HSTS e **Referrer-Policy**.
- Injeção de arquivos maliciosos: Impedida pelo uso de **object-src 'none'** e restrições de fontes.

Essas medidas não apenas aumentam a segurança, mas também demonstram um compromisso com as melhores práticas de desenvolvimento web. É essencial revisar essas configurações regularmente para garantir que a aplicação continue protegida contra novas ameaças.