

Relatório de digitalização

ZAP

Gerado com  ZAP em qua. 9 abr. 2025, às 17:11:20

Versão ZAP: 2.16.1

ZAP por [Checkmarx](#)

Conteúdo

- [Sobre este relatório](#)
 - [Parâmetros do relatório](#)
- [Resumos](#)
 - [Contagens de alertas por risco e confiança](#)
 - [Contagens de alertas por local e risco](#)
 - [Contagens de alertas por tipo de alerta](#)
- [Alertas](#)
 - [Risco = Médio, Confiança = Alto \(2\)](#)
 - [Risco = Médio, Confiança = Médio \(2\)](#)
 - [Risco = Baixo, Confiança = Alto \(1\)](#)
 - [Risco = Baixo, Confiança = Médio \(2\)](#)
 - [Risco = Informativo, Confiança = Médio \(2\)](#)

- [Risco = Informativo, Confiança = Baixo \(1\)](#)
- [Apêndice](#)
 - [Tipos de alerta](#)

Sobre este relatório

Parâmetros do relatório

Contextos

Nenhum contexto foi selecionado, então todos os contextos foram incluídos por padrão.

Sítios

Os seguintes sites foram incluídos:

- <https://www.gstatic.com>
- <http://127.0.0.1:5500>

(Se nenhum site foi selecionado, todos os sites foram incluídos por padrão.)

Um site incluído também deve estar dentro de um dos contextos incluídos para que seus dados sejam incluídos no relatório.

Níveis de risco

Incluído : [Alto](#) , [Médio](#) , [Baixo](#) , [Informativo](#)

Excluído : Nenhum

Níveis de confiança

Incluído : [Usuário Confirmado](#) , [Alto](#) , [Médio](#) , [Baixo](#)

Excluídos : [Usuário Confirmado](#) , [Alto](#) , [Médio](#) , [Baixo](#) , [Falso Positivo](#)

Resumos

Contagens de alertas por risco e confiança

Esta tabela mostra o número de alertas para cada nível de risco e confiança incluídos no relatório.

(As porcentagens entre parênteses representam a contagem como uma porcentagem do número total de alertas incluídos no relatório, arredondado para uma casa decimal.)

		Confiança			
Risco	Usuário confirmado	Alto	Médio	Baixo	Total
	Alto	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	2 (20,0%)	2 (20,0%)	0 (0,0%)
	Baixo	0 (0,0%)	1 (10,0%)	2 (20,0%)	0 (0,0%)
	Informativo	0 (0,0%)	0 (0,0%)	2 (20,0%)	1 (10,0%)
	Total	0 (0,0%)	3 (30,0%)	6 (60,0%)	1 (10,0%)

Contagens de alertas por local e risco

Esta tabela mostra, para cada site para o qual um ou mais alertas foram gerados, o número de alertas gerados em cada nível de risco.

Alertas com nível de confiança de "Falso Positivo" foram excluídos dessas contagens.

(Os números entre parênteses são o número de alertas gerados para o site nesse nível de risco ou acima dele.)

	Risco			
	Alto (= Alto)	Médio (>= Médio)	Baixo (>= Baixo)	Informativo (>= Informativo)
https://www.gstatistic.com	0 (0)	1 (1)	1 (2)	2 (4)
Site http://127.0.0.1:5500	0 (0)	3 (3)	2 (5)	1 (6)

Contagens de alertas por tipo de alerta

Esta tabela mostra o número de alertas de cada tipo de alerta, juntamente com o nível de risco do tipo de alerta.

(As porcentagens entre parênteses representam cada contagem como uma porcentagem, arredondada para uma casa decimal, do número total de alertas incluídos neste relatório.)

Tipo de alerta	Risco	Contar
CSP: Falha na definição de diretiva sem fallback	Médio	3 (30,0%)
Configuração Incorreta Entre Domínios	Médio	2 (20,0%)
Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido	Médio	3 (30,0%)
Total		10

Tipo de alerta	Risco	Contar
<u>Cabeçalho anti-clickjacking ausente</u>	Médio	3 (30,0%)
<u>Inclusão de arquivo de origem JavaScript entre domínios</u>	Baixo	6 (60,0%)
<u>Cabeçalho Strict-Transport-Security não definido</u>	Baixo	2 (20,0%)
<u>Cabeçalho X-Content-Type-Options ausente</u>	Baixo	8 (80,0%)
<u>Divulgação de Informações - Comentários Suspeitos</u>	Informativo	2 (20,0%)
<u>Aplicação Web Moderna</u>	Informativo	2 (20,0%)
<u>Obtido do Cache</u>	Informativo	1 (10,0%)
Total		10

Alertas

Risco = Médio , Confiança = Alto (2)

http://127.0.0.1:5500 (2)

CSP: Falha na definição de diretiva sem recurso (1)

► OBTER <http://127.0.0.1:5500/robots.txt>

Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido (1)

► OBTENHA <http://127.0.0.1:5500/>

Risco = Médio , Confiança = Médio (2)

<https://www.gstatic.com> (1)

Configuração Incorreta Entre Domínios (1)

► OBTENHA <https://www.gstatic.com/firebasejs/9.0.0/firebase-app-compat.js>

<http://127.0.0.1:5500> (1)

Cabeçalho anti-clickjacking ausente (1)

► OBTENHA <http://127.0.0.1:5500/>

Risco = Baixo , Confiança = Alto (1)

<https://www.gstatic.com> (1)

Cabeçalho Strict-Transport-Security não definido (1)

► OBTENHA <https://www.gstatic.com/firebasejs/9.0.0/firebase-app-compat.js>

Risco = Baixo , Confiança = Médio (2)

<http://127.0.0.1:5500> (2)

Inclusão de arquivo de origem JavaScript entre domínios (1)

► OBTENHA <http://127.0.0.1:5500/>

Cabeçalho X-Content-Type-Options ausente (1)

► OBTER <http://127.0.0.1:5500/js/auth.js>

Risco = Informativo , Confiança = Médio (2)

<https://www.gstatic.com> (1)

Recuperado do Cache (1)

► OBTENHA <https://www.gstatic.com/firebasejs/9.0.0/firebase-app-compat.js>

<http://127.0.0.1:5500> (1)

Aplicação Web Moderna (1)

► OBTENHA <http://127.0.0.1:5500/>

Risco = Informativo , Confiança = Baixo (1)

<https://www.gstatic.com> (1)

Divulgação de Informações - Comentários Suspeitos (1)

► OBTENHA <https://www.gstatic.com/firebasejs/9.0.0/firebase-app-compat.js>

Apêndice

Tipos de alerta

Esta seção contém informações adicionais sobre os tipos de alertas no relatório.

CSP: Falha na definição de diretiva sem fallback

Fonte	levantado por um scanner passivo (CSP)
Identificação do CWE	693
Identificação do WASC	15
Referência	<ul style="list-style-type: none">▪ https://www.w3.org/TR/CSP/▪ https://caniuse.com/#search=content+security+policy▪ https://content-security-policy.com/▪ https://github.com/HtmlUnit/htmlunit-csp▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Configuração Incorreta Entre Domínios

Fonte	gerado por um scanner passivo (Configuração Incorreta Entre Domínios)
Identificação do CWE	264
Identificação do WASC	14

Referência

- https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido**Fonte**

gerado por um scanner passivo ([Cabeçalho da Política de Segurança de Conteúdo \(CSP\) Não Definido](#))

Identificação do CWE

[693](#)

Identificação do WASC

15

Referência

- https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- <https://www.w3.org/TR/CSP/>
- <https://w3c.github.io/webappsec-csp/>
- <https://web.dev/articles/csp>
- <https://caniuse.com/#feat=contentsecuritypolicy>
- <https://content-security-policy.com/>

Cabeçalho anti-clickjacking ausente

Fonte	levantado por um scanner passivo (Cabeçalho Anti-clickjacking)
Identificação do CWE	1021
Identificação do WASC	15
Referência	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Inclusão de arquivo de origem JavaScript entre domínios

Fonte	gerado por um scanner passivo (inclusão de arquivo de origem JavaScript entre domínios)
Identificação do CWE	829
Identificação do WASC	15

Cabeçalho Strict-Transport-Security não definido

Fonte	gerado por um scanner passivo (Cabeçalho Strict-Transport-Security)
Identificação do CWE	319
Identificação do WASC	15
Referência	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

- <https://owasp.org/www-community/Security-Headers>
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- <https://caniuse.com/stricttransportsecurity>
- <https://datatracker.ietf.org/doc/html/rfc6797>

Cabeçalho X-Content-Type-Options ausente

Fonte	gerado por um scanner passivo (X-Content-Type-Options Header Missing)
Identificação do CWE	693
Identificação do WASC	15
Referência	<ul style="list-style-type: none">▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)).▪ https://owasp.org/www-community/Security-Headers

Divulgação de Informações - Comentários Suspeitos

Fonte	levantado por um scanner passivo (Divulgação de Informações - Comentários Suspeitos)
-------	--

**Identificação
do CWE** 615

**Identificação
do WASC** 13

Aplicação Web Moderna

Fonte gerado por um scanner passivo ([Aplicação Web Moderna](#))

Obtido do Cache

Fonte gerado por um scanner passivo ([obtido do cache](#))

Referência

- <https://tools.ietf.org/html/rfc7234>
- <https://tools.ietf.org/html/rfc7231>
- <https://www.rfc-editor.org/rfc/rfc9110.html>