DAREDE
à nuvem

ENGIE

CSP e Security Headers

Setembro/2024

Introdução

- Este documento detalha a análise de CSP e Security Headers no sites Engie:
    - Website Engie
    - Alem da Energia
    - Energy Place
    - Site E-Conomiza

DAREDE à nuvem | Consulting AWS Partner of the year 2021 aws

Website Engie

Website Engie

- **Uso do unsafe-inline na diretiva style-src e unsafe-eval na diretiva script-src:** Para eliminar o uso de unsafe-inline em uma CSP, é necessário evitar scripts e estilos inline (ou seja, scripts e CSS diretamente no HTML). Para o unsafe-eval, deve-se substituir o uso de eval() por métodos mais seguros, aqui deve-se revisar o uso de bibliotecas externas que podem utilizar estes métodos. Necessário verificação do time de desenvolvimento no código.

- **Uso do Subresource Integrity (SRI):** Necessário alteração no código para adicionar o hash dos script envolvidos.

Website Engie

- **Uso do “data:” na diretiva img-src e de unsafe-eval na diretiva font-src:** Será avaliada a remoção e verificação de eventuais problemas.

- **Inclusão da diretiva form-action:** A diretiva form-action na Content Security Policy (CSP) controla para onde os formulários de uma página podem ser enviados, ou seja, define quais URLs são permitidas como destino para ações de envio de formulários. Serão avaliados quais os necessários.
- **Code injection:** Só é possível ao se retirar os valores “unsafe”.

DAREDE à nuvem | Consulting AWS Partner of the year 2021 aws

Energy Place

Energyplace

- **Uso do unsafe-inline na diretiva style-src e font-src e unsafe-eval na diretiva script-src:** Para eliminar o uso de unsafe-inline em uma CSP, é necessário evitar scripts e estilos inline (ou seja, scripts e CSS diretamente no HTML). Para o unsafe-eval, deve-se substituir o uso de eval() por métodos mais seguros, aqui deve-se revisar o uso de bibliotecas externas que podem utilizar estes métodos. Necessário verificação do time de desenvolvimento no código.

- **Uso do Subresource Integrity (SRI):** Necessário alteração no código para adicionar o hash dos script envolvidos.

Energy Place

- **Uso do “data:” na diretiva img-src e de unsafe-eval na diretiva font-src: S**erá avaliada a remoção e verificação de eventuais problemas.

- **Inclusão da diretiva form-action:** A diretiva form-action na Content Security Policy (CSP) controla para onde os formulários de uma página podem ser enviados, ou seja, define quais URLs são permitidas como destino para ações de envio de formulários. Serão avaliados quais os necessários.
- **Code injection:** Só é possível ao se retirar os valores “unsafe”.

DAREDE à nuvem | Consulting AWS Partner of the year 2021 aws

E-Conomiza

E-Conomiza

- **Uso do unsafe-inline na diretiva style-src e unsafe-eval na diretiva script-src e font-src:** Para eliminar o uso de unsafe-inline em uma CSP, é necessário evitar scripts e estilos inline (ou seja, scripts e CSS diretamente no HTML). Para o unsafe-eval, deve-se substituir o uso de eval() por métodos mais seguros, aqui deve-se revisar o uso de bibliotecas externas que podem utilizar estes métodos. Necessário verificação do time de desenvolvimento no código.

- **Uso do Subresource Integrity (SRI):** Necessário alteração no código para adicionar o hash dos script envolvidos.

E-Conomiza

- **Atualização da lib de integração com o salesforce:** select2.min.js por parte do time de desenvolvimento.
- **Uso do “blob:” na diretiva img-src e de unsafe-eval na diretiva font-src:** Será avaliada a remoção e verificação de eventuais problemas.
- **Code injection:** Só é possível ao se retirar os valores “unsafe”.
- **Revisão dos domínios incluídos nas diretivas default-src e connect-src por não estarem em conformidade com o W3C CSP.**

DAREDE à nuvem | Consulting AWS Partner of the year 2021 aws

Alem da Energia

Alem da Energia

- **Uso do unsafe-inline nas diretivas script-src, style-src e script-elem-src e do unsafe-eval na diretiva script-src:** Para eliminar o uso de unsafe-inline em uma CSP, é necessário evitar scripts e estilos inline (ou seja, scripts e CSS diretamente no HTML). Necessário verificação do time de desenvolvimento no código

- **Uso do Subresource Integrity (SRI):** Necessário alteração no código para adicionar o hash dos script envolvidos.

Alem da Energia

- **Uso do “data:” na diretiva img-src e na diretiva font-src:** Será avaliada a remoção e verificação de eventuais problemas.

- **Code injection:** Só é possível ao se retirar os valores “unsafe”.

DAREDE à nuvem | Consulting AWS Partner of the year 2021 aws

Avaliação dos Sites

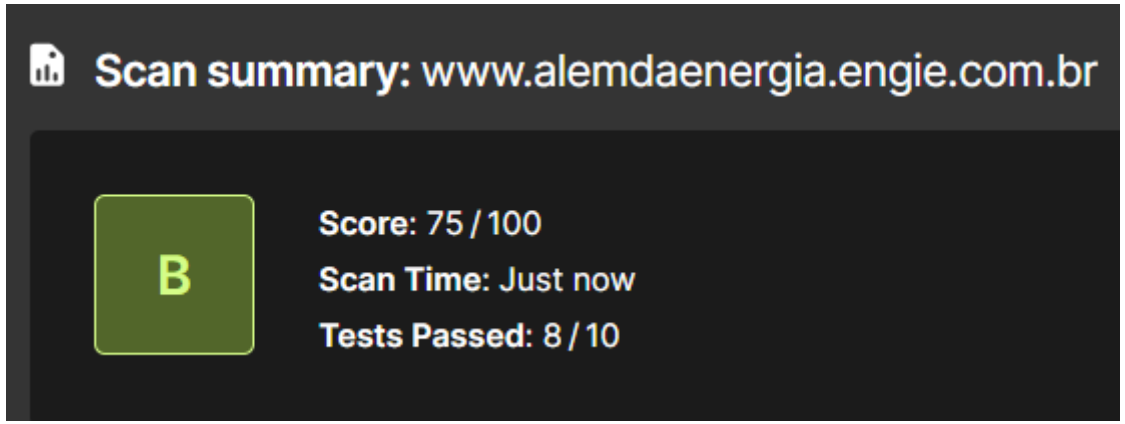
Avaliação dos Sites

A seguir, temos a avaliação de segurança dos sites segundo o Mozilla Observatory, utilizando somente a home dos mesmos:

Website Engie: https://developer.mozilla.org/en-US/observatory/analyze?host=www.engie.com.br

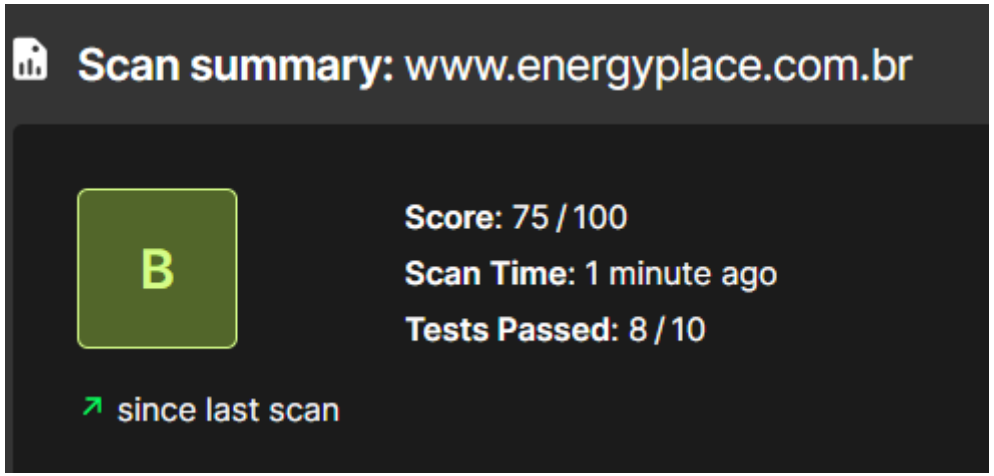
Avaliação dos Sites

Além da Energia: https://developer.mozilla.org/en-US/observatory/analyze?host=www.alemdaenergia.engie.com.br



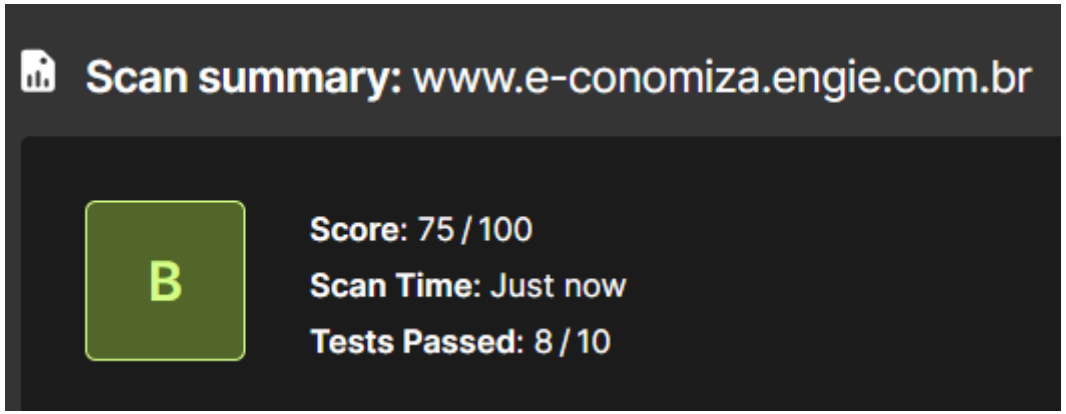
Avaliação dos Sites

Energy Place: https://developer.mozilla.org/en-US/observatory/analyze?host=www.energyplace.com.br



Avaliação dos Sites

E-Conomiza: https://developer.mozilla.org/en-US/observatory/analyze?host=www.e-conomiza.engie.com.br



Avaliação dos Sites

Para todos, temos a nota que o uso do unsafe-inline, unsafe-eval, data ou blob prejudicam a nota, bem como o não uso do SRI.

Scoring | CSP analysis | Raw server headers | Cookies | Scan history | Benchmark comparison

Test	Score	Reason	Recommendation
Content Security Policy (CSP)	−20 ✕	Content Security Policy (CSP) implemented unsafely. This includes `'unsafe-inline'` or `data:` inside `script-src`, overly broad sources such as `https:` inside `object-src` or `script-src`, or not restricting the sources for `object-src` or `script-src`.	Remove `unsafe-inline` and `data:` from `script-src`, overly broad sources from `object-src` and `script-src`, and ensure `object-src` and `script-src` are set.
Subresource Integrity	−5 ✕	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS.	Add SRI to external scripts.

DAREDE à nuvem

Consulting AWS Partner of the year 2021 aws

Pablo Parucci

Arquiteto de soluções em Nuvem

aws certified Cloud Practitioner FOUNDATIONAL

pablo.parucci@darede.com.br

DAREDE à nuvem

www.darede.com.br

/company/darede

darede.com.br/

t.me/cloudevangelist

/daredeti

/daredeservicosdeti

/daredeti

COLABORE COM NOSSA COMUNIDADE. PARTICIPE DOS CANAIS DIGITAIS DA DAREDE!

Obrigado!

DAREDE à nuvem

Consulting AWS Partner of the year 2021

aws