December 8th 2023

Exploring Content Security Policies

What even is it?



Added layer of security for websites



Allowlist of website resources



A W3C standard for browser implementations

How it works

Browser



Please load font from fonts.google.com



Browser loads fonts from fonts.google.com



How it works

Browser



Please load script from malicious.domain.net

CSP

It depends...



How it works

Browser



Please load script from malicious.domain.net



It depends...



In short... A CSP is a bouncer



Pros & Cons

O Benefits

- Blocks malicious resources
- Blocks browser extension modifications
- O Identifies external resources being used
- Improves our security score

O Cons

- Allowlist approach is a big ask
- Potentially slow to roll out
- Somewhat complicated for developers to understand
- Can break your website!

The list... mostly

- Directives: Types of resources the website might load
 - script-src: Scripts (Javascript)
 - style-src: Styles (CSS)
 - O Etc...
- O Directive Values: What is allowed for the given directive
 - O URL: https://fonts.google.com or https://fonts.google.com/family/font/style.css
 - 'self': Tells the browser the website is allowed to load resources from the website
 - data:: Tells the browser embedded data is allowed (Typically used for img-src directive)
 - blob:: Tells the browser blob data is allowed (Typically used for img-src directive)
 - O 'none': Tells the browser there are no allowed resources for the directive
 - 'unsafe-inline': Tells the browser it's okay to render resources that are embedded in the html
 - 'unsafe-eval': Tells the browser it's okay to perform script evals
 - 'nonce-' or 'sha256-': Tells the browser it's okay to trust files or inline items if they match hashes
- report-uri & report-to: Where should the browser send violation reports?

The list... mostly

- O Directives: Types of resources the website might load
 - script-src: Scripts (Javascript)
 - style-src: Styles (CSS)
 - O Etc...

This was

intentional

- Directive Values: What is allowed for the given directive
 - O URL: https://fonts.google.com or https://fonts.google.com/family/font/style.css
 - 'self': Tells the browser the website is allowed to load resources from the website
 - o date::: Tells the browser embedded data is allowed (Typically used for img-src directive)
 - blod:::Tells the browser blob data is allowed (Typically used for img-src directive) Maybe use this sometimes...
 - 'none': Tells the browser there are no allowed resources for the directive
 - 'unsafe-inline': Tells the browser it's okay to render resources that are embedded in the html
 - 'unsafe-eval': Tells the browser it's okay to perform script evals
 - 'nonce-' or 'sha256-': Tells the browser it's okay to trust files or inline items if they match hashes
- report-uri & report-to: Where should the browser send violation reports?

• Options

- Content-Security-Policy Header
- Content-Security-Policy-Report-Only Header



• Options

- O Content-Security-Policy Header
- Content-Security-Policy-Report-Only Header



O Options

- Content-Security-Policy Header
- O Content-Security-Policy-Report-Only Header



O Options

- Content-Security-Policy Header
- Content-Security-Policy-Report-Only Header



Options

- Content-Security-Policy Header
- O Content-Security-Policy-Report-Only Header



OevTools - local-dev.robotti.private/	
K Lo Elements Console Sources Network Performance Memory Application Se	ecurity Lighthouse Recorder 凸 Performance insights 凸
🧧 🖉 🝸 🔍 🗆 Preserve log 🗌 Disable cache 🛛 No throttling 🔻 😪 🛧 🛃	
Filter Invert Hide data URLs Hide extension URLs All Doc JS	Fetch/XHR CSS Font Img Media Manifest WS Wasm Other Blocked response cookies B
10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms	90 ms 100 ms 110 ms 120 ms 130 ms 140 ms 150 ms 160 ms 17
Name	* X Headers Payload Preview Response Initiator Timing Cookies
activities.png	▼Request Payload view source
1 fa-solid-900.woff2	▼ {csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",…}}
🗊 fa-regular-400.woff2	▼ csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",}
I fa-brands-400.woff2	<pre>blocked-uri: "https://www.google.com/recaptcha/api.js"</pre>
memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTS-muw.woff2	disposition: "enforce"
memtYaGs126MiZpBA-UFUIcVXSCEkx2cmgvXIWgWuU6F.woff2	document-uri: "https://local-dev.robotti.private/"
😣 api,is	original-policy: "default-src 'self':report-uri https://local-dev.robotti.private/c
	referrer: ""
septiment-infield.html	script-sample: ""
	status-code: 200
3666 nuntime is	violated-directive: "script-src-elem"
32 requests 8.2 MB transferred 8.3 MB resources Finish: 252 ms DOMContentLoaded: 136 ms Load	d: 🕢

📀 DevTools - local-dev.robotti.private/ Elements Console Sources Network Performance Memory Application Lighthouse Recorder **Z** Performance insights ⊥ Security 🍸 🔍 🗌 Preserve log 🗌 Disable cache 🛛 No throttling 🔻 🙃 🗠 土 0 Invert Hide data URLs Hide extension URLs All Doc JS Fetch/XHR CSS Font Manifest WS Wasm Other Blocked response cookies B Img Media 10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms 90 ms 100 ms 110 ms 120 ms 130 ms 140 ms 150 ms 160 ms X Headers Payload Preview Response Initiator Timing Cookies ▼Request Payload view source ▼ {csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",...}} v csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",...} blocked-uri: "https://www.google.com/recaptcha/api.js" disposition: "enforce" -muw.woff2 document-uri: "https://local-dev.robotti.private/" memtYaGs126MiZpBA-UF ive: "script-src-elem" Name Status Type Initiator 😵 api.js "default-src 'self';report-uri https://local-dev.robotti.private/c 🙁 api.is 🖸 csp script-sample: "" webclient-infield.html status-code: 200 favicon.ico violated-directive: "script-src-elem" 3666.runtime.js 6297.infield.js 32 requests 8.2 MB transferred 8.3 MB resources Finish: 252 ms DOMContentLoaded: 136 ms Load:

DevTools - local-dev.robotti.private/



OevTools - local-dev.robotti.private/	
🔀 🗖 Elements Console Sources <u>Network</u> Performance Memory Application Sec	curity Lighthouse Recorder 즈 Performance insights 즈
🧧 🖉 🍸 🔍 🗆 Preserve log 🗆 Disable cache 🛛 No throttling 🔻 😪 土 보	
Filter Invert Hide data URLs Hide extension URLs All Doc JS F	etch/XHR CSS Font Img Media Manifest WS Wasm Other 🛛 Blocked response cookies 🗖 B
10 ms 20 ms 30 ms 40 ms 50 ms 60 ms 70 ms 80 ms	90 ms 100 ms 110 ms 120 ms 130 ms 140 ms 150 ms 160 ms 17
Name	X Headers Payload Preview Response Initiator Timing Cookies
activities.png	▼Request Payload view source
1 fa-solid-900.woff2	▼ {csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",…}}
🔟 fa-regular-400.woff2	<pre>v csp-report: {document-uri: "https://local-dev.robotti.private/", referrer: "",}</pre>
I fa-brands-400.woff2	<pre>blocked-uri: "https://www.google.com/recaptcha/api.js" So lets add this</pre>
II memvYaGs126MiZpBA-UvWbX2vVnXBbObj2OVTS-muw.woff2	disposition: "enforce"
memtYaGs126MiZpBA-UFUIcVXSCEkx2cmgvXIWgWuU6F.woff2	document-uri: "https://local-dev.robotti.private/"
😣 apilis	original-policy: "default-src 'self':report-uri https://local-dev.robotti.private/c
O CSD	referrer: ""
webclient-infield.html	script-sample: ""
	status-code: 200
3666 nuntime is	violated-directive: "script-src-elem"
32 requests 8.2 MB transferred 8.3 MB resources Finish: 252 ms DOMContentLoaded: 136 ms Load	4

Wait... what?

DevTools - local-dev.robotti.private/	– o ×
🔆 🗖 Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder 🛽 Performance insights 🖉	፡ ፡ ፡ ፡ ፡ ፡ ፡ : : : : : : : : : : : : :
E Ø top ▼ Ø Filter	📃 Default levels 🔻 📔 16 Issues: 🗖 8 🏴 7 🛱 1 🛛 🕄
Navigated to https://local-dev.robotti.private/	
A The key "user-scale" is not recognized and ignored.	<u>local-dev.robotti.private/:7</u>
Refused to load the script ' <url>' because it violates the following Content Security Policy directive: "script-src-elem <url>".</url></url>	
Sefused to load the script 'https://local-dev.robotti.private/js/jquery.min.js' because i violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
® Refused to load the script ' <u>https://local-dev.robotti.private/js/bootstrap.min.js</u> ' becaus it violates the following Content Security Policy directive: "script-src-elem <u>https://www.google.com/recaptcha/api.js</u> ".	<pre>local-dev.robotti.private/:1</pre>
Sefused to load the script 'https://local-dev.robotti.private/js/glightbox.min.js' becaus it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
Sefused to load the script 'https://local-dev.robotti.private/is/aos.js' because it viola es the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
Refused to load the script ' <u>https://local-dev.robotti.private/js/purecounter.js</u> ' because t violates the following Content Security Policy directive: "script-src-elem <u>https://www.google.com/recaptcha/api.js</u> ".	<pre>local-dev.robotti.private/:1</pre>
Refused to load the script 'https://local-dev.robotti.private/js/swiper-bundle.min.js' be ause it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js'	". <u>local-dev.robotti.private/:1</u>
8 Refused to load the script 'https://local-dev.robotti.private/js/main.jg' because it viol tes the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.jg".	<pre>local-dev.robotti.private/:1</pre>
Sefused to load the script 'https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha en.js' because it violates the following Content Security Policy directive "script-src-elem https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha en.js' because it violates the following Content Security Policy directive "script-src-elem https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha en.js' because it violates the following Content Security Policy directive "script-src-elem https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha en.js' because it violates the following Content Security Policy directive "script-src-elem https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha en.js' because it violates the following Content Security Policy directive "script-src-elem https://www	<u>w.google.com/recaptcha/api.js</u> ". <u>api.js:1</u>

So now, because we have a script-src-elem directive all our scripts are blocked?



Because we didn't include 'self' for that directive

Wait... what?

DevTools - local-dev.robotti.private/	– o ×
🔆 🗖 Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder 🛽 Performance insights 🛽	⊗8▲1 ¤8 🕄
E ⊘ top ▼ ③ [Filter	🗌 Default levels 🔻 🕴 16 Issues: 🛤 8 🛤 7 🛤 1 🛛 🕄
Navigated to https://local-dev.robotti.private/	
A The key "user-scale" is not recognized and ignored.	<pre>local-dev.robotti.private/:7</pre>
💌 Refused to load the script ' <url>' because it violates the following Content Security Policy directive: "script-src-elem <url>".</url></url>	
8 Refused to load the script 'https://local-dev.robotti.private/js/jquery.min.js' because it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
8 Refused to load the script 'https://local-dev.robotti.private/js/bootstrap.min.js' because it violates the following Content Security Policy directive: "script-src-elem https://local-dev.robotti.private/js/bootstrap.min.js".	<pre>local-dev.robotti.private/:1</pre>
🛿 Refused to load the script 'https://local-dev.robotti.private/js/glightbox.min.js' because it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
8 Refused to load the script 'https://local-dev.robotti.private/js/aos.js' because it violates the following Content Security Policy directive: "script-src-elem https://hww.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
😵 Refused to load the script 'https://local-dev.robotti.private/js/purecounter.js' because it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
8 Refused to load the script 'https://local-dev.robotti.private/js/swiper-bundle.min.js' because it violates the following Content Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js"	". <u>local-dev.robotti.private/:1</u>
Refused to load the script 'https://local-dev.robotti.private/js/main.js' because it violates the following Content_Security Policy directive: "script-src-elem https://www.google.com/recaptcha/api.js".	<pre>local-dev.robotti.private/:1</pre>
8 refused to load the script 'https://www.gstatic.com/recaptcha/releases/-QbJqHfGOUB8nuVRLvzFLVed/recaptcha_en.js' because it violates the following Content Security Policy directive: "script-src-elem https://ww	w.google.com/recaptcha/api.js". api.js:1
	A

We also have this new script that is being blocked?



Because the script we allowed pulled it in

Lets be smarter about it



Lets be smarter about it

💽 The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	
8 The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	<u>local-dev.robotti.private/:1</u>
⊗ ►The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	web-client-content-script.js:2
She Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	recaptcha en.js:49
She Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	recaptcha en.js:23
She Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	<u>recaptcha en.js:23</u>
Navigated to https://local-dev.robotti.private/	
A The key "user-scale" is not recognized and ignored.	<pre>local-dev.robotti.private/:7</pre>
[Report Only] Refused to load media from 'https://local-dev.robotti.private/images/cincinnati skyline.mp4' because it violates the following Content Security Policy directive: "default-src none". Note that 'media-src' was not explicitly set, so 'default-src' is used as a fallback.	<u>local-dev.robotti.private/:1</u>
[Report Only] Refused to load media from 'https://local-dev.robotti.private/images/cincinnati skyline.mp4' because it violates the following Content Security Policy directive: "default-src none". Note that 'media-src' was not explicitly set, so 'default-src' is used as a fallback.	<u>local-dev.robotti.private/:1</u>
[Report Only] Refused to load the script <u>'https://www.google.com/recaptcha/api.js'</u> because it violates the following Content Security Policy directive: "script-src 'self'". Note that 'script-src-elem' was not explicitly set, so 'script-src' is used as a fallback.	<u>local-dev.robotti.private/:1</u>
Seport Only] Refused to load the script https://www.gstatic.com/recaptcha/releases/-ObJqHf60UB8nuVRLvzFLVed/recaptcha_en.js pecause it violates the following Content Security Policy directive: "script-src 'self'". Note that was not explicitly set, so 'script-sry' is used as a ranuack.	nt 'script-src-elem' <u>api.js:1</u>
[Report Only] Refused to frame 'http://www.google.com/' because it violates the following Content Security Policy directive: "defaulty src none". Note that 'frame-src' was not explicitly set, so 'default-src' is used as a fallow	ck. <u>www.gstatic.com/:1</u>
[Report Only] Refused to frame 'https://www.google.com/' because it violates the following Content Security Policy directive: "default-sr none". Note that 'frame-src' was not explicitly set, so 'default-src' is used as a falled	ck. <u>www.gstatic.com/:1</u>

Because we used the content-security-policy-report-only we reported, but didn't block

Which means this script was loaded and also reported

Lets be smarter about it

💽 The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	
8 The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	<pre>local-dev.robotti.private/:1</pre>
S ► The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	web-client-content-script.js:2
She Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	recaptcha en.js:49
She Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	recaptcha en.js:23
Ø ►The Content Security Policy directive 'upgrade-insecure-requests' is ignored when delivered in a report-only policy.	recaptcha en.js:23
Navigated to https://local-dev.robotti.private/	
A The key "user-scale" is not recognized and ignored.	<pre>local-dev.robotti.private/:7</pre>
[Report Only] Refused to load media from 'https://local-dev.robotti.private/images/cincinnati skyline.mp4' because it violates the following Content Security Policy directive: "default-src none". Note that 'media-src' was no explicitly set, so 'default-src' is used as a fallback.	t <u>local-dev.robotti.private/:1</u>
[Report Only] Refused to load media from 'https://local-dev.robotti.private/images/cincinnati skyline.mp4' because it violates the following Content Security Policy directive: "default-src none". Note that 'media-src' was no explicitly set, so 'default-src' is used as a fallback.	t <u>local-dev.robotti.private/:1</u>
[Report Only] Refused to load the script 'https://www.google.com/recaptcha/api.js' because it violates the following Content Security Policy directive: "script-src 'self'". Note that 'script-src-elem' was not explicitly set, 'script-src' is used as a fallback.	<pre>so local-dev.robotti.private/:1</pre>
Seport Only] Refused to load the script 'https://www.gstatic.com/recaptcha/releases/-ObJqHf6OUB8nuVRLvzFLVed/recaptcha_en.js' because it violates the following Content Security Policy directive "script-src 'self'". Note was not explicitly set, so 'script-src' is used as a fallback.	e that 'script-src-elem' <u>api.js:1</u>
[Report Only] Refused to frame 'https://www.google.com/' because it violates the following Content Security Policy directive: "default-src none". Note that 'frame-src' was not explicitly so', so 'default-src' is used as a fa	llback. www.gstatic.com/:1
🔕 [Report Only] Refused to frame 'https://www.google.com/' because it violates the following Content Security Policy directive: "default-src none". Note that 'frame-src' was not explored by the state of the state	llback. www.gstatic.com/:1

But there's something off about this...



I never added script-src 'self'

Well we assumed...

	Raw		
Connection:		keep-alive	
Content-Length:		15293	
Content-Security-Policy-Report	t-Only:	default-src 'none';report-uri https://local-dev.robotti.pr	ivate/csp;base-uri 'self <mark>'</mark> font-src 'self' https: data <mark>f</mark> orm-action 'self;frame-ancestors 'self';img-src 'self'
		data;;object-src 'none';script-src 'self';script-src-attr 'no	ne style-src 'self' https: 'unsafe-inline upgrade-insecure-requests
Content-Type:		text/html; charset=utf-8	
Cross-Origin-Opener-Policy:		same-origin	
Cross-Origin-Resource-Policy:		same-origin	
Date:		Fri, 01 Dec 2023 15:14:58 GMT	What's worse is they sometimes assume bad not great things
Etag:		W/"3bbd-IfcJhoz2YaRw7FBp1zAoTAXi67k"	,
Keep-Alive:		timeout=5	
Origin-Agent-Cluster:		?1	
Referrer-Policy:		same-origin	

Some libraries that handle these headers assume you need certain directives set.

Directives:

- base-uri
- font-src
- form-action
- frame-ancestors
- img-src
- script-sreader
- style-src

Okay... Big brain smart time

Let's be super explicit with our policy. And set everything to 'none'



Okay... Big brain smart time

Navigated to https://local-dev.robotti.private/

A The key "user-scale" is not recognized and ignored.

local-dev.robotti.private/:7

www.gstatic.com/:1

www.gstatic.com/:1

not explicitly set, so 'script-src' is used as a fallback.

"default-src 'none'". Note that 'media-src' was not <u>local-dev.robotti.private/:1</u>

😥 [Report Only] Refused to load the stylesheet '<URL>' because it violates the following Content Security Policy directive: "style-src 'none'". Note that 'style-src-elem' was not explicitly set, so 'style-src' is used as a fallback.

(F178) [Report Only] Refused to load the font '<URL>' because it violates the following Content Security Policy directive: "font-src 'none'".

[Report Only] Refused to load the image '<URL>' because it violates the following

(Not the second termination of termination

[Report Only] Refused to load media from 'https://local-dev.robotti.private/images/ci explicitly set, so 'default-src' is used as a fallback.

[Report Only] Refused to frame 'https://www.google.com/' because it violates the foll

[Report Only] Refused to frame 'https://www.google.com/' because it violates the foll



205 Violations for one page

- Violation reporting services exist
 - O Report-uri.com
 - Csper.com



module.exports = { \$id: 'cspReport', description: 'URI Violation Request Schema', type: 'object', additionalProperties: false, properties: { 'document-uri': {--referrer: {---'blocked-uri': { ·· 'effective-directive': { --'violated-directive': { ·· 'original-policy': { -disposition: { ··· 'status-code': {---'script-sample': {---'source-file': {---'line-number': {··· 'column-number': { sample: {… required: ['blocked-uri', 'document-uri'. 'violated-directive',

'effective-directive': { type: 'string', enum: ['child-src', 'connect-src', 'default-src', 'font-src'. 'frame-src', 'img-src', 'manifest-src', 'media-src', 'object-src', 'prefetch-src', 'script-src', 'script-src-elem', 'script-src-attr', 'style-src', 'style-src-elem', 'style-src-attr', 'worker-src'. 'base-uri', 'sandbox', 'form-action'. 'frame-ancestors', 'navigate-to', 'require-trusted-types-for', 'trusted-types', 'upgrade-insecure-requests',

cons	<pre>t { ServiceBusClient } = require('@azure/service-bus'); the serviceDusClient'</pre>
cons	s ajy = require(_ajy), s schema = require(',./schemas/schema');
nodu	le exports = asymc (req, context) => {
	if (reg.method i== 'POST') (
	status: 405,
	body: Pethod Not Allowed ,
	Const validate a silv (; constantia (schown))
	const domain = req.query.set('domain'):
	const json = mmait reg.json();
	typeof domain [== 'string'
	[] domain_indext(f(f)) > 1 // Domain_shouldn't_contain_dny "/" characters [] three (7.250) block should excit.
	1 json / some ord should enter a body should contain a cta-report key
	typeof json['csp-report'] ! 'object' // The Json body csp-report should be an object
	!validate(json['csp-report']) // The csp-report should poss schema validation
	json['csp-report']['document-uri'].indexOf('://\$[reg.query.get('domain']]/') < 4 // The domain should be in the document-uri of the csp report at either the 4th or 5th pail
	[] Json['csp-report']['document-uri'].indexOr(://s(reg.query.get('domain'))/) > 5 // 4 would be http: Monormal and a should be http://statics.com/article
	context.warn(JSON.stringify()
	message: 'Invalid request',
	url: reg.url,
	method: reg.method,
	body: neg.body,
	and a second sec
	status: 400,
	body: 'Bad Request',
	<pre>const ch()int _ not control (abs/ch() = proces.env; const ch()int _ not control (abs/ch() = proces.env;</pre>
	const shSender = wailt shClient.createSender(shPath):
	await sb5ender.sendMessages([
	body: (
	domain,
	Tepa c. Jon Cartena c. 1.
	contentType: 'application/json',
	status: 204,
	catch (em) /
	context.eror(350N.stringify()
	message: err?.message,
	uni: reg.uni,
	nethod: reinethod,
	stat. missiat,
	Peters (
	status: 500,
	body: 'An Unexpected Error Occured',

Why all the validation? 1. Because this is open to all 2. I'm not hypocrite 3. It's javascript

1f (req.method !== 'POST') (
status: 485,
body: 'Method Not Allowed',
$(\alpha + \beta + $
const wildste = sky.com/lo(schem):
cost domain = reg.query.set('domain'):
const ison - await reg.ison();
typeof domain Imm 'string'
domain_indexOf('/') > -1 // Domain shouldn't contain any "/" characters
11 Ijson // JSON body should exist
[] [json['csp-report'] // json body shound contain a csp-report key
[] typeof json['csp-report'] 1 'object' // The json body csp-report should be an object
[Ivalidate(json['csp-report']) // The csp-report should pass schema validation
<pre>ijson['sp-report]['document-uri'].indexOf('://S[reg.query.get('domain')]/') < 4 // The domain should be in the document-uri of the csp report at either the 4th or 5th position</pre>
1 Json csp-report IL document-uni l'indexnet style regimery get domain (1/) > 5 // 2 would be http: [] Json csp-report IL document-uni l'indexnet style regimery get domain (1/) > 5 // 2 would be http:
Professor users(1904) statistic for (2)
contextage: 'Invalid request'
set hod _ rea.set hod
body: reg.body
status: 400,
body: 'Bad Request',
<pre>const (sbConnectionString, sbPath) = process.env;</pre>
const socilent = new ServiceWusClient(sbConnectionstring);
const spender = imait soliter.createsender(spratn);
awat sosenor.senoressages(
dowin
report icon (csp.penet).
contentType: 'application/json',
status: 204,
) catch (err) (
context.error(350%.stringity(
message: err/.message,
uni: Mag.uni,
atory and tank
Poly Control C
status: 500.
body: 'An Unexpected Error Occured',

Scaling Across Organization

- Training Developers
- Communication
- Pilot Groups
- Provide Tooling Access
- Phased Approach
- Progress Over Perfection

For science

- What do you do with the reports?
- Bandwidth?
- Other Pages?
- Recommended?
- Was it worth the effort?