

30 JULY 2018 / #JAVASCRIPT

# How to use JSON padding (and other options) to bypass the Same Origin Policy



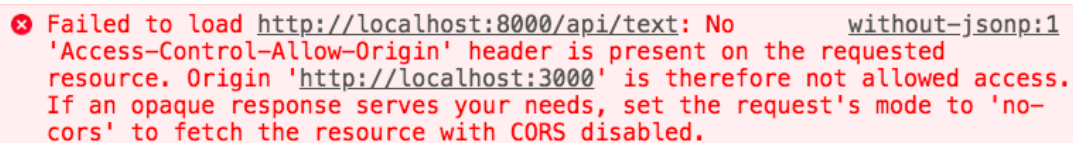
by Anthony Ng

In this article, we will be looking at what JSONP is, its drawbacks, and some alternatives to JSONP.

one origin to another. For example, we have a page served from localhost:3000 that is calling an API from localhost:8000.

**Note:** We will refer to localhost:3000 as our client server. We will refer to localhost:8000 as our API server.

But we see this intimidating error.



```
✖ Failed to load http://localhost:8000/api/text: No without-jsonp:1
'Access-Control-Allow-Origin' header is present on the requested
resource. Origin 'http://localhost:3000' is therefore not allowed access.
If an opaque response serves your needs, set the request's mode to 'no-
cors' to fetch the resource with CORS disabled.
```

Error when trying to make fetch call from client server to api server

This is the Same-Origin Policy protecting us. This policy restricts how resources from one origin interact with resources from another origin. It is a critical security mechanism in the browser. But there are instances where we want to make cross-origin requests to trusted resources.

JSONP (JSON with Padding) provides a work-around for this Same-Origin Policy problem. Let's look at how JSONP came to be.

## Technical dive

We can run JavaScript code inside our HTML file with `<script>` tags.

We can move our JavaScript code into a separate JavaScript file and reference it with our script tag. Our webpage now makes an external network call for the JavaScript file. But functionally, everything works the same.

browser will interpret content as JavaScript if the response's Content-Type is JavaScript. ( text/javascript , application/javascript ).

Most servers allow you to set the content type. In Express, you would do:



Setting Content-Type header for Response

Your `<script>` tag can reference a URL that doesn't have a js extension.

Script tags are not limited by the Same-Origin Policy. There are other tags, such as `<img>` ; and `<video>` tags, that are not limited by the Same-Origin Policy. So our JavaScript can live on a different origin.

The code inside the JavaScript file has access to everything that is in scope. You can use functions defined earlier in your HTML file.

You can pass arguments as you would for a normal function call.

In the above example, we passed a hard-coded string. But we could also pass in data coming from a database. Our API server can construct the JavaScript file with this dynamic information.

make an API call to retrieve data, we used a `<script>` tag. Because we used a `&lt;script>` tag, we were able to bypass the Same-Origin Policy.

As I mentioned above, JSONP means JSON with Padding. What does the padding mean? Normal API responses return JSON. In JSONP responses, we return the JSON response surrounded (or padded) with a JavaScript function.



Artist rendition of JSON with Padding

Most servers allow you to specify the name of your padding function.

The server takes your padding function name as a query. It invokes your padding function with the JSON data as an argument.

You are not limited to passing function names as your callback. You can pass inline JavaScript in your query.

I have not thought of a reason to do this.


## Alternatives to using JSONP

There is no official spec for JSONP. I think of JSONP as more of a hack.

`<script>` tags can only make GET requests. So JSONP can only make GET requests.

Cross-Origin Resource Sharing has an official specification, and is the preferred way of getting around the Same-Origin Policy.

You can enable Cross-Origin Resource Sharing by adding a header to our Response.



```
response.set('Access-Control-Allow-Origin', '*');
```

This means all origins can use this resource without fear of the Same-Origin Policy.

Sometimes, you don't have control over the server-code though. You would not be able to include the `Access-Control-Allow-Origin` header. An alternate solution is to make your own proxy server make the cross-origin request for you. The Same-Origin policy only applies to the browser. Servers are free to make cross-origin requests

Questions? Comments? Please leave a message below.

## Resources

- [Same Origin Policy](#)
- [Github Repository with JSONP and CORS examples](#)
- [Detailed explanation of JSONP](#)

Show comments

Countinue reading about

## JavaScript

Conquering Job Interview Code Challenges v1.0

---

Why Naked Promises Are Not Safe For Work - and What to Do Instead

---

The Cure to Javascript Fatigue - and All Other Fatigues

---

See all 1469 posts →



#TECH

## Amazon Web Services (AWS) explained by operating a brewery

A YEAR AGO

# BABEL

#JAVASCRIPT

## Why We Removed Babel's Stage Presets: Explicit Opt-In of Experimental Proposals

A YEAR AGO

Our mission is help people learn to code for free. We accomplish this by creating thousands of videos, articles, and interactive coding lessons - all freely available to the public. We also have thousands of freeCodeCamp study groups around the world.

Donations to freeCodeCamp go toward our education initiatives, and help pay for servers, services, and staff. You can [make a tax-deductible donation here](#).

### Our Nonprofit

About  
Donate  
Shop  
Alumni Network  
Open Source  
Support  
Sponsors  
Academic Honesty  
Code of Conduct  
Privacy Policy  
Terms of Service  
Copyright Policy

### Best Examples

Python Example  
JavaScript Example  
React Example  
Linux Example  
HTML Example  
CSS Example  
SQL Example  
Java Example  
Angular Example  
jQuery Example  
Bootstrap Example  
PHP Example

### Best Tutorials

Python Tutorial  
Git Tutorial  
Linux Tutorial  
JavaScript Tutorial  
React Tutorial  
HTML Tutorial  
CSS Tutorial  
SQL Tutorial  
Java Tutorial  
Angular Tutorial  
WordPress Tutorial  
Bootstrap Tutorial

### Trending Reference

2019 Web Developer Roadmap  
Linux Command Line Guide  
Git Reset and Git Revert  
Git Merge and Git Rebase  
JavaScript Array Map  
JavaScript Array Reduce  
JavaScript Date  
JavaScript String Split  
CSS Flexbox Guide  
CSS Grid Guide  
Create a Linux Sudo User  
How to Set Up SSH Keys