

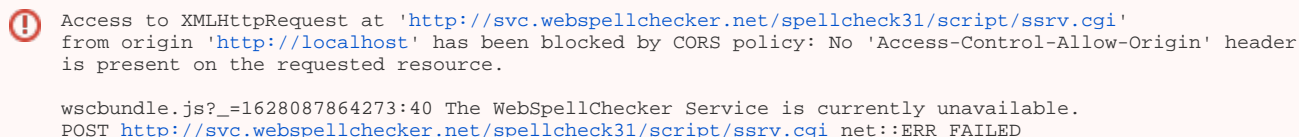
# CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.

## Problem and Symptoms

All of a sudden, starting August 5, 2021, the spell checking service stopped working despite the fact that previously it worked properly. There are CORS errors in browser console and failed request observed in network tabs.

**Affected products/integrations:** WProofreader add-on for RTEs, WProofreader plugin for CKEditor 5, SCAYT and Spell Check Dialog (WSC) plugins for CKEditor 4 utilizing the Cloud version.

Here is an example of an error thrown in the browser console:

A screenshot of a browser console error. It features a red warning icon on the left. The text of the error is: "Access to XMLHttpRequest at 'http://svc.webspellchecker.net/spellcheck31/script/ssrv.cgi' from origin 'http://localhost' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource." Below this, there is a log entry: "wscbundle.js?\_=1628087864273:40 The WebSpellChecker Service is currently unavailable. POST http://svc.webspellchecker.net/spellcheck31/script/ssrv.cgi net::ERR\_FAILED".

```
! Access to XMLHttpRequest at 'http://svc.webspellchecker.net/spellcheck31/script/ssrv.cgi'
  from origin 'http://localhost' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header
  is present on the requested resource.

wscbundle.js?_=1628087864273:40 The WebSpellChecker Service is currently unavailable.
POST http://svc.webspellchecker.net/spellcheck31/script/ssrv.cgi net::ERR_FAILED
```

## Root cause

Effective August 5, 2021, we introduced the security update/improvement for all cloud services that restricts the access to the service over HTTP. Technically, all the requests to HTTP are redirected to HTTPS. It works properly for static web content and direct API requests but not for API requests originated from other origins which are blocked by cross-origin resource sharing (CORS) policy.

## Solution

To solve the issue, the service resources must be loaded via HTTPS. Thus, the updates in the configuration of the service are required. It doesn't mean that you need to change the configuration of your website or web app to HTTPS right away. However, it is highly recommended as a modern best practice to ensure data security, integrity and privacy.

### SCAYT & WSC plugins for CKEditor 4

If you are using the plugins for CKEditor 4, please add the **scayt\_srcUrl** (for SCAYT) or **wsc\_customLoaderScript** (for WSC) to CKEditor **config.js** along with the rest settings that will load the plugin resources via HTTPS.

```
// for SCAYT
config.scayt_srcUrl = 'https://svc.webspellchecker.net/spellcheck31/wscbundle/wscbundle.js';

// for WSC
config.wsc_customLoaderScript = 'https://svc.webspellchecker.net/spellcheck/lf/22/js/wsc_fck2plugin.js';
```

### WProofreader add-on for RTEs

In case of WProofreader integration, just load **wscbundle.js** script over HTTPS.

```
<script type="text/javascript" src="https://svc.webspellchecker.net/spellcheck31/wscbundle/wscbundle.js"><
/script>
```