Access-Control-Allow-Origin (CORS) header beállítása .htaccess segítségével

Első lépésként ha még nem létezik .htaccess fájl az érintett domain név dokumentum root könyvtárában akkor hozza létre. Ehhez az alábbi leírásban találhat segítséget:

Hogyan hozhatok létre .htaccess fájlt?

Abban az esetben ha a fájl már létezik akkor az alábbi leírások alapján tudja Őket szerkeszteni:

- Fájl létrehozása és módosítása FTP-n keresztül
- Fájl létrehozása és módosítása SSH-n keresztül

Íme egy gyorsan beilleszthető kód részlet, amelyet akkor használhat, ha be kell állítania az Access-Control-Allow-Origin fejléceket a .htaccess fájljában.

Az Access-Control-Allow-Origin meghatározása:

Biztonsági okokból a böngészők korlátozzák a szkripteken belül kezdeményezett, több forrásból származó HTTP-kéréseket. Például az XMLHttpRequest ugyanazt a származási házirendet követi. Tehát egy XMLHttpRequest alkalmazást használó webalkalmazás csak HTTP kéréseket küldhet a saját domain nevére. A webes alkalmazások fejlesztése érdekében a fejlesztők arra kérték a böngészőgyártókat, hogy engedélyezzék az XMLHttpRequest számára, hogy domain nevek közötti kéréseket engedélyezzék.

[…]

A CORS a webszerverekhez a domain nevek közötti hozzáférés-vezérlést biztosít, amelyek lehetővé teszik a biztonságos domain nevek közötti adatátvitelt.

Access-Control-Allow-Origin

A CORS BEÁLLÍTÁSA

A használatához tehát be kell állítania a megfelelő fejléceket. A `.htaccess` fájlban adja hozzá az alábbi kódrészletet:

```
Header Set Access-Control-Allow-Origin "https://az.on.kulso.eroforrasanak.cime.vegzodes"
```

A fentiek lehetővé teszik a fejlécet küldő webhely számára, hogy erőforrásokat (például AJAX kéréseket vagy webes betűtípusokat) kérjen a *„https: //az.on.kulso.eroforrasanak.cime.vegzodes”* domain név alatt elhelyezett weboldalról. Vegye figyelembe a protokollt, ez – ebben az esetben – csak a HTTPS kéréseket teszi lehetővé. A HTTP -kérések továbbra is blokkolva lesznek.

A CORS LETILTÁSA

Ha teljesen le szeretné tiltani a CORS-t (amit nem javaslunk, azonban tesztelés esetében hasznos lehet) akkor az alábbi kódrészletet helyezze el a `.htaccess` fájlban:

```
Header Set Access-Control-Allow-Origin "*"
```

Mint fentebb említettük, biztonságosabb úgy beállítani, hogy az Access-Control-Allow-Origin tartalmazza azokat a domain neveket, amelyekről az alkalmazás adatokat kérhet (vagy adatokat küldhet).

A CORS ENGEDÉLYEZÉSE TÖBB DOMAIN NÉVRE VONATKOZÓAN

Ha több domain neve van, és CORS fejlécet szeretne beállítani az adott domain név alapján, akkor használhatja az alábbi kódrészletet a `.htaccess` fájlban:

```
SetEnvIf Origin "http(s)?://(www\.)?(google.com|staging.google.com|development.google.com)$" Acc
Header add Access-Control-Allow-Origin %{AccessControlAllowOrigin}e env=AccessControlAllowOrigir
```

Mivel a fejlécben csak egy CORS domain név lehet, ezért létre kell hoznia egy változót, ha ezt több helyen szeretné használni.

Változat #3
DotRoll Tudásbázis hozta létre 2023-09-21 09:46:51 CEST
DotRoll Tudásbázis frissítette 2023-09-26 10:46:18 CEST