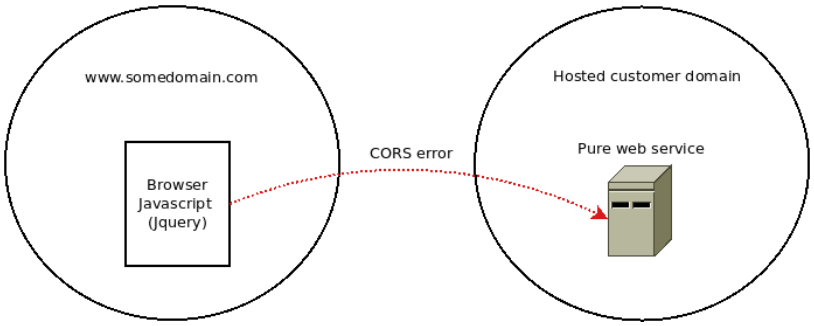
CORS header missing

Pure customers sometimes try to leverage data from Pure by trying to call the Pure web service directly from JQuery from a different web site/domain. This results in the browser refusing to make the call with the message ***CORS header 'Access-Control-Allow-Origin' missing***. To disable this fundamental security feature by adding this header to all requests cannot be recommended.

Although this may seem like a very convenient way of leveraging data there are some inherent problems with this.

1. Security. If the Pure web service is called directly from JQuery then data will be returned directly into the browser. This means that even though the web site potentially only displays some of the retrieved data fields then all the data can be seen in the browsers console. This could lead to disclosure of sensitive customer data.
2. Performance. The Pure web service was not designed to handle browser traffic from outside Pure, think bots harvesting the website. How much load to the service will be added by the new use of the service? For instance, will the service be called each time someone visits another web site?



Solution

In stead of calling the Pure web service directly from JQuery you should build a small server application, e.g. a REST service, that runs on the same domain. Then the browser will no longer complain because the JQuery request is for a resource on the same domain. This solution has the potential to address the problems mentioned above.

1. Security. The server application/service can implement filtering of the data returned from Pure so that not everything is returned to the browser and only the intended data for the web page.
2. Performance. The server application/service can implement caching so that the Pure web service is not called many times a day for the same data. The /changes endpoint can be used to trigger updates to remotely stored data.