## H2.CL Downgrade attack

This type of attack targets specifically the HTTP/2 version and happens when the frontend accepts the HTTP/2 protocol, but the backend only does the HTTP/1. This will create a mismatch and consequently a Disconnect attack.

### Exploit example

Let's take as example that we send to the frontend the following payload(header name is red, header values are green and body is yellow):

:method POST

:path /

:authority http2.htb

:scheme http

content-length 0

GET /smuggled HTTP/1.1

Host: http2.htb

In the http/2 the body length is calculated by the protocol so shipping the CL in the request is obsolete but what if the frontend that supports the HTTP/2 protocol parses it wrongly? This means that the frontend with rely back by rewriting the request to a HTTP/1 protocol version using the (CL=wrong size) resulting to 2 different streams that will be sent forward to the backend webserver:

POST / HTTP/1.1

Host: http2.htb

Content-Length: 0

GET /smuggled HTTP/1.1

Host: http2.htb

The problem arises here because the frontend will see the request incoming as HTTP/2 with only the POST / and the GET /smuggled will be part of the body in a same request, but the frontend will receive from the frontend 2 different HTTP/1 request and create a missmatch.