18th January 2023

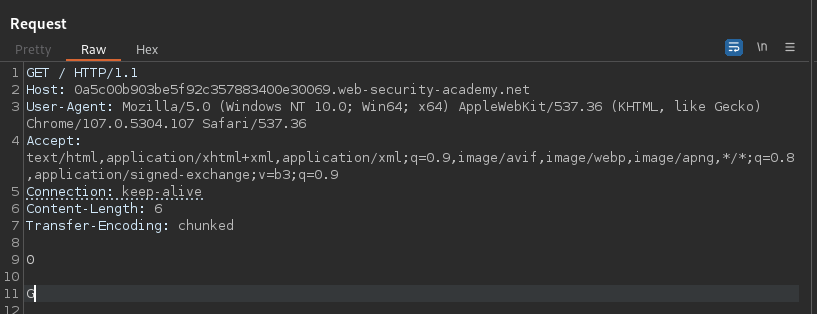
**HTTP REQUEST SMUGGLING LAB 1**

**Summary of Results**

The lab involves a front-end and back-end server, and the front-end server doesn't support chunked encoding. The front-end server rejects requests that aren't using the GET or POST method. Since the front-end server uses ‘Content-length’ header, a request is smuggled to the back-end server, so that the next request processed by it appears to use the method GPOST.

**Attack Narrative**

A request to the blog site is intercepted in burp suit’s proxy, and both the headers, ‘Content-Length’ and ‘Transfer-Encoding’ supported by HTTP specifications are added.



The request is forwarded to the website twice, which returns an ‘Unrecognised method GPOST’from the server.

This occurs because the Content-length specifies 6 bytes till the end of zero. This request is processed by the front-end server. The back-end server processes only the ‘Transfer-Encoding’ header which is terminated with a chunk of size zero.

The response ‘Unrecognised method GPOST’ confirms the presence of CL.TE vulnerability.

