

HTTP Request Smuggling

A scenic view of a harbor at sunset. The sky is filled with vibrant orange, pink, and purple clouds. In the foreground, a paved walkway with trees and streetlights leads towards the water. A small pier extends into the harbor, where several sailboats are docked. In the background, a city skyline is visible on the left, and a range of mountains is on the right. The overall atmosphere is peaceful and picturesque.



Motivation

New Technique

Flexible

- Web cache poisoning
- Web cache deception
- Session Hijacking
- ...

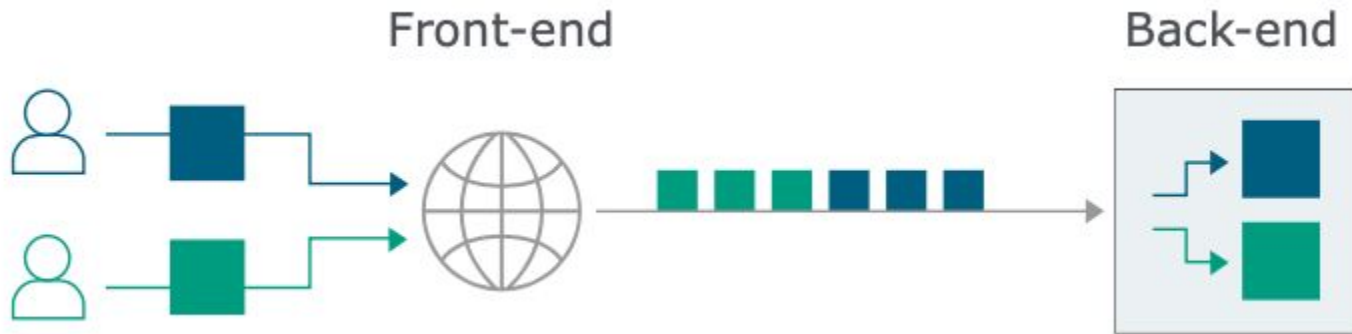
HTTP 1 vulnerabilities

Problem

HTTP request smuggling takes advantage of how a front and back end reads requests differently



Problem



Problem





Challenges

Implementation

- Legal issue
- Complex HTML architecture
- Uncertainty of indicators

Countermeasure

- HTTP/1.1 itself's vulnerability

Solutions

- Tutorial web page designed for the attack
- Brute-force attack template
- Upgrade to HTTP/2





Results

- Burp Suite (Tool used to send requests)
- CL.TE Attack (Content Length Transfer Encoded)
- TE.CL Attack (Transfer Encoded Content Length)

Basic CL.TE Attack

Burp Suite Community Edition

Burp Suite Community Edition v2020.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to https://acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net:443 [18.200.141.238]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
1 GET / HTTP/1.1
2 Host: acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://portswigger.net/web-security/request-smuggling/lab-basic-cl-te
8 DNT: 1
9 Connection: close
10 Cookie: session=vQEDYiFHMH0cA9eY2qIK0Yy426ZxEQhr
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14
```

0 matches

HTTP request smuggling, basic CL.TE vulnerability - Mozilla Firefox

HTTP request smuggling X +

WEB SECURITY ACADEMY

HTTP request smuggling, basic CL.TE vulnerability

LAB Not solved

Back to lab description >>

WE LIKE TO BLOG

Waiting for acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net...

Basic CL.TE Attack

Burp Suite Community Edition

Burp Suite Community Edition v2020.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Send Cancel < >

Target: <https://acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net>

Request

Raw Params Headers Hex

```
1 GET / HTTP/1.1
2 Host:
  acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:73.0)
  Gecko/20100101 Firefox/73.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer:
  https://portswigger.net/web-security/request-smuggling/lab-b
  asic-cl-te
8 DNT: 1
9 Connection: close
10 Cookie: session=vQEDYiFmH0cAseYzqIK0Yy426ZxE0h2
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
```

Response

Raw

Optional: Remove extra information. Done for clarity in the demo although not necessary.

HTTP request smuggling, basic CL.TE vulnerability - Mozilla Firefox

HTTP request smuggling: X +

http://120%

WEB SECURITY ACADEMY

HTTP request smuggling, basic CL.TE vulnerability

LAB Not solved

Back to lab description >>

WE LIKE TO BLOG

Basic CL.TE Attack

The image shows a dual-screen setup. The left screen displays Burp Suite Community Edition v2020.1. The 'Repeater' tab is active, showing a request to `https://acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net`. The request is a POST with headers: `Host: acdf1f321f0f1dc58065174b00a200c0.web-security-academy.net`, `Connection: keep-alive`, `Content-Type: application/x-www-form-urlencoded`, `Content-Length: 12`, and `Transfer-Encoding: chunked`. The body contains `0` followed by `CMFT479`. Annotations include a blue line pointing to the Host header, a green line pointing to the Transfer-Encoding header, and a red line pointing to the body content.

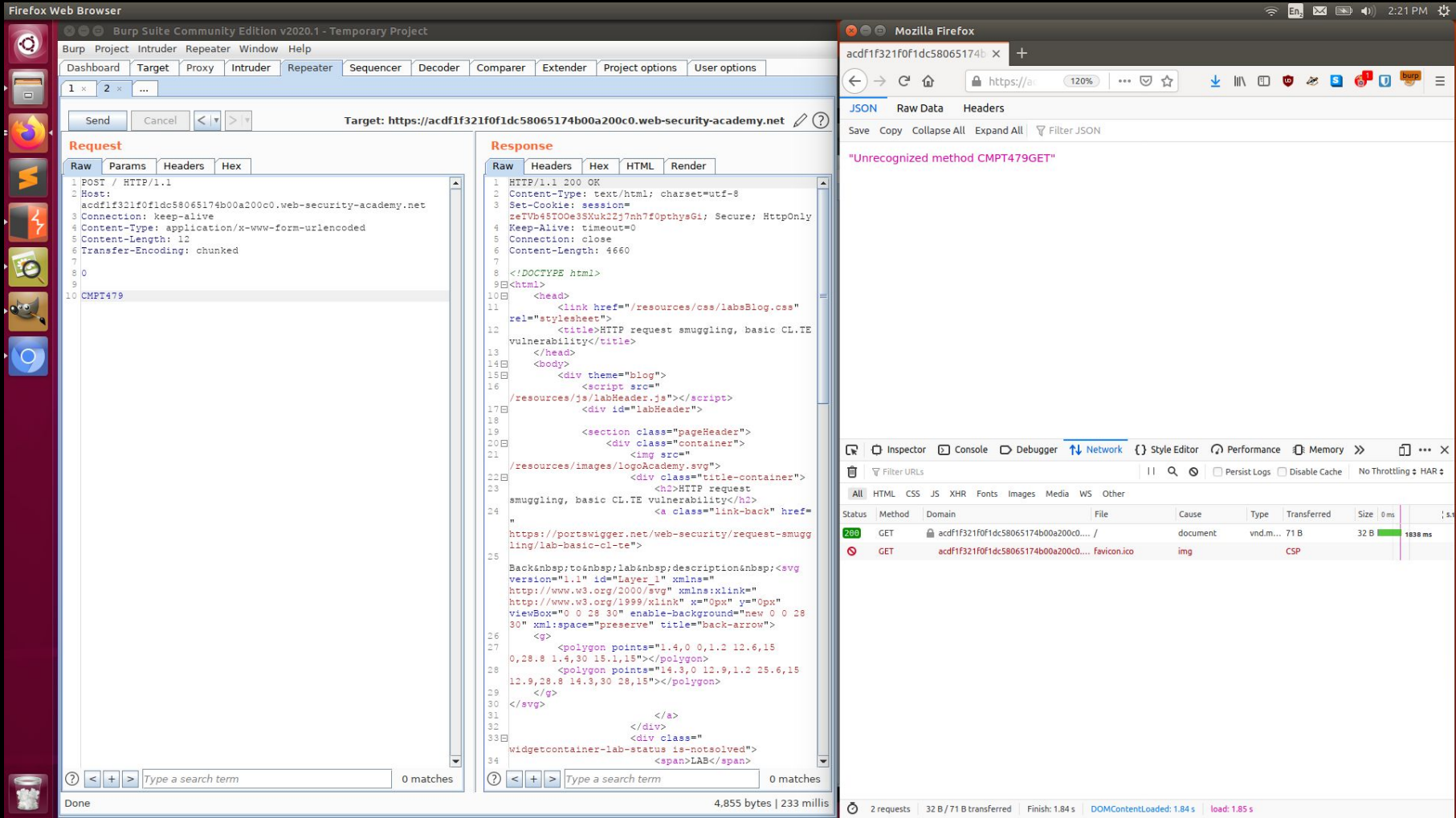
Step 1: Switch GET to POST

Step 2: Establish the use of both CE.TE headers

Step 3: Craft your attack for the next user of the site

The right screen shows a Mozilla Firefox browser window titled 'HTTP request smuggling, basic CL.TE vulnerability - Mozilla Firefox'. The address bar shows `http://` with a 120% zoom. The page content includes the 'WEB SECURITY ACADEMY' logo, a 'LAB Not solved' badge, and the text 'HTTP request smuggling, basic CL.TE vulnerability'. Below this is a 'Back to lab description' link. The main content area features the text 'WE LIKE TO BLOG' with a stylized face icon, and a background image of a crowd at a festival with their hands raised.

Basic CL.TE Attack



Questions?

