
HTTP Request Smuggling

Motivation

New Technique

Flexible

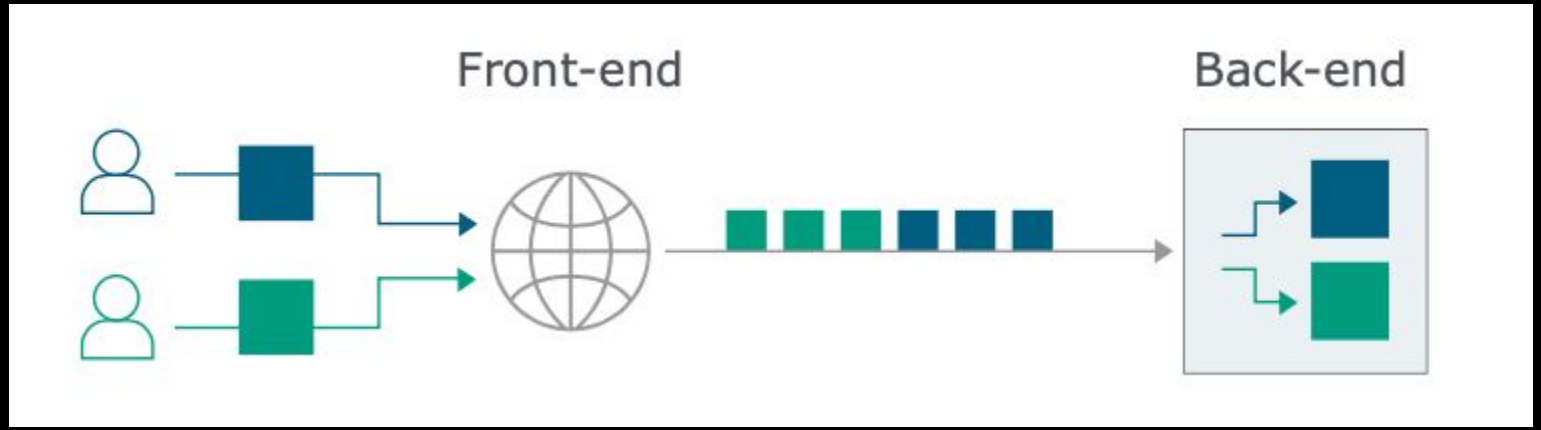
- Web cache poisoning
- Web cache deception
- Session Hijacking
- ...

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

Burp Project Intruder Repeater Window Help

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 Comment this item

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

WEB SECURITY ACADEMY

HTTP request smuggling, basic CL.TE vulnerability

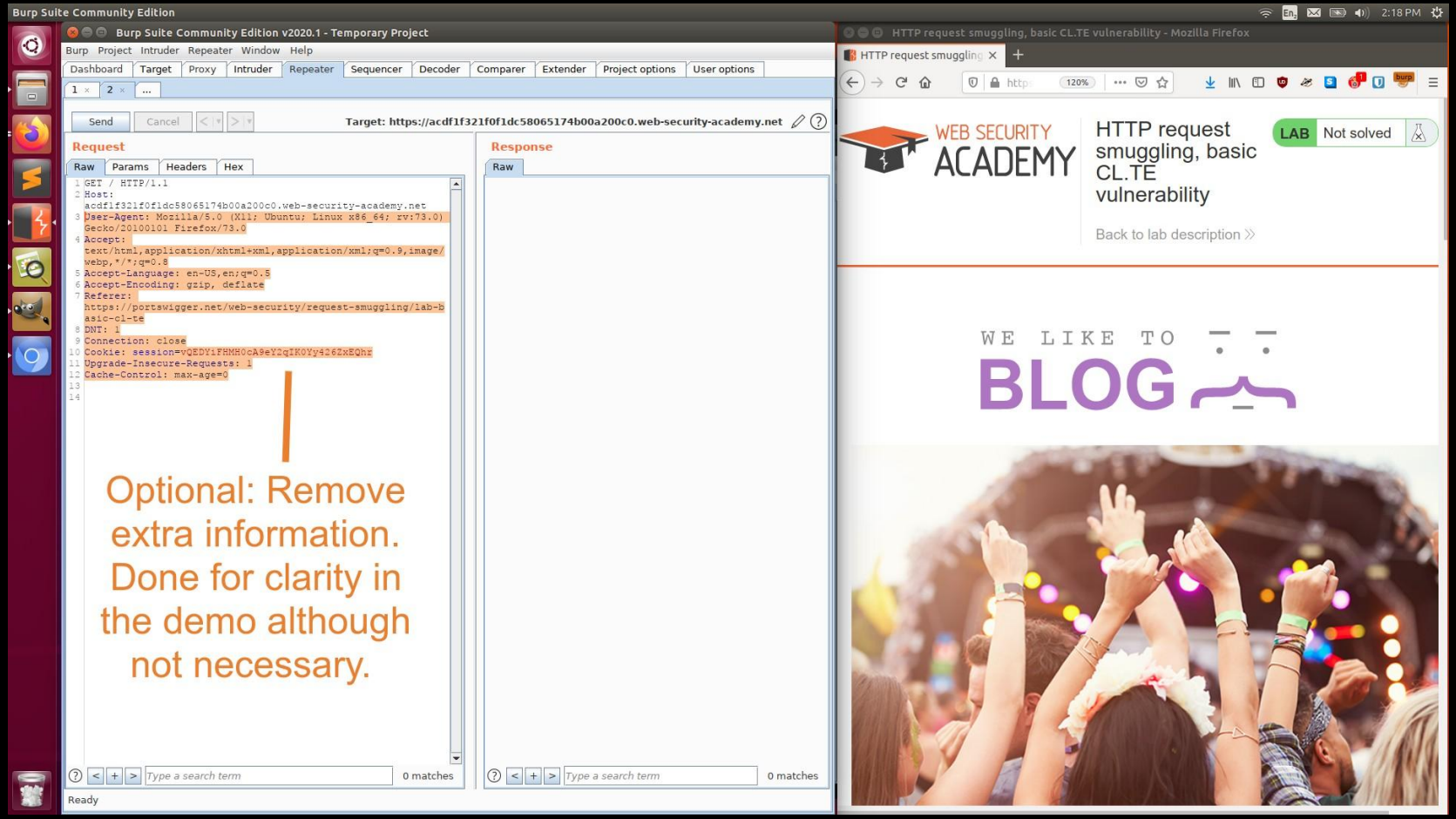
LAB Not solved

Back to lab description

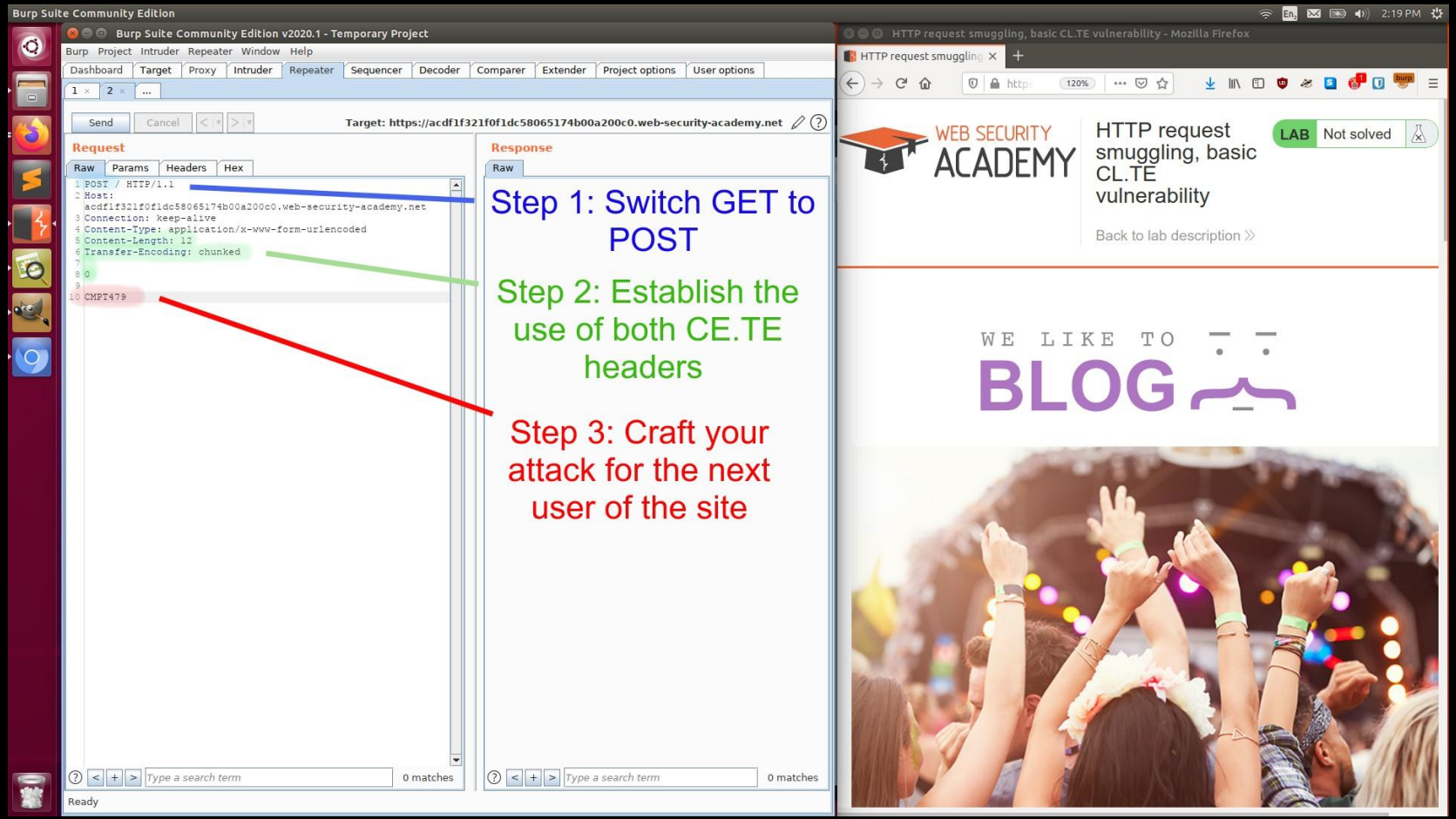
WE LIKE TO BLOG

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

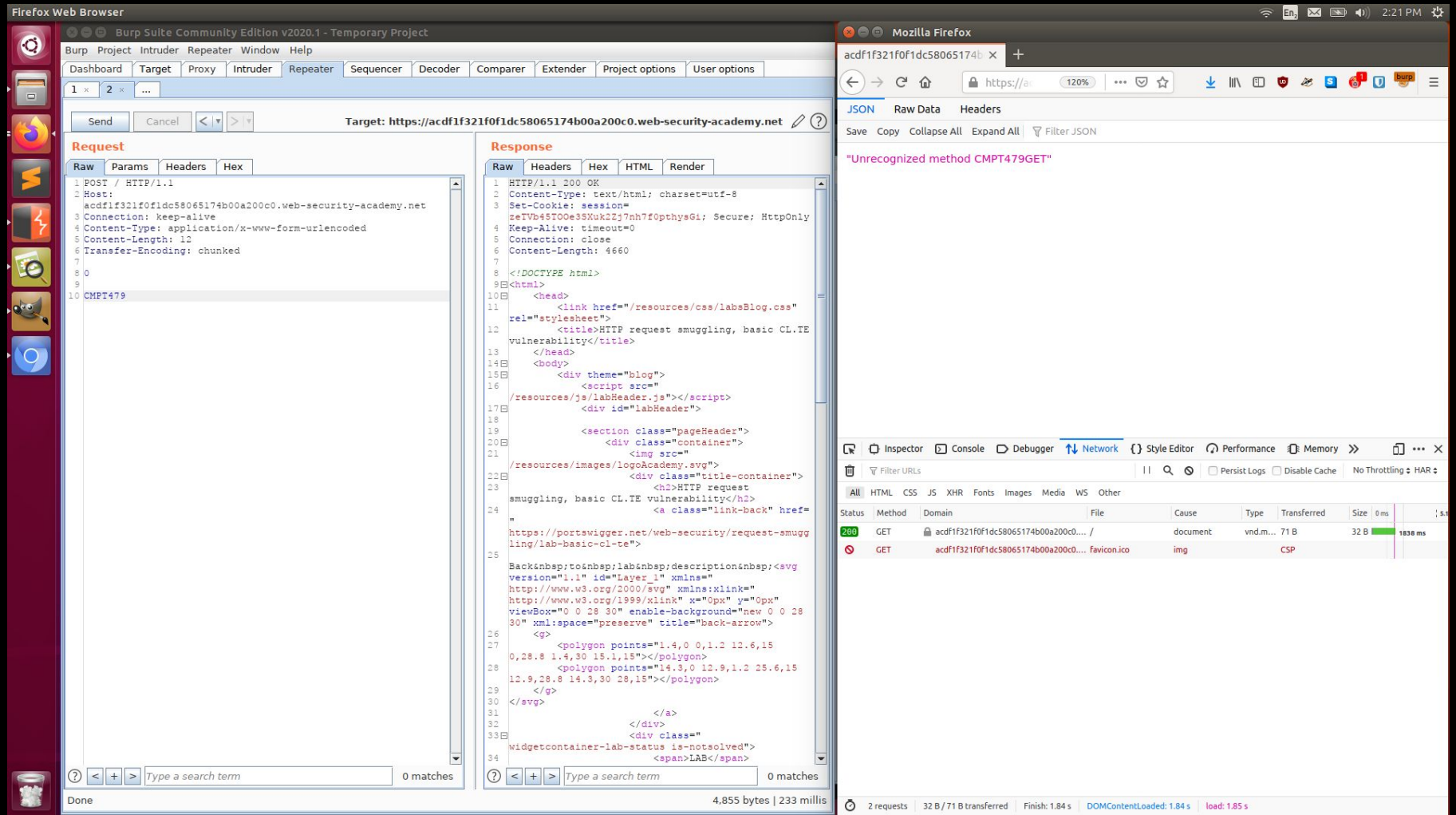
Basic CL.TE Attack



Basic CL.TE Attack



Basic CL.TE Attack



Questions?