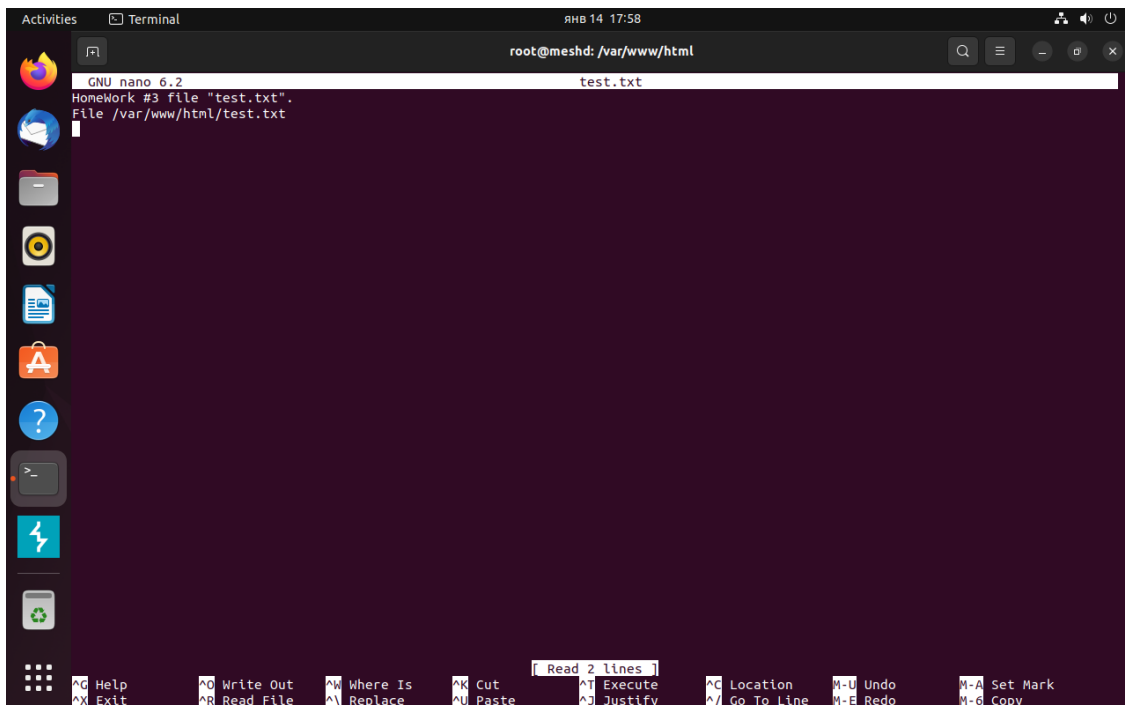


Выполнил Мешечкин Д. Инфобез-2345

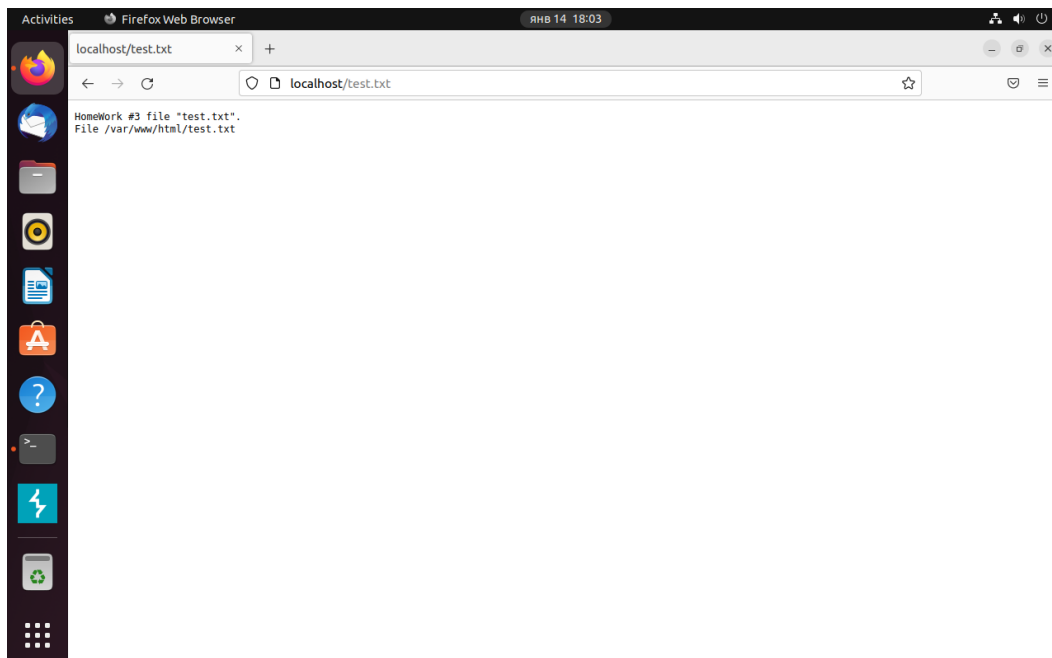
Задание 1: Создать файл test.txt в корневом каталоге сервера. Получить этот файл через браузер.

- Установить в терминале программу curl, получить тот же файл с помощью этой программы.
- Установить telnet или netcat, получить тот же файл с помощью одной из этих программ.

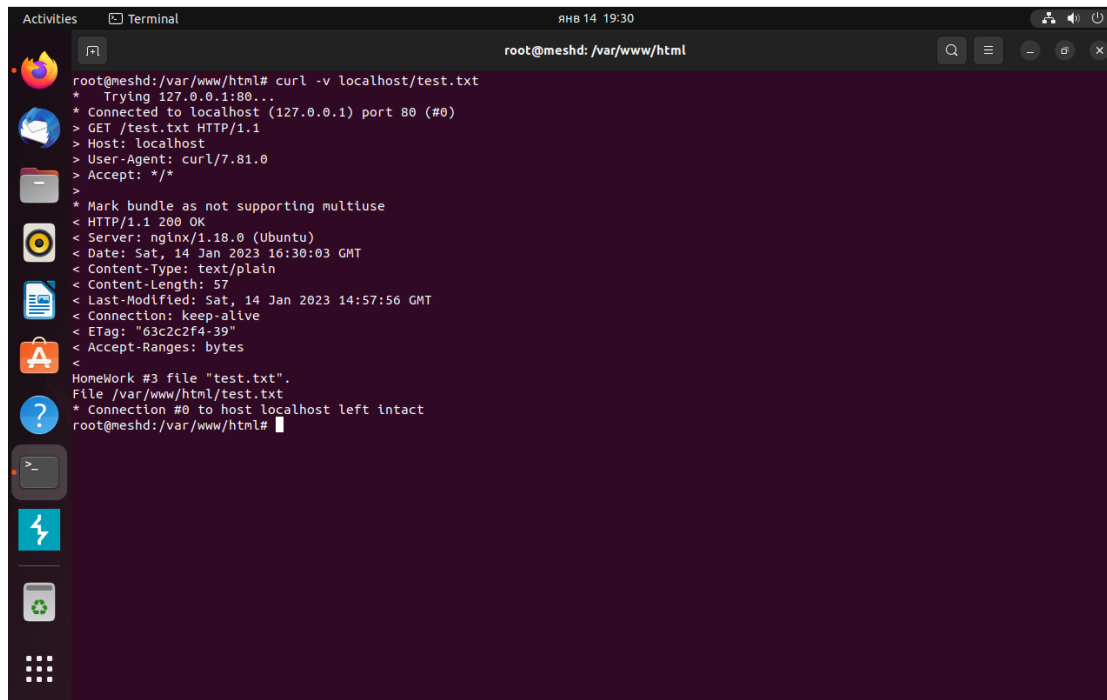
Первым делом создаётся файл test.txt с некоторым наполнением.



Получение файла через браузер.

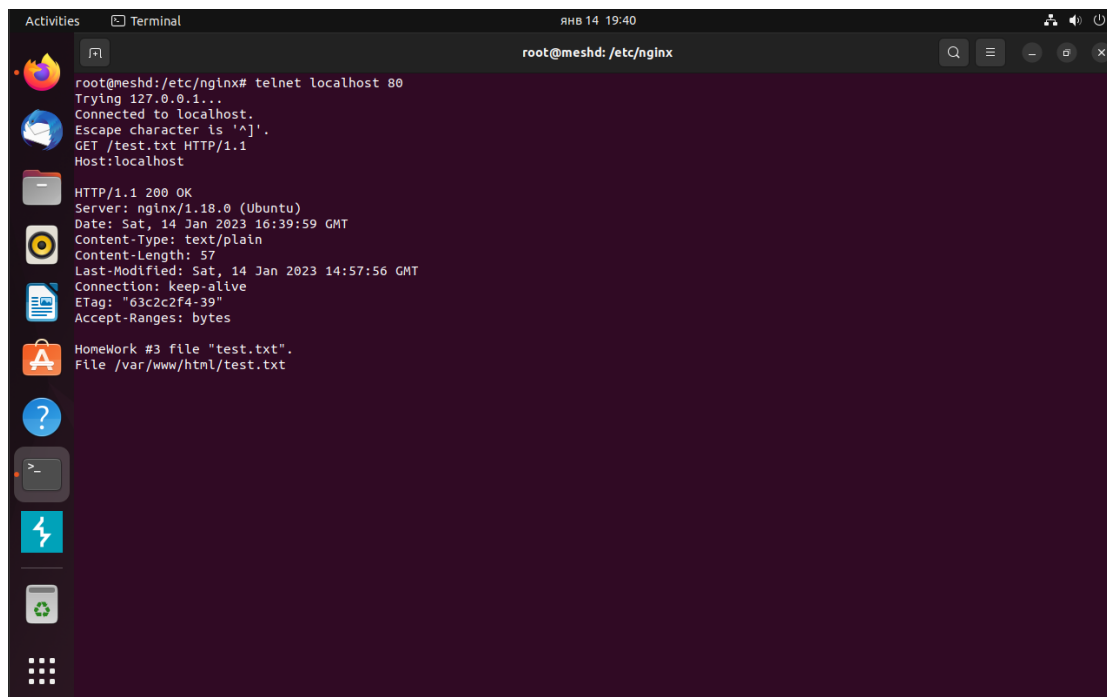


Получение файла задания через curl запрос



```
root@meshd:/var/www/html# curl -v localhost/test.txt
* Trying 127.0.0.1:80...
* Connected to localhost (127.0.0.1) port 80 (#0)
> GET /test.txt HTTP/1.1
> Host: localhost
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Sat, 14 Jan 2023 16:30:03 GMT
< Content-Type: text/plain
< Content-Length: 57
< Last-Modified: Sat, 14 Jan 2023 14:57:56 GMT
< Connection: keep-alive
< ETag: "63c2c2f4-39"
< Accept-Ranges: bytes
<
HomeWork #3 file "test.txt".
File /var/www/html/test.txt
* Connection #0 to host localhost left intact
root@meshd:/var/www/html#
```

Получение файла задания через telnet запрос



```
root@meshd:/etc/nginx# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /test.txt HTTP/1.1
Host:localhost

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 14 Jan 2023 16:39:59 GMT
Content-Type: text/plain
Content-Length: 57
Last-Modified: Sat, 14 Jan 2023 14:57:56 GMT
Connection: keep-alive
ETag: "63c2c2f4-39"
Accept-Ranges: bytes

HomeWork #3 file "test.txt".
File /var/www/html/test.txt
```

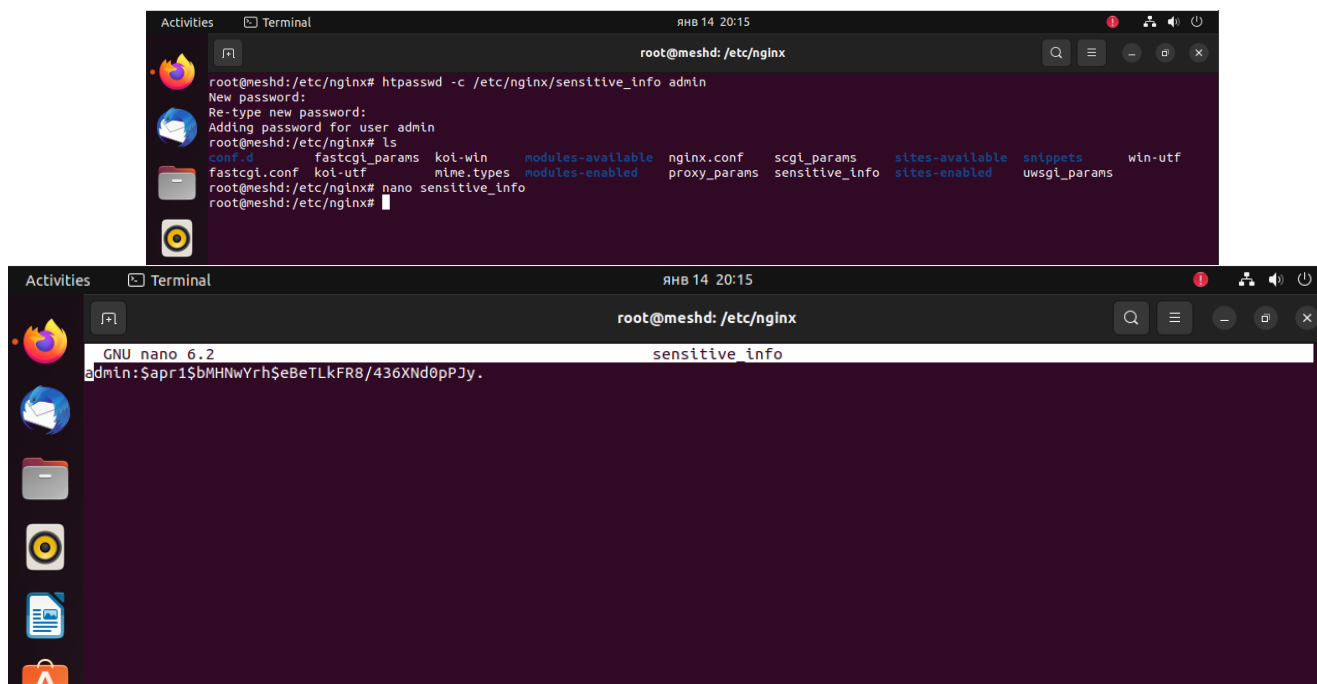
Задание 2: Создать на сервере файл sensitive_info.txt. Добавить базовую HTTP авторизацию для этого файла.

- Получить этот файл через браузер.
- Получить тот же файл с помощью curl и telnet или netcat.

Для создания базовой авторизации на сервере nginx воспользуюсь созданием файла авторизации через htpasswd

htpasswd -c /etc/nginx/sensitive_info admin #используется с sudo htpasswd

Таким образом в директории nginx будет создан файл содержащий записи "логин/пароль"



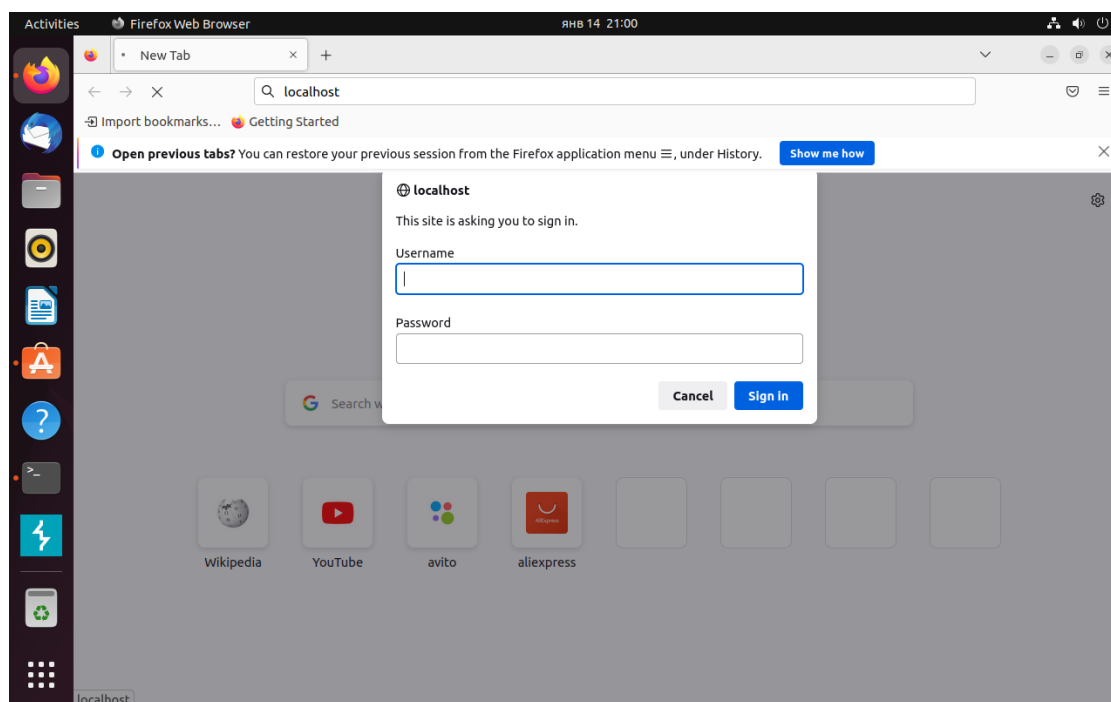
В зависимости от секции добавления `http/location` данный файл будет защищать весь сайт/ директиву сайта. Для выполнения данного задания данный файл "засуну" просто в секцию `http` файла `/etc/nginx/nginx.conf`

После необходимо перезагрузить конфигурацию сервера.

`nginx -s stop` #остановить nginx

`nginx` #запустить nginx

Запрос через браузер выдаёт запрос на ввод пары логин/пароль.



Далее запросы через curl и telnet.

```
Activities Terminal ЯНВ 14 21:06 root@meshd: /etc/nginx

root@meshd:/etc/nginx# curl localhost
<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
root@meshd:/etc/nginx#
```

```
Activities Terminal ЯНВ 14 21:07 root@meshd: /etc/nginx

root@meshd:/etc/nginx# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
GET / HTTP/1.1
Host:localhost

HTTP/1.1 401 Unauthorized
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 14 Jan 2023 18:07:06 GMT
Content-Type: text/html
Content-Length: 188
Connection: keep-alive
WWW-Authenticate: Basic realm="Need Login/Password"

<html>
<head><title>401 Authorization Required</title></head>
<body>
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
```

Задание 3: Открыть инструменты разработчика, вкладку Сеть (Network). Зайти на сайт <https://geekbrains.ru>. Проанализировать куки каждого запроса за HTML и картинками. Какие запросы уходят с куками, а какие без кук? Почему в каждом из случаев происходит именно такое поведение?

The screenshot shows the GeekBrains website in a browser. The Network tab is open, displaying a list of requests. The selected request is a POST to `https://gb.ru/event/token...`. The response headers for this request are:

- `access-control-allow-credentials: true`
- `access-control-allow-headers: Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization, Host, X-Auth-Token`
- `access-control-allow-methods: POST, GET, OPTIONS, PUT, DELETE, UPDATE, PATCH`
- `access-control-allow-origin: https://gb.ru`
- `access-control-max-age: 86400`
- `content-length: 15`
- `content-type: application/json; charset=utf-8`
- `date: Sat, 14 Jan 2023 18:58:05 GMT`
- `server: QVAROR`
- `strict-transport-security: max-age=15724800`
- `X-Frame-Options: deny`

The request headers show:

- `Accept: */*`
- `Accept-Encoding: gzip, deflate, br`

Первый рассматриваемый запрос json - текстовый запрос на основе JavaScript. В данном кука имеет в себе атрибуты ID, вариант аутентификации, регион, срок жизни, домен и , подробнее можно рассмотреть через BurpSuite.

Cookie: qrator_msid=1673720439.096.hxfB4ZLyn4OAEg60-ule1b7c644jrf8unvncueb0e6qcg51a; auth.strategy=local; gb_lang_cookie=ru; regionIdV1=RU; lastDefinedRegionIdV1=RU; sbjs_migrations=1418474375998%3D1; sbjs_current_add=fd%3D2023-01-14%2021%3A20%3A48%7C%7C%7Cep%3Dhttps%3A%2F%2F2Fgb.ru%2F%7C%7C%7Cr%3D%28none%29; sbjs_first_add=fd%3D2023-01-14%2021%3A20%3A48%7C%7C%7Cep%3Dhttps%3A%2F%2F2Fgb.ru%2F%7C%7C%7Cr%3D%28none%29; sbjs_current=typ%3Dtypein%7C7C%7Csrc%3D%28direct%29%7C7C%7Ccmdm%3D%28none%29%29%7C7C%7Ccmp%3D%28none%29...a8bd55a1c130-7; _ym_visitor-w; tmt_detector=0%7C1673722632455; _ym_isad=1; cto_bundle=JBjUJl9IDOVit1oxM1ZYdDU1OWtOVHNHJZHjVHI3cUJaWzJtMtRRUR4SFVPtklDUE53aHpUalpmUDlnM1RYUjYyRXZXVXYwWng4b3BFUEVfOCUYQk15aHdiamNGMGFRSFnFiExtasUYqM0zM0Awc2hXZ3d4TmwafEIMkZych3u2TEVSMHpt3SDNqg; OABLOCK=1262.1673721360_1275.1673721601; OACAP=1262.3_1275.2; OASCAP=1262.3_1275.2; _app_session=ade7cac80ct16e65df3fa8d817134cf7f1; advcake_trackid=f2b88e26-6937-64b7-5611-f2fc92daa956; _OACAP[1262]=1; _OASCAP[1262]=1; _dc_gtm_UA-283414367=1

Второй запрос - HTML. Имеет тот же самый ID, и некоторые атрибуты аналогичные предыдущему рассмотренному запросу, имеет аналогичную привязку к региону.

Inspector | Console | Debugger | **Network** | Style Editor | Performance | Memory | Storage | Accessibility | Application

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	gb.ru	/	document	html	508.62 kB	508.2...
200	GET	gb.ru	bdf.php	script	js	cached	0 B
200	GET	gb.ru	5b76f04.js	script	js	cached	0 B
200	GET	gb.ru	a8dc47a.js	script	js	cached	0 B
200	GET	gb.ru	64b017e.js	script	js	cached	0 B
200	GET	gb.ru	e6203a5.js	script	js	cached	0 B
200	GET	gb.ru	133464b.js	script	js	cached	0 B
200	GET	gb.ru	1b6bb2d.js	script	js	cached	0 B
200	GET	gb.ru	cbe697a.js	script	js	cached	0 B
200	GET	gb.ru	dfof6e5.js	script	js	cached	0 B
200	GET	gb.ru	994d382.js	script	js	cached	0 B
200	GET	gb.ru	7f55811.js	script	js	cached	0 B
200	GET	gb.ru	ec45ea6.js	script	js	cached	0 B
200	GET	gb.ru	b35e0ae.js	script	js	cached	0 B
200	GET	gb.ru	820200a.js	script	js	cached	0 B
200	GET	gb.ru	6ea22bc.js	script	js	cached	0 B
200	GET	gb.ru	407eb61.js	script	js	cached	0 B
200	GET	gb.ru	98b246e.js	script	js	cached	0 B

Headers | Cookies | Request | Response | Timings | Security

Filter Headers

- vary: Accept-Encoding
- X-Firefox-Spdy: h2
- x-frame-options: SAMEORIGIN

Request Headers (2.703 KB)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: qurator_midid=1673720439.096.hX9B4ZLyn4oEAQ6ogeUbtC644jfrJuvncnuBe0eqg5A1; auth.strategy=local; gb_lang_cookie=nr; regionIdv1=RU; lastDefinedRegionIdv1=RUS; sbps_migrations=1418474375998f3D1; sbps_current_add=dfb3d02d31-01-14%2021%3A20%3AAB%7C%7C%CEph3DHdpSp3AAk2P%2Agpuw2F3C7c%7C%7C%3D%2Bnone%29; sbps_currency-uiid=f584d723-f68d-4d5b-9c85-abbd55a11310-7_ym_visorcw; test_detect=0%7C167372370665_ym_isad1; cto_bundie-UdegW916CWpmUwmJJmJSy1tuxHJOWTfwEDNwJTJCQQxpIQOfnctCd2xQMzVtZKVNmnRQOICtJUWmZRUR5WSONKmcWUC84WKSUTikSnmOfrcHzKmUenphOWGZDE3a2iwNTUylentHdxkIRTBzwFDlnZJTCMEISSZKRceDBHVRbnZRA; OABLOCK=1262.1673721601; OACAP=+1262.32752; OASCAP=1262.3_1275-2; advcake_trackid=5733295-d6e3607-ft6bf1da8dgc_app_session-a67cacdb16e65dfba8b1734137f1

Host: gb.ru
SecFetch-Dest: document
SecFetch-Mode: navigate
SecFetch-Site: none
SecFetch-User: 71
TE: trailers
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; x86_64; rv:108.0) Gecko/20100101 Firefox/108.0

```
Cookie: qrtor_msid=1673720439.096.hXfB4ZLyn4OAEg60-ule1b7c644jrf8unvcneub0e6qcg51a; auth.strategy=local; gb_lang_cookie=ru; regionIdV1=RU; lastDefinedRegionIdV1=RU; sbjs_migrations=1418474375998%3D1; sbjs_current_add=fdf%3D2023-01-14%2021%3A20%3A4A8%7C7%7C7Cep%3Dhttps%3A%2F%2F2Fgb.ru%2F%2F%2F%2F%2FCr%3D%28none%29%; sbjs_first_add=fdf%3D2023-01-14%2021%3A20%3A4A8%7C7C7C7Cep%3Dhttps%3A%2F%2F2Fgb.ru%2F%2F%2F%2FCr%3D%28none%29%; sbjs_current=typ%3Dttypein%3D%7C7C7Csrc%3D%28direct%29%7C7C7Ctmdm%3D%28none%29%7C7C7C7Ccpmp%3D%28none%29...dT5=1673720461538; flocktory-uuid=5a8427d3-658d-4d5b-9cc5-a8bd55a1c130-7; _ym_visitor=c; tmr_detect=0%7C1673722307665; _ym_isad=1; cto_bundle=UGBuq196OWPwUWmJlemJx1lxdHJWTFwdDNvJTJCQXJQFOncTcd2xQLIMkzTv2VKNmTRQOLCTHJUWwmZIRUSWS0NKKehkWUG64VwtkUKUtsak5nM0FcZhlQMnUnephOWFQEzDe3a2lWNtYumNtmHdkxiRTrzcWFDblNJTCJMCETSSR2K6EDbhVjrVb2NZRA; OABLOCK=1262.1673721360.1275.6173721601; OACAP=1262.3 1275.2; OASCAP=1262.3 1275.2; advckate Brack=5b732954623607-f607-1bfdb1fdadbae; app session=ade7ca80b1c6e65df3fa8d817134cf7c1
```

В обоих случаях запросы уходят с одним и тем же ID, что говорит к привязке ответа сервера, предназначенного именно для конкретного пользователя.

В противовес двум запросам идёт запрос IMG.

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

gb.ru

Status

Method

Domain

File

Initiator

Type

Transferred

Size B

GET

gb.ru

favicon-16x16.png

img

png

692 B (cached)

692 B

GET

gb.ru

51a944c7203268b68b3d44b165a9f6c.svg

img

svg

184 B (cached)

205 B

200

GET

hit.acstat.com

gibebbrains/r?tsid=9ca0a216-dc49-741c-7910-4831

img

plain

306 B

0 B

GET

gb.ru

/libjs

script

js

19.90 kB (cached)

19.90...

GET

ctm.gb.ru

mtc.js

script

js

100.47 kB (cached)

100.4...

200

GET

gb.ru

bfd5cd.php?bannerid=1262&campaignid=9&zone=

img

gif

667 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=1276&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=81&6&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=1097&6&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=1279&6&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=923&6&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=1039&6&campaignid=8&zone=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

bfd5cd.php?bannerid=0&6&campaignid=0&zoneid=

img

gif

517 B

43 B

200

GET

gb.ru

faviconico

img

icon

23.46 kB (cached)

23.46...

Headers

Cookies

Request

Response

Timings

Security

Filter Headers

pragma: no-cache

server: ORATOR

set-cookie: OAD=d3dc3b7c282599c87c3737ceb1fba; expires=Sun, 14-Jun-2024 18:57:04 GMT; Max-Age=31536000; path=/; secure; SameSite=none

strict-transport-security: max-age=15724800

X-Header-For: h2

x-powered-by: PHP/7.4.27

Request Headers (2.721 KB)

Accept: image/avif,image/webp,*/*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Cookie: qtrator_msid=1673720439.096.JXf842YwIDAEG60-ule1b7c644jgbvunvneub0e9q51a; auth.strategicalc.gb_lang_cookie=regionRV1-RU; lastDefinedZoneid=1-RU; ads_migration=14184737599893D1; ads_curr...defn=14184737599

Запрос идёт с тем же ID, и свойственными для пользователя атрибутами. Ответ в свою очередь идёт общим для посетителей.