

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

По дисциплине «Информационная безопасность»

Лабораторная работа №7
Безопасность браузера и анализ сетевого трафика

Студент:

Дениченко Александр Олегович Р3412

Практик:

Маркина Татьяна Анатольевна

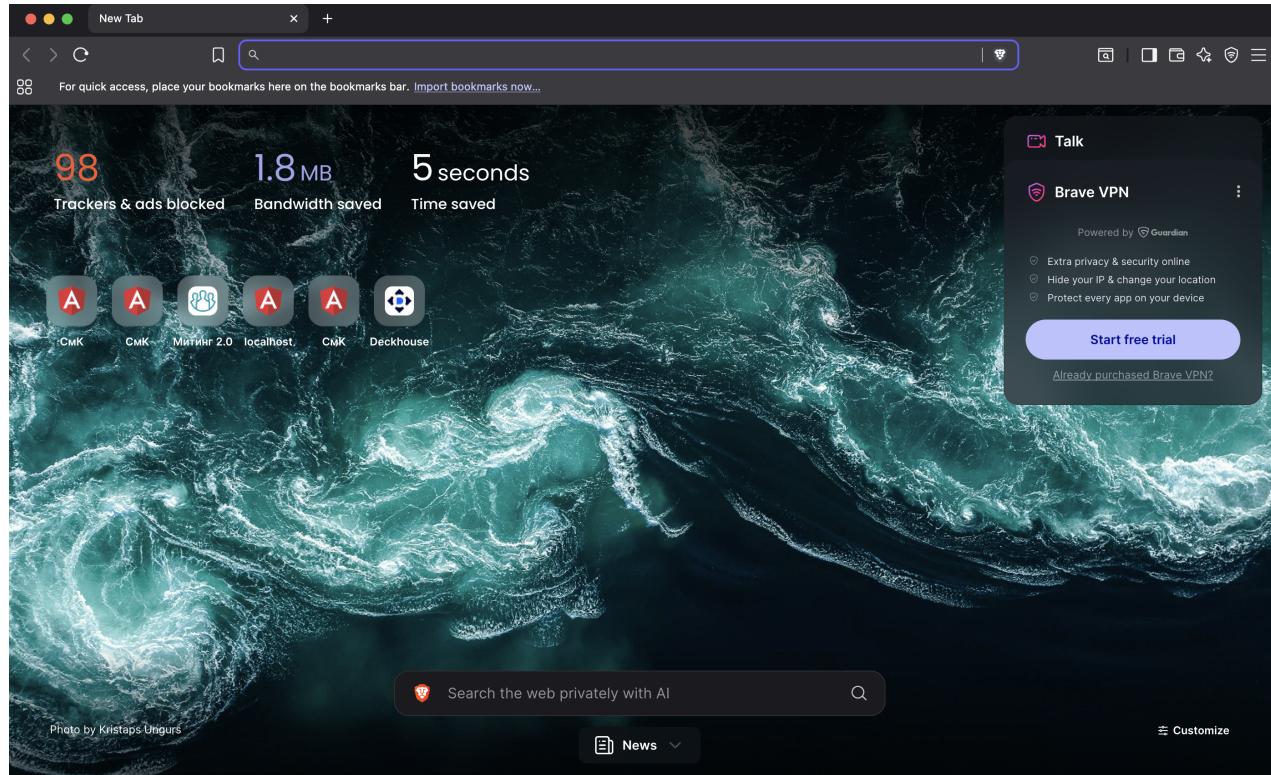
Санкт-Петербург
2025 г.

Цель

Изучить настройки безопасности браузера и понять, какие данные передаются между браузером и сайтом.

1 Настройка браузера

Я буду использовать браузер Brave.



Нашёл в настройках безопасности и конфиденциальности следующие настройки:

Block trackers and ads which follow you across the web.

These are the default Shields settings. They apply to all websites unless you change something in the Shields panel on a particular site. Changing these won't affect your existing per-site settings.

This will block most ads on websites.

Show the number of blocked items on the Shields icon



Trackers & ads blocking

Standard



Upgrade connections to HTTPS

Standard



Block scripts



Block fingerprinting



Block cookies

Block third-party cookies



Forget me when I close this site

Clears cookies and other site data when you close a site.



Store contact information for future broken site reports

If you provide contact info it will be stored for future reports



Content filtering



Enable custom filters that block regional and language-specific trackers and Annoyances.

- Включил более агрессивную блокировку трекеров и рекламы.
- Включил более строгое преобразование подключений в https.
- Включил стирание куков после закрытия сайта (и других данных).

Почистили куки и данные с сайтов.

Delete browsing data

Basic

Advanced

On exit

Time range

All time



- Browsing history**
Deletes history, including in the search box
- Cookies and other site data**
Signs you out of most sites
- Cached images and files**
Frees up 313 MB. Some sites may load more slowly on your next visit.



Your search engine is Yandex. See their instructions for deleting your search history, if applicable.

Clear Brave Ads data...

Cancel

Delete data

Далее выставил настройку, чтобы браузер стирал автоматически все данные при закрытии.

Delete browsing data

Basic

Advanced

On exit

- Browsing history
1 item
- Download history
None
- Cookies and other site data
From 2 sites
- Leo AI
Chat history
- Cached images and files
Less than 1 MB
- Passwords and other sign-in data
None
- Autofill form data
None
- Site and Shields Settings

Cancel

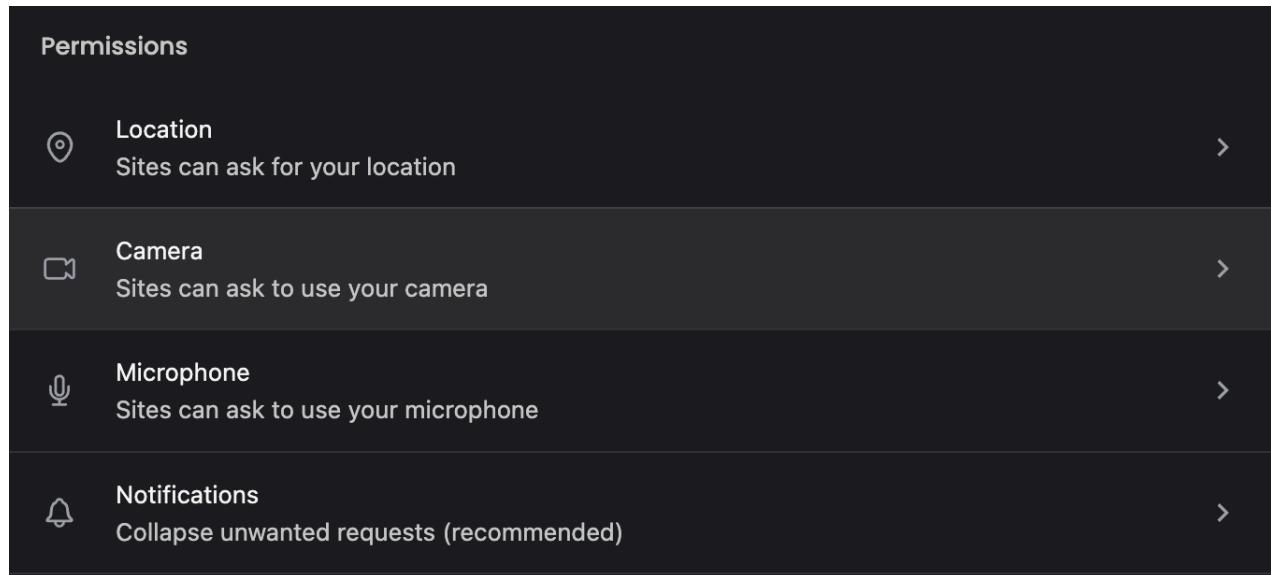
Save

Включил стандартную защиту от сомнительных сайтов (при скачивании файлов, просмотре сайтов) и расширений.

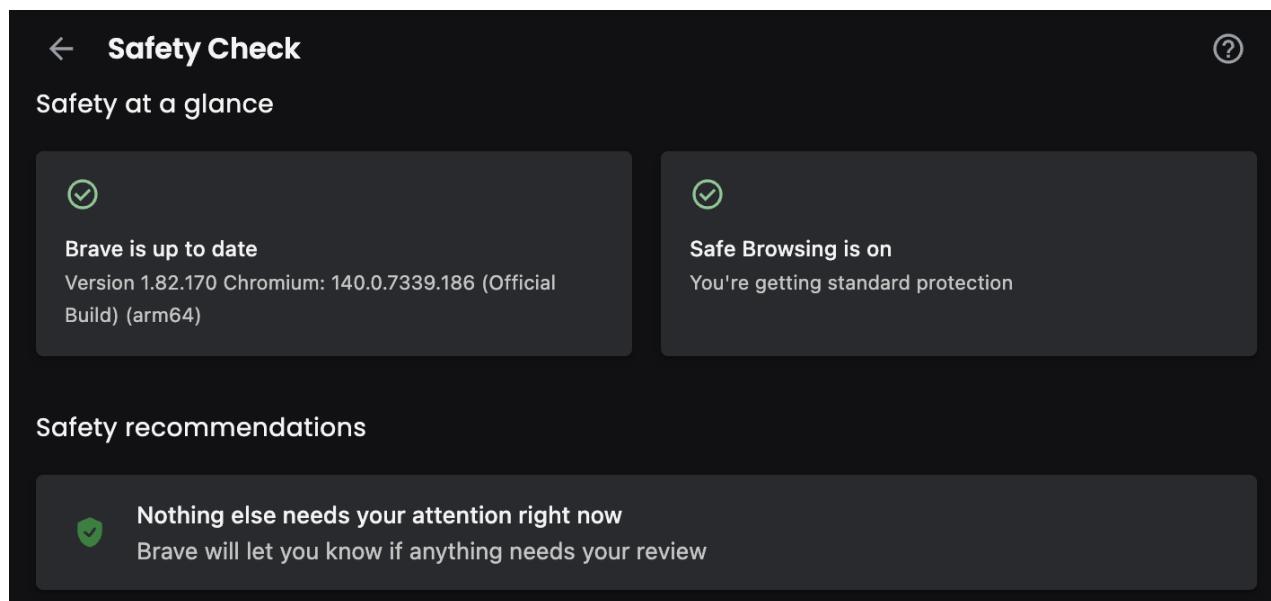
Safe Browsing

- Standard protection
Protects against sites, downloads, and extensions that are known to be dangerous.
- No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions.

Сделал все permission чтобы браузер спрашивал доступ к устройству.

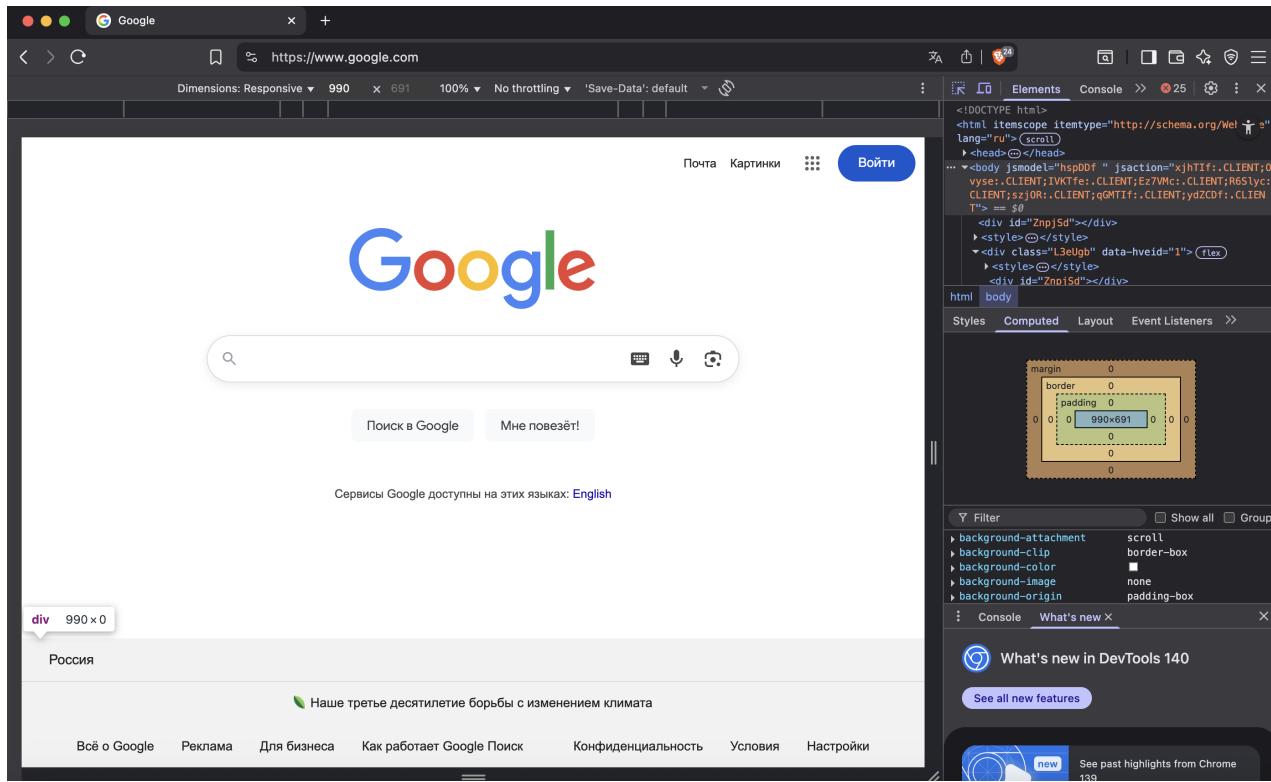


В браузере есть проверка моей защищённости от взлома.

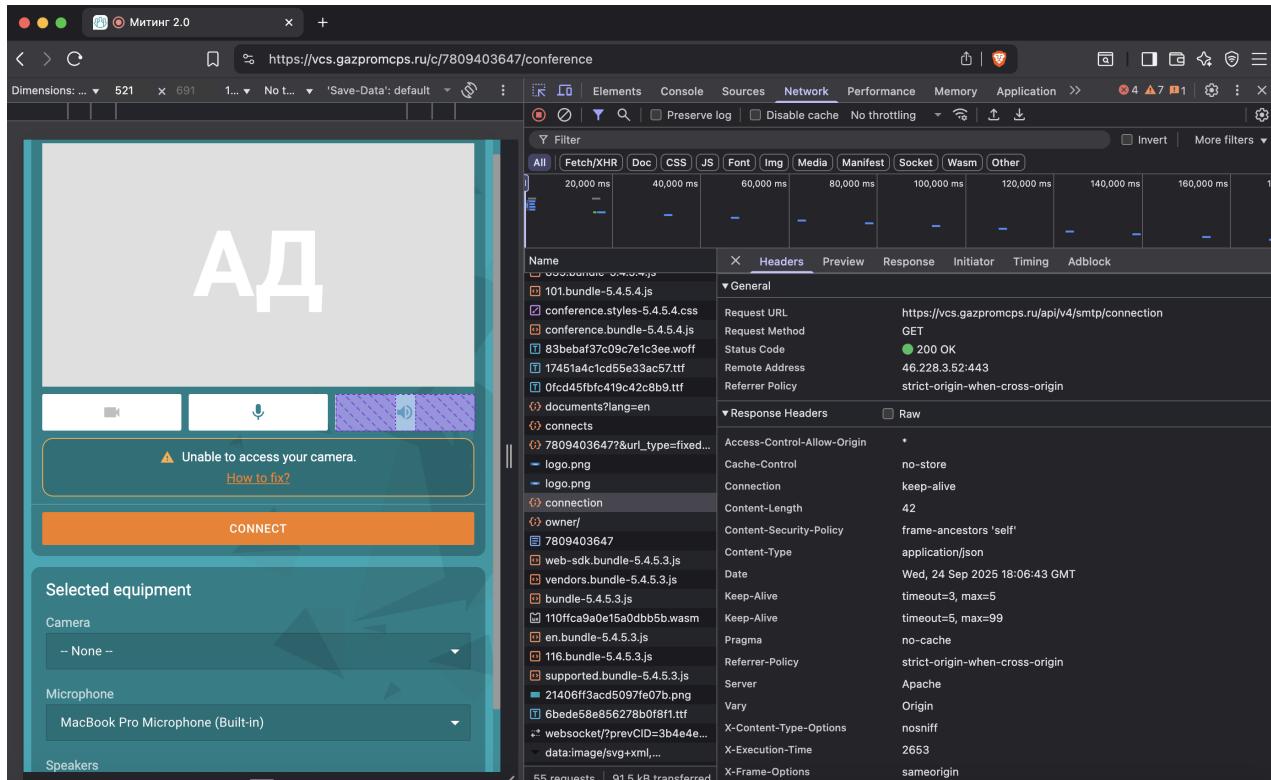


2 Анализ трафика

Открытая консоль разработчика



Перешёл на сайт VSC.



Нашёл один из GET запросов.

conference	Request URL	https://vcs.gazpromcps.ru/c/7809403647/conference
tc-server-utils.bundle-5.4.5.4.js	Request Method	GET
tc-vue-ui-kit.bundle-5.4.5.4.js	Status Code	200 OK
styles-5.4.5.4.css	Remote Address	46.228.3.52:443
vendors.bundle-5.4.5.4.js	Referrer Policy	strict-origin-when-cross-origin
bundle-5.4.5.4.js	▼ Response Headers	
data:image/svg+xml;...	Access-Control-Allow-Origin	*
server?lang=en	Cache-Control	no-store
manifest.webmanifest	Connection	keep-alive
favicon.ico	Content-Encoding	gzip
6bede58e856278b0f8f1.ttf	Content-Length	2107
en.bundle-5.4.5.4.js	Content-Type	text/html; charset=UTF-8
conference-public	Date	Wed, 24 Sep 2025 18:06:43 GMT
7809403647?url_type=fixed...	Keep-Alive	timeout=3, max=5
clients?&lang=en&call_id=780...	Keep-Alive	timeout=5, max=100
839.bundle-5.4.5.4.js	Pragma	no-cache
101.bundle-5.4.5.4.js	Referrer-Policy	strict-origin-when-cross-origin
conference.styles-5.4.5.4.css	Server	Apache
conference.bundle-5.4.5.4.js	Vary	Origin,Accept-Encoding
83bebafe37c09c7e1c3ee.woff	X-Content-Type-Options	nosniff
17451a4c1cd55e33ac57.ttf	X-Execution-Time	16346
0fcda45fbfc419c42c8b9.ttf	X-Request-Id	NJXBJGgpoxlVFDMfhZGkTYJhPyNAxurK
documents?lang=en	X-Tracking-Ref	<0.18996.1141>
connects	X-Twiceconf-Request-X	
7809403647?url_type=fixed...		
logo.png		
58 requests	106 kB transferred	

Запрос был выполнен методом GET, данных в теле запроса не передавалось.

В ответе много стандартных технических заголовков для безопасности (nosniff), идентификации (X-Request-Id, X-Tracking-Ref), сжатия (gzip) и управления кешированием (no-store, no-cache).

Присутствуют параметры CORS (Access-Control-Allow-Origin: *), что разрешает междоменные запросы на этот ресурс.

▼ Request Headers	<input type="checkbox"/> Raw
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding	gzip, deflate, br, zstd
Accept-Language	en-US,en;q=0.9
Cache-Control	max-age=0
Connection	keep-alive
Host	vcs.gazpromcps.ru
Sec-Ch-Ua	"Chromium";v="140", "Not=A?Brand";v="24", "Brave";v="140"
Sec-Ch-Ua-Mobile	?1
Sec-Ch-Ua-Platform	"Android"
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Sec-Fetch-Site	cross-site
Sec-Fetch-User	?1
Sec-Gpc	1
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Mobile Safari/537.36

В данном GET-запросе передаётся стандартный набор заголовков, определяющих:

- Accept: Клиент ожидает различные типы контента, включая HTML, XML, изображения в форматах avif, webp, apng.
- Accept-Encoding: gzip, deflate, br, zstd — поддерживаемые алгоритмы сжатия данных для ответа.
- Accept-Language: en-US, en — основной язык общения клиента с сервером (английский).
- Cache-Control: max-age=0 — запрещает кэширование ответа, требует свежий контент.
- Connection: keep-alive — соединение остаётся открытым для возможных дальнейших запросов.
- Host: vcs.gazpromcps.ru — имя целевого сервера.
- Sec-CH-UA, Sec-CH-UA-Mobile, Sec-CH-UA-Platform: Информация о бренде браузера (Chromium, Brave), мобильности (?1), платформе ("Android").
- Sec-Fetch-Dest, Mode, Site, User: Контекст запроса (document, navigate, cross-site, пользователя).
- Sec-GPC: 1 — indicates user opted for privacy (Global Privacy Control).
- Upgrade-Insecure-Requests: 1 — клиент запрашивает обновление с http на https при возможности.
- User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 ... Chrome/140.0.0.0 Mobile) — подробные сведения о платформе, системе, браузере, его версии

▼ General	
Request URL	https://vcs.gazpromcps.ru/api/v4/endpoints/connects
Request Method	GET
Status Code	● 200 OK
Remote Address	46.228.3.52:443
Referrer Policy	strict-origin-when-cross-origin
▼ Response Headers	
	<input type="checkbox"/> Raw
Access-Control-Allow-Origin	*
Cache-Control	no-store
Connection	keep-alive
Content-Length	53
Content-Security-Policy	frame-ancestors 'self'
Content-Type	application/json
Date	Wed, 24 Sep 2025 18:06:43 GMT
Keep-Alive	timeout=3, max=5
Keep-Alive	timeout=5, max=100
Pragma	no-cache
Referrer-Policy	strict-origin-when-cross-origin
Server	Apache
Vary	Origin
X-Content-Type-Options	nosniff
X-Execution-Time	45212
X-Frame-Options	sameorigin

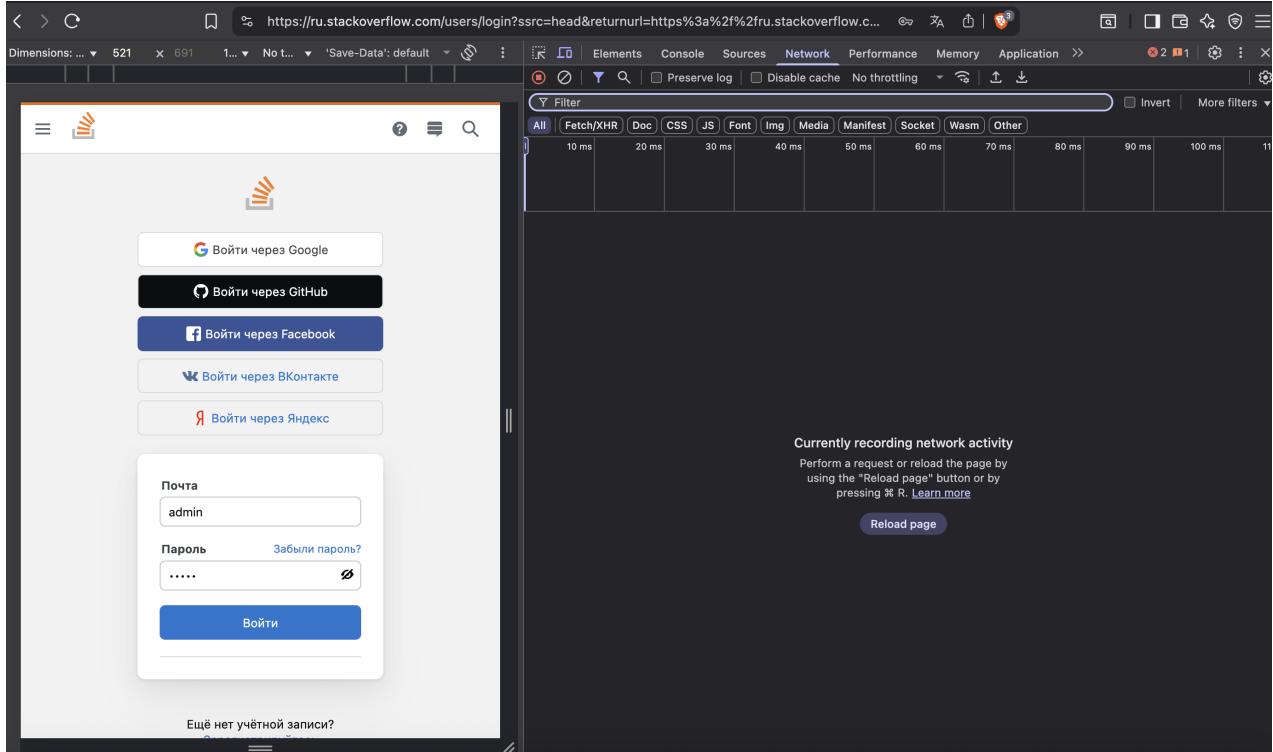
- Access-Control-Allow-Origin: * (разрешён кросс-доменный доступ)
- Cache-Control: no-store (кэширование запрещено)
- Connection: keep-alive (удержание соединения)
- Content-Length: 53 (размер JSON-ответа в байтах)
- Content-Security-Policy: frame-ancestors 'self' (ответ может быть открыт во фрейме только на своём же источнике)
- Content-Type: application/json (ответ в формате JSON)
- Date: Wed, 24 Sep 2025 18:06:43 GMT
- Keep-Alive: timeout=3, max=5; timeout=5, max=100
- Pragma: no-cache (отключение кэширования)
- Referrer-Policy: strict-origin-when-cross-origin
- Server: Apache

- Vary: Origin (зависимость кеширования от варианта Origin)
- X-Content-Type-Options: nosniff (браузеру запрещено определять MIME-тип “на лету”, повышает безопасность)
- X-Execution-Time: 45212 (время обработки на сервере, мс)
- X-Frame-Options: sameorigin (ответ может быть открыт во фрейме только на том же источнике)

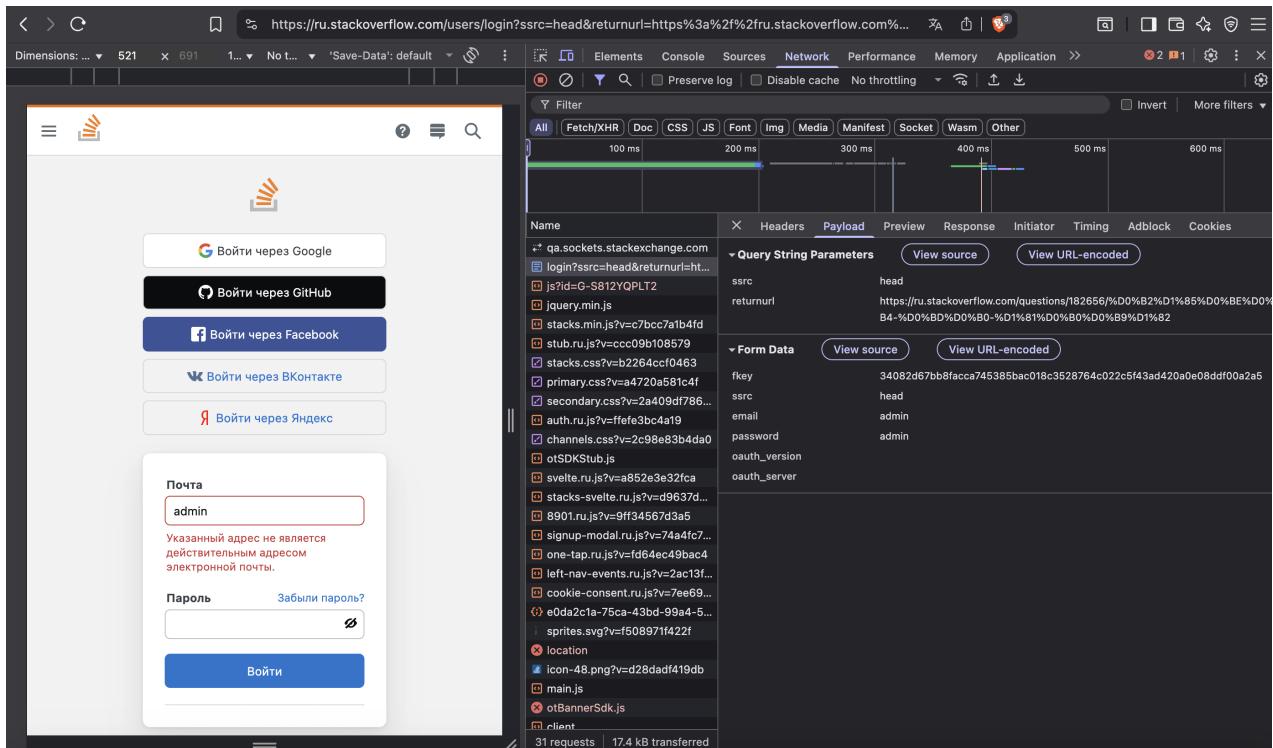
<input checked="" type="checkbox"/> Request Headers	<input type="checkbox"/> Raw
Accept	application/json, text/plain, */*
Accept-Encoding	gzip, deflate, br, zstd
Accept-Language	en-US,en;q=0.9
Connection	keep-alive
Host	vcs.gazpromcps.ru
Referer	https://vcs.gazpromcps.ru/c/7809403647/conference
Sec-Ch-Ua	"Chromium";v="140", "Not=A?Brand";v="24", "Brave";v="140"
Sec-Ch-Ua-Mobile	?1
Sec-Ch-Ua-Platform	"Android"
Sec-Fetch-Dest	empty
Sec-Fetch-Mode	cors
Sec-Fetch-Site	same-origin
Sec-Gpc	1
User-Agent	Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Mobile Safari/537.36

- Accept: application/json, text/plain, */* — ожидаемые форматы ответа
- Accept-Encoding: gzip, deflate, br, zstd — поддерживаемые способы сжатия данных
- Accept-Language: en-US, en;q=0.9 — предпочтительные языки ответа
- Connection: keep-alive — поддержание постоянного соединения
- Host: vcs.gazpromcps.ru — целевой сервер запроса
- Referer: https://vcs.gazpromcps.ru/c/7809403647/conference — адрес отправителя запроса
- Sec-Ch-Ua: "Chromium";v="140" "Not-A?Brand";v="24" "Brave";v="140" — информация о браузере
- Sec-Ch-Ua-Mobile: ?1 — признак мобильного устройства
- Sec-Ch-Ua-Platform: "Android" — платформа устройства
- Sec-Fetch-Dest: empty — цель запроса (API, не страница)
- Sec-Fetch-Mode: cors — использование CORS политики
- Sec-Fetch-Site: same-origin — запрос с того же источника
- Sec-Gpc: 1 — глобальная настройка приватности
- User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Mobile Safari/537.36 — информация о браузере и устройстве

3 Форма входа



Попробуем отправить admin admin



Данные логина и пароля в данном случае передаются в открытом виде (без явного шифрования на клиенте) в теле POST-запроса. За их безопасность отвечает только защищённое HTTPS-соединение между клиентом и сервером. Если бы трафик передавался по HTTP, пароль и логин были бы уязвимы для перехвата. Дополнительного шифрования или маскирования на уровне данных формы не наблюдается.

Результаты

Изучил настройки безопасности браузера и понял, какие данные передаются между браузером и сайтом.