Web Audit Report: OPENAI - CHATGPT October 13th, 2023
Kelvin Lin, Alim Kura, Asya Dente, Lily Jihyun Son CAS CS 357

PRIVACY & POLICY

OpenAI's data policy implies that the collection of user data is meant for the purpose of business operations, complying with legal requirements and enhancing the overall user experience. The information that is collected automatically when a user uses OpenAI's products seems to fit this definition laid out by OpenAI and can be for legitimate purposes [1]. For example, the information provided such as usage data, cookies, and their online analytics products can feasibly be used to enhance the user experience. Other forms of information such as log data and device information can also be used from a diagnostics point of view [2]. On the other hand, the data that is collected when a user provides it and its use, is more suspect. The collection of financial information such as account credentials, payment card information, and its transaction history [3] seem to be largely unnecessary and pose a large risk should this data be leaked. Moreover, OpenAI collects communication information such as the contents of any messages sent, and personal social media information [3] could also prove very dangerous should a malicious party manage to gain access and exploit this information. When distributing data with external third parties, OpenAI does so for legitimate purposes. OpenAI may also disclose personal information to affiliates, which are entities that control, are controlled by, or are under common control with OpenAI. One of such affiliates is the company Intercom. Intercom is an AI customer service solution that utilizes the ChatGPT API in their services [4]. Through the inspection of the ChatGPT AI text generator in use, it is revealed that data is sent to Intercom through the network. OpenAI is GDPR compliant according to OpenAI's security portal. They are also compliant with the CCPA and SOC2 Type 2 [5]. According to OpenAI, they have been evaluated by third-party security auditors, claiming that the OpenAI API undergoes annual third-party penetration testing with the goal of "[identifying] security weaknesses before they can be exploited by malicious actors [6]."

GDPR NOTICE

The company has recently found itself in hot water in a filed complaint with the Polish data protection authority. The complaint was filed by a privacy researcher on 29 August, 2023 alleging that OpenAI has violated the General Protection Regulation (GDPR); They allege that the policy was violated on the basis of transparency, fairness, data access rights, and privacy. The file claims that they are infringing on the EU privacy rules. OpenAI has also been accused in the past by the Italian data protection authority, the Garante, violating the GDPR, citing that OpenAI has unlawfully processed people's data, and that OpenAI lacked any system in place to prevent minors from its products [7]. Overall, OpenAI's privacy policy is much in line with its industry peers. There are incidents as cited above, but nothing that has been overly egregious as to cause vast damage. Most information is collected for legitimate business and operation reasons, but some information is largely unnecessary and can be dangerous if exposed.

COOKIES

ChatGPT is the most commonly used feature of OpenAI thus one of the most interesting in terms of its security. By inspecting the website, we discovered ChatGPT uses multiple cookies (around 16) enhancing user experience and security. All the cookies come from the following domains: .openai.com ; .chat.openai.com ; .tcr9i.chat.openai.com [8]. Their purpose varies a lot, the cookies are used for login, secure authentication, anonymity, defense against popular attacks (such as CSRF), user-friendliness of the platform, and they make it easy for users to navigate through the website. Some cookies have as a main objective to ensure a fast response mechanism and make sure it's easy for the user to log on and avoid having trouble with the security from Cloudflare (a security preventing attacks from bots and controlling web traffic). The cookies storing personal information of the user could present security risks where an attacker could impersonate the user, entailing possible data leakage. The ones making sure your personal information remains anonymous (using random identifiers) are still vulnerable to cookie theft as well as session hijacking attacks. And the ones not containing any personally identifiable information do not create high security risks if implemented correctly. Additionally, most cookies were secure, but not all of them. The ones involving authentication as well as protection from malicious bots' attacks and CSRF attacks were secure, however some of the ones containing our personal identification as well as our random identifier or improving our user experience were not secure. In the same way, the HTTP Only cookies were the same ones to be secure cookies. This means a XSS attack could still have security implications, although not at high risk as the most important cookies are protected against such attacks (HTTP Only prevents such attacks). We found most cookies to be persistent, with the exception of the main authentication ones which are session cookies. Although there isn't much information about all of the cookies, one of the cookies could represent a tracking cookie which is neither secure or HTTP Only, but is persistent. This could increase the risk of an attack directed to this cookie (it is not too much of a malicious attack) and result in the attacker following your behavior across the website and potentially finding valuable information. In general, the most you would be able to learn from the user is potentially their username and password (but rather secure), as well as their online activity on that platform (still not completely defenseless).[8]

CSRF DEFENSE

Rate limiting is a defense on the ChatGPT API and for OpenAI. This is a defense that limits the amount of attempts a party can make in a given time. By restricting the number of times an attacker can make requests, it makes carrying out large-scale CSRF attacks more difficult. User authentication is also an important part of protection against CSRF attacks. ChatGPT and OpenAI both utilize this by requiring the user to login and provide credentials before allowing the user access to its services. This ensures that only those that are authorized are able to access and interact with the site. In the research conducted, we were unable to access the implementation details of ChatGPT and its use of Javascript libraries. However, since the application is still very much in its infancy, and that it is regularly updated (ChatGPT 4 released in March, 2023)[10], it is more probable than not, that ChatGPT is not utilizing outdated Javascript libraries, especially since this is a very known avenue of cyber attacks.

URLS

ChatGPT makes multiple calls to different URLs. Some URLs are fetched many times through different methods (namely GET, POST and OPTIONS), the following URL is offsite, and ChatGPT fetches it a few times : events.statsigapi.net. Most of the other fetched URLs are all onsite and come from the domain chat.openai.com, except for one other URL which appears to be fetched through featuregates.org and one which was a ping file from api-iam.intercom.io[12]. This last one has a "strict-origin-when-cross-origin" policy which makes it more secure since it contains valuable information about the user's ip address, and location. Clicking on them brought us to different error codes which showed a minimum security [11]. All the URLs ChatGPT fetches are also protected with HTTPS. The URLs fetched on-site might represent security risks as they do contain sensitive information such as the tokens' values as well as information about the current running session[13]. However, they seem to be rather well protected against attacks as they're all under the "same-origin" policy, and the others are under "cross-site" but still using CORS fetch method[12][13].

MIXED CONTENT

We found no tracking pixels used on ChatGPT[9], as well as no discussion of them in the privacy policy. Facebook Pixel was not found anywhere on the website which usually is a rather popular thing to see. Moreover, there were no ad trackers to be found and no third-party cookies, which are all good privacy measures to take. In terms of the website's accessibility, we were not able to access the website via HTTP. It would simply reload to HTTPS on all browsers. The website is protected by Cloudflare Delivery Network and verified by them with a certificate [14]. The user's communication to the website is being encrypted and attackers are less likely to tamper with it. Thus, also reducing insecure redirects in cases where a user might forget to specify HTTPS. Openai is making use of HSTS [15] which ensures the website only uses HTTPS [16]. If a user includes only HTTP, HSTS will redirect the user to the correct page. However, there are still security risks as the initial request remains unprotected from active attacks when using plain HTTP.

ADVERTISEMENTS & PLUGINS

Ads on ChatGPT are nonexistent through our research and the experiences of other users [17]. Although ChatGPT does not have ads on its own site, it cannot enforce an ad free policy for the businesses that they license the ChatGPT application to. ChatGPT is gradually rolling out plugins in order to "study their real-world use, impact, and safety and alignment challenges." ChatGPT hosts two plugins as well; a web browser and a code interpreter. Although plugins can be extremely useful for providing new opportunities, it also poses a significant risk to security. Plugins can take unintended and harmful actions which can increase the damage capabilities of any would-be adversaries. However, according to OpenAI, plugins have been made with this risk in mind. By collaborating with internal and external parties, they thoroughly test a plugin before it is readily available to the general public [18].

SIGN-UP AND LOGIN FLOWS

OpenAI.com facilitates user authentication through a variety of methods. Users can either create an account directly on the platform or opt to sign up and log in via third-party accounts such as Google, Microsoft, or Apple [19]. In the case of third-party authentication, a two-step verification is initiated where a confirmation notification is sent to another device sharing the same account, enhancing the security of the authentication process. Alternatively, for direct account creation on OpenAI.com, users are prompted to provide a valid email and to create a password, the only stipulation being a minimum length of 8 characters [20]. This particular password policy could be perceived as a potential security flaw since it may not provide a robust defense against common cyber threats like brute force attacks, especially in the absence of additional complexity requirements such as the inclusion of uppercase and lowercase letters, numbers, and symbols [2]. The password entry during sign-up and login is managed by the <input type="password"> HTML element which conceals each character typed with a dot symbol [21], although a 'show password' toggle button is present to reveal the password for user convenience. Following this, a one-time confirmation email is sent to the user's inbox containing a 'Verify your email' button, which upon being clicked, completes the account verification process enabling users to log in. After the user is authenticated by either of these methods, they are asked to input their first name, last name, birthday, and phone number, with a one-time SMS code being sent for verification, paving the way for account creation. In scenarios of forgotten passwords of directly created accounts, the platform provides a 'Forgot Password' link [22] enabling users to initiate a password reset, which sends a reset link to the registered email address to facilitate password recovery [23]. If the email address is not registered to OpenAI, you will still be able to see the page where you are notified of the password recovery email. However, the email will not be sent. The absence of mandatory multi-factor authentication (MFA) for directly created accounts elevates security concerns, as MFA significantly bolsters account security by requiring multiple forms of identity verification. Furthermore, post account creation, the login process only necessitates the user's email and password, which could potentially be a security concern if a user's password is compromised. These points underscore the potential upgrade to a more comprehensive password policy and multi-factor authentication to enhance account security and mitigate potential cyber threats.

GENERAL CONCLUSION

The OpenAI website balances user and visitor privacy and security with a multifaceted approach. On one hand, it collects a wide range of data for legitimate purposes. However, data collected directly from users, such as financial information and personal communication data [3], raises concerns due to potential privacy and security risks if exposed. The information found on the privacy and policy page [1] is rather limited to users as they don’t have access to much of it which may raise a red flag as one may question why he has such limited access (for instance, the description of their use of cookies is really brief and superficial). The site also shares data with external third parties for legal purposes. While OpenAI claims to comply with GDPR [5], allegations of GDPR violations have been raised [6], casting doubt on the extent of OpenAI’s commitment to data privacy. Furthermore, the site’s password policy lacks complexity requirements [20] and MFA is not mandatory when logging in, presenting potential security risks if a user’s password is compromised. Therefore, OpenAI demonstrates a mixed approach to user and visitor privacy and security. While some security measures are in place, there's room for enhancement, particularly in terms of user account security. The site prioritizes user privacy through the absence of ads [17] but should work towards ensuring comprehensive privacy and security. Finally, another small aspect of the site that seemed questionable was when we looked at the bug crowd site, many parts of OpenAI were categorized as “off-scope” [24] meaning we’re not able to look more closely at their security. This could mean their security is not well implemented in these areas yet, which could lead to potential attacks being carried out, or they’re protecting very sensitive data in which case, it could still implicate rather big security risks. Overall, OpenAI and ChatGPT should be more open about their security measures and not forget to increase their password complexity to ensure user’s security.

LINK TO POSTER:

https://docs.google.com/presentation/d/1rvUtlILOxzFMN72rtvvkqjvgzqomhKE5hRwc8l0QS1k/edit?usp=sharing

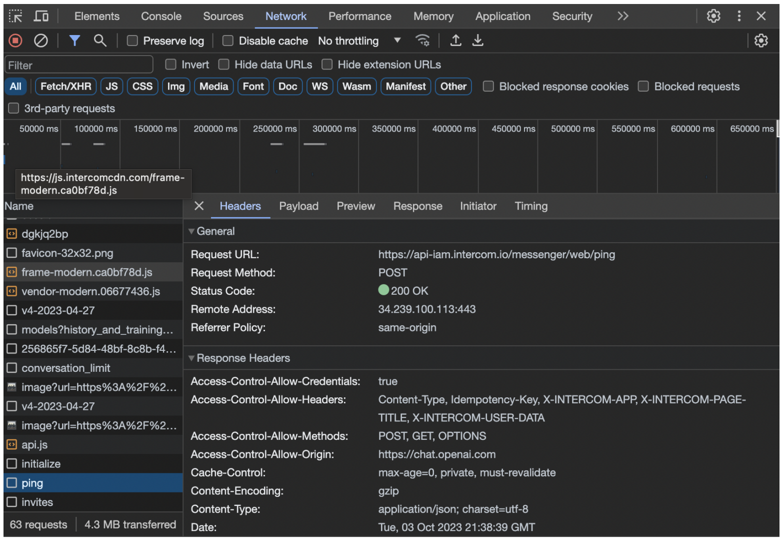
APPENDIX

[1] https://openai.com/policies/privacy-policy

[2] https://tech.co/news/does-chatgpt-save-my-data

[3] https://www.makeuseof.com/chatgpt-privacy-issues/

[4]



https://js.intercomcdn.com/frame-modern.ca0bf78d.js

```
Name
dgkjq2bp
favicon-32x32.png
frame-modern.ca0bf78d.js
vendor-modern.06677436.js
v4-2023-04-27
models?history_and_training…
256865f7-5d84-48bf-8c8b-f4…
conversation_limit
image?url=https%3A%2F%2…
v4-2023-04-27
image?url=https%3A%2F%2…
api.js
initialize
ping
invites
63 requests | 4.3 MB transferred
```

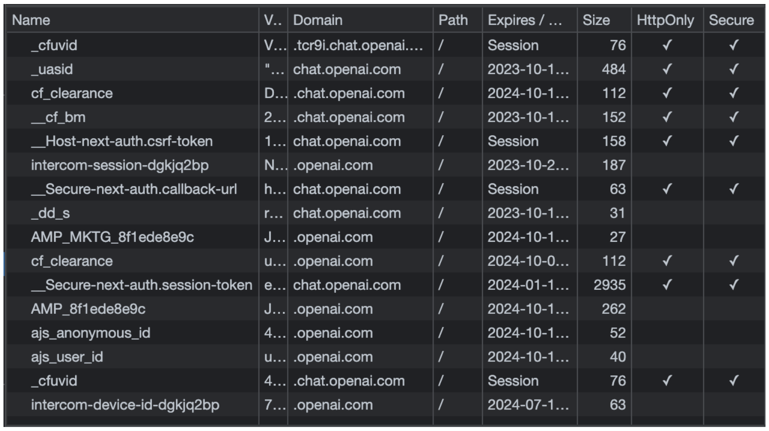
```
▼ General
Request URL:                        https://api-iam.intercom.io/messenger/web/ping
Request Method:                     POST
Status Code:                        ● 200 OK
Remote Address:                     34.239.100.113:443
Referrer Policy:                    same-origin

▼ Response Headers
Access-Control-Allow-Credentials:   true
Access-Control-Allow-Headers:       Content-Type, Idempotency-Key, X-INTERCOM-APP, X-INTERCOM-PAGE-
                                    TITLE, X-INTERCOM-USER-DATA
Access-Control-Allow-Methods:       POST, GET, OPTIONS
Access-Control-Allow-Origin:        https://chat.openai.com
Cache-Control:                      max-age=0, private, must-revalidate
Content-Encoding:                   gzip
Content-Type:                       application/json; charset=utf-8
Date:                               Tue, 03 Oct 2023 21:38:39 GMT
```

[5]https://trust.openai.com/?itemUid=45220873-6e51-4dbb-b1b1-37d66ee9ef95&source=click

[6] https://openai.com/security

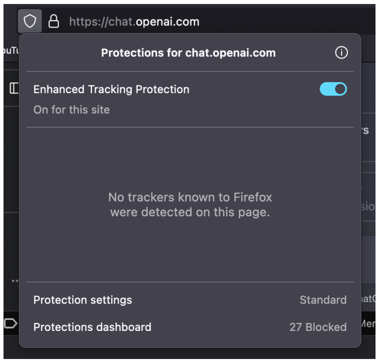
[7]https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher/

[8]



Name	V..	Domain	Path	Expires / ...	Size	HttpOnly	Secure
_cfuvid	V...	.tcr9i.chat.openai....	/	Session	76	✓	✓
_uasid	"...	chat.openai.com	/	2023-10-1...	484	✓	✓
cf_clearance	D...	.chat.openai.com	/	2024-10-1...	112	✓	✓
__cf_bm	2...	.chat.openai.com	/	2023-10-1...	152	✓	✓
__Host-next-auth.csrf-token	1...	chat.openai.com	/	Session	158	✓	✓
intercom-session-dgkjq2bp	N...	.openai.com	/	2023-10-2...	187		
__Secure-next-auth.callback-url	h...	chat.openai.com	/	Session	63	✓	✓
_dd_s	r...	chat.openai.com	/	2023-10-1...	31		
AMP_MKTG_8f1ede8e9c	J...	.openai.com	/	2024-10-1...	27		
cf_clearance	u...	.openai.com	/	2024-10-0...	112	✓	✓
__Secure-next-auth.session-token	e...	chat.openai.com	/	2024-01-1...	2935	✓	✓
AMP_8f1ede8e9c	J...	.openai.com	/	2024-10-1...	262		
ajs_anonymous_id	4...	.openai.com	/	2024-10-1...	52		
ajs_user_id	u...	.openai.com	/	2024-10-1...	40		
_cfuvid	4...	.chat.openai.com	/	Session	76	✓	✓
intercom-device-id-dgkjq2bp	7...	.openai.com	/	2024-07-1...	63		

[9]



https://chat.openai.com

Protections for chat.openai.com

Enhanced Tracking Protection

On for this site

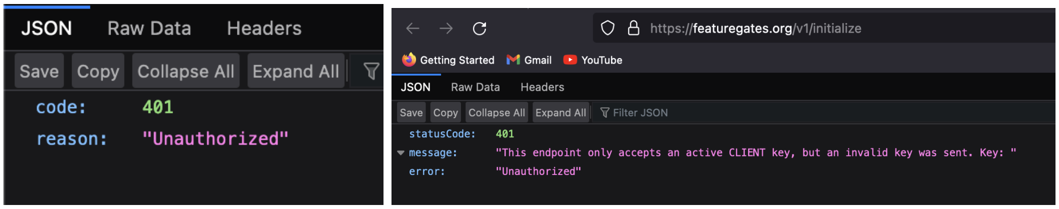
No trackers known to Firefox were detected on this page.

Protection settings Standard

Protections dashboard 27 Blocked

[10] https://help.openai.com/en/articles/6825453-chatgpt-release-notes

[11]

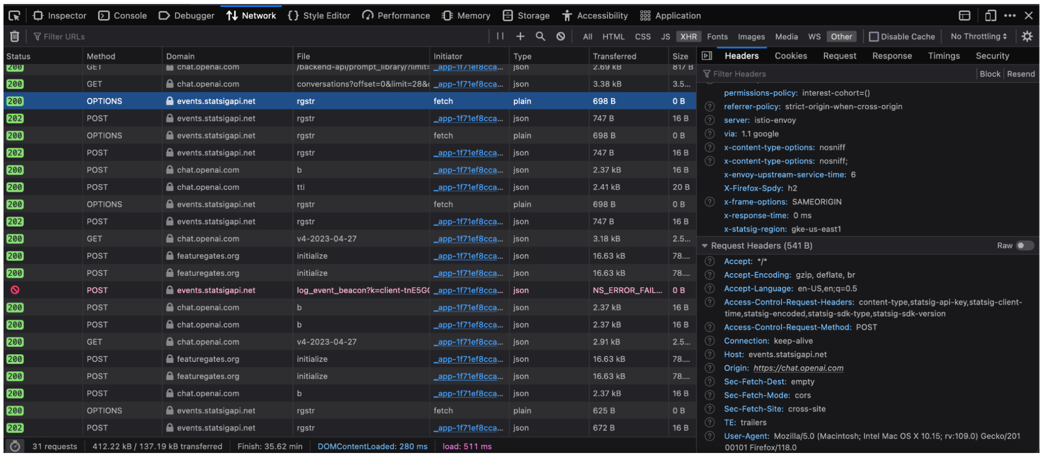


```
code:      401
reason:    "Unauthorized"
```

https://featuregates.org/v1/initialize

```
statusCode:   401
message:      "This endpoint only accepts an active CLIENT key, but an invalid key was sent. Key: "
error:        "Unauthorized"
```

[12]

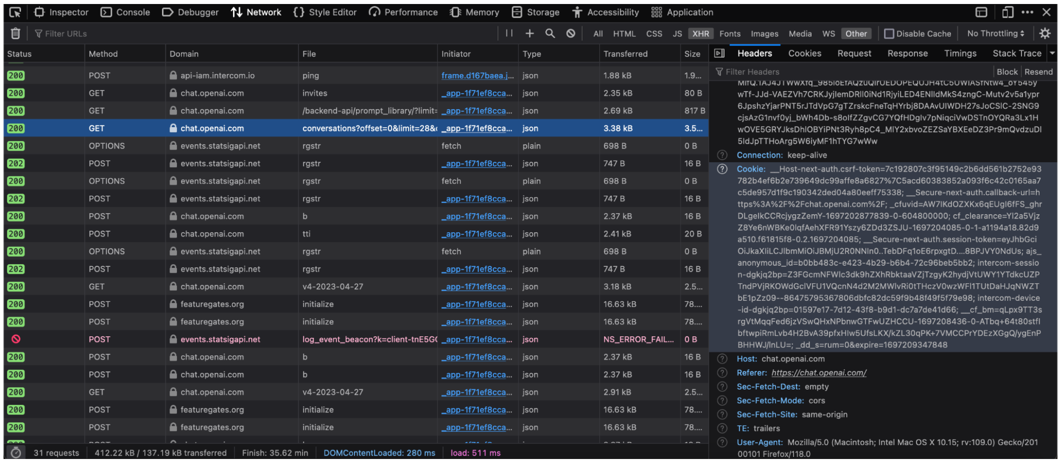


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	chat.openai.com	/backend-api/prompt_library/?limit=	_app-1f71ef8cca...	json	2.69 kB	817 B
200	GET	chat.openai.com	conversations?offset=0&limit=28&	_app-1f71ef8cca...	json	3.38 kB	3.5...
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	POST	chat.openai.com	tti	_app-1f71ef8cca...	json	2.41 kB	20 B
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	GET	chat.openai.com	v4-2023-04-27	_app-1f71ef8cca...	json	3.18 kB	2.5...
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
⊘	POST	events.statsigapi.net	log_event_beacon?k=client-tnE5G(	_app-1f71ef8cca...	json	NS_ERROR_FAIL...	0 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	GET	chat.openai.com	v4-2023-04-27	_app-1f71ef8cca...	json	2.91 kB	2.5...
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	625 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	672 B	16 B

31 requests | 412.22 kB / 137.19 kB transferred | Finish: 35.62 min | DOMContentLoaded: 280 ms | load: 511 ms

```
permissions-policy: interest-cohort=()
referrer-policy: strict-origin-when-cross-origin
server: istio-envoy
via: 1.1 google
x-content-type-options: nosniff
x-content-type-options: nosniff;
x-envoy-upstream-service-time: 6
X-Firefox-Spdy: h2
x-frame-options: SAMEORIGIN
x-response-time: 0 ms
x-statsig-region: gke-us-east1
Request Headers (541 B)
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Access-Control-Request-Headers: content-type,statsig-api-key,statsig-client-time,statsig-encoded,statsig-sdk-type,statsig-sdk-version
Access-Control-Request-Method: POST
Connection: keep-alive
Host: events.statsigapi.net
Origin: https://chat.openai.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
TE: trailers
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
```

[13]

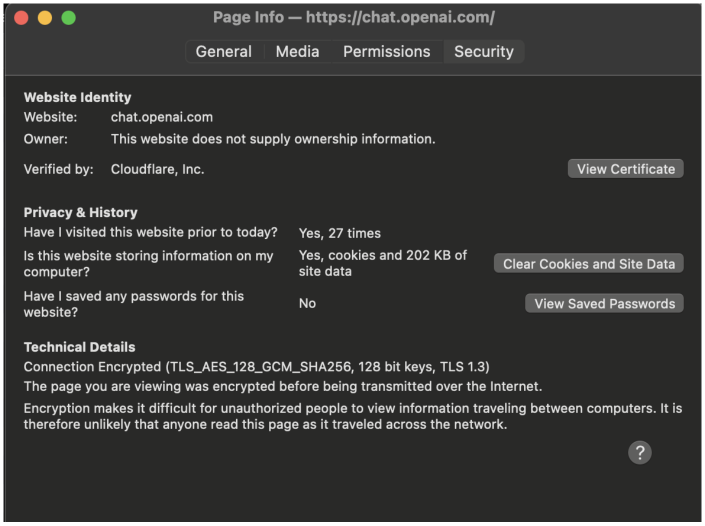


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	api-iam.intercom.io	ping	frame.d167baea.j...	json	1.88 kB	1.9...
200	GET	chat.openai.com	invites	_app-1f71ef8cca...	json	2.35 kB	80 B
200	GET	chat.openai.com	/backend-api/prompt_library/?limit=	_app-1f71ef8cca...	json	2.69 kB	817 B
200	GET	chat.openai.com	conversations?offset=0&limit=28&	_app-1f71ef8cca...	json	3.38 kB	3.5...
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	POST	chat.openai.com	tti	_app-1f71ef8cca...	json	2.41 kB	20 B
200	OPTIONS	events.statsigapi.net	rgstr	fetch	plain	698 B	0 B
202	POST	events.statsigapi.net	rgstr	_app-1f71ef8cca...	json	747 B	16 B
200	GET	chat.openai.com	v4-2023-04-27	_app-1f71ef8cca...	json	3.18 kB	2.5...
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
⊘	POST	events.statsigapi.net	log_event_beacon?k=client-tnE5G(	_app-1f71ef8cca...	json	NS_ERROR_FAIL...	0 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	POST	chat.openai.com	b	_app-1f71ef8cca...	json	2.37 kB	16 B
200	GET	chat.openai.com	v4-2023-04-27	_app-1f71ef8cca...	json	2.91 kB	2.5...
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....
200	POST	featuregates.org	initialize	_app-1f71ef8cca...	json	16.63 kB	78....

31 requests | 412.22 kB / 137.19 kB transferred | Finish: 35.62 min | DOMContentLoaded: 280 ms | load: 511 ms

```
wTf-JJd-VAEZVh7CRKJyjlemDRll0iNd1RjyiLED4ENlldMkS4zngC-Mutv2v5a1ypr
6JpshzYjarPNT5rJTdVpG7gTZrskcFneTqHYrbj8DAAvUIWDH27sJoCSlC-2SNG9
cjsAzG1nvf0yj_bWh4Db-s8olfZZgvCG7YQfHDglv7pNiqciVwDSTnOYQRa3Lx1H
wOVE5GRYJksDhlOBYiPNt3Ryh8pC4_MlY2xbvoZEZSaYBXEeDZ3Pr9mQvdzuDl
5ldJpTTHoArg5W6iyMF1hTYG7wWw
Connection: keep-alive
Cookie: __Host-next-auth.csrf-token=7c192807c3f95149c2b6dd561b2752e93782b4ef6b2e739649dc99affe8a6827%7C5acd60383852a093f6c42c0165aa7c5de957d1f9c190342ded04a80eeff75338; __Secure-next-auth.callback-url=https%3A%2F%2Fchat.openai.com%2F; _cfuvid=AW7IKdOZXKx6qEUgl6fFS_ghrDLgelkCCRcjygzZemY-1697202877839-0-604800000; cf_clearance=Yl2a5VjzZ8Ye6nWBKe0lqfAehXFR91Yszy6ZDd3ZSJU-1697204085-0-1-a1194a18.82d9a510.f61815f8-0.2.1697204085; __Secure-next-auth.session-token=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIn0..TebDFq1oE6rpxgtD....8BPJVY0NdUs; ajs_anonymous_id=b0bb483c-e423-4b29-b6b4-72c96beb5bb2; intercom-session-dgkjq2bp=Z3FGcmNFWlc3dk9hZXhRbktaaVZjTzgyK2hydjVtUWY1YTdkcUZPTndPVjRKOWdGclVFU1VQcnN4d2M2MWlvRi0tTHczV0wzWFl1TUtDaHJqNWZTbE1pZz09--86475795367806dbfc82dc59f9b48f49f5f79e98; intercom-device-id-dgkjq2bp=01597e17-7d12-43f8-b9d1-dc7a7de41d66; __cf_bm=qLpx9TT3srgVtMqqFed6jzVSwQHxNPbnwGTFwUZHCCU-1697208436-0-ATbq+64t80stflbftwpiRmLvb4H2BvA39pfxHlw5UfsLKX/kZL30qPK+7VMCCPrYDEzXGgQ/ygEnPBHHWJ/lnLU=; _dd_s=rum=0&expire=1697209347848
Host: chat.openai.com
Referer: https://chat.openai.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
TE: trailers
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
```

[14] https://blog.cloudflare.com/announcing-ai-gateway/



Page Info — https://chat.openai.com/

Website Identity

Website: chat.openai.com

Owner: This website does not supply ownership information.

Verified by: Cloudflare, Inc.

Privacy & History

Have I visited this website prior to today? Yes, 27 times

Is this website storing information on my computer? Yes, cookies and 202 KB of site data

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

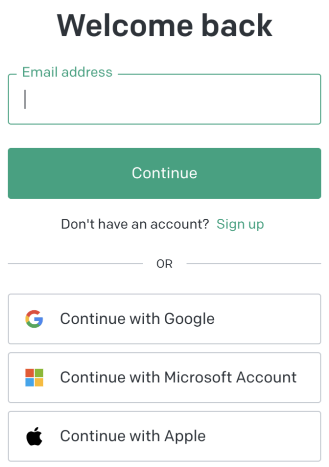
[15] https://www.upguard.com/security-report/openai

[16]https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

[17] https://community.openai.com/t/are-ads-allowed-in-plugins/273197

[18] https://openai.com/blog/chatgpt-plugins

[19]

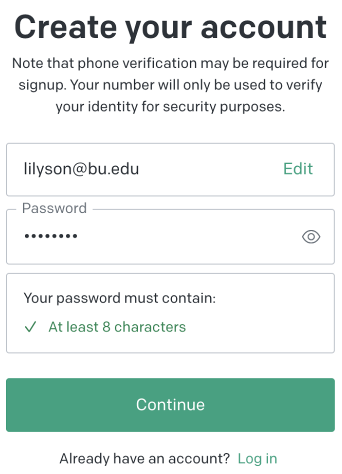


Welcome back

Email address

Don't have an account? Sign up

[20]



Create your account

Note that phone verification may be required for signup. Your number will only be used to verify your identity for security purposes.

lilyson@bu.edu

Password

••••••••

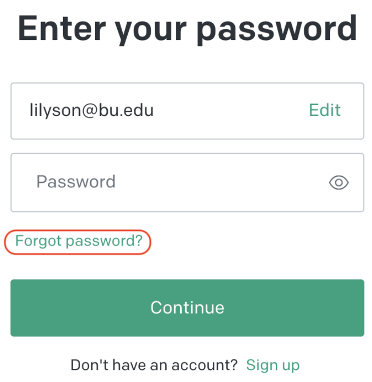
Your password must contain:

✓ At least 8 characters

Already have an account? Log in

[21] https://developer.mozilla.org/en-US/docs/Web/HTML/Element/input/password.

[22]



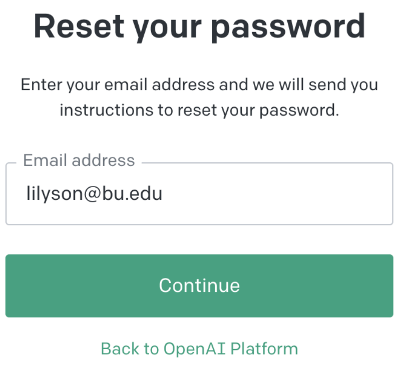
Enter your password

lilyson@bu.edu

Password

Don't have an account? Sign up

[23]



Reset your password

Enter your email address and we will send you instructions to reset your password.

Email address

lilyson@bu.edu

[24] https://bugcrowd.com/openai