WEB AUDITING OPENAI

KELVIN LIN, ALIM KURA, ASYA DENTE, LILY JIHYUN SON

SECURITY

COOKIES

- 16 cookies: authentication, personal information, user experience, CSRF ...
- Low security risks for authentication
- Both persistent and session cookies, possibly risky
- Some cookies are not HTTP Only and not secure, could contain personal information and thus a security risk

Name	V..	Domain	Path	Expires / ...	Size	HttpOnly	Secure
__cf_bm	I...	.chat.openai.com	/	2023-10-1...	152	✓	✓
AMP_8f1ede8e9c	J...	.openai.com	/	2024-10-1...	262		
ajs_anonymous_id	4...	.openai.com	/	2024-10-1...	52		
__Secure-next-auth.session-token	e...	chat.openai.com	/	2024-01-0...	2935	✓	✓
cf_clearance	L...	.chat.openai.com	/	2024-10-0...	112	✓	✓
__Host-next-auth.csrf-token	1...	chat.openai.com	/	Session	158	✓	✓
intercom-session-dgkjq2bp	M...	.openai.com	/	2023-10-1...	187		
__Secure-next-auth.callback-url	h...	chat.openai.com	/	Session	63	✓	✓
_dd_s		chat.openai.com	/	2023-10-1...	5		
AMP_MKTG_8f1ede8e9c	J...	.openai.com	/	2024-10-1...	27		
cf_clearance	u...	.openai.com	/	2024-10-0...	112	✓	✓
_cfuvid	9...	.chat.openai.com	/	Session	76	✓	✓
ajs_user_id	u...	.openai.com	/	2024-10-1...	40		
intercom-device-id-dgkjq2bp	7...	.openai.com	/	2024-07-0...	63		

- Website not accessible through HTTP, use of HSTS
- No tracking pixels, no Facebook Pixel
- No ad trackers as well as no ads (although can't enforce for third parties)
- Two-step verification (only for third-party authentication)

THE GENERAL PROTECTION REGULATION (GDPR)

- OpenAI is GDPR compliant according to its security portal
- However, there have been suits filed against OpenAI and ChatGPT
- One by a security researcher and another by The Garante

PRIVACY POLICY

- Collects user data for business operations, legal compliance, and improving the user experience, including usage data and cookies.
- Shares data with third parties for legitimate reasons
- Vendors receive data via the network for their services.

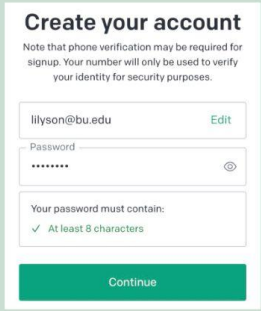
OpenAI

Plugins

- ChatGPT is gradually rolling out plugins in order to "study their real-world use, impact, and safety and alignment challenges."
- Can take unintended actions which can increase capabilities of any adversaries.
- Designed with this in mind

POTENTIAL VULNERABILITIES/EXPLOITS

Direct Account Creation:
The password policy pictured in the image above may pose a security risk because it lacks strong defenses against common cyber threats like brute force attacks. It does not require additional complexity elements like uppercase and lowercase letters, numbers, and symbols.



Absence of MFA when logging in:
Since MFA (multi-factor authentication) significantly bolsters account security by requiring multiple forms of identity verification, the absence of MFA elevates the security concerns

CSRF DEFENSES

- Rate Limiting, User Authentication, CORS Policies

JAVASCRIPT LIBRARIES

- Unable to access the implementation details but it is not likely that they are using outdated libraries