



AICamp Experience Test Report

Date: 21st August 2024

URL: <https://aicamp.so/>

Title: Personal ChatGPT For Your Team | AICamp

Testers: [Rahul Parwal](#) & [Rishikesh Vajre](#)

Mission

Identify potential usability issues, security flaws, and functional bugs within the AICamp website. Evaluate the platform's adherence to its claims of privacy, security, and collaboration features, ensuring a seamless user experience and robust security measures.

Coverage

Exploratory Testing: Conducted a normal routine exploration of the AICamp website using Microsoft Edge browser. Focused on user account creation, navigation, UI/UX design, security protocols, and overall functionality.

Obstacles

Encountered difficulties in testing due to inconsistent user interface elements and lack of clear instructions for certain features, which could impact user retention and the platform's overall usability.

Audience

Aimed at stakeholders including AlCamp's development and security teams, as well as potential enterprise customers concerned with the platform's security and user experience.

Techniques

Utilized exploratory testing techniques with a focus on real-world user interactions. Investigated security protocols, UI/UX design, and functionality, with an emphasis on identifying issues that could affect user trust and platform adoption.

Environment

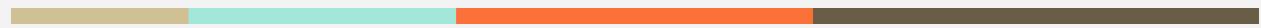
Testing was conducted in the following environment:

Edition	Windows 11 Home Single Language, 64-bit operating system
Version	23H2
Installed on	17-06-2023
OS build	22631.4037
Browser	Microsoft Edge browser (Version 127.0.2651.105)

Using only manual methods to simulate various user scenarios and stress-test the platform's capabilities. Google docs is used for note-taking and documentation with screenshots and screen-capturing of bugs purposes.

Risk

The current state of the platform poses significant risks, including the potential for data breaches due to weak password policies, poor user interface design leading to user frustration, and outdated legal documentation that may not adequately protect users' privacy and security.



Conclusion (as of 23rd Aug, 24)

The AICamp platform, while promising in its mission, requires substantial improvements in security protocols and user experience design. Addressing the identified issues will be crucial for building user trust and ensuring the platform meets its claims of privacy, security, and seamless collaboration.

Exploratory Testing and Observations (Issues Found, if any)

1. Environment: Using Microsoft edge (Version 127.0.2651.105)
2. I visited AI Camp website here [Personal ChatGPT For Your Team | AICamp https://aicamp.so/](https://aicamp.so/) and read their claims about optimized assistance and collection of your AI/LLMs answers and data that you will be using in your project work to develop your product or any similar situations
3. The UI of their landing page looks clean as of now, keeping in mind that this is just a superficial survey!
4. I will need to check on this with the help of tools for deeper testing!

SECURITY

**Relentless protection,
every time**

 **GDPR-compliant**

We prioritize data privacy and adhere to GDPR regulations. Our platform, along with many of our models, is hosted within the EU.

 **ISO 27001 and SOC 2 Type 2**

AICamp is obtaining ISO 27001 and SOC 2 Type 2, showcasing our commitment to secure data management. You can contact us for further query.

 **No training data for LLMs**

We enforce stringent data usage policies. Our models do not undergo re-training with user data, guaranteeing that your information stays yours.

 **Custom data retention**

You can set the retention period for your data. You have control on your preferences.

5. I clicked on the **sign up for free** button and got redirected to this url: [Authentication \(aicamp.so\)](https://chat.aicamp.so/auth) / <https://chat.aicamp.so/auth> to register my account!

[Sign Up for Free](#)

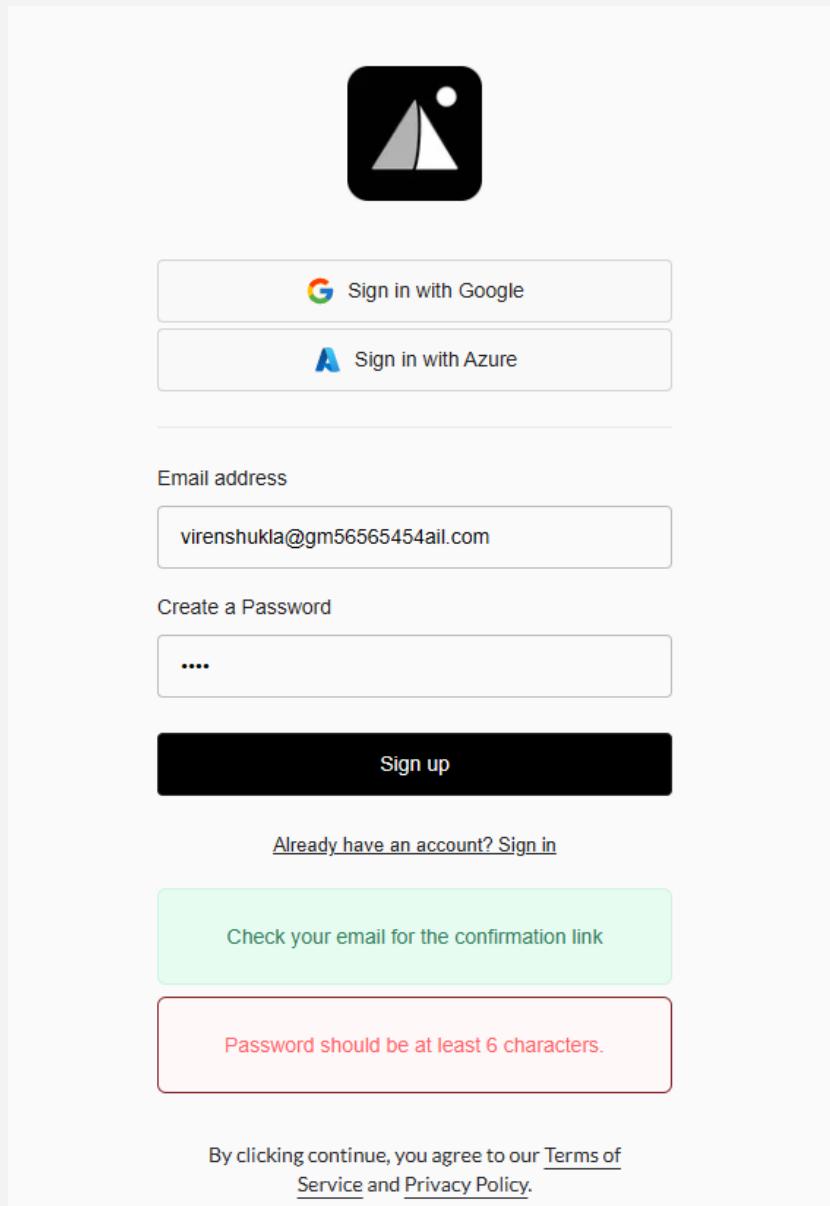
6. Email Validation and Password Requirements

Observation

During the sign-up process, the system accepted an incorrectly formatted email address "virensukla@gm56565454ail.com" without triggering any validation errors. Additionally,

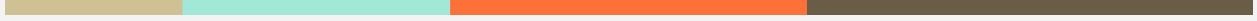
the password field only requires a minimum of 6 characters without requesting a confirmation of the password, potentially increasing the risk of user entry errors.

Screenshot



Potential Consequences

- **User Experience Impact:** Users who accidentally input incorrect email addresses may never receive confirmation emails, leading to frustration and potential loss of users.

- 
- **Security Concerns:** Accepting malformed email addresses without proper validation could be exploited by malicious actors to flood the system with invalid requests, potentially leading to performance issues or abuse.
 - **Operational Overhead:** Sending emails to invalid addresses can result in bounces, increasing the load on the mail server and potentially causing deliverability issues for legitimate emails.
 - **Data Integrity:** Invalid email entries can clutter the user database with unusable records, making it difficult to maintain accurate user data.
 - **Password Security:** Allowing users to set passwords without requiring confirmation increases the likelihood of typos or weak passwords, which could compromise account security.

Recommendation

- Implement both ***client-side & server-side*** validation to ensure that email addresses adhere to the correct format before submission.
 - Enhance password security by ***requiring users to confirm their password*** during the sign-up process to reduce the risk of entry errors and encourage stronger password practices.
7. Another issue I found here is that if I click on the “**Don't have an account? Sign up**” linkText then it does nothing, just disappears from the page and the same form is available to fill and create the account!

AICamp

"

Results are much better using v4 at lower costs for the entire team. Saving a chat to collection helps us a lot. I'd highly recommend if you've team and want to offer GPT-4 to your team in budget, go with AICamp. Requesting to add search across collections.



Jay Shah
CEO @Vistaran Techtronix



Sign in with Google

Sign in with Azure

Email address

Your email address

Your Password

Your password

Sign in

[Forgot your password?](#)

[Don't have an account? Sign up](#)

By clicking continue, you agree to our [Terms of Service](#) and [Privacy Policy](#).

- a. What is the use of it when it's going to leave us on the same page? Aren't there any more kinds of information to ask for preventing generation of fake accounts and related GIGO data.
 - b. Will it not give us unnecessary fake customer data if you want to train your marketing pixels-data points for better advertisement and reach?
 - c. Also it does not look good as per the user perspective; looks like a flaky glitchy behavior of the website.
 - d. Moreover the security of the user account is in question!
8. Then I clicked on this linkText of "**terms and conditions**" <https://aicamp.so/legal/terms-and-conditions> on the same page and went to the bottom of T&Cs, where I can see the date **27th December 2023**. **Is it an updated**

Terms & Conditions? (Looks pretty old)

These Terms were originally written in English. We may translate these terms into other languages, and in the event of a conflict between a translated version of these Terms and the English version, the English version will control.

19. Miscellaneous

The Agreement (together with any other terms we provide that apply to any specific Service) constitutes the entire agreement between us and you concerning our Services. If any part of the Agreement is unlawful, void, or unenforceable, that part is severable from the Agreement and does not affect the validity or enforceability of the rest of the Agreement. A waiver by either party of any term or condition of the Agreement or any breach thereof, in any one instance, will not waive such term or condition or any subsequent breach thereof. We may assign our rights under the Agreement without condition. You may only assign your rights under the Agreement with our prior written consent.

Changes

[27th December 2023](#)

AICamp

GDPR ISO 27001 AICPA SOC

Platform Resources Company

Chat Blog Get in touch

- a. Because any decent customer/user/enterprise or organization would like to know your Terms and Conditions are updated or not to make sure there won't be any security/data breach considering the privacy of an organization's private chats (includes strategies, plans and much more private data)
9. Later when I clicked on the "forgot password" linkText I got redirected here <https://chat.aicamp.so/auth> and the first thing I did was fill the input field with a random and unstructured string and clicked send reset password instructions.

Email address

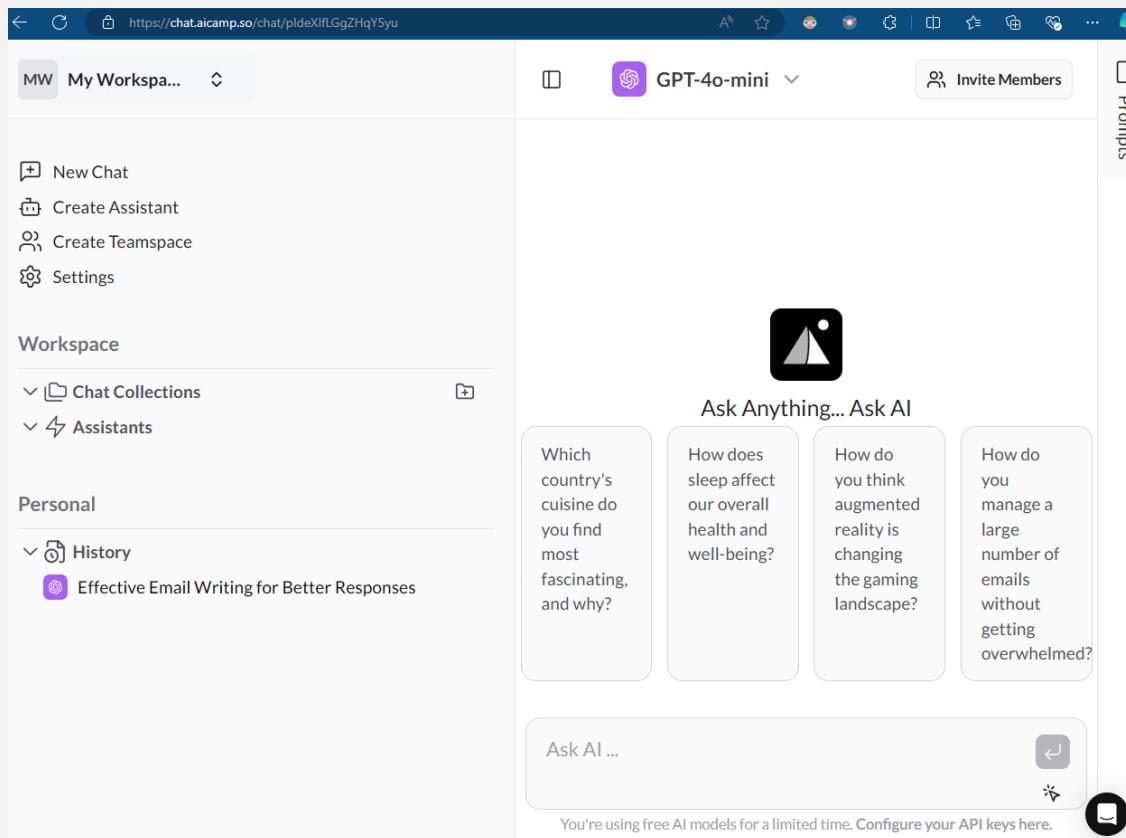
10. Which resulted in the message of "**Check your email for the password reset link**". This is a serious issue for a user who has forgotten which Email address he/she has

used for login on the website.

The screenshot shows a password reset form. At the top, it says "Email address" followed by a text input field containing "deasddpo###ol@gail.com". Below the input field is a large black button with the text "Send reset password instructions". Underneath the button, there is a link "Already have an account? Sign in". A green callout box at the bottom right contains the text "Check your email for the password reset link".

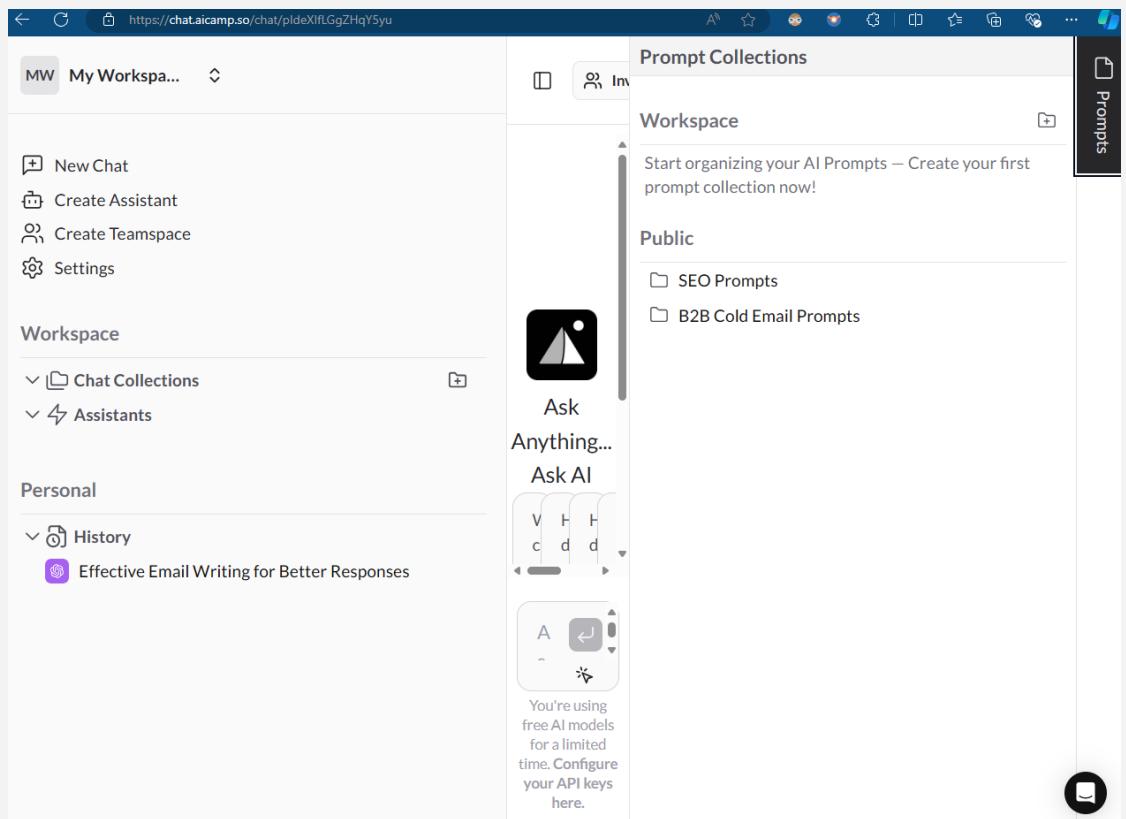
- a. This shows **there is no data binding with the database of the user account** on this website.
- b. Users will find it difficult to login and there is a serious certainty of data loss of company's private user/group chats, history of queries and solutions provided by the LLMs as per your claim as well as the integration of APIs and much more.

11. Upon login into the website I got directed to my chat (homepage), but User layout of the chat page looks kind of odd:



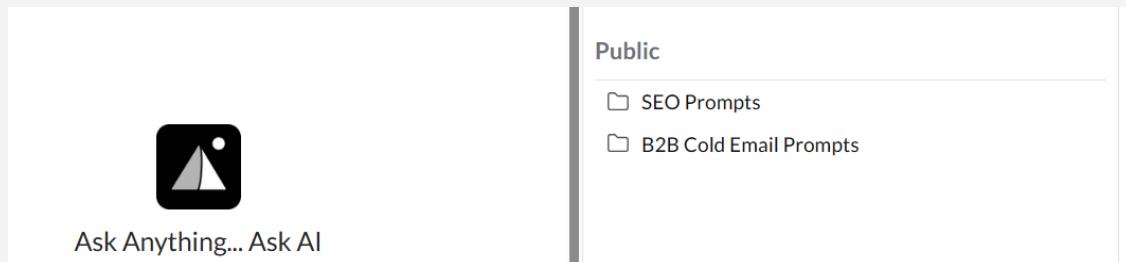
- a. Left Menu panel takes almost half of the screen, which is **unnecessary** if you compare it with ChatGPT and gemini or other available LLM
- b. Neither is there any way to reduce that to optimize user experience which is very necessary in this competitive market of AI!

12. When I clicked on the **Prompts** vertically situated button on the upper right corner, the resulting screen looks like this



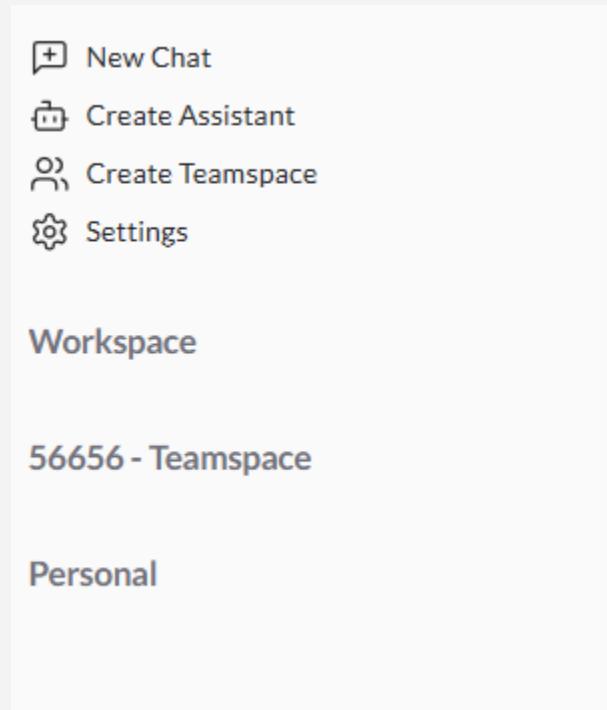
- which is not very appealing to the human eye and if you are targeting big firms to use your product, you must showcase your well polished product. Wrapping your gift box is very important!
- This makes it very difficult to use the actual chat box of LLMs
- Hence, the left panel should be dynamically retracted if there is a click on the **Prompts** (vertically situated button; top right corner)

13. Users may have to face difficulties due to the accident touches and they might wonder where the options went!

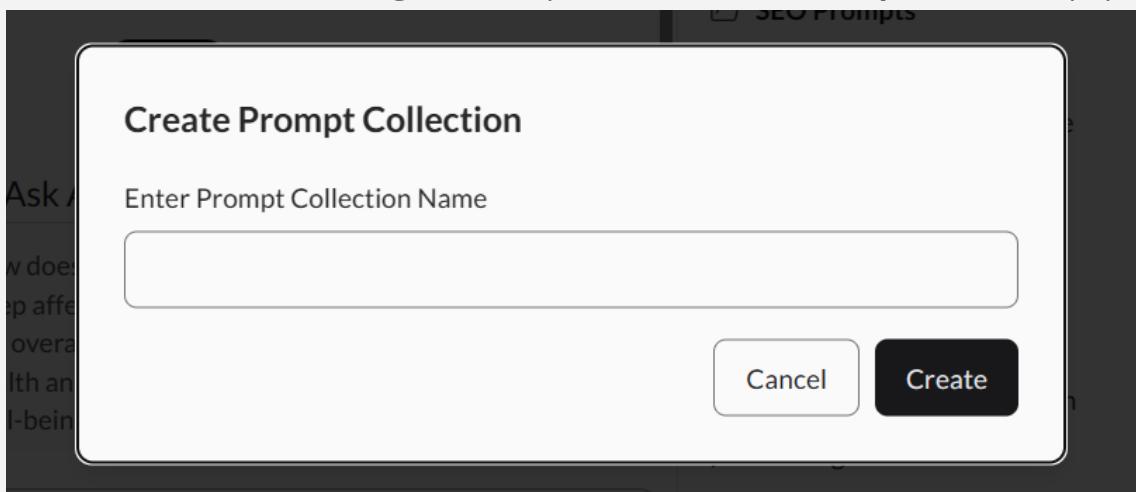


- Here, on the right panel clicking on the Public text or space on the right, results in the sudden retraction of 2 prompts options!

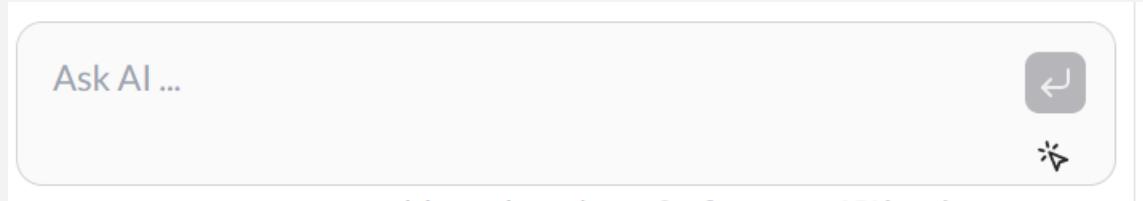
- b. Which is unnecessary at this stage of this website and if you are planning to add more options to the panel then at least give some kind of dropdown menu symbols ("+" or "▼" or "▼").
- c. Another example of it ↗



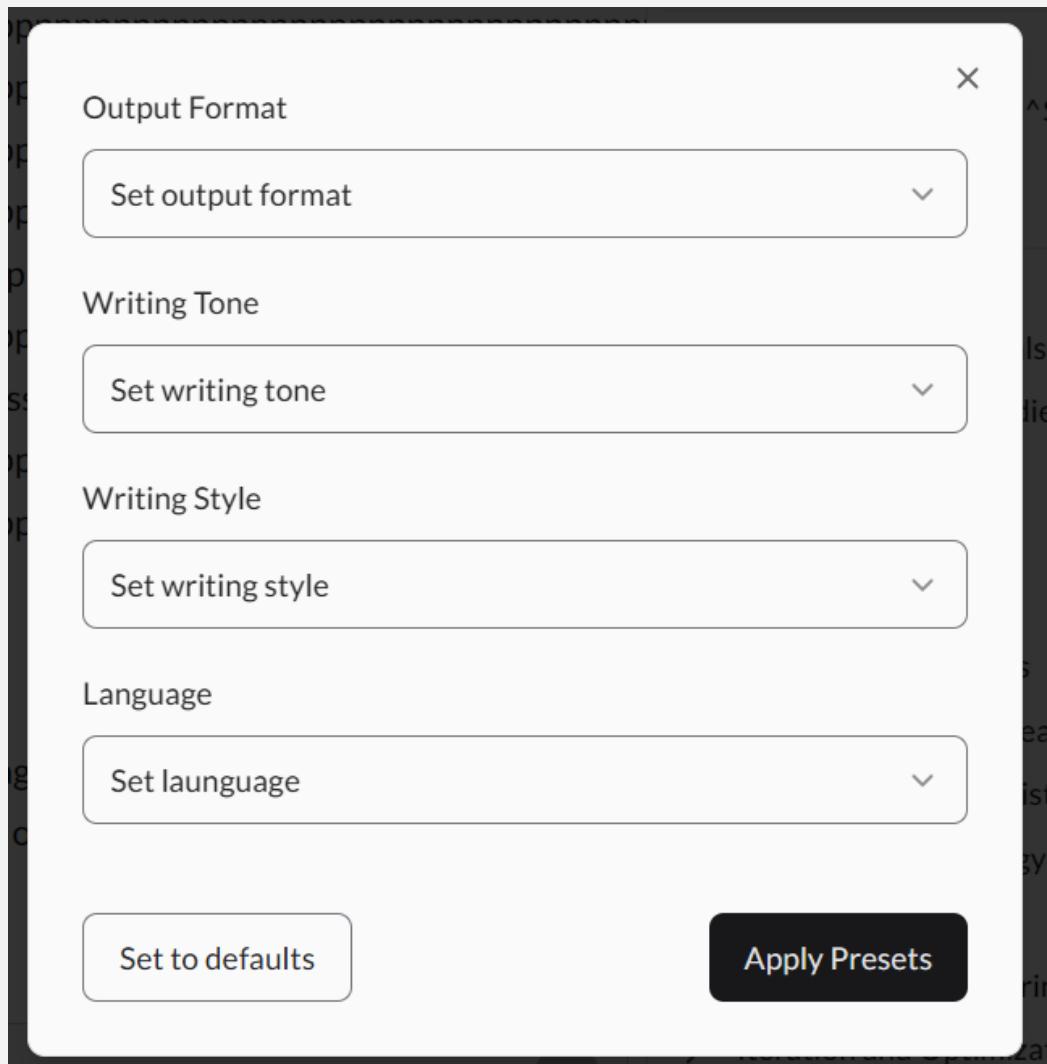
14. There is no word limit message to this input field in **Create Prompt Collection** popup



15. There is no hover-highlighted Text here for the **prompt enter button and custom Output**

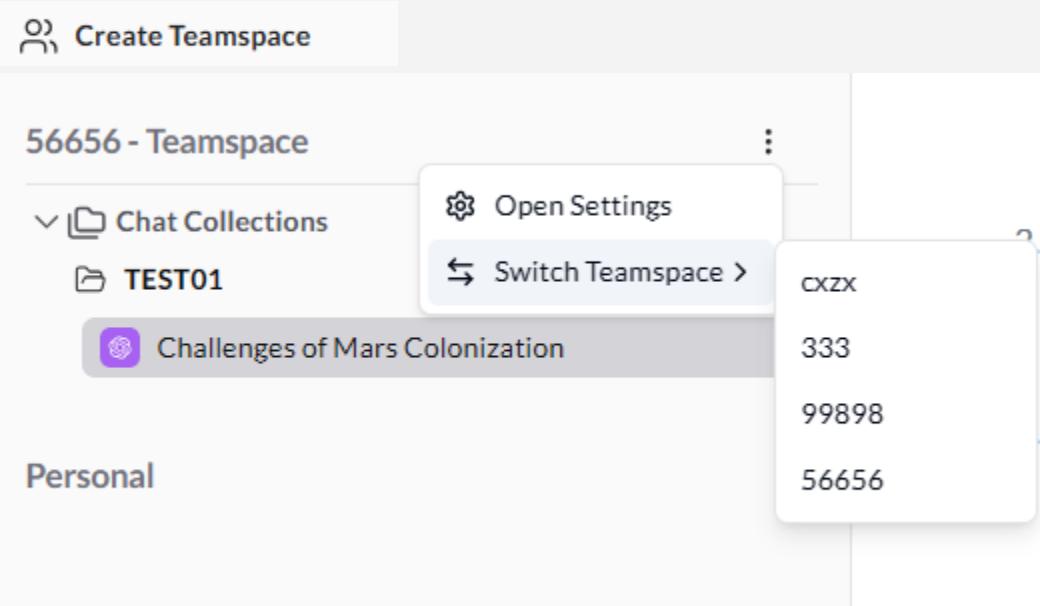


- a. Getting confused while trying to prompt and mis-clicking the "Output format" button, resulting in this popup window



- b. Confusing symbols due to close proximity?

16. While exploring through left menu panel I created “TeamSpace” by clicking on ↗

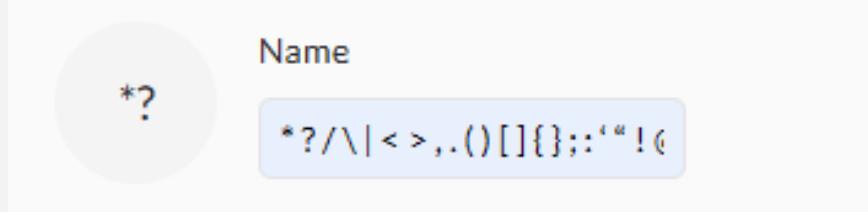


- a. No proper instructions on how to select between different team spaces created previously
- b. Hard to find the options, **not good for user retention!**
- c. Earlier I thought previous team spaces have been deleted automatically and was not even shown in the history

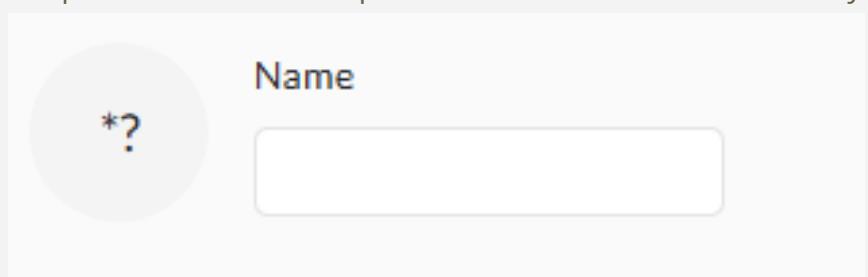
17. Next, I clicked “Settings” redirected to this url:
<https://chat.aicamp.so/settings/workspace/general> And I clicked on first option on left menu panel “User”

The screenshot shows the 'My Profile' settings page. The left sidebar has 'My Workspace' and 'User' selected under 'Profile'. The main area has sections for 'My Profile' (with a placeholder '@'), 'Account Security' (with a 'Change Password' button), and 'General' (under 'Workspace'). At the bottom, there's a 'Go back to chats' link.

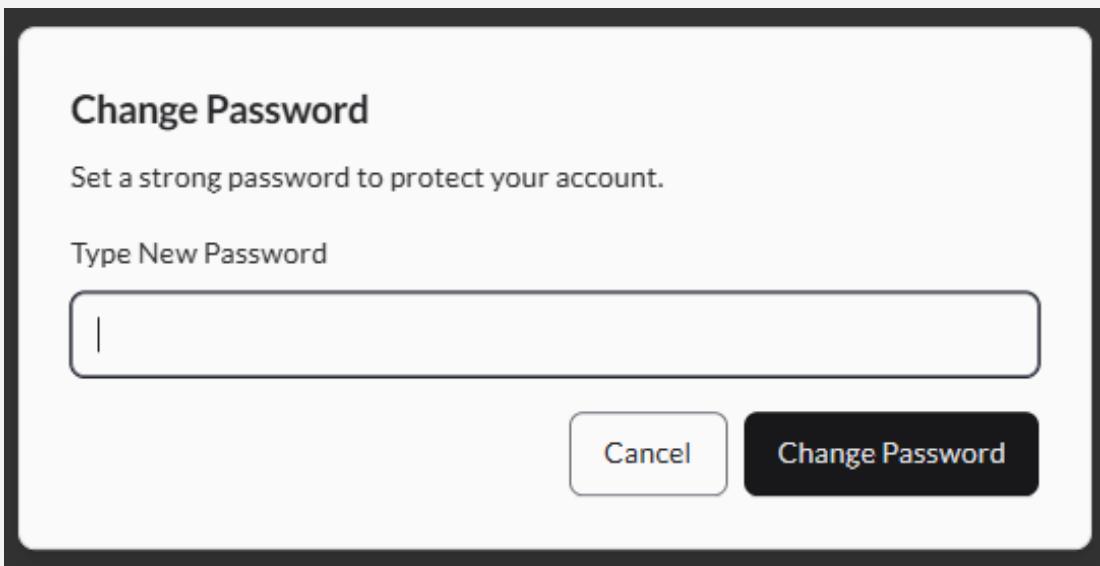
- a. Is the UI very simple and dull? Looks very dry
 b. Not able to click on the circle favicon image and no option for uploading image/display-picture for the user
18. The circle is taking any character typed in the input field



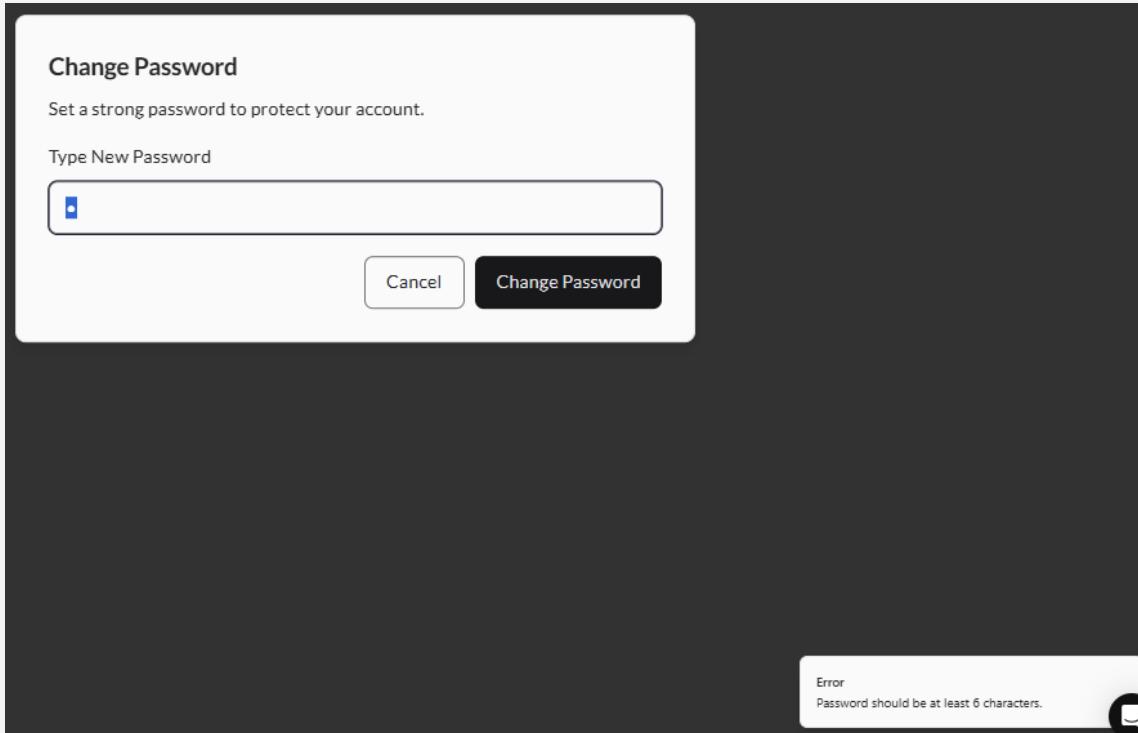
- a. Looks very glitchy and buggy
 b. No polished product appeal to the end user's eye
19. No placeholder in the input field and it does not show any error of empty field



20. About the “Account Security” :
- Account Security**
- Change Password
Set a strong password to protect your account.
- Change
- a. Via clicking on change, this prompt appears



- b. Again no placeholder for the input field and default no word limit message
21. On entering a single variable in the input field and clicking the change password button it shows this error message at the bottom-right corner.



- a. Is this the only requirement of creating a password? (Hence, see point 4).
22. Following observation is to be taken seriously***

Observations on Password Security

1. Weak Password Vulnerability:

Risk of Brute-Force Attacks: A simple 6-character password is highly susceptible to brute-force attacks. Given the vast number of possible combinations, even with a mix of letters, numbers, and symbols, modern algorithms can crack such a password quickly.

Risk of Dictionary Attacks: Simple passwords, especially those that are common or follow predictable patterns (e.g., "abc123" or "password1"), are



vulnerable to dictionary attacks, where attackers use a precompiled list of common passwords.

2. Insufficient Password Complexity:

Lack of Length and Variety: Passwords of only 6 characters lack the complexity needed to provide adequate security. Longer passwords with a mix of uppercase and lowercase letters, numbers, and special characters are recommended.

Failure to Meet Best Practices: Many security guidelines recommend a minimum of 8-12 characters for passwords, incorporating diverse character sets to enhance security. A 6-character password does not meet these best practices.

3. Potential Exploitation:

Social Engineering: Simple passwords can be easier to guess or obtain through social engineering tactics, where attackers manipulate individuals into revealing their credentials.

Risk to Confidential Information: If an attacker compromises a weak password, they could gain unauthorized access to sensitive data or critical features, potentially leading to data breaches or other security incidents.

4. Contradiction with Security Claims:

Inconsistent with Security Standards: While AICamp promotes **GDPR compliance** and is obtaining *ISO 27001 and SOC 2 Type 2 certifications*, allowing or using simple 6-character passwords could undermine these security measures, especially in a business environment where data security is paramount.

False Sense of Security: Users might assume that because the platform is secure overall, their password choice does not need to be strong. However, individual account security is crucial to maintaining the platform's overall integrity.

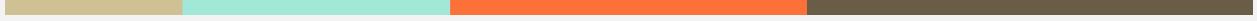
Recommendations:

- **Enforce Stronger Password Policies:** Recommend that the platform enforce a minimum password length of 12 characters, incorporating a mix of character types.
- **Encourage Multi-Factor Authentication (MFA):** Suggest the implementation of MFA to add an additional layer of security beyond just passwords.
- **User Education:** Advise the platform to educate users on the importance of strong passwords and the risks associated with weak ones.

While AICamp presents itself as a secure and private AI platform, the allowance of simple 6-character passwords poses significant security risks. Strengthening password policies and implementing additional security measures are crucial steps to align the platform's practices with its security claims.

Next Scope for deeper testing:

- **Data Encryption Practices:** Examine the robustness of encryption methods used to protect sensitive user data, both at rest and in transit.
- **Multi-Factor Authentication (MFA):** Assess the implementation and effectiveness of MFA to enhance security, especially for administrative and high-privilege accounts.
- **Stress Testing:** Conduct rigorous load testing to evaluate how the platform performs under high traffic and user concurrency, identifying potential bottlenecks.
- **Cross-Browser Compatibility:** Ensure that the platform's functionality and user experience are consistent across different browsers and devices.
- **Accessibility Compliance:** Evaluate the platform's adherence to accessibility standards, ensuring it is usable by individuals with disabilities.
- **API Security:** Test the security of exposed APIs, focusing on vulnerabilities like unauthorized access, data leakage, and input validation.

- 
- **User Data Handling:** Analyze the processes for data collection, storage, and deletion to ensure compliance with privacy regulations and best practices.

Each of these areas requires thorough examination to prevent potential issues and align the platform with its security and usability commitments.

