Submit #564451: PrivateGPT 0.6.2 CWE-942: Permissive Cross-domain Policy with Untrusted Domains

Title	**PrivateGPT 0.6.2 CWE-942: Permissive Cross-domain Policy with Untrusted Domains**
Description	Private GPT's CORS settings are misconfigured, allowing any origin to interact with the application without restriction. This flaw exposes sensitive user data to attackers who can deploy malicious JavaScript on their websites and trick users into executing it. By exploiting this vulnerability, attackers can bypass the intended isolation of Private GPT, even in environments deployed on internal networks, and extract sensitive information such as credentials or private documents.
Source	⚠️ https://gist.github.com/superboy-zjc/2a727cb0c1d468f21a91e0416d006ffe
User	Gavin Zhong (UID 84092)
Submission	04/23/2025 07:51 PM (17 days ago)
Moderation	05/09/2025 04:54 PM (16 days later)
Status	Accepted
VulDB Entry	308235 [Zylon PrivateGPT up to 0.6.2 settings.yaml allow_origins cross-domain policy]
Points	20

⚠ Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling