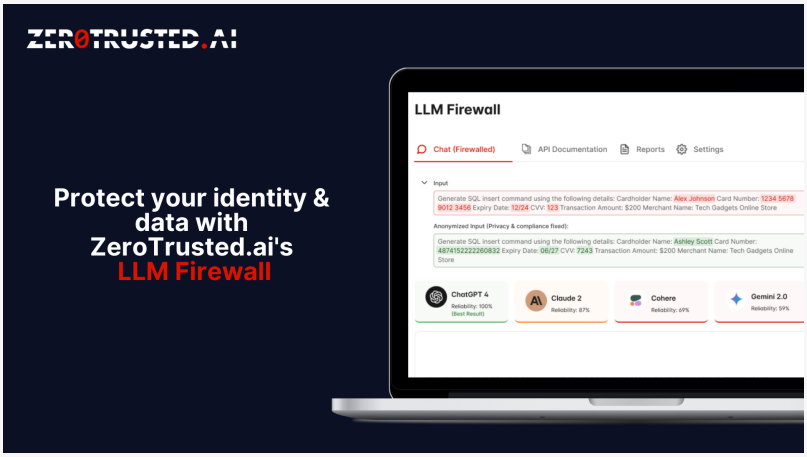
Securing the Future of Language Models: ZeroTrusted.ai Tackles Critical Flaw in ChatGPT

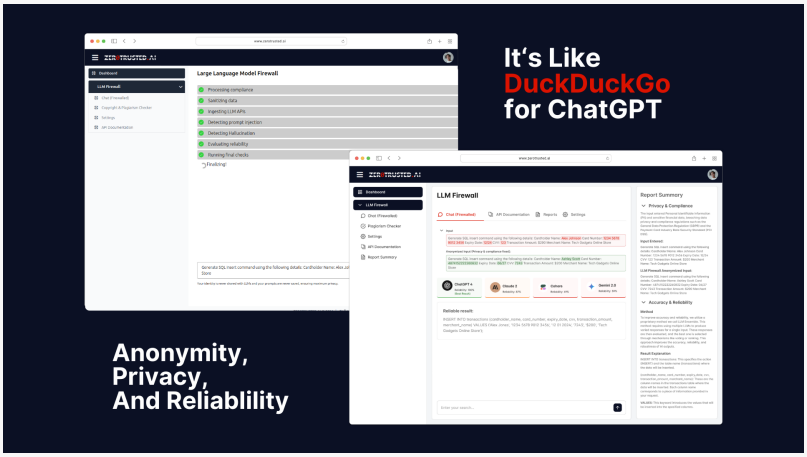
Cutting-edge technology addresses vulnerability, ensuring privacy and security in AI interactions

KISSIMMEE, FLORIDA, USA, March 19, 2024 /EINPresswire.com/ -- As Language Model (LLM) technologies like ChatGPT and Microsoft CoPilot continue to revolutionize human interactions with artificial intelligence, concerns over cybersecurity vulnerabilities have emerged. Recently, a team of red team researchers uncovered a critical flaw affecting leading LLM platforms, including ChatGPT and Microsoft CoPilot, raising alarms about the security of digital interactions.

ZeroTrusted.ai Logo



Protect your Identity and Data

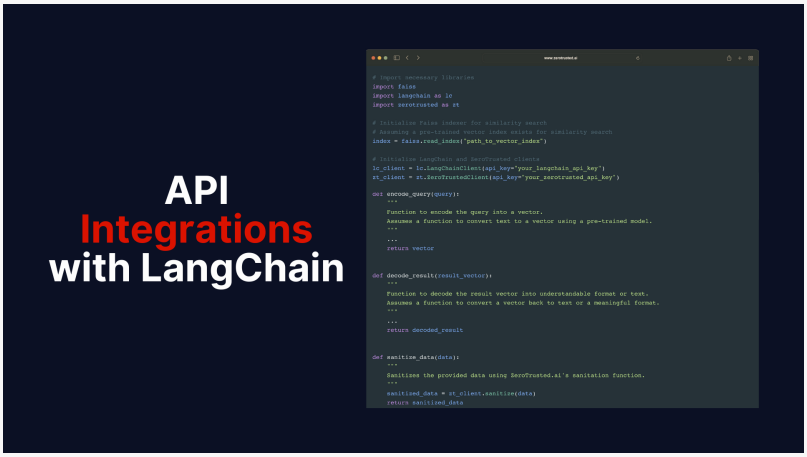


It's like DuckDuckGo for ChatGPT

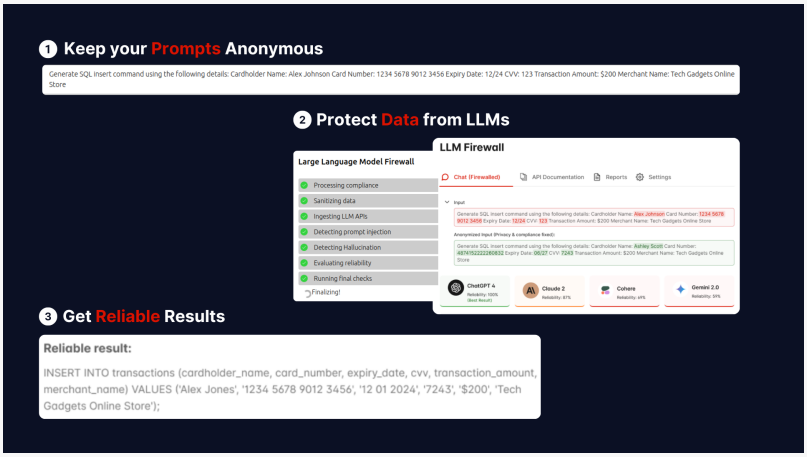
The flaw, as outlined in a recent article on Ars Technica, exploits the token-based response system utilized by these LLMs. By analyzing the length of each token, attackers can decrypt conversations and deduce the contents of user prompts and responses, compromising seemingly secure communications.

In response to increasing LLM threats, ZeroTrusted.ai has developed an innovative LLM Firewall solution that enhances the privacy and security of AI assistant interactions. This solution addresses the token-length vulnerability by transmitting data in bulk, significantly reducing the attack surface and

mitigating against LLM inference attacks. Moreover, ZeroTrusted.ai is bolstering its defenses with additional encryption to counter targeted man-in-the-middle attacks, ensuring users can harness the benefits of popular LLMs without sacrificing privacy or security.



API Integrations with LangChain



Keep Your Prompts Anonymous, Protect Data from LLMs, and Get Reliable Results

ZeroTrusted.ai's commitment to user privacy and security is further emphasized through its privacy-centric features, including anonymous searches, no search history, and a strict no data tracking policy. These measures underscore ZeroTrusted.ai's dedication to providing users with a robust defense against the evolving landscape of digital threats.

"Our mission at ZeroTrusted.ai is to empower users to navigate the world of LLMs confidently, without compromising their digital privacy," said Femi Fashakin, CTO at ZeroTrusted.ai. "By integrating advanced security measures and prioritizing user privacy, ZeroTrusted.ai enables individuals to embrace AI technologies securely and confidently."

For individuals seeking a safer way to interact with AI, ZeroTrusted.ai's LLM Firewall offers a comprehensive solution. To learn more and sign up, visit www.zerotrusted.ai.

About ZeroTrusted.ai
ZeroTrusted.ai is a pioneering company in the field of Generative AI security, starting with Zero Trust Architecture (ZTA) and dedicated to protecting corporate data in the LLM ecosystem. With a focus on innovation and compliance, ZeroTrusted.ai delivers unparalleled solutions for organizations navigating the complex world of AI and data privacy.

Sharon Lam
ZeroTrusted.ai
+1 407-507-9350
contact@zerotrusted.ai
Visit us on social media: