SOJIB AHMMED

AI Research & Cybersecurity · sojibahmmed.com

Media Contact: Sojib Ahmmed | press@sojibahmmed.com | sojibahmmed.com
Twitter/X: @sojibahmmed | LinkedIn: /in/sojibahmmed

FOR IMMEDIATE RELEASE

DHAKA, BANGLADESH — June 5, 2026

Sojib Ahmmed Launches sojibahmmed.com to Bridge AI Research and Cybersecurity

A new home for original research, technical writing, and practitioner-grade tooling at the intersection of machine learning and security.

sojibahmmed.com officially launches today as the personal platform of **Sojib Ahmmed**, an AI researcher and cybersecurity practitioner. The site consolidates years of work across adversarial machine learning, LLM safety, offensive security, and applied threat research into a single, openly accessible publication.

Unlike vendor blogs and aggregator newsletters, sojibahmmed.com is built around primary material: reproducible experiments, annotated code, threat write-ups, and long-form analysis intended for engineers, researchers, and security leaders who need depth rather than headlines.

“The gap between AI capability research and the security teams who have to defend production systems is widening,” said Sojib Ahmmed. “This site is my attempt to close it — in public, with working artifacts instead of marketing.”

What’s on the site at launch

• **Original research** on prompt injection, model extraction, and red-teaming methodology for LLM-backed applications.
• **Technical write-ups** covering AI-assisted offensive security, detection engineering, and secure-by-design ML pipelines.
• **Open tooling and notebooks** that accompany each post so readers can reproduce and extend the work.
• **Commentary** on emerging policy, disclosure norms, and the practical risk surface of frontier AI systems.

Who it’s for

Security engineers integrating AI into existing stacks, ML practitioners shipping models into hostile environments, and researchers tracking the fast-moving boundary between the two fields.

About Sojib Ahmmed

Sojib Ahmmed has worked across AI research and cybersecurity since 2021, focusing on adversarial ML, LLM safety, and applied offensive security. His writing and tooling are used by independent researchers and security teams worldwide.

■ ■ ■

Media inquiries: press@sojibahmmed.com · Web: sojibahmmed.com