𝗣𝗿𝗼𝗺𝗽𝘁 𝗜𝗻𝗷𝗲𝗰𝘁𝗶𝗼𝗻, 𝗧𝗿𝗮𝗶𝗻𝗶𝗻𝗴 𝗗𝗮𝘁𝗮 𝗣𝗼𝗶𝘀𝗼𝗻𝗶𝗻𝗴, 𝗮𝗻𝗱 𝗘𝘅𝗰𝗲𝘀𝘀𝗶𝘃𝗲 𝗔𝗴𝗲𝗻𝗰𝘆.

This interactive experience equips with the knowledge and tools to identify and mitigate these emerging risks in LLM applications.

Other interactive labs by Kontra(Security Compass) 👨🏻‍💻

1. OWASP Top 10 for Web - https://application.security/free/owasp-top-10

2. OWASP Top 10 for API - https://application.security/free/owasp-top-10-API

3. Front-end Top 5 - https://application.security/free/kontra-front-end-top-5

4. AWS Top 10 - https://application.security/free/kontra-aws-clould-top-10

5. OWASP Top 10 for iOS - https://application.security/free/marketing-iphone-swift

6. Docker CLI Top 10 - https://application.security/free/docker-top-10

7. Docker Compose Top 10 - https://application.security/free/docker-compose-top-10

8. OWASP Top 10 for Kubernetes - <https://application.security/free/OWASP-Top-10-for-Kubernetes>

C:\Users\MN>ipconfig

C:\Users\MN>netstat –ano

<https://dashboard.shadowserver.org/>

Hardcode: code er modde user id and password dewa ace.

<https://github.com/MobSF/Mobile-Security-Framework-MobSF>

<https://mobsf.live/>