AI által generált weboldalak kockázat**AI**

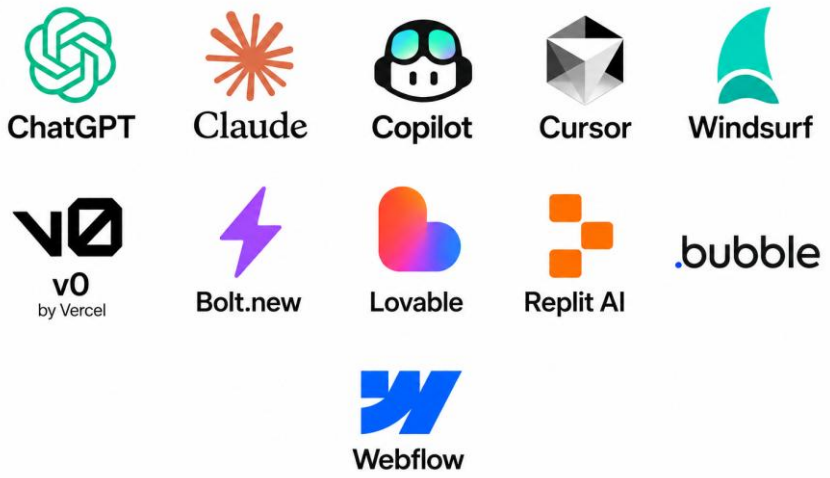
avagy a működő kód nem ugyanaz, mint a biztonságos kód.

Kiss Tamás László
NBSZ NKI főosztályvezető

NEMZETI KIBERBIZTONSÁGI INTÉZET

ONLINE AI FEJLESZTŐPLATFORMOK

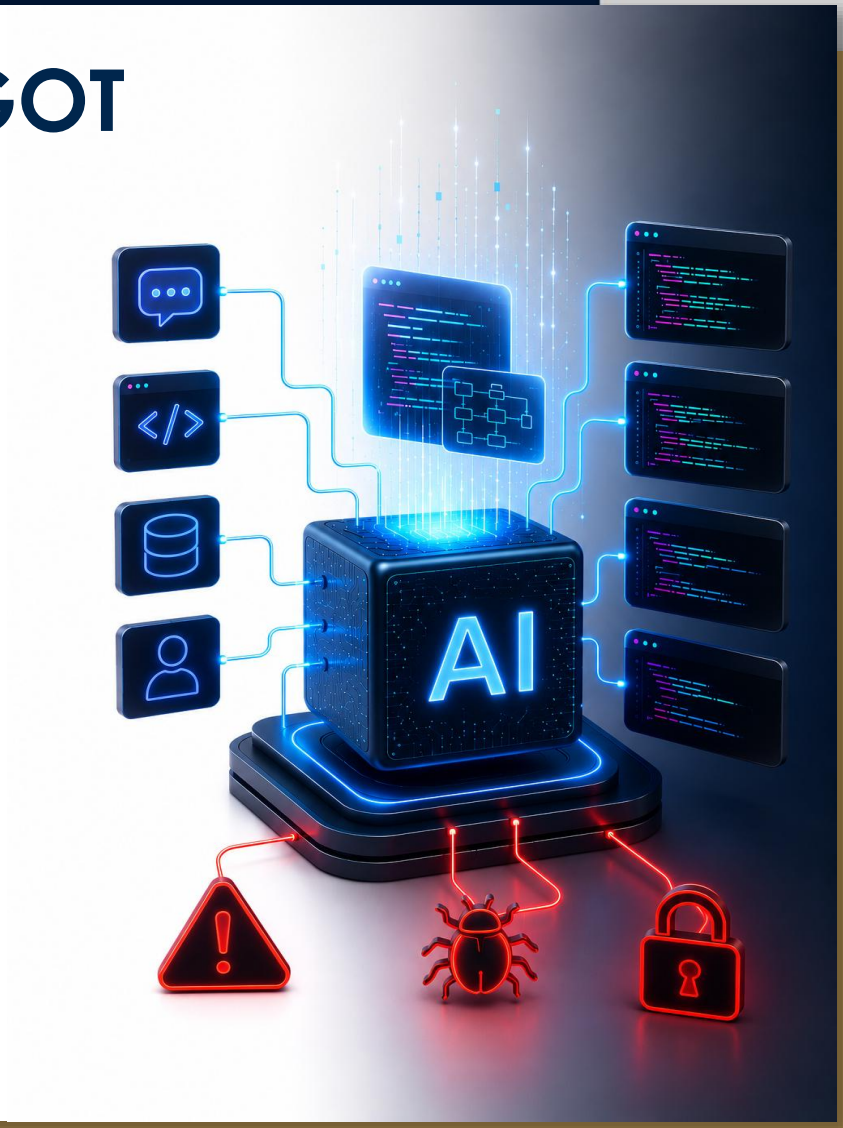
- gyors prototípuskészítés
- boilerplate generálás
- frontend fejlesztés gyorsítása
- CRUD rendszerek percek alatt
- kisebb fejlesztői tudással is működő rendszer készíthető



AZ AI NEM ÉRTI A BIZTONSÁGOT

- nem gondolkodik
- nem ért üzleti logikát
- nem tudja, mi a „jó security”
- statisztikai minták alapján generál

- A tréningadatok tartalmaznak:
  - sérülékeny mintákat
  - elavult megoldásokat
  - hibás konfigurációkat
- Eredmény:
  - működőnek tűnő
  - de sérülékeny kód



TIPIKUS AI ÁLTAL GENERÁLT SÉRÜLÉKENYSÉGEK

- SQL injection
- Cross site scripting
- Hardcoded secret
- Engedékeny hozzáférések
- Hallucinált security
  - nem létező security header
  - hibás autentikációs flow
  - hibás API használat
- Supply-chain kockázat
  - sérülékeny kiegészítők
  - elavult csomagok

MIÉRT NEM VESZIK ÉSZRE?

- működik, ezért biztonságosnak tűnik
- az AI magabiztosan generál hibás kódot is
- a generált kód „professzionálisnak” néz ki
- a fejlesztő nem mindig érti a generált kódot
- nincs megfelelő security review
- a gyorsaság fontosabb lesz, mint a biztonság
- a sérülékenységek nem látszanak első ránézésre
- hiányzik a sérülékenységvizsgálat
- a hibák sokszor csak éles környezetben derülnek ki

HOGYAN VÉDEKEZÜNK?

- Fejlesztés közben
  - secure coding guideline
  - AI usage policy
  - kötelező code review
- Automatizált ellenőrzések
  - SAST
  - SCA
  - secrets scanning
  - dependency monitoring
- Release előtt
  - sérülékenységvizsgálat
  - API security teszt
  - konfiguráció audit
  - jogosultságvizsgálat

AI-asszisztált fejlesztés ≠ kontroll nélküli fejlesztés

Az AI nem érti a biztonságot,
a felelősség továbbra is emberé!

Köszönöm a figyelmet!

Kiss Tamás László
NBSZ NKI főosztályvezető

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI
KIBERBIZTONSÁGI
INTÉZET