

# SECURITATEA APLICATIILOR ASISTATA DE LLM

Student: Emil Marian  
Pașca

Coordonator: Prof. Dr.  
Ing. Olivu Dorin Matei

---

# PROBLEMA

Companiile testează dacă API-urile returnează datele corecte.

Mult mai rar testează sistematic dacă API-ul refuză accesul greșit:

- un client accesează documentele altui client;
- un rol primește mai multe drepturi decât ar trebui;

Aceasta este zona în care apar vulnerabilități de tip BOLA / IDOR.

Aspecte probematice din punct de vedere a testării continue și mentenanței API-urilor

- testarea manuală și mentenanța sunt costisitoare;

# De ce contează: nu este doar un bug tehnic

Impactul unei vulnerabilități BOLA / IDOR



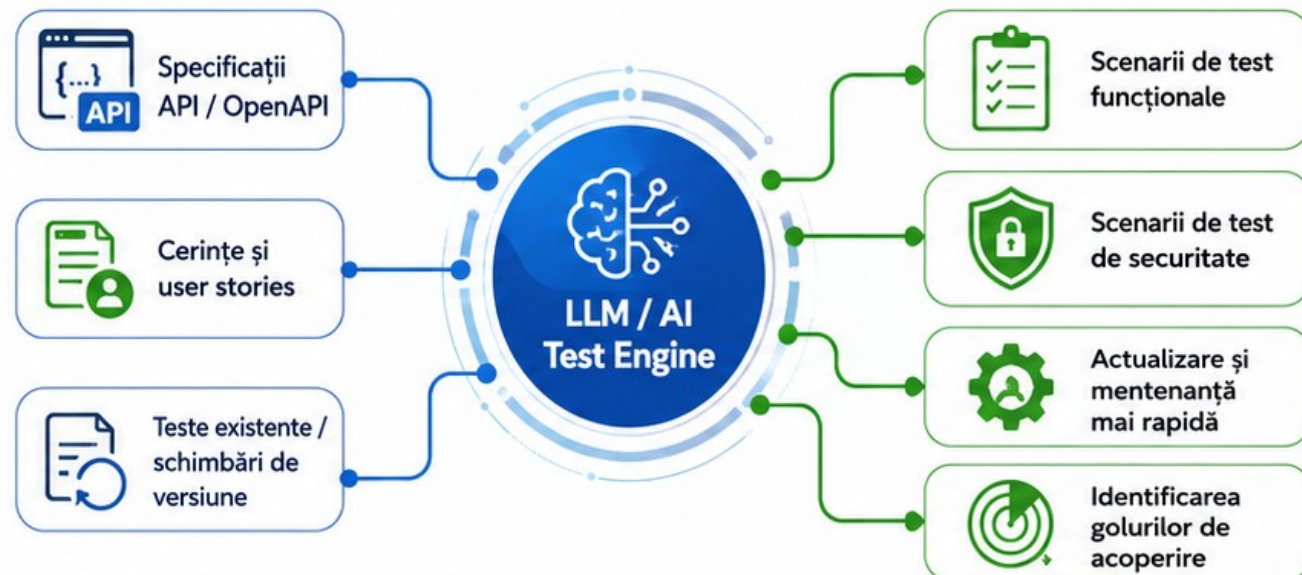
# Cum accelerează AI ciclul de viață al testării software

Generare asistată de LLM pentru teste funcționale și de securitate

## Abordare tradițională



## Soluția mea: generare de teste asistată de AI



## Impact în ciclul de viață al software-ului



## AI reduce timpul dintre schimbare și testare relevantă



## Ideea-cheie

LLM-ul nu doar generează teste mai repede, ci îmbunătățește mentenanța și extinde acoperirea către zone funcționale și de securitate.

# Validare în contexte reale de business



**API-uri reale / specificații OpenAPI**  
pentru a testa și îmbunătăți abordarea



**Companii fintech, banking, SaaS**  
cu API-uri complexe și cerințe de securitate



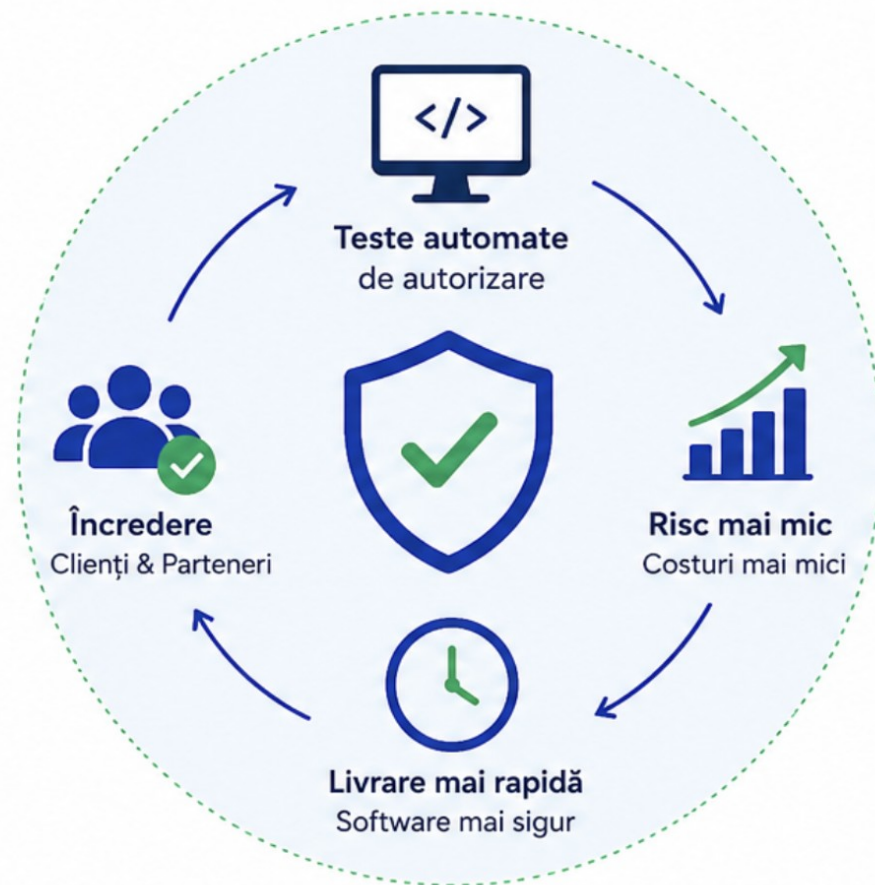
**Feedback de la echipe**  
QA, Security, Development, Product



**Pilot / Proof of Concept**  
integrare în fluxul existent (CI/CD)



**Parteneriate & colaborări**  
pentru validare, extindere și impact real



**Obiectiv:** să validăm dacă această abordare reduce efortul de testare și crește acoperirea pe autorizare, înainte ca problemele să devină incidente.

The image features a minimalist design with two thick, horizontal gray bars at the top and bottom. A thin, vertical purple line is positioned to the left of the central text.

MULTUMESC!