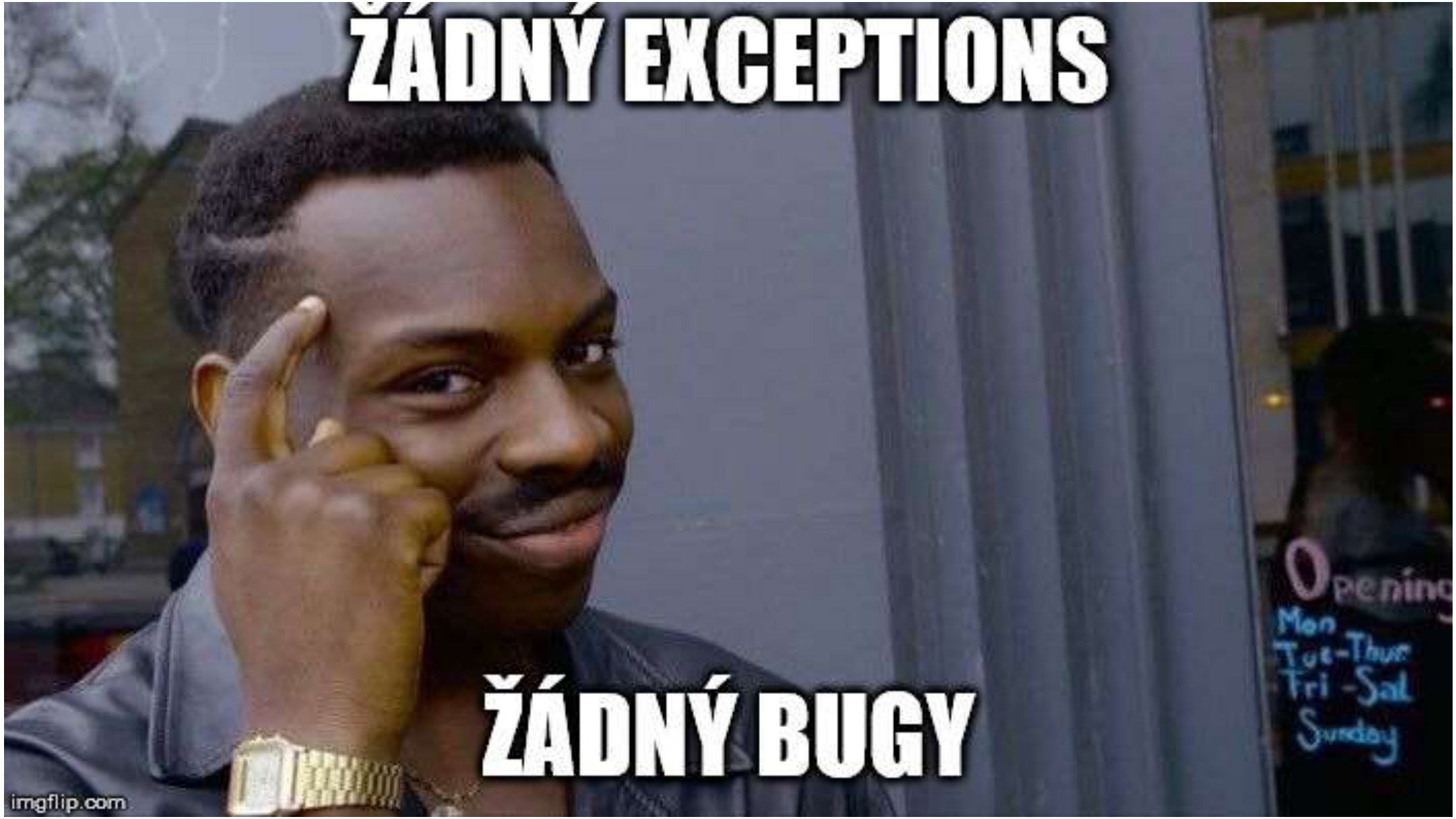
Defenzivní programování

Mgr. Jiří Činčura
MVP
www.tabsoverspaces.com
@cincura_net


ŽÁDNÝ EXCEPTIONS
ŽÁDNÝ BUGY
imgflip.com

Defenzivní programování

- *Cvičení: Napište metodu, která dostane na vstupu Stream a na pozici 0x10 změní hodnotu z 0x00 na 0xFF.*

Defenzivní programování

- Program by měl fungovat i v případě neočekávaného stavu nebo vstupu
- Především pro safety/security části a HA
  - Secure programming jako podmnožina
- Týká se i návrhu API

Defenzivní programování

Defenzivní programování

- Predikovatelné chování na neočekávaném vstupu/...
  - Memory corruption
- Obecná kvalita kódu

- Buffer overflow, vlastní auth, vlastní encrypt, SQL injection, ...

Defenzivní programování

- "Defend against the impossible, because the impossible will happen."
- Všechna data jsou důležitá, dokud někdo neprokáže opak
- Všechna data jsou "nabořená", dokud někdo neprokáže opak
- Všechna data jsou "nebezpečná", dokud někdo neprokáže opak
- Včetně "interních" komponent/dat/struktur
  - Dlouho žijící projekty
  - Mnoho lidí
  - Značná maintenance

Defenzivní programování

- Vývojářům/knihovnám se nevěří
  - A uživatelům už vůbec ne
- Řízení na silnici…
  - Myslíme za jiné
- Velké projekty
  - Motivace
  - Rozdílné zkušenosti

Defenzivní programování

- Ne paranoia
- Ne debilní testy všeho
  - Čitelnost a udržovatelnost kódu
- Korektnost
  - Snaha napravit vše
- Risk management

Defenzivní programování

- Verifikace korektnosti, ne nekorektnosti
- Whitelisty, ne blacklisty
- Striktní kód
- (Znovu)využívání kódu
- Knihovny, abstrakce
  - Prověřené
  - "Don't reinvent the wheel."
- Coding styles
- Immutable objekty

Defenzivní programování

- Design by contract
- Formálně definované a verifikovatelné specifikace
  - Nemusí to nutně být kód
- Nástroje
  - Preconditions
  - Asserts
  - Postconditions
  - Invariants (code-flow, class, internal, …)
- Kontrakty jsou efektivně self-testy
  - Doplňují unit-, akceptační-, …, testy

Defenzivní programování

- Precondition
  - Co metoda/... očekává
- Postcondition
  - Co metoda/... garantuje
- Invariant
  - Co metoda/... zachovává

Defenzivní programování

- Návrh API
  - Špatné použití
  - Nepochopení
  - Existuje více cest/možností?
  - Jednotky
  - Závislosti, pořadí
    - Objekt by nikdy neměl být v nekonzistentním stavu

Demo

Otázky

Mgr. Jiří Činčura
MVP
www.tabsoverspaces.com
@cincura_net