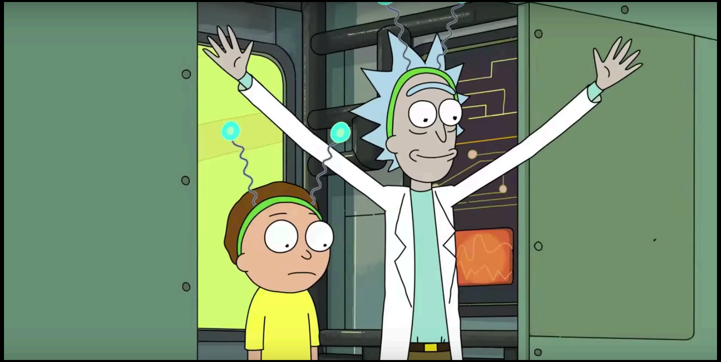
AuthoRIZAtioN bypAss

HOW (AND WHY) YOUR QA TEAM CAN SAVE THE DAY

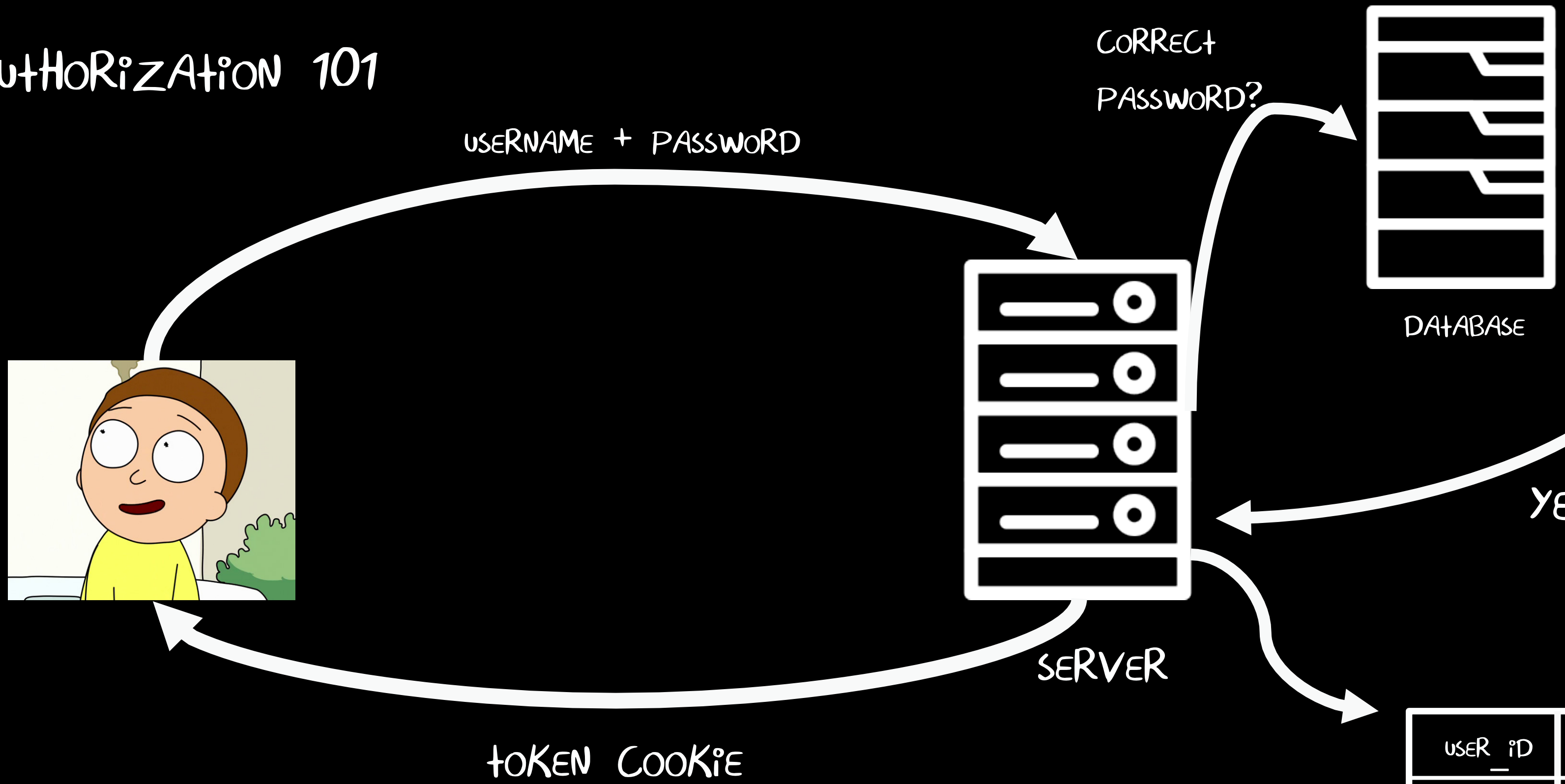
WIX.com

GREETINGS!

- GILAD KATZIR
- SECURITY RESEARCHER AT WIX.COM
- LIVE IN TEL-AVIV
- PII FANATIC, STATISTICS ENTHUSIASTIC, STRONG BELIEVER IN QA SECURITY



AUTHORIZATION 101



USERNAME + PASSWORD

CORRECT PASSWORD?

DATABASE

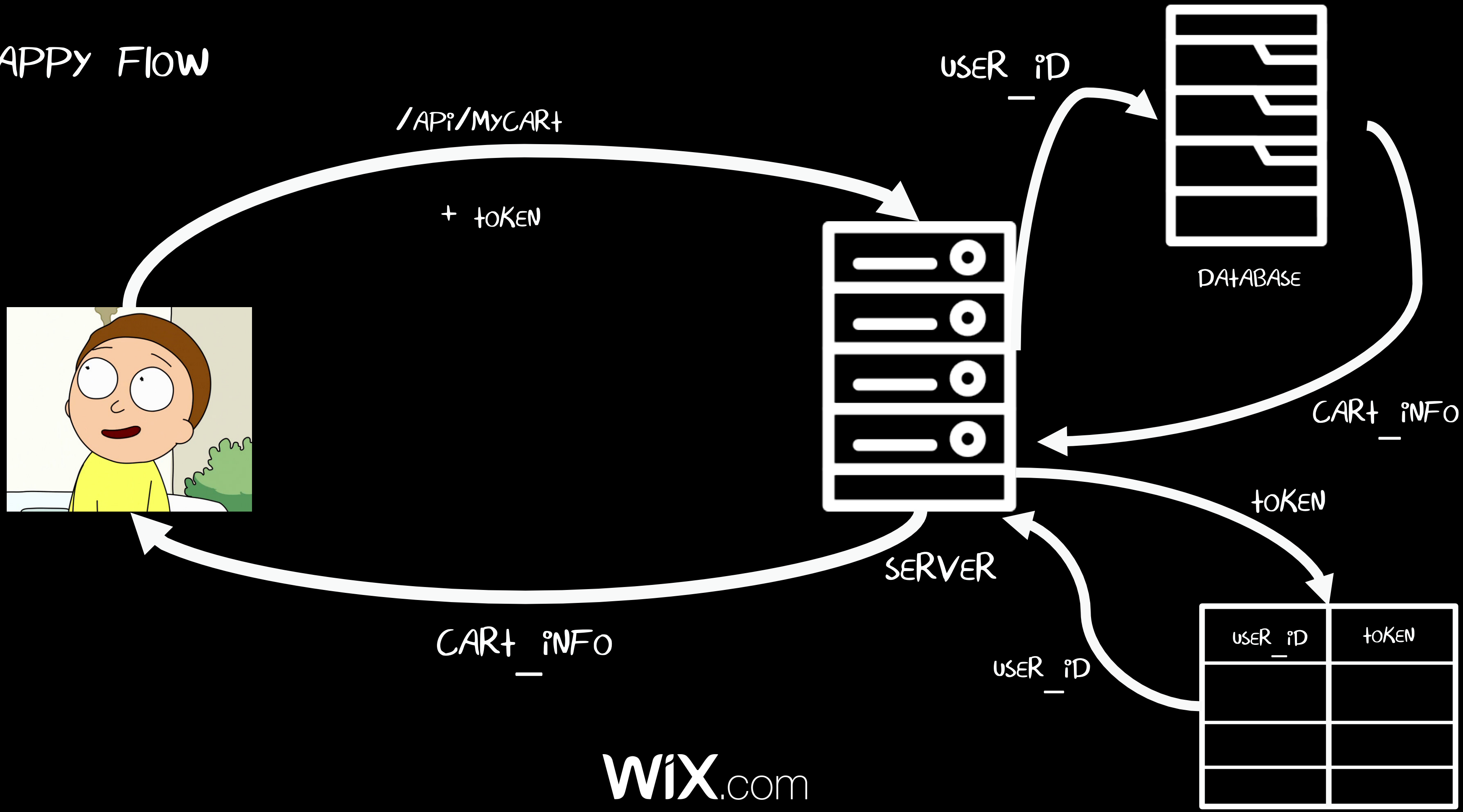
YES!

SERVER

TOKEN COOKIE

USER_ID	TOKEN

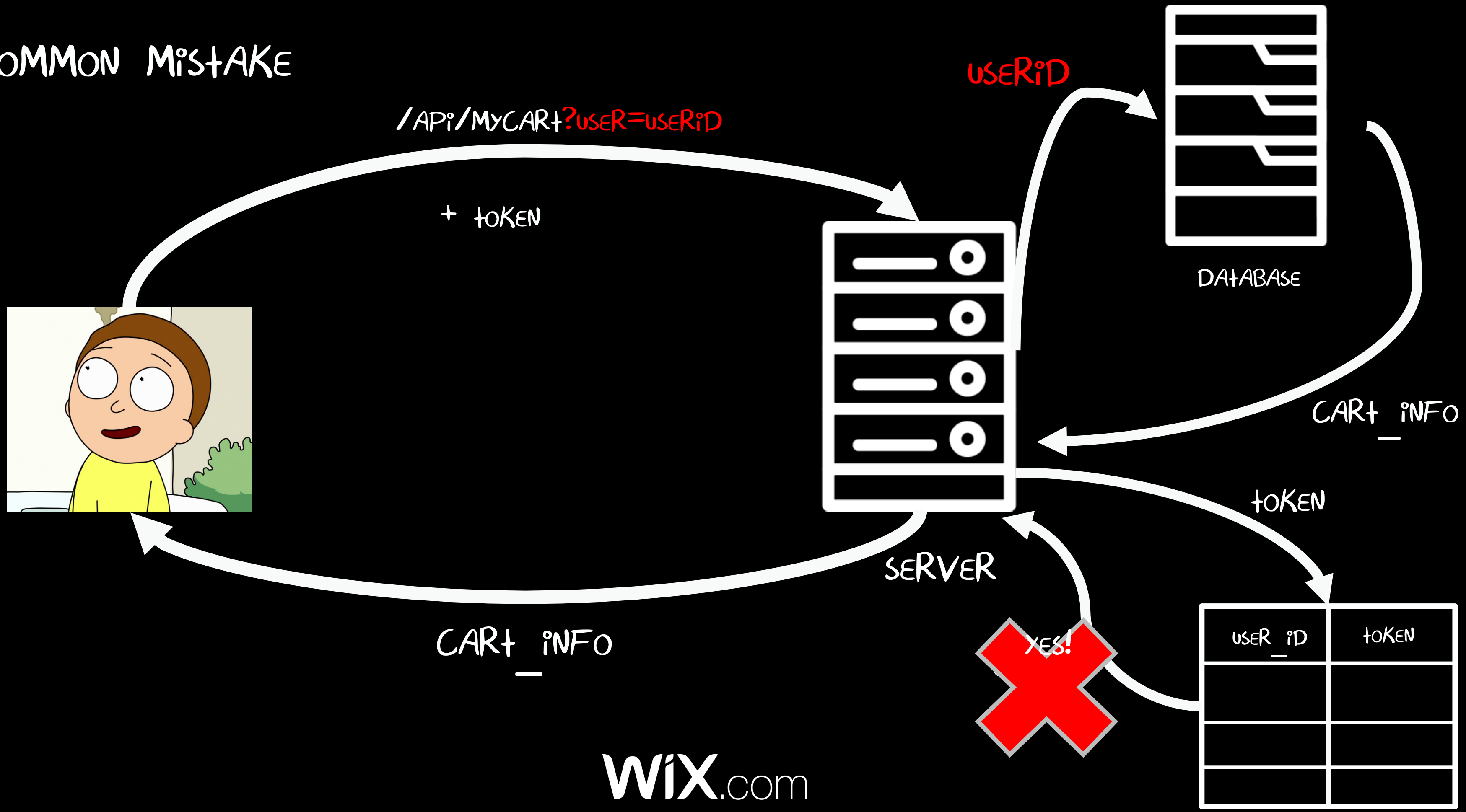
HAPPY FLOW



USER_ID	TOKEN

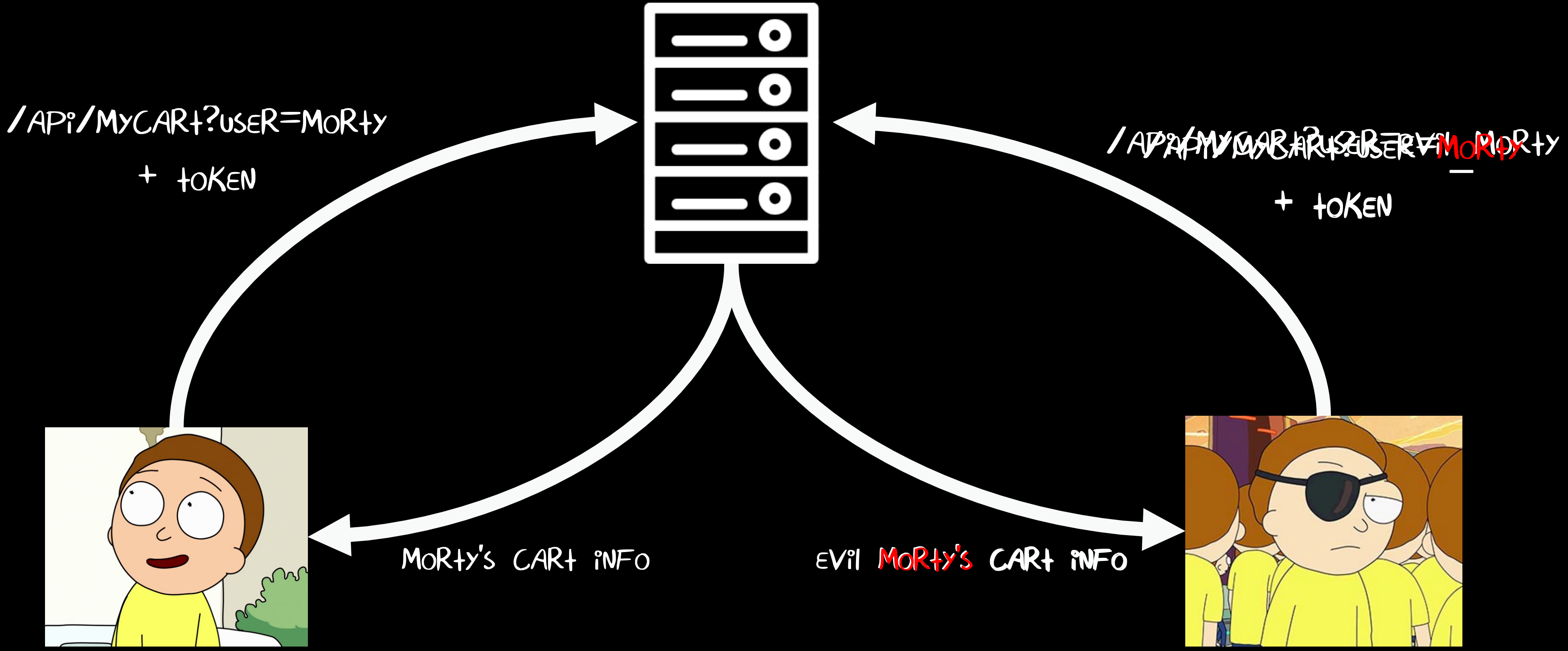
WiX.com

COMMON MISTAKE



WiX.com

EASY EXPLOIT



/API/MYCART?USER=MORTY

+ TOKEN

/API/MYCART?USER=EVIL_MORTY

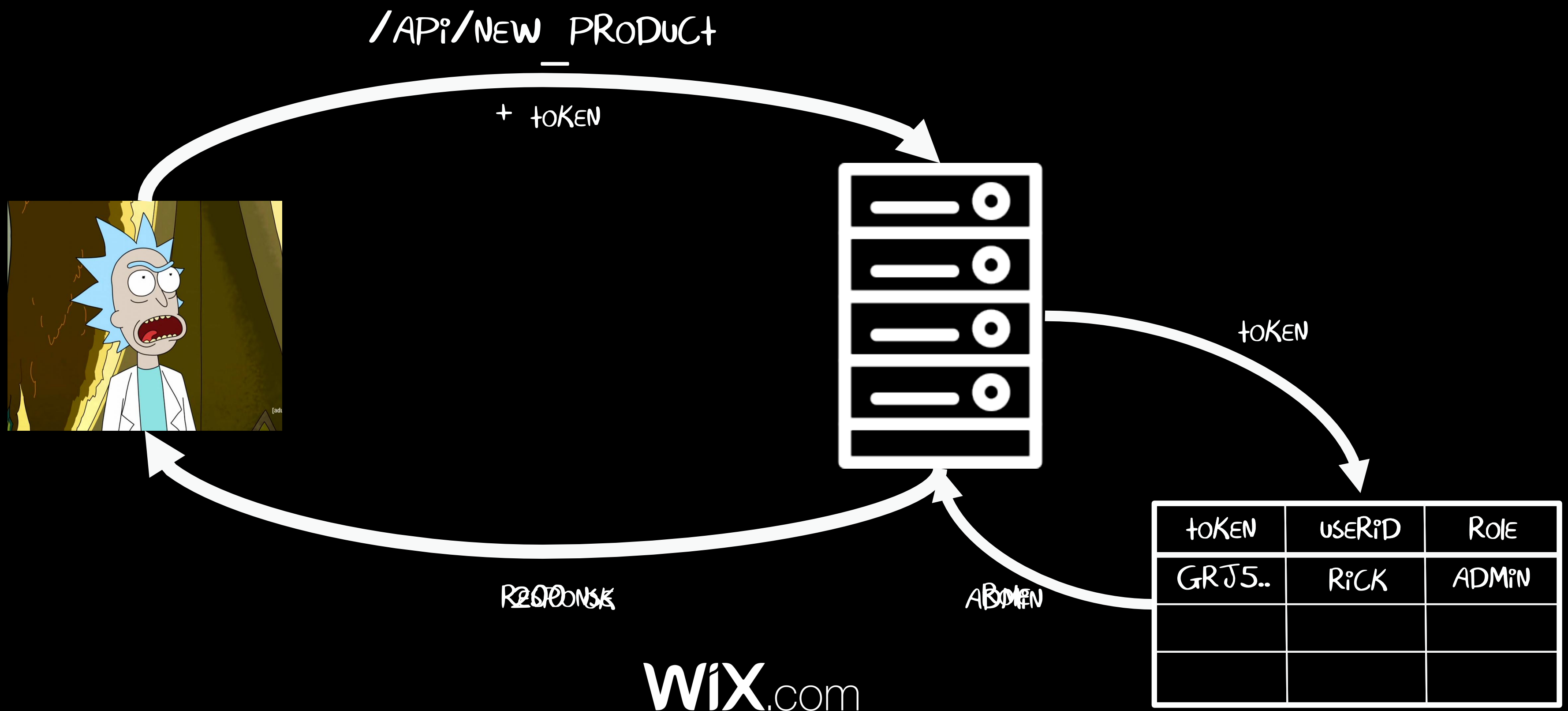
+ TOKEN

MORTY'S CART INFO

EVIL MORTY'S CART INFO

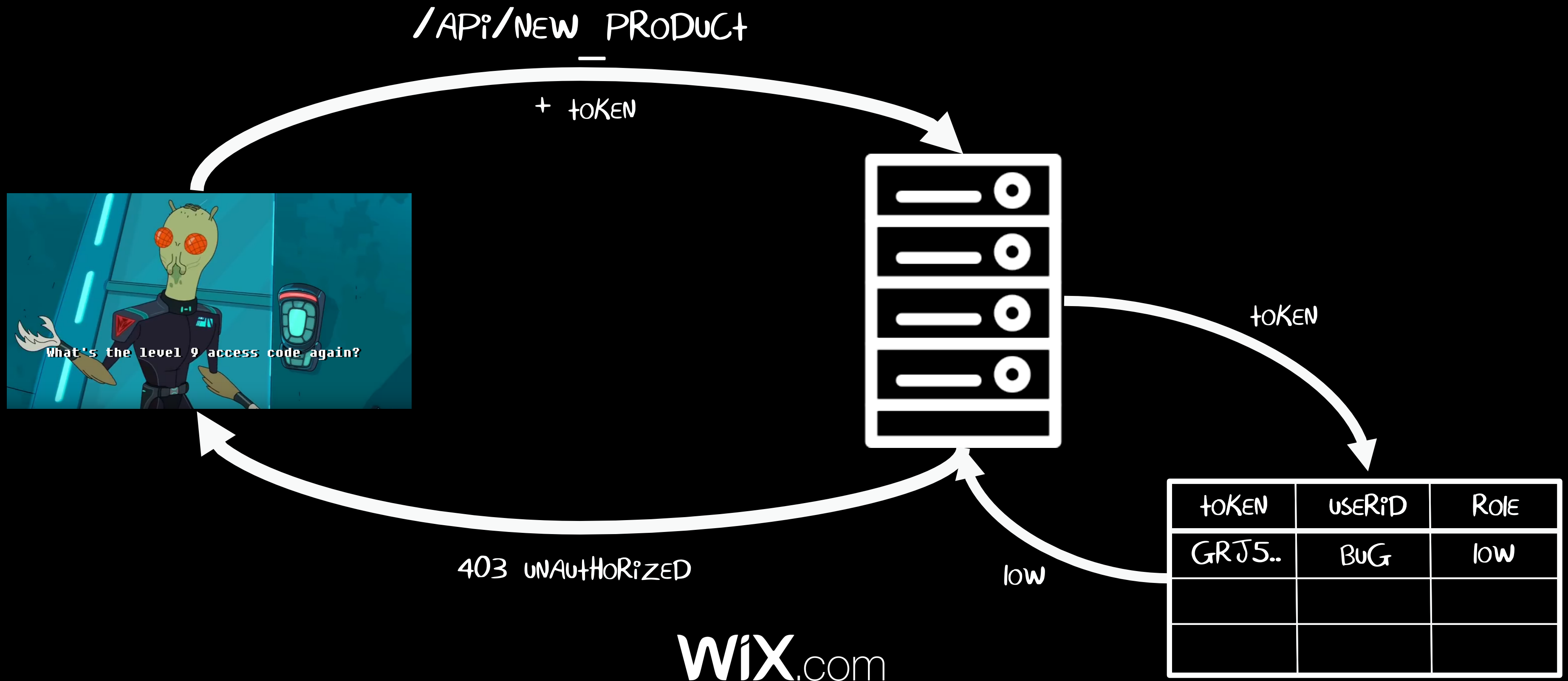
let's start with a demo...

ACCESS CONtROl 101



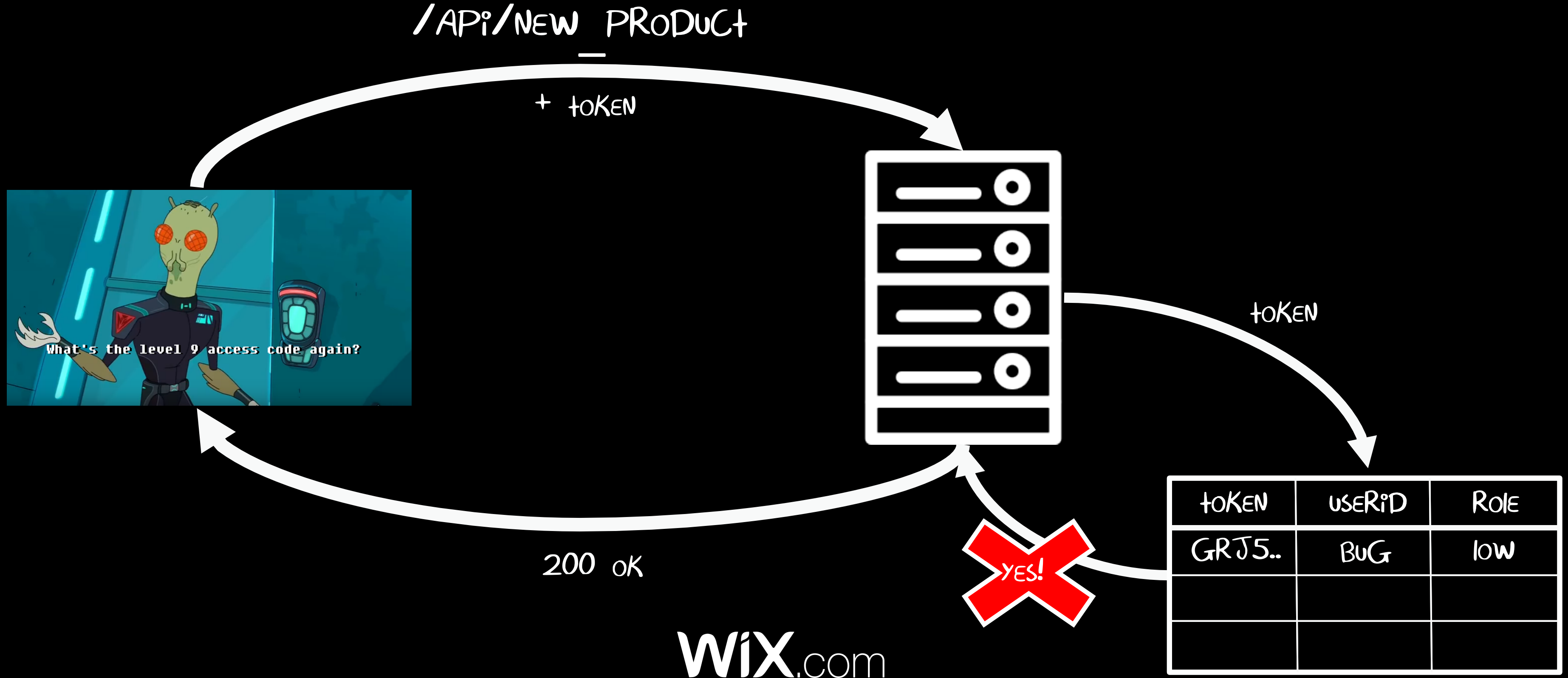
tOKEN	USERiD	ROlE
GRJ5..	RiCK	ADMiN

ACCESS CONTROL 101



TOKEN	USERID	ROLE
GRJ5..	BUG	low

FORCEFUL BROWSING

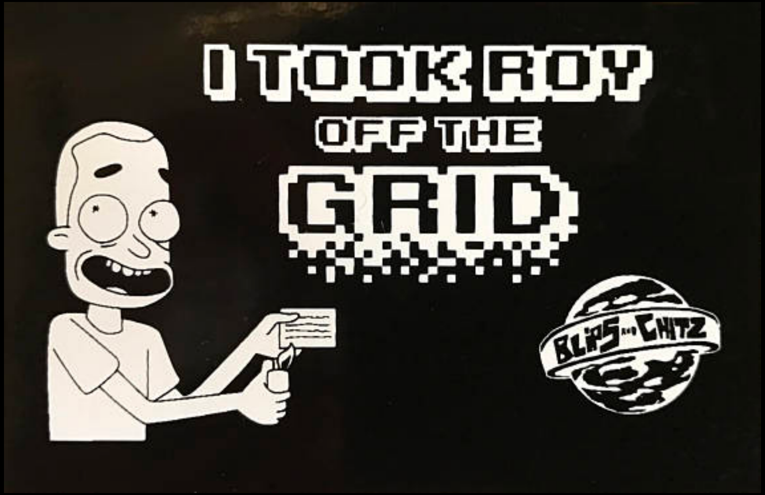


TOKEN	USERID	Role
GRJ5..	BUG	low

WIX.com

All SHAPES AND SiZES

- PARAMETER tAMPERiNG
- FORCEFUl BROWSiNG
- FORGOttEN/HiDDEN CONtENt
  - DEFAUlt COMPONENtS
  - URl GUESSiNG
- HORiZONtAl/VERtiCAl



WiX.com

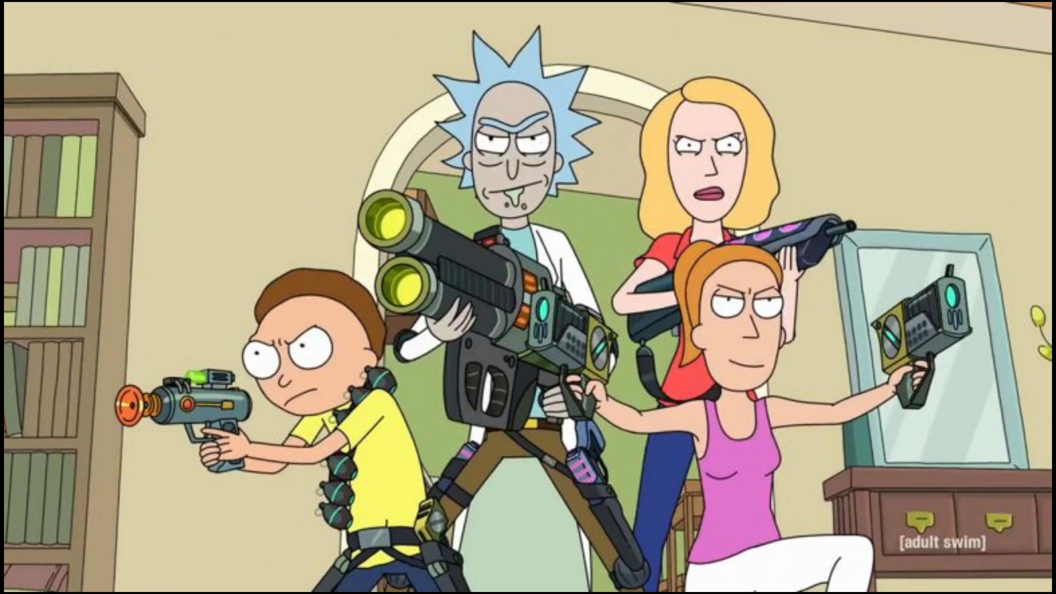
NO PROBlEM _ OuR PROGRAMMERS ARE GREAt!

- tHis is BASiC, sHoulD BE EASY
- tHERE is AlWAYS tHis ONE ENDPOiNt tHAt WAS MiSSED
- MiCROSERViCES ARE tHE WORSt!
  - DOZENS OF REQuEStS, SiNGlE ButtON CliCK.
  - REStFul APi - DiFFERENt REStRiCtiON FOR DiFFERENt MEtHOD (PAtCH, uPDAtE, Put, GEt).

so to sum things up

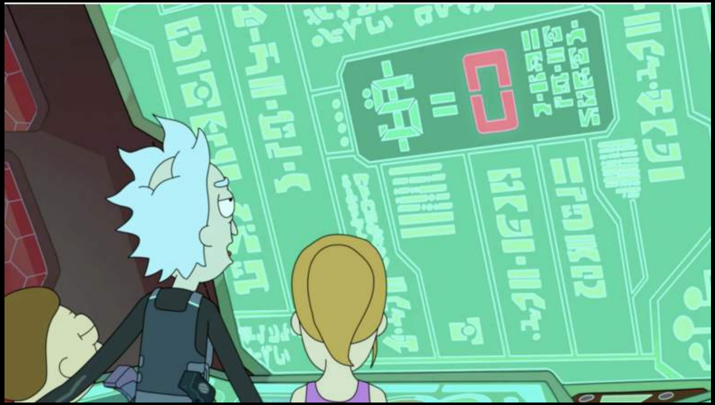
- ~x1000 of endpoints.
- specific business logic for each endpoint
- Multiple Roles/tenants
- All tests need to be manual
- AND...

YOU ONLY HAVE 4 SECURITY ANALYSTS



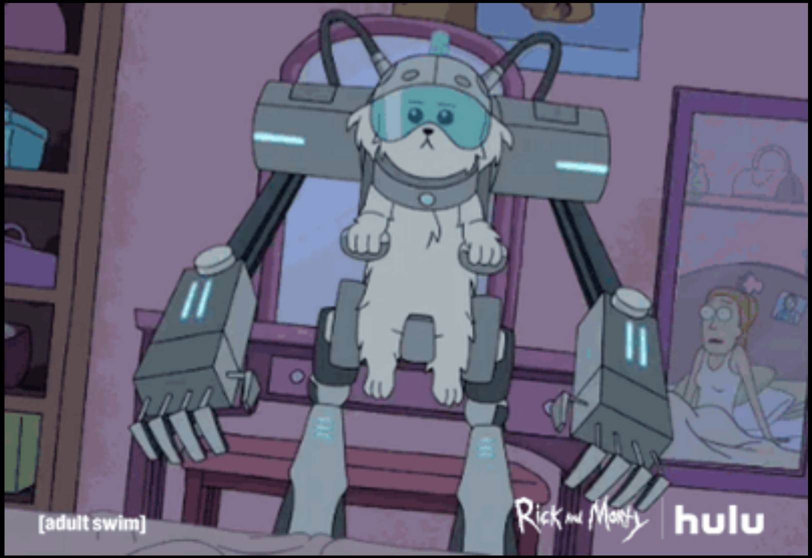
QA to tHe RescUe!

- PURE BUSINESS LOGIC BUG
- INTIMATE KNOWLEDGE
- MANUALLY TESTING
- NO NEED FOR SPECIAL SECURITY SKILLS
- „QUALITY ASSURANCE" DEFINITION
- WE STILL HAVE ONE PROBLEM THOUGH...



Wix.com

INTRODUCING AUTORIZE



My two Cents

- security is everyone's Job
- sometimes it only takes one small Mistake

QuestioNs?