



QUALITY #17
MEETUP


24 maja 2018, 18:00

Strefa Centralna
plac Sejmu Śląskiego 2, 40-001 Katowice

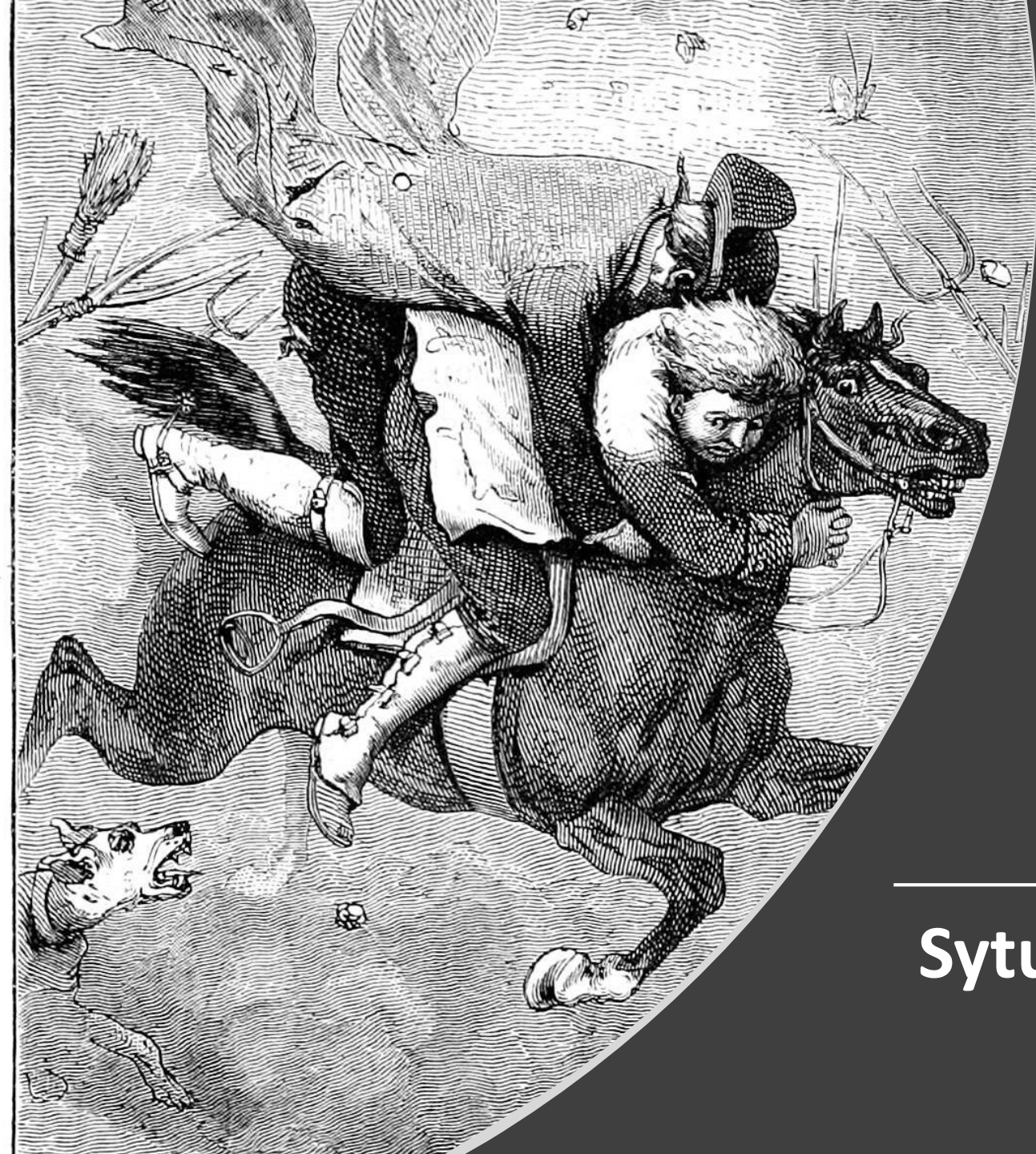
WYŚCIG ŚMIERCI

W APLIKACJACH WEBOWYCH

□ Zanim zaczniemy...

- Adrian `Vizzdoom` Michalczyk
 - starszy inżynier ds. bezpieczeństwa IT
 -  Future Processing
 - 10-letnie doświadczenie w branży
 - <http://adrian.michalczyk.website/about-me>
- prezentacja i kody źródłowe online:
<https://github.com/vizzdoom/infosec-coffee>





RACE CONDITIONS

Sytuacja wyścigu/hazard danych

Chciałbym zamówić X



Rozumiem, jedną chwilkę
(sprawdź stan magazynowy)

To kosztuje Y zł



Płacę
(czy mam tyle pieniędzy na koncie)?



Przygotowuję zamówienie / Brak środków



klient -= wartość zamówienia zł
barman += wartość zamówienia zł



Chciałbym zamówić X



Rozumiem, jedną chwilkę
(sprawdź stan magazynowy)

To kosztuje Y zł



Płacę
(czy mam tyle pieniędzy na koncie)?

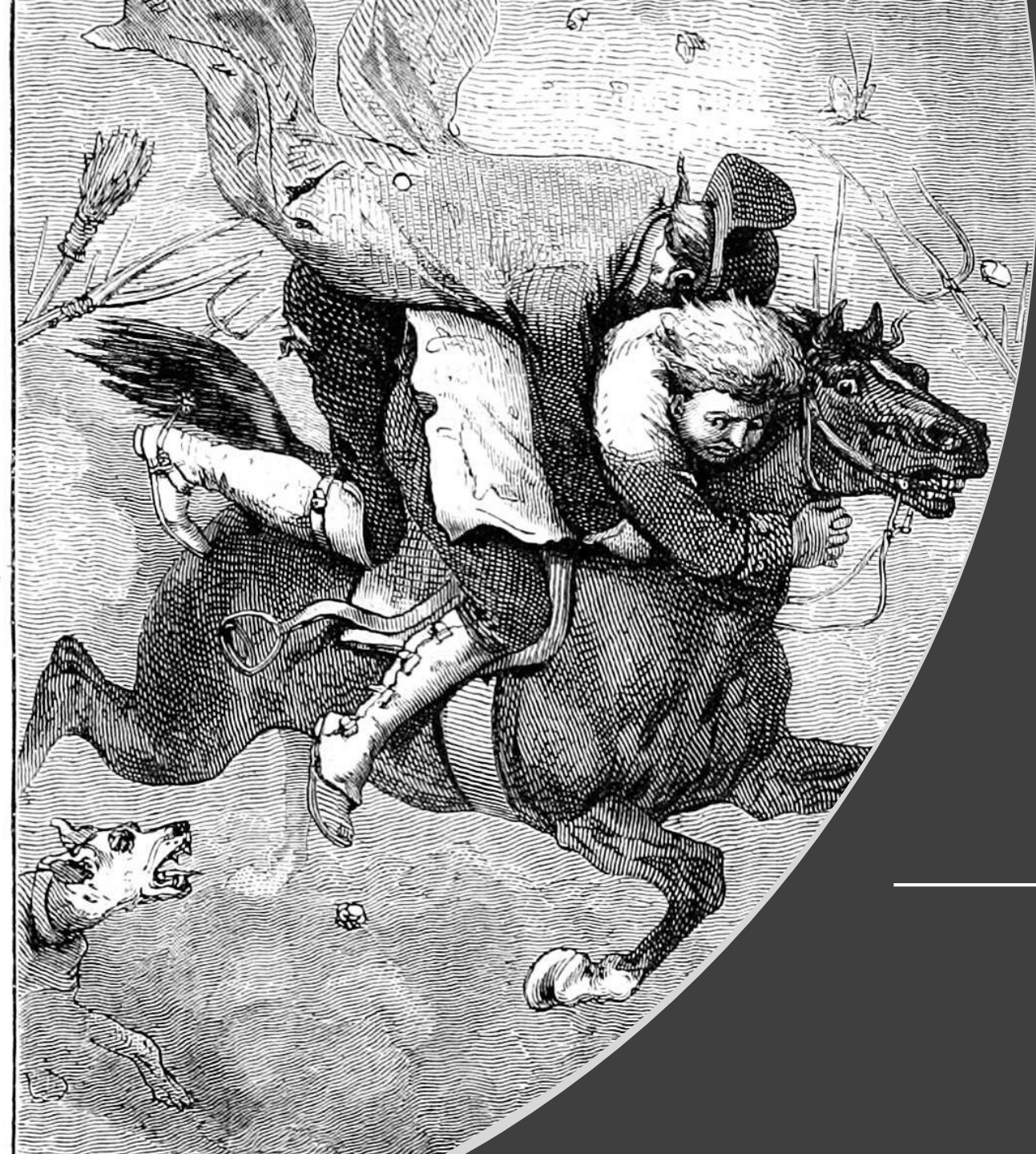


Przygotowuję zamówienie / Brak środków



Szybko! Jeszcze raz to samo!





DEMO

INFOSEC COFFEE



Jednym prostym trickiem znalazł sposób
na promocję swojego fanpage na Facebooku!

Marketingowcy go nienawidzą!



□ Race conditions – Facebook

1. Oceń stronę na 5 gwiazdek i przechwyć żądanie HTTP do: `/ajax/pages/review/add`
2. Wyślij wiele żądań HTTP w najkrótszym możliwym czasie.
3. Liczba ocen zwiększy się (przykładowo o 5 nowych recenzji).
4. Odwiedź stronę raz jeszcze i przejdź do sekcji „All reviews”.
5. Usuń jedną ze swoich recenzji. Strona ma teraz 4 recenzje.
6. Możesz wystawić nową recenzję. Powtórz kroki 2-5.
7. Gratulacje! Masz teraz świetnie wypromowaną stronę!

<https://josipfranjkoVIC.blogspot.com/2015/04/race-conditions-on-facebook.html>



Race conditions – Slack

<https://hackerone.com/reports/165570>

Billing



You have **\$225** in credits!

Learn more in our [Guide to billing at Slack](#).

Overview

History

Settings

Contacts

Team Changes

Payment Methods



Go To

← August 2016

September 2016

Date	Item	Charges
2016-09-03	Survey completed	Credited \$100
2016-09-03	Survey completed	Credited \$100



Race conditions – Digital Ocean

<https://josipfranjkojic.blogspot.com/2015/04/race-conditions-on-facebook.html>



Billing

Manage Payments



Create Droplet

Balance & Usage

Droplets

\$230.00

\$0.00

Images

You have credit

SSH Keys

Billing

Support

DNS

Apps & API

Settings

Logout

Billing History

Date	Description	Amount
January 17, 2015	Promotional Credit from AdRoll Promo Q2 - 4/22/14!	-\$10.00
January 17, 2015	Promotional Credit from AdRoll Promo Q2 - 4/22/14!	-\$10.00
January 17, 2015	Promotional Credit from AdRoll Promo Q2 - 4/22/14!	-\$10.00

☐ Race conditions – Starbucks



<https://sakurity.com/blog/2015/05/21/starbucks.html>

#prepare transfer details in both sessions

```
curl starbucks/step1 -H "Cookie: session=s1"
```

```
--data "amount=1&from=wallet1&to=wallet2"
```

```
curl starbucks/step1 -H "Cookie: session=s2"
```

```
--data "amount=1&from=wallet1&to=wallet2"
```

#send \$1 simultaneously from wallet1 to wallet2

```
curl starbucks/step2?confirm
```

```
-H "Cookie:session=s1" &
```

```
curl starbucks/step2?confirm
```

```
-H "Cookie: session=s2" &
```


□ Nietransakcyjne przetwarzanie danych

```
account_1 = User::getAccount()
```

```
coupon = Coupon::getCoupon()
```

```
if (coupon.isActive())
```

```
    User::setWallet(+10zł)
```

```
    Coupon::setInactive()
```

DATABASE

dane lokalne

dane „prawdziwe”

□ Transakcyjność

- **A** – Atomicity (niepodzielność)
- **C** – Consistency (spójność)
- **I** – Isolation (izolacja)
- **D** – Durability (trwałość)



Atomicity (niepodzielność danych)

Zbiór logicznie powiązanych

ze sobą operacji

musi zostać wykonany w całości.

Albo wcale.



Isolation (izolacja danych)

Transakcje wykonywane
w tym samym czasie
i na tych samych danych
muszą być wykonywane
sekwencyjnie.

□ Transakcyjne przetwarzanie danych

DB::runTransaction(Us

CODE	ACTIVE	VALUE	USERID	ACCOUNT
CODE1000	0	1000	UID 1	2499
CODE2000	1	2000	UID 2	1999
CODE3000	1	3000	UID 3	999
CODE4000	1	4000	UID 4	499



dane lokalne

dane „prawdziwe”

□ Jak testować hazard danych?

- blackbox > whitebox

□ Jak testować hazard danych?

- blackbox > whitebox

```
$conn = new PDO(DB_CONNECTION_STRING, DB_USERNAME, DB_PASSWORD);  
$q = $conn->prepare("UPDATE `users` SET `wallet` = :newWallet");  
$q->bindParam(":newWallet", $newWallet);  
$q->execute();
```

□ Jak testować hazard danych?

- blackbox > whitebox
- najpierw musisz mocno obciążyć system
- localhost != staging != live
- testuj szybko i równolegle



DZIĘKUJĘ ZA UWAGĘ

<https://github.com/vizzdoom/infosec-coffee>
<http://adrian.michalczyk.website/contact-me>