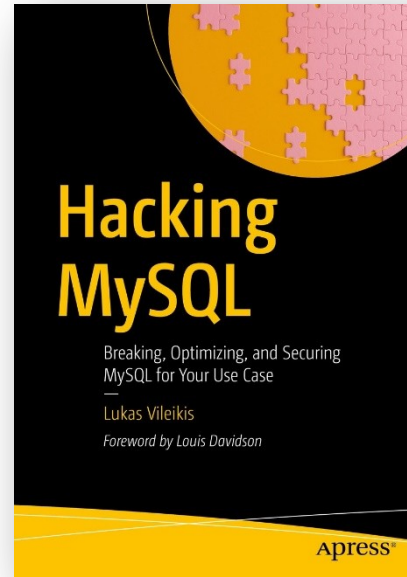


How I Broke MySQL

And Wrote a Book About It



FOSDEM 2025

Lukas Vileikis

lukasvileikis.com
BreachDirectory.com

whoami

- **Author** @ "Hacking MySQL", Apress
- **Content** @ Severalnines, Arctype, DbVisualizer, Redgate
- **Speaker** @ Percona LIVE, defCamp, Build Stuff...
- **Founder** @ BreachDirectory.com (DBSE)

Why listen to me?

Hacking MySQL {

Breaking: BUG #104263 ("@" sign)

Optimizing: DBSE* Query Speed <= 0.1s!

Securing: Data Breach Search Engine

}

*Data Breach Search Engine

lukasvileikis.com
BreachDirectory.com

Yet Another Book...

- **MySQL @** High Performance MySQL & etc.
- **Indexes @** Relational Database Index Design & the Optimizers
- **Design @** Database Design & Modeling
- ...



Hacking MySQL

Breaking, Optimizing, and Securing
MySQL for Your Use Case

—
Lukas Vileikis

Foreword by Louis Davidson

Apress®

lukasvileikis.com
BreachDirectory.com

“You don’t need to read books to break MySQL.”

How did we come to this?

- **What** are developers doing to the point that their databases break?
- **Where** did they mess up?
- **How** to fix that?

How did I come to this?

BreachDirectory.com

Does Somebody Have Your Password?

We're archiving **9,401,476,750** records from **521** data breaches.

The data breach database was last updated at 2024/10/08 23:00 GMT. See [recently added data breaches](#)

So far, the search engine has helped protect **22,760,403** people from identity theft. [It helped me too!](#)

Follow @breachdirectory

When compromised data includes [\(Expand/Collapse\)](#):

Email

Username

IP Address

Website Domain

Website Title

🔍 Enter Your Query Here...

® _ *

Search >

I want to be notified when my email address is found in a data breach in the future. We may also notify you monthly about what's happening in the cyberspace. For us to be able to notify you, your input will be recorded.

! Your account is at risk of identity theft!

Your account was found in the *000webhost* data breach.

lukasvileikis.com
BreachDirectory.com

Data Breach Search Engine BreachDirectory.com

- **Billions** of rows (data breach data)
- **Search** functionality(-ies)

Does Somebody Have Your **Password?**

We're archiving **9,401,476,750** records from **521** data breaches.
The data breach database was last updated at 2024/10/08 23:00 GMT. See recently added data breaches
So far, the search engine has helped protect **22,760,403** people from identity theft. [It helped me too!](#)

[Follow @breachdirectory](#)

When compromised data includes [\(Expand/Collapse\)](#):

Email Username IP Address Website Domain Website Title

I want to be notified when my email address is found in a data breach in the future. We may also notify you monthly about what's happening in the cyberspace. For us to be able to notify you, your input will be recorded.

! Your account is at risk of identity theft!
Your account was found in the *000webhost* data breach.

lukasvileikis.com
BreachDirectory.com

Full-Text Search (FTS)

How did *that* happen?

1. SELECT * FROM `demo` WHERE MATCH(`column`)
AGAINST("demo");
2. SELECT * FROM `demo` WHERE MATCH(`column`)
AGAINST(' "demo@demo.com" ' [IN BOOLEAN MODE]);

How did *that* happen?

1) 0.01s

2) ???

Old versions at fault?

The @ char full text anomaly



From [Charles Bell](#) on 2021-07-09 18:00

 [Details](#)  [Headers](#)  [Plain text](#)

Hi,

I haven't given up, but I've reached an impasse trying to recreate the issue. Everything works perfectly under MySQL 8.0.23 and the @ character weirdness isn't there (both queries execute in < 3 secs), but I crash the server trying to create the full text index in 5.7.33.

I filed a bug for this. Once this is resolved or I get a workaround, I'll try again. See [BUG#104263](#).

Chuck

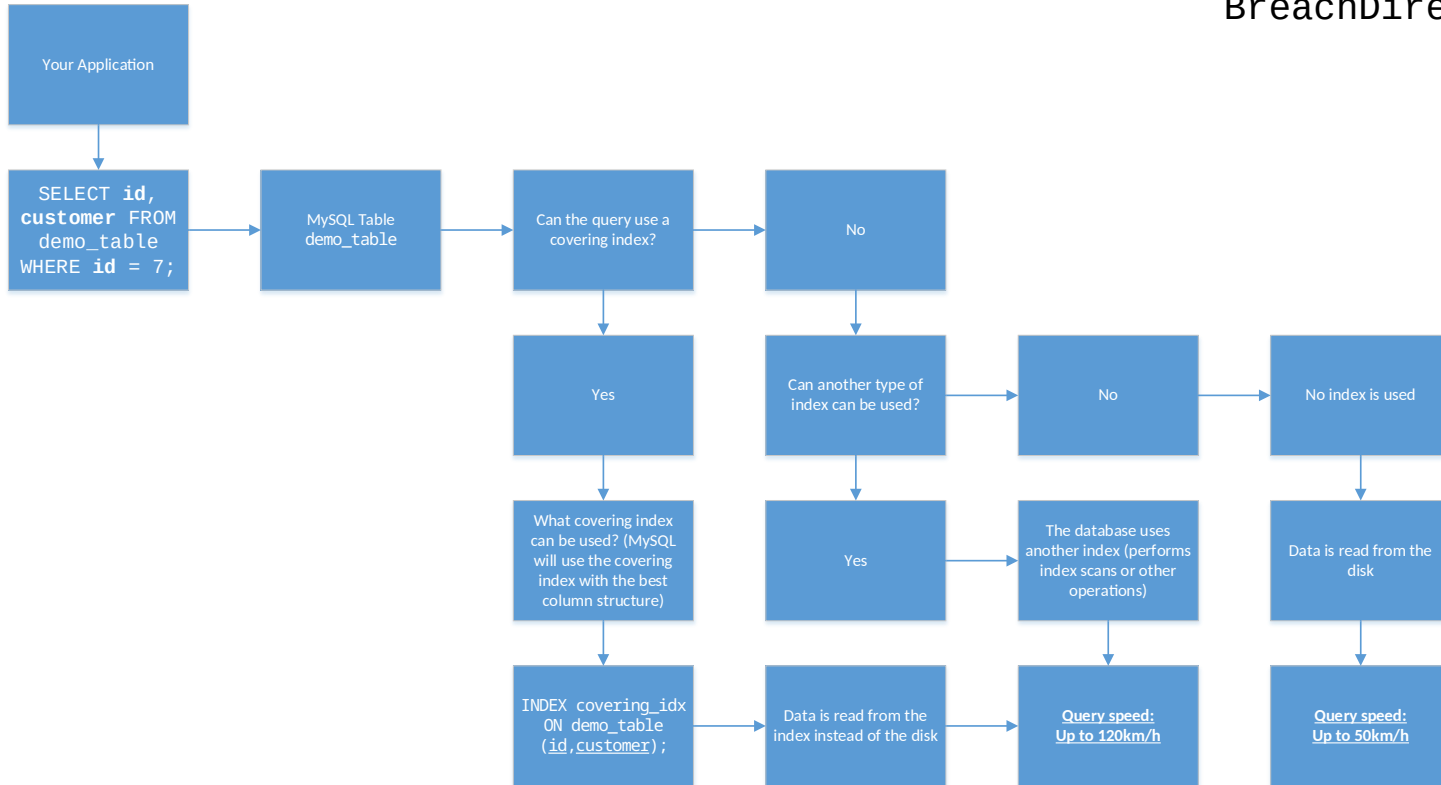
BUG#104263.

No @ signs for MySQL <= 5.7.**

Not the only thing!

Indexing

lukasvileikis.com
BreachDirectory.com



Use Cases => Problems

BreachDirectory.com

Does Somebody Have Your Password?

We're archiving **9,502,102,410** records from **521** data breaches.
The data breach database was last updated at 2024/10/08 23:00 GMT. See recently added data breaches
So far, the search engine has helped protect **22,760,403** people from identity theft. [It helped me too!](#)

Follow @breachdirectory

When compromised data includes [\(Expand/Collapse\)](#):

Email

Username

IP Address

Website Domain

Website Title

Q Enter Your Query Here...

®

*

Search

>



I want to be notified when my email address is found in a data breach in the future. We may also notify you monthly about what's happening in the cyberspace.
For us to be able to notify you, your input will be recorded.

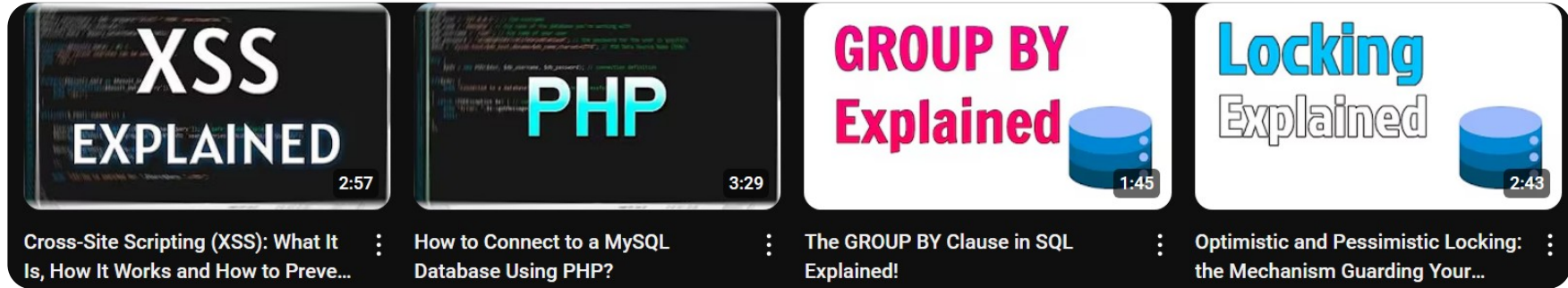
! Your account is at risk of identity theft!

Your account was found in the *000webhost* data breach.

If you've searched for a website title or a domain, this means that the data from this website has been compromised.

Problems => Solutions

YouTube.com/@DatabaseDive

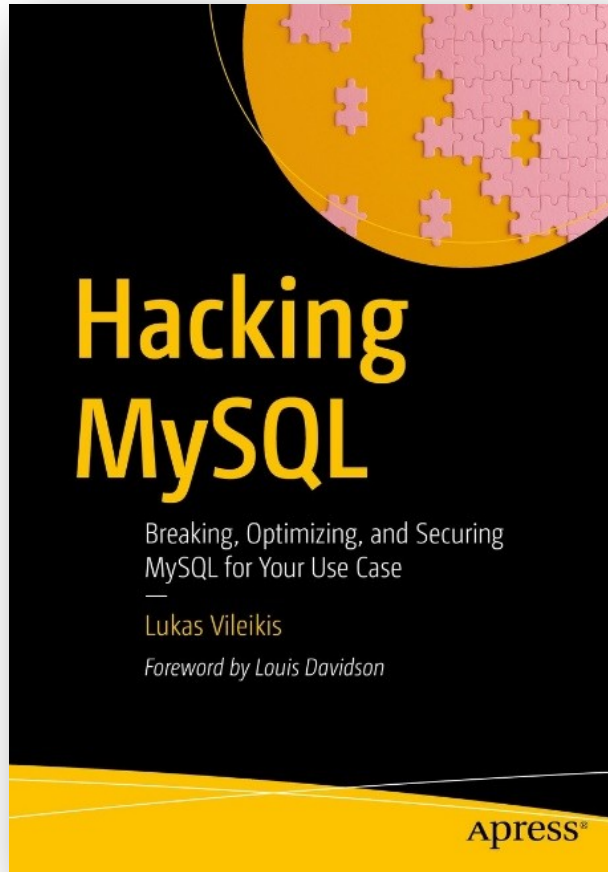


Solutions -> Outcomes

- ~30,000,000 Searches Made
 - The basics rock!
 - You can index and partition... apparently 😊
 - Schrödinger's tables
 - ???
- Use Cases
 - OSINT
 - Terrorism Prevention
 - Personal Use Cases
 - ???

Outcomes => Book

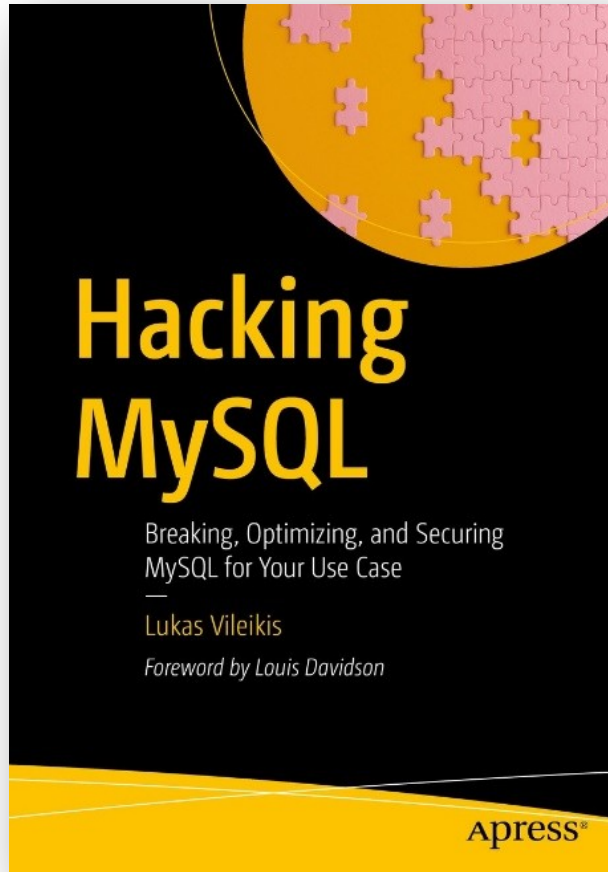
HackingMySQL.com



lukasvileikis.com
BreachDirectory.com

Not without mistakes

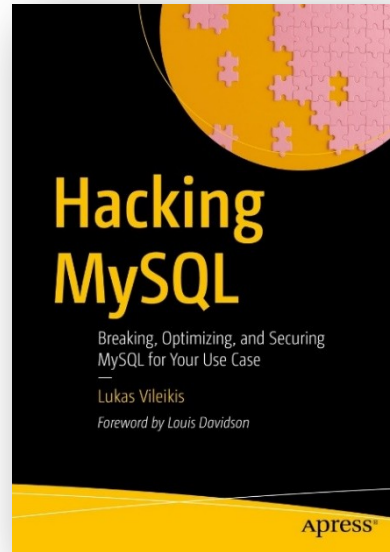
HackingMySQL.com



lukasvileikis.com
BreachDirectory.com

See You @ the Book Signing!

- [BreachDirectory.com](https://breachdirectory.com)
- [HackingMySQL.com](https://hackingmysql.com)
- lukas@lukasvileikis.com



lukasvileikis.com
[BreachDirectory.com](https://breachdirectory.com)

FOSDEM 2025

Thank You!

Lukas Vileikis

lukasvileikis.com

lukas@lukasvileikis.com

BreachDirectory.com