‘create table user;’ Considered Harmful

Dan Moore
CodeMash 2022
Jan 13, 2021

Imagine Yourself…

Imagine Yourself…

- About to ship your product when the PM comes up and says

Imagine Yourself…

- About to ship your product when the PM comes up and says
- “We need to support verifying people’s email”

Imagine Yourself…

- About to ship your product when the PM comes up and says
- “We need to support verifying people’s email”
- You get to work, and build it

WHO'S AWESOME?
YOU'RE AWESOME
quickmeme.com

Now Imagine

Now Imagine

- And then, just before you’re about to ship again, the PM comes up and says

Now Imagine

- And then, just before you’re about to ship again, the PM comes up and says
- “We need to make sure our passwords conform to NIST publication 800-63B”

Now Imagine

- And then, just before you’re about to ship again, the PM comes up and says
- “We need to make sure our passwords conform to NIST publication 800-63B”
- And you get to work and build it

YOU'RE AWESOME
2009
AND YOU'RE AWESOME
AND YOU'RE AWESOME
YOU'RE ALL AWESOME

And Then

- Just before you’re about to ship, the PM comes up and…

And Then

- Just before you’re about to ship, the PM comes up and…
- You get the idea.

This Is a Problem

And an
Auth Server
Can Help

What I’ll Cover

- What is auth
- Options for auth
- Reasons to outsource
- Evaluation criteria

About FusionAuth

- FusionAuth is the authentication and authorization platform built for developers, by developers.
- FusionAuth solves the problem of building essential user security without adding risk or distracting from the primary application.

There Are Others

About Me

About Me

- Who cares

Questions

- Just ask
  - Please wave your hand

Poll: How many applications does your company have?

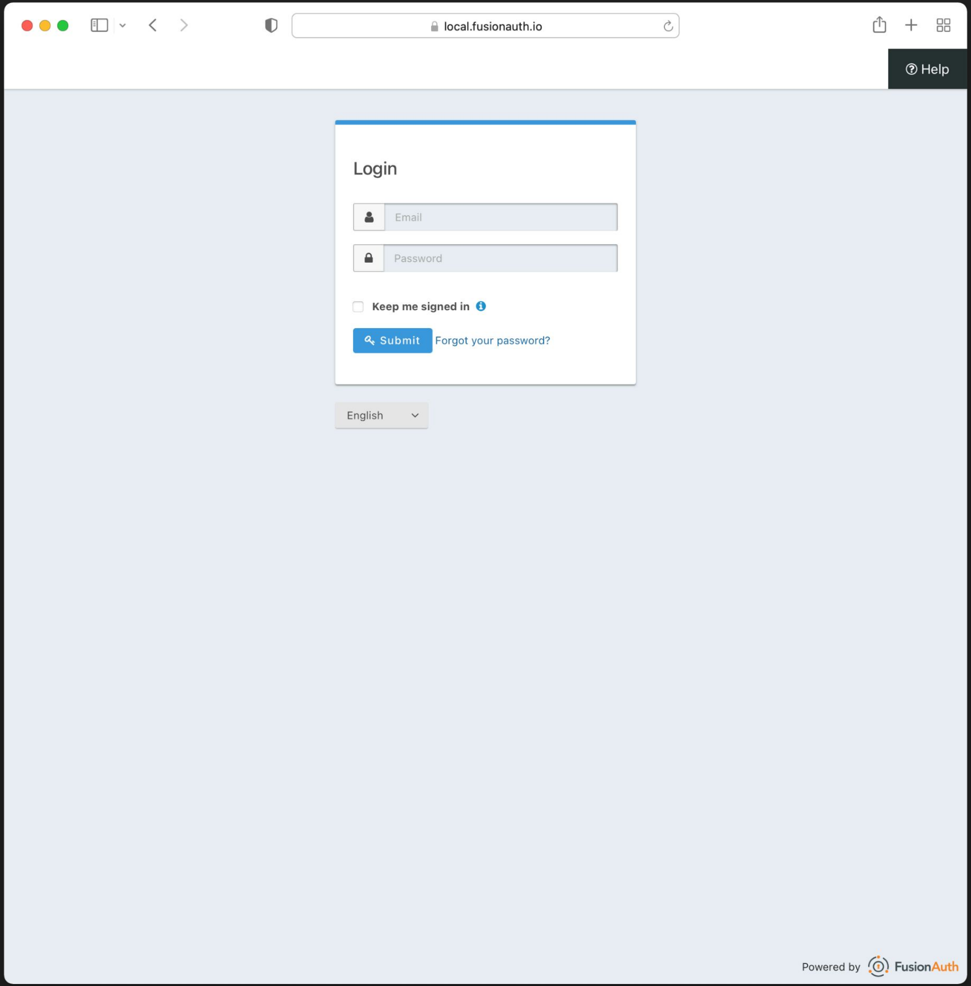
What is Auth

What is Auth

- Portmanteau of authentication and authorization

What is Authentication

- Who you are



local.fusionauth.io

Help

Login

Email

Password

□ Keep me signed in

Submit Forgot your password?

English

Powered by FusionAuth

@mooreds

FusionAuth

What is Authentication

- Many ways to do this

What is Authentication

- Many ways to do this
  - Called ‘factors of authentication’

What is Authentication

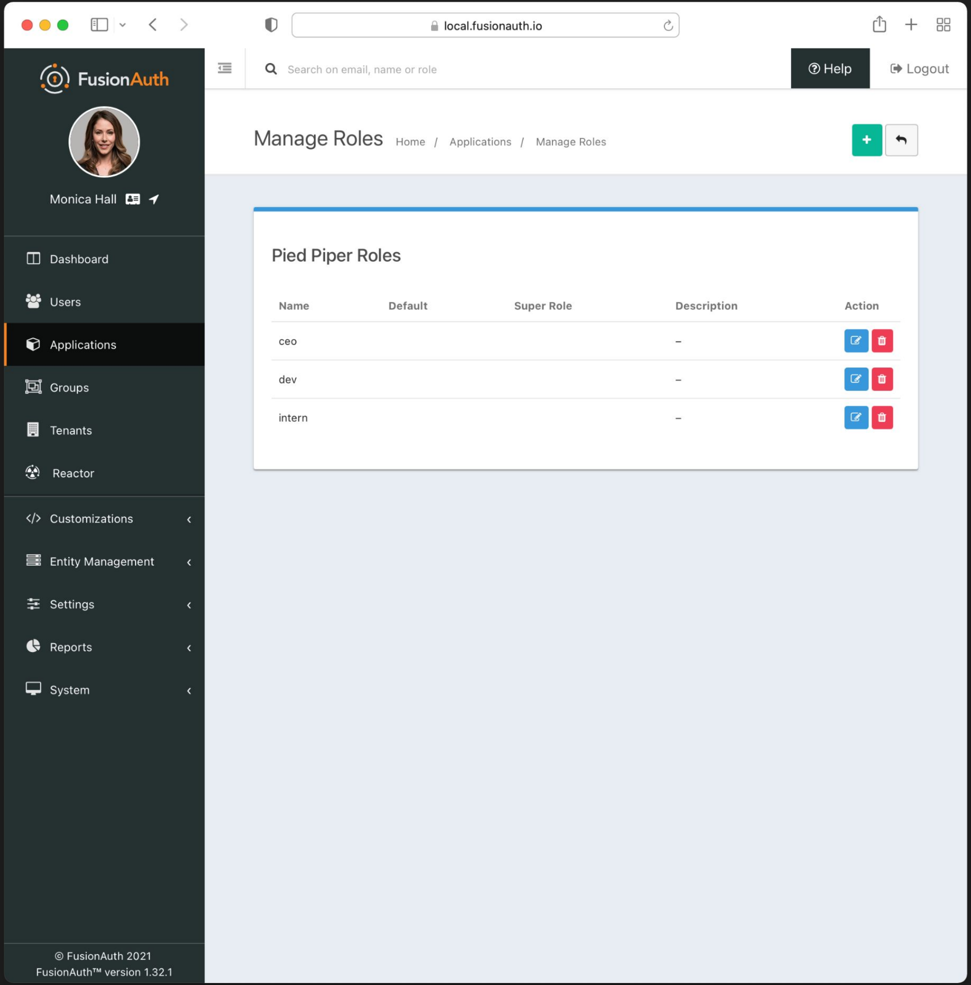
- Many ways to do this
  - Called ‘factors of authentication’
- All trying to ascertain you are who you say you are

What is Authentication

- Many ways to do this
  - Called ‘factors of authentication’
- All trying to ascertain you are who you say you are
- Common attributes

What is Authorization

- What you can do



Manage Roles

Pied Piper Roles

Name	Default	Super Role	Description	Action
ceo			–	
dev			–	
intern			–	

@mooreds

FusionAuth

What is Authorization

- Business specific

What is Authorization

- Business specific
- Efforts like OPA try to make it more generic
  - https://www.openpolicyagent.org/

One More Thing

- User management

One More Thing

- User management
  - CRUDL for users and their attributes

Questions?

Auth Options

Don’t Use Auth At All

Don’t Use Auth At All

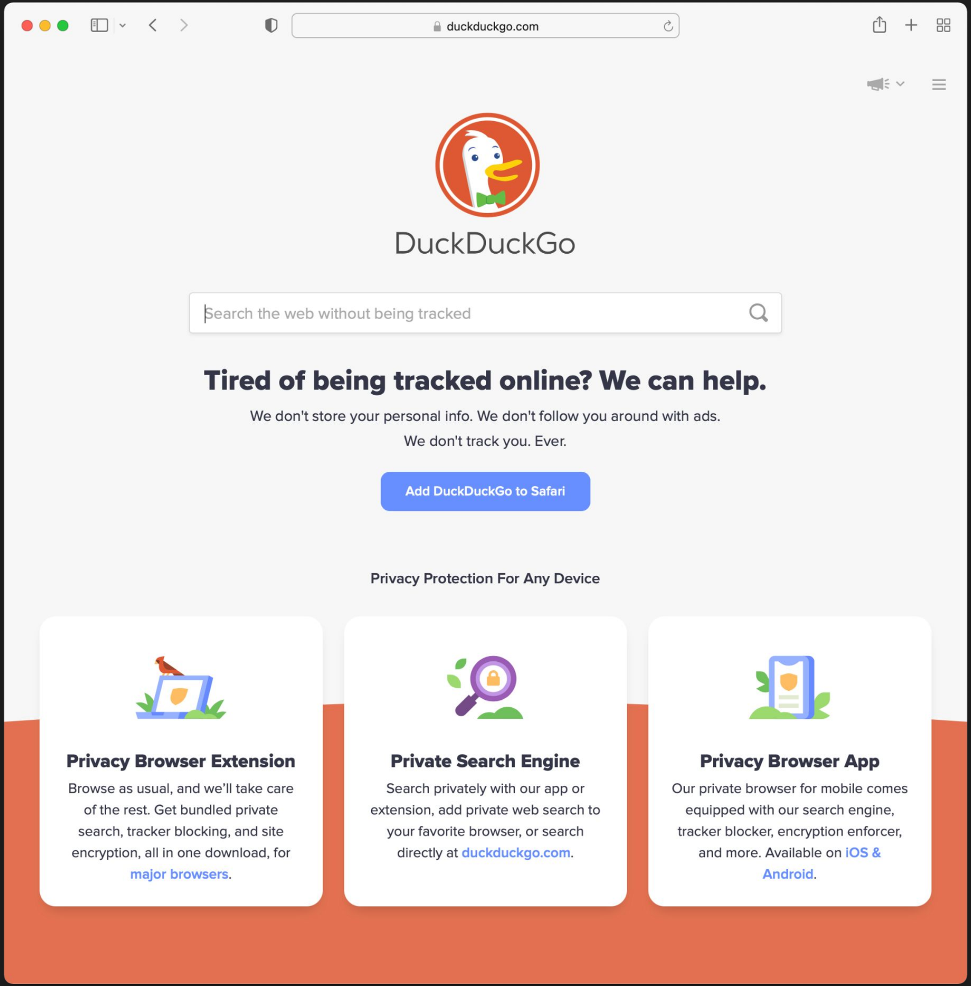
- Online directories

Don’t Use Auth At All

- Online directories
- Public websites

Don’t Use Auth At All

- Online directories
- Public websites
- No concept of a user



DuckDuckGo

Search the web without being tracked

Tired of being tracked online? We can help.

We don't store your personal info. We don't follow you around with ads.
We don't track you. Ever.

Add DuckDuckGo to Safari

Privacy Protection For Any Device

Privacy Browser Extension

Browse as usual, and we'll take care of the rest. Get bundled private search, tracker blocking, and site encryption, all in one download, for major browsers.

Private Search Engine

Search privately with our app or extension, add private web search to your favorite browser, or search directly at duckduckgo.com.

Privacy Browser App

Our private browser for mobile comes equipped with our search engine, tracker blocker, encryption enforcer, and more. Available on iOS & Android.

@mooreds

FusionAuth

Roll Your Own

```
CREATE TABLE user (
  id INT NOT NULL,
  email VARCHAR(40) NOT NULL,
  password CHAR(40) NOT NULL,
  PRIMARY KEY (id)
);
```

Roll Your Own

- But what about

Roll Your Own

- But what about
  - Secure hashing

Roll Your Own

- But what about
    - Secure hashing
    - Forgot password

Roll Your Own

- But what about
  - Secure hashing
  - Forgot password
  - Social login

Roll Your Own

- But what about
  - Secure hashing
  - Forgot password
  - Social login
  - MFA

Roll Your Own

- But what about
  - Secure hashing
  - Forgot password
  - Social login
  - MFA
  - GDPR/CCPA

Roll Your Own

- But what about
  - Secure hashing
  - Forgot password
  - Social login
  - MFA
  - GDPR/CCPA
  - SAML/SSO

Roll Your Own

- But what about
    - Secure hashing
    - Forgot password
    - Social login
    - MFA
    - GDPR/CCPA
    - SAML/SSO
    - ...

OH MAN !
THAT'S BAD !
memeshappen.com

Building Auth Yourself

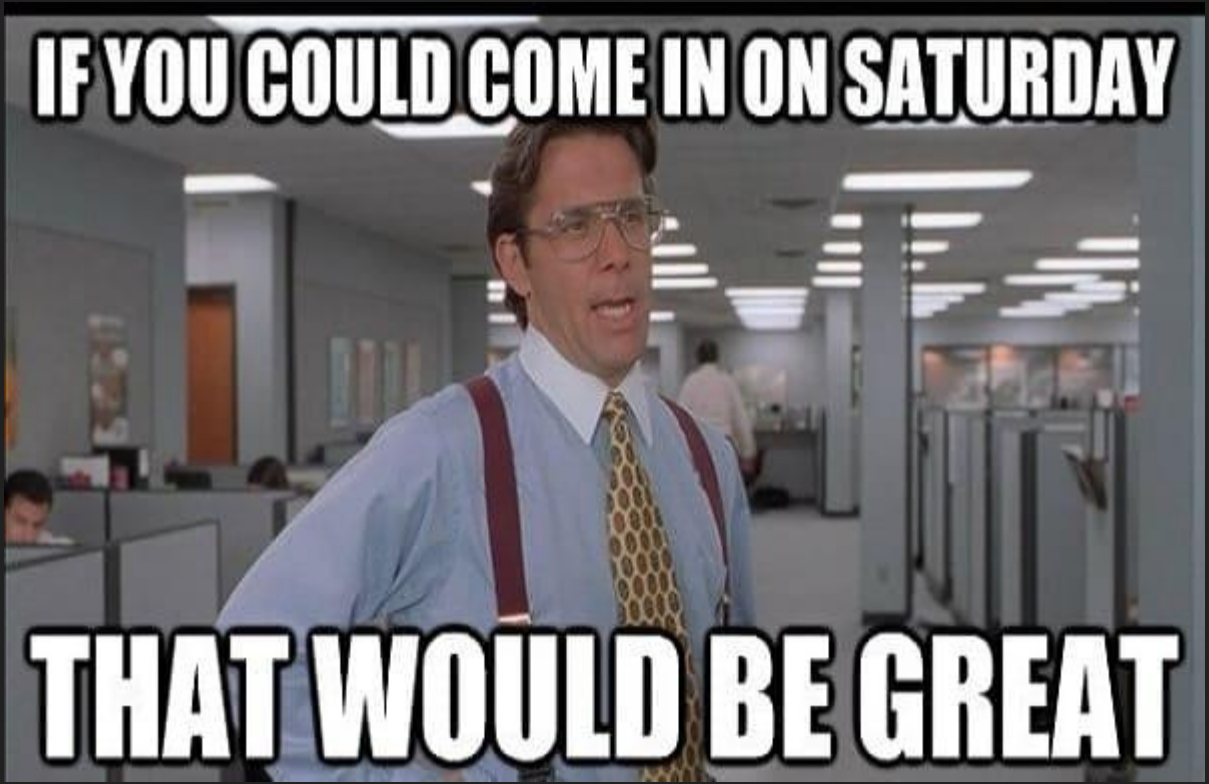
- Not impossible but not easy

Building Auth Yourself

- Not impossible but not easy
- Necessary but not sufficient for your application

Building Auth Yourself

- Not impossible but not easy
- Necessary but not sufficient for your application
- Not differentiated work, but still effort


IF YOU COULD COME IN ON SATURDAY
THAT WOULD BE GREAT

Would You Build Your Own Database?

Better Options

- Use a library (OSS, framework)
- Outsource to dedicated server

Library

- Available for different languages
  - Gems like devise for rails

Library

- Available for different languages
    - Gems like devise for rails
    - ASP.NET authentication and authorization support like [Authorize] filter

Library

- Available for different languages
  - Gems like devise for rails
  - ASP.NET authentication and authorization support like [Authorize] filter
  - Spring security

Library

- Available for different languages
  - Gems like devise for rails
  - ASP.NET authentication and authorization support like [Authorize] filter
  - Spring security
- Simple to get started

Library

- Available for different languages
  - Gems like devise for rails
  - ASP.NET authentication and authorization support like [Authorize] filter
  - Spring security
- Simple to get started
- Simple operationally
  - Just deploy the application

Great for One Application

THERE CAN BE
ONLY ONE
memegenerator.net

But Who Has Only One Application?

Another Option

Outsourced Auth Server

- Independent application
    - Similar to a database server

Outsourced Auth Server

- Independent application
- Specialization
  - Features
  - Security
  - Like a team of extra devs

Outsourced Auth Server

- Independent application
- Specialization
- Single view of the user
    - Across applications
    - Metrics
    - Onboarding/offboarding
    - Better for the end user

Outsourced Auth Server

- Independent application
- Specialization
- Single view of the user
- Standards based
  - Avoid lock-in … sort of
  - Edge cases
  - Experts

Outsourced Auth Server

- Independent application
- Specialization
- Single view of the user
- Standards based
- Increased security
    - Limit access
    - Monitor carefully
    - Reduce risk

Outsourced Auth Server

- Independent application
- Specialization
- Single view of the user
- Standards based
- Increased security
- Focus
  - Your team
  - Outsourced auth server provider

Why don't we have both?

Grow From Library to Outsourced Auth Server

- When?
  - You have multiple applications
  - You need the data isolation
  - You want the separation from your main application
  - Different availability requirements

Grow From Library to Outsourced Auth Server

- When?
  - You have multiple applications
  - You need the data isolation
  - You want the separation from your main application
  - Different availability requirements
- Prepare by using standards where possible

Grow From Library to Outsourced Auth Server

- When?
  - You have multiple applications
  - You need the data isolation
  - You want the separation from your main application
  - Different availability requirements
- Prepare by using standards where possible
- Easier if you do it right at first
  - Architectural investment you may want to make

CHOICES
makeameme.org

Questions?

So You Want to Outsource Your Auth

Let’s Talk About Criteria

Self-hosted or SaaS

- Operational complexity
- Team skills/bandwidth
- Focus
- If self-hosted, OS/container compatibility
- Network compliance requirements

Regulations

- Data residency
- Regulatory compliance
  - SOC2
  - PCI
  - HIPAA
  - GDPR
  - FedRAMP

Auth Functionality

- Authentication
- Authorization
- User management
- Or some combination of these

Standards Support

- OAuth grants
- Other identity standards
- Other standards

Integrations

- APIs
- Look and feel
- Webhooks
- Extension points
- Custom login flows
- SDKs
- l10n/i18n

Security Features

- Auditability
- Logging
- Secrets compatibility
- Security specific features
  - New device notifications
  - Rate limiting

Provider Due Diligence

- Certifications achieved
- Transparency
- Notification
- Bug bounty
- Pen testing
- Availability

Feature Set

- 3 Categories
  - Basic
  - Unique
  - Nice to have
- POC
- Roadmap

Migration Factors

- Matching concepts
- Password hashes
- Custom hashing

Release Cadence

- How often
- What size
- What do upgrades look like
  - Can you avoid?
- Transparency

Open Source or Commercial

- OSS
  - What type
  - Who is driving project
  - Bugfix responsiveness
- Commercial
  - Source code escrow

Support Options

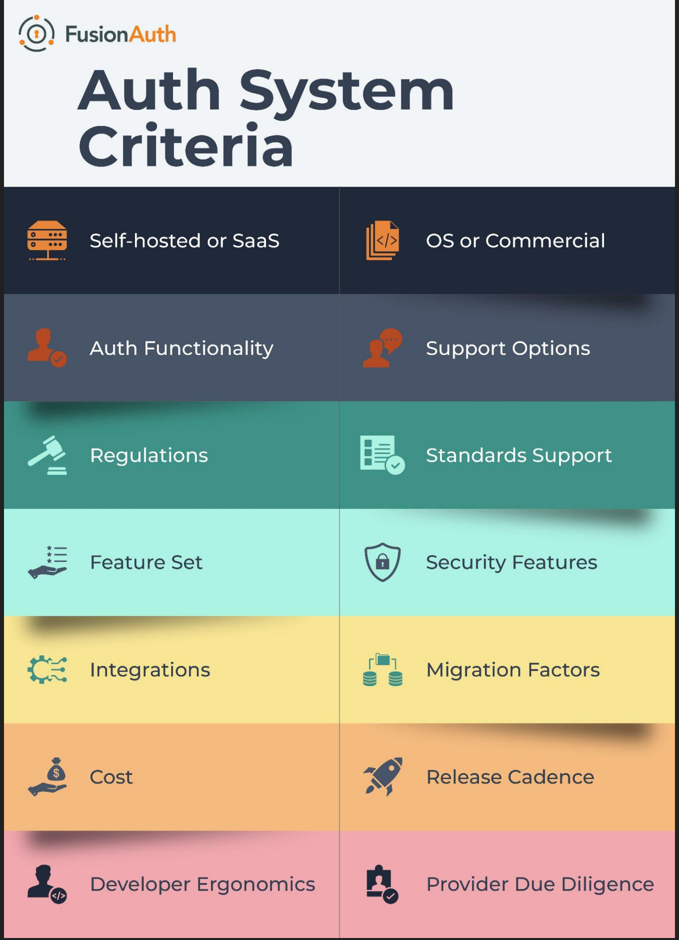
- Community size
- Professional support options
- Ecosystem
  - Integration partners
  - Consulting partners

Developer Ergonomics

- API mouthfeel
- Documentation
- CI/CD friendliness
- Free tier

Cost

- Dollars
- Hours
- Business risk



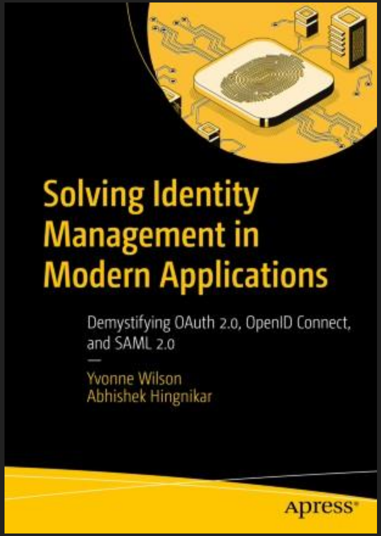
FusionAuth

Auth System Criteria

- Self-hosted or SaaS
- OS or Commercial
- Auth Functionality
- Support Options
- Regulations
- Standards Support
- Feature Set
- Security Features
- Integrations
- Migration Factors
- Cost
- Release Cadence
- Developer Ergonomics
- Provider Due Diligence

Additional Resources

- https://fusionauth.io/learn/expert-advice/identity-basics/
- https://idpro.org/body-of-knowledge/
- Solving Identity Management in Modern Applications



Solving Identity Management in Modern Applications

Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0

Yvonne Wilson
Abhishek Hingnikar

Apress

Thanks and More

- Mobile app feedback!
- Contact
  - Our booth
  - fusionauth.io/ult-auth-ebook/
  - dan@fusionauth.io
  - FusionAuth.io
  - @mooreds

FusionAuth

The Ultimate Guide to Outsourcing Your Auth