passbolt

Open source
password manager
for teams

Throwback from the past

Passbolt team at Fosdem in 2017

Who is using a password manager?

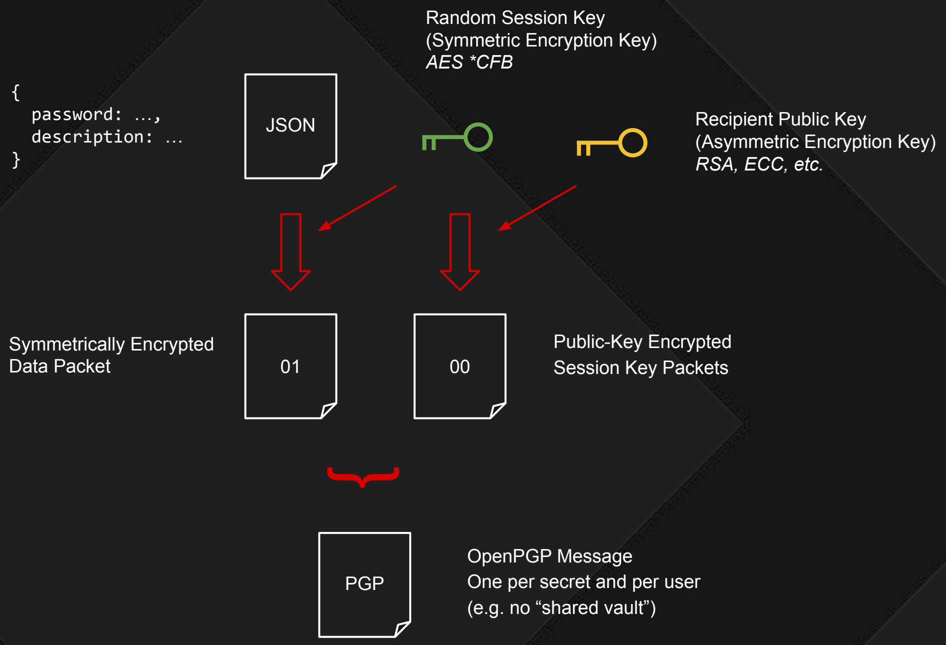
Wait another password manager?

or how is passbolt different from...

Based on OpenPGP and public key cryptography.

Standing on OpenPGP.js, GopenPGP & Gnupg shoulders

- + No “master key” derived from the user password using PBKDF2 (*warden, Lastpass), or Argon2 (Keepass, Dashlane).
- + Encryption strength is not dependent on user password strength or number of derivation rounds.
- + Interoperability and support for new/future algorithms (Curve25519).
- - Harder for the end-user, they must not lose their private key nor their passphrase.
- - Similarly, requires complex key transfer protocols (e.g. QR codes)



```
{
  password: …,
  description: …
}
```

JSON

Random Session Key
(Symmetric Encryption Key)
*AES *CFB*

Recipient Public Key
(Asymmetric Encryption Key)
RSA, ECC, etc.

Symmetrically Encrypted
Data Packet

01

00

Public-Key Encrypted
Session Key Packets

PGP

OpenPGP Message
One per secret and per user
(e.g. no “shared vault”)

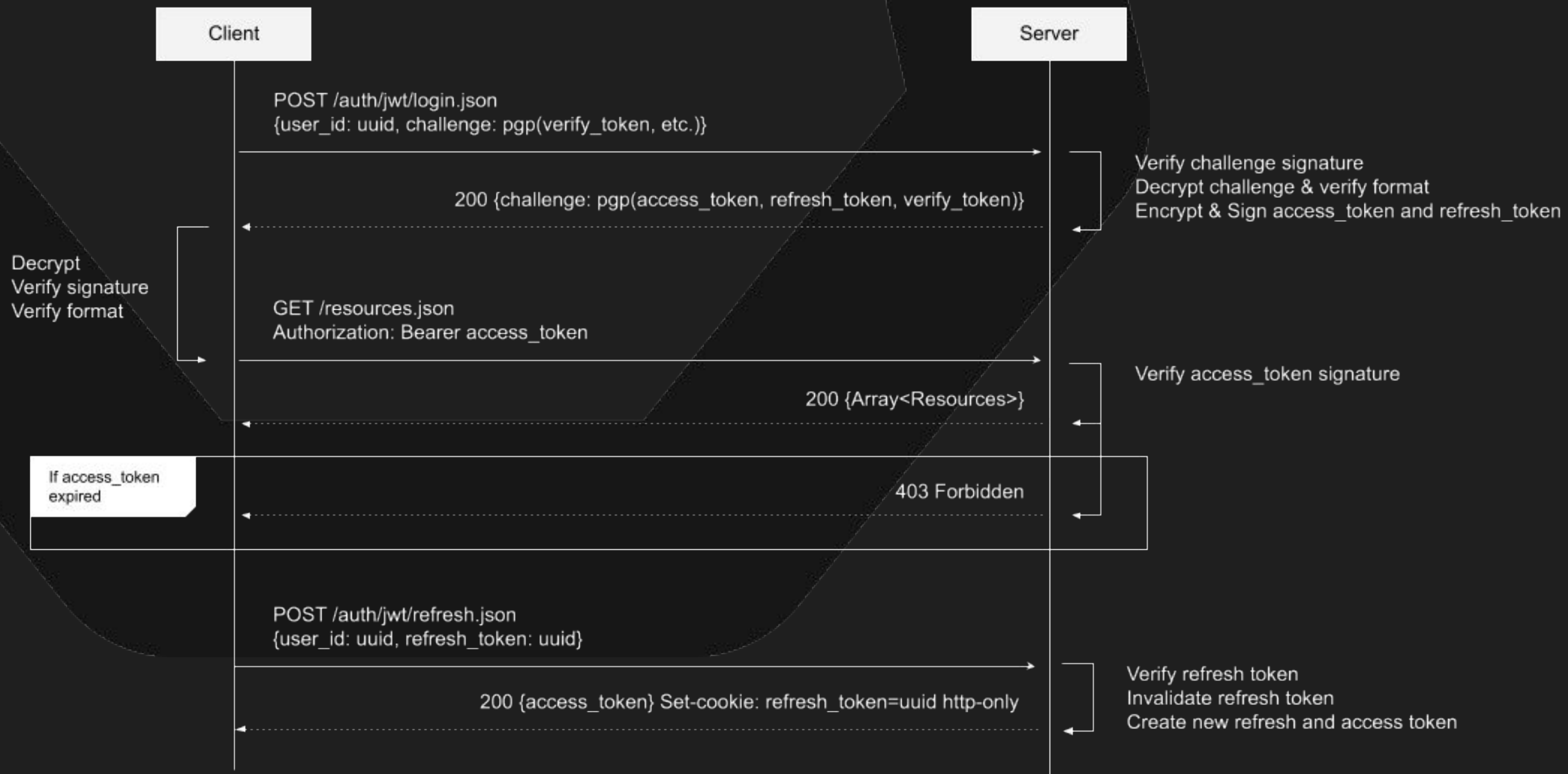
Signature + challenge authentication

Using gpgauth principles with a twist.

+ Not prone to credential stuffing.

+ Not prone to phishing.

- More complex to implement for developers. Not a standard (yet 😉)



Client

Server

POST /auth/jwt/login.json
{user_id: uuid, challenge: pgp(verify_token, etc.)}

Verify challenge signature
Decrypt challenge & verify format
Encrypt & Sign access_token and refresh_token

200 {challenge: pgp(access_token, refresh_token, verify_token)}

Decrypt
Verify signature
Verify format

GET /resources.json
Authorization: Bearer access_token

Verify access_token signature

200 {Array<Resources>}

If access_token expired

403 Forbidden

POST /auth/jwt/refresh.json
{user_id: uuid, refresh_token: uuid}

Verify refresh token
Invalidate refresh token
Create new refresh and access token

200 {access_token} Set-cookie: refresh_token=uuid http-only

Mandatory browser extension

JavaScript cryptography considered harmful? (the return)

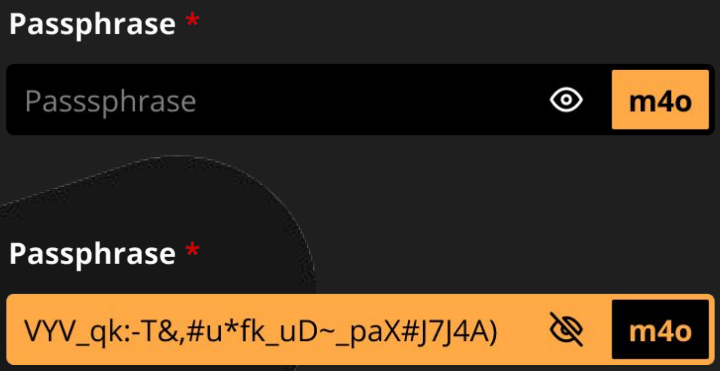
- + If server is compromised an attacker cannot add javascript to the login page to extract the master password (and secret key if any).
- + Using the background page sandbox allows to isolate decrypted private key (reduced XSS impact).
- + Automatic rollout of signed updates for all clients in case of cryptography issues.
- + Extension is tied to run only on a trusted domain. In an iframe.
- + Bonus: quick access / form integrations possible.

- - Not useful when attacker has read access on the client OS. (unlike keepass)
- - Need to trust firefox, etc. stores. Or build and host your own.
- - 3rd party websites can find out extension is installed.

Anti-phishing passphrase protection by default.

“Something” selected by the user only known by the client.

- + Protect every sensitive operations against phishing attacks.
- + Interactive, prevent an attacker to put “one more layer on top”.
- - The majority of users interviewed do not understand the concept of phishing in general.
- ~ More services are warming up to this (banks, competitors, etc.).



Passphrase *

Passsphrase

m4o

Passphrase *

VYV_qk:-T&,#u*fk_uD~_paX#J7J4A)

m4o

An anti-phishing token appears each time an end-user is prompted to enter their master password.

#Friends: Check out mailvelope for similar concepts in the field of email encryption.

Full transparency

Clear about both the strengths & the residual risks.

+ No opt-out telemetry / analytics. No “phoning home”.
+ 100% Open Source. No open core. Yes, even the “pro” offer.
+ Independent 3rd party audits at least once a quarter or for new large feature launches (cure53).
+ Annual SOC2 Type II audited report.
+ Financially stable.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

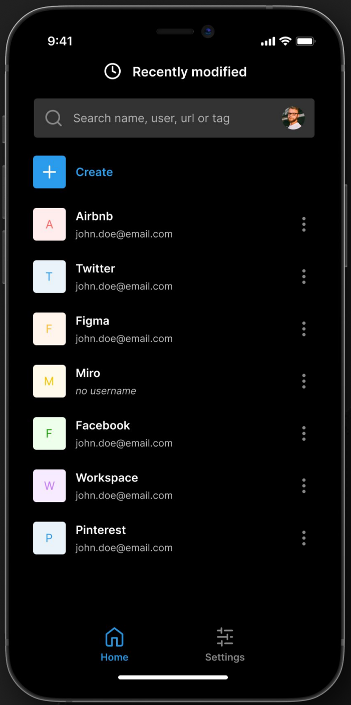
MADE IN LUXEMBOURG

- Server is trusted for public key distribution. No clear key signatures.
- Searchable API = unencrypted metadata.
- No quantum resistant algorithm available yet.
- Export feature is on by default.
- No clear indications when passwords should be rotated.
- No user key rotations
- **We’re only humans after all.**

How does it look like?

Available on most browsers and devices.

Safari support and desktop app coming in 2023



9:41

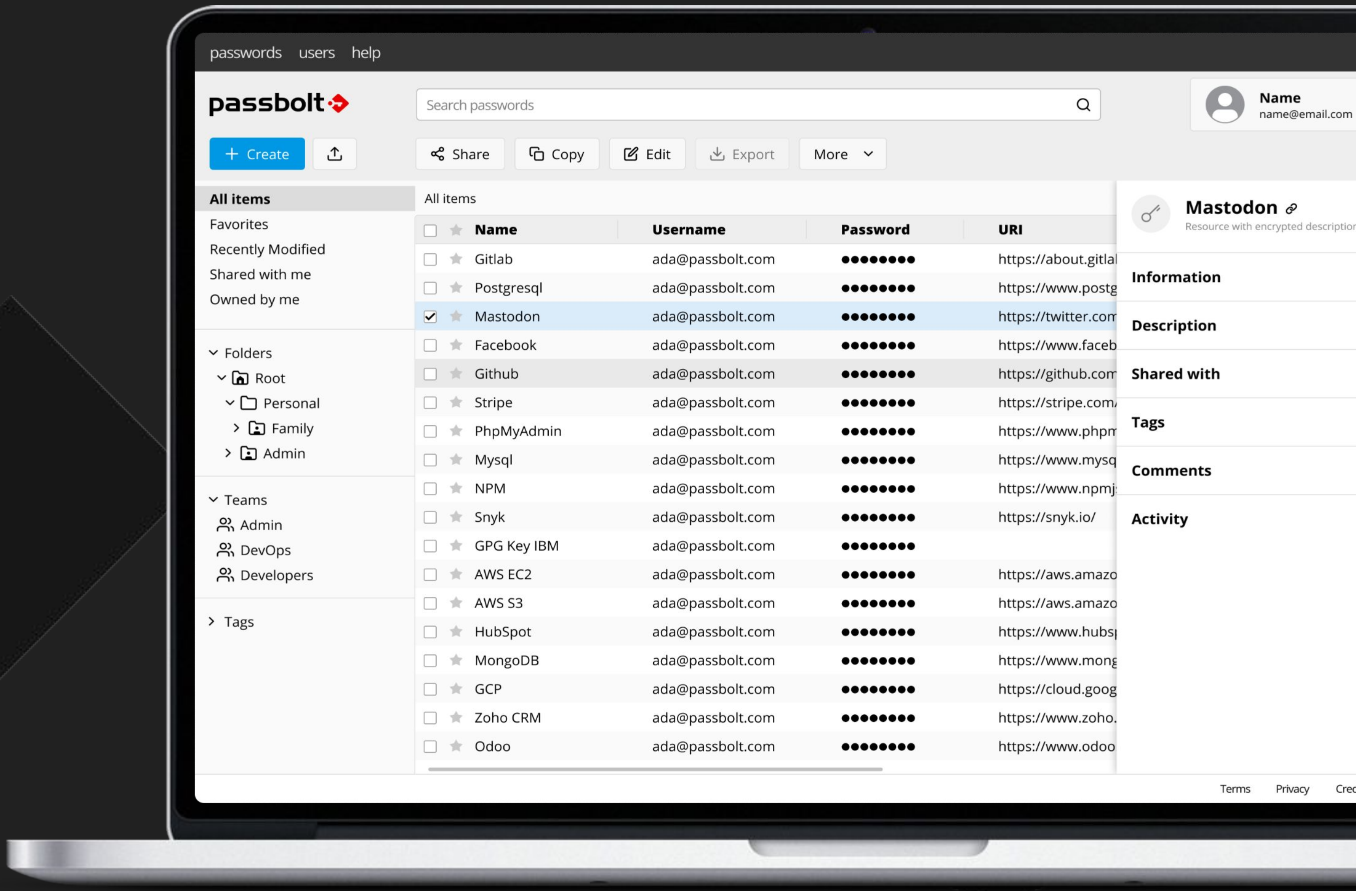
Recently modified

Search name, user, url or tag

Create

A	Airbnb john.doe@email.com
T	Twitter john.doe@email.com
F	Figma john.doe@email.com
M	Miro *no username*
F	Facebook john.doe@email.com
W	Workspace john.doe@email.com
P	Pinterest john.doe@email.com

Home Settings



passwords users help

passbolt

Search passwords

Name
name@email.com

Create | Share | Copy | Edit | Export | More

All items
Favorites
Recently Modified
Shared with me
Owned by me

Folders
- Root
  - Personal
    - Family
  - Admin

Teams
- Admin
- DevOps
- Developers

Tags

All items

□	★	Name	Username	Password	URI
□	★	Gitlab	ada@passbolt.com	●●●●●●●●	https://about.gitlal
□	★	Postgresql	ada@passbolt.com	●●●●●●●●	https://www.postg
☑	★	Mastodon	ada@passbolt.com	●●●●●●●●	https://twitter.com
□	★	Facebook	ada@passbolt.com	●●●●●●●●	https://www.faceb
□	★	Github	ada@passbolt.com	●●●●●●●●	https://github.com
□	★	Stripe	ada@passbolt.com	●●●●●●●●	https://stripe.com/
□	★	PhpMyAdmin	ada@passbolt.com	●●●●●●●●	https://www.phpm
□	★	Mysql	ada@passbolt.com	●●●●●●●●	https://www.mysq
□	★	NPM	ada@passbolt.com	●●●●●●●●	https://www.npmj
□	★	Snyk	ada@passbolt.com	●●●●●●●●	https://snyk.io/
□	★	GPG Key IBM	ada@passbolt.com	●●●●●●●●	
□	★	AWS EC2	ada@passbolt.com	●●●●●●●●	https://aws.amazo
□	★	AWS S3	ada@passbolt.com	●●●●●●●●	https://aws.amazo
□	★	HubSpot	ada@passbolt.com	●●●●●●●●	https://www.hubs
□	★	MongoDB	ada@passbolt.com	●●●●●●●●	https://www.mong
□	★	GCP	ada@passbolt.com	●●●●●●●●	https://cloud.goog
□	★	Zoho CRM	ada@passbolt.com	●●●●●●●●	https://www.zoho.
□	★	Odoo	ada@passbolt.com	●●●●●●●●	https://www.odoo

Mastodon
Resource with encrypted descriptio

Information

Description

Shared with

Tags

Comments

Activity

Terms Privacy Cre

and most terminals.

Via official or community maintained CLIs, libraries, etc. or just Curl and Gpg

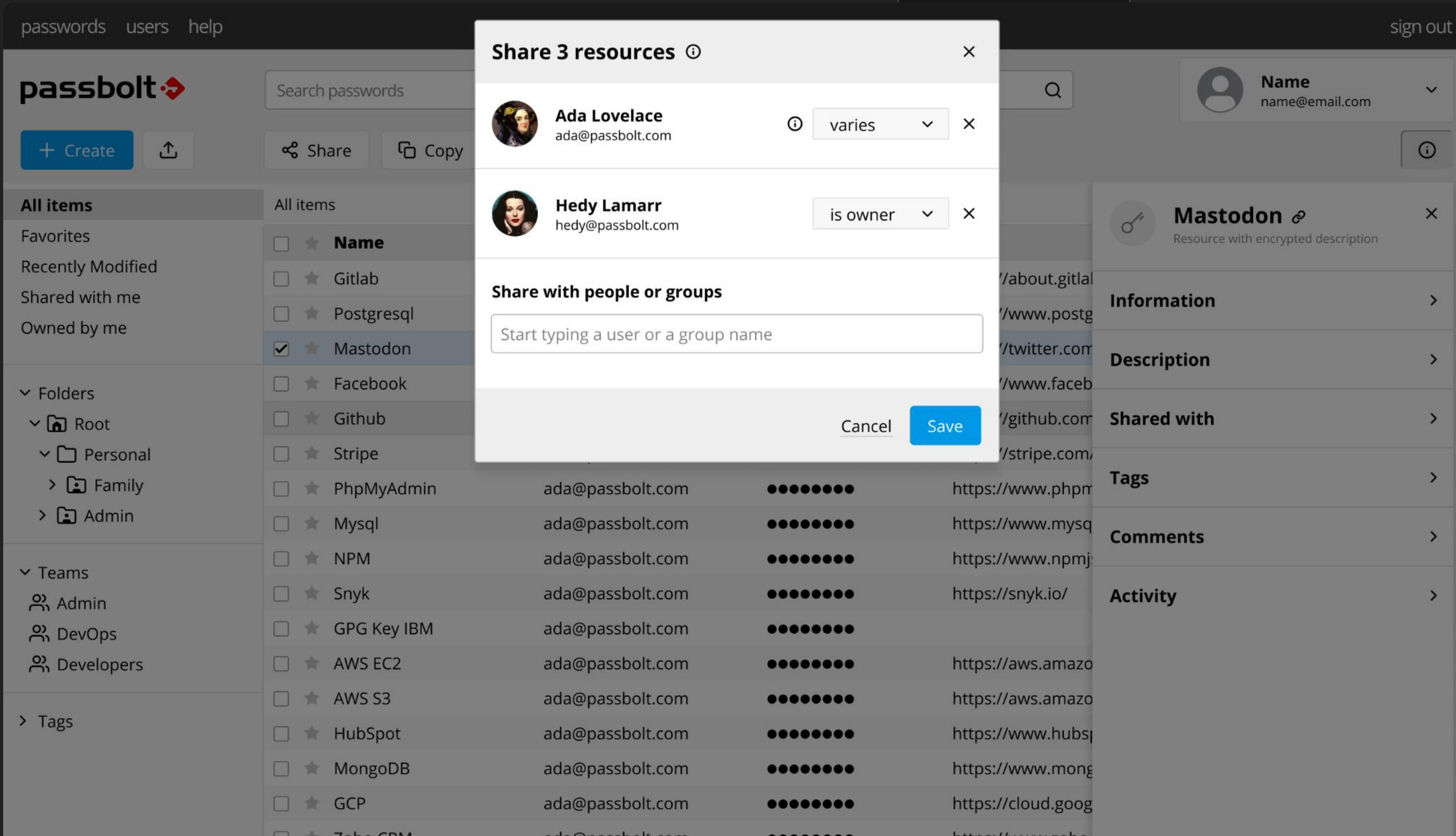
```
$> passbolt get 664735b2-4be7-36d9-a9f8-08d42998faf8
-----BEGIN PGP MESSAGE-----


$> passbolt get \
   $(passbolt find  | awk '/server/ { print $NF }')\
   | gpg -q --no-tty
```

- ✓ Retrieve, store, and share passwords programmatically with the JSON api.
- ✓ Automate recurring tasks with CLI.
- ✓ Use with Ansible collection, Gitlab, etc.

```
$> export SECRET=`curl --location --request GET '${PASSBOLT_URL}'\
    --header 'Authorization: ${ACCESS_TOKEN}' \
    --header 'Content-Type: application/json' \
   | jq -j '.body.data' \
   | gpg -q --no-tty \
   | jq -j '.password`
```

Go ahead share your secrets

We won’t tell the others.



Share 3 resources

Ada Lovelace ada@passbolt.com	varies	×
Hedy Lamarr hedy@passbolt.com	is owner	×

Share with people or groups

Start typing a user or a group name

Cancel | Save

	Name			
□	Gitlab			/about.gitlal
□	Postgresql			/www.postg
☑	Mastodon			/twitter.com
□	Facebook			/www.faceb
□	Github			/github.com
□	Stripe			/stripe.com/
□	PhpMyAdmin	ada@passbolt.com	●●●●●●●●	https://www.phpm
□	Mysql	ada@passbolt.com	●●●●●●●●	https://www.mysq
□	NPM	ada@passbolt.com	●●●●●●●●	https://www.npmj:
□	Snyk	ada@passbolt.com	●●●●●●●●	https://snyk.io/
□	GPG Key IBM	ada@passbolt.com	●●●●●●●●	
□	AWS EC2	ada@passbolt.com	●●●●●●●●	https://aws.amazo
□	AWS S3	ada@passbolt.com	●●●●●●●●	https://aws.amazo
□	HubSpot	ada@passbolt.com	●●●●●●●●	https://www.hubs
□	MongoDB	ada@passbolt.com	●●●●●●●●	https://www.mong
□	GCP	ada@passbolt.com	●●●●●●●●	https://cloud.goog

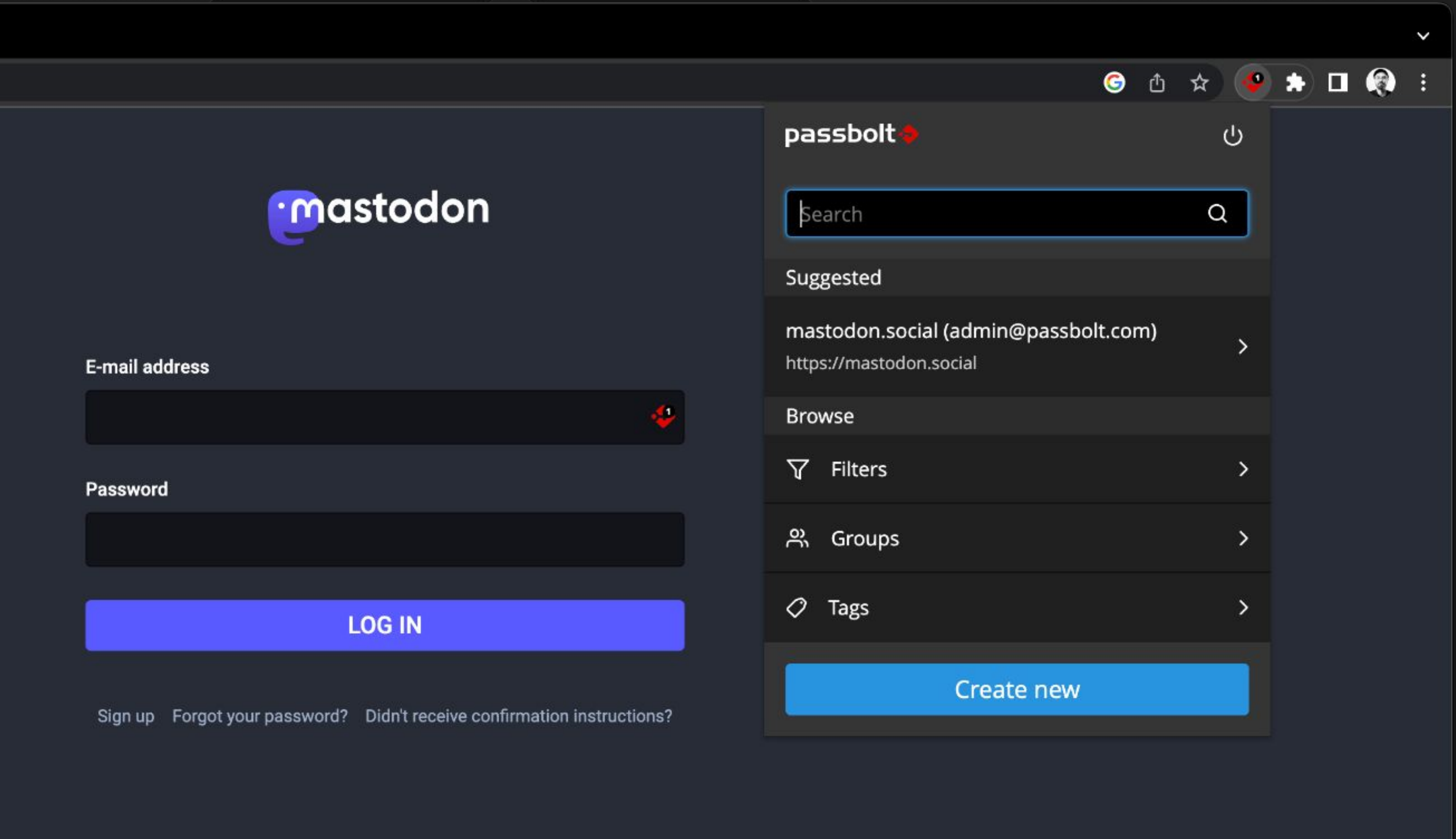
Mastodon

Resource with encrypted description

- Information
- Description
- Shared with
- Tags
- Comments
- Activity

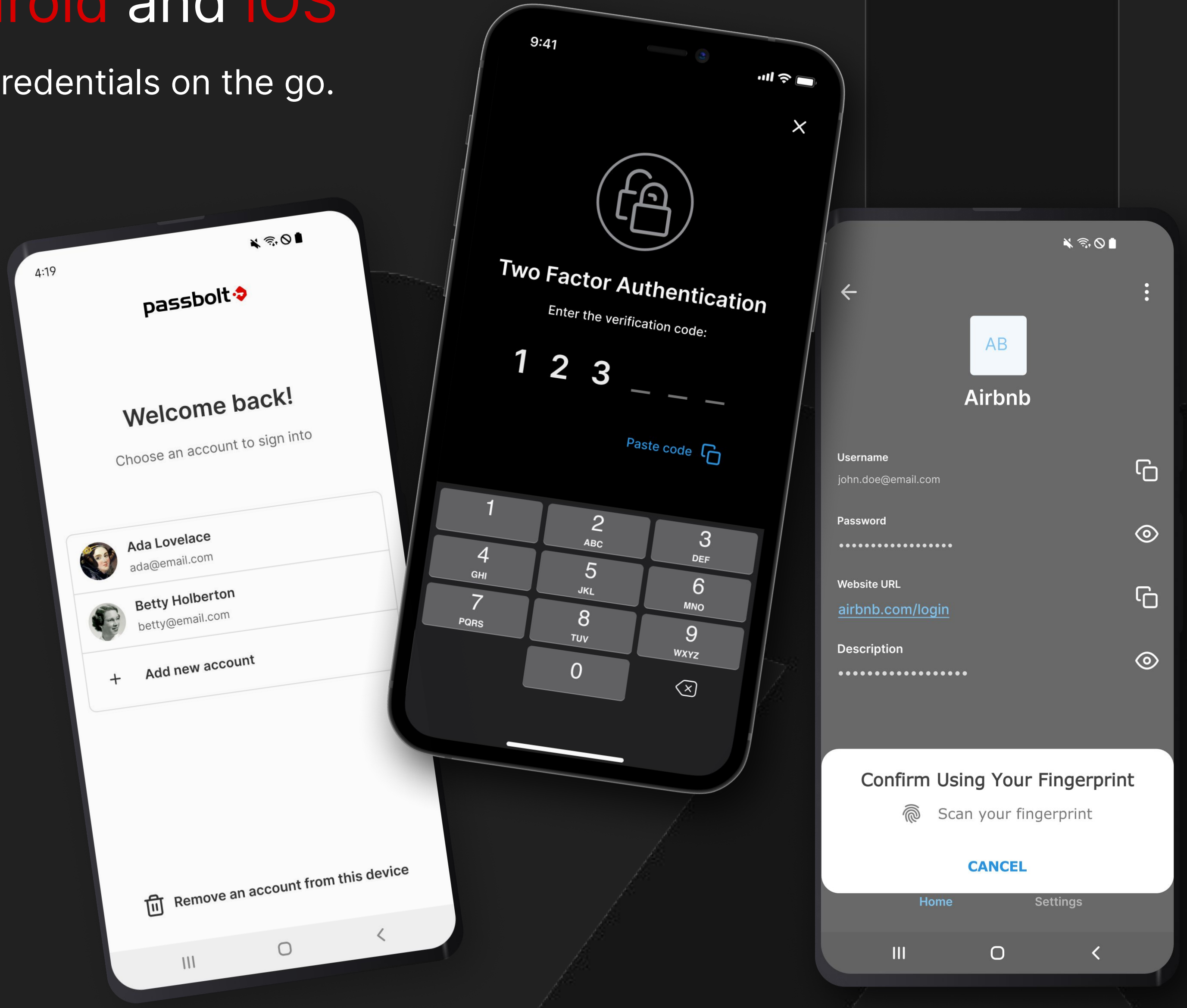
Quick access & in form menu

Fast & furious.



Android and iOS

Your credentials on the go.



4:19

passbolt

Welcome back!

Choose an account to sign into

Ada Lovelace
ada@email.com

Betty Holberton
betty@email.com

+ Add new account

Remove an account from this device

9:41

Two Factor Authentication

Enter the verification code:

1 2 3 _ _ _

Paste code

AB

Airbnb

Username
john.doe@email.com

Password
•••••••••••••••••

Website URL
airbnb.com/login

Description
••••••••••••••••••

Confirm Using Your Fingerprint

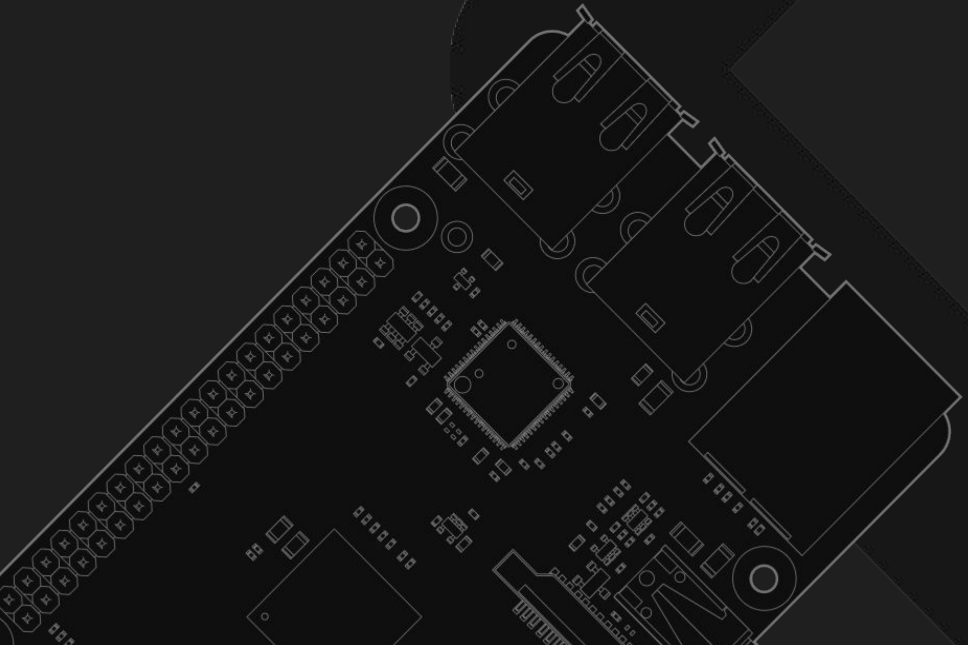
Scan your fingerprint

CANCEL

Got trust issues? Host it yourself!

Works in air-gapped environments or on a Raspberry Pi

- ✓ Docker images (rootless / distroless)
- ✓ Debian / Ubuntu packages
- ✓ RPM packages (RHEL, Centos, etc).
- ✓ Helm charts
- ✓ AWS AMI, Digital Ocean, etc.



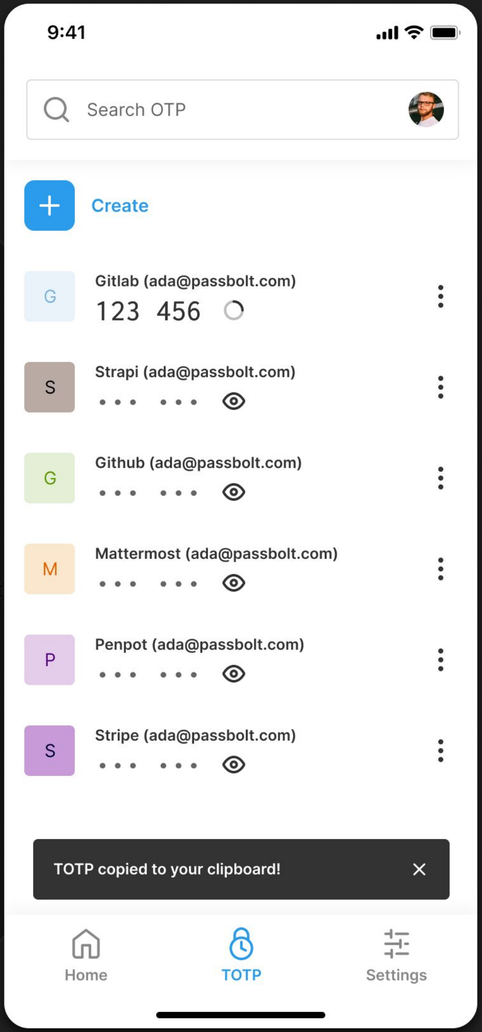
What’s cooking?

Q1/Q2 2023 Community Roadmap

- ✓ Mobile to mobile key transfer
- ✓ Enforce MFA policy
- ✓ User self-registration (allowed domains)
- ✓ Passkeys (Webauthn) support for 2FA
- ✓ Grid configuration & improvements
- ✓ New help site
- ✓ TOTP on mobile devices
- ✓ Desktop application

& beyond...

- ✓ Manifest v3
- ✓ Passwords expiry
- ✓ Custom fields / more content types



Gitlab (ada@passbolt.com)
123 456

Strapi (ada@passbolt.com)
••• •••

Github (ada@passbolt.com)
••• •••

Mattermost (ada@passbolt.com)
••• •••

Penpot (ada@passbolt.com)
••• •••

Stripe (ada@passbolt.com)
••• •••

TOTP copied to your clipboard!

What is it made of?

(the secret ingredient is love)

Three main application layers.

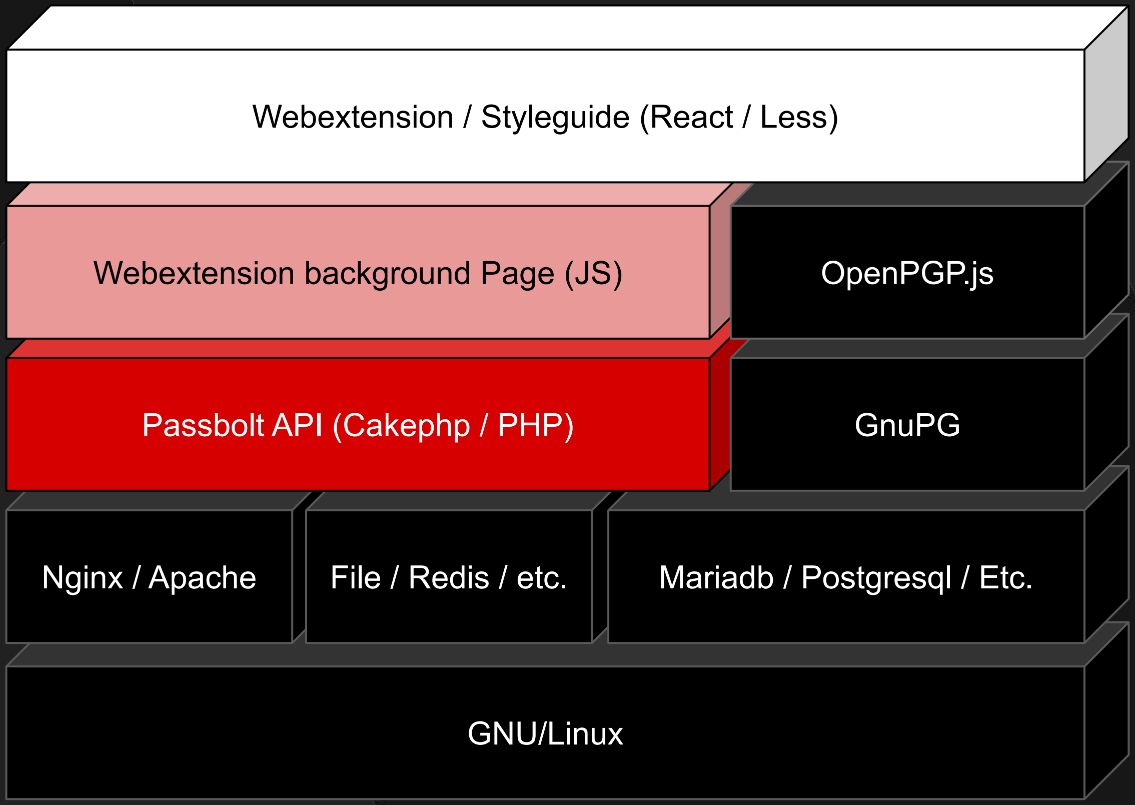
Styleguide, Browser Extension, Web API

User Interface
Interactions, Styling

Sensitive operations
Crypto, validation, API calls

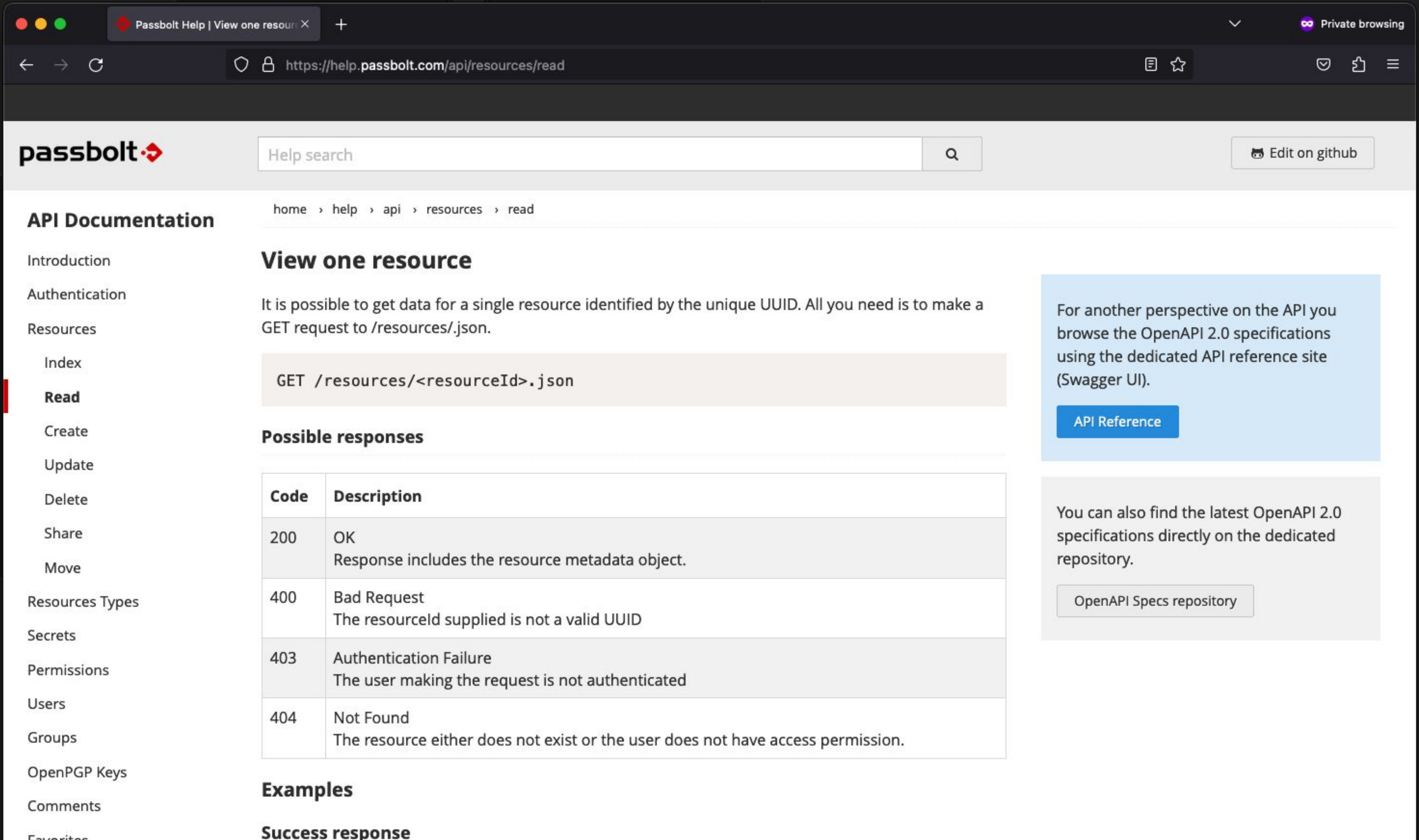
JSON API
(Some HTML content)

Baseline services
LAMP or similar


Webextension / Styleguide (React / Less)
Webextension background Page (JS)
OpenPGP.js
Passbolt API (Cakephp / PHP)
GnuPG
Nginx / Apache
File / Redis / etc.
Mariadb / Postgresql / Etc.
GNU/Linux

Web application layer

https://help.passbolt.com/api



Passbolt Help | View one resour
Private browsing
https://help.passbolt.com/api/resources/read
passbolt
Help search
Edit on github

home › help › api › resources › read

API Documentation

- Introduction
- Authentication
- Resources
  - Index
  - **Read**
  - Create
  - Update
  - Delete
  - Share
  - Move
- Resources Types
- Secrets
- Permissions
- Users
- Groups
- OpenPGP Keys
- Comments

View one resource

It is possible to get data for a single resource identified by the unique UUID. All you need is to make a GET request to /resources/.json.

```
GET /resources/<resourceId>.json
```

Possible responses

Code	Description
200	OK Response includes the resource metadata object.
400	Bad Request The resourceId supplied is not a valid UUID
403	Authentication Failure The user making the request is not authenticated
404	Not Found The resource either does not exist or the user does not have access permission.

Examples

Success response

For another perspective on the API you browse the OpenAPI 2.0 specifications using the dedicated API reference site (Swagger UI).

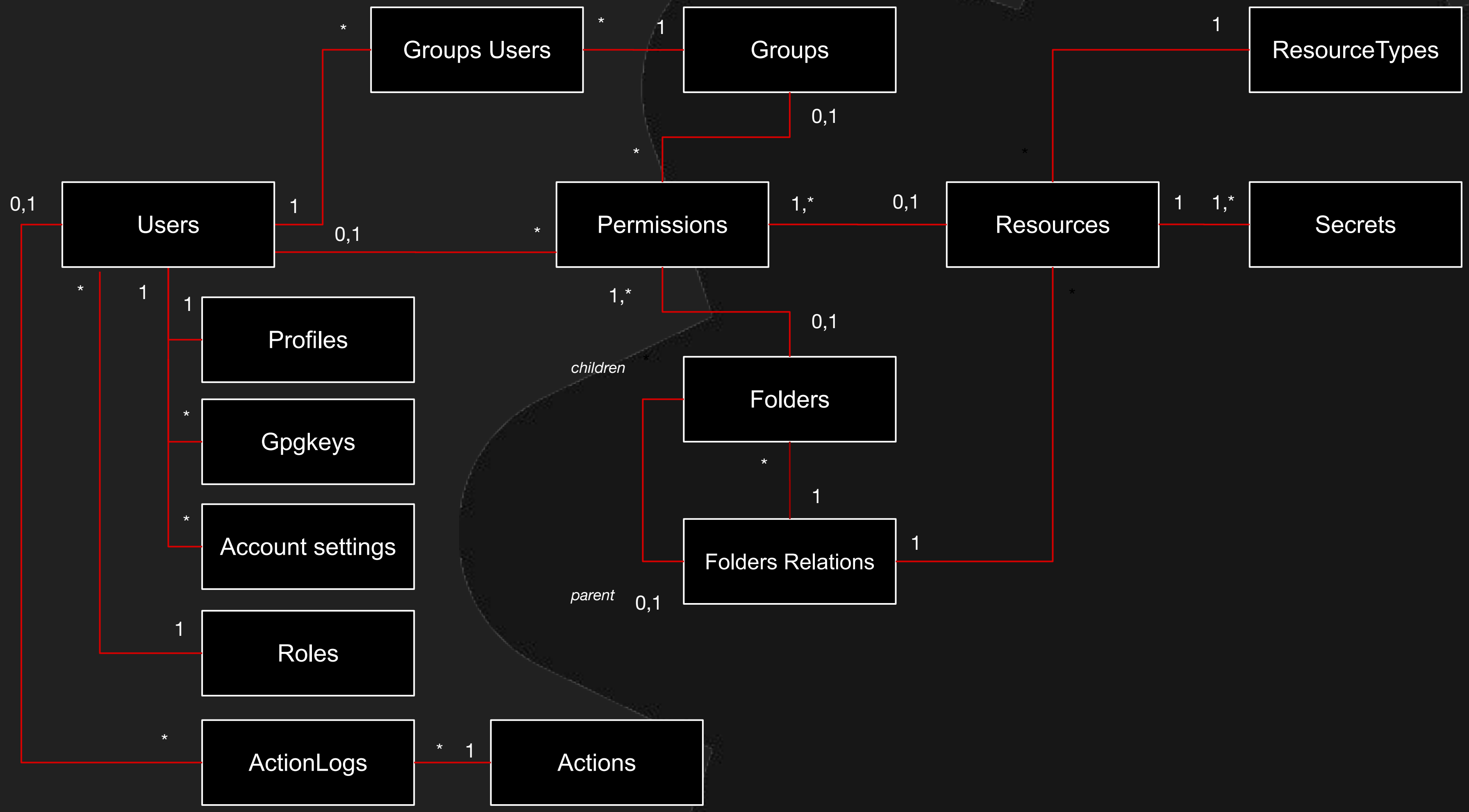
API Reference

You can also find the latest OpenAPI 2.0 specifications directly on the dedicated repository.

OpenAPI Specs repository

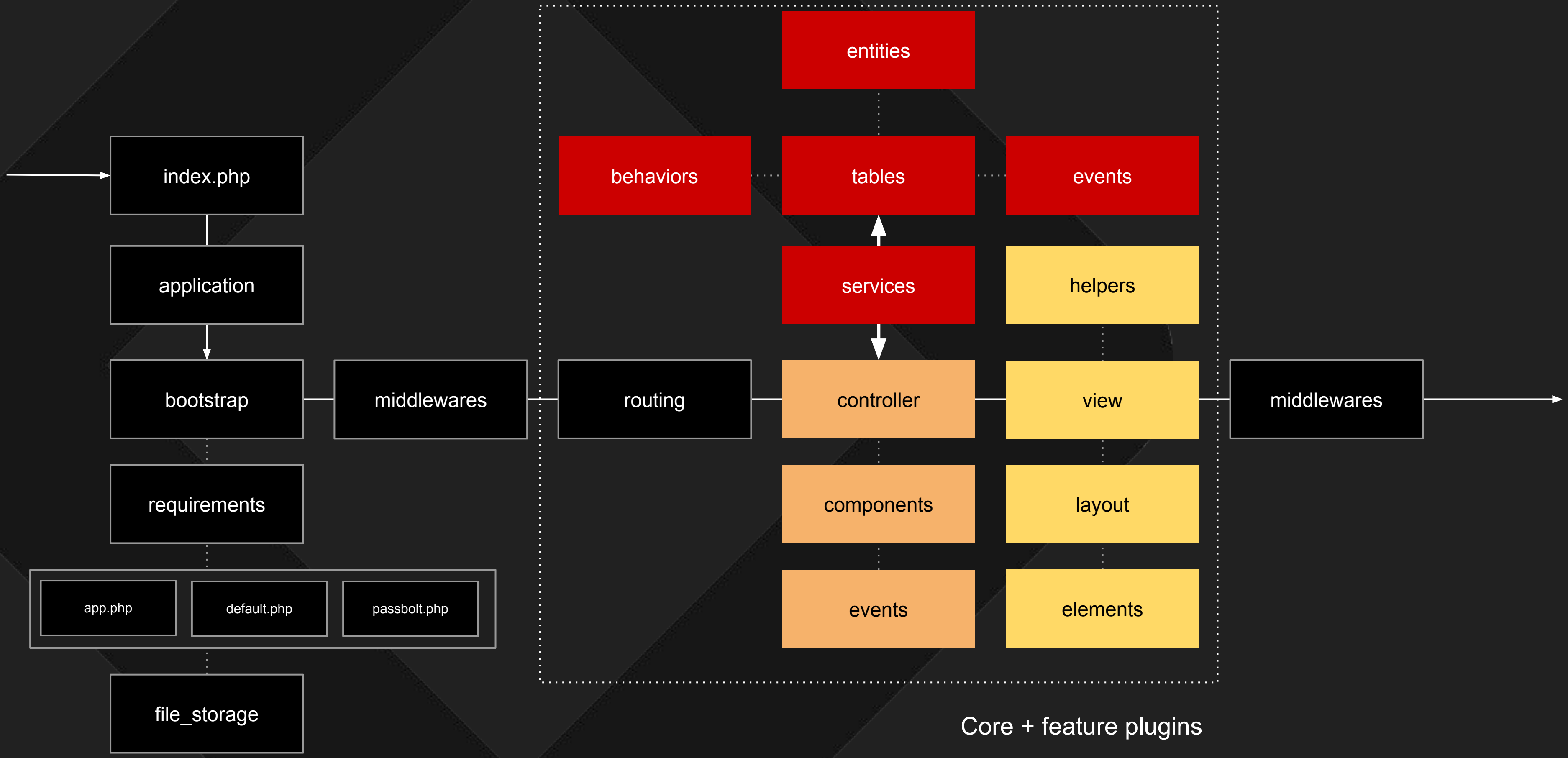
Web application layer

Database tables (main ones)



Web application layer

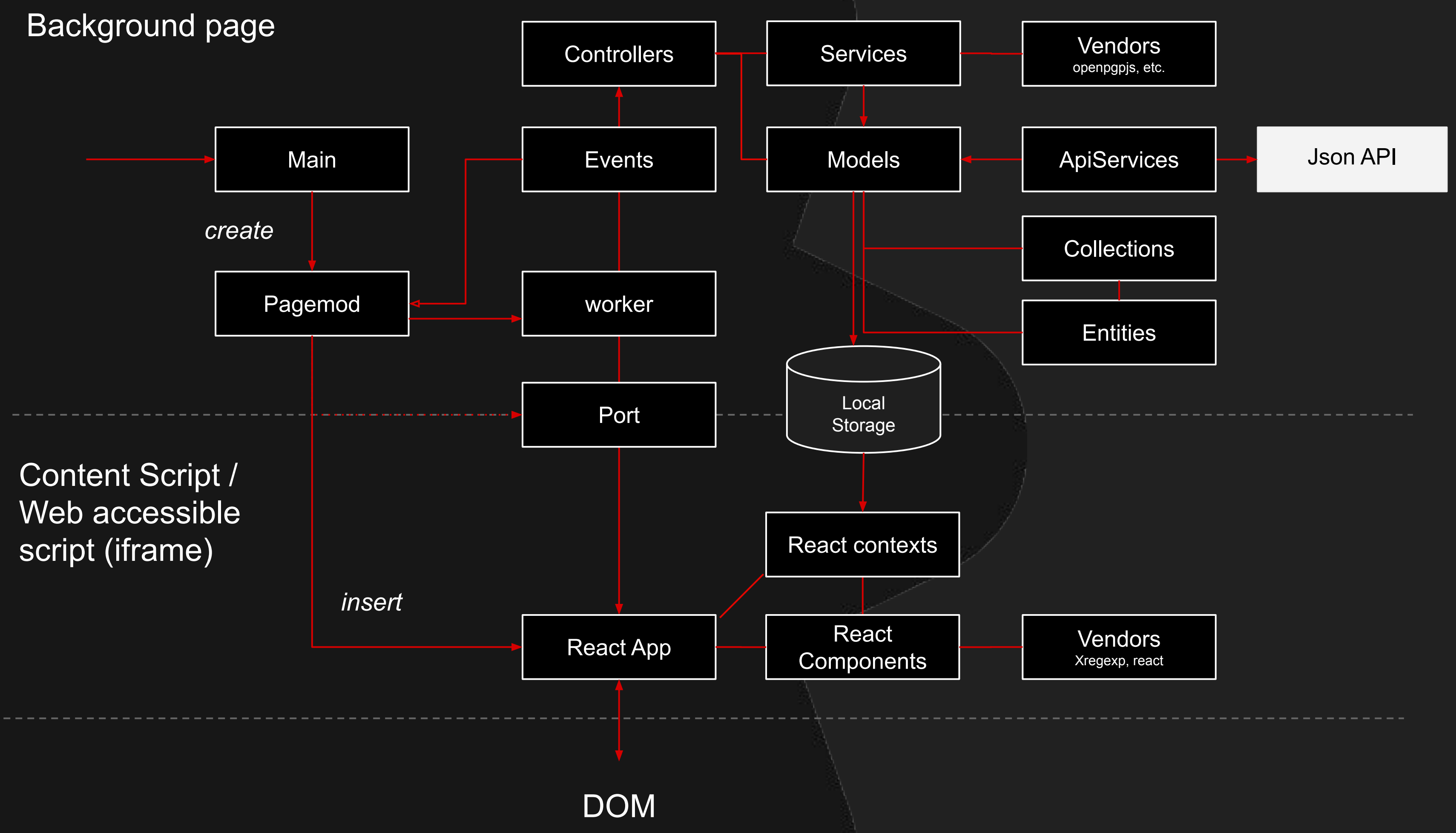
A day in the life of a HTTP request in a typical MVC application



Core + feature plugins

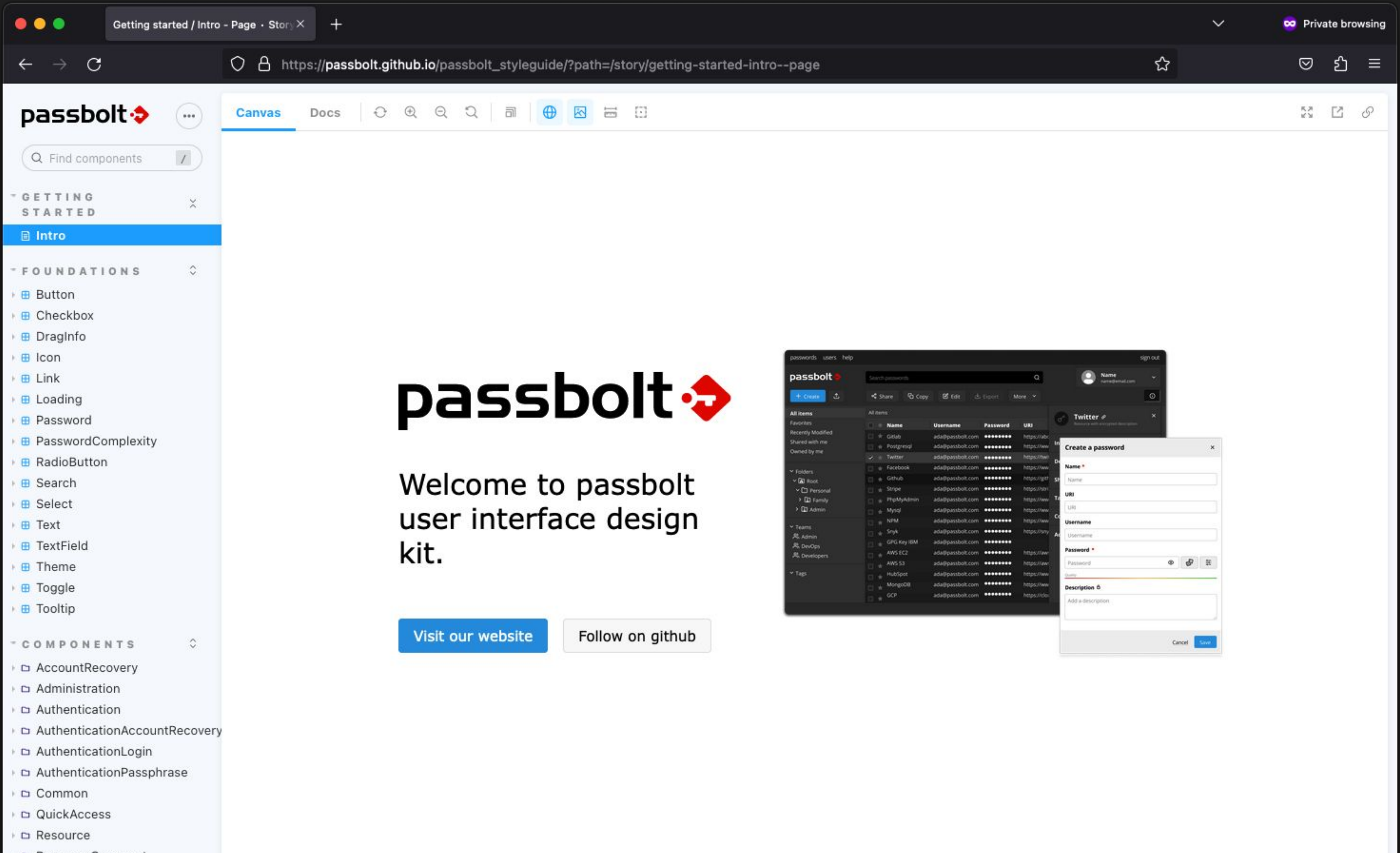
Browser extension

Manifest v2 and beyond...



Passbolt styleguide (Storybook)

https://passbolt.github.io/passbolt_styleguide



https://passbolt.github.io/passbolt_styleguide/?path=/story/getting-started-intro--page

Welcome to passbolt user interface design kit.

Thank you Fosdem ❤️

See you at the bar at 18:00
for some swag & 🍻