WEB AUTHENTICATION

Implementing User Authentication with Passkeys

MAXIMILIANO FIRTMAN

FIRT
.DEV

MAXIMILIANO FIRTMAN

MOBILE+WEB DEVELOPER

HTML since 1996

JavaScript since 1998

AUTHOR

Authored 13 books and +70 courses

Published +150 webapps

@FIRT . FIRT.DEV

WEB.DEV/LEARN/PWA

Filter

Welcome to Learn Progressive Web Apps!
Progressive Web Apps
Getting started
Foundations
App design
Assets and data
Service workers
Caching
Serving
Workbox
Offline data
Installation
Web app manifest
Installation prompt
Update
Enhancements
Detection

Welcome to Learn Progressive Web Apps!

A course that breaks down every aspect of modern progressive web app development.

This course covers the fundamentals of Progressive Web App development in easy-to-understand pieces. Over the following modules, you'll learn what a Progressive Web App is, how to create one or upgrade your existing web content, and how to add all the pieces for an offline, installable app. Use the menu pane to navigate the modules. (The menu is at left on desktop or behind the hamburger menu on mobile.)

You'll learn PWA fundamentals like the Web App Manifest, service workers, how to design with an app in mind, how to use other tools to test and debug your PWA. After these fundamentals, you'll learn about integration with the platform and operating system, how to enhance your PWA's installation and usage experience, and how to offer an offline experience.

Each module includes interactive demos and self-assessments for you to test your knowledge. You will be able to test and try demos on your mobile phone, tablet, or laptop while playing with code to understand the fundamentals of what makes a Progressive Web App.

This course is created for a beginner and advanced web developers alike. You can go through the series from start to finish to get a general understanding of PWA from top to bottom, or you can use it as a reference for specific subjects. For those new to web development you will need a grounding in HTML, CSS, and JavaScript to follow along. Check out Learn CSS, and the HTML and JavaScript courses on MDN.

Here's what you'll learn:

Getting started

Frontend Masters

PLURALSIGHT

LinkedIn Learning

awwwards.academy

What we'll cover

- Authentication
- State of Techniques
- Login Forms
- New Flows
- Data Structure
- Web Services
- Web Authentication
- Passlinks

Let’s Start!

Pre-requisites

auth.firt.dev

Questions?

FullStack Authentication

1

Introduction

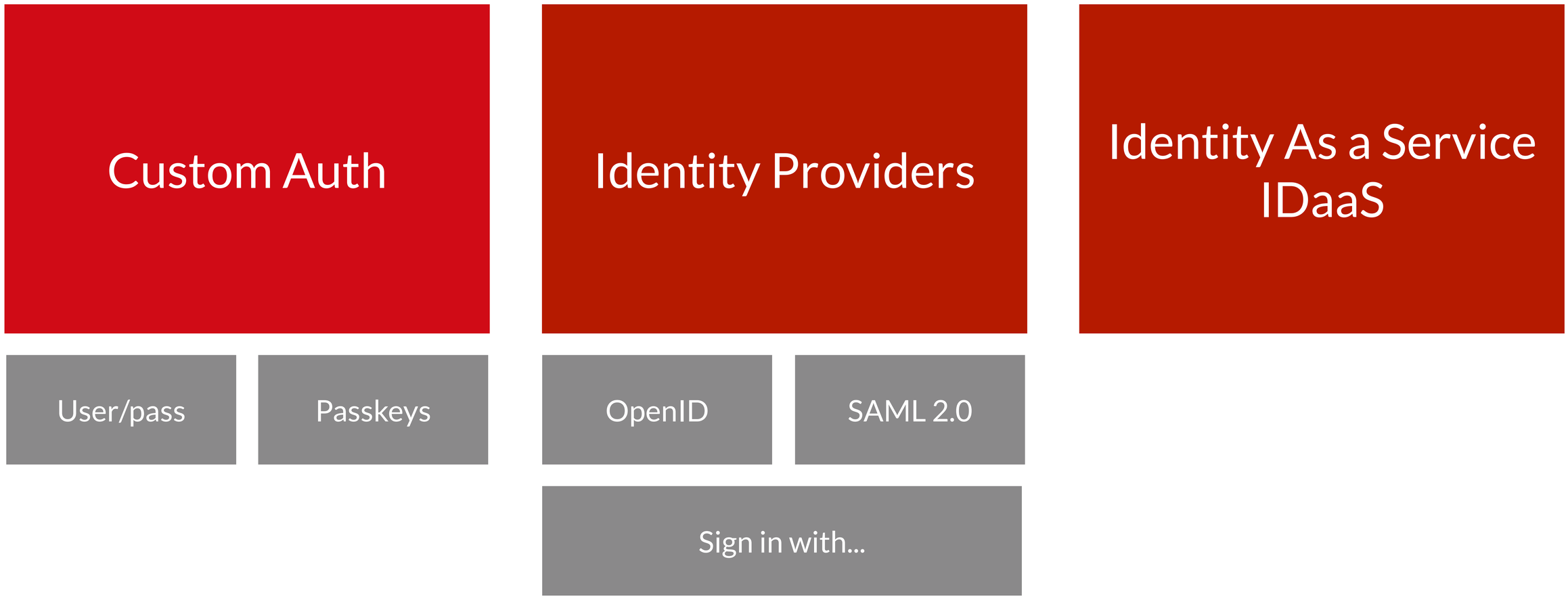
Authentication

Authorization

Authentication (Authn) verifies the identity of a user or service.

We will discuss authentication on the Web

Implementing Authentication



2

Authentication on the Web

World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
: Pointers to the world's online information, subjects , W3 servers, etc.

Help
: on the browser you are using

Software Products
: A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)

Technical
: Details of protocols, formats, program internals etc

Bibliography
: Paper documentation on W3 and references.

People
: A list of some people involved in the project.

History
: A summary of the history of the project.

How can I help ?
: If you would like to support the web..

Getting code
: Getting the code by anonymous FTP , etc.

Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Sl

Bookmarks Go to: http://www.unicode.org/mail-arch/unicode-ml/y2002-m01/

Username and Password Requi...

Enter username for Unicode-MailList-Archives at www.unicode.org:

User Name:

Password:

OK Cancel

ALIWEB Form Search

This form queries a mirror of the ALIWEB database at WWW.FUNET.FI se

---

What would you like to search for? [ ] Submit Reset

There are several types of search: Case Insensitive Substring

Which fields would you like to search?
☑ Titles ☑ Descriptions ☑ Keywords ☐ URL's

What fields would you like displayed in addition to the title?
☑ Descriptions ☐ Keywords ☐ URL's

You can restrict the results to a domain (e.g. "fi"): [ ]

You can restrict the number of results): [ ]

Martijn Koster

A List Apart — For People Who Make Websites.

Use the form below to join **A List Apart,** our free, moderated mailing list for people who make websites. If you prefer to use email, send a blank message to join@alistapart.com and you will be added to the list.

Problems using this form? Report them to brian@alistapart.com.

Name: (optional)

Email:

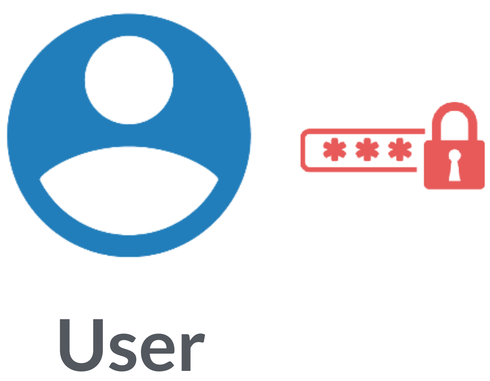
Join

Thousands of designers, writers & programmers agree.

A List Apart is good reading for people who make websites.

© 1999 Jeffrey Zeldman and Brian M. Platz.

HTTP Auth / Login Forms



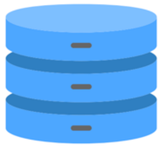
HTTP Auth / Login Forms

HTTP Auth / Login Forms

Browser

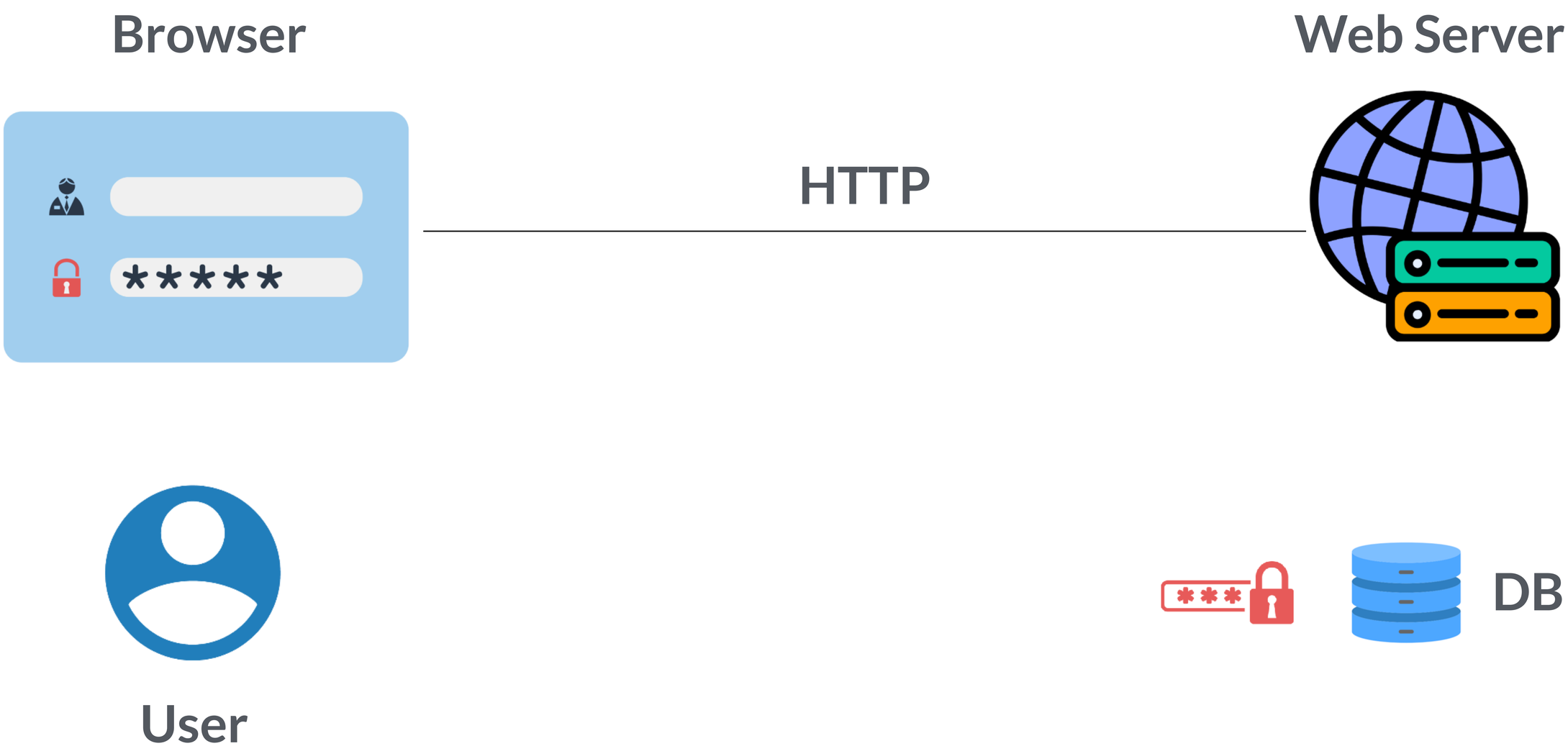
Web Server

User

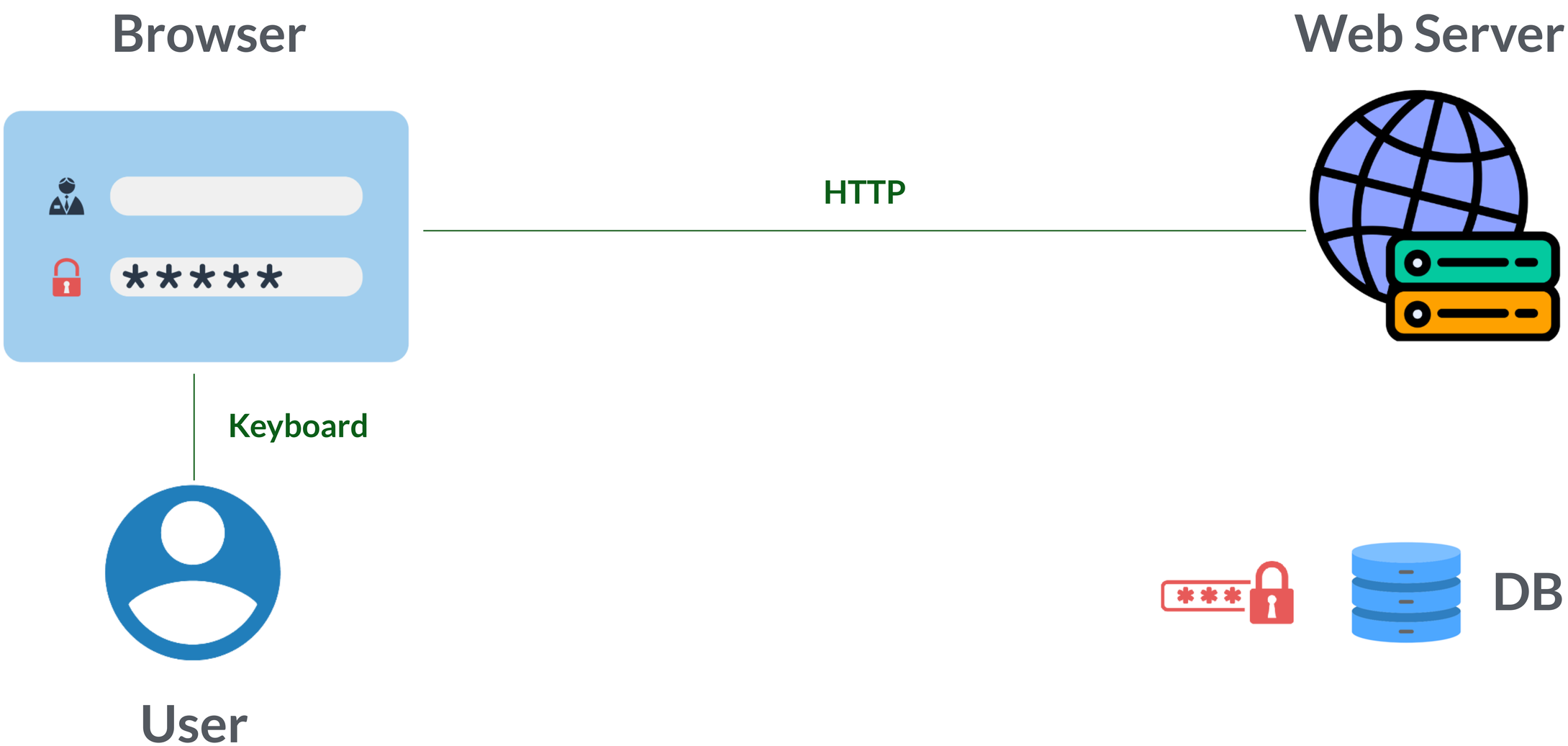


DB

HTTP Auth / Login Forms



HTTP Auth / Login Forms



HTTP Auth / Login Forms

HTTP Auth / Login Forms

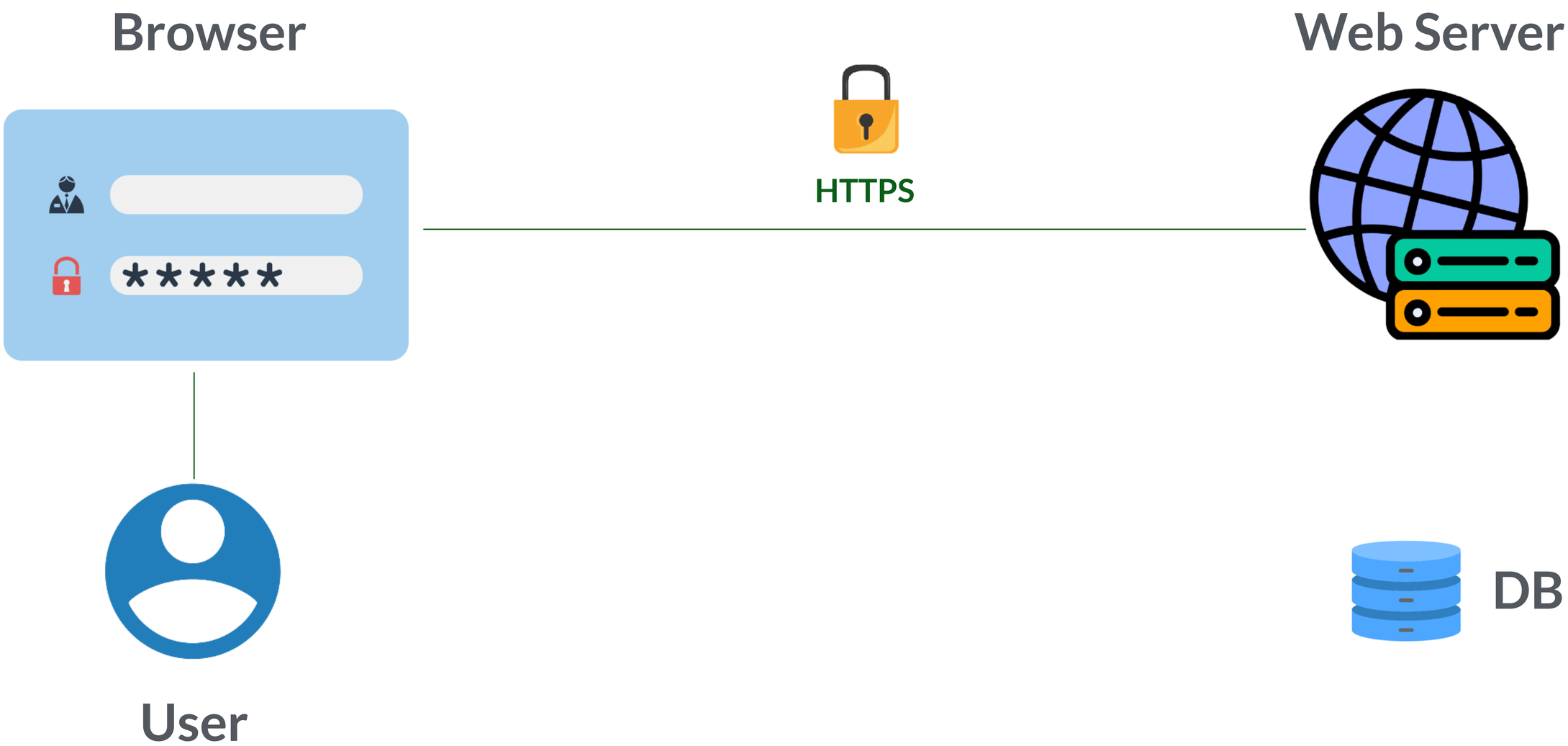
HTTP Auth / Login Forms

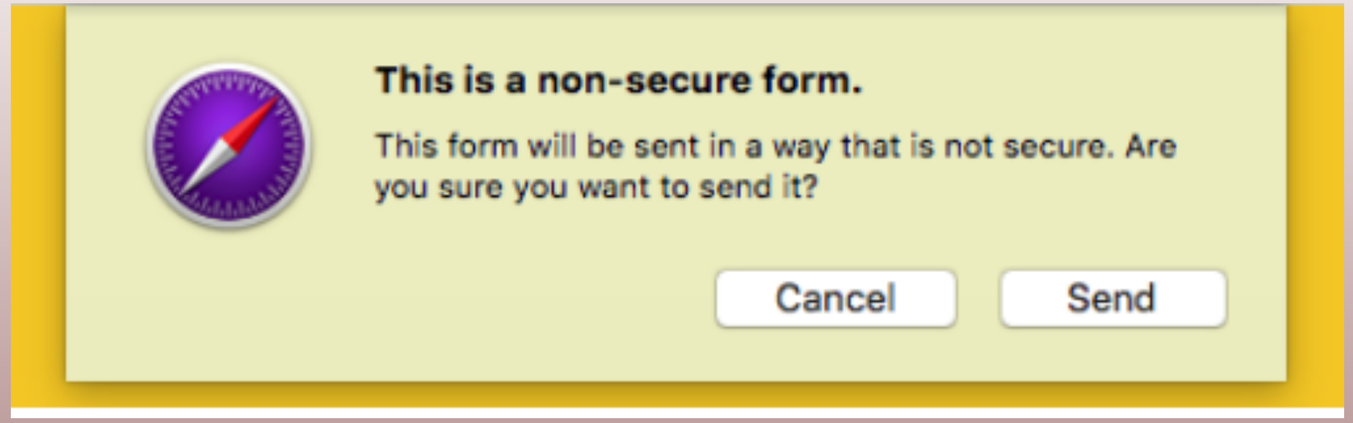
HTTP Auth / Login Forms

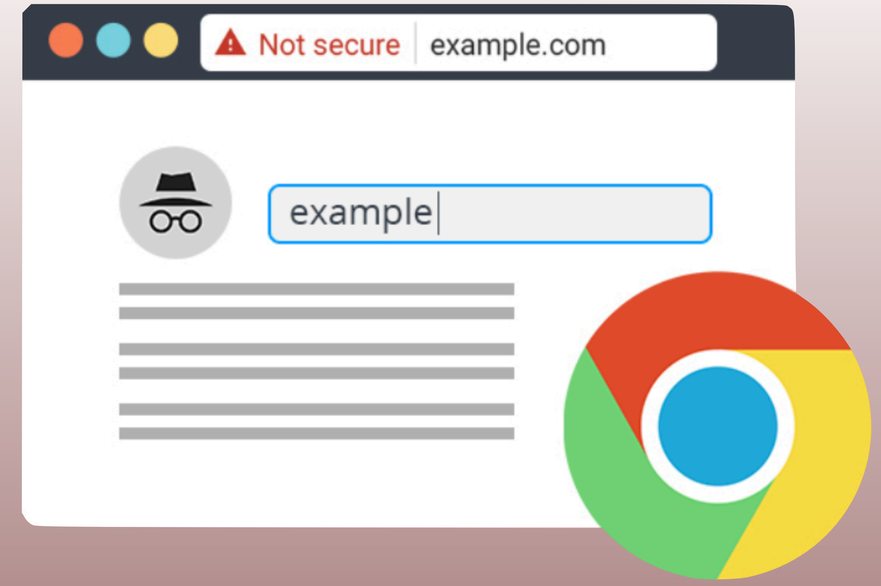
HTTP Auth / Login Forms

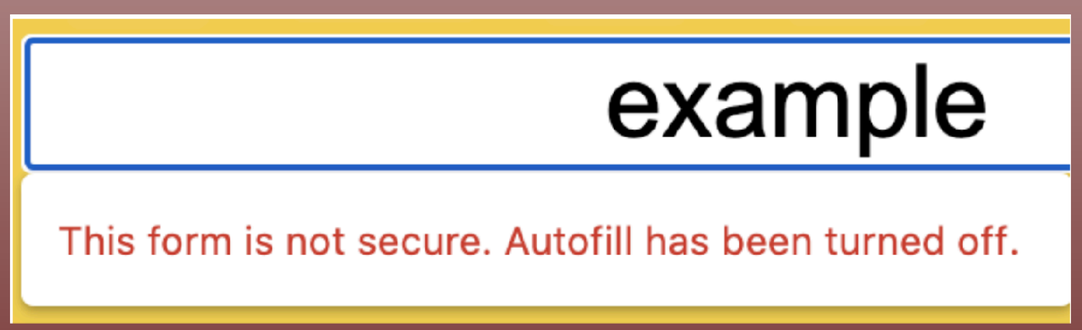
HTTP Auth / Login Forms

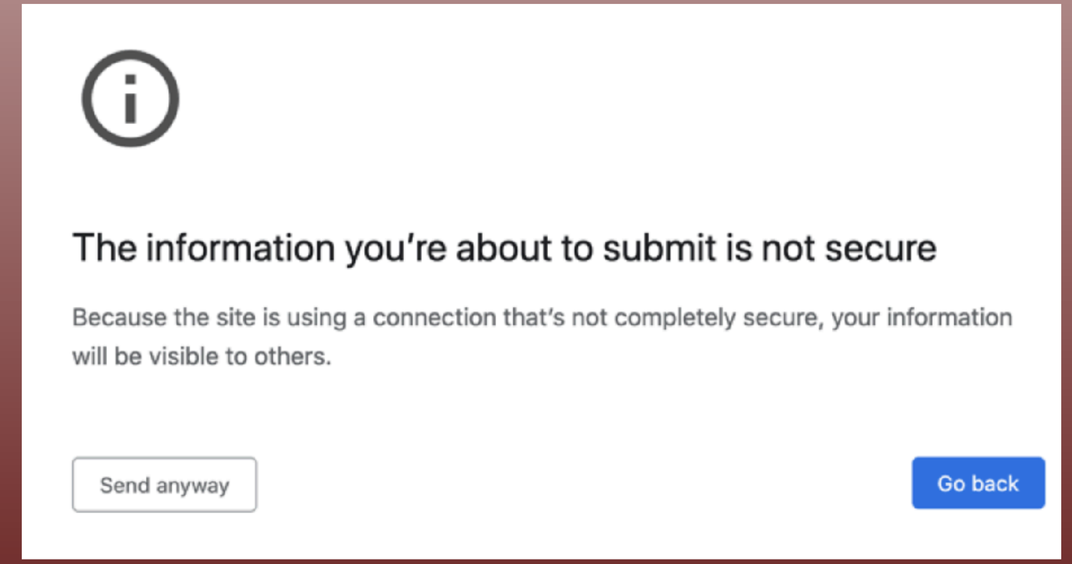
HTTP Auth / Login Forms



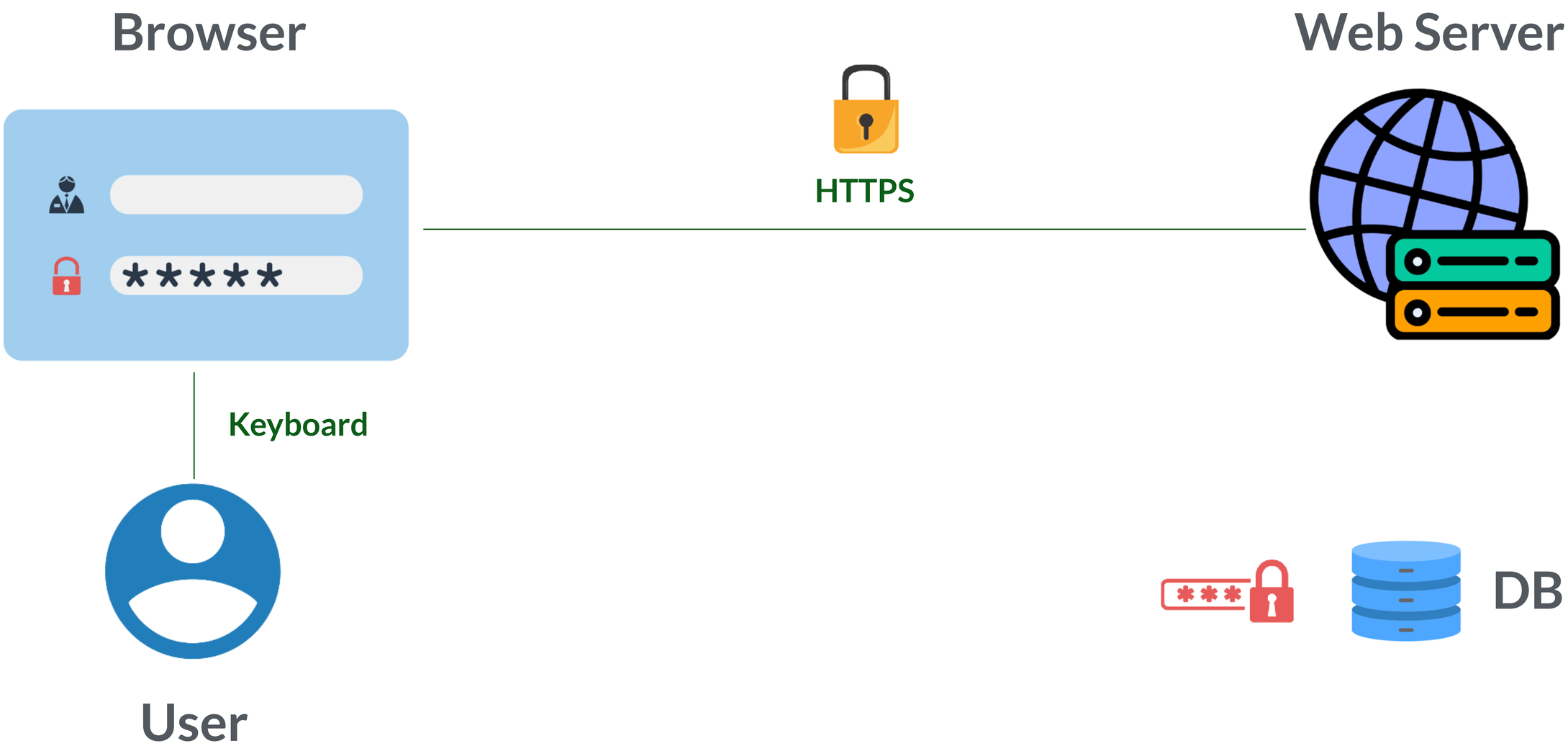

This is a non-secure form.
This form will be sent in a way that is not secure. Are you sure you want to send it?
Cancel
Send


Not secure
example.com
example

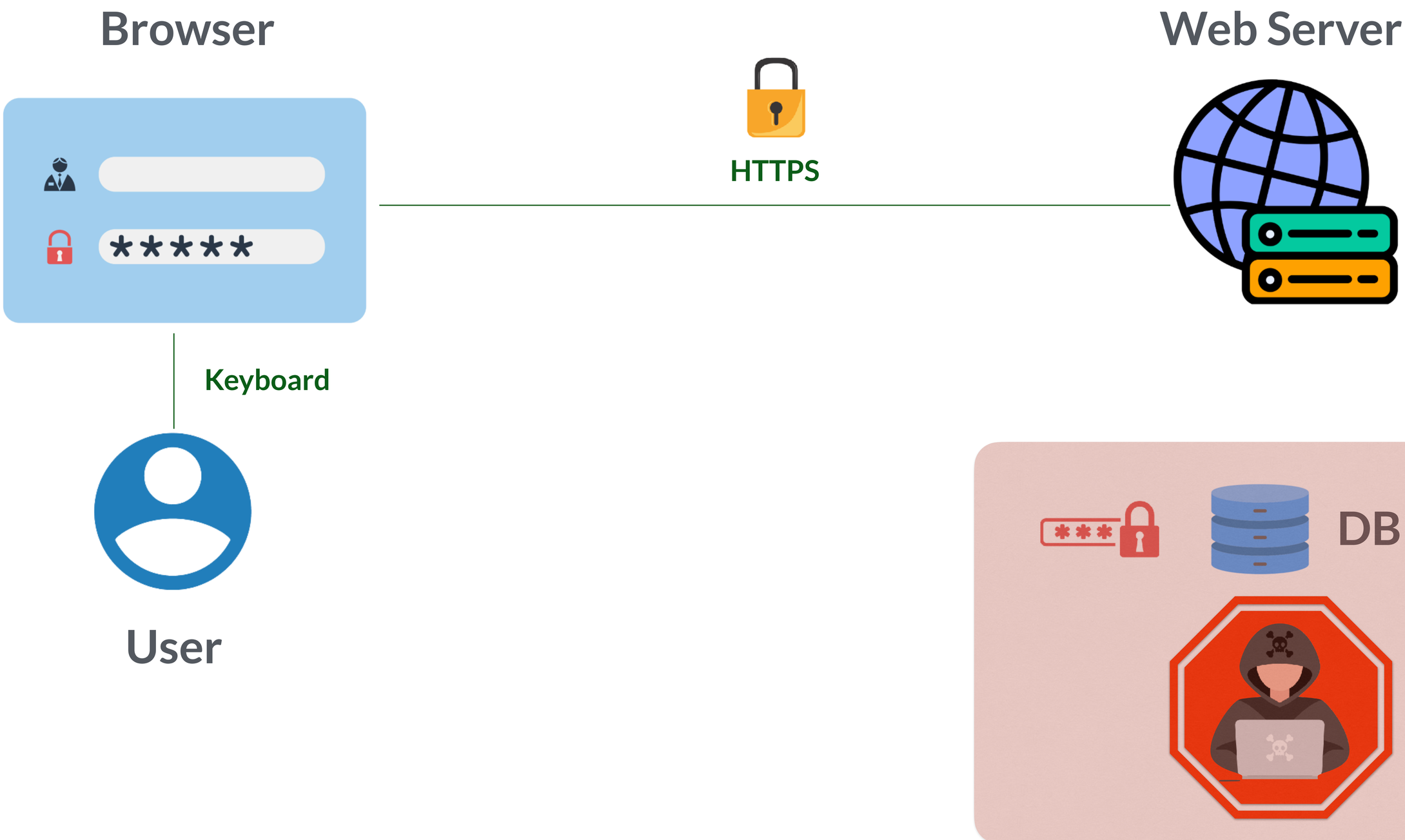

example
This form is not secure. Autofill has been turned off.


The information you're about to submit is not secure
Because the site is using a connection that's not completely secure, your information will be visible to others.
Send anyway
Go back

HTTP Auth / Login Forms



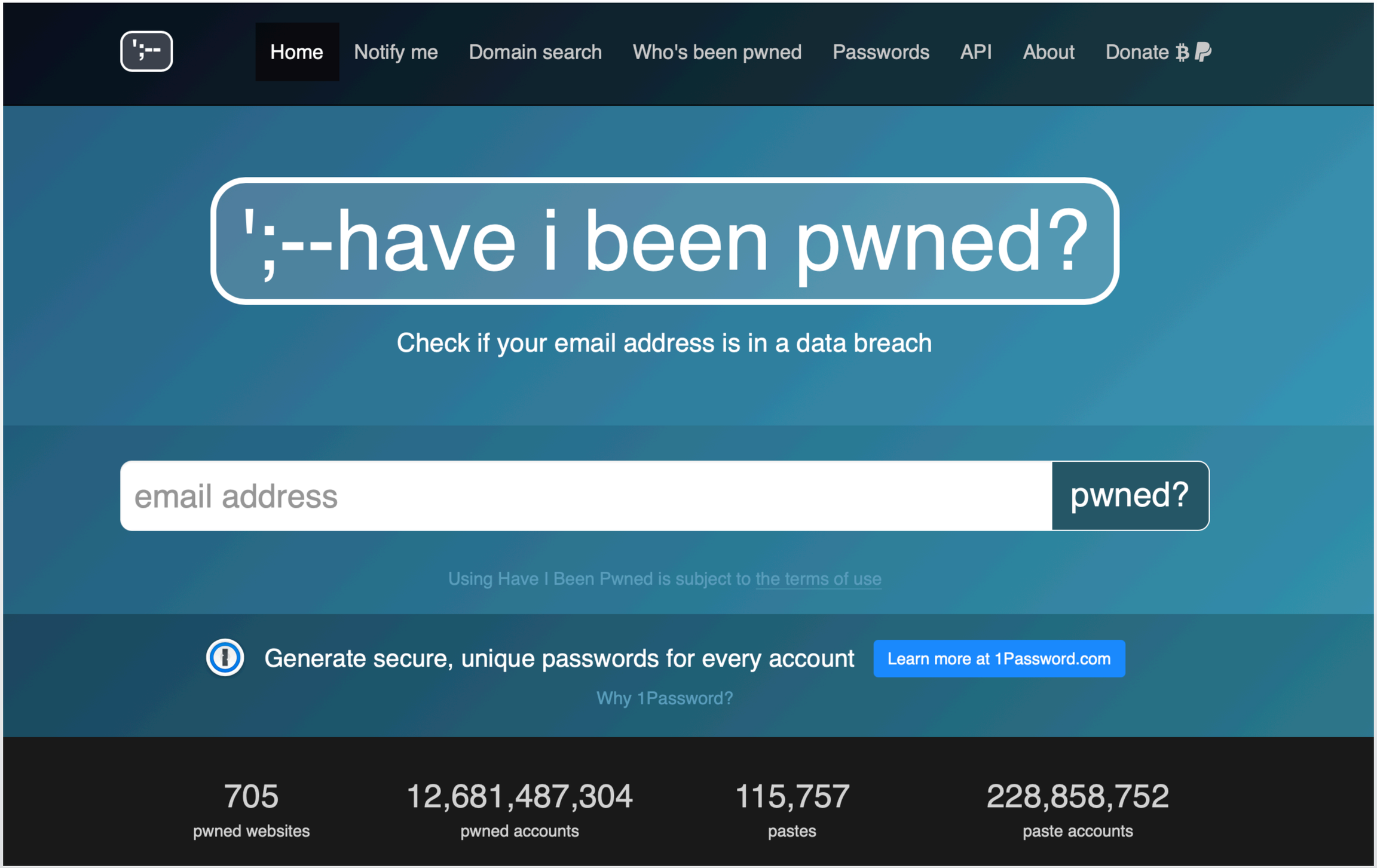
HTTP Auth / Login Forms



BIGGEST DATA BREACHES IN THE USA

(2013-2017)

COMPANY	RECORDS BREACHED	TYPE OF BREACH	SOURCE OF BREACH
YAHOO!	1,000,000,000	Identity Theft	Malicious Outsider
FRIENDFINDER NETWORKS	412,214,295	Existential Data	Malicious Outsider
myspace	360,000,000	Account Access	Malicious Outsider
DEEP ROOT	198,000,000	Identity Theft	Accidental Loss
Adobe	152,000,000	Financial Access	Malicious Outsider
EQUIFAX	147,900,000	Identity Theft	Malicious Outsider
ebay	145,000,000	Identity Theft	Malicious Outsider
alteryx	123,000,000	Identity Theft	Accidental Loss
Target	110,000,000	Financial Access	Malicious Outsider


';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
email address
pwned?
Using Have I Been Pwned is subject to the terms of use
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
705
pwned websites
12,681,487,304
pwned accounts
115,757
pastes
228,858,752
paste accounts

Back **Security Recommendations**

Detect Compromised Passwords

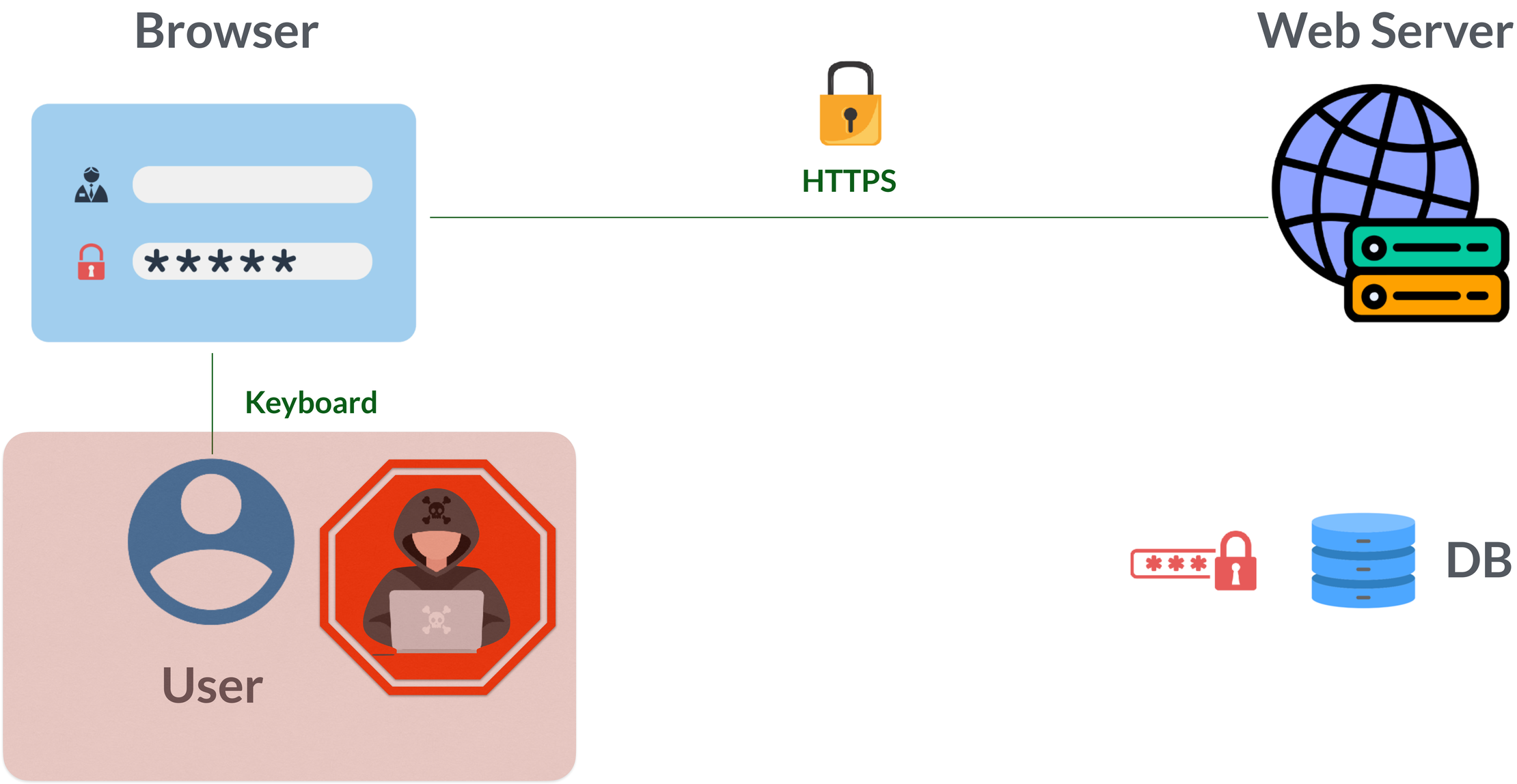
iPhone can securely monitor your passwords and alert you if they appear in known data leaks. About Passwords & Privacy...

HIGH PRIORITY

.com —

Change Password on Website

HTTP Auth / Login Forms



Password Requirements

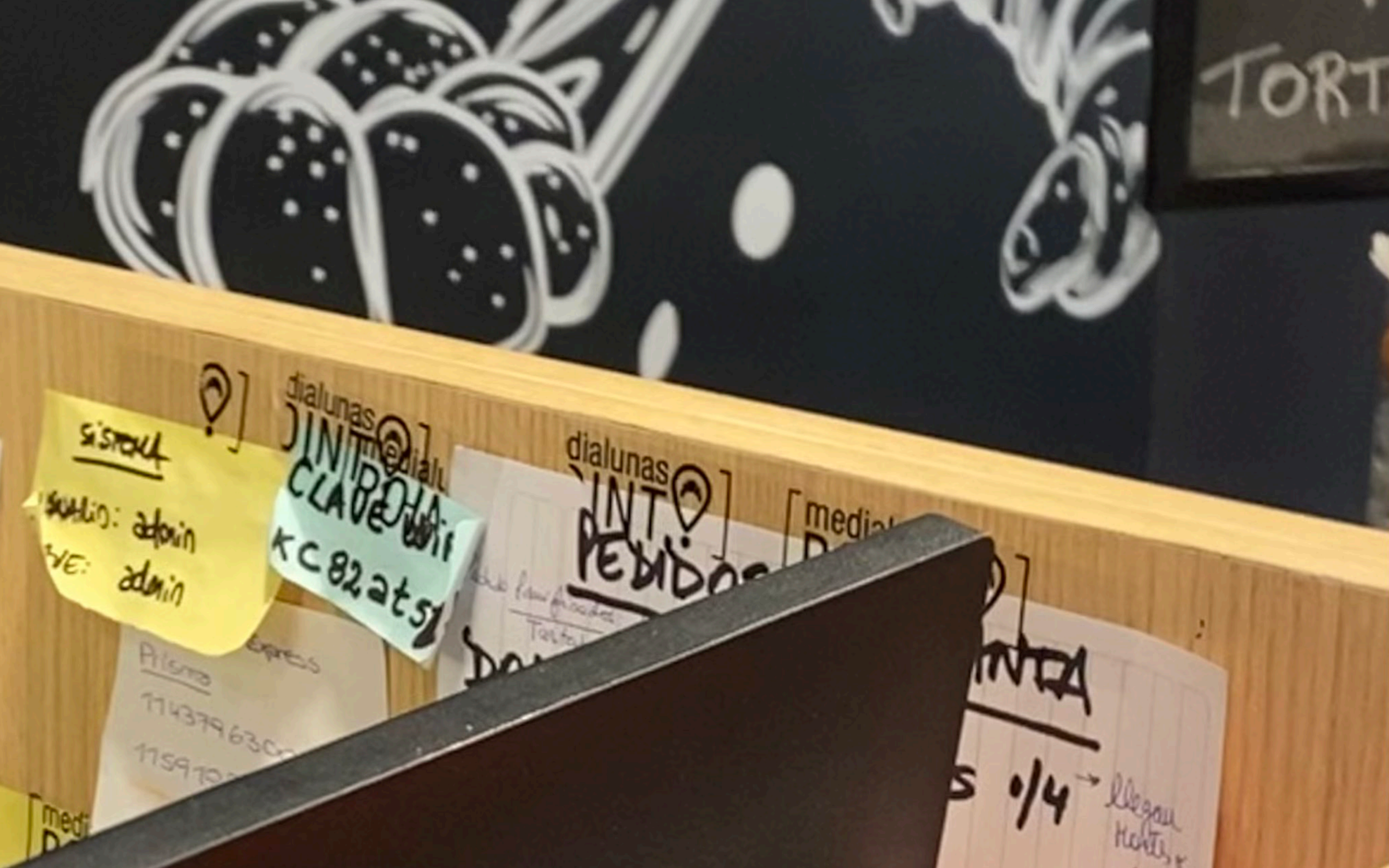
- ✕ MUST contain at least 8 characters (12+ recommended)
- ✕ MUST contain at least one uppercase letter
- ✕ MUST contain at least one lowercase letter
- ✕ MUST contain at least one number
- ✕ MUST contain at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)
- ✔ MAY NOT contain more than two identical characters in a row
- ✔ MAY NOT contain first name, last name, email address mailbox or domain, company name or commonly used passwords
- ✔ MAY NOT match commonly used password character patterns

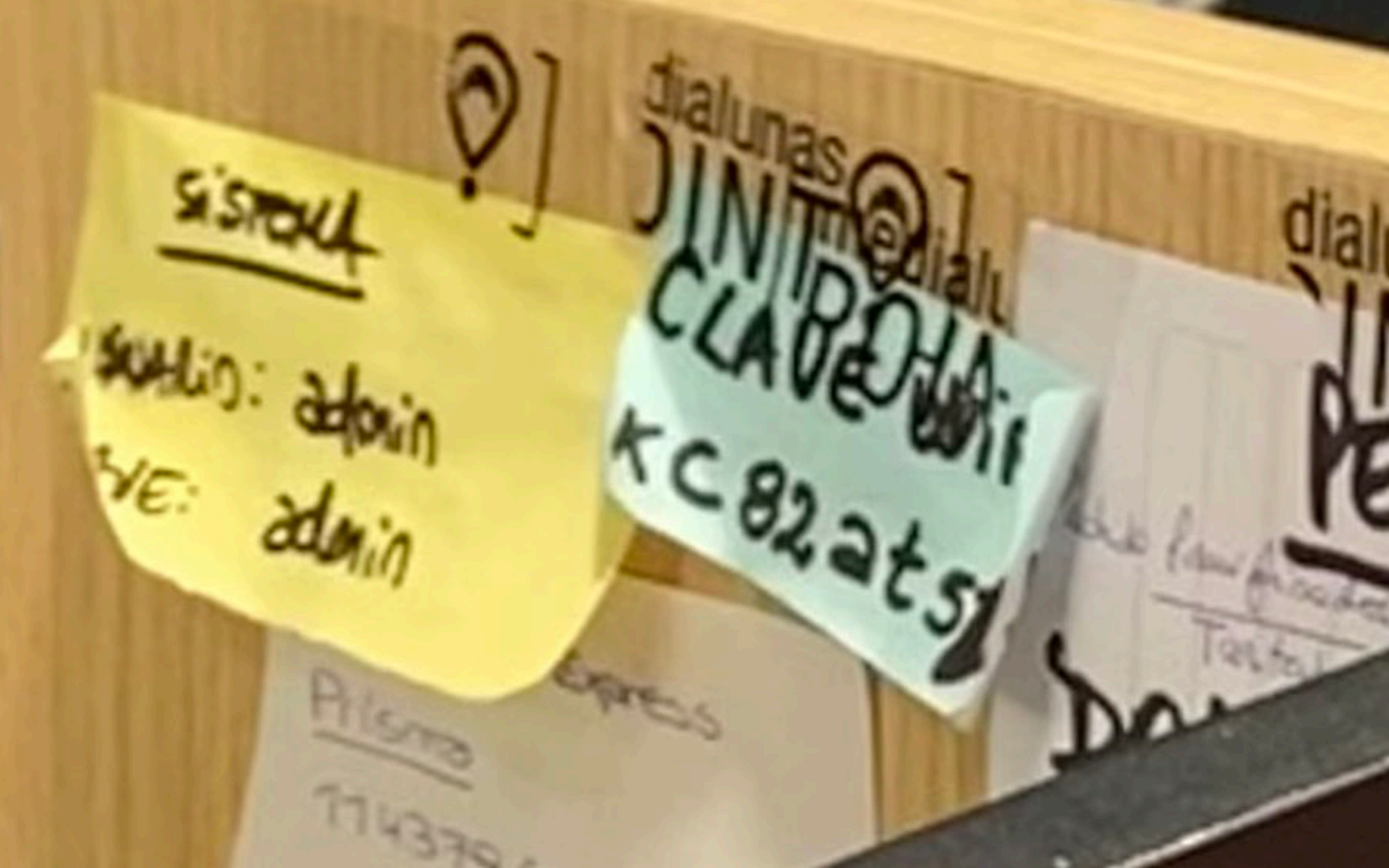
5 remaining rules need to be met

Mots de passe Wifi

Wifi columbus Client

Suivez_Columbus_cafe_nantes_sur_insta


TORT
dialunas
dialunas
admin
admin
kc82atsj
PEDIDOS
1/4


SISTRAL
admin
admin
JINTRO
CLABEDA
KC82atsy
dialunas
Prisma
Express

ABAPPRA
ASOCIACIÓN DE BANCOS PÚBLICOS Y PRIVADOS DE LA REPÚBLICA ARGENTINA
El Banco nunca te va a pedir la clave.
Las claves no se comparten
Fogaba
BPN
BANCOR
BCH
BICE
Banco Formosa
BancoCiudad
Banco Nación
Banco Provincia

Why You Should Stop Using LastPass After New Hack Method Update

Davey Winder Senior Contributor
Co-founder, Straight Talking Cyber

Follow

6

Mar 3, 2023, 08:00am EST

Log in to your PayPal account

Not Secure | paypal--accounts.com

PayPal

Email or mobile number

Password

Log In

Log in to your PayPal account

Not Secure paypal--accounts.com

PayPal

Email or mobile number

Password

Log In

Log in to your PayPal account

https://paypal--accounts.com

PayPal

Email or mobile number

Password

Log In

Google Account

Search Google Account

- Home
- Personal info
- Data & privacy
- Security
- People & sharing
- Payments & subscriptions
- About

How you sign in to Google

Make sure you can always access your Google Account by k

- 2-Step Verification
- Passkeys
- Password
- Security keys
- Authenticator
- Google prompt

About

Authenticator

Google prompt

2-Step Verification phones

Recovery phone

Recovery email

Google Account PIN

Security question

Backup codes

Two conclusions

Security Risks

- Man in the Middle Attacks
- Keyloggers
- Easy to guess passwords
- Web Servers and DBs Attacks
- Phishing and Social Engineering Attacks

Easy to guess passwords
and reuse of passwords
are another risk

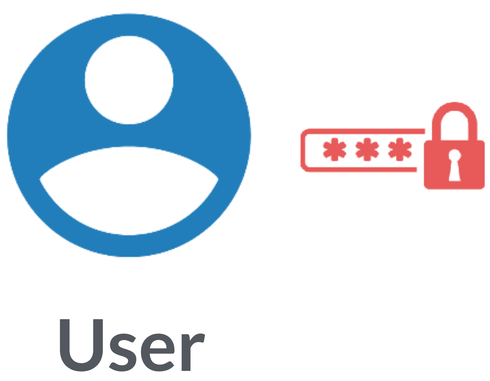
Password managers help with both problems but still not perfect

Workshop time

haveibeenpwned.com

Multi-factor Authentication

Multi-factor Authentication



Multi-factor Authentication

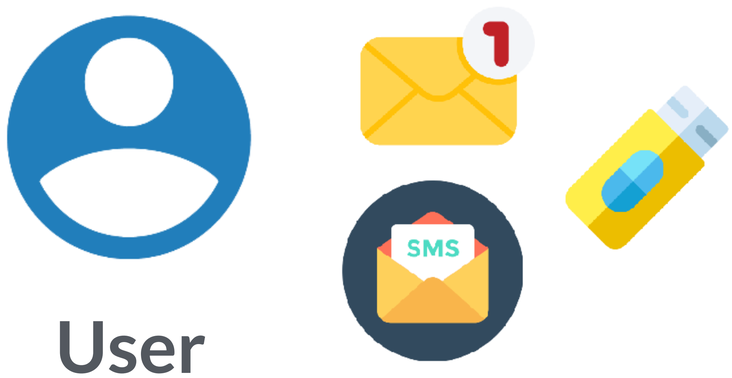
User

Multi-factor Authentication

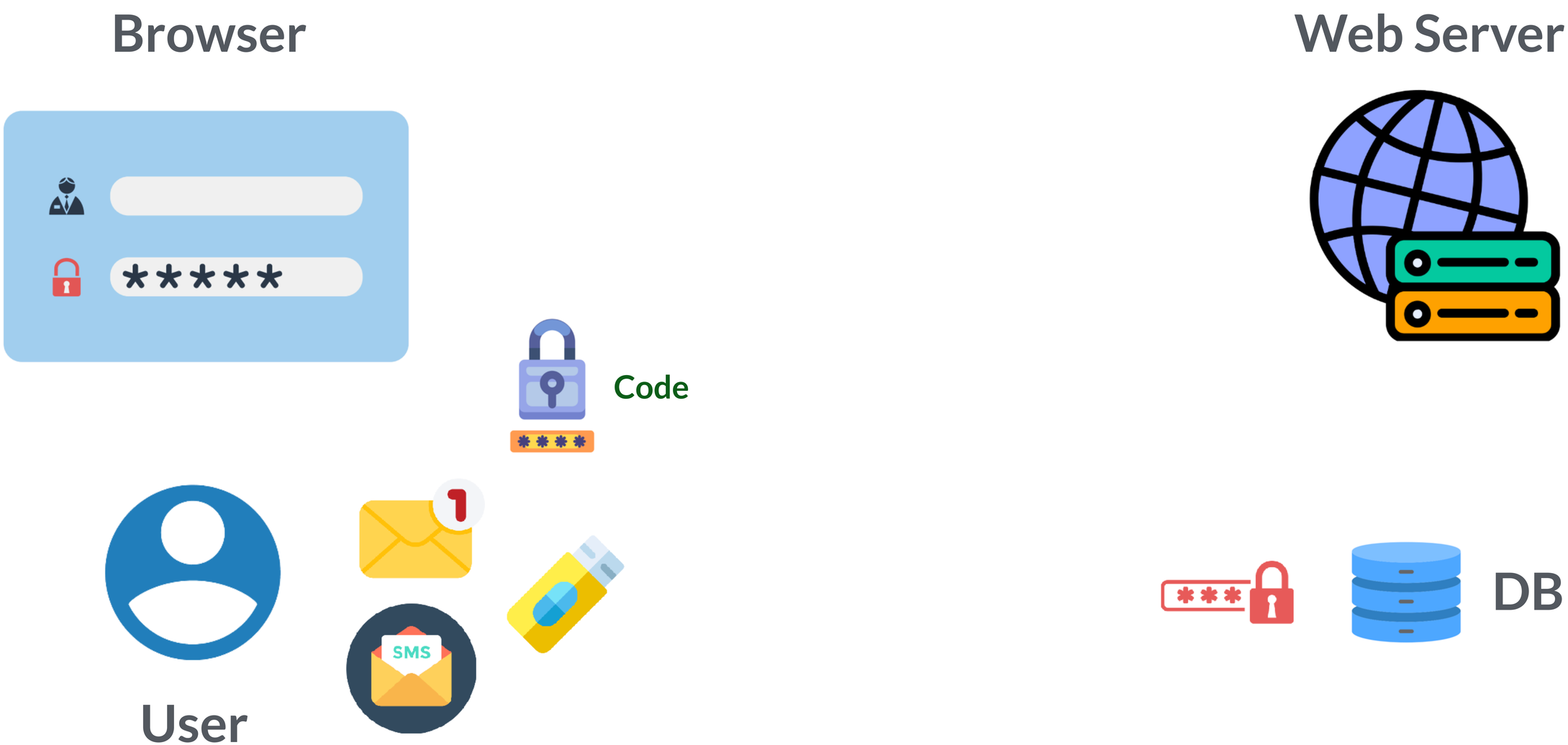
User

DB

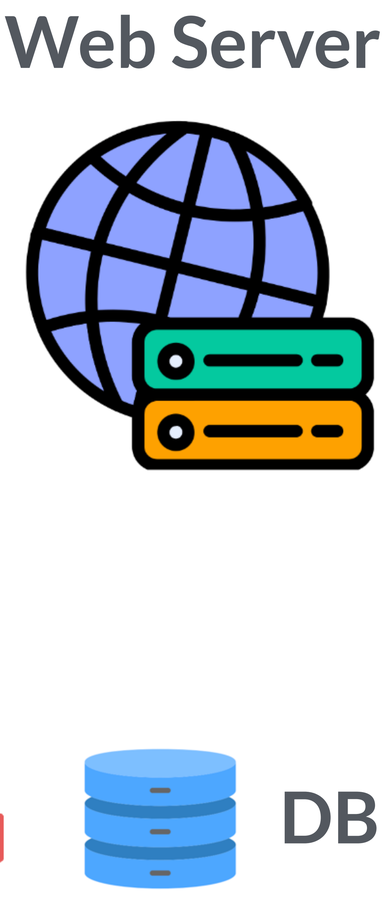
Multi-factor Authentication

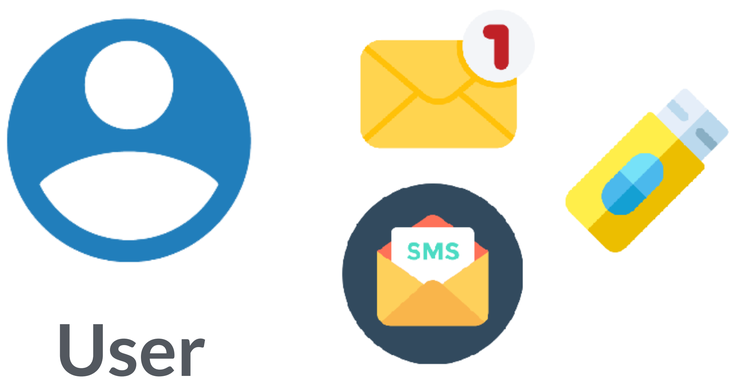


Multi-factor Authentication



Multi-factor Authentication





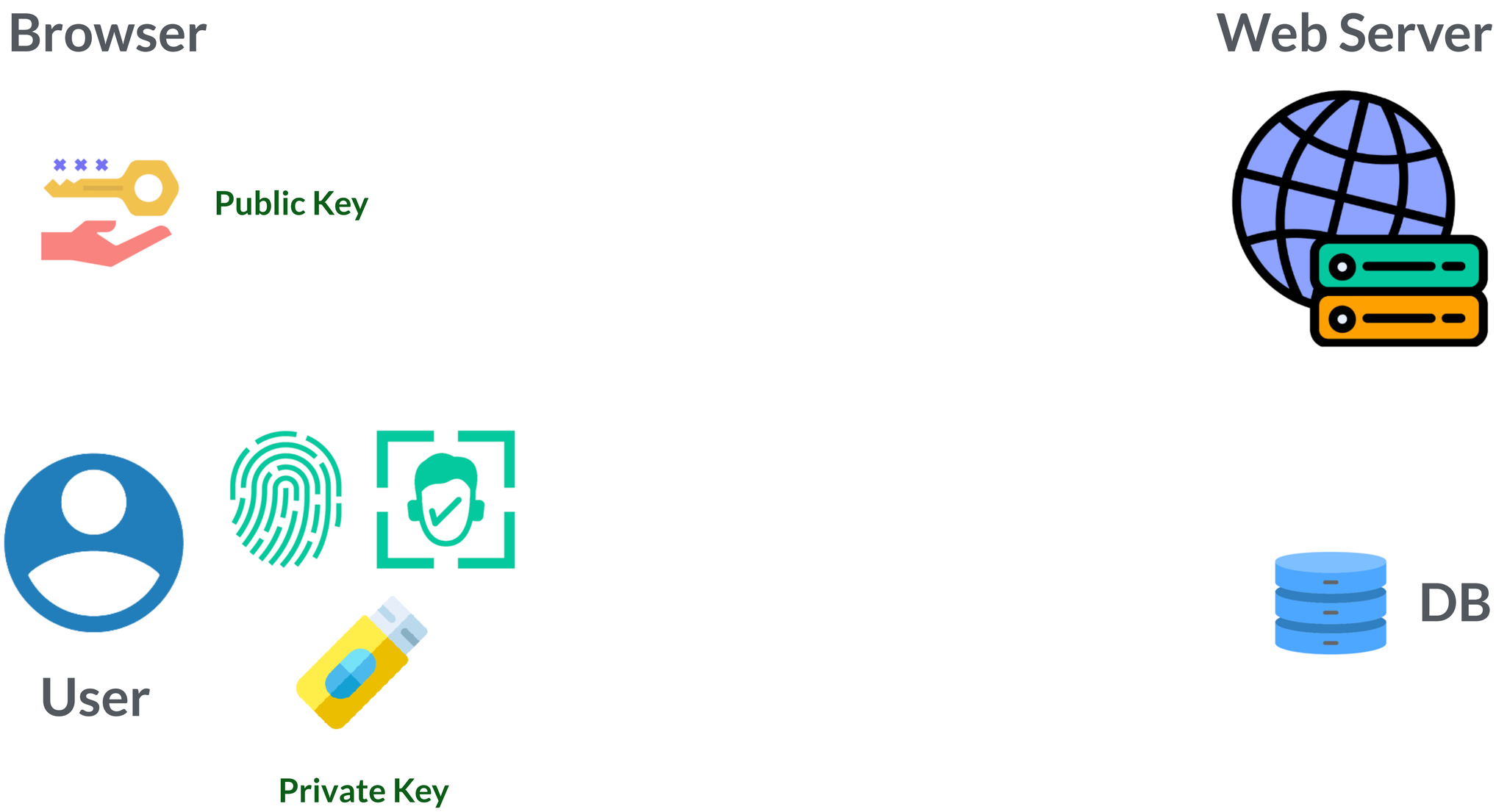
Multi-factor Authentication

User experience becomes a problem and the risk is still there are secrets and/or MF can be vulnerable

Passkeys

Passkeys

Passkeys



Passkeys

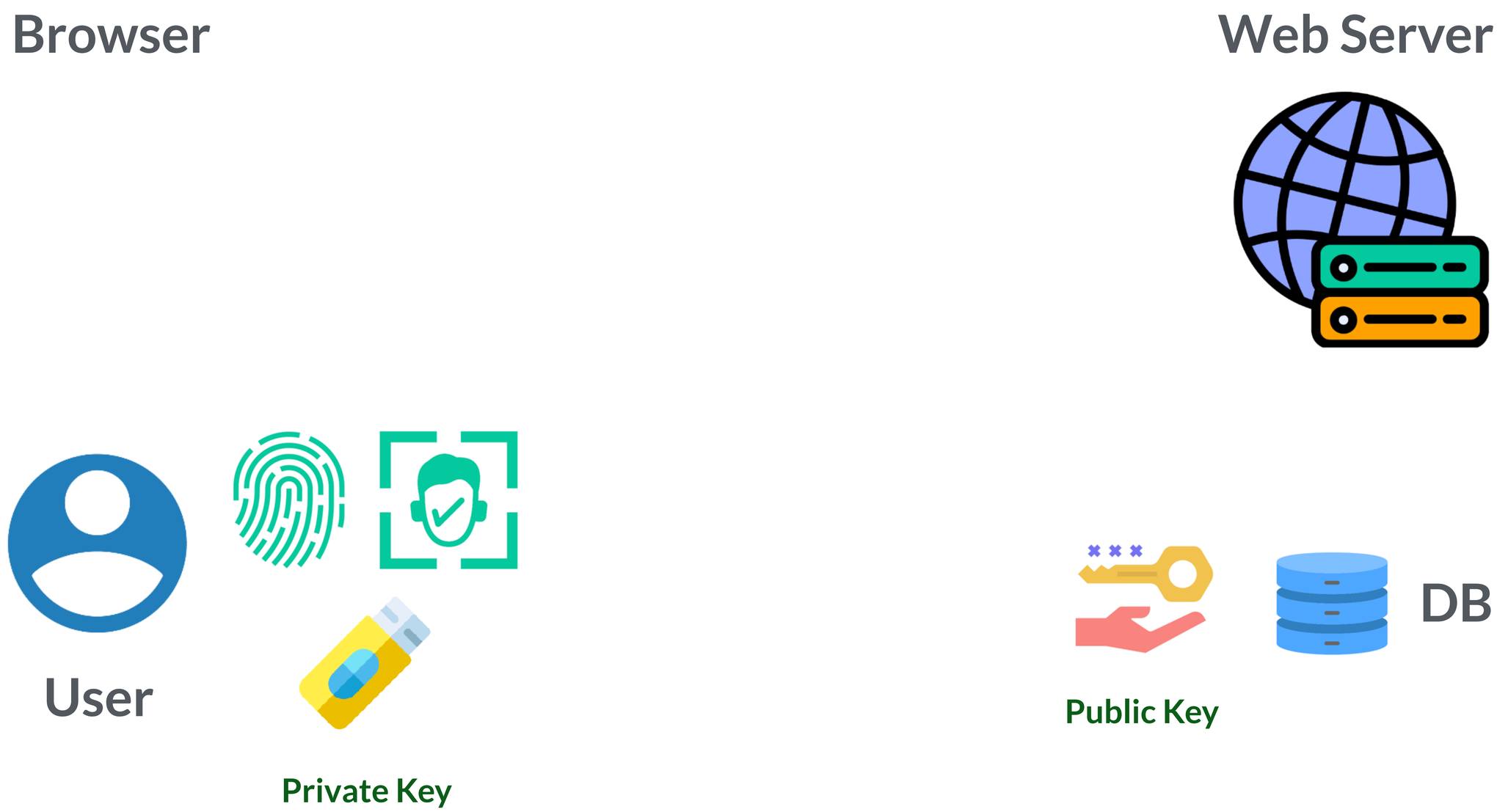
Browser

Web Server

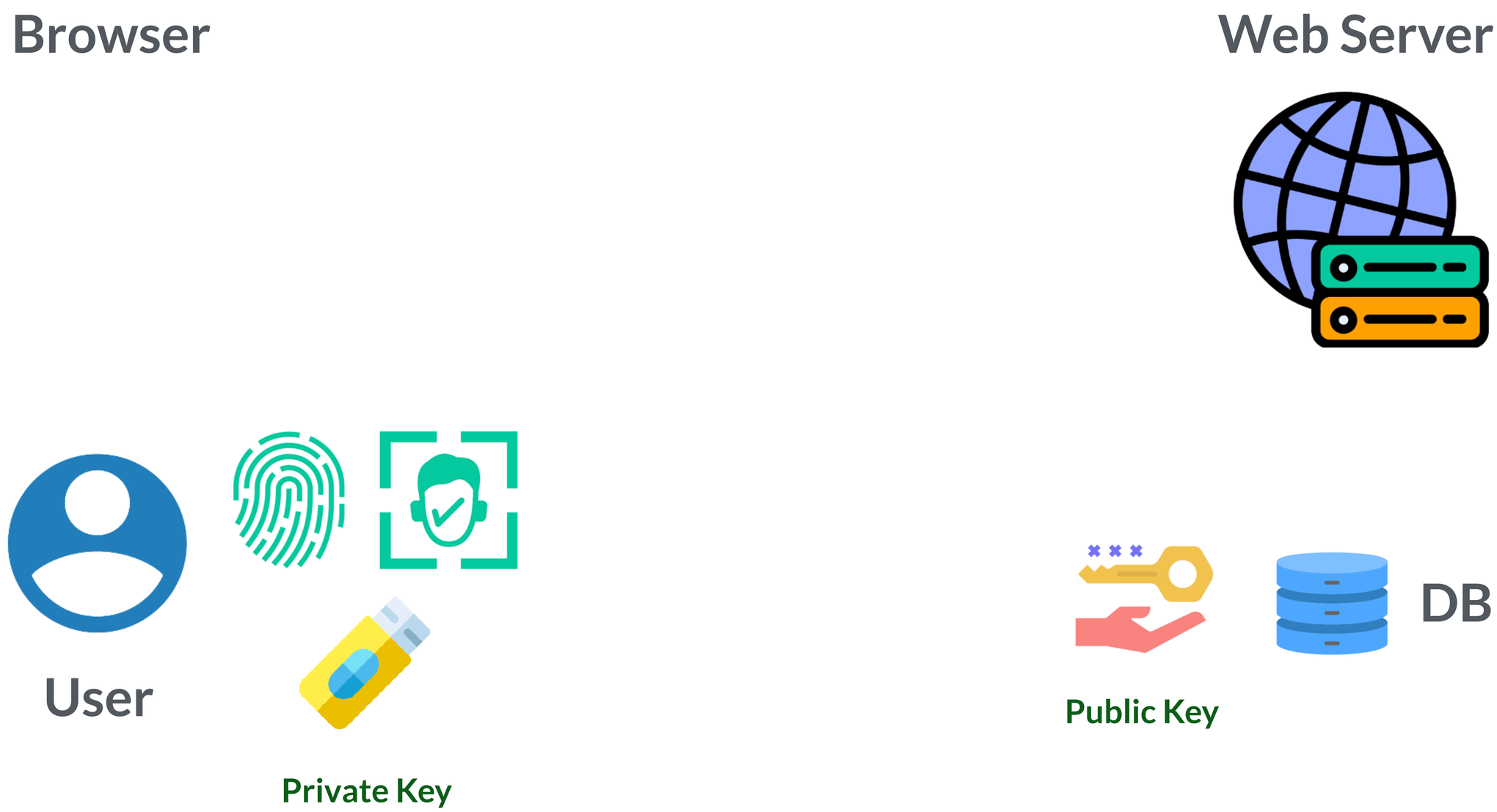
User

DB

Passkeys



Passkeys



Passkeys

Browser

Web Server

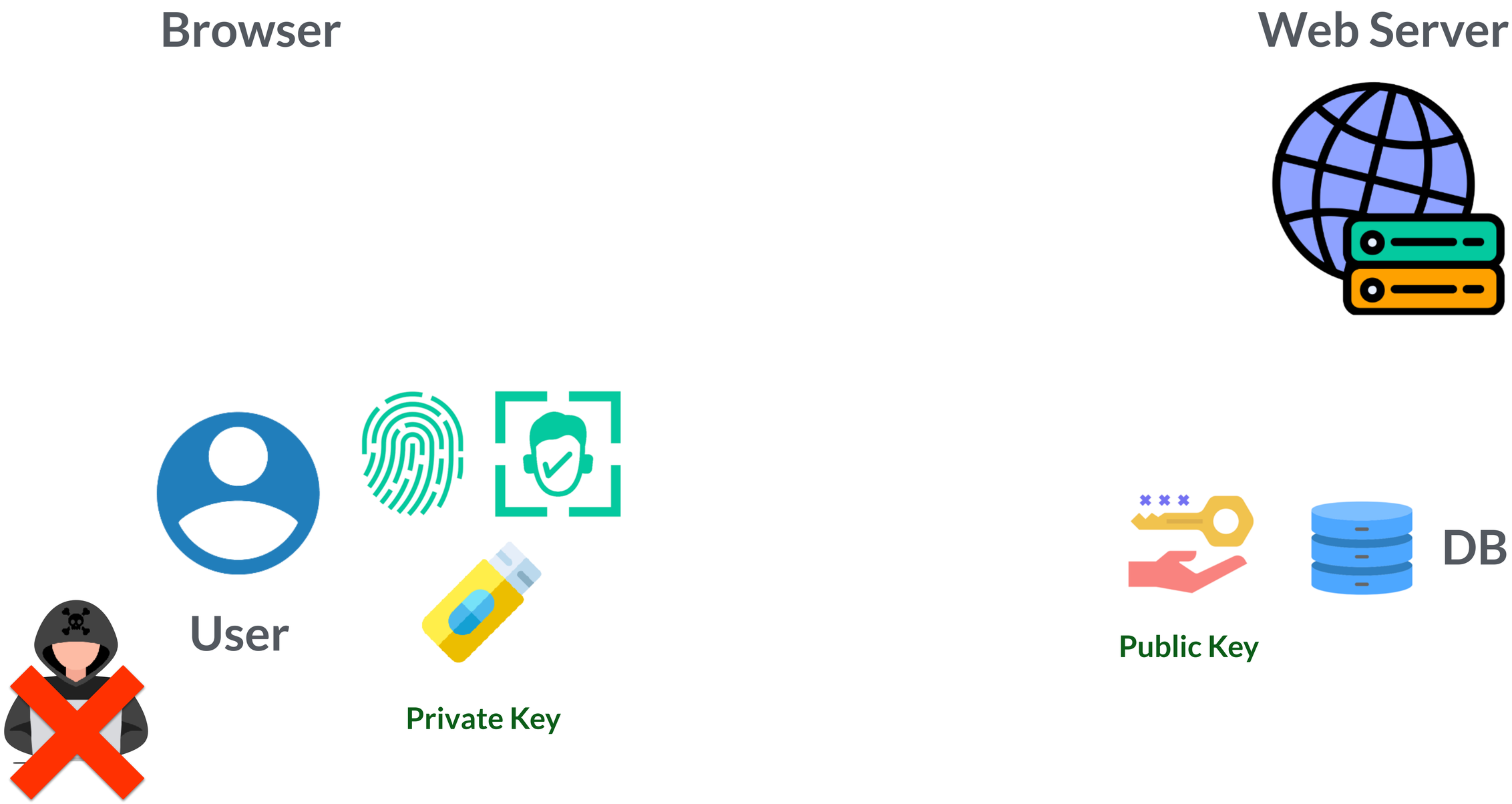
User

Private Key

DB

Public Key

Passkeys



Passkeys

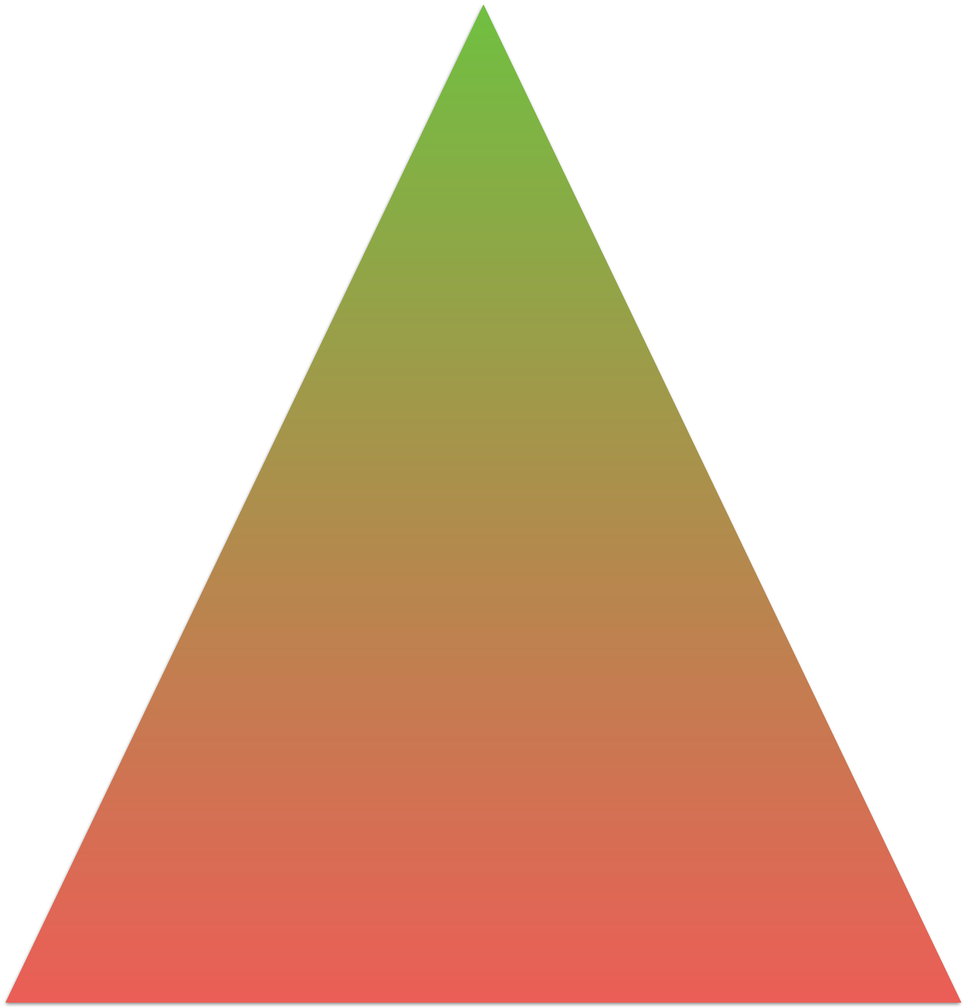
Based on WebAuthn API

- Multi-Factor Authentication
- Single-Factor Authentication

Keys can be stored

- On Device
- External hardware
- Cloud

Status



Passwordless Auth

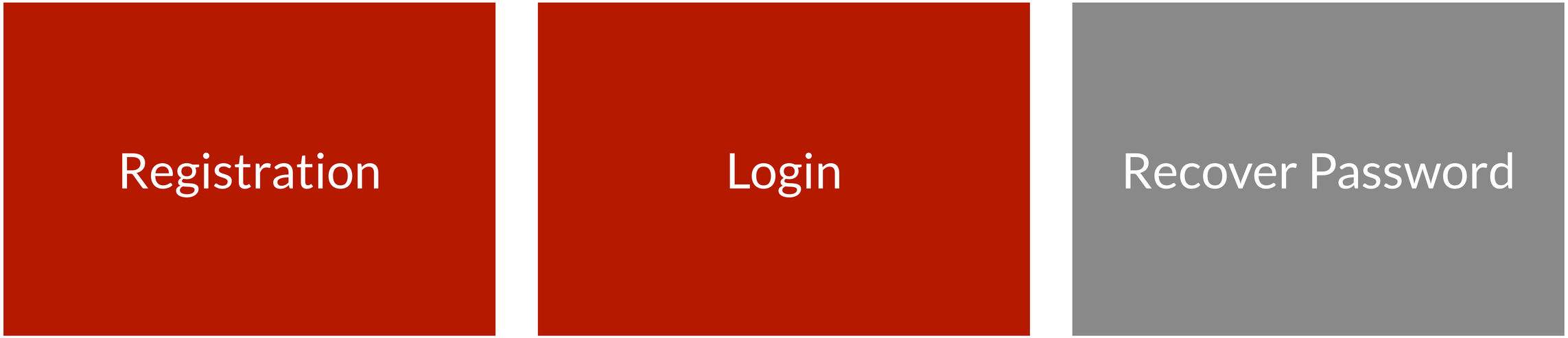
Multi-factor Auth

Form-based Auth

3

Classic Login Flow

Login Form Flow



Enhancing Login Forms

- Connected Labels for each element
- Don't use placeholder as labels
- Using HTML semantics
- On SPAs, form names different for registration and login forms
- Let the user make the password visible
- Help Password Managers with autocomplete HTML attributes
- Help Accessibility with aria-describedby attribute for instructions
- On SPAs, use submit form event and submission will be triggered by a pushState

Enhanced Login Form

index.html

```
<input type="password" autocomplete="new-password">

<input type="password" autocomplete="current-password">

<input type="text" autocomplete="name">

<input type="email" autocomplete="username">
```

Workshop time

FullStack Authentication

4

Data Storage and Auth APIs

Data Storage

E-mail or Username

Name

Password (hashed)

TODO:

Last time logged in

Last 99 login timestamps

Last 99 IP addresses

Code for recovering passwords

Multi-factor information

API endpoints

We will use HTTPS REST APIs using POST with a JSON body

/register

/login

Our code won't be production ready

There are much more to do in terms of security and data consistency! :)

Workshop time

5

Identifier-First Flow

Identifier-First Flow

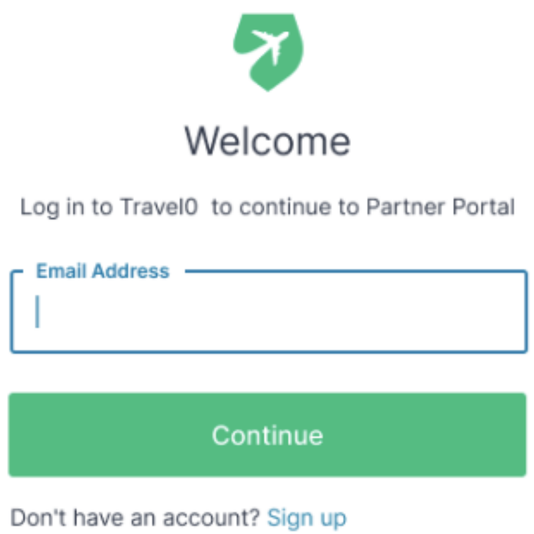
Instead of a login form with username and password:

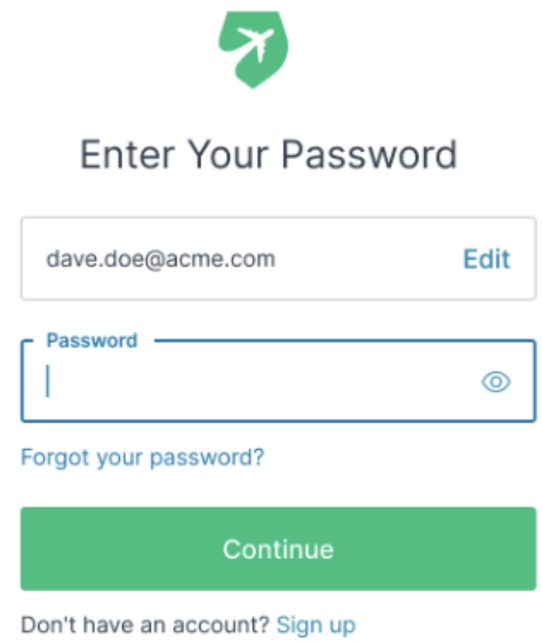
1- We first ask for identity (username)

2- We ask the browser about the login options for that user

3- We offer the user enter a password or login with other options

Identifier-First Login Forms





* images from Auth0 blog

Workshop time

Credential Management

It let us save and retrieve in the browser's password manager:

* Credentials (username/password)
* Federated Credentials
* Public/Private Keys

It let us implement auto login safely.

For credentials, it's Chromium-only.

Safari supports only public/private keys, used for WebAuthn API.

Credential Management API

script.js

```
const credentials = new PasswordCredential({
                    id: "admin",
                    password: "12345"
});

await navigator.credentials.store(credentials);
```

Credential Management API

script.js

```
const credentials = await navigator.credentials
                        .get({password: true});
```

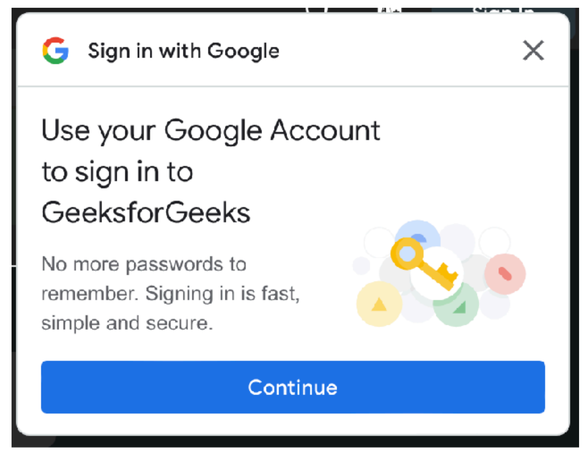
Workshop time

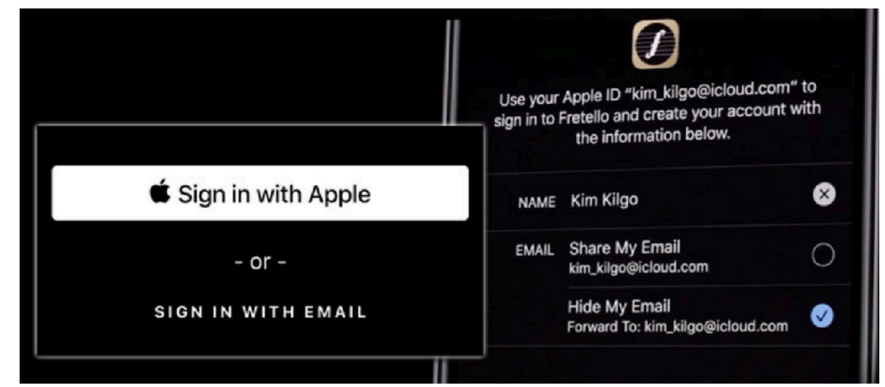
Federated Login

Using OAuth you can use many providers

Sign In with Google

Sign In with Apple





FullStack Authentication

6

Passkeys and WebAuthn

A multi-vendor effort

FIDO Alliance and W3C

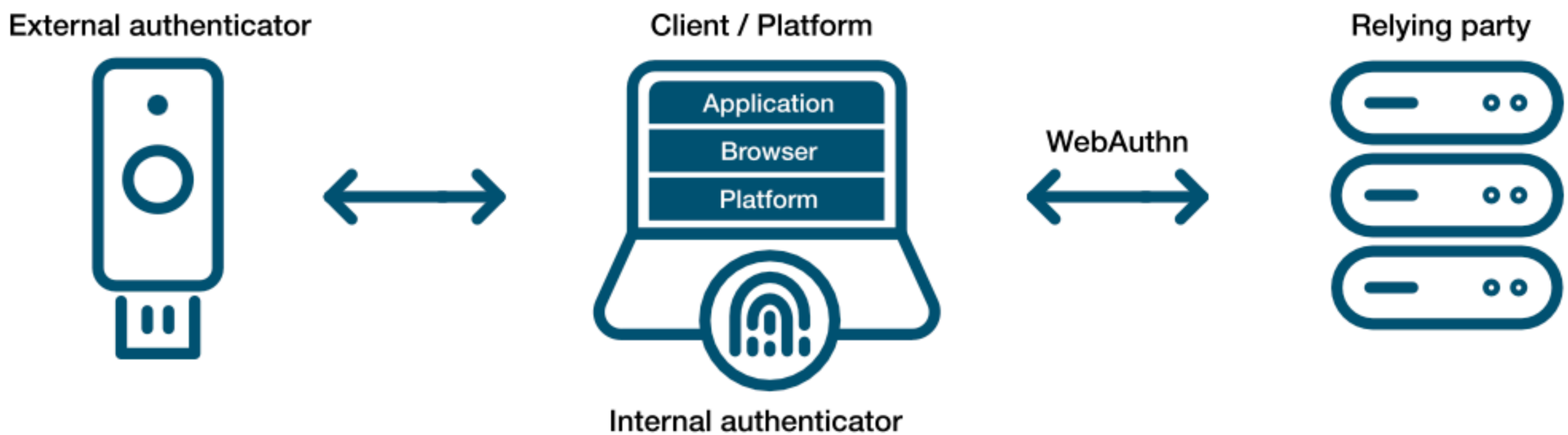
Store safely private keys while sending public keys for the server

It can work with FIDO2 and platform authenticators

It works on every browser with different techniques and abilities:

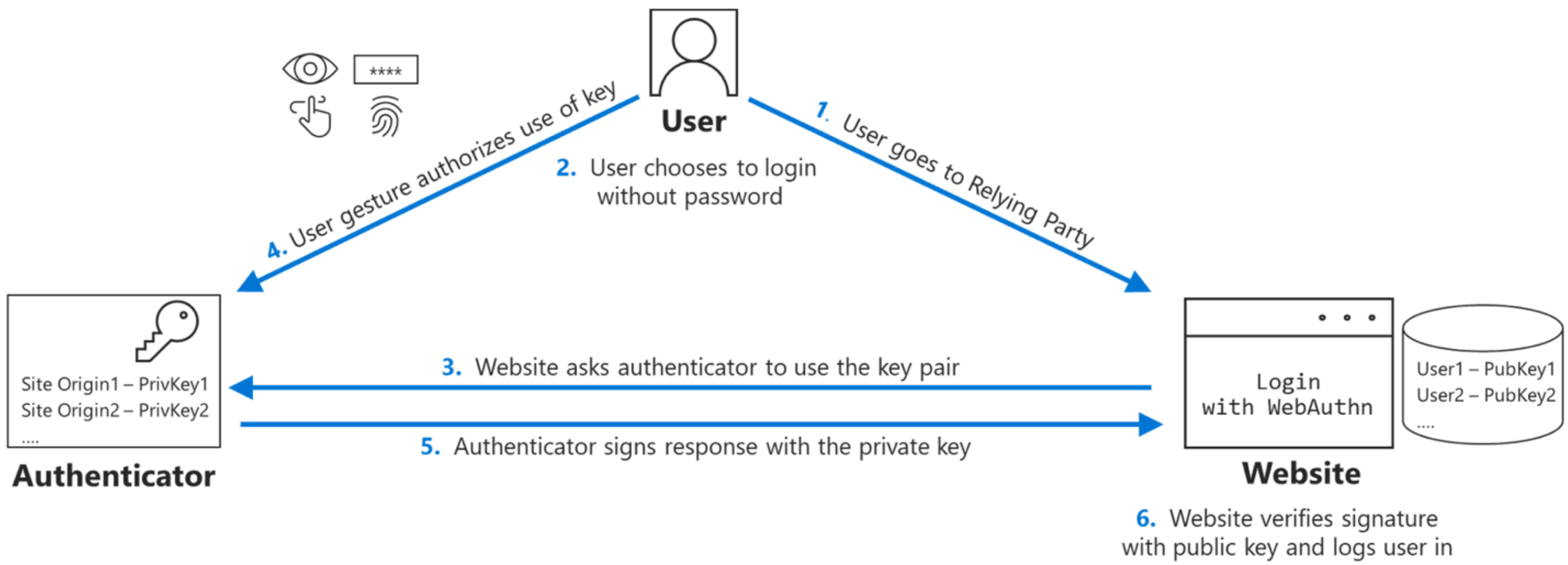
- **PIN-based keys**
- **FIDO2 USB keys** (such as Yubico)
- **Biometric Authenticators**
  (TouchID, FaceID, Windows Hello, Android)

WebAuthn



* images from yubico

WebAuthn



* images from Microsoft

WebAuthn Support

webauthn.me

Crafted by Auth0

TUTORIAL INFORMATION DEBUGGER

Roaming Authenticators

Roaming Authenticators are separate hardware authenticators, that can be connected to your device in a number of ways. The most common ones connect through USB, Bluetooth or NFC. These are most commonly security keys like Yubikeys or Titan Keys.

	Android 7+	iOS 14.5+	Windows 10	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	Yes
Safari	N/A	Yes	N/A	Yes	Yes	N/A
Firefox	No	Yes	Yes	Yes	Yes	Yes
Brave	No	Yes	Yes	Yes	Yes	Yes
Edge	No	No	Yes	Yes	Yes	Yes

WebAuthn Support

webauthn.me

Crafted by Auth0

TUTORIAL INFORMATION DEBUGGER

Platform Authenticators

Platform authenticators are built into your devices like computers and smartphone. They can often be unlocked using biometrics, a finger print with Touch ID, or your face with Windows Hello or Face ID.

	Android 7+	iOS 14.5+	Windows 10 *(with Windows Hello)*	macOS Catalina	macOS Big Sur	Desktop Linux
Chrome	Yes	Yes	Yes	Yes	Yes	-
Safari	N/A	Yes	N/A	No	Yes	N/A
Firefox	No	Yes	Yes	No	No	-
Brave	No	Yes	Yes	Yes	Yes	-
Edge	No	Yes	Yes	Yes	Yes	-

BEST BUY

Return to previous page

Sign In to Best Buy

Email Address

⚠ Please enter a valid email address.

Show password

Password

Forgot your password?

Sign In

Keep me signed in.

or

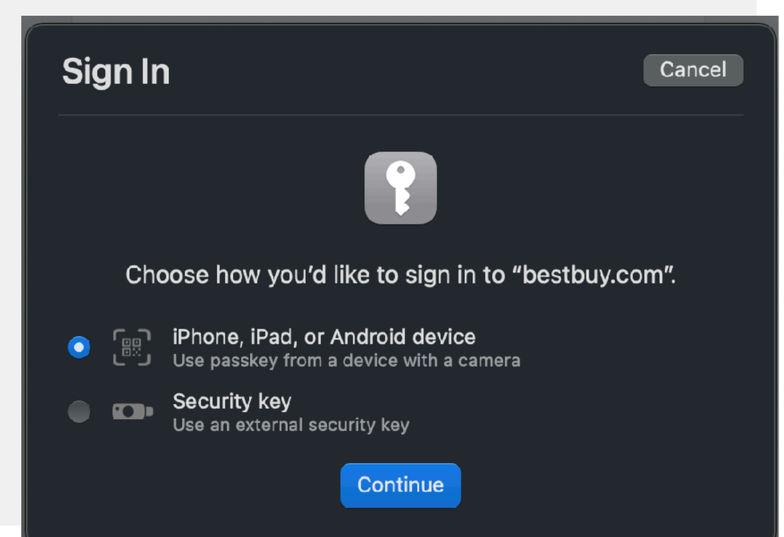
Sign in with a Passkey

Sign in with Apple

Sign in with Google

By continuing you agree to our Terms and Conditions, our Privacy Policy, and the My Best Buy™ Program Terms.

Don't have an account? Create an account

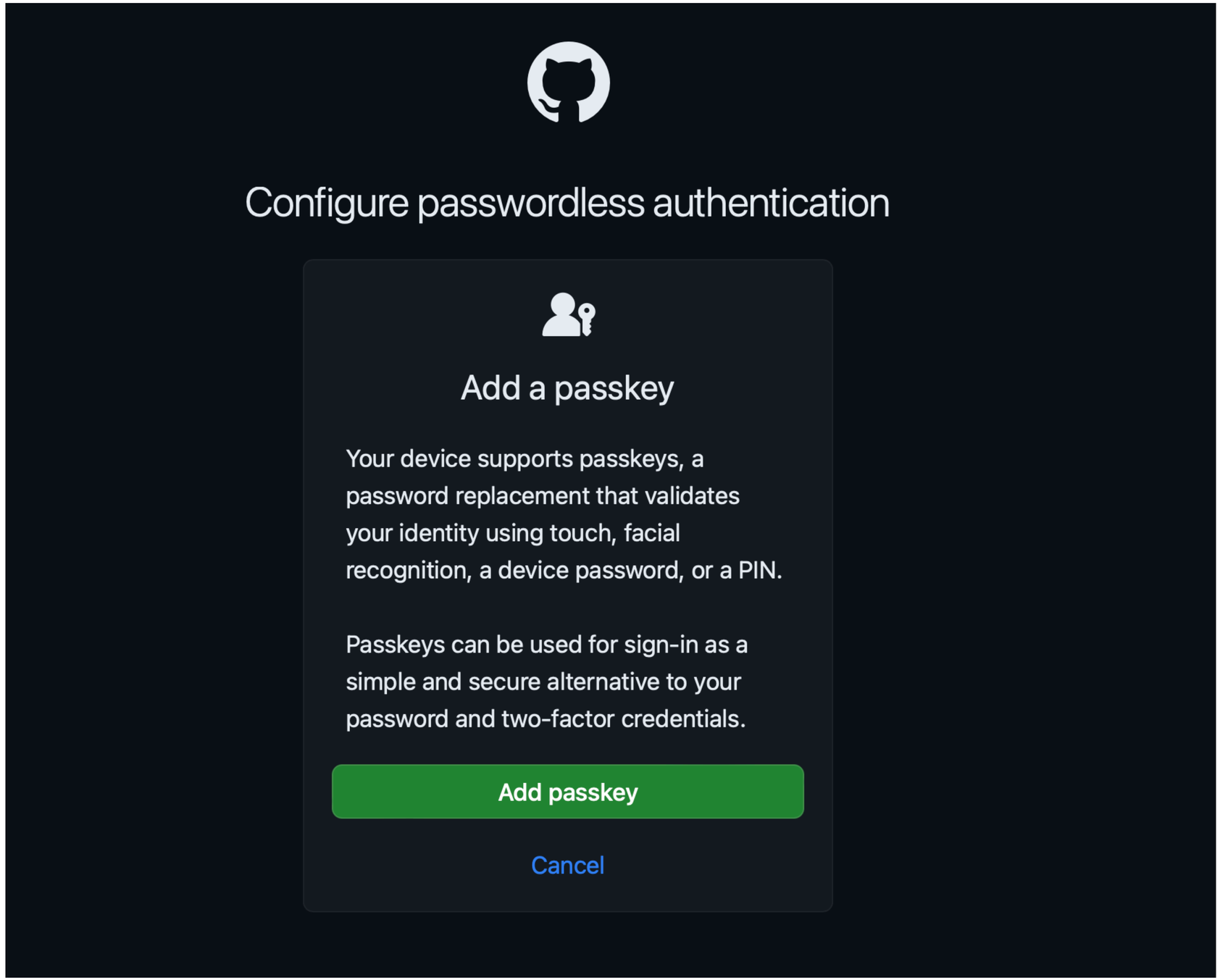


Passkeys

Passwordless sign-in with passkeys

Passkeys are a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN. Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.

Add a passkey


Configure passwordless authentication
Add a passkey
Your device supports passkeys, a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN.
Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.
Add passkey
Cancel

Cloud-based Passkey support

iOS and iPadOS 16+

macOS 13+, using Safari

(other browsers coming)

Android 9+

Windows 11 23H2

Passkeys

It's the new DNA of WebAuthn

The idea is to use WebAuthn as a First Factor

Authenticators are saving the keys (known as passkeys) in the cloud, so you can use them on different devices, and even share with other users

It includes a Conditional UI that lets the browser autocomplete a login form without the user typing anything

Advantages

Phishing-resistant

Security: Unique per service

Data Breach-resistant

Convenience: Quick access on Multidevices

PWAs on iOS, iPadOS and macOS

Important Actions

On-device Authentication

Remote Authentication

Share passkeys on trusted contacts

What do you need

Four web services

Implement the WebAuthn spec server-side (libraries available)

Implement the WebAuthn API client-side

Store n credentials per user

Make a decision:

- Use passkeys for MFA
- Use passkeys as SFA for a user
- Use passkeys as SFA without a user

WebAuth Flows

Registration

Authentication
(Login)

Library

We will be using
https://simplewebauthn.dev

It has a server and a client library

Workshop time

https://webauthn.io

Workshop time

7

Going Passwordless

Passwordless Options

Magic Links

OTP

Passkeys

BEST BUY

Return to previous page

Sign In to Best Buy

Email Address

⚠ Please enter a valid email address.

Show password

Password

Forgot your password?

Sign In

Keep me signed in.

or

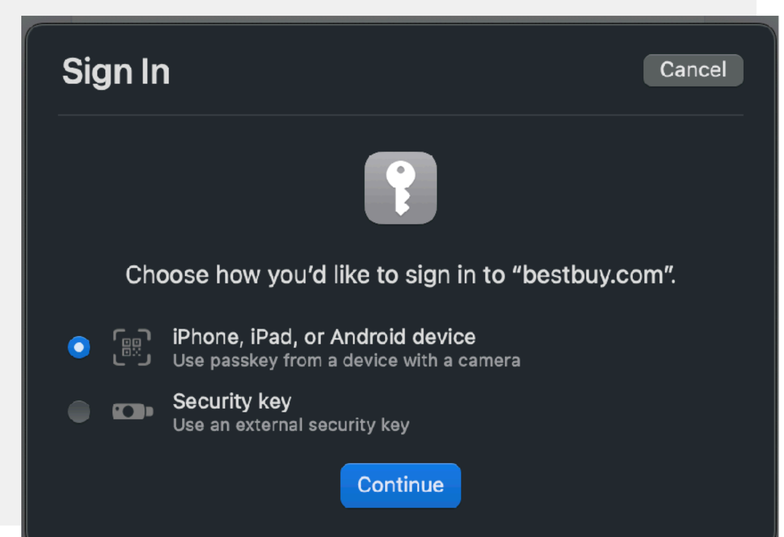
Sign in with a Passkey

Sign in with Apple

Sign in with Google

By continuing you agree to our Terms and Conditions, our Privacy Policy, and the My Best Buy™ Program Terms.

Don't have an account? Create an account

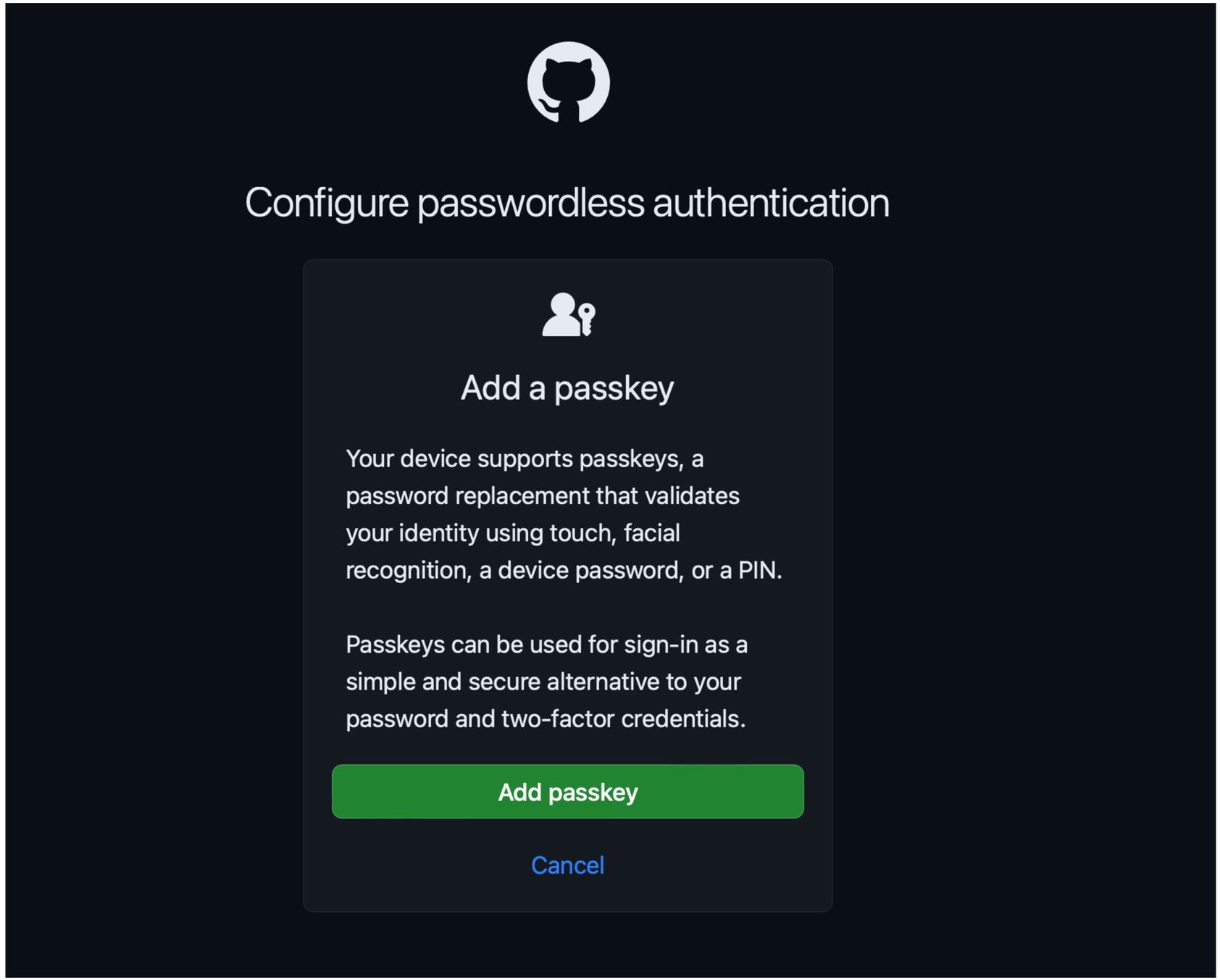


Passkeys

Passwordless sign-in with passkeys

Passkeys are a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN. Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.

Add a passkey


Configure passwordless authentication
Add a passkey
Your device supports passkeys, a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN.
Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.
Add passkey
Cancel

Workshop time

https://passkeys.io

FullStack Authentication

8

Best Practices

Native Apps

There are ways to connect your login credentials between the web and native

For password managers

For Passkeys

Handshake between your site and native app

Ideas

Keep user's destination after login

Always confirm user emails

Ask the user about autologin

Check Privacy's legislation

Security is too important

Test your login UX flows

Project TODO

- Validations
- Better database integrity
- Forget Password Flow
- Confirm email on registration
- Federated Logins
- Magic Link login
- Passkeys autoregistration

What we've covered

- Authentication
- State of Techniques
- Login Forms
- New Flows
- Data Structure
- Web Services
- Web Authentication
- Passkeys

THANKS! 🤗

Implementing User Authentication with Passkeys

MAXIMILIANO FIRTMAN

Slides and project open source thanks to FrontendMasters

FIRT.DEV