Maximiliano Firtman
@firt firt.dev

Implementing User Authentication with PASSKEYS

MAXIMILIANO FIRTMAN

MOBILE+WEB DEVELOPER

AUTHOR

13 books and +70 courses

@FIRT . FIRT.DEV

Frontend Masters

PLURALSIGHT

LinkedIn Learning

awwwards.academy

Learn PWA!

Search

000 Learn PWA ✓

001 Progressive Web Apps ✓

002 Getting started ✓

003 Foundations ✓

004 App design ✓

005 Assets and data

006 Service workers

007 Caching

008 Serving

009 Workbox

010 Offline data

web.dev/learn/pwa

000

Learn PWA

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

Welcome to Learn Progressive Web Apps!

Welcome to Learn Progressive Web Apps!

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.

Let’s Start!

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:

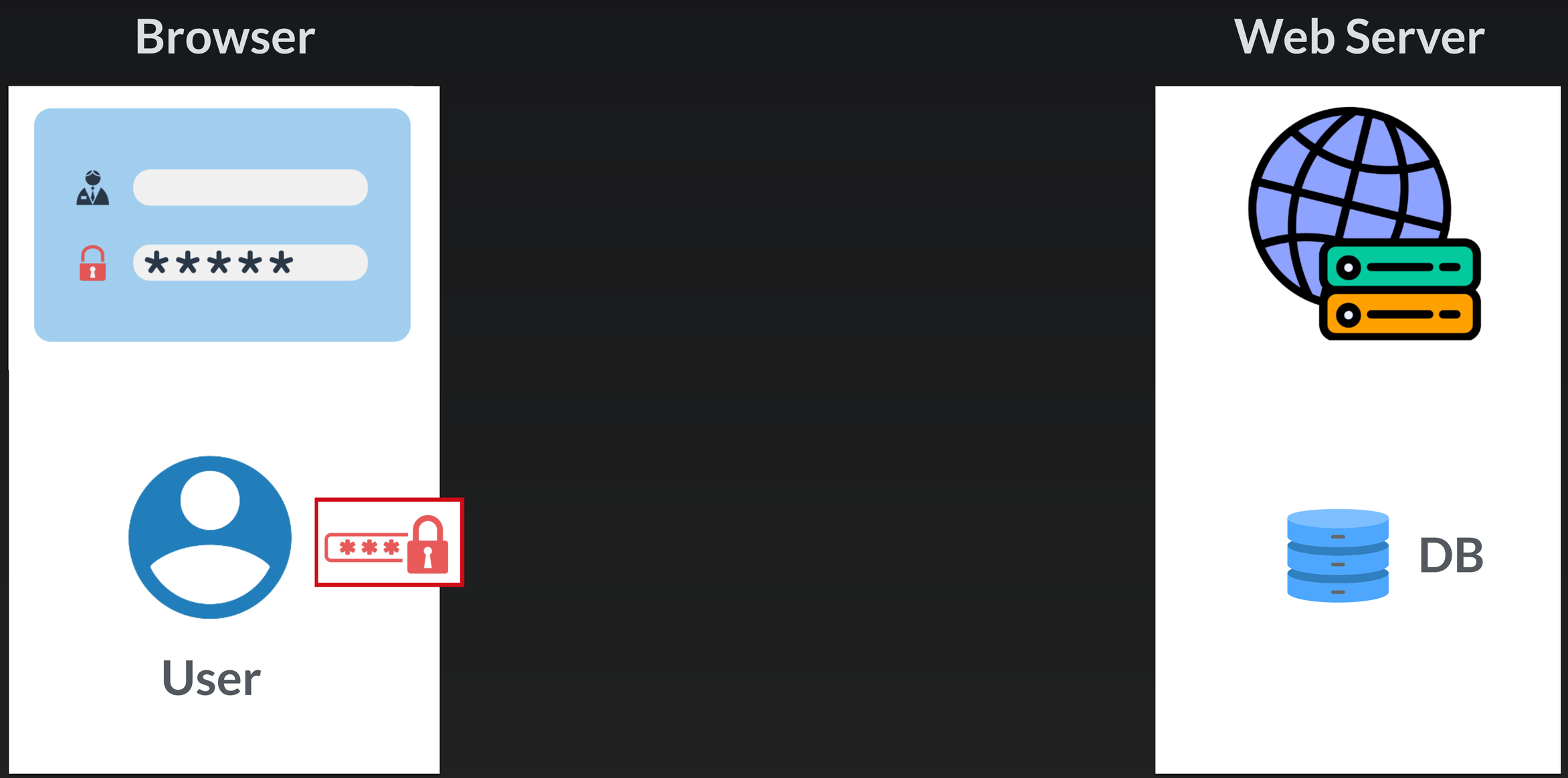
Join

Thousands of designers, writers & programmers agree.

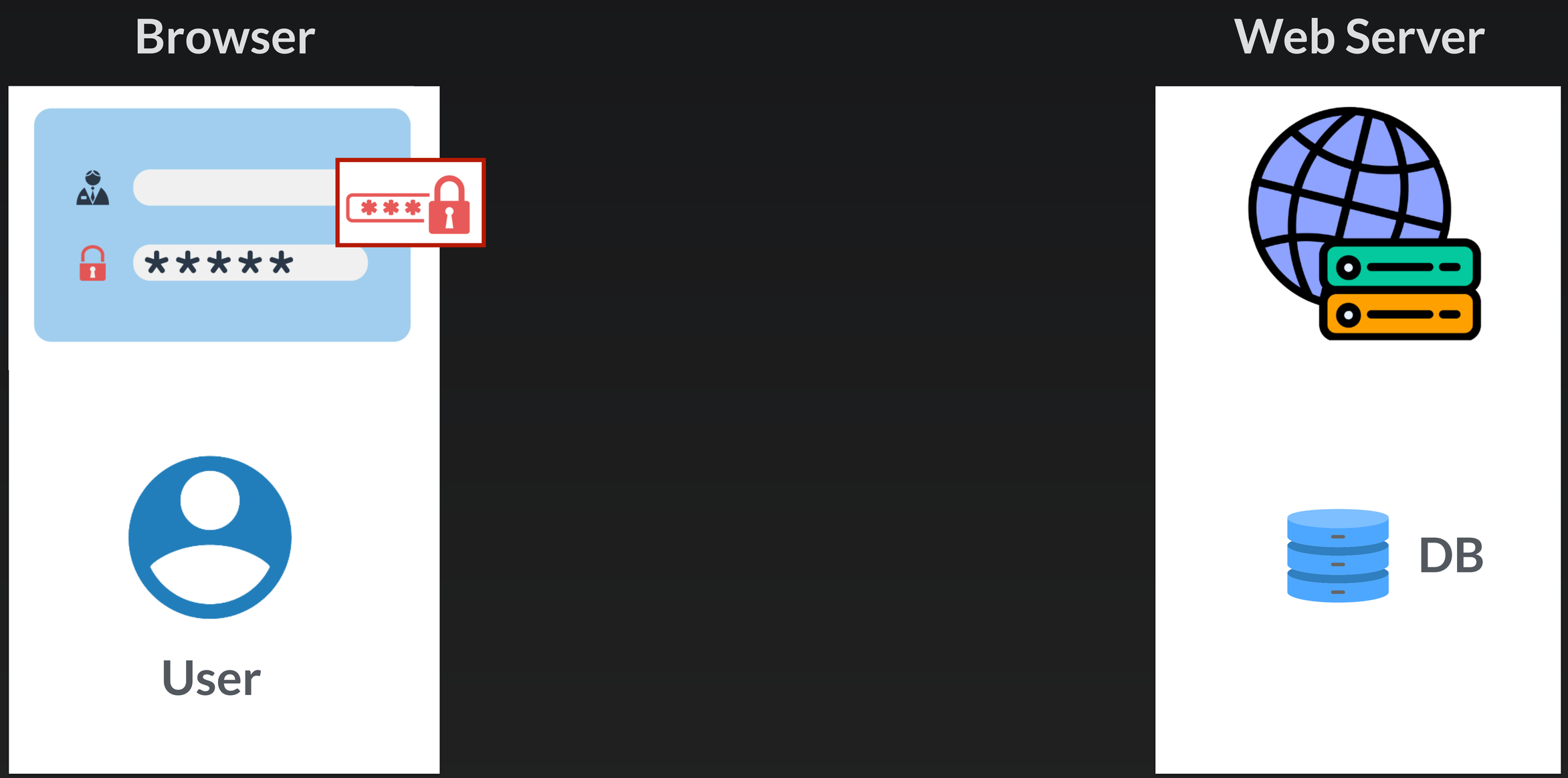
A List Apart is good reading for people who make websites.

© 1999 Jeffrey Zeldman and Brian M. Platz.

HTTP Auth / Login Forms

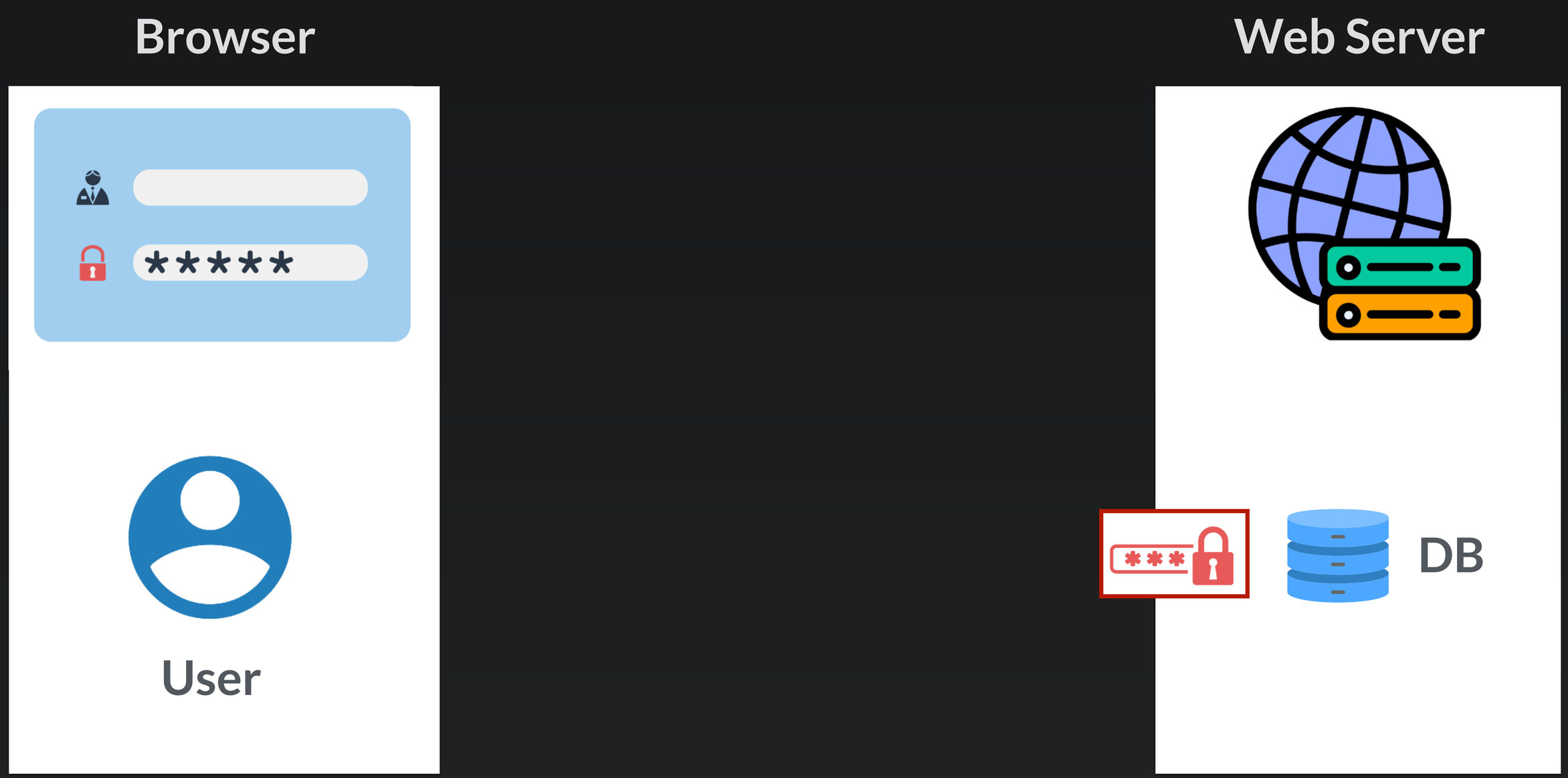


HTTP Auth / Login Forms

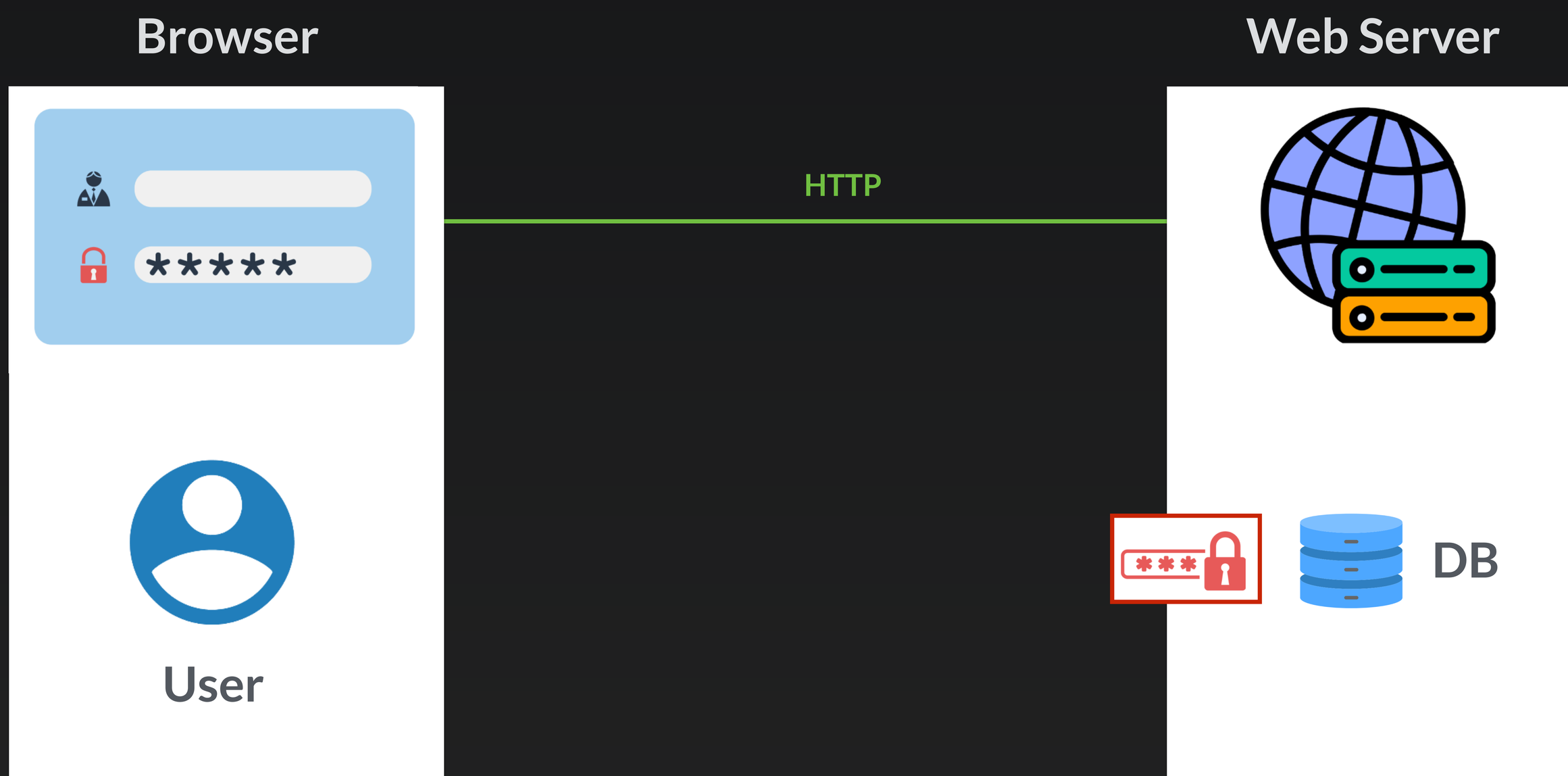


HTTP Auth / Login Forms

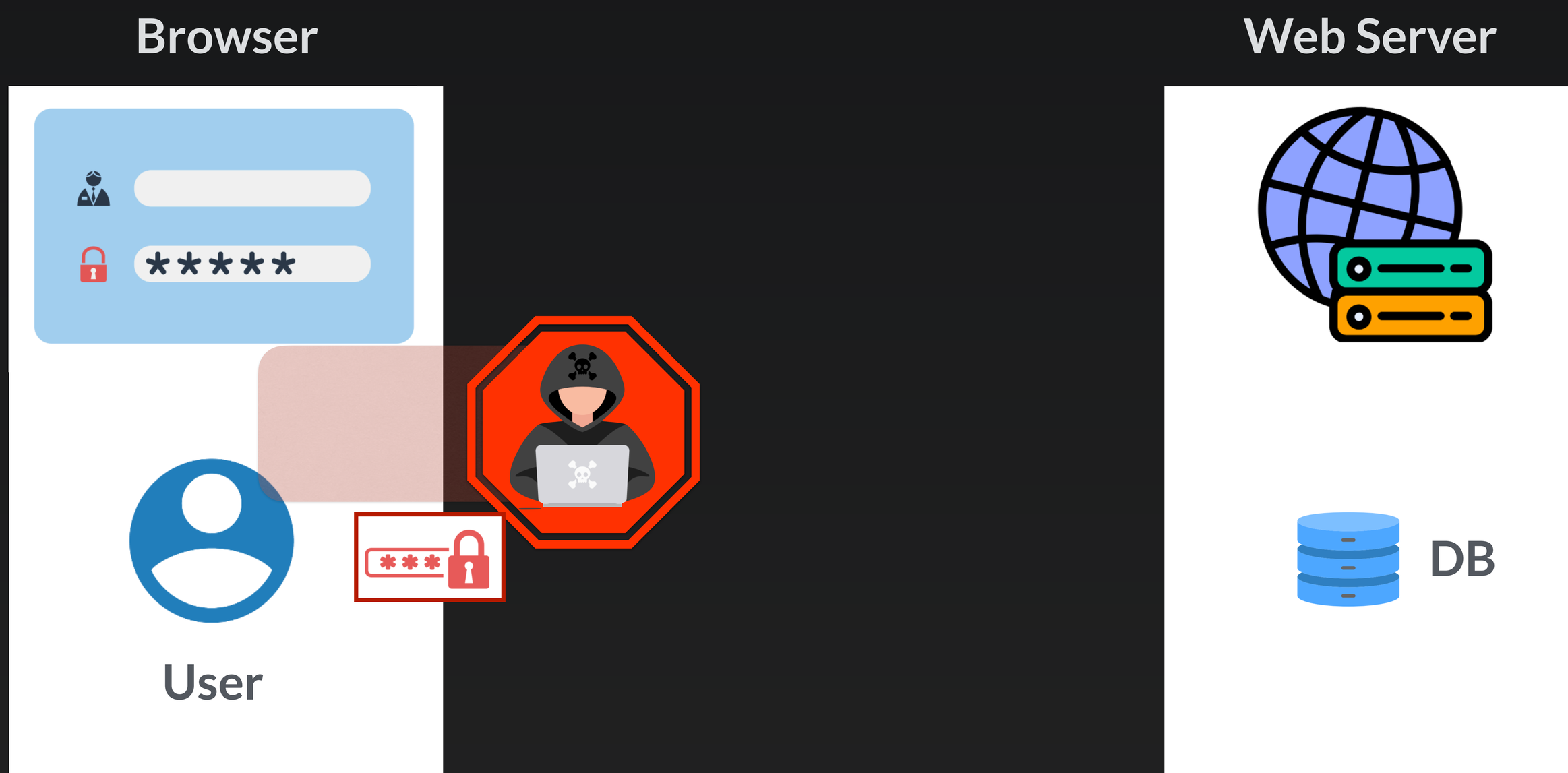
HTTP Auth / Login Forms



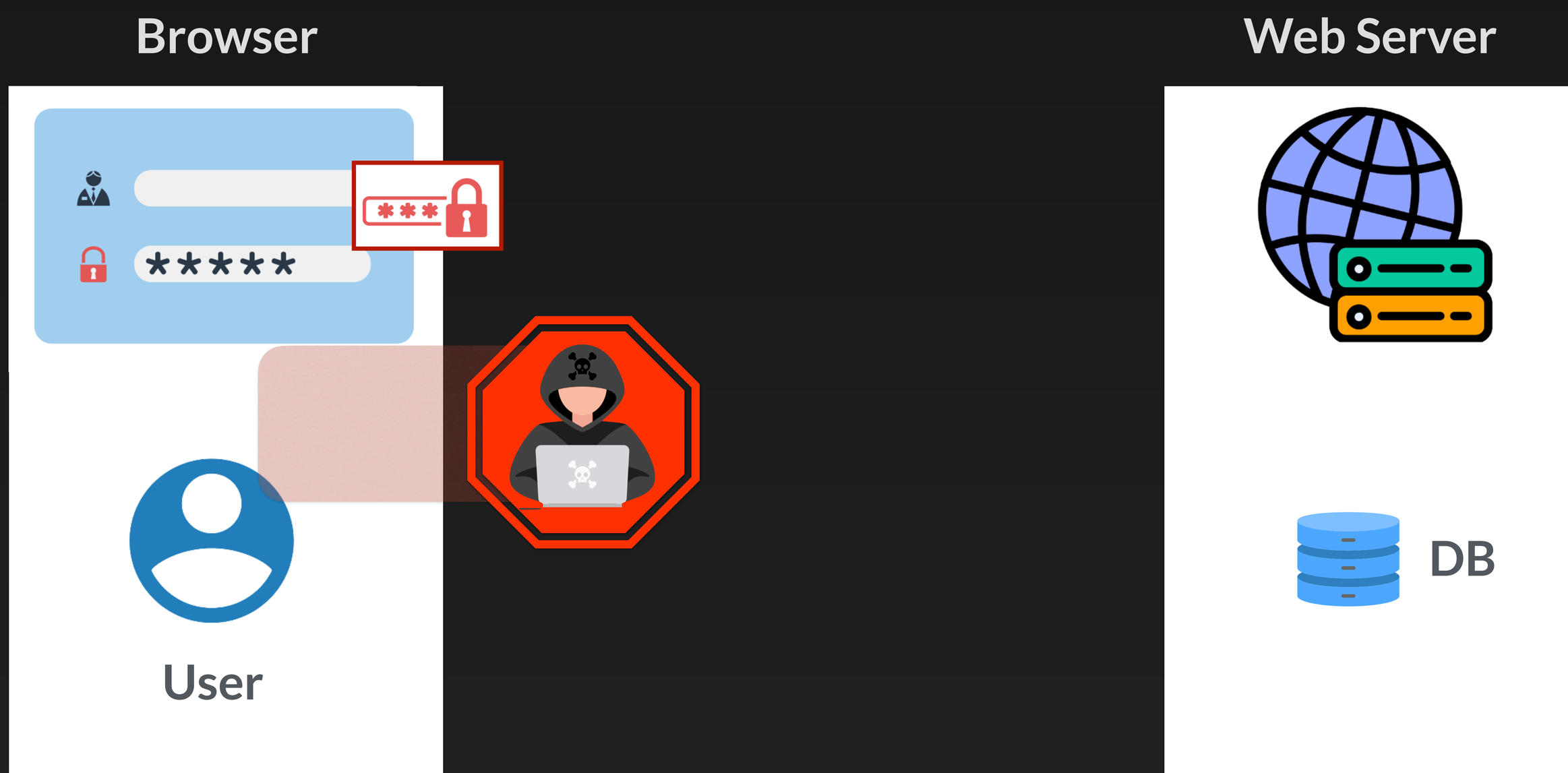
HTTP Auth / Login Forms



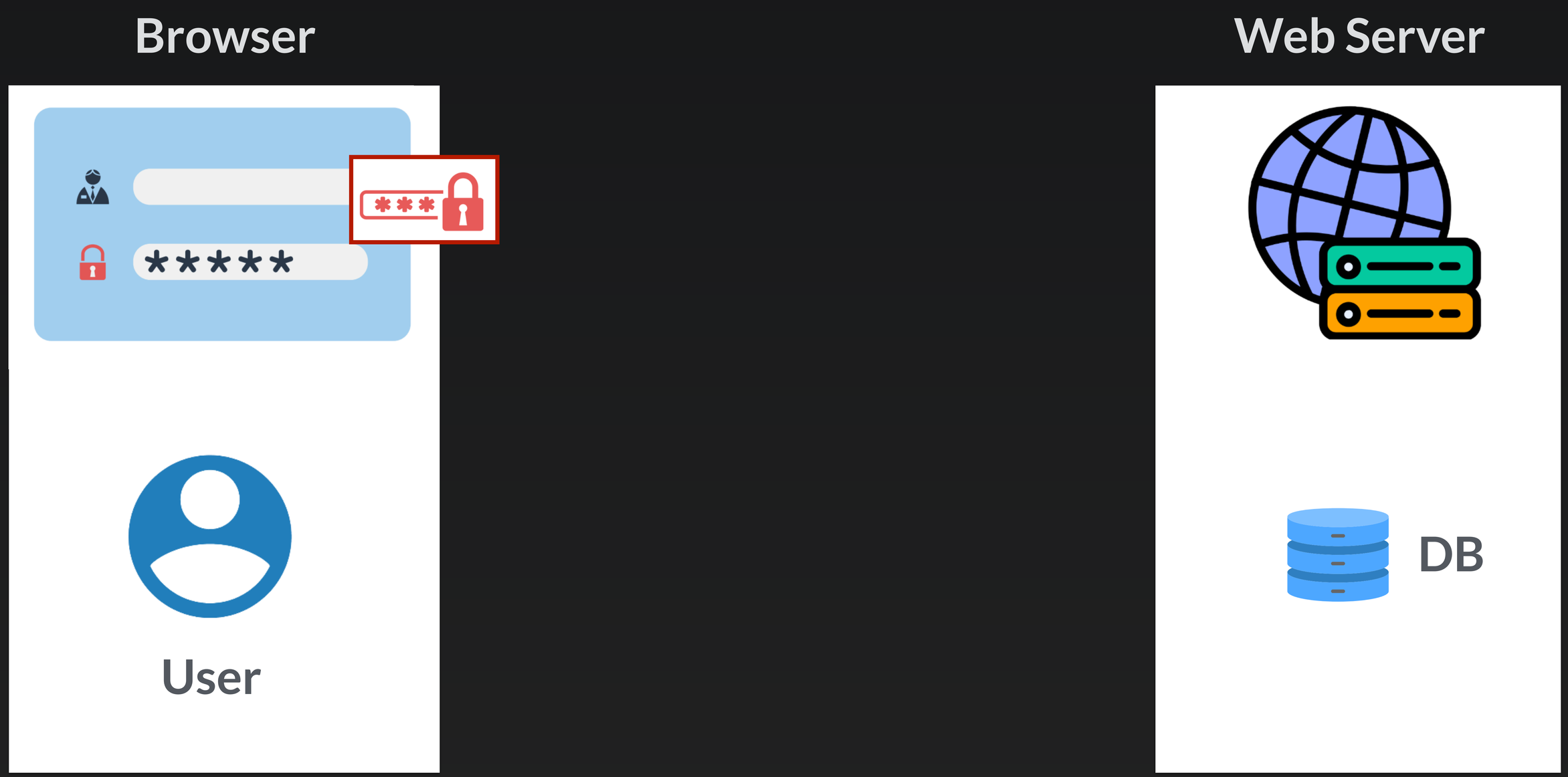
HTTP Auth / Login Forms



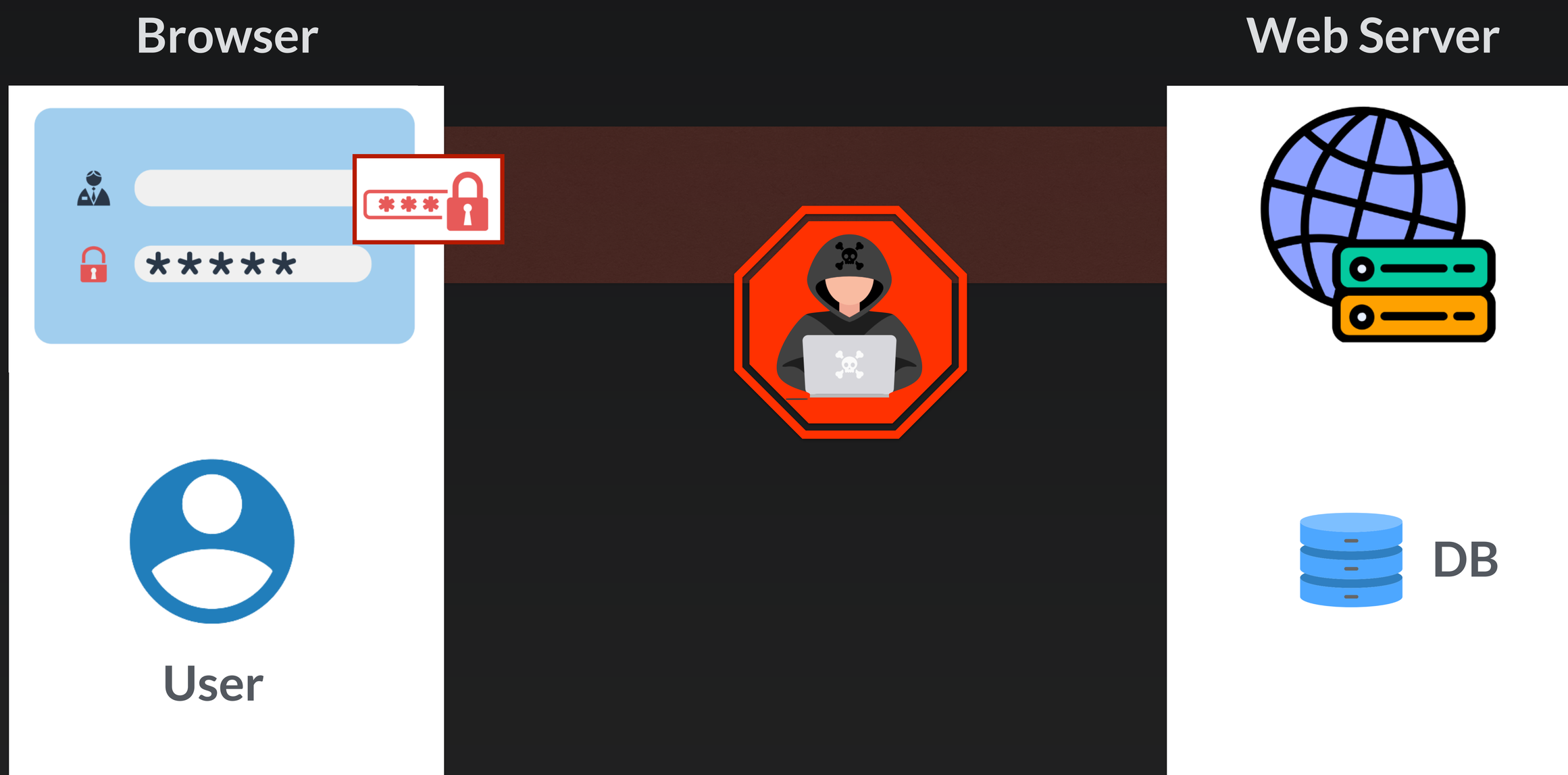
HTTP Auth / Login Forms



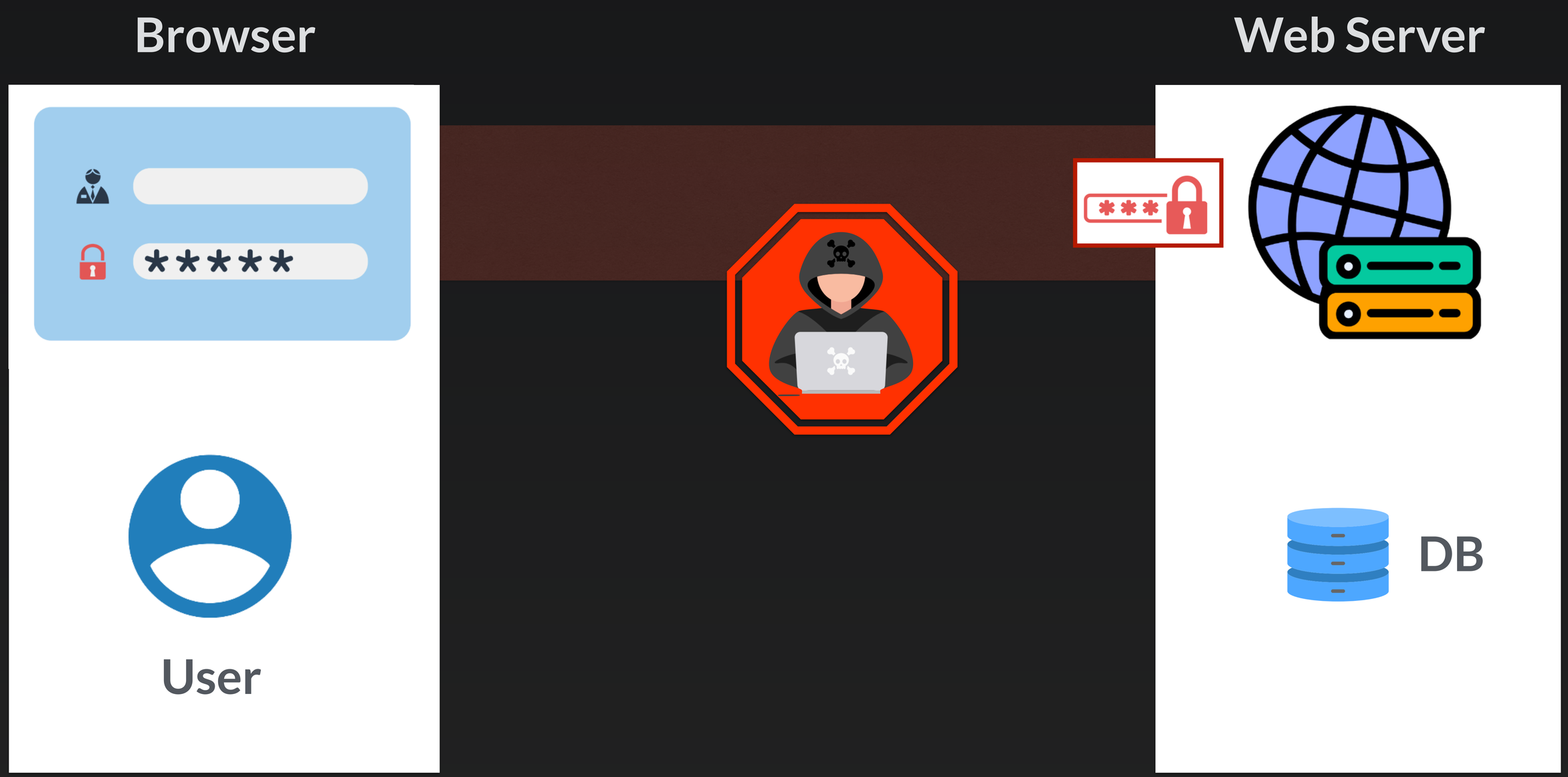
HTTP Auth / Login Forms



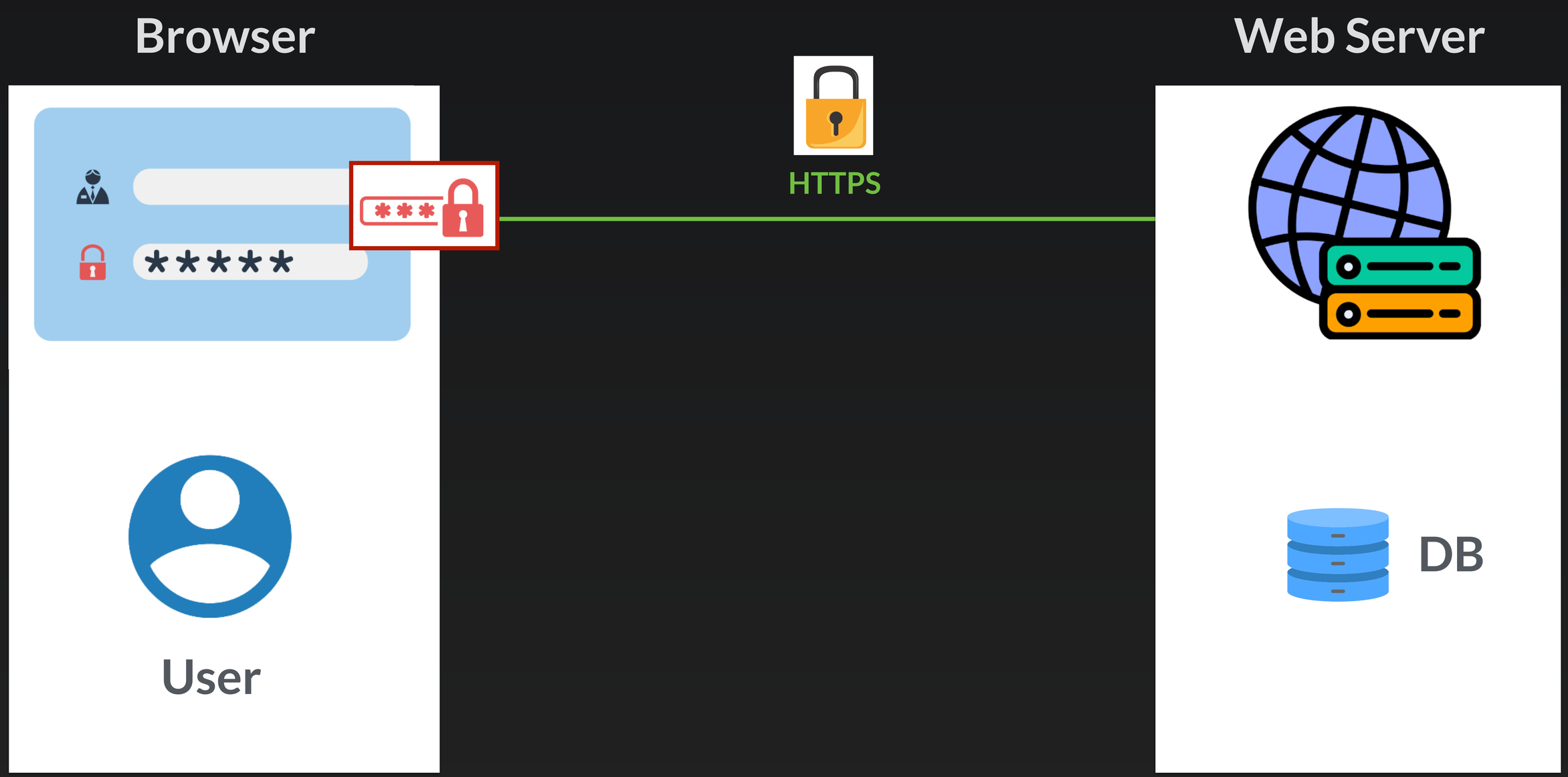
HTTP Auth / Login Forms

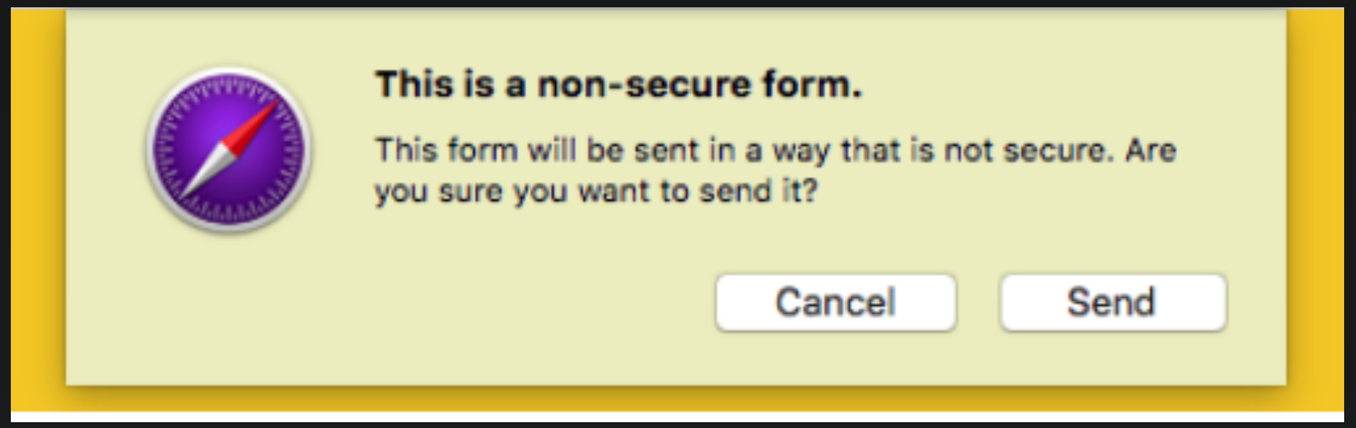


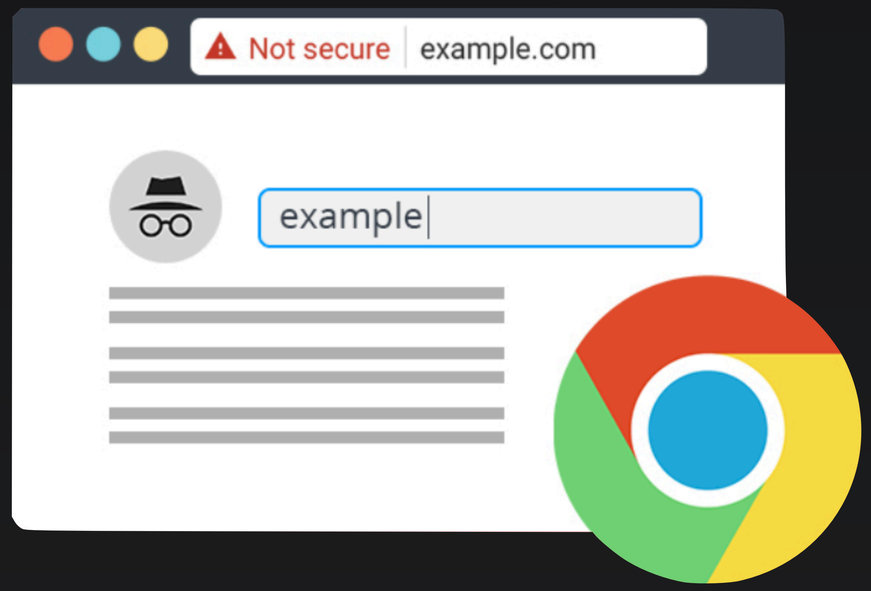
HTTP Auth / Login Forms

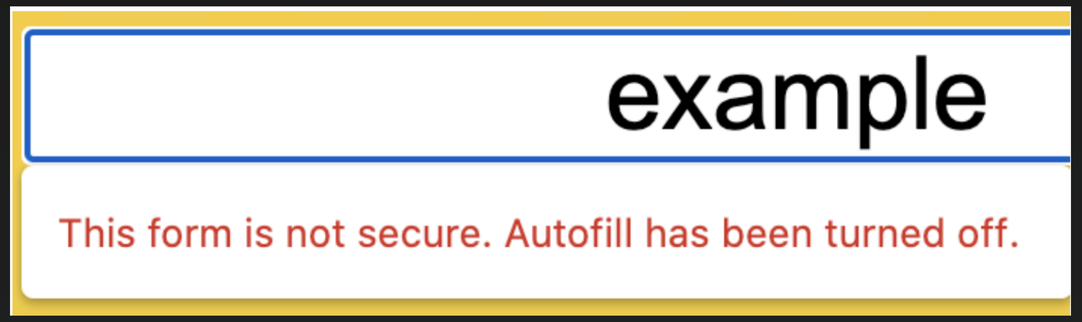


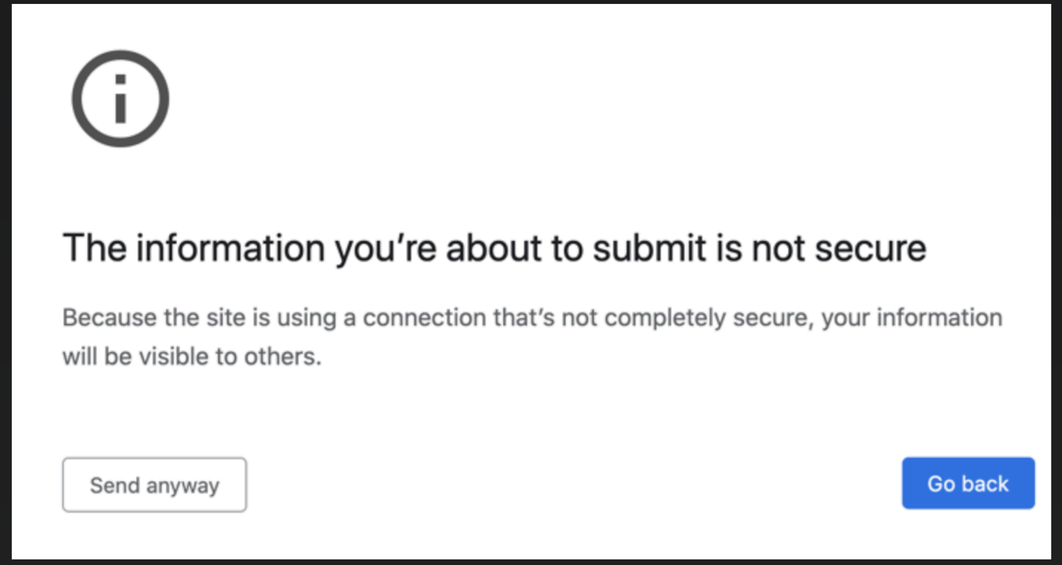
HTTP Auth / Login Forms



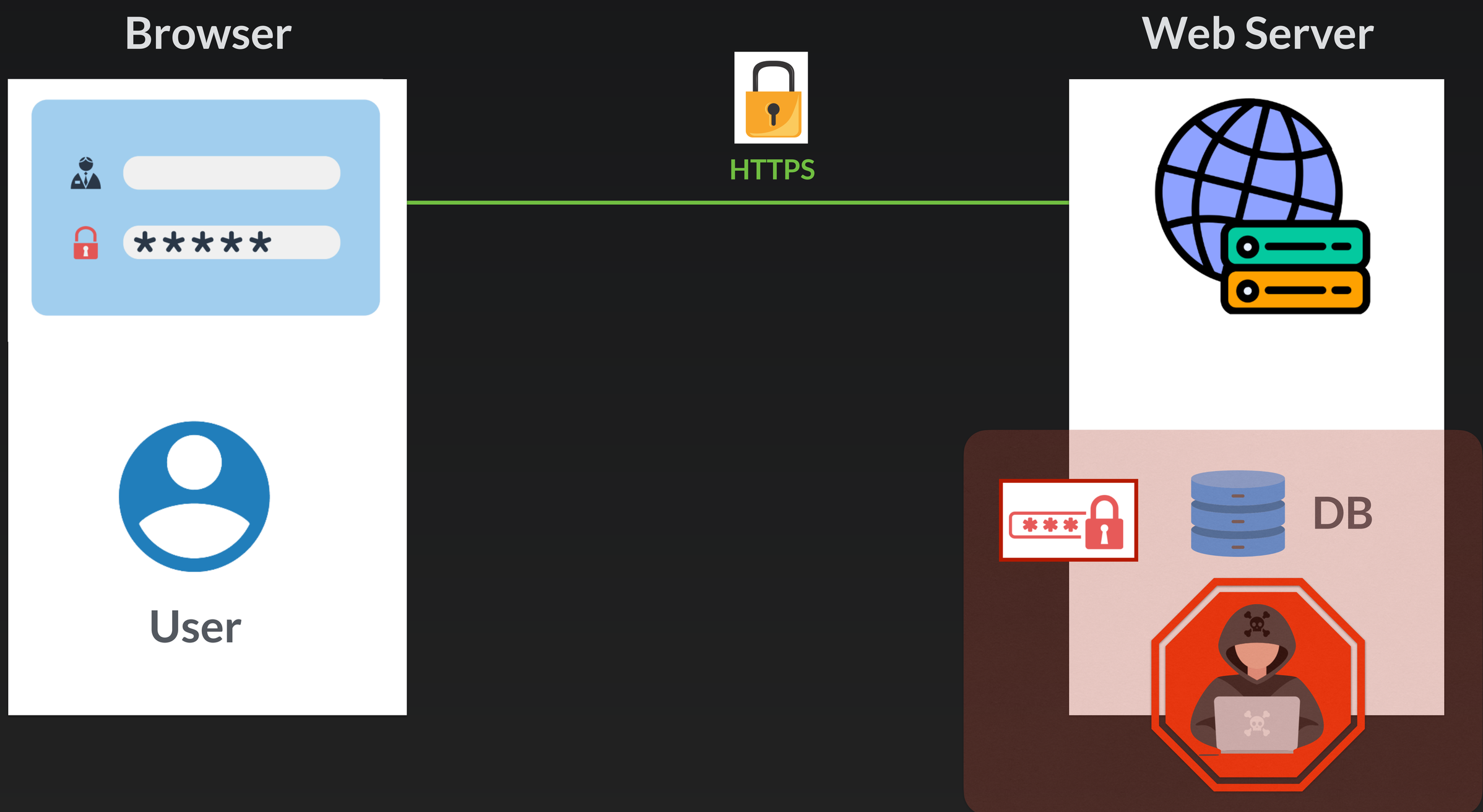

This is a non-secure form.
This form will be sent in a way that is not secure. Are you sure you want to send it?
Cancel
Send


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

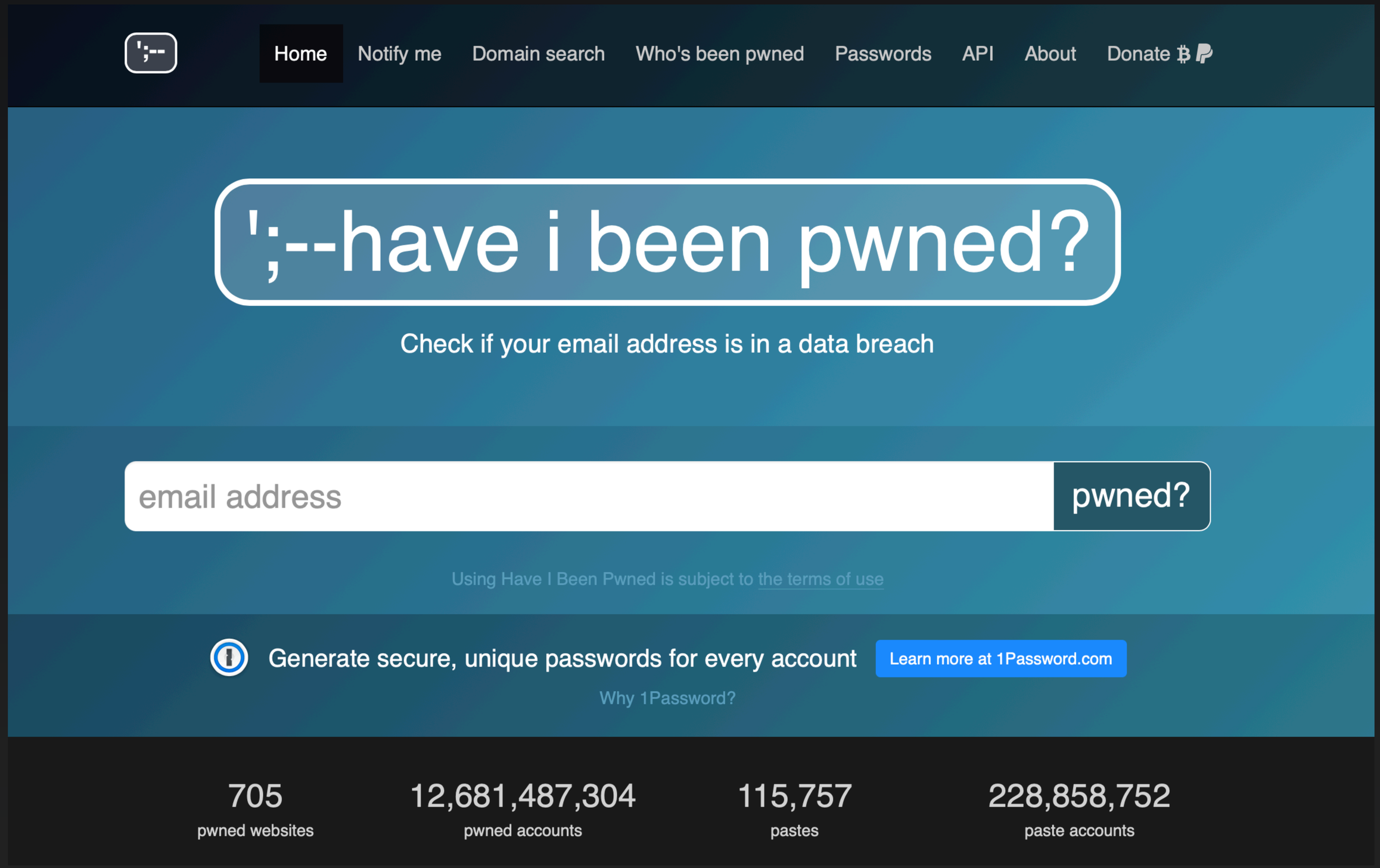
HTTP Auth / Login Forms

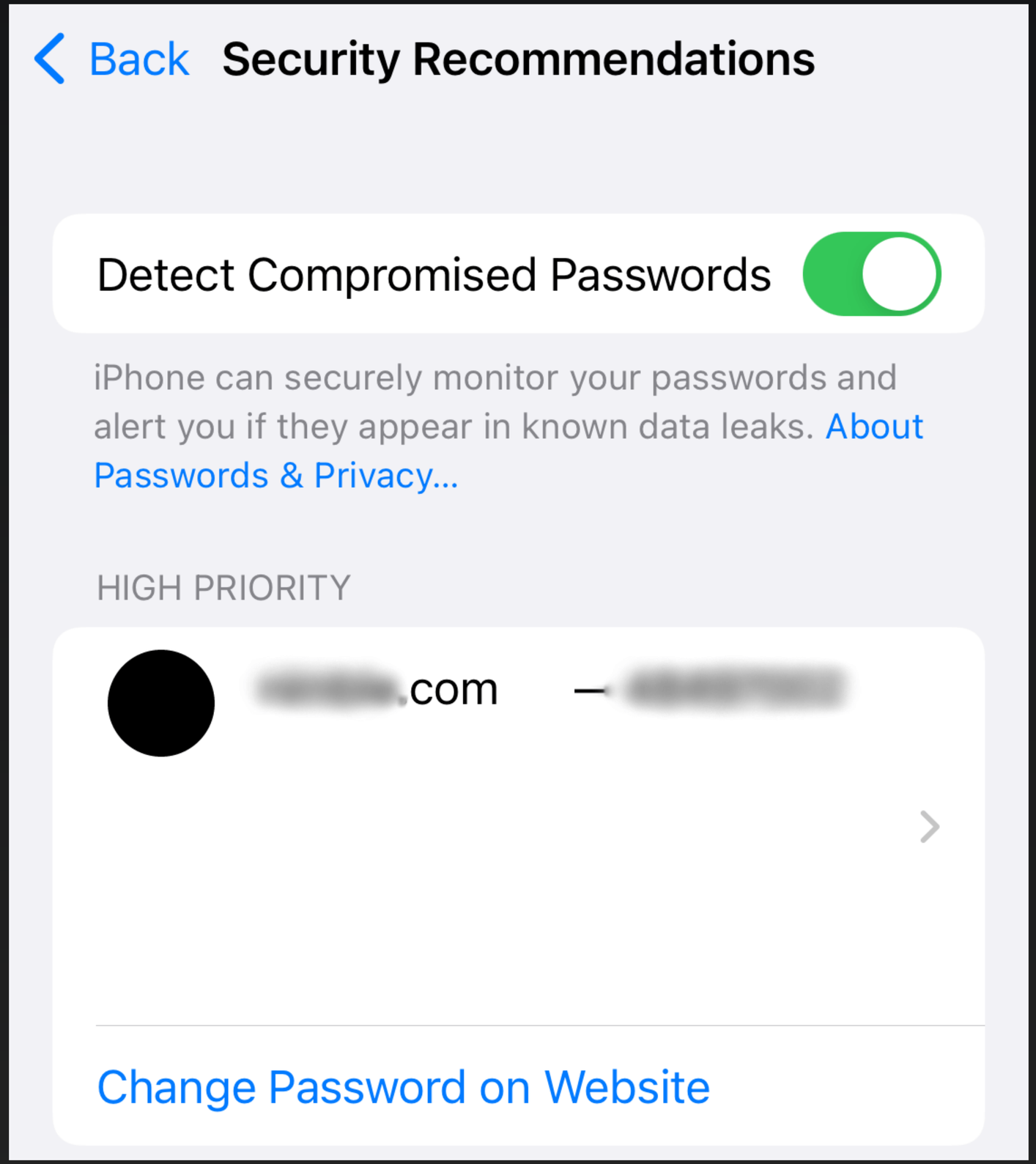


BIGGEST DATA BREACHES IN THE USA

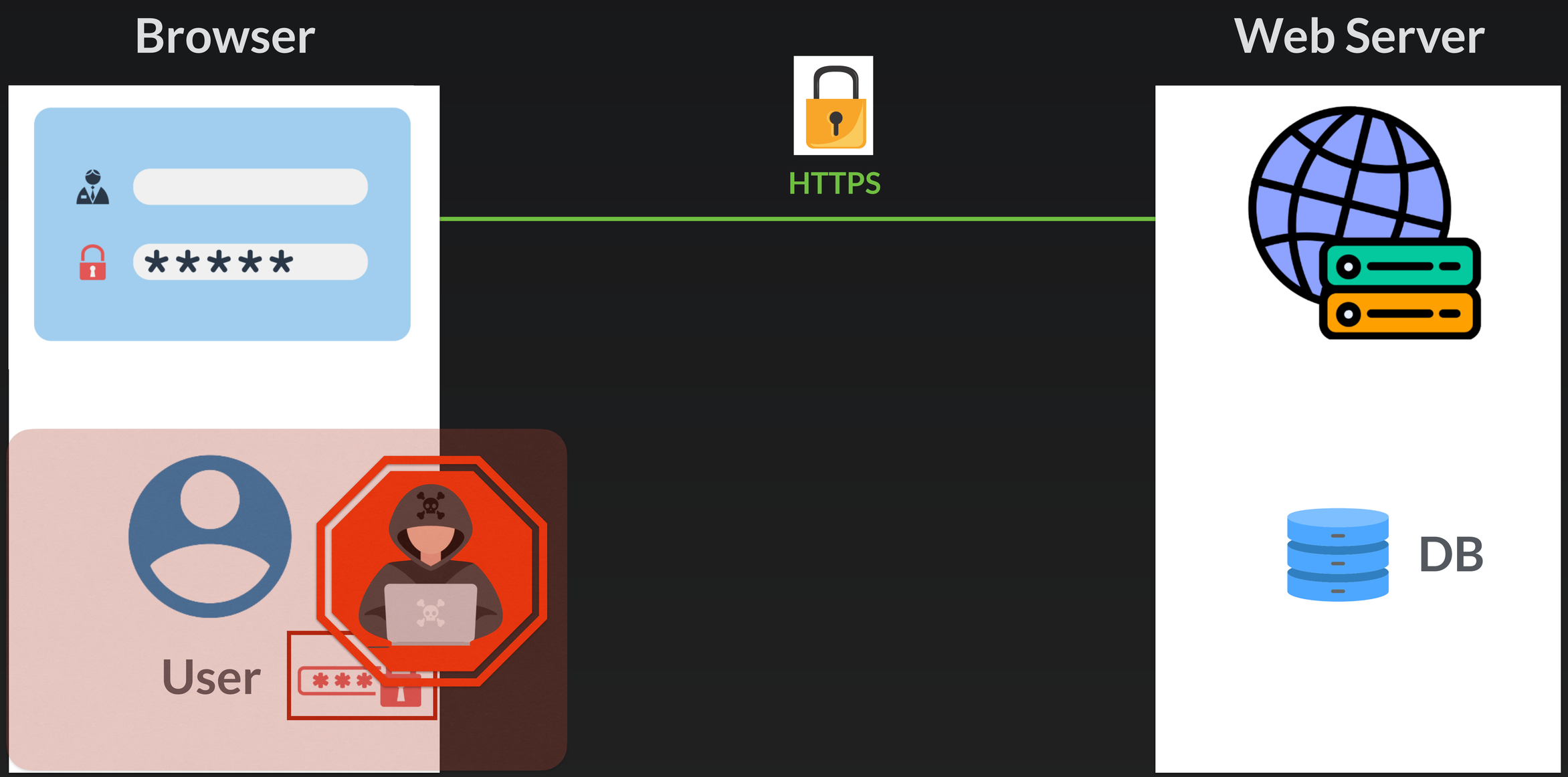
(2013-2017)

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

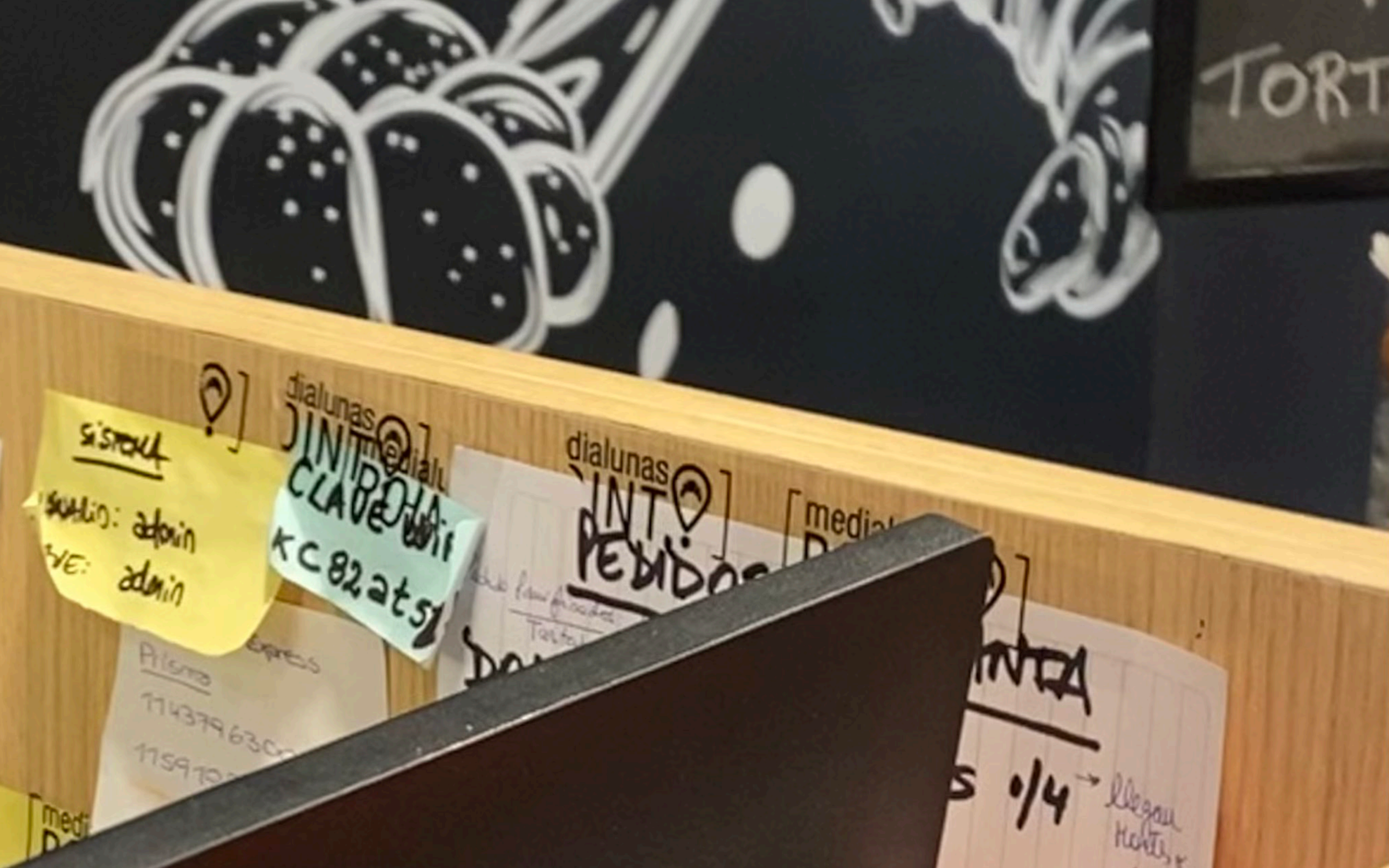
- ✕ MUST contain at least 8 characters (12+ recommended)
- ✕ MUST contain at least one uppercase letter
- ✕ MUST contain at least one lowercase letter
- ✕ MUST contain at least one number
- ✕ MUST contain at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~)
- ✔ MAY NOT contain more than 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

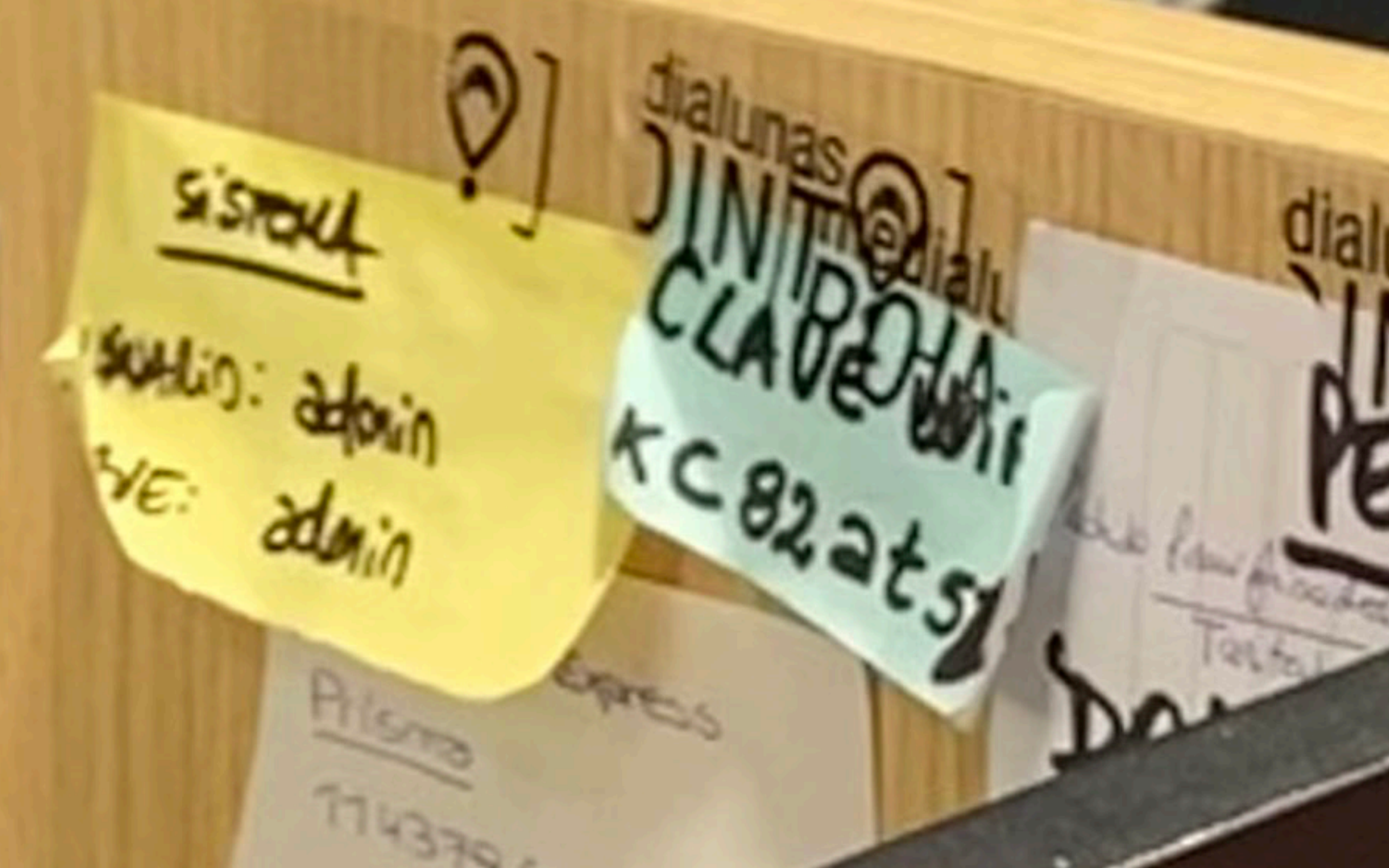
5 remaining rules need to be met

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

Passkeys

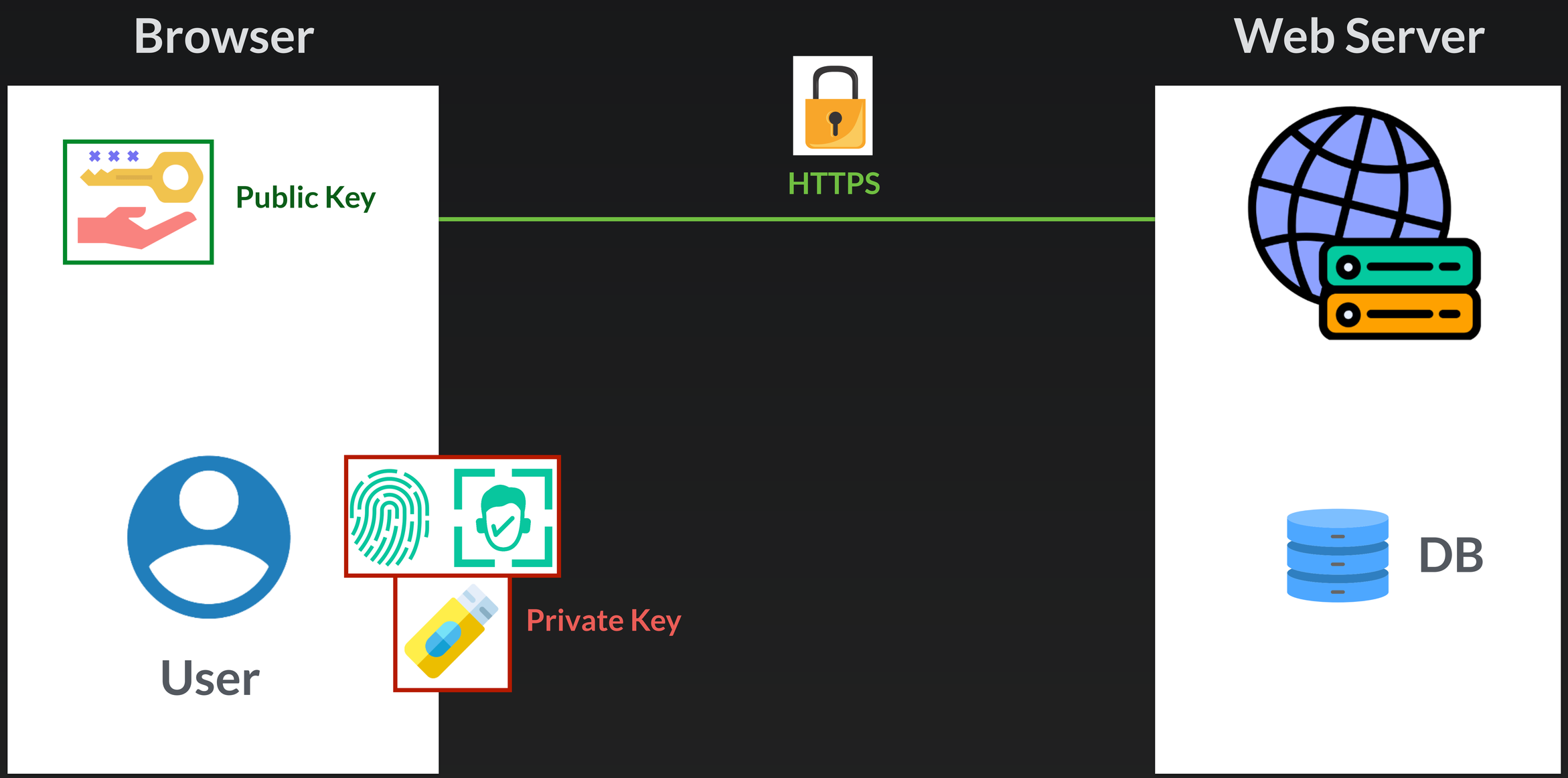
LAB

https://**github**.com/**firtman**/**passkeys-short**

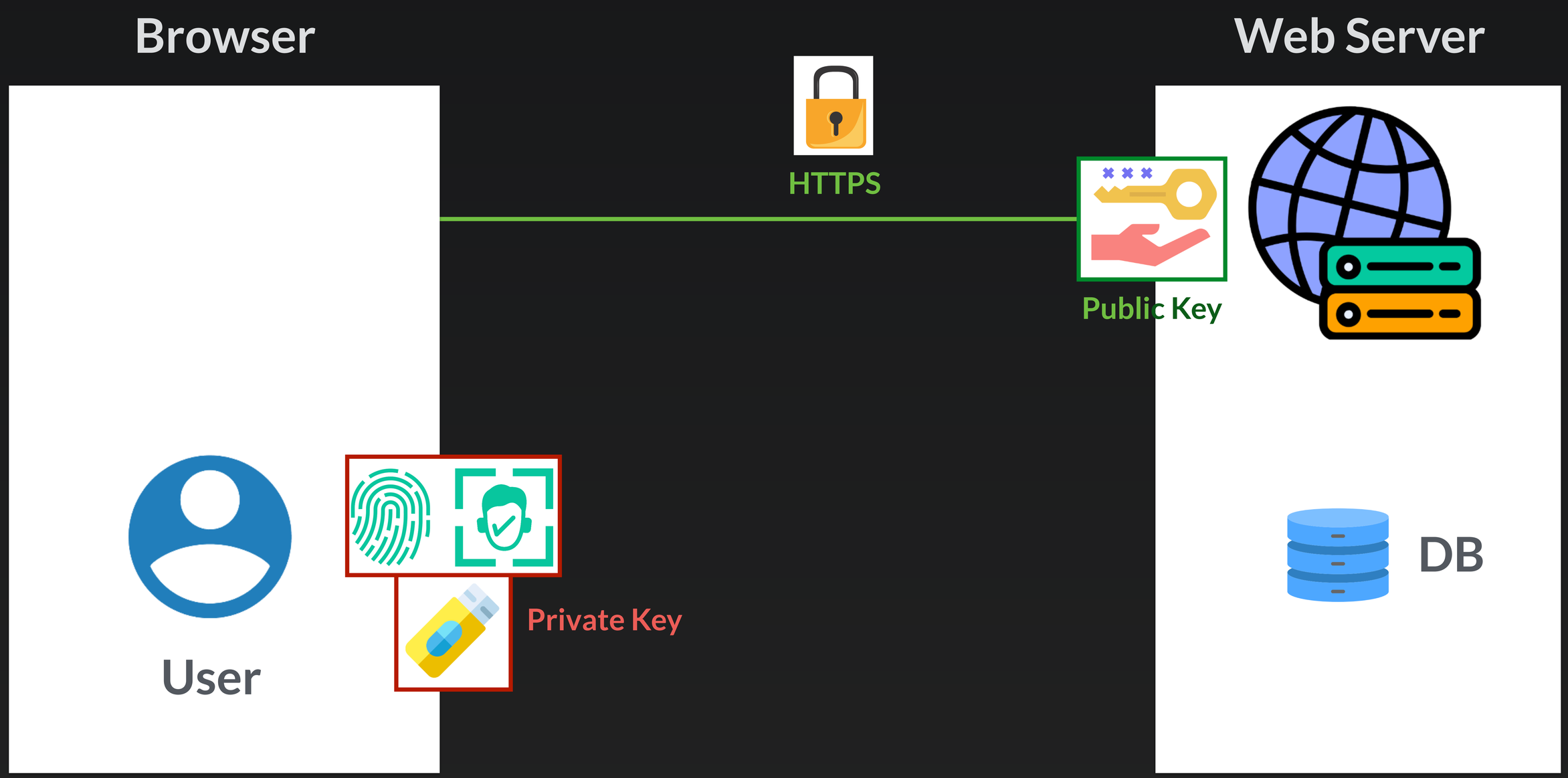
Passkeys

Passkeys

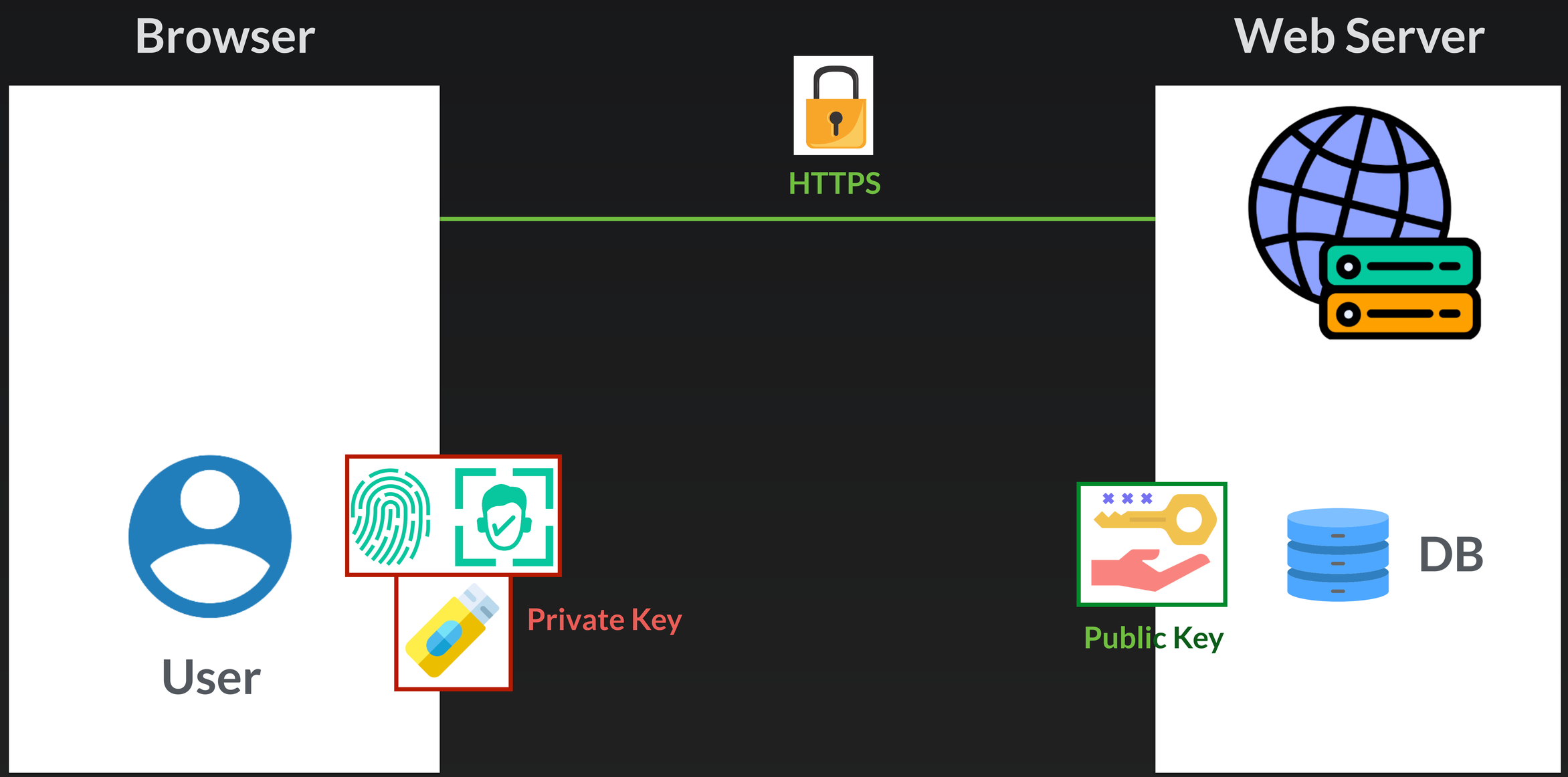
Passkeys



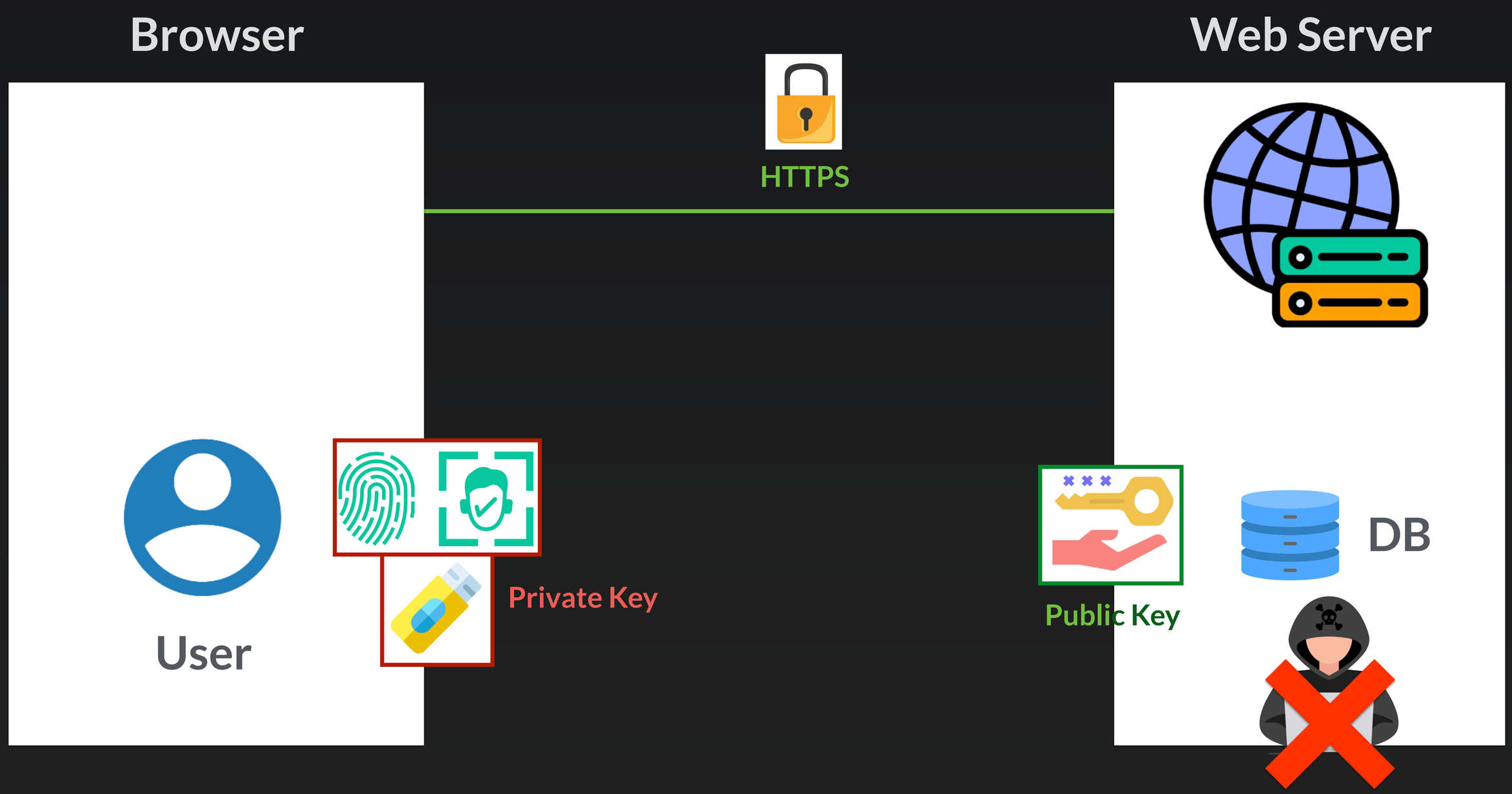
Passkeys



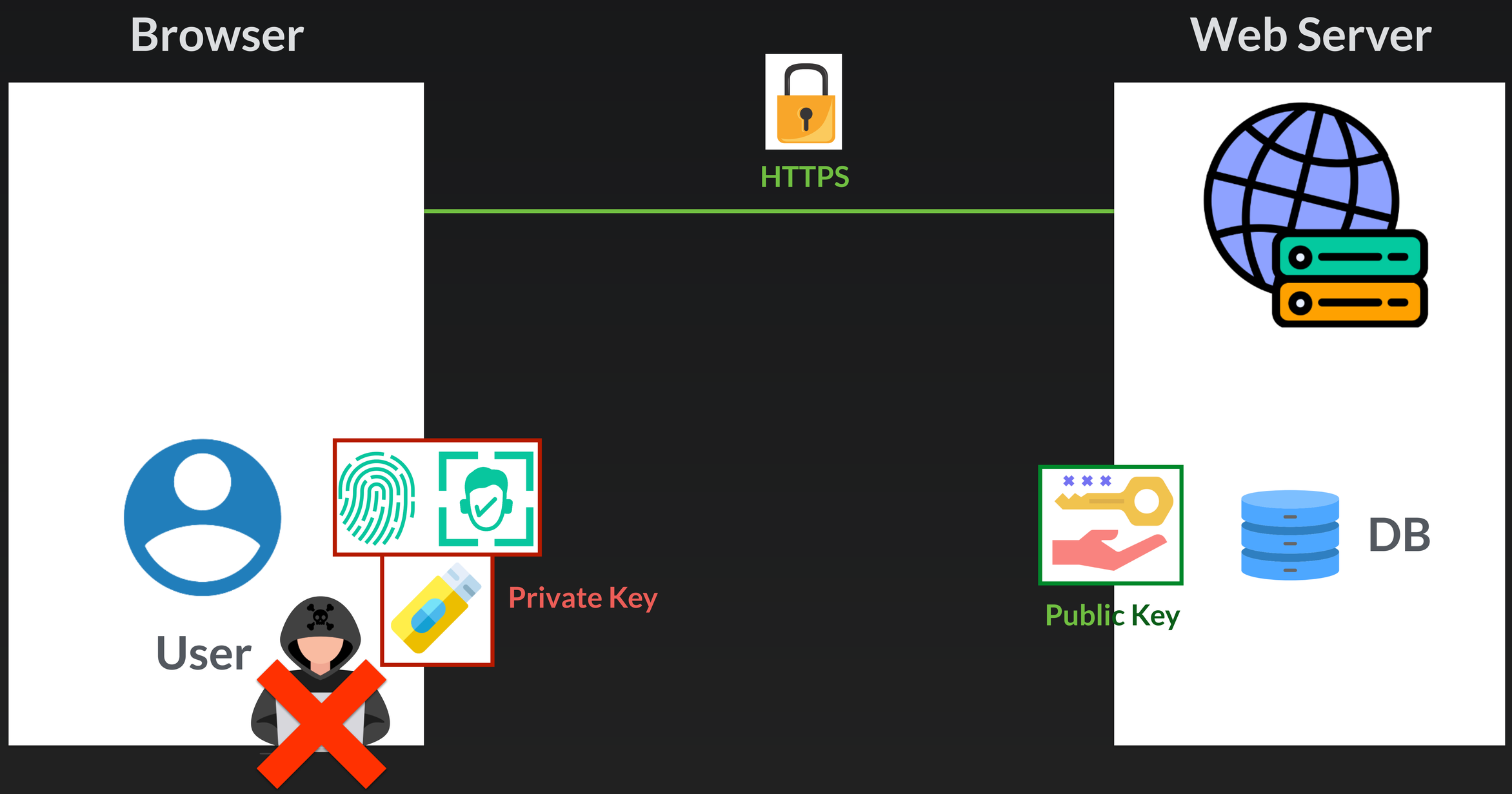
Passkeys



Passkeys



Passkeys



Passkeys

Passkey is a common noun

It's a replacement for passwords

It's based on WebAuthn API

- Multi-Factor Authentication
- Single-Factor Authentication

Keys can be stored

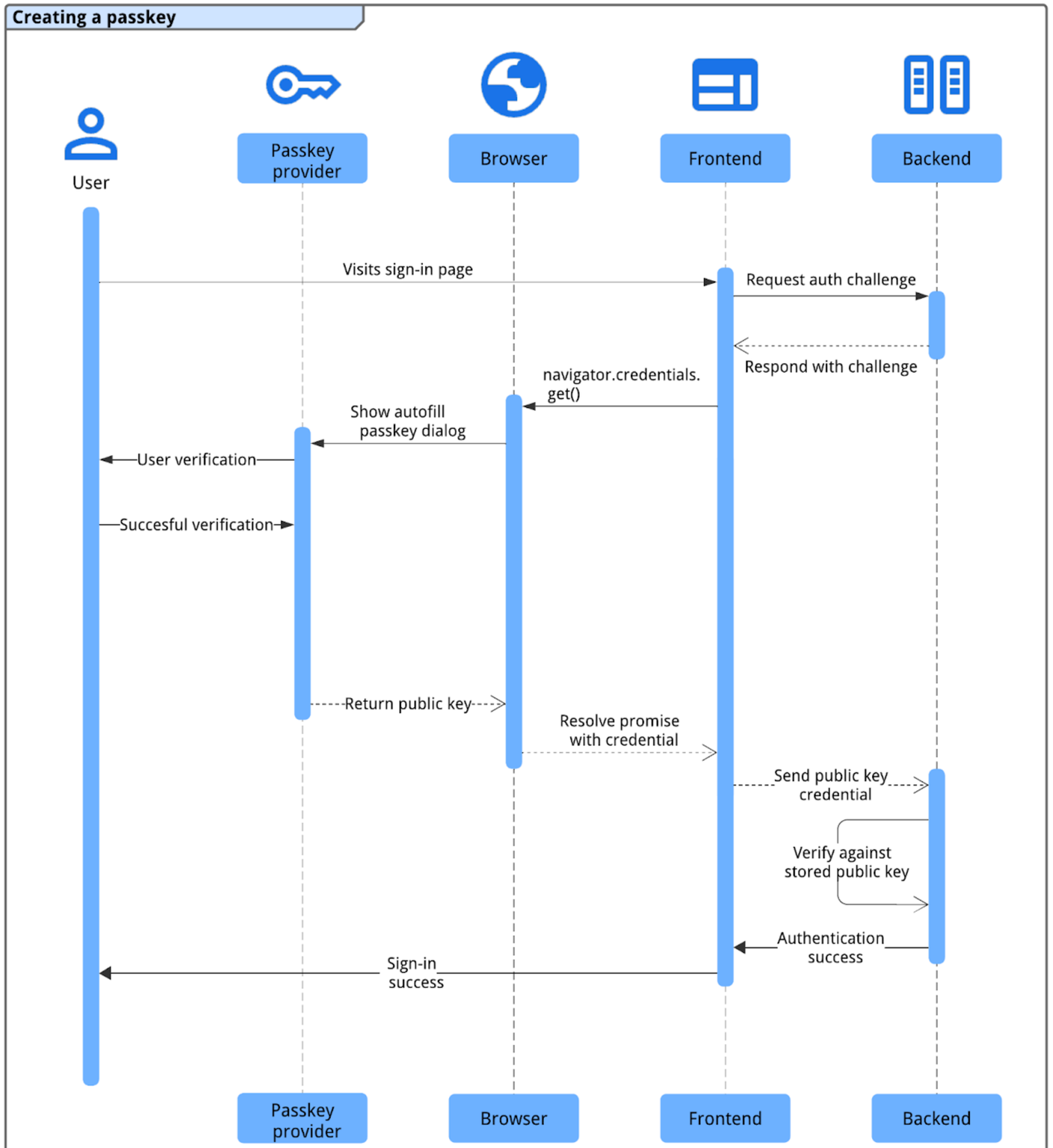
- On Device
- External hardware
- Cloud

Security

Passkeys

Multi-factor Auth

Form-based Auth


Creating a passkey
User
Passkey provider
Browser
Frontend
Backend
Visits sign-in page
Request auth challenge
Respond with challenge
navigator.credentials. get()
Show autofill passkey dialog
User verification
Succesful verification
Return public key
Resolve promise with credential
Send public key credential
Verify against stored public key
Authentication success
Sign-in success
Passkey provider
Browser
Frontend
Backend

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

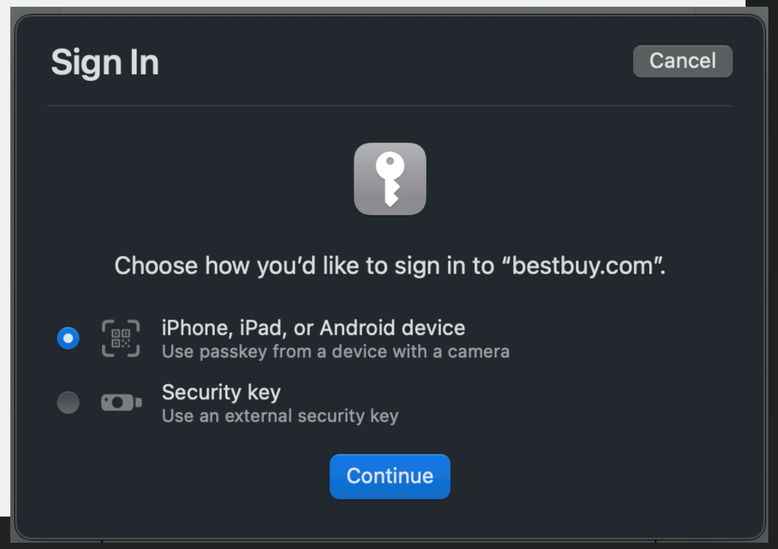
Sign in with a Passkey

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

4x higher login success

2x faster logins

800M accounts using passkeys

KAYAK

66% new users use passkeys

Sign-up and sign-in time reduced to half

3x faster logins

8x faster logins with MFA

3x successful logins 98% vs 32%

99% finishes passkey registration

CVS Health®

98% drop in mobile fraud

State of Michigan help desk password reset calls dropped by 1,300 in a month

state-of-passkeys.io

Passkeys

Based on the public/private key architecture

It's using WebAuthentication API and specs

Authenticators are saving the keys (known as passkeys) in the cloud

Since 2024 Passwords managers can be passkeys managers.

Recent features

- Conditional UI
- Conditional Registration

Advantages

- Phishing-resistant
- Security: Unique per service
- Data Breach-resistant
- Convenience: Quick access on Multidevices
- Web and native apps
- PWAs on iOS, iPadOS and macOS

Cloud-based Passkey support

iOS and iPadOS 16+

macOS 13+, using Safari and Chrome

Android 9+

Windows 11 23H2

Web Authentication (WebAuthn)

A multi-vendor effort

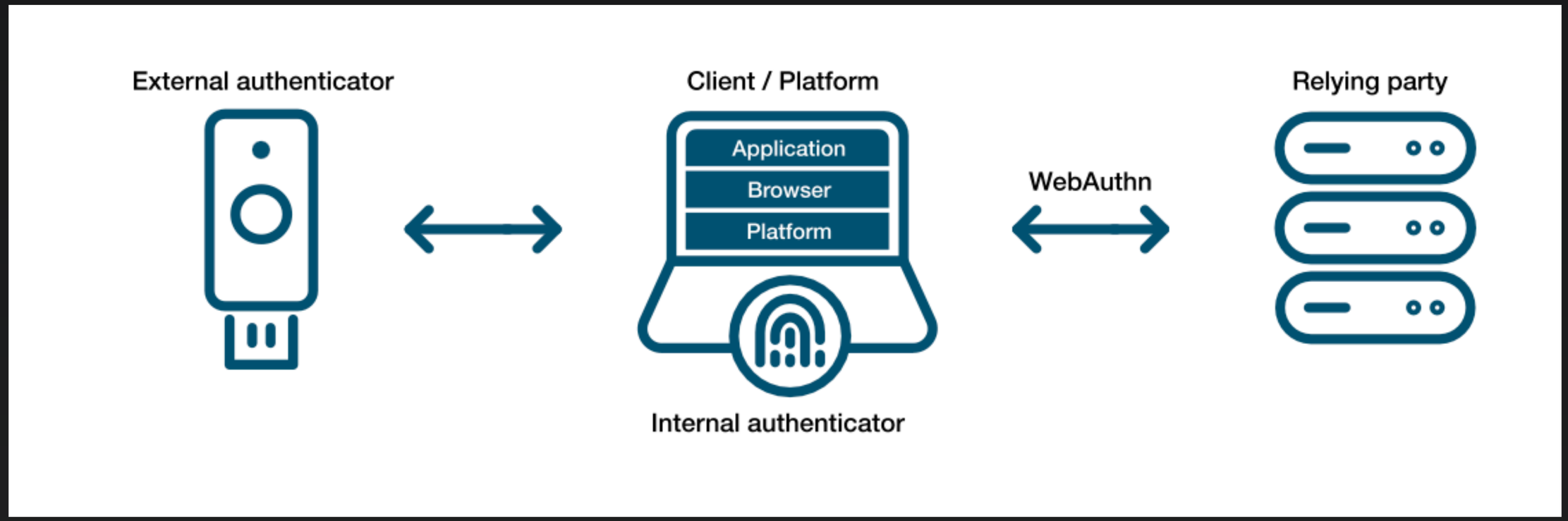
FIDO Alliance and W3C

Store safely private keys while sending public keys for the server

It works on every browser with different techniques and abilities:

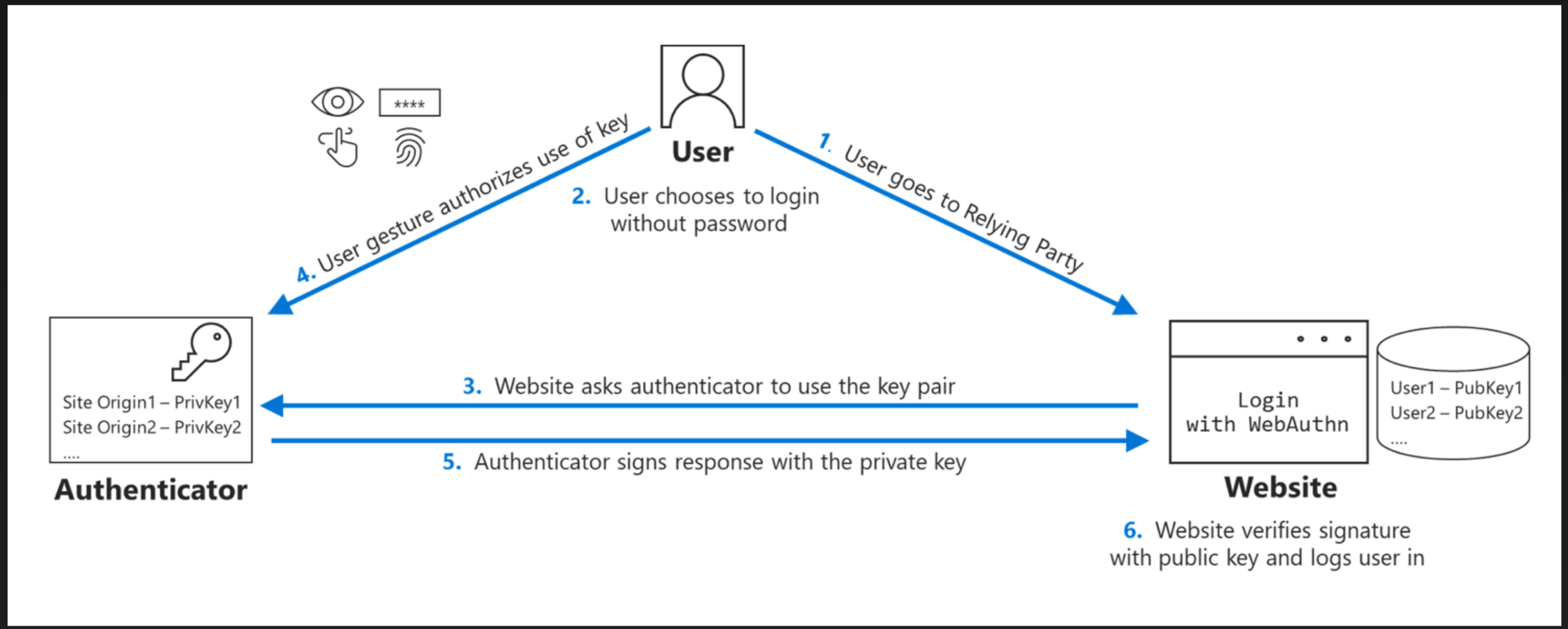
- **PIN-based keys**
- **FIDO2 USB keys** (such as Yubico)
- **Biometric Authenticators** (TouchID, FaceID, Windows Hello, Android)

WebAuthn



* images from yubico

WebAuthn



* images from Microsoft

Important Actions

On-device Authentication

Remote Authentication

Share passkeys on trusted contacts

Import / Export Passkeys

What do you need to do

- Create four web services server-side
- Implement the WebAuthn API client-side
- Implement Identity-first flow
- Store n credentials per account

Identifier-First Flow

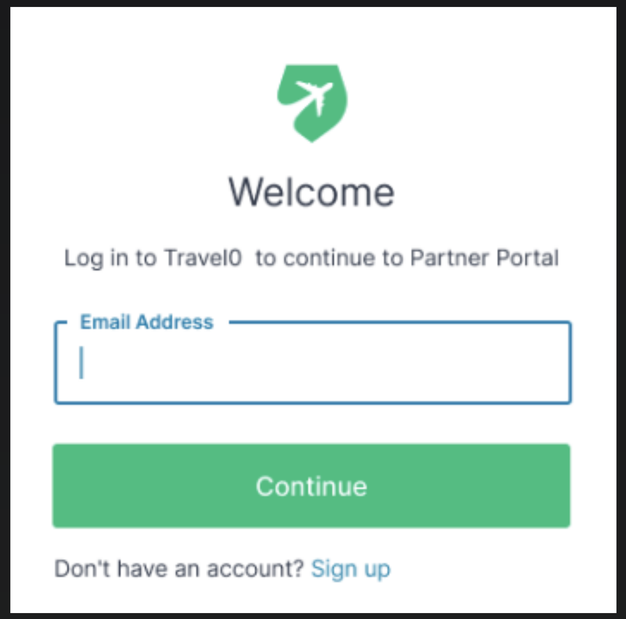
Instead of a login form with username and password:

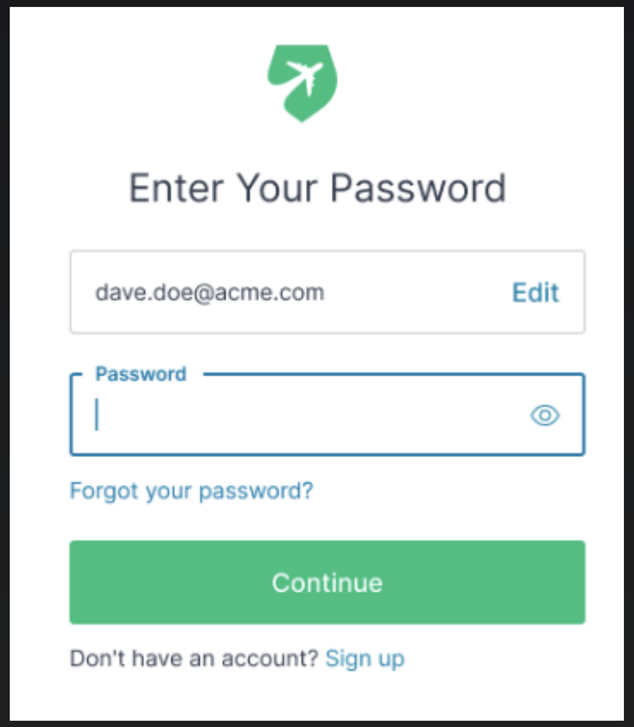
1- We first ask for identity (username)

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





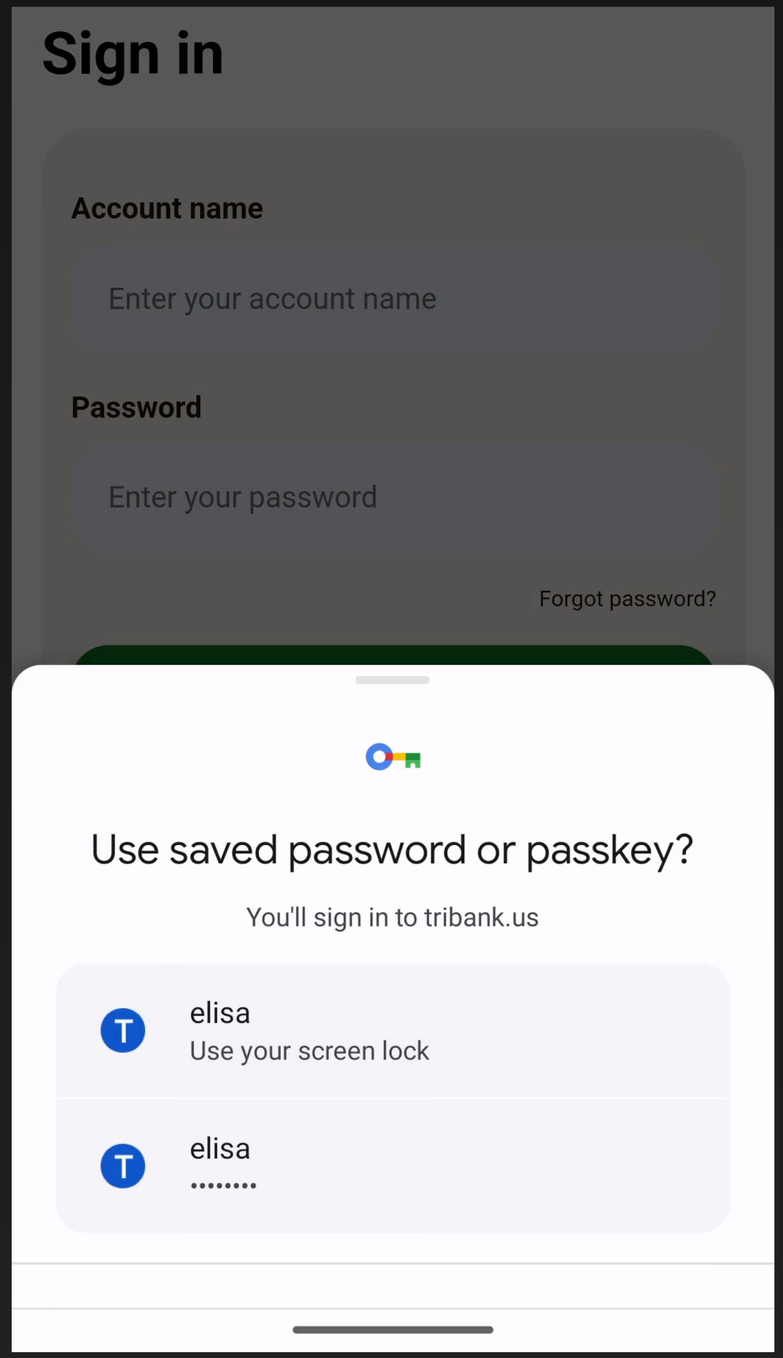
* images from Auth0 blog

LAB

Autofill / Conditional UI

Let us avoid selecting a username

Autofill / Conditional UI



Autofill / Conditional UI

The user taps on the username input field,

An autofill suggestion dialog pops up

If the user picks a passkey, it will initiate authentication

We need:

- one input with autocomplete="webauthn"

- support for authentication verification without username in the backend

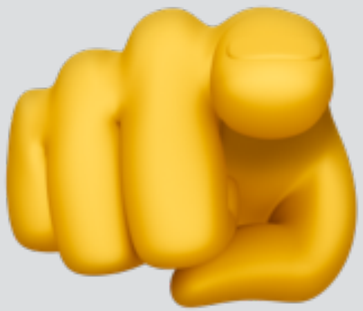
- initiate an authentication verification on page load

LAB

Project To-do

- Validations
- Better database integrity
- Forget Password Flow
- Confirm email on registration
- Sign in with Apple
- Magic Link login
- Passkeys conditional creation

Passkeys are the future of authentication



It's now on you to implement it in your websites and apps

Maximiliano Firtman
@firt firt.dev

Thanks!

Questions or feedback? hi@firt.dev