Microservice

security


BNP PARIBAS.net


2 Cliquez pour composer les 6 chiffres de votre
Code secret
0
1
2 3
4 5 6
7 8 9
x effacer


AGRANDIR
FERMER
VOTRE CODE SECRET
9 4
8
5 1 7 2
3 6 0
CORRIGER
VALIDER


SOCIETE GENERALE
Banque & Assurances


Enter
Shift


438754

Verified by VISA

Validez votre paiement

Pour vous protéger contre l'utilisation frauduleuse de votre carte bancaire, la Société Générale vous demande de vous identifier en validant votre PASS SECURITE dans l'APPLI Société Générale.
Cette authentification est nécessaire pour valider votre transaction en cours.
En cas de refus de votre part, la transaction sera annulée.

Marchand : Xmarque
Montant : 1500.00 EUR
Date : 03/07/2013
N° de carte : xxxx xxxx xxxx 1234

Horodatage :
03/07/2013 16:39:45
Terminal :
Tel de Kevin(Iphone)

Ne pas m'identifier et continuer mon achat

Aide

Expéditeur: "Service Banque en ligne Société Génér.." <mail1@mail.riseup.net>
Date: 27 novembre 2017 à 18:34:14 UTC+1
Destinataire:
Objet: TR : CODES SÉCURITÉ - DEMANDE D'ENREGISTREMENT DE VOTRE PASS SÉCURITÉ.

Chère Cliente, cher Client,

Société Générale est dotèe d'un dispositif de contrôle des paiements depuis votre mobile
est approuvé par vous-même.Ce Service est entièrement gratuit.

Notre système a détecté que vous n'avez pas encore activé le pass sécurité

NB: Pour activer votre pass sécurité vous devez.

> Suivre la démarche
> pour activer ce service : Docs: N°54678956

Ces modifications entreront en vigueur sur vos comptes dans un délai de 1 mois à compter
de la réception du présent message.

Nous vous rappelons que l'absence de contestation de ces modifications
dans un délai de 2 mois vaudra une acceptation des dites modifications de votre part.

Cordialement

Rapheal Kivine,directeur de la relation Clients

FIDO2 / Windows Hello / Passwordless

https://webauthn.me/

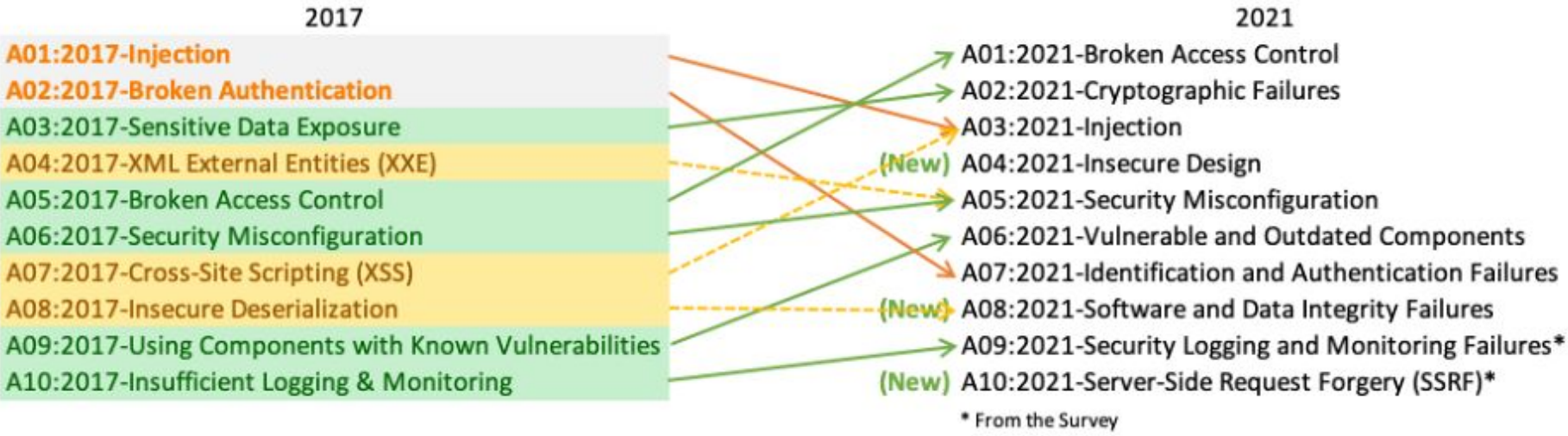
C'EST QUI LE PIGEON ?

OWASP

https://owasp.org/

Open Web Application Security Project®

OWASP

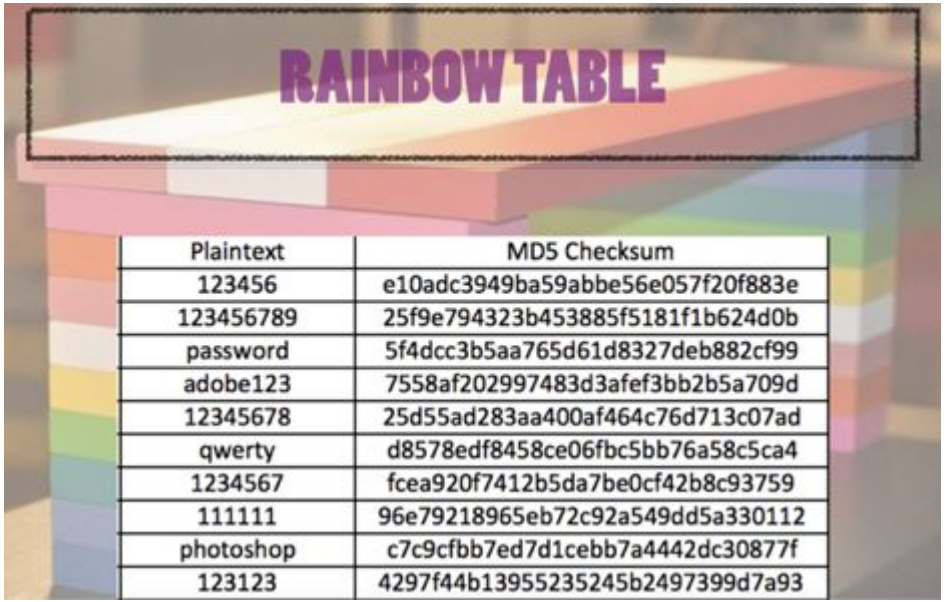

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

OWASP Top Ten

- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

OWASP Top Ten

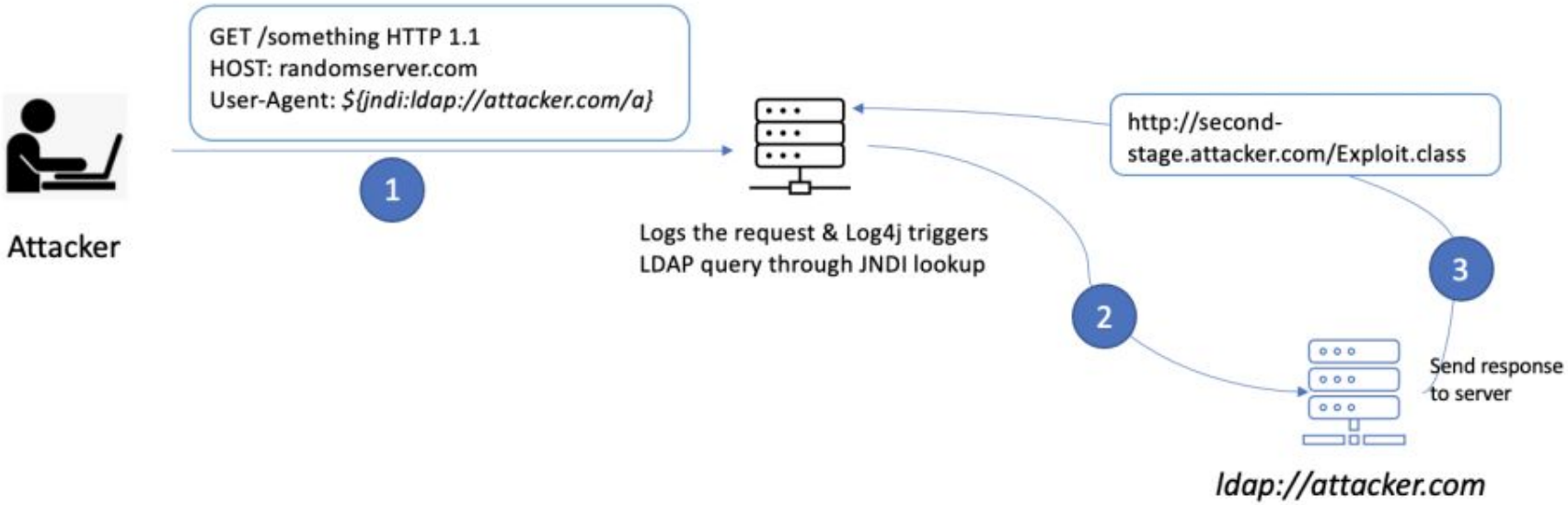
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.



Plaintext	MD5 Checksum
123456	e10adc3949ba59abbe56e057f20f883e
123456789	25f9e794323b453885f5181f1b624d0b
password	5f4dcc3b5aa765d61d8327deb882cf99
adobe123	7558af202997483d3afef3bb2b5a709d
12345678	25d55ad283aa400af464c76d713c07ad
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567	fcea920f7412b5da7be0cf42b8c93759
111111	96e79218965eb72c92a549dd5a330112
photoshop	c7c9cfbb7ed7d1cebb7a4442dc30877f
123123	4297f44b13955235245b2497399d7a93

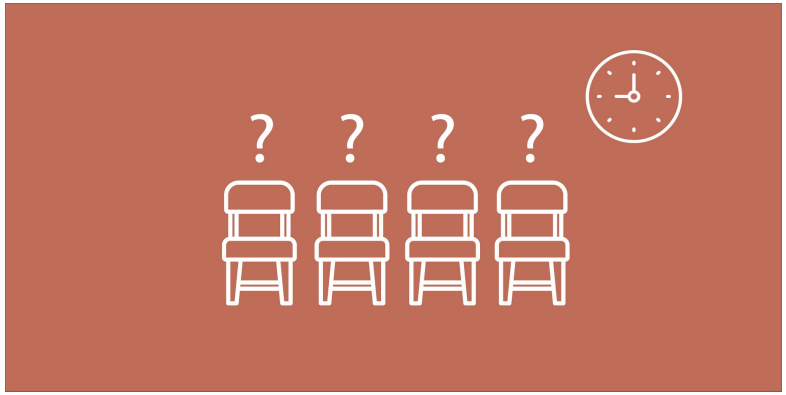
OWASP Top Ten

- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.



OWASP Top Ten

- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

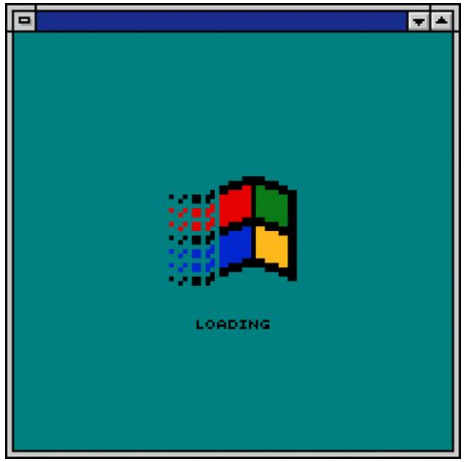


OWASP Top Ten

- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.

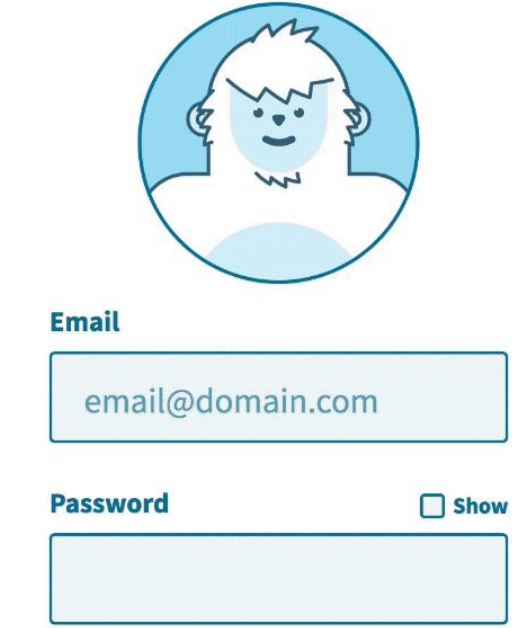
OWASP Top Ten

- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.



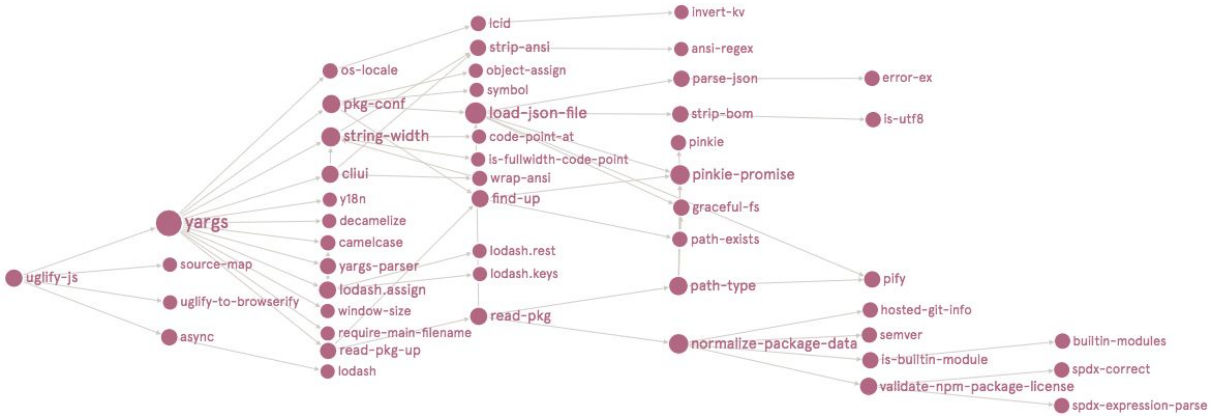
OWASP Top Ten

- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.



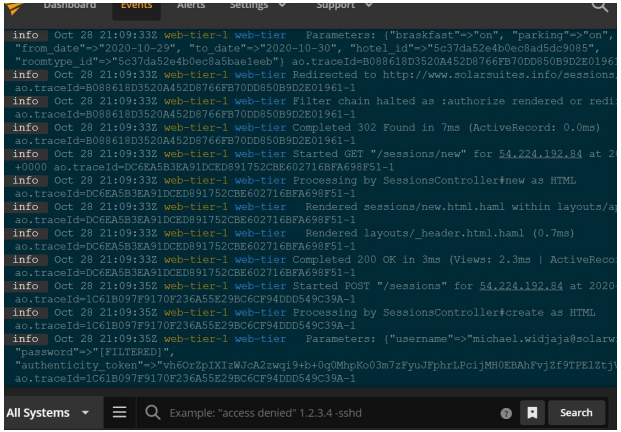
OWASP Top Ten

- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.



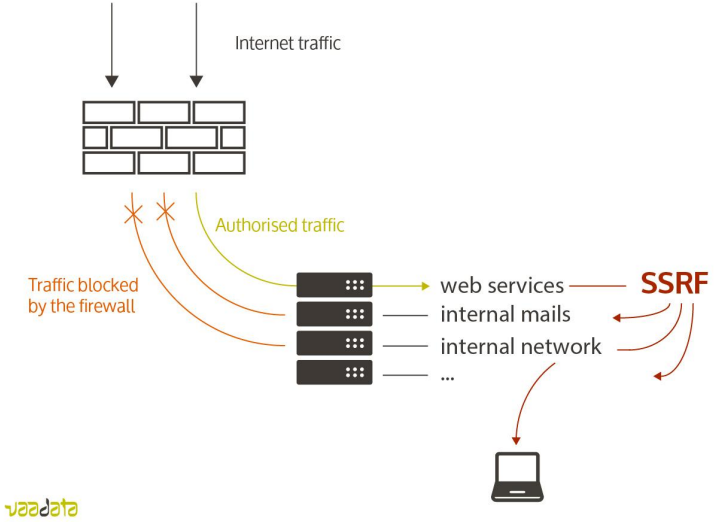
OWASP Top Ten

- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.



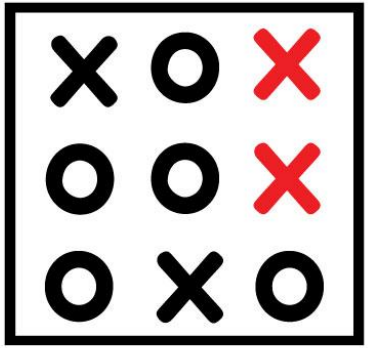
OWASP Top Ten

- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it’s not illustrated in the data at this time.




OWASP
Open Web Application
Security Project

THINK OUTSIDE THE BOX



Physical attack

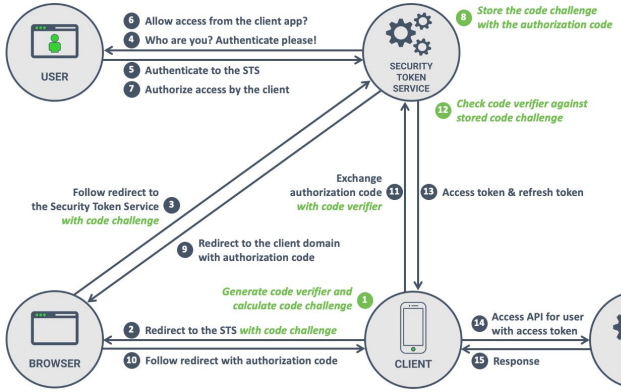
Authentification in motus App

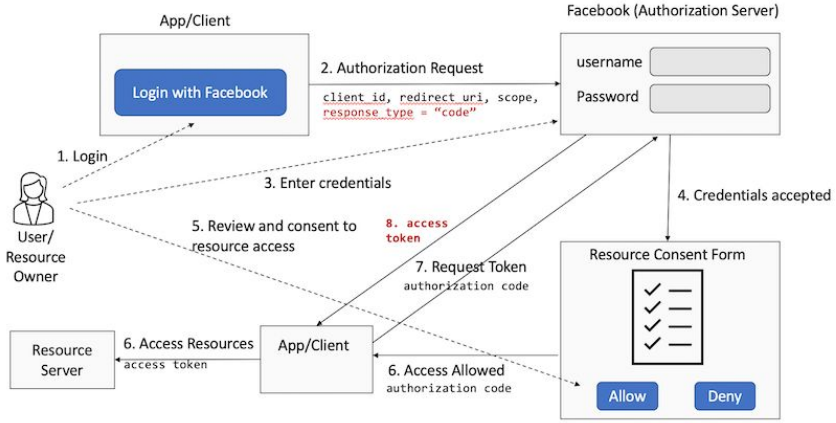
https://simongomezuniv.github.io/td_auth

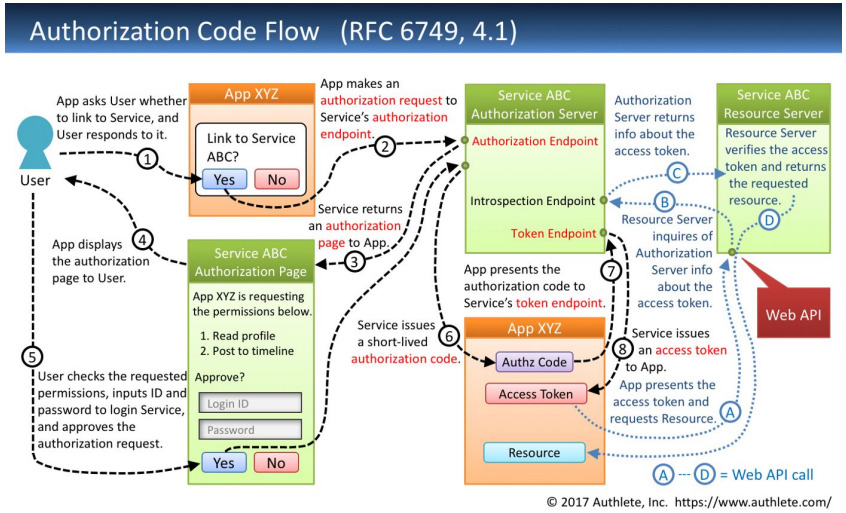
Authentification : the micro service way

oauth2 and openID

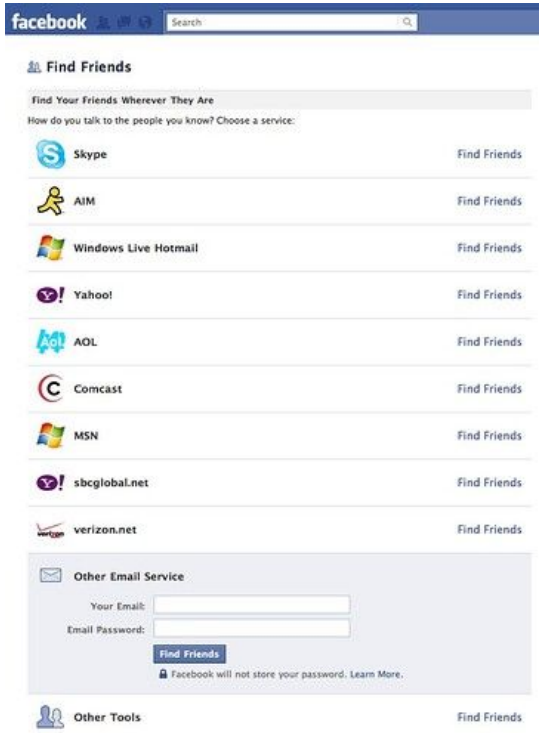
Standard

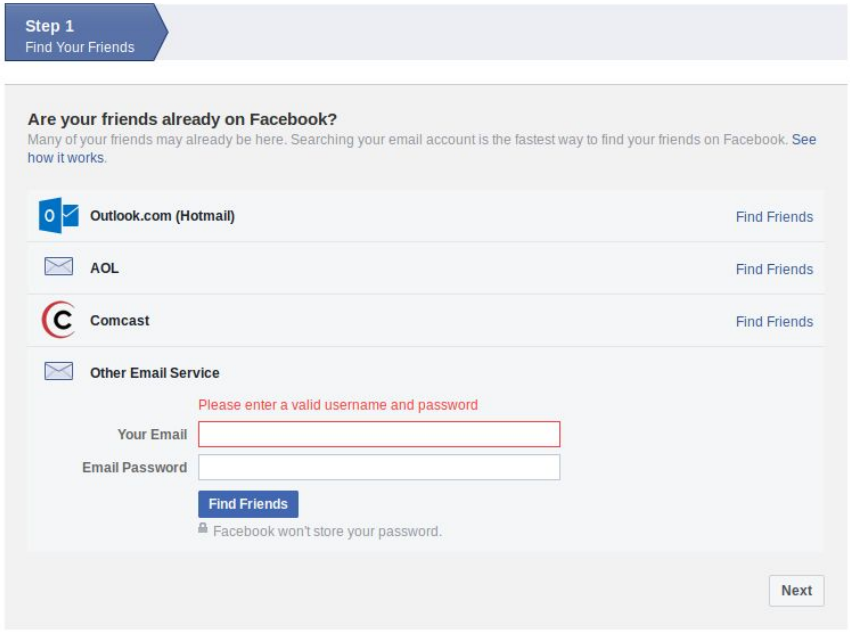

USER
SECURITY TOKEN SERVICE
BROWSER
CLIENT
API
6 Allow access from the client app?
4 Who are you? Authenticate please!
5 Authenticate to the STS
7 Authorize access by the client
8 Store the code challenge with the authorization code
12 Check code verifier against stored code challenge
Follow redirect to the Security Token Service 3 with code challenge
Exchange authorization code 11 with code verifier
13 Access token & refresh token
9 Redirect to the client domain with authorization code
Generate code verifier and calculate code challenge 1
2 Redirect to the STS with code challenge
10 Follow redirect with authorization code
14 Access API for user with access token
15 Response


App/Client
Facebook (Authorization Server)
Login with Facebook
2. Authorization Request
client_id, redirect_uri, scope, response_type = "code"
username
Password
1. Login
3. Enter credentials
4. Credentials accepted
User/ Resource Owner
5. Review and consent to resource access
8. access token
7. Request Token
authorization code
Resource Consent Form
Resource Server
6. Access Resources
access token
App/Client
6. Access Allowed
authorization code
Allow
Deny

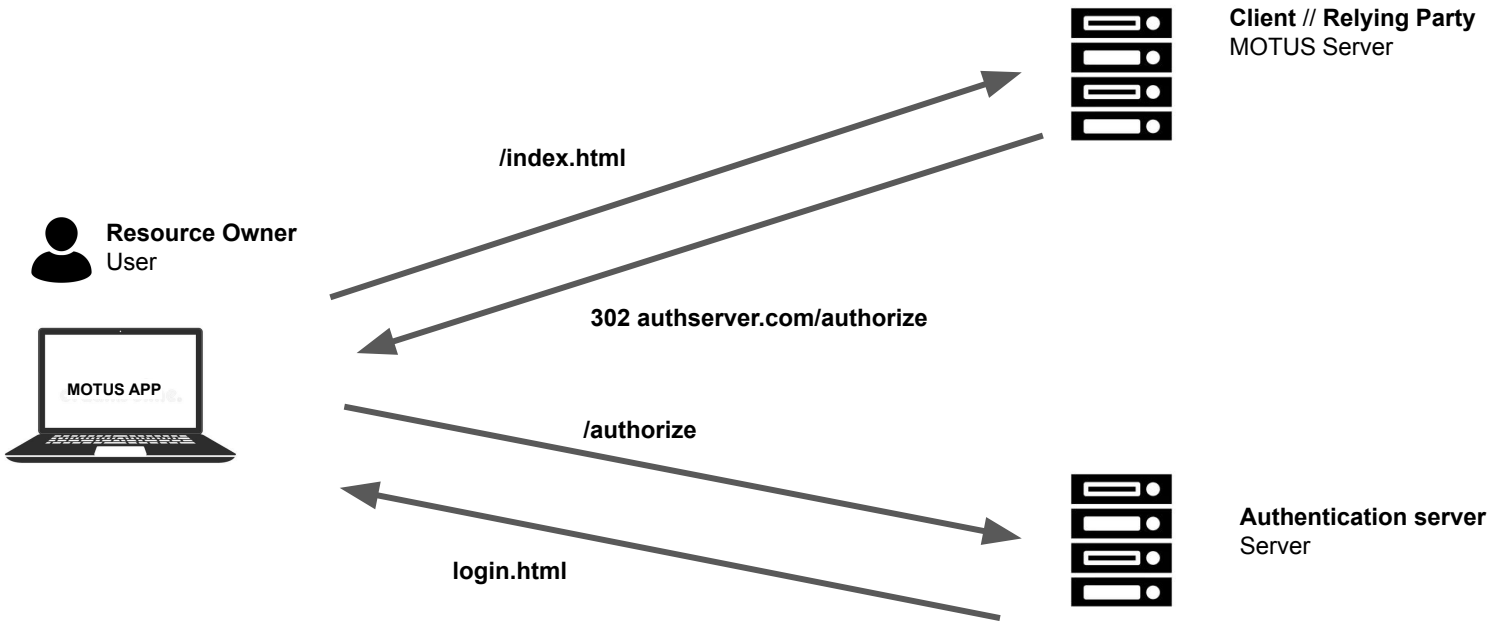

Authorization Code Flow (RFC 6749, 4.1)
App asks User whether to link to Service, and User responds to it.
User
App XYZ
Link to Service ABC?
Yes
No
App makes an authorization request to Service's authorization endpoint.
Service ABC Authorization Server
Authorization Endpoint
Introspection Endpoint
Token Endpoint
Authorization Server returns info about the access token.
Service ABC Resource Server
Resource Server verifies the access token and returns the requested resource.
Service returns an authorization page to App.
App displays the authorization page to User.
Service ABC Authorization Page
App XYZ is requesting the permissions below.
1. Read profile
2. Post to timeline
Approve?
Login ID
Password
Yes
No
User checks the requested permissions, inputs ID and password to login Service, and approves the authorization request.
Resource Server inquires of Authorization Server info about the access token.
Web API
App presents the authorization code to Service's token endpoint.
Service issues a short-lived authorization code.
App XYZ
Authz Code
Access Token
Resource
Service issues an access token to App.
App presents the access token and requests Resource.
A --- D = Web API call
© 2017 Authlete, Inc. https://www.authlete.com/

Oauth2 : Why

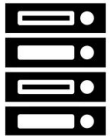

facebook
Search
Find Friends
Find Your Friends Wherever They Are
How do you talk to the people you know? Choose a service:
Skype
Find Friends
AIM
Find Friends
Windows Live Hotmail
Find Friends
Yahoo!
Find Friends
AOL
Find Friends
Comcast
Find Friends
MSN
Find Friends
sbcglobal.net
Find Friends
verizon.net
Find Friends
Other Email Service
Your Email:
Email Password:
Find Friends
Facebook will not store your password. Learn More.
Other Tools
Find Friends


Step 1
Find Your Friends
Are your friends already on Facebook?
Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook. See how it works.
Outlook.com (Hotmail)
Find Friends
AOL
Find Friends
Comcast
Find Friends
Other Email Service
Please enter a valid username and password
Your Email
Email Password
Find Friends
Facebook won't store your password.
Next
Facebook stores your contact list for you so that we can help you reach more people and connect friends.
Learn more.

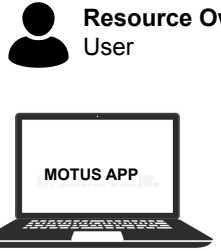
Oauth 2.0


Client // Relying Party
MOTUS Server
/index.html
Resource Owner
User
302 authserver.com/authorize
MOTUS APP
/authorize
Authentication server
Server
login.html

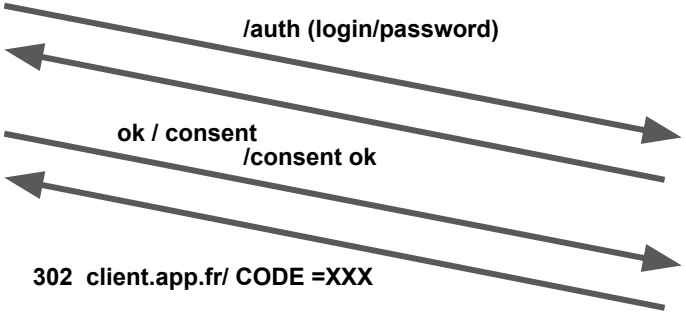
Oauth 2.0

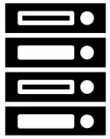


Client // Relying Party
MOTUS Server



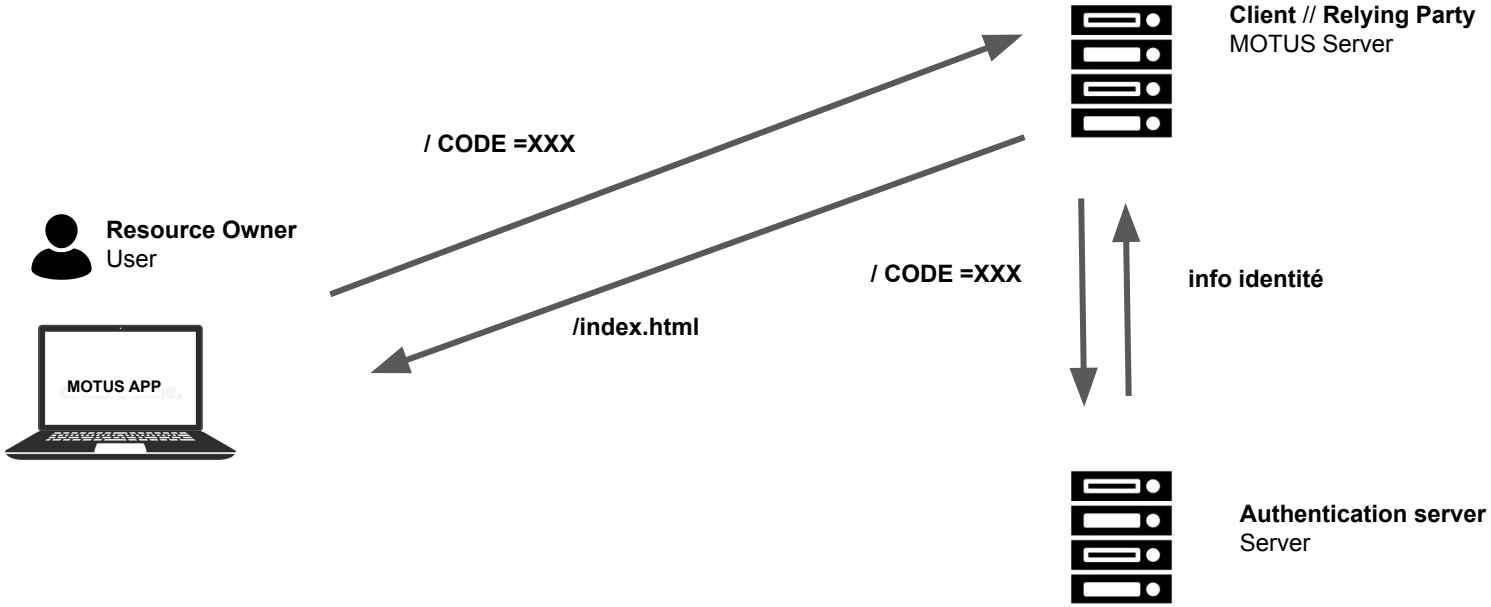
Resource Owner
User



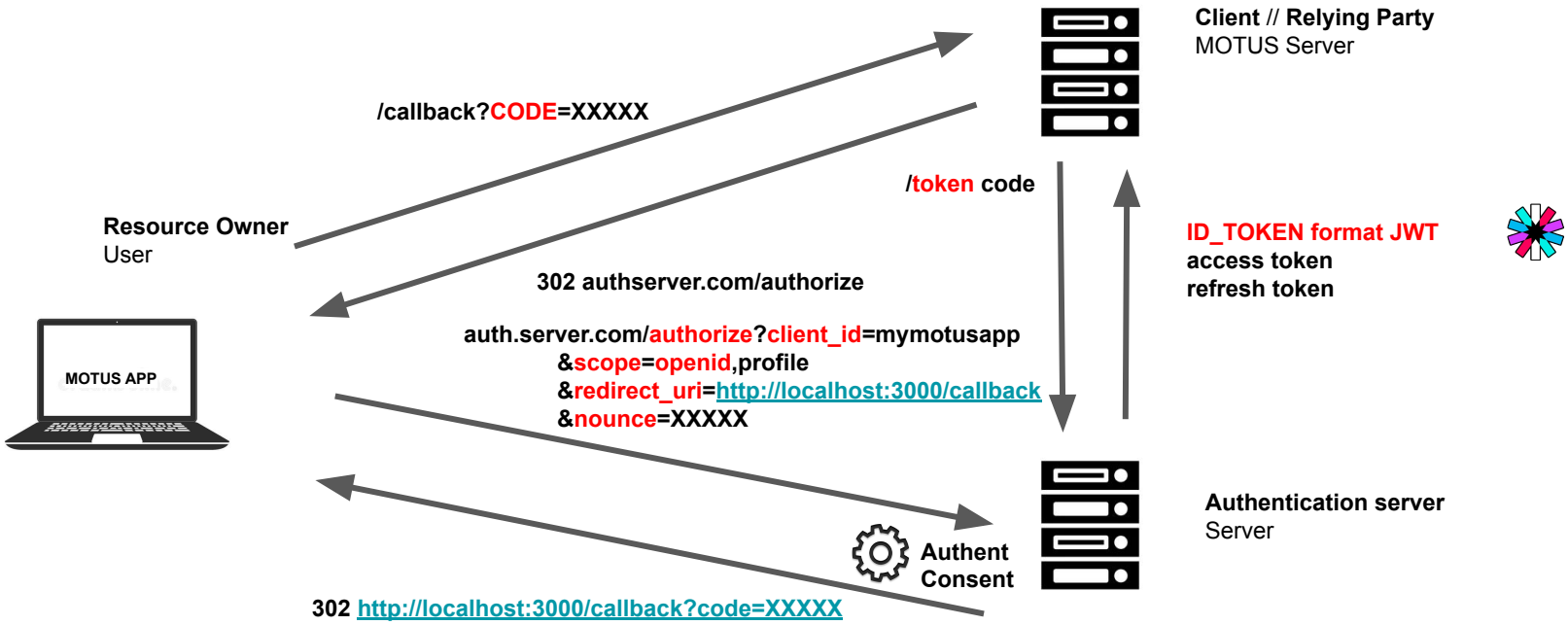


Authentication server
Server

Oauth 2.0


Client // Relying Party
MOTUS Server
/ CODE =XXX
Resource Owner
User
/ CODE =XXX
info identité
/index.html
MOTUS APP
Authentication server
Server

OPENID

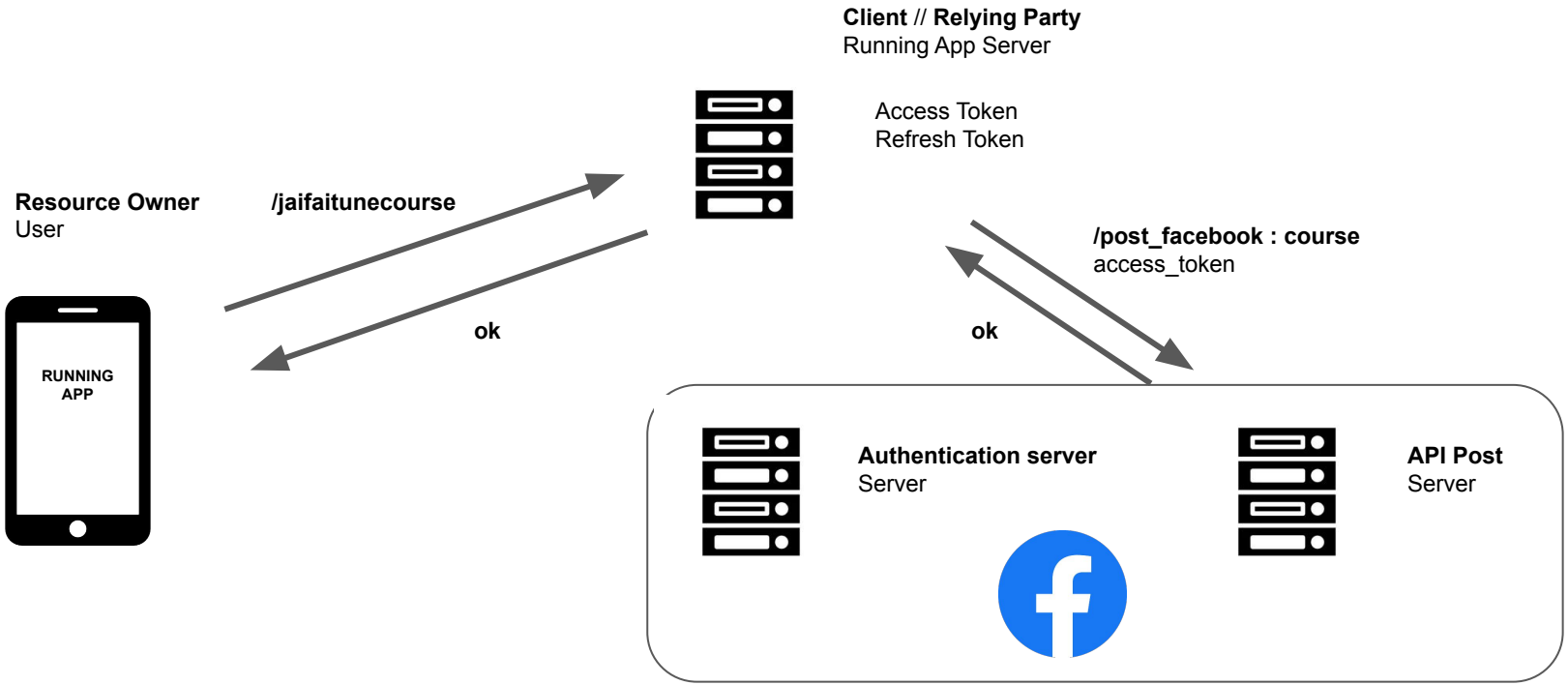

Client // Relying Party
MOTUS Server
/callback?CODE=XXXXX
/token code
Resource Owner
User
ID_TOKEN format JWT
access token
refresh token
302 authserver.com/authorize
auth.server.com/authorize?client_id=mymotusapp
&scope=openid,profile
&redirect_uri=http://localhost:3000/callback
&nounce=XXXXX
MOTUS APP
Authentication server
Server
Authent
Consent
302 http://localhost:3000/callback?code=XXXXX

JWT

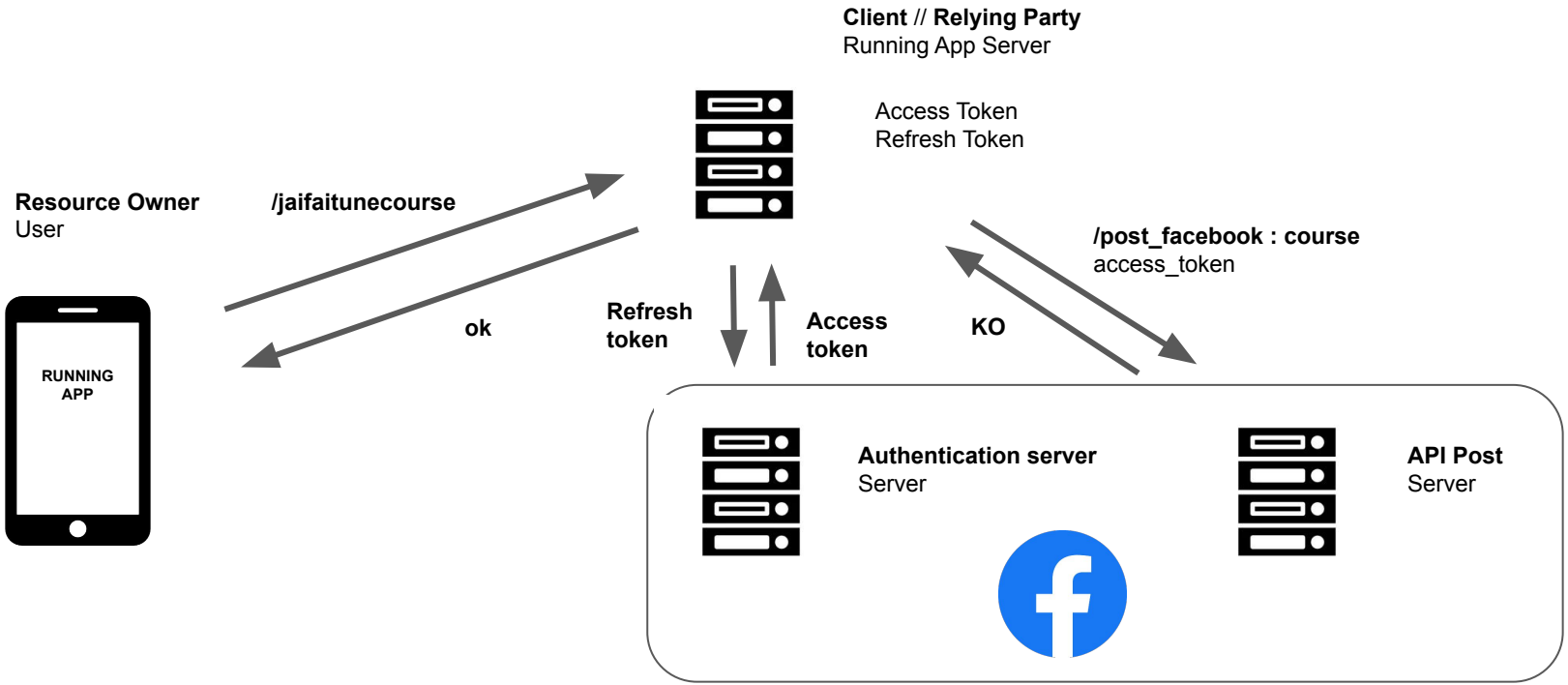
http://jwt.io

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjUwMDAiLCJzdWIiOiJzaW1vbiIsImF1ZCI6Im15bW90dXNhcHAiLCJub25jZSI6Im1sc2prZmRtbGtkZiIsImV4cCI6MTY2NDI3NjE4MSwiaWF0IjoxNjY0MjcyNTgxLCJzY29wZSI6InByb2ZpbGUifQ.hH7Fy72YhzEMRgbhQM6jCuKjuJGkH4gMapP4yp73g_k

Access Token & refresh token



Access Token & refresh token



Authentification in motus App

https://simongomezuniv.github.io/td_oauth2