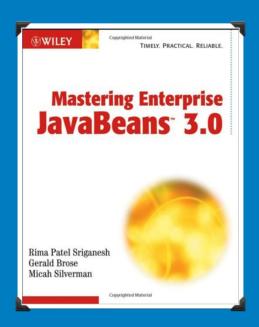
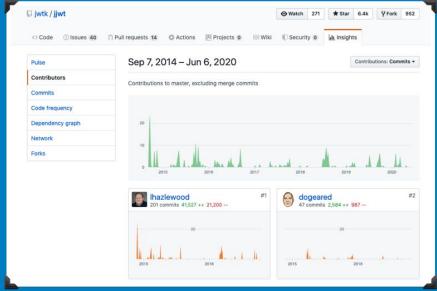
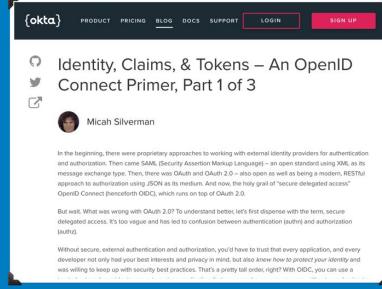
Hacking OAuth: Pitfalls and Remedies







https://github.com/jwtk/jjwt



https://bit.ly/OIDCPrimer

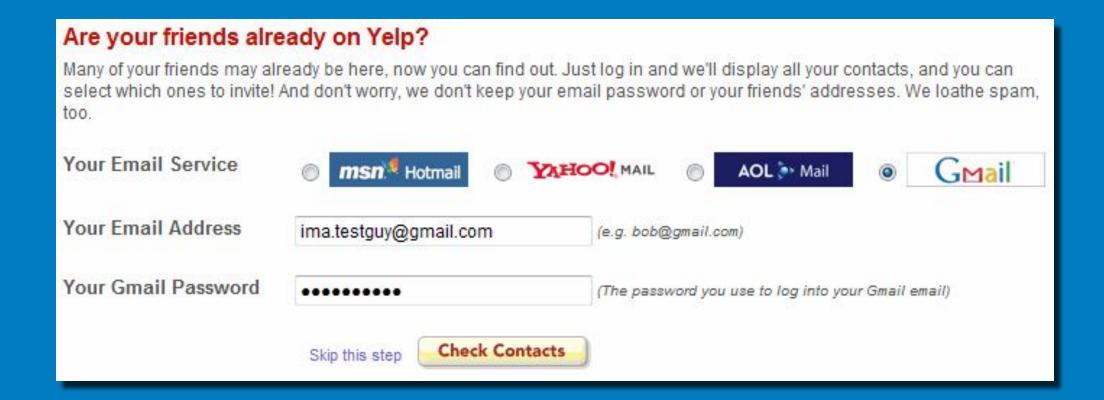
MICAH SILVERMAN
Senior Security H@XOR
@AFITNERD
@OKTADEV



Identity use cases (circa 2007)

- ★ Simple login forms and cookies
- ★ Single sign-on across sites SAML
- ★ Mobile app login ???
- ★ Delegated authorization ???

Don't do it this way!



Don't do it this way!

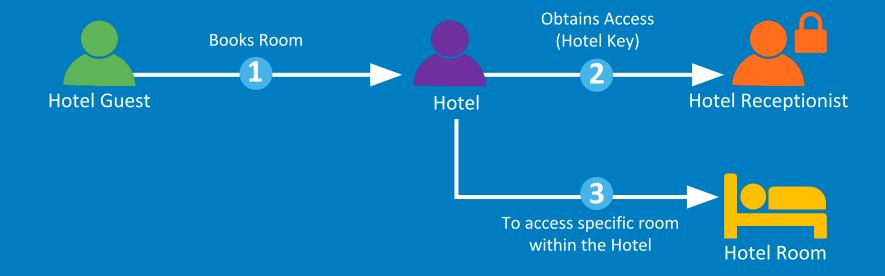


The delegated authorization problem HOW CAN I LET A WEBSITE ACCESS MY DATA, WITHOUT GIVING IT MY PASSWORD?

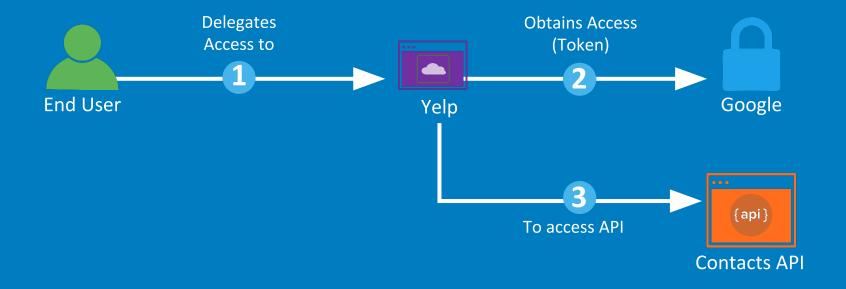
A lot of confusion around OAuth:

- Terminology and jargon
- × Incorrect advice
- Hard to find a life-like example

Hotel Analogy



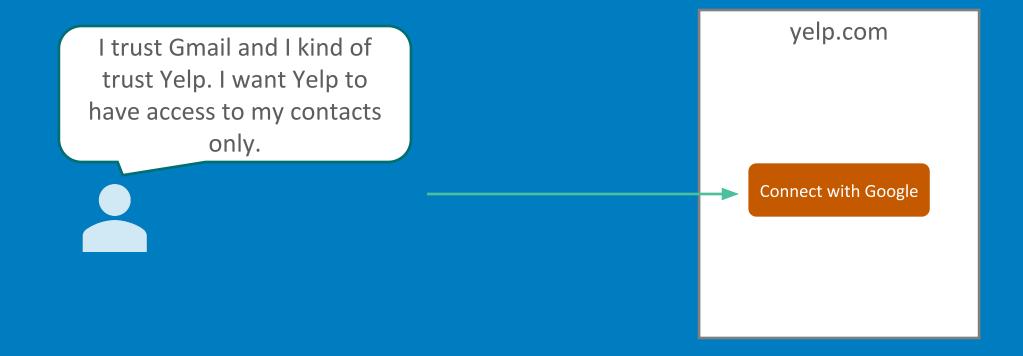
OAuth: App Scenario



OAuth 2.0 Terminology

Hotel	Арр	OAuth	Description
Hotel Guest	End User	Resource Owner	Wants a Client App to do something on their behalf
Hotel	Yelp	Client Application	Needs authorization to interact with an API on behalf of a user
Hotel Receptionist	Google	Authorization Server	Grants access (in the form of tokens) to an app
Hotel Room	Contacts API	Resource Server	Has an API that an app can use if presented with a token

Delegated authorization with OAuth 2.0



OAuth 2.0 implicit flow

Client

Yelp Angular app

Hello!

Go to authorization server

Redirect URI: yelp.com/callback

With token redirect URI

Response type: token

Scope: profile contacts

Resource owner

Talk to resource server with access token

contacts.google.com



Authorization server

accounts.google.com

Email

Password

Request consent from resource owner

accounts.google.com

Allow Yelp to access your public profile and contacts?

No

Yes

More OAuth 2.0 terminology

- ★ Back channel (highly secure channel)
- ★ Front channel (less secure channel)

OAuth 2.0 implicit flow

Client

Yelp Angular app

Hello!

Go to authorization server

Redirect URI: yelp.com/callback

Response type: token

Scope: profile contacts

Resource owner I

Talk to resource server with access token (back channel)

contacts.google.com



Back to redirect URI

(front channel)

Authorization server

accounts.google.com

Email

Password

Request consent from resource owner

accounts.google.com

Allow Yelp to access your public profile and contacts?

No

Yes

DEMO Implicit Flow Detector

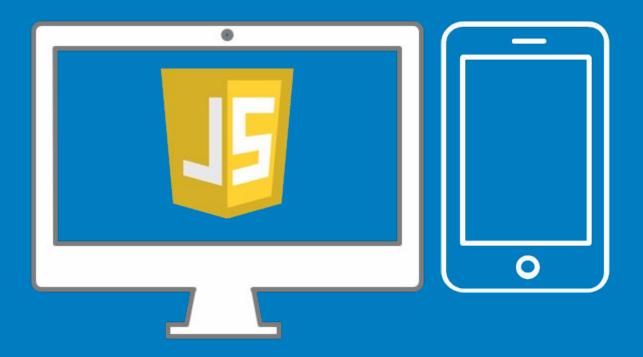
Confidential Clients

Public Clients





Has the ability to keep strings secret since code is running in a trusted environment



The application can't keep strings secret

Javascript/Single-Page apps: "view source" Native apps: decompile and extract strings

OAuth 2.0 authorization code flow

Client App

yelp.com

Connect with Google

Go to authorization server (front channel)

Redirect URI: yelp.com/callback

Response type: code

Scope: profile contacts

Resource owner

Talk to resource server with access token (back channel)

yelp.com/callback

Loading...



Exchange authorization code for access token (back channel) contacts.google.com

Back to redirect URI

with authorization code (front channel)

Authorization server

accounts.google.com

Email

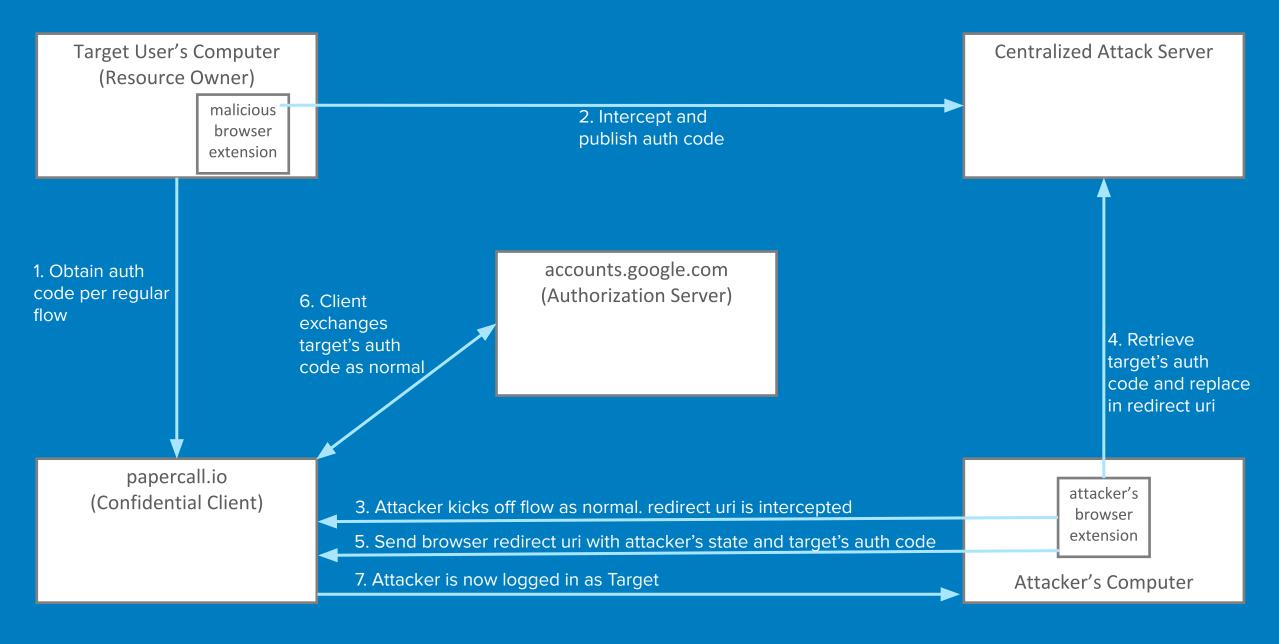
Password

Request consent from resource owner

accounts.google.com

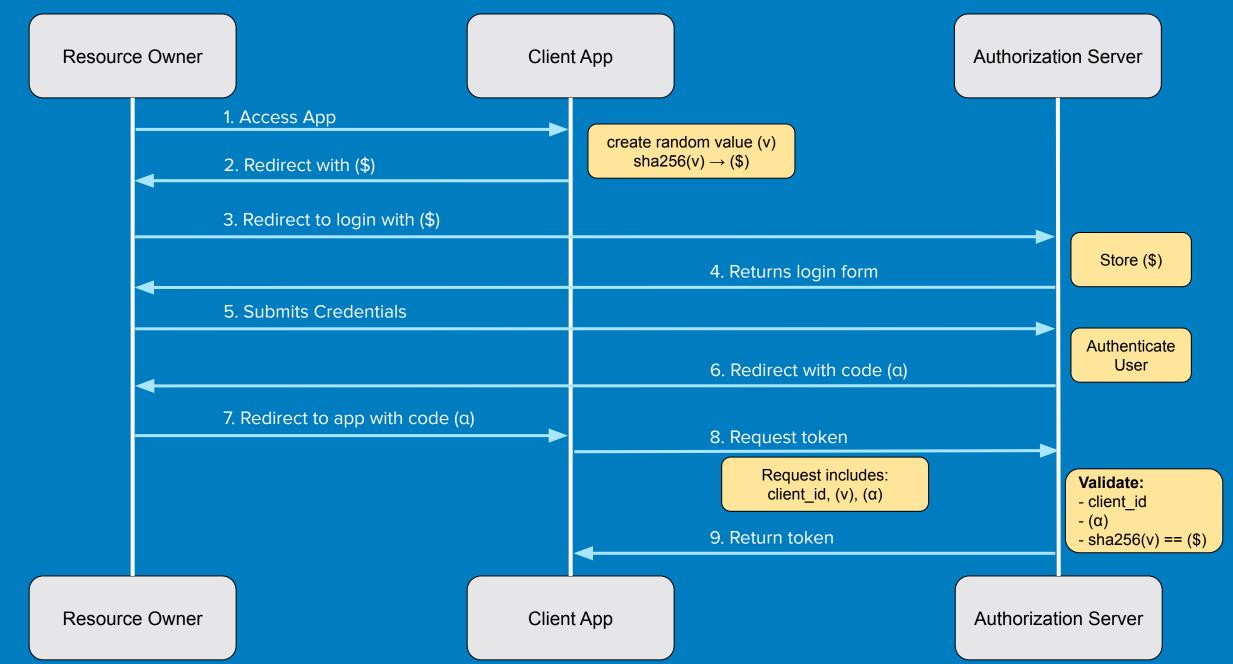
Allow Yelp to access your public profile and contacts?

Authorization Code Injection Attack



DEMO Auth Code Injection

OAuth 2.0 authorization code flow with PKCE



DEMO pkce-cli

Micah Silverman @afitnerd

@oktadev



Free hosted authorization server: developer.okta.com