draft-ietf-oauth-browser-based-apps-00
OAuth 2.0 for Browser-Based Apps

Aaron Parecki, David Waite

IETF 104
Mar 28 2019, Prague
OAuth 2.0 for Browser Based Apps

• Includes recommendations for implementors building browser-based apps using OAuth 2.0

• "Browser-based apps" are defined as applications running solely in a browser with no server-side component
OAuth 2.0 for Browser Based Apps

• **MUST** use the OAuth 2.0 authorization code flow with the PKCE extension

• **MUST NOT** return access tokens in the front channel (e.g. no Implicit flow)

• **MUST** use the OAuth 2.0 state parameter to carry one-time use CSRF tokens

• The AS **SHOULD** require an exact match of the redirect URI

• The AS **SHOULD NOT** issue refresh tokens to browser-based apps
High Level Questions

• Should the scope of this document be pure-JS apps, or broaden to any web app using JavaScript even if it has a backend component?

• With the Security BCP recommending PKCE for CSRF instead of state, should this document follow suit?

• Is there anything in the Security BCP that either does or does not work easily in browsers that we should handle differently here?
Specific Questions

• Does anyone have a deployment scenario that requires matching only the hostname of the redirect URL?

• For PKCE, is S256 reasonable to require in JavaScript? (are there good browser APIs or JS libraries for this?)

• Should we also disallow the password grant in JS apps?
Q & A