Exercise 4.3: Writing an OPA Policy for Lead vs Contributor Access

1. Write an OPA policy for an API server that allows a Team-Lead READ/WRITE/UPDATE/DELETE access to the /members endpoint and allows a Team-Contributor READ access to the /members endpoint
2. Extra Challenge: Modify the example provided for buyer user types to work for engineering platform user types

To tackle this exercise, you'll need to remember our learnings from 3.3 with OPA and incorporate what we learned about OIDC to write a successful attribute-based policy. Think about how you might apply this policy in the real world; what identity systems might you use to authenticate your users? What authorization servers work with your identity system? For an added challenge, test your policy with real tokens; you can generate them at https://jwt.io, which is an open, industry-standard way of generating secure web tokens

Solution