Authentication (OpenID)

## Summary

The purpose of this exercise is to understand a single sign-on mechanism for web sites, OpenID, and then comment on its usefulness and security. Read about OpenID in the Stallings book, the OpenID website <http://openid.net/connect/faq/> or the Google Identity Platform: <https://developers.google.com/identity/protocols/OpenIDConnect>.

For this assignment, you will need an account from at least one of the following: Google, Facebook, Twitter(X), or GitHub. You will interact with a test site I have created for this lab: <https://kengraf-auth2.firebaseapp.com/>

You will complete the following actions:

1. Connect with your social network identity
2. Analyze the access token
3. Revoke access

## Tools/Resources

Websites:

<https://kengraf-auth2.firebaseapp.com/>

<https://jwt.io>

## Walkthrough

1. Install
2. A

A screenshot of a computer

Description automatically generated

I used Google with popup (pick yours)

A screenshot of a login

Description automatically generated

Result

A screenshot of a computer

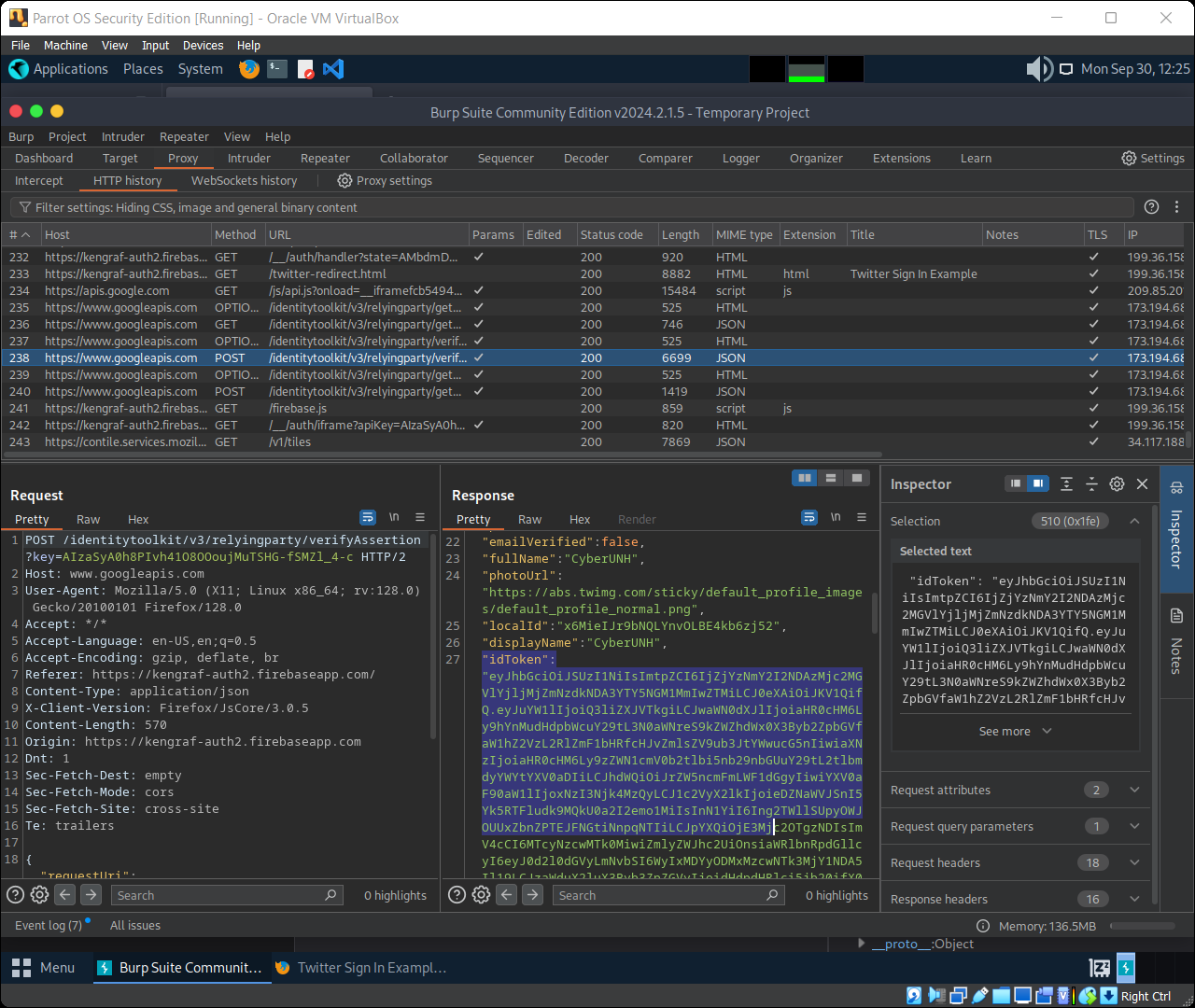
Description automatically generated

The access token is managed as a locally stored value and returned as an authentication token.

A screenshot of a computer

Description automatically generated

Or via Burp



Review the access token

Cut and paste your accessToken in to the online JWT decoder here. The signature

will not validate because the key material is not part of the JWT.

Capture screenshots of a successful login and the output from decoding the accessToken.

A screenshot of a computer

Description automatically generated

**Tips/Questions:**

Why do some sites require a real email address as the user name?

Were there additional headers in the browser response not shown on the web page?

What does a refresh token do?