Jonathan Disla

Assignment 8.1

Web 420

Prof. Krasso

Modern internet users are used to web cache that allows for sites they visit normally to load up faster. Caching either on a server or client-side improves the site performance. When a request comes in through HTTP, the browser cache checks if the resource is available in cache memory. If the resource is not in the browser cache on the client-side, then the data is fetched from the server (the roadmap). The data can then become part of the cache for later use. However, it can be dangerous if sensitive and private information is stored in the cache. Cache-control is a feature that can tell the header to cache certain types of information as long as the response doesn’t contain a separate statement (webpwnized).

There are different types of authentication methods to manage security in APIs. Within the basic methods are HTTP and Bearer. HTTP is the least secure while bearer authentication uses tokens to authorize the “bearer” of the information to gain access. Another way to manage security in APIs is to use API keys. “In this method, a unique generated value is assigned to each first-time user, signifying that the user is known..their unique key...is used to prove that they’re the same user as before” (Levin). API keys are used in other settings as well. OAuth 1 and 2 are very commonly used which is when logging into a site requires a token. The token is checked by the server and has a limited age of validity. JWT was developed by Auth0 allows for the generation of tokens.

References

Levin Guy. “*4 Most Used Rest API Authentication Methods*”.Restcase, 26 July 2019.

<https://blog.restcase.com/4-most-used-rest-api-authentication-methods/>

The Roadmap. “*Everything you need to know about HTTP Caching”.* YouTube, 4 October 2020.

https://www.youtube.com/watch?v=HiBDZgTNpXY&ab\_channel=theroadmap

Webpwnized. “*How Cache Control Headers Work*”.YouTube, 25 February 2021.

<https://www.youtube.com/watch?v=Df8l_epP38k&ab_channel=webpwnized>