Can we create multiple JWT's against one user? #231

Closed **Awais-cb** opened this issue on Oct 24, 2018 · 3 comments

Awais-cb commented on Oct 24, 2018 • edited

I have some questions

1. Can we create multiple tokens against one user if yes how? if no why?
2. lets consider a scenario where users wants to be logged in from mobile and web application too at the same what would happen?
3. what if user wants to logout how we are supposed to refresh/destroy/replace old token?

any help regarding would be really appreciated also it would be nice if i can a documentation about this library

😄 1

cottton commented on Oct 26, 2018

1. You can create more than one JWT for one user. *Even for the same device (which would not make sense but ...).*

2. Each device gets its own JWT.
   Example:

- User logged in via mobile (server creates and returns JWT)
- User logged in via web app (server creates and returns JWT)
- User requests via mobile using its JWT. Server validates JWT and sends response.
- User requests via web app using its JWT. Server validates JWT and sends response.

Web apps actually could use another adapter like PHP session cookies. Imo you should add adapters anyway. One for JWT session, one for PHP session cookies, ...

JWT is **not** like your passport.
The passport would be your login credentials.
Lets say the JWT is a bus ticket.

- You request one bus ticket with your passport.
- You request another bus ticket with your passport.

You of curse COULD set a limit by the server. F.e. 5 JWT per user id or 1 JWT per device. You then would have to store the JWT on the server. But thats not the point of JWT. JWT is meant to be stateless. They are signed and their content immutable.
The server created the JWT using a private key. Clients can validate the JWT (signature) using the public key. If you change the token (content) then the signature does not fit and its no longer valid.

3.

Logout: Same answer as posted here: #230
Refresh: client wants a new access token

- client sends refresh token
- server validate stored refresh token
- server removes the (now burned) refresh token
- server creates new refresh and access -token
- server returns both tokens
  A refresh token is for one time use only

Destroy: Is a logout.
Replace: ? Would be a refresh.

👍 5

NielsDom commented on Jun 29, 2019

@cottton very good answer thanks
@Awais-cb you should close this issue

Awais-cb commented on Jun 29, 2019 Author

yeah thanks cotton your answer is great

Awais-cb closed this on Jun 29, 2019

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Linked pull requests

Successfully merging a pull request may close this issue.

None yet

3 participants