AuthController – API Authorization

Create a new util file -> enum -> Authority.java

```
package org.studyeasy.SpringRestdemo.util.constants;

public enum Authority {
    READ,
    WRITE,
    UPDATE,
    USER,   //CAN UPDATE DELETE SELF OBJECT, READ ANYTHING
    ADMIN   //CAN READ UPDATE DELETE ANY OBJECT
}
```

Modify Account.java

```
private String role;
```

to

```
private String Authorities;
```

Fix Error in AccountService.java and do in others where you get error

Instead of getRole() and setRole(), replace with getAuthorities() and setAuthorities()

In save() method – change the below line

```
public Account save(Account account) {
        account.setPassword(passwordEncoder.encode(account.getPassword()));
        if(account.getAuthorities() == null){
            account.setAuthorities("ROLE_USER);
        }
        return accountRepository.save(account);
    }
```

```
account.setAuthorities("ROLE_USER);
```

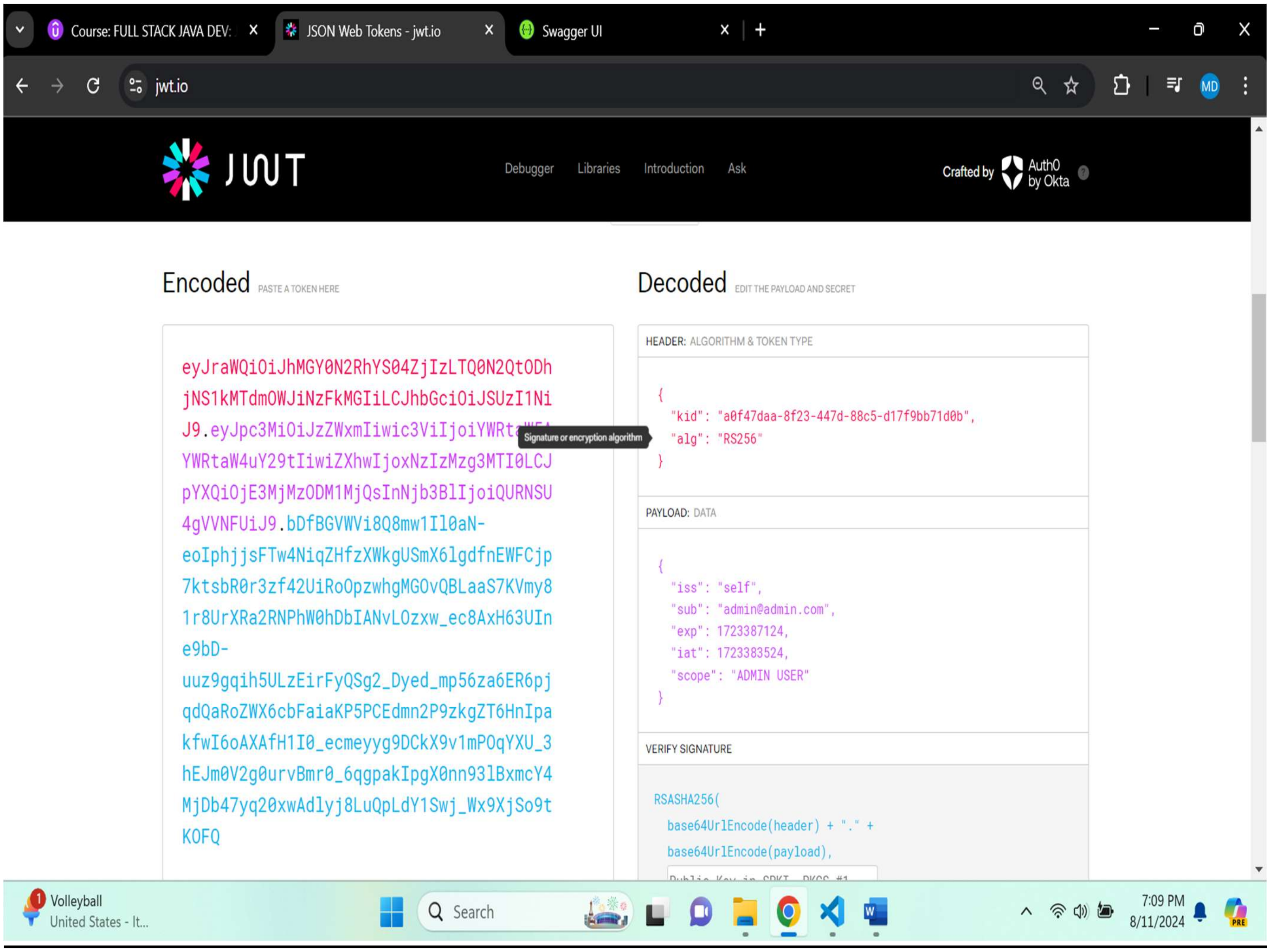
Update to

```
 account.setAuthorities(Authority.USER.toString());
```

Updated SeedData.java

```
package org.studyeasy.SpringRestdemo.config;

import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.boot.CommandLineRunner;
import org.springframework.stereotype.Component;
import org.studyeasy.SpringRestdemo.model.Account;
import org.studyeasy.SpringRestdemo.service.AccountService;
import org.studyeasy.SpringRestdemo.util.constants.Authority;

@Component
public class SeedData implements CommandLineRunner{

    @Autowired
    private AccountService accountService;

    @Override
    public void run(String... args) throws Exception {
        Account account01 = new Account();
        Account account02 = new Account();

        account01.setEmail("user@user.com");
        account01.setPassword("pass987");
        account01.setAuthorities(Authority.USER.toString());
        accountService.save(account01);

        account02.setEmail("admin@admin.com");
        account02.setPassword("pass987");
        account02.setAuthorities(Authority.ADMIN.toString() + " " +
Authority.USER.toString());
        accountService.save(account02);
    }

}
```

Output



Encoded PASTE A TOKEN HERE

```
eyJraWQiOiJhMGY0N2RhYS04ZjIzLTQ0N2QtODh
jNS1kMTdmOWJiNzFkMGIiLCJhbGciOiJSUzI1Ni
J9.eyJpc3MiOiJzZWxmIiwic3ViIjoiYWRta
YWRtaW4uY29tIiwiZXhwIjoxNzIzMzg3MTI0LCJ
pYXQiOjE3MjMzODM1MjQsInNjb3BlIjoiQURNSU
4gVVNFUiJ9.bDfBGVWVi8Q8mw1Il0aN-
eoIphjjsFTw4NiqZHfzXWkgUSmX6lgdfnEWFCjp
7ktsbR0r3zf42UiRoOpzwhgMGOvQBLaaS7KVmy8
1r8UrXRa2RNPhW0hDbIANvLOzxw_ec8AxH63UIn
e9bD-
uuz9gqih5ULzEirFyQSg2_Dyed_mp56za6ER6pj
qdQaRoZWX6cbFaiaKP5PCEdmn2P9zkgZT6HnIpa
kfwI6oAXAfH1I0_ecmeyyg9DCkX9v1mPOqYXU_3
hEJm0V2g0urvBmr0_6qgpakIpgX0nn93lBxmcY4
MjDb47yq20xwAdlyj8LuQpLdY1Swj_Wx9XjSo9t
KOFQ
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "kid": "a0f47daa-8f23-447d-88c5-d17f9bb71d0b",
  "alg": "RS256"
}
```

PAYLOAD: DATA

```
{
  "iss": "self",
  "sub": "admin@admin.com",
  "exp": 1723387124,
  "iat": 1723383524,
  "scope": "ADMIN USER"
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
```

In SecurityConfig.java

Update below line

```
.requestMatchers("/auth/users").hasAuthority("SCOPE_ROLE_USER")
```

To

```
.requestMatchers("/auth/users").hasAnyAuthority("SCOPE_ADMIN")
```

Output

In this, when you want to display list of users -> you get error.

So, you authorize using token by generating it and authorizing it. Try to display list of users (ADMIN), you get list of users.

So, you authorize using token by generating it and authorizing it. Try to display list of users (USER), you get error.