Week 2: Security Enhancements -

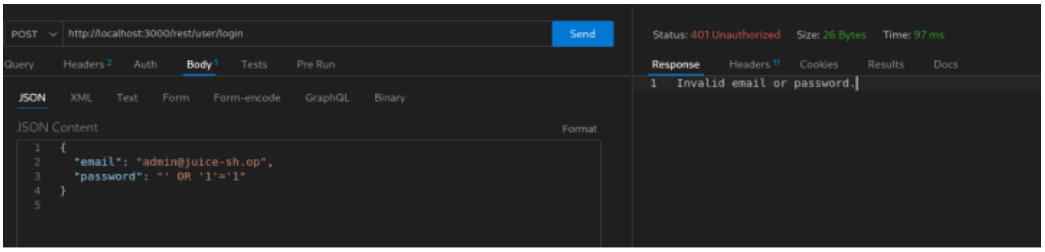
1. Input Validation:
Implemented validation using express-validator and manual checks in all user input routes including login, register, and profile.

2. Password Hashing:
Passwords are securely hashed using bcrypt before saving to the database to prevent credential theft in case of a data breach.

3. JWT Authentication:
Implemented JSON Web Token (JWT) authentication for secure session management and authorization.

4. Security Headers with Helmet.js:
Added Helmet middleware to the Express app to set security-related HTTP headers and mitigate common vulnerabilities.

Attached Evidences:



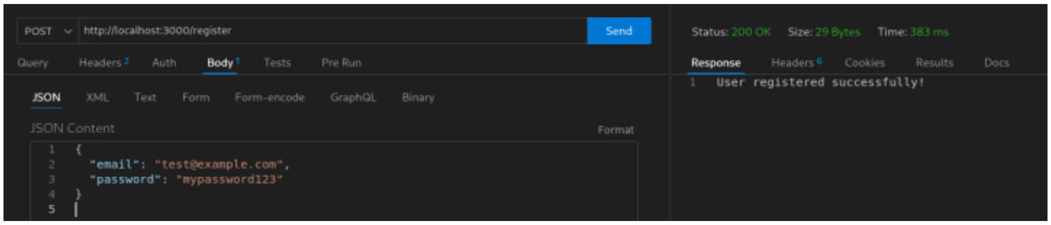
POST http://localhost:3000/rest/user/login

Status: 401 Unauthorized Size: 26 Bytes Time: 97 ms

JSON Content

```
{
  "email": "admin@juice-sh.op",
  "password": "' OR '1'='1"
}
```

```
Invalid email or password.
```



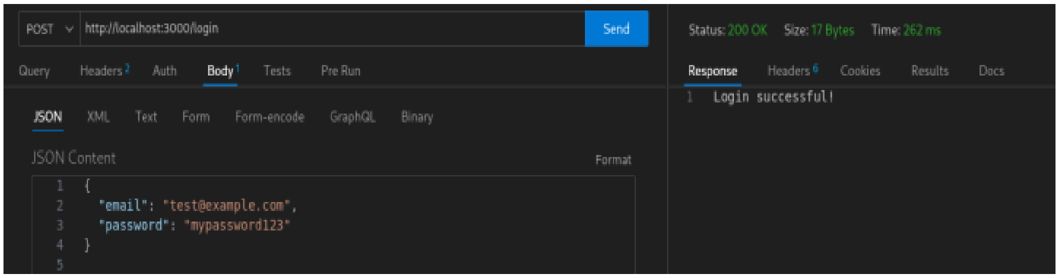
POST http://localhost:3000/register

Status: 200 OK Size: 29 Bytes Time: 383 ms

JSON Content

```
{
  "email": "test@example.com",
  "password": "mypassword123"
}
```

```
User registered successfully!
```



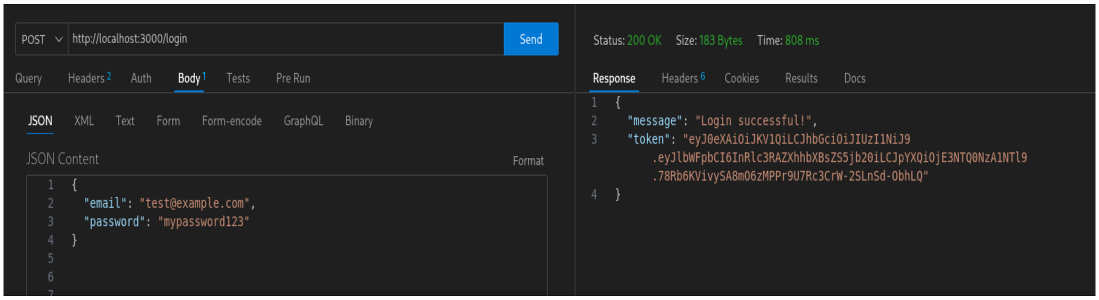
POST http://localhost:3000/login

Status: 200 OK Size: 17 Bytes Time: 262 ms

JSON Content

```
{
  "email": "test@example.com",
  "password": "mypassword123"
}
```

```
Login successful!
```

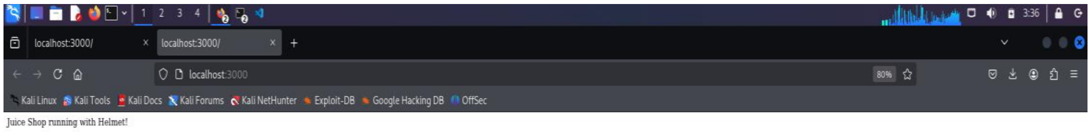


http://localhost:3000/login

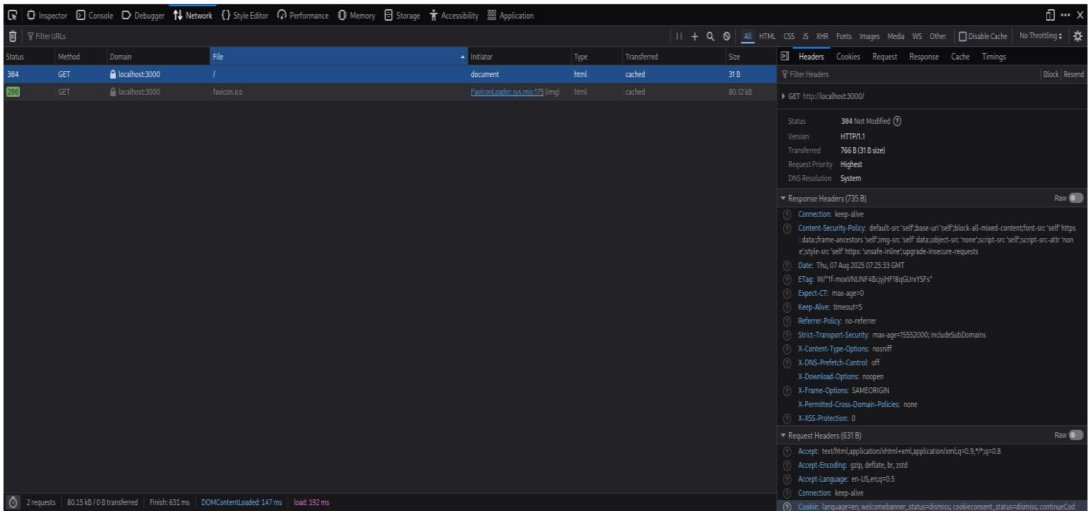
```
{
  "email": "test@example.com",
  "password": "mypassword123"
}
```

Status: 200 OK   Size: 183 Bytes   Time: 808 ms

```
{
  "message": "Login successful!",
  "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
     .eyJlbWFpbCI6InRlc3RAZXhhbXBsZS5jb20iLCJpYXQiOjE3NTQ0NzA1NTl9
     .78Rb6KVivySA8mO6zMPPr9U7Rc3CrW-2SLnSd-ObhLQ"
}
```



Juice Shop running with Helmet!



Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	localhost:3000	/	document	html	cached	31 B
200	GET	localhost:3000	favicon.ico	FaviconLoader.sys.mjs:175 (img)	html	cached	80.12 kB

GET http://localhost:3000/

Status 304 Not Modified
Version HTTP/1.1
Transferred 766 B (31 B size)
Request Priority Highest
DNS Resolution System

Response Headers (735 B)

```
Connection: keep-alive
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;font-src 'self' https
: data:;frame-ancestors 'self';img-src 'self' data:;object-src 'none';script-src 'self';script-src-attr 'non
e';style-src 'self' https: 'unsafe-inline';upgrade-insecure-requests
Date: Thu, 07 Aug 2025 07:25:33 GMT
ETag: W/"1f-moxVNUNF4BcjyjHF18qGUnYSFs"
Expect-CT: max-age=0
Keep-Alive: timeout=5
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Content-Type-Options: nosniff
X-DNS-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 0
```

Request Headers (631 B)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCod
```

2 requests | 80.15 kB / 0 B transferred | Finish: 631 ms | DOMContentLoaded: 147 ms | load: 192 ms