

نمای کلی این API برای **احراز هویت کاربران، مدیریت کاربران، مدیریت توکن‌ها و تغییر نقش‌ها** استفاده می‌شود. از **JWT** برای توکن‌های دسترسی و تازه‌سازی و از **پایگاه داده MySQL** برای ذخیره اطلاعات کاربران استفاده می‌کند. تنها کاربران با نقش **admin** می‌توانند به برخی endpointها مانند مشاهده همه کاربران، حذف کاربر یا تغییر نقش دسترسی داشته باشند.

آدرس پایه: http://<server_ip>:8080 احراز هویت: توکن JWT به صورت Bearer (برای endpointهای محافظت شده)

Endpoint

1. ثبت نام (Sign Up)

ایجاد یک کاربر جدید. - آدرس: /signup - روش: POST - هدرها: Content-Type: application/json - بدنه درخواست:

```
{
  "username": "john",
  "password": "mypassword"
}
```

- پاسخ‌ها: 201 ایجاد شد: { "message": "user registered successfully" } - 401 عدم دسترسی!
- 400 درخواست نادرست: { "error": "username or password are not valid" } - نمونه curl:

```
curl -X POST http://localhost:8080/signup
-H "Content-Type: application/json"
-d '{"username": "john", "password": "mypassword"}'
```

2. ورود (Login)

احراز هویت کاربر و دریافت توکن دسترسی و تازه سازی. - آدرس: /login - روش: POST - هدرها: Content-Type: application/json - بدنه درخواست:

```
{
  "username": "john",
  "password": "mypassword"
}
```

- پاسخها: - OK 200 ✓:

```
{
  "success": true,
  "role": "user",
  "message": "Login successful",
  "access_token": "<ACCESS_TOKEN>",
  "refresh_token": "<REFRESH_TOKEN>"
}
```

- **401 عدم دسترسی** - رمز عبور یا کاربر اشتباه است - **400 درخواست نادرست** ! - نام کاربری یا رمز عبور خالی است - نمونه curl:

```
curl -X POST http://localhost:8080/login
-H "Content-Type: application/json"
-d '{"username": "john", "password": "mypassword"}'
```

3. تازہسازی توکن دسترسی (Refresh Token)

دریافت توکن دسترسی جدید با استفاده از توکن تازہسازی معتبر. - آدرس: /refresh - روش: POST - هدرها: Content-Type: application/json - بدنه درخواست:

```
{
  "refresh_token": "<REFRESH_TOKEN>"
}
```

- پاسخها: - **OK 200** : "new access token generated", "success": true } - **401 عدم دسترسی** - توکن تازہسازی منقضی یا نامعتبر است - **400 درخواست نادرست** ! - توکن تازہسازی ارائه نشده - نمونه curl:

```
curl -X POST http://localhost:8080/refresh
-H "Content-Type: application/json"
-d '{"refresh_token": "<REFRESH_TOKEN>"}'
```

4. مشاهده همه کاربران (Admin Only)

لیست همه کاربران ثبت نام شده (فقط برای مدیران). - آدرس: /users - روش: GET - هدرها: Authorization: Bearer <ACCESS_TOKEN> - پاسخها: - **OK 200** - بازگشت آرایه ای از کاربران

```
[
  { "username": "john", "role": "user" },
  { "username": "admin", "role": "admin" }
]
```

- **403 ممنوع** - کاربران غیرمدیر نمی‌توانند دسترسی داشته باشند - **401 عدم دسترسی** - توکن ارائه نشده یا نامعتبر است - **نمونه curl:**

```
curl -X GET http://localhost:8080/users
-H "Authorization: Bearer <ACCESS_TOKEN>"
```

5. حذف کاربر (Delete User)

حذف کاربر بر اساس نام کاربری (فقط برای مدیران). - آدرس: `/users/{username}` - روش: **DELETE** - هدرها: `Authorization: Bearer <ACCESS_TOKEN>` - پاسخها: **OK 200** - حذف کاربر با موفقیت انجام شد - **404 یافت نشد** - کاربر موجود نیست - **403 ممنوع** - کاربران غیرمدیر یا توکن نامعتبر - **400 درخواست نادرست** - نام کاربری نادرست - **نمونه curl:**

```
curl -X DELETE http://localhost:8080/users/john
-H "Authorization: Bearer <ACCESS_TOKEN>"
```

6. تغییر نقش کاربر (Change User Role)

تغییر نقش یک کاربر (فقط برای مدیران). - آدرس: `/users/{username}` - روش: **PUT** - هدرها: `Authorization: Bearer <ACCESS_TOKEN>` - بدنه درخواست:

```
{
  "new_role": "admin"
}
```

- پاسخها: **OK 200** - نقش با موفقیت تغییر کرد - **404 یافت نشد** - کاربر موجود نیست - **403 ممنوع** - کاربران غیرمدیر یا توکن نامعتبر - **400 درخواست نادرست** - نام کاربری یا نقش نامعتبر - **نمونه curl:**

```
curl -X PUT http://localhost:8080/users/john
-H "Authorization: Bearer <ACCESS_TOKEN>"
-H "Content-Type: application/json"
-d '{"new_role": "admin"}'
```

احراز هویت

- **توکن دسترسی:** JWT کوتاه‌مدت (۱ ساعت)، برای endpoint های محافظت شده (`/users`, `/delete`, `/refresh`) استفاده می‌شود.
- **توکن تازه‌سازی:** JWT بلندمدت (۱۰ روز)، برای دریافت توکن دسترسی جدید از طریق `/refresh` استفاده می‌شود.
- توکن‌ها در هدر `Authorization` به صورت `Bearer <token>` ارسال می‌شوند.

کدهای خطا

کد وضعیت	توضیح
200	✓ موفقیت آمیز
201	✓ ایجاد منبع جدید
400	⚠ درخواست نادرست (پارامترهای ناقص یا نامعتبر)
401	⊖ عدم دسترسی (اعتبارنامه یا توکن نامعتبر)
403	⊖ ممنوع (دسترسی کافی نیست)
404	⚠ مورد یافت نشد
500	خطای سرور (پایگاه داده یا خطای داخلی)