ÖDEV-7

Swagger Nedir?

Swagger Rest API geliştirmek için gereken bir sözleşme standartıdır. İki bilgisayarın anlaşmasını Rest API'ler kullanarak gerçekleştiriyoruz. Fakat bu bir standart olmadığı için haberleşme konusunda kolaylık sağlamamaktadır. Swagger OpenAPI standardı sayesinde API'lerimizi hem insanların hem de makinelerin anlayacağı ortak bir dilde sunabilmekteyiz. Bir diğer önemli nokta ise dokümantasyondur. Servislerimizde API methodlarının ne işe yaradıklarını herkesin anlayacağı bir şekilde dokümanının hazırlamalıyız. Bunu yapmak geliştiriciler için zor bir durumdur ayrıca güncel tutmak oldukça zordur. Bu dokümanların otomatik bir şekilde oluşturmasını Swagger ile yapabiliriz.

Nasıl Kullanılır?

API'nizin sunduğu endpoint'leri, parametreleri, veri türlerini ve verdiği cevapları tanımlayabiliriz. Bu tanımlamaları yaparken, Swagger kendi dili olan Swagger YAML veya JSON formatında bir dosyaya yazılır.

Swagger'ın İşlevleri Nelerdir?

API Dokümantasyonu

Swagger, API'nin işlevselliğini parametreleri ve yanıtları ayrıntılı bir şekilde belgeleyerek geliştiricilere açık bir rehberlik sağlar.

Test İmkanı

Swagger UI, geliştiricilere API'yi test etme olanağı tanır. API çağrıları yapılarak gerçek zamanlı sonuçlar görüntülenebilir.

Kod Üretme

Swagger, API'ye dayalı olarak otomatik olarak kod üretebilir. Geliştiricilere zaman kazandırır.

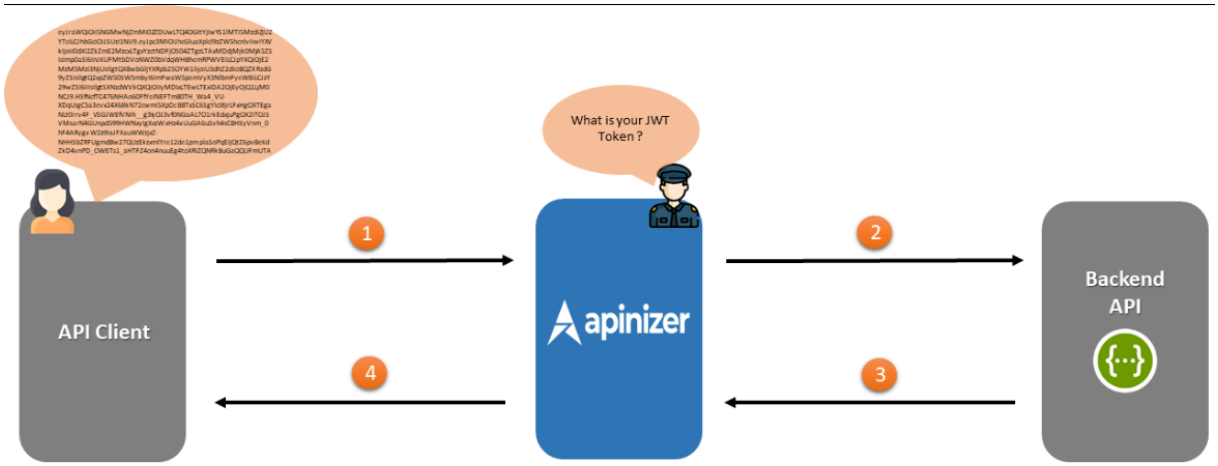
Mükemmel Uyumluluk

Swagger, RESTful API'lerle çok iyi uyumluluk sağlar.

JWT, Basic Auth yapıları swagger ile nasıl test edilir?

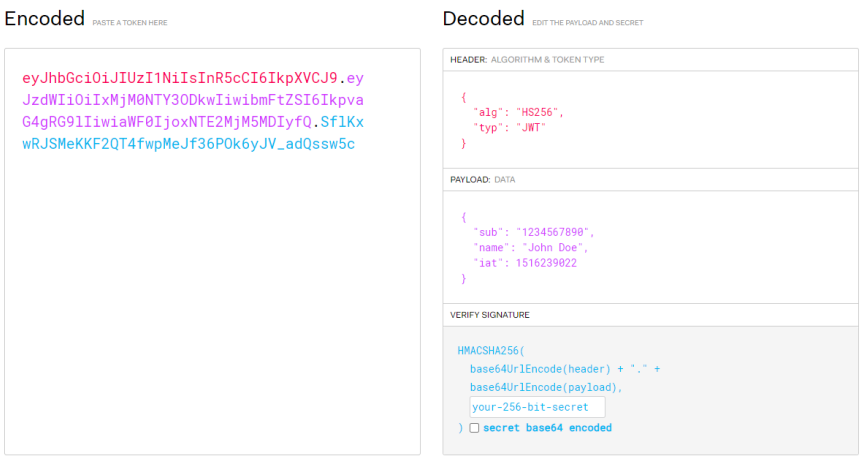
JWT (Json Web Token), IETF kuruluşu tarafından tasarlanan standart bir token biçimi olarak tanımlanır. Haberleşen iki sistem arasında kullanıcı doğrulama, kullanıcı tanıma bilgi güvenliğini koruma gibi işlemler gerçekleştirir.

Örneğin sunucu kullanıcının yönetici ayrıcalıklarına sahip olduğunu belirten bir anahtar (token) oluşturabilir. Bunu kullanıcıya gönderebilir ve kullanıcı bu anahtar ile kendisine tanımlanmış olan yönetici yetkisini bir istemci de kullanabilir. Kullanıcı siteye bulunduğu ilk istekte site tarafından kimlik doğrulamasına oluşur. Web sitesi JSON parçası gönderir. Kullanıcı tekrar sisteme giriş yapmak istediğinde bu parça ile giriş yapar ve web sitesi tarafından doğrulanır. Ayrıca Swagger UI'de authorization kullanmak, API güvenliğini sağlama ve kontrolü artırma konusunda önemli bir stratejidir.



Bu token, 3 segmentten oluşmaktadır.

- 1.segment: Kullanılan algoritmanın tipini söyler.
- 2.segment: Bu token üzerinde yaşayan bilgileri söyler. Yani claimi ifade eder.
- 3.segment: Bu tokenin hash kodunu söyler. Hash kodu, kırılırsa token kırılmış olur. Hash kodu kırılamadığı sürece bu tokenın kırılamayacağı anlaşılır. Bu token ile methodları çağırıyoruz.



Test işleminin adımları:

1.adım ***securitySchemes tanımlama***

API tarafından kullanılan tüm **securitySchemeler** components/securitySchemes bölümünde tanımlanmalıdır.

http – Temel, Taşıyıcı ve diğer HTTP kimlik doğrulama şemaları için

apiKey – API anahtarları ve çerez kimlik doğrulaması için

oauth2 – OAuth 2 için

openIdConnect – OpenID Connect Discovery için

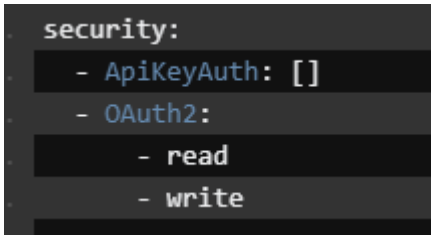
BasicAuth gibi çeşitli securitychemesların nasıl tanımlandığını gösterilmektedir.

```yaml
components:
  securitySchemes:

    BasicAuth:
      type: http
      scheme: basic

    BearerAuth:
      type: http
      scheme: bearer

    ApiKeyAuth:
      type: apiKey
      in: header
      name: X-API-Key

    OpenID:
      type: openIdConnect
      openIdConnectUrl: https://example.com/.well-known/openid-configuration

    OAuth2:
      type: oauth2
      flows:
        authorizationCode:
          authorizationUrl: https://example.com/oauth/authorize
          tokenUrl: https://example.com/oauth/token
          scopes:
            read: Grants read access
            write: Grants write access
            admin: Grants access to admin operations
```

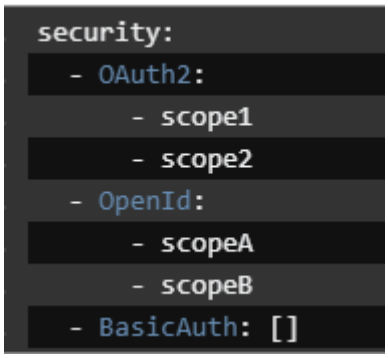
Güvenliği Uygulama

securitySchemes bölümünde güvenlik şemalarını tanımladıktan sonra, güvenlik bölümünü sırasıyla işlem düzeyine ekleyerek bunları tüm API'ye veya tek tek işlemlere uygulayabilirsiniz. Kök seviyesinde kullanıldığında security, işlem seviyesinde geçersiz kılınmadığı sürece belirtilen güvenlik şemalarını global olarak tüm API işlemlerine uygular.

Resimde API çağrıları bir API anahtarı veya OAuth 2 kullanılarak doğrulanabilir. ApiKeyAuth ve OAuth2 adları daha önce securitySchemes içinde tanımlanan şemaları ifade eder.



OAuth 2 ve OpenID Connect, çeşitli kullanıcı kaynaklarına yönelik izinleri kontrol etmek için kapsamları kullanır. Örneğin, bir evcil hayvan mağazası için kapsamlar read_pets, write_pets, read_orders, write_orders, admin'i içerebilir. Güvenlik uygulanırken, OAuth 2 ve OpenID Connect'e karşılık gelen girişlerin belirli bir işlem) veya tüm API çağrıları için gereken kapsamların bir listesini belirtmesi gerekir.



Postman ile API'yi Test Etme:

RestAPI, SOAP vb. Web tabanlı API çağrılarını test etmeye yarayan 3th parti bir araçtır. Testerlar tarafından kullanılan bir araçtır. Developerlar method çağrıları yaparken, testerlar güvenlik açıklarına odaklanır.

Swagger Dosyasını İçe Aktarma:Swagger ile oluşturduğunuz API tanım dosyasını Postman'e içe aktarın.

Request Oluşturma ve Gönderme:Postman'de API'nin her bir endpoint'ini test etmek için bir request oluşturun. Bu request'lerle API'ye çeşitli HTTP metodları ve parametreleri gönderebilirsiniz.

Response'ları Kontrol Etme:Her bir request'in response'ını kontrol edin. Başarılı veya başarısız yanıtları, durum kodlarını ve body içeriğini inceleyerek API'nin doğru şekilde çalışıp çalışmadığını kontrol edin.

Swagger Codegen ile API Test Etme

Swagger Codegen kullanarak API client kodu oluşturabilir ve bu kodu kullanarak API'yi test edebilirsiniz. Swagger Codegen ile API client kodunu oluşturmak için öncelikle API'nin Swagger tanım dosyasını seçmeniz gerekmektedir. Ardından Swagger Codegen aracını kullanarak, istediğiniz programlama dili ve çıktı formatı için API client kodunu üretmelisiniz. Bu kodu inceleyerek API'yi kullanmak için gerekli olan sınıfları, fonksiyonları ve yapıları görebilirsiniz.

API client kodunu projenize entegre ettikten sonra, API'yi test etmek için gerekli olan HTTP isteklerini yapabilirsiniz. Swagger Codegen tarafından üretilen API client kodu, API'nin her bir endpoint'ini kullanmak için gerekli olan fonksiyonları ve yapıları içerir. Bu fonksiyonları kullanarak, API'ye istek gönderebilir ve aldığınız response'ları kontrol edebilirsiniz.