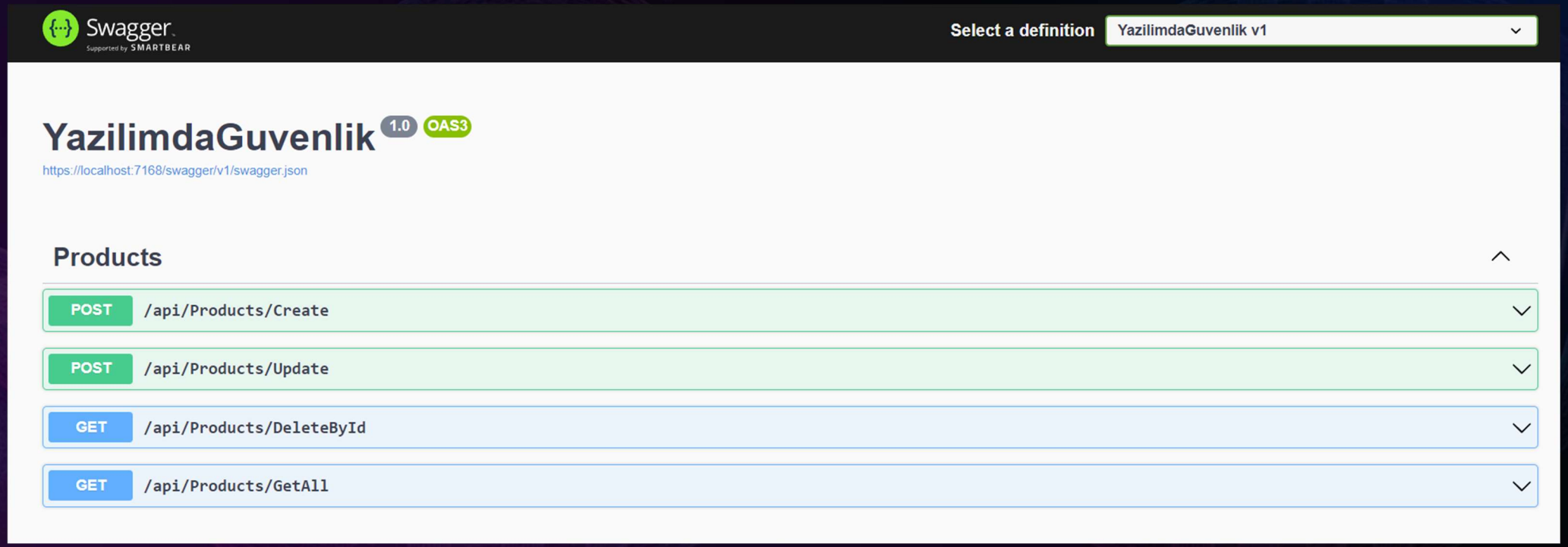
GÜVENLİ UYGULAMA GELİŞTİRME

Taner Saydam

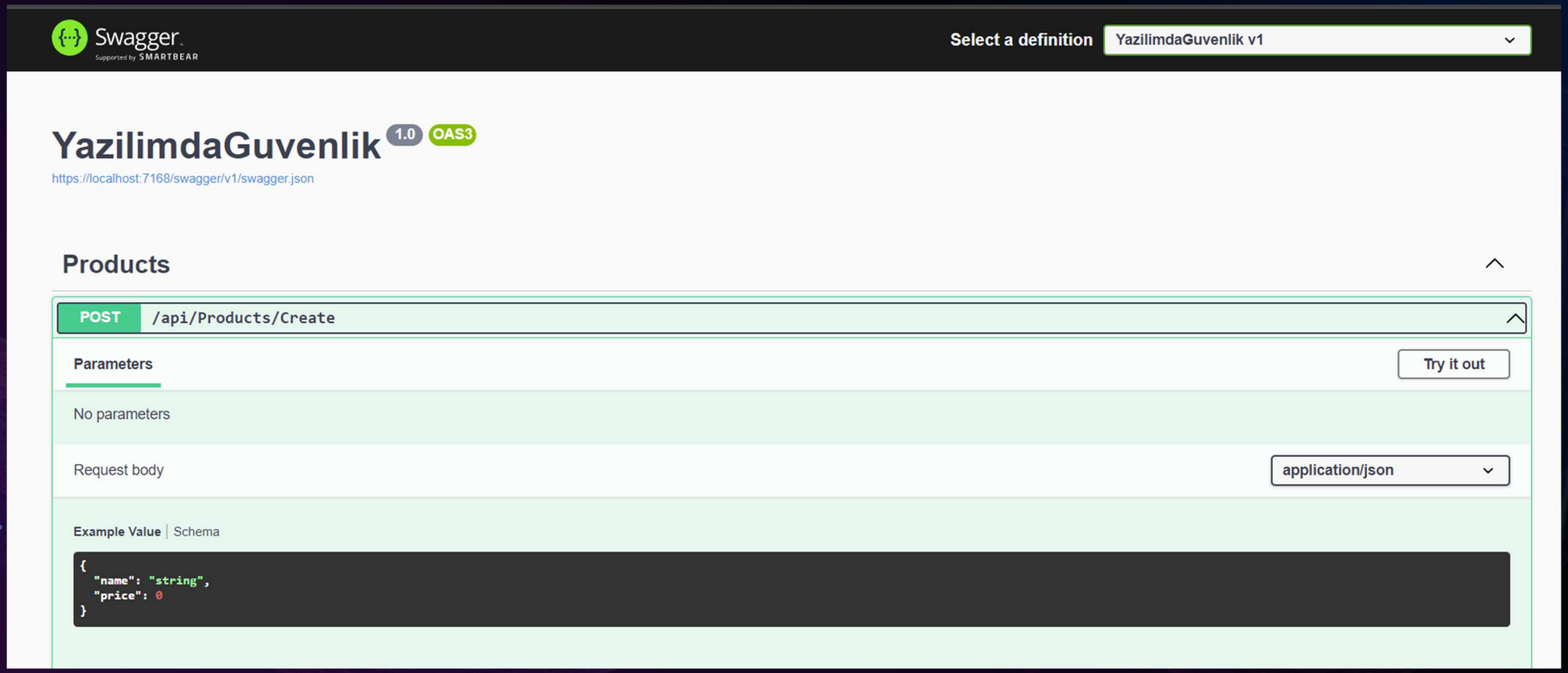
.NET Web Templates

- ASP.NET Web MVC
- ASP.NET Web API
- ASP.NET Blazor

```
namespace YazilimdaGuvenlik.Controllers;
[Route("api/[controller]/[action]")]
[ApiController]
0 references
public class ProductsController : ControllerBase
{
    [HttpPost]
    0 references
    public async Task<IActionResult> Create(CreateProductDto request, CancellationToken cancellationToken)...

    [HttpPost]
    0 references
    public async Task<IActionResult> Update(UpdateProductDto request, CancellationToken cancellationToken)...

    [HttpGet]
    0 references
    public async Task<IActionResult> DeleteById(int id, CancellationToken cancellationToken)...

    [HttpGet]
    0 references
    public async Task<IActionResult> GetAll(CancellationToken cancellationToken)...
}
```

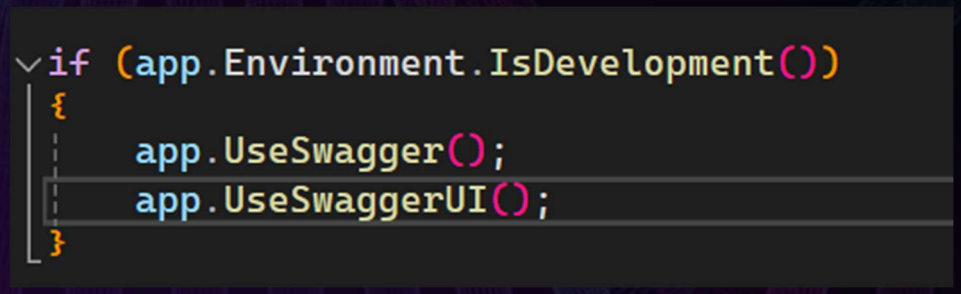

Swagger
Supported by SMARTBEAR
Select a definition
YazilimdaGuvenlik v1
YazilimdaGuvenlik
1.0
OAS3
https://localhost:7168/swagger/v1/swagger.json
Products
POST
/api/Products/Create
POST
/api/Products/Update
GET
/api/Products/DeleteById
GET
/api/Products/GetAll

```
if (app.Environment.IsDevelopment() | app.Environment.IsProduction())
{
    app.UseSwagger();
    app.UseSwaggerUI();
}
```


Swagger
Supported by SMARTBEAR
Select a definition
YazilimdaGuvenlik v1
YazilimdaGuvenlik
1.0
OAS3
https://localhost:7168/swagger/v1/swagger.json
Products
POST
/api/Products/Create
Parameters
Try it out
No parameters
Request body
application/json
Example Value
Schema
{
"name": "string",
"price": 0
}

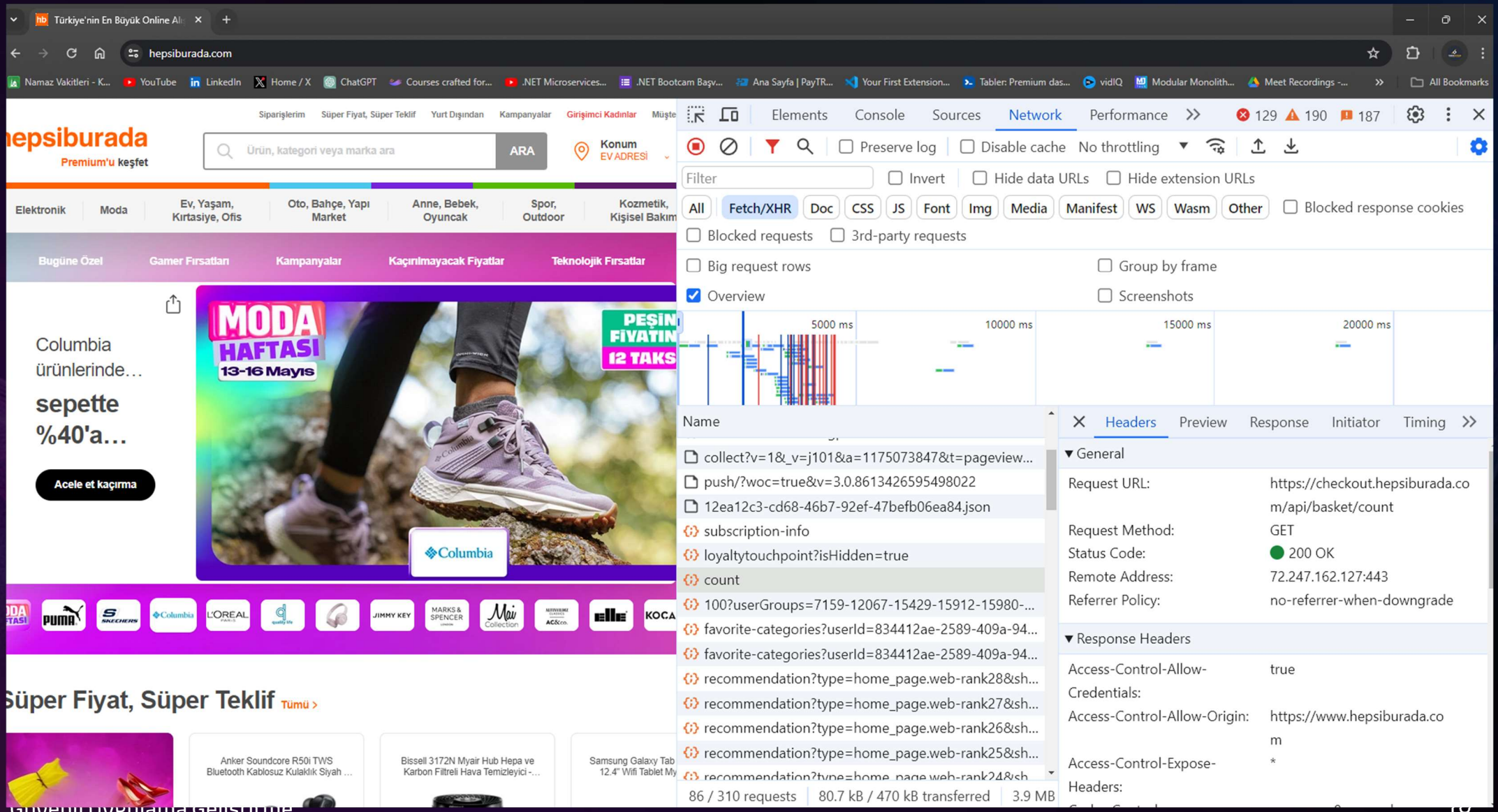
Olabilecek Güvenlik Açıkları

1. Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulabilirler


if (app.Environment.IsDevelopment())
{
app.UseSwagger();
app.UseSwaggerUI();
}

Olabilecek Güvenlik Açıkları

1. ~~Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulabilirler~~


Türkiye'nin En Büyük Online Al
hepsiburada.com
Namaz Vakitleri - K...
YouTube
LinkedIn
Home / X
ChatGPT
Courses crafted for...
.NET Microservices...
.NET Bootcam Başv...
Ana Sayfa | PayTR...
Your First Extension...
Tabler: Premium das...
vidIQ
Modular Monolith...
Meet Recordings -...
All Bookmarks
hepsiburada
Premium'u keşfet
Ürün, kategori veya marka ara
ARA
Konum
EV ADRESİ
Siparişlerim
Süper Fiyat, Süper Teklif
Yurt Dışından
Kampanyalar
Girişimci Kadınlar
Elektronik
Moda
Ev, Yaşam, Kırtasiye, Ofis
Oto, Bahçe, Yapı Market
Anne, Bebek, Oyuncak
Spor, Outdoor
Kozmetik, Kişisel Bakım
Bugüne Özel
Gamer Fırsatları
Kampanyalar
Kaçırılmayacak Fiyatlar
Teknolojik Fırsatlar
Columbia ürünlerinde…
sepette %40'a…
Acele et kaçırma
MODA HAFTASI
13-16 Mayıs
PEŞİN FİYATIN
12 TAKS
Columbia
Süper Fiyat, Süper Teklif
Tümü
Anker Soundcore R50i TWS Bluetooth Kablosuz Kulaklık Siyah ...
Bissell 3172N Myair Hub Hepa ve Karbon Filtreli Hava Temizleyici -...
Samsung Galaxy Tab 12.4" Wifi Tablet My
Elements
Console
Sources
Network
Performance
129
190
187
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Blocked response cookies
Blocked requests
3rd-party requests
Big request rows
Group by frame
Overview
Screenshots
5000 ms
10000 ms
15000 ms
20000 ms
Name
collect?v=1&_v=j101&a=1175073847&t=pageview...
push/?woc=true&v=3.0.8613426595498022
12ea12c3-cd68-46b7-92ef-47befb06ea84.json
subscription-info
loyaltytouchpoint?isHidden=true
count
100?userGroups=7159-12067-15429-15912-15980-...
favorite-categories?userId=834412ae-2589-409a-94...
favorite-categories?userId=834412ae-2589-409a-94...
recommendation?type=home_page.web-rank28&sh...
recommendation?type=home_page.web-rank27&sh...
recommendation?type=home_page.web-rank26&sh...
recommendation?type=home_page.web-rank25&sh...
86 / 310 requests
80.7 kB / 470 kB transferred
3.9 MB
Headers
Preview
Response
Initiator
Timing
General
Request URL:
https://checkout.hepsiburada.com/api/basket/count
Request Method:
GET
Status Code:
200 OK
Remote Address:
72.247.162.127:443
Referrer Policy:
no-referrer-when-downgrade
Response Headers
Access-Control-Allow-Credentials:
true
Access-Control-Allow-Origin:
https://www.hepsiburada.com
Access-Control-Expose-Headers:
*

Olabilecek Güvenlik Açıkları

1. ~~Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulabilirler~~
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilirler

```
builder.Services.AddCors(action =>
{
    action.AddDefaultPolicy(policy =>
    {
        policy
        .WithOrigins("https://www.myui.com")
        .WithMethods("GET", "POST", "PUT", "DELETE")
        .WithHeaders("Authorization");
    });
});
```

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilirler

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler

```
using Microsoft.AspNetCore.Mvc;

namespace YazilimdaGuvenlik.Controllers;
[Route("api/[controller]/[action]")]
[ApiController]
0 references
public sealed class ValuesController : ControllerBase
{
    [HttpGet]
    0 references
    public async Task<IActionResult> SendAPIRequest(CancellationToken cancellationToken)
    {
        for (int i = 0; i < 1000000; i++)
        {
            HttpClient client = new HttpClient();
            await client.GetAsync("https://myapi.com/api/Product/GetAll", cancellationToken);
        }

        return NoContent();
    }
}
```

```
builder.Services.AddRateLimiter(options =>
{
    options.AddFixedWindowLimiter("fixed", configure =>
    {
        configure.PermitLimit = 100;
        configure.QueueLimit = 100;
        configure.Window = TimeSpan.FromSeconds(1);
        configure.QueueProcessingOrder = QueueProcessingOrder.OldestFirst;
    });
});
```

```
app.UseRateLimiter();
```

```
app.MapControllers().RequireRateLimiting("fixed");
```

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler

```
namespace YazilimdaGuvenlik.Controllers;
[Route("api/[controller]/[action]")]
[ApiController]
0 references
public sealed class ValuesController : ControllerBase
{
    [HttpGet]
    0 references
    public async Task<IActionResult> SendAPIRequest(CancellationToken cancellationToken)
    {
        HttpClient client = new HttpClient();

        HttpResponseMessage message = await client.GetAsync("https://myapi.com/api/Product/GetAll", cancellationToken);
        if (message.IsSuccessStatusCode)
        {
            object? products = await message.Content.ReadFromJsonAsync<object>();
            return Ok(products);
        }

        return BadRequest(new { Message = "We cannot reach the API!" });


    }
}
```

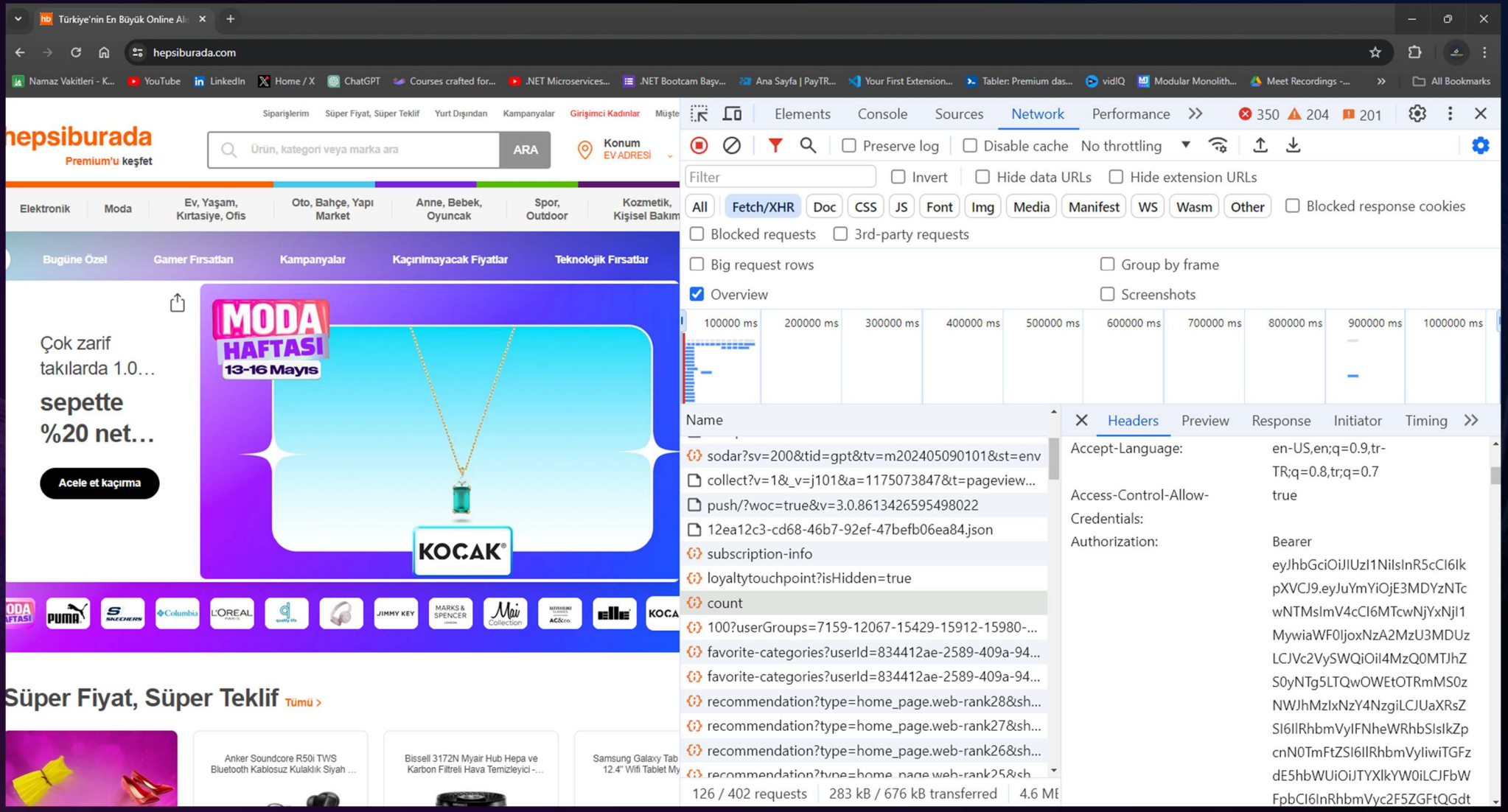
```
builder.Services.AddAuthentication().AddJwtBearer(options =>
{
    options.TokenValidationParameters = new()
    {
        ValidateIssuer = true,
        ValidateAudience = true,
        ValidateIssuerSigningKey = true,
        ValidateLifetime = true,
        ValidIssuer = builder.Configuration.GetSection("JWT:Issuer").Value,
        ValidAudience = builder.Configuration.GetSection("JWT:Audience").Value,
        IssuerSigningKey = signingKey
    };
});
builder.Services.AddAuthorization();
```

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler~~
5. Browserdan Authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler


hepsiburada.com
hepsiburada
Premium'u keşfet
ARA
Elektronik
Moda
Ev, Yaşam, Kırtasiye, Ofis
Oto, Bahçe, Yapı Market
Anne, Bebek, Oyuncak
Spor, Outdoor
Kozmetik, Kişisel Bakım
Bugüne Özel
Gamer Fırsatları
Kampanyalar
Kaçırılmayacak Fiyatlar
Teknolojik Fırsatlar
Çok zarif takılarda 1.0…
sepette %20 net…
Acele et kaçırma
MODA HAFTASI
13-16 Mayıs
KOCAK
Süper Fiyat, Süper Teklif
Tümü
Elements
Console
Sources
Network
Performance
Preserve log
Disable cache
No throttling
Filter
Invert
Hide data URLs
Hide extension URLs
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
Blocked response cookies
Blocked requests
3rd-party requests
Big request rows
Group by frame
Overview
Screenshots
Name
Headers
Preview
Response
Initiator
Timing
Accept-Language:
Access-Control-Allow-Credentials:
Authorization:
126 / 402 requests
283 kB / 676 kB transferred

Authentication Güvenlik Önlemleri

Two Factor Authentication

Aynı anda bir kişi giriş yapabilir

Belirli saatlerde erişim izni

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.AspNetCore": "Warning"
    }
  },
  "AllowedHosts": "*",
  "ConnectionStrings": {
    "SqlServer": "Connection String"
  },
  "JWT": {
    "Issuer": "Taner Saydam",
    "Audience": "www.tanersaydam.net",
    "Secret Key": "my secret key my secret key my secret key my secret key my secret key my
     secret key my secret key my secret key"
  }
}
```

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler~~
5. ~~Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler~~
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler

Hassas Bilgileri Sakala

Hassas bilgiler şifrenebilir

AWS Secrets Manager gibi Cloud sistemlere saklanabilir

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler

	Id	Name	Price
	1	Domates	1
	2	Salatalık	5
	3	Muz	15
	4	Patlıcan	100
▶*	NULL	NULL	NULL

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler~~
5. ~~Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler~~
6. ~~Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler~~
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler

Database verileri güvenlik önlemleri

Database erişimi IP bazlı kısıtlanabilir

Sürekli yedek alınarak (saatte bir) olası bir sorunda sorun tespit edilmeye çalışılabilir

Database'e atılan veriler şifrelenip, okunurken çözülebilir

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler

	Id	Name	Price
	1	Domates	1
	2	Salatalık	5
	3	Muz	15
	4	Patlıcan	100
▶*	NULL	NULL	NULL

www.myeticaret.com/products?id=1

Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler~~
5. ~~Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler~~
6. ~~Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler~~
7. ~~Database'de bulunan bilgilerimize erişip manipüle edilebilirler~~
8. ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir

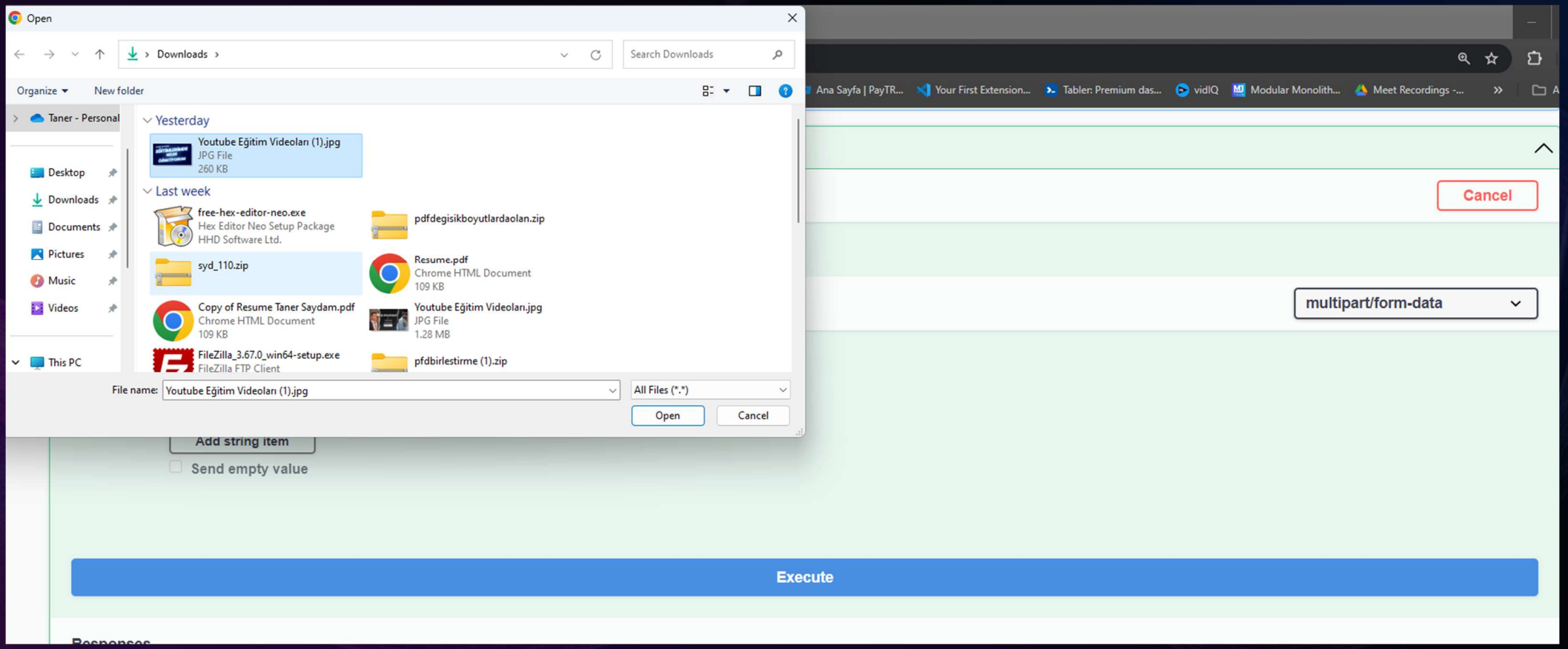
	Column Name	Data Type	Allow Nulls
🔑	Id	uniqueidentifier	☐
	Name	varchar(150)	☐
	Price	money	☐
			☐

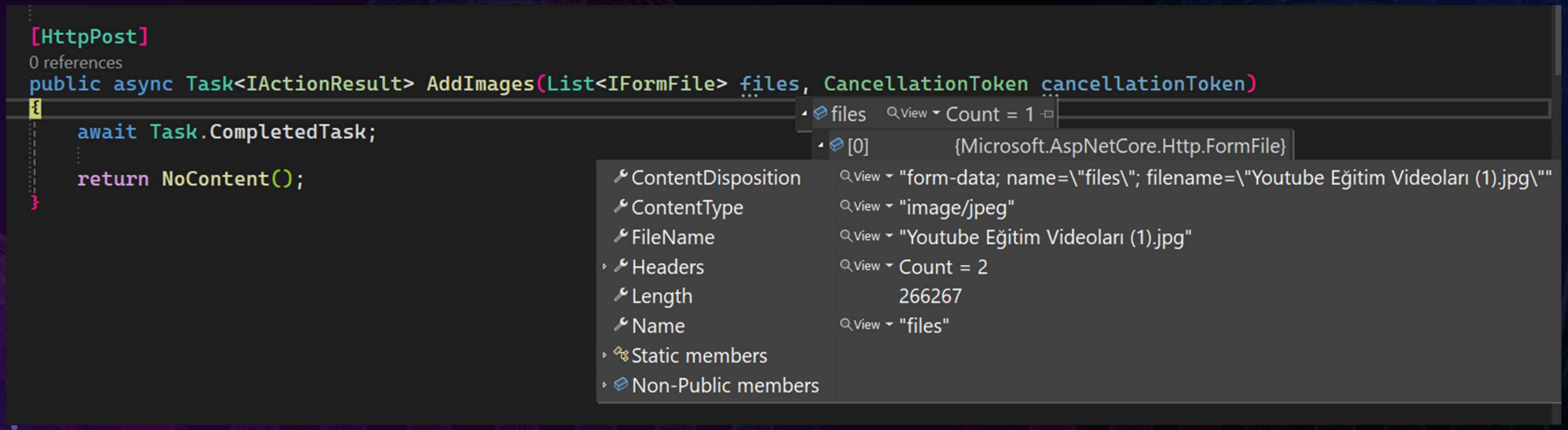
	Id	Name	Price
	2ef2c3a1-0722-4950-b286-513d5babc80f	Salatalık	2.0000
	29a3247b-1adf-4120-b299-58bb25a33fc6	Patlıcan	100.0000
	5b306436-edf0-4c39-8977-c2e992e45e21	Domates	1.0000
	60c60c5b-d9cc-4288-8d90-e6021a847802	Muz	10.0000
▶*	NULL	NULL	NULL

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler
8. ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir

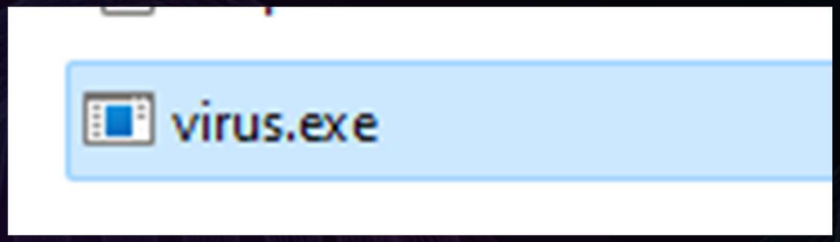
```
[HttpPost]
0 references
public async Task<IActionResult> AddImages(List<IFormFile> files, CancellationToken cancellationToken)
{
    await Task.CompletedTask;

    return NoContent();
}
```

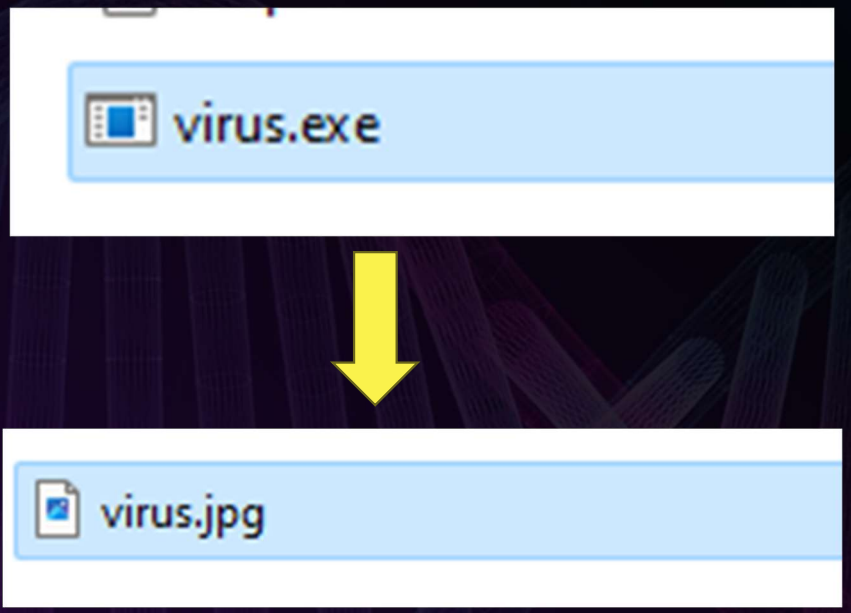

Open
Downloads
Search Downloads
Organize
New folder
Taner - Personal
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Yesterday
Youtube Eğitim Videoları (1).jpg
JPG File
260 KB
Last week
free-hex-editor-neo.exe
Hex Editor Neo Setup Package
HHD Software Ltd.
pdfdegisikboyutlardaolan.zip
syd_110.zip
Resume.pdf
Chrome HTML Document
109 KB
Copy of Resume Taner Saydam.pdf
Chrome HTML Document
109 KB
Youtube Eğitim Videoları.jpg
JPG File
1.28 MB
FileZilla_3.67.0_win64-setup.exe
FileZilla FTP Client
pfdbirlestirme (1).zip
File name:
Youtube Eğitim Videoları (1).jpg
All Files (*.*)
Open
Cancel
Ana Sayfa | PayTR...
Your First Extension...
Tabler: Premium das...
vidIQ
Modular Monolith...
Meet Recordings -...
Cancel
multipart/form-data
Add string item
Send empty value
Execute

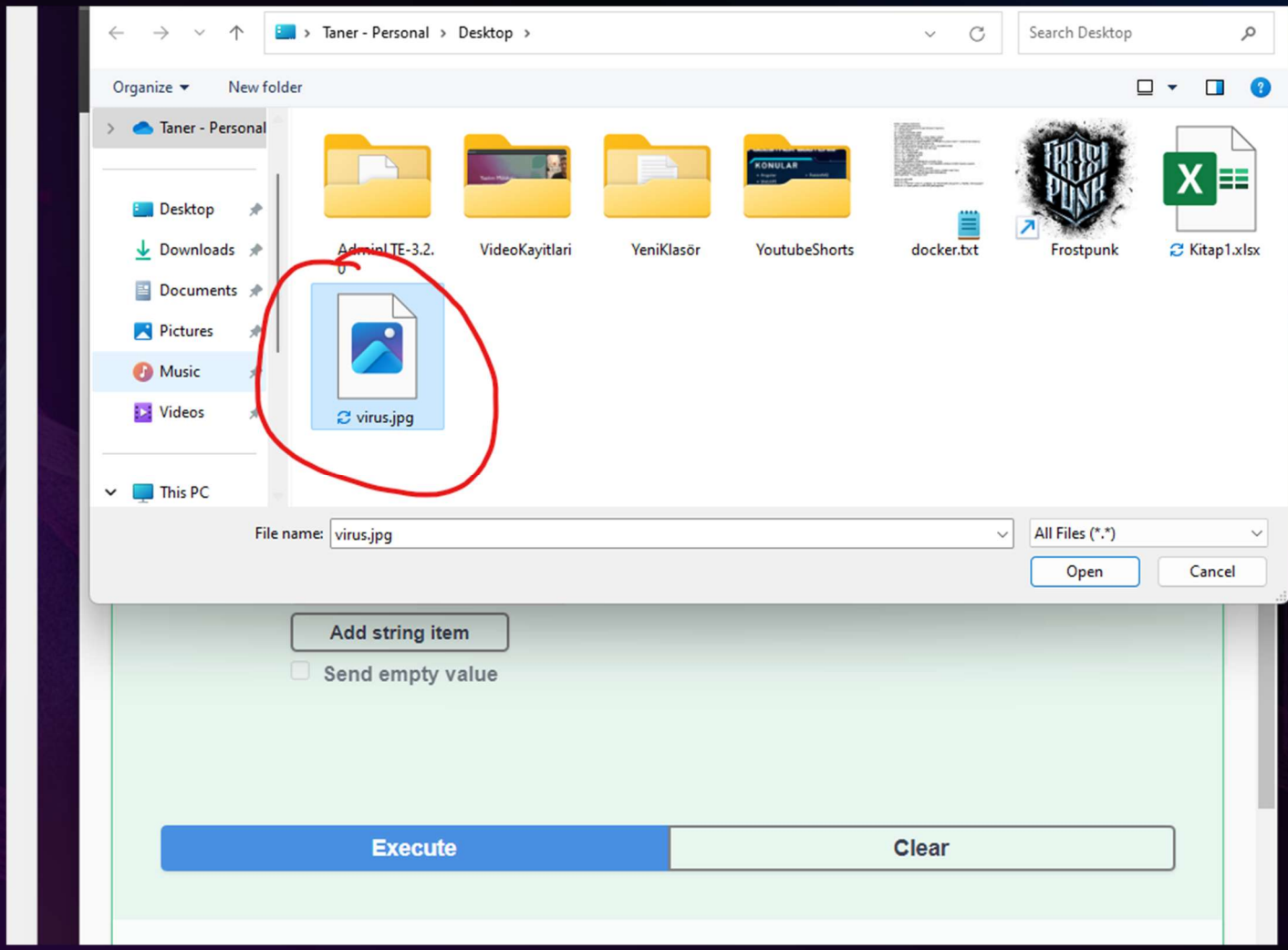

[HttpPost]
0 references
public async Task<IActionResult> AddImages(List<IFormFile> files, CancellationToken cancellationToken)
{
await Task.CompletedTask;
return NoContent();
}
files View Count = 1
[0] {Microsoft.AspNetCore.Http.FormFile}
ContentDisposition View "form-data; name=\"files\"; filename=\"Youtube Eğitim Videoları (1).jpg\""
ContentType View "image/jpeg"
FileName View "Youtube Eğitim Videoları (1).jpg"
Headers View Count = 2
Length 266267
Name View "files"
Static members
Non-Public members

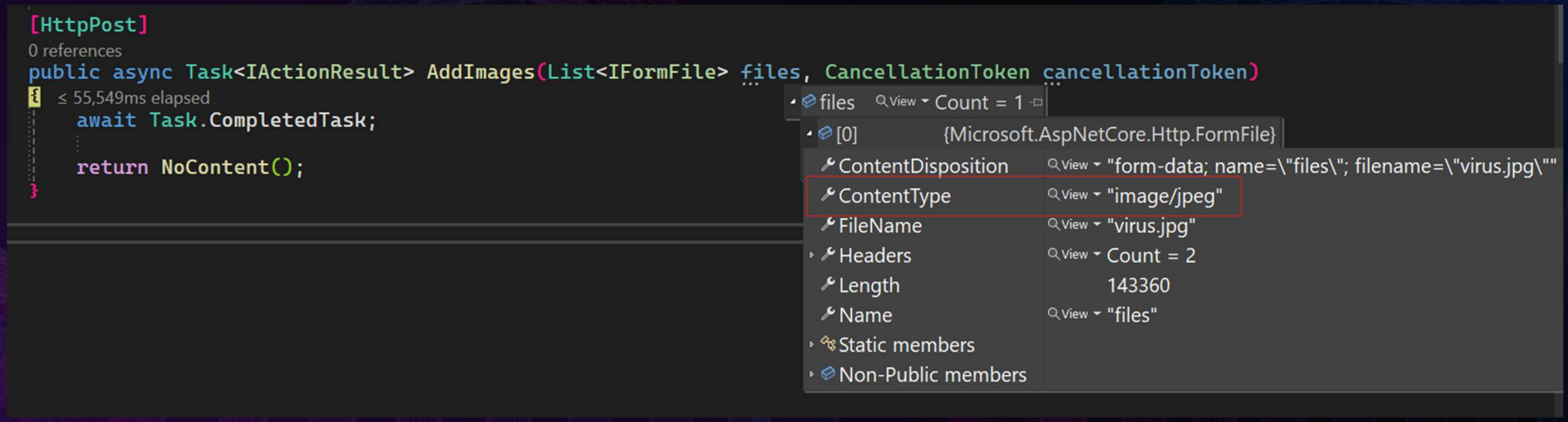
Olabilecek Güvenlik Açıkları

1. ~~(Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir~~
2. ~~Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir~~
3. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler~~
4. ~~Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler~~
5. ~~Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler~~
6. ~~Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler~~
7. ~~Database'de bulunan bilgilerimize erişip manipüle edilebilirler~~
8. ~~ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir~~
9. Virüs dosyasının formatını resim dosyası yaparak sisteme göndermeye çalışabilir


virus.exe

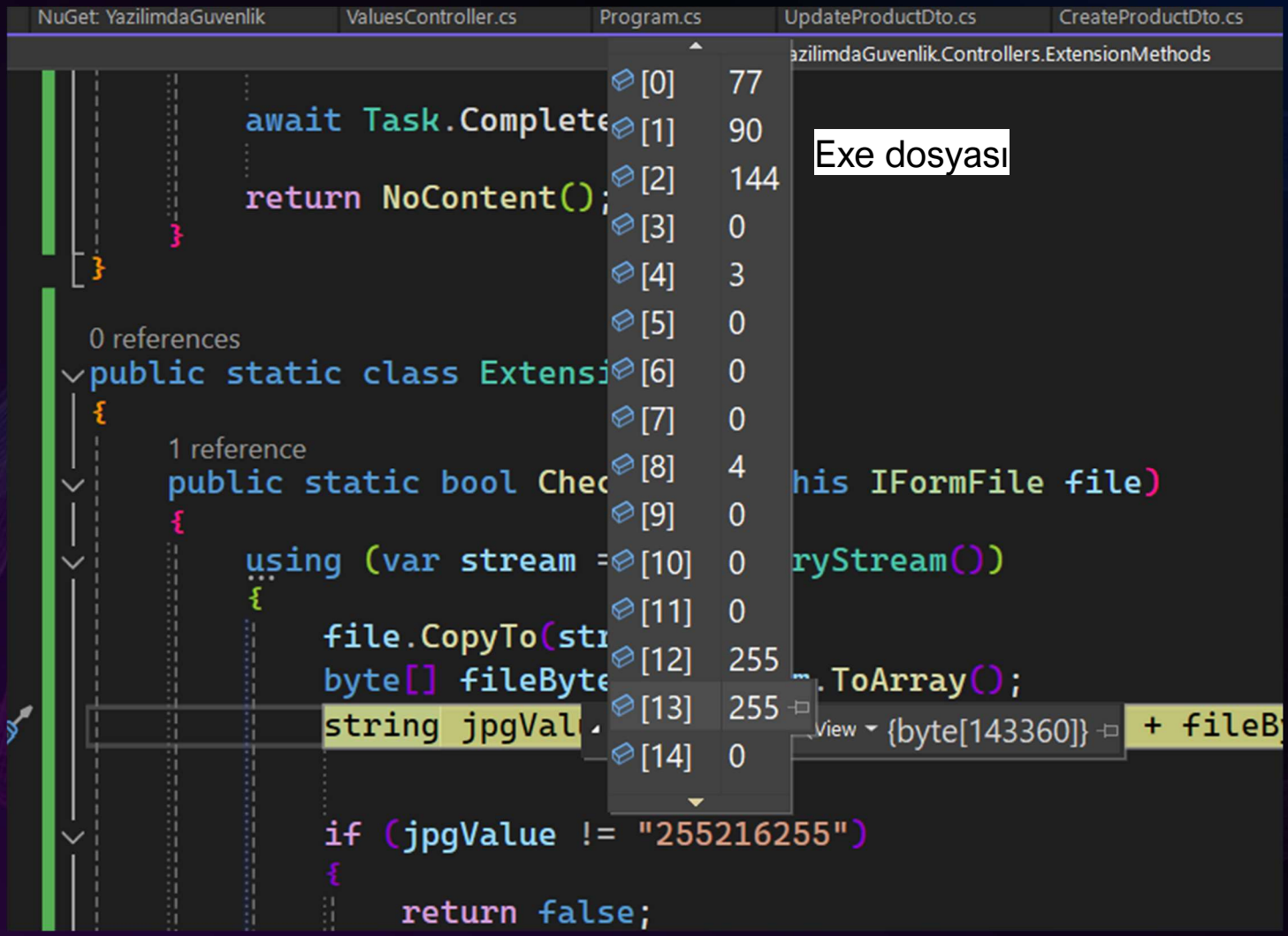

virus.exe
virus.jpg

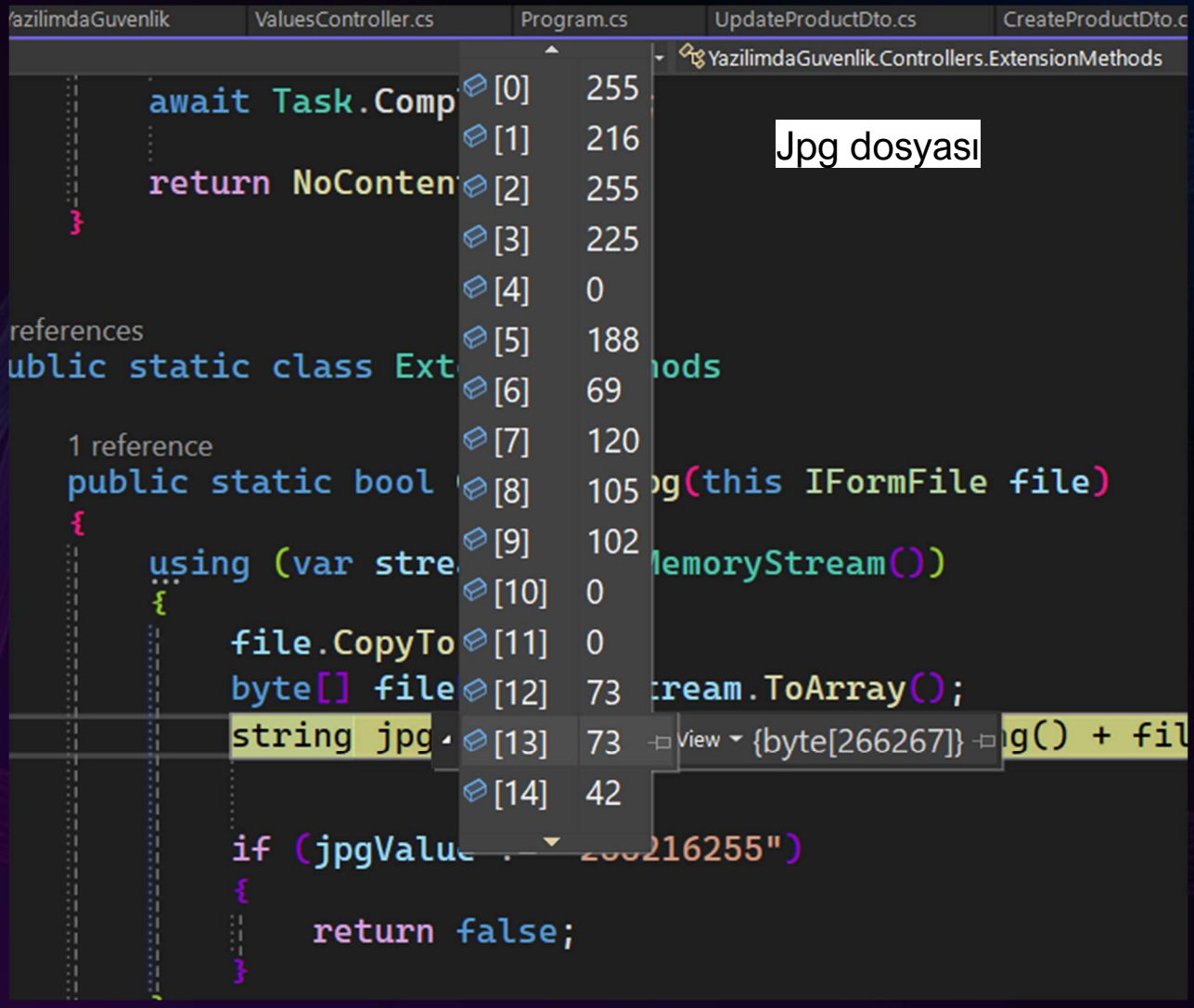

Taner - Personal › Desktop ›
Search Desktop
Organize
New folder
Taner - Personal
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
AdminLTE-3.2.0
VideoKayitlari
YeniKlasör
YoutubeShorts
docker.txt
Frostpunk
Kitap1.xlsx
virus.jpg
File name: virus.jpg
All Files (*.*)
Open
Cancel
Add string item
Send empty value
Execute
Clear


[HttpPost]
0 references
public async Task<IActionResult> AddImages(List<IFormFile> files, CancellationToken cancellationToken)
{ ≤ 55,549ms elapsed
await Task.CompletedTask;
return NoContent();
}
files View Count = 1
[0] {Microsoft.AspNetCore.Http.FormFile}
ContentDisposition View "form-data; name=\"files\"; filename=\"virus.jpg\""
ContentType View "image/jpeg"
FileName View "virus.jpg"
Headers View Count = 2
Length 143360
Name View "files"
Static members
Non-Public members

```
0 references
public static bool CheckForJpg(this IFormFile file)
{
    using (var stream = new MemoryStream())
    {
        file.CopyTo(stream);
        byte[] fileBytes = stream.ToArray();
        string jpgValue = fileBytes[0].ToString() + fileBytes[1].ToString() + fileBytes[2].ToString();


        if (jpgValue != "255216255")
        {
            return false;
        }
    }
    return true;
}
```

PNG: 137807871


NuGet: YazilimdaGuvenlik
ValuesController.cs
Program.cs
UpdateProductDto.cs
CreateProductDto.cs
azilimdaGuvenlik.Controllers.ExtensionMethods
await Task.Complete
return NoContent();
0 references
public static class Extensi
1 reference
public static bool Chec
his IFormFile file)
using (var stream =
ryStream())
file.CopyTo(str
byte[] fileByte
.ToArray();
string jpgVal
View {byte[143360]}
+ fileB
if (jpgValue != "255216255")
return false;
[0] 77
[1] 90
[2] 144
[3] 0
[4] 3
[5] 0
[6] 0
[7] 0
[8] 4
[9] 0
[10] 0
[11] 0
[12] 255
[13] 255
[14] 0
Exe dosyası


YazilimdaGuvenlik
ValuesController.cs
Program.cs
UpdateProductDto.cs
CreateProductDto.c
YazilimdaGuvenlik.Controllers.ExtensionMethods
Jpg dosyası
[0] 255
[1] 216
[2] 255
[3] 225
[4] 0
[5] 188
[6] 69
[7] 120
[8] 105
[9] 102
[10] 0
[11] 0
[12] 73
[13] 73
[14] 42
View {byte[266267]}
await Task.Comp
return NoConten
references
ublic static class Ext
ods
1 reference
public static bool
g(this IFormFile file)
using (var stre
emoryStream())
file.CopyTo
byte[] file
ream.ToArray();
string jpg
g() + fil
if (jpgValu
216255")
return false;

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler
8. ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir
9. Virüs dosyasının formatını resim dosyası yaparak sisteme göndermeye çalışabilir

500

Undocumented Error: response status is 500

Response body

```
System.DivideByZeroException: Attempted to divide by zero.
   at YazilimdaGuvenlik.Controllers.ProductsController.GetAll(CancellationToken cancellationToken) in C:\Test\YazilimdaGuvenlik\Controllers\ProductsController.cs:line 37
   at Microsoft.AspNetCore.Mvc.Infrastructure.ActionMethodExecutor.TaskOfIActionResultExecutor.Execute(ActionContext actionContext, IActionResultTypeMapper mapper, ObjectMethodExecutor executo
r, Object controller, Object[] arguments)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ControllerActionInvoker.<InvokeActionMethodAsync>g__Awaited|12_0(ControllerActionInvoker invoker, ValueTask`1 actionResultValueTask)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ControllerActionInvoker.<InvokeNextActionFilterAsync>g__Awaited|10_0(ControllerActionInvoker invoker, Task lastTask, State next, Scope scope, Objec
t state, Boolean isCompleted)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ControllerActionInvoker.Rethrow(ActionExecutedContextSealed context)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ControllerActionInvoker.Next(State& next, Scope& scope, Object& state, Boolean& isCompleted)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ControllerActionInvoker.InvokeInnerFilterAsync()
--- End of stack trace from previous location ---
   at Microsoft.AspNetCore.Mvc.Infrastructure.ResourceInvoker.<InvokeFilterPipelineAsync>g__Awaited|20_0(ResourceInvoker invoker, Task lastTask, State next, Scope scope, Object state, Boolean
isCompleted)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ResourceInvoker.<InvokeAsync>g__Awaited|17_0(ResourceInvoker invoker, Task task, IDisposable scope)
   at Microsoft.AspNetCore.Mvc.Infrastructure.ResourceInvoker.<InvokeAsync>g__Awaited|17_0(ResourceInvoker invoker, Task task, IDisposable scope)
   at Microsoft.AspNetCore.Authorization.AuthorizationMiddleware.Invoke(HttpContext context)
   at Microsoft.AspNetCore.RateLimiting.RateLimitingMiddleware.InvokeInternal(HttpContext context, EnableRateLimitingAttribute enableRateLimitingAttribute)
   at Swashbuckle.AspNetCore.SwaggerUI.SwaggerUIMiddleware.Invoke(HttpContext httpContext)
   at Swashbuckle.AspNetCore.Swagger.SwaggerMiddleware.Invoke(HttpContext httpContext, ISwaggerProvider swaggerProvider)
   at Microsoft.AspNetCore.Authentication.AuthenticationMiddleware.Invoke(HttpContext context)
   at Microsoft.AspNetCore.Diagnostics.DeveloperExceptionPageMiddlewareImpl.Invoke(HttpContext context)

HEADERS
=======
Accept: */*
Host: localhost:7168
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
```

Download

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler
8. ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir
9. Virüs dosyasının formatını resim dosyası yaparak sisteme göndermeye çalışabilir
10. Exception hatalarından gelen StackTrace bilgisini uygulamaya zarar vermek için kullanabilirler

```
using Microsoft.AspNetCore.Diagnostics;
using System.Text.Json;

namespace YazilimdaGuvenlik;

0 references
public sealed class MyExceptionHandler : IExceptionHandler
{
    0 references
    public async ValueTask<bool> TryHandleAsync(HttpContext context, Exception exception,
     CancellationToken cancellationToken)
    {
        context.Response.StatusCode = 500;
        context.Response.ContentType = "application/json";
        object errorMessage = new { Message = exception.Message };
        string errorMessageString = JsonSerializer.Serialize(errorMessage);
        await context.Response.WriteAsync(errorMessageString, cancellationToken);

        return true;
    }
}
```

```
builder.Services
    .AddExceptionHandler<MyExceptionHandler>()
    .AddProblemDetails();
```

```
app.UseExceptionHandler();
```

500

Undocumented

Error: response status is 500

Response body

```
{
  "Message": "Attempted to divide by zero."
}
```

Olabilecek Güvenlik Açıkları

1. (Sorun) Endpointlerin listesine kolayca ulaşılırsa, oradan sisteme zarar verebilecek bilgiler bulunabilir
2. Web Browserdan endpointi elde edip kendi sitesinde kullanarak uygulamayı klonlayabilir ya da zarar vermeye çalışabilir
3. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve milyonlarca isteği aynı anda göndermeye çalışarak uygulamamızı kilitlemeye çalışabilirler
4. Postman, Swagger, http ya da bir proje üzerinden API isteği atarak API'mıza erişebilir ve ondaki verileri alarak kendi uygulamasında kullanmaya çalışabilirler
5. Browserdan authentication bilgimizi alıp API endpointimize erişerek verilerimizi almaya çalışabilirler
6. Hassas bilgilerimizi kolayca elde edebilecek dosyalardan alıp uygulamamıza zarar vermek için kullanabilirler
7. Database'de bulunan bilgilerimize erişip manipüle edilebilirler
8. ID alanını tahmin edilmesi kolay bir tip tutarsak, onu tahmin ederek erişmemesi gereken kayıtlara erişmeye çalışabilir
9. Virüs dosyasının formatını resim dosyası yaparak sisteme göndermeye çalışabilir
10. Exception hatalarından gelen StackTrace bilgisini uygulamaya zarar vermek için kullanabilirler

Cloud Fundamentals: C# Developers için AWS Services

Taner Saydam

4.9 ★★★★★ (5)

5 total hours · 87 lectures · All Levels

Ücretsiz kupon kodu

C4A6E944BFA26A94DC17

.NET 8 ve Angular 17 ile e-Muhasebe Uygulaması

Taner Saydam

5.0 ★★★★★ (4)

15.5 total hours · 67 lectures · Intermediate

Ücretsiz kupon kodu

2AD053A9C3F6BBD875EE

.NET Developers için Pratik İpuçları

Taner Saydam

4.9 ★★★★★ (20)

3.5 total hours · 21 lectures · Intermediate

Ücretsiz kupon kodu

507E813654C292DB6C4F

Teşekkürler

Taner Saydam

www.tanersaydam.net

tanersaydam@gmail.com