



Agenda:

- Inauguración del Meetup de En Mi Local Funciona Barcelona
- Protegiendo tu API REST con JWT en aplicaciones .NET
- Cervezas y picoteo.



Comenzamos el blog en 2016



¡Bienvenidos a enmilocalfunciona!

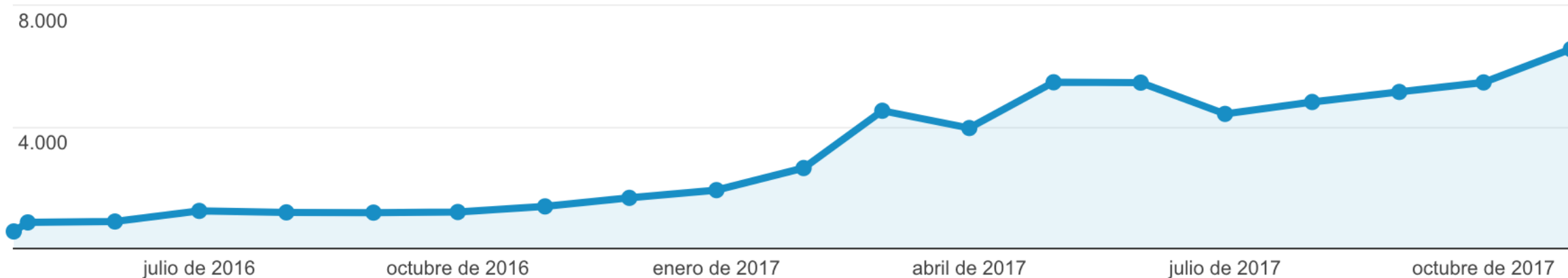
Publicado por [Antonio David Fernández Reyes](#) el 26 April 2016

[Getting Started](#)

[atSistemas](#)

Y poco a poco hemos ido creciendo:

● Sesiones





Gracias a todos los que lo habéis hecho posible

Más de 90 posts de más de 50 compañeros





Protegiendo tu API REST con JWT en aplicaciones .NET



Autor

SANTI MACIAS

Lider Técnico Comunidad Microsoft en atSistemas y friki de pelis y series de ciencia ficción en mi tiempo libre.



EN MI LOCAL FUNCIONA

1. Conceptos básicos de seguridad
2. Cookies vs Tokens
3. Definiciones de JWT
4. Fundamentos de JWT
5. Anatomía de JWT
6. Estructura de un Token
7. Nuestros amigos debuggers
8. Ciclo de vida de un Token
9. Librerías y vulnerabilidades
10. Vamos a la acción



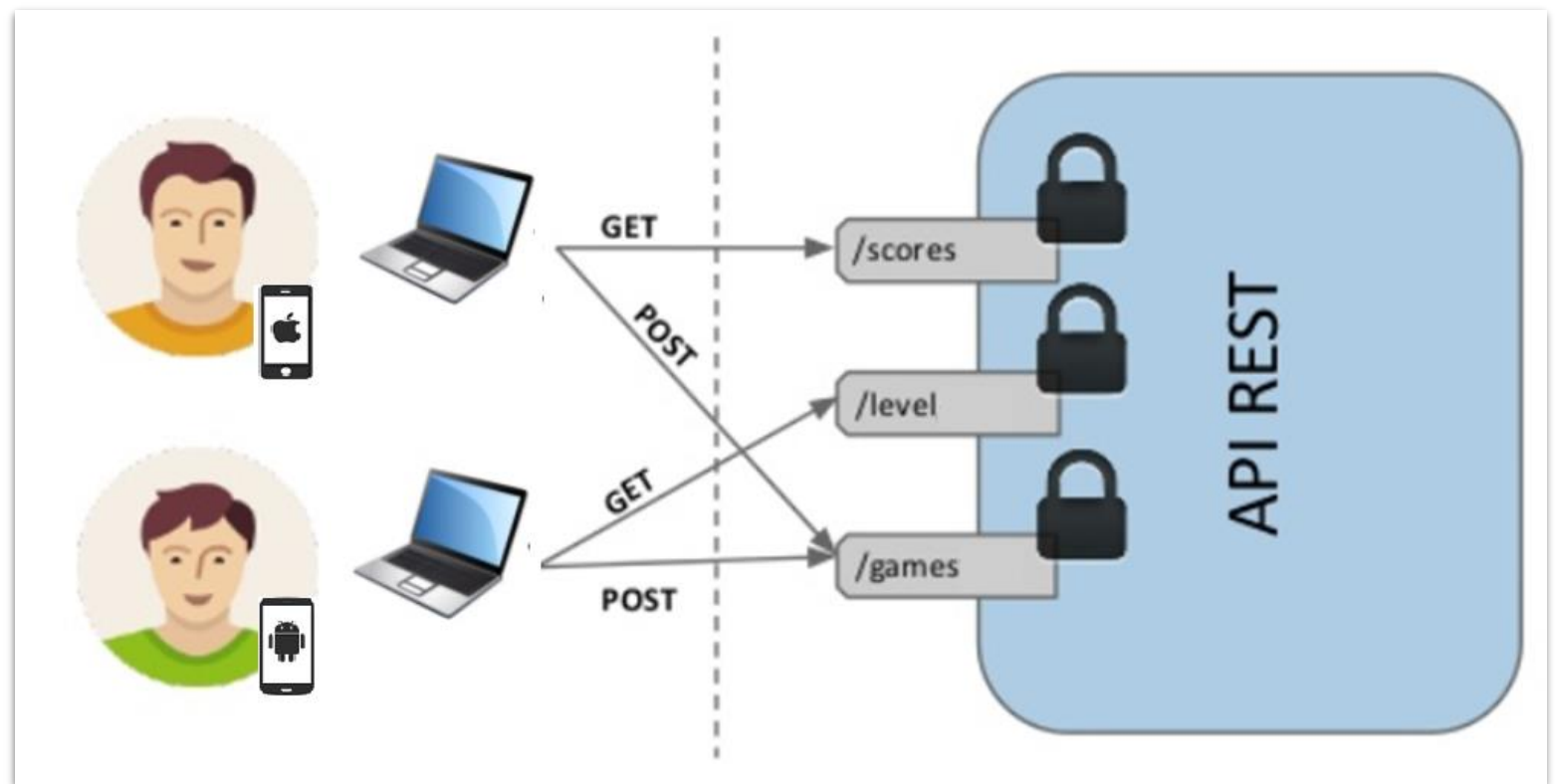
UN REPASO A CONCEPTOS BASICOS

Autenticación

- Recepción hotel
- Login con password
- HTTP 401 Unauthorized

Autorización

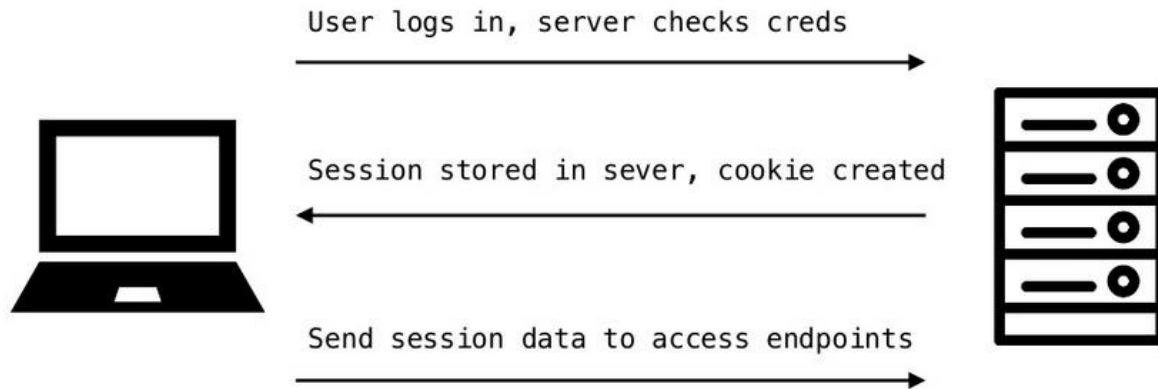
- Llave de la habitación
- Permisos de acceso
- HTTP 403 Forbidden





Cookies vs Tokens

Traditional Authentication Systems

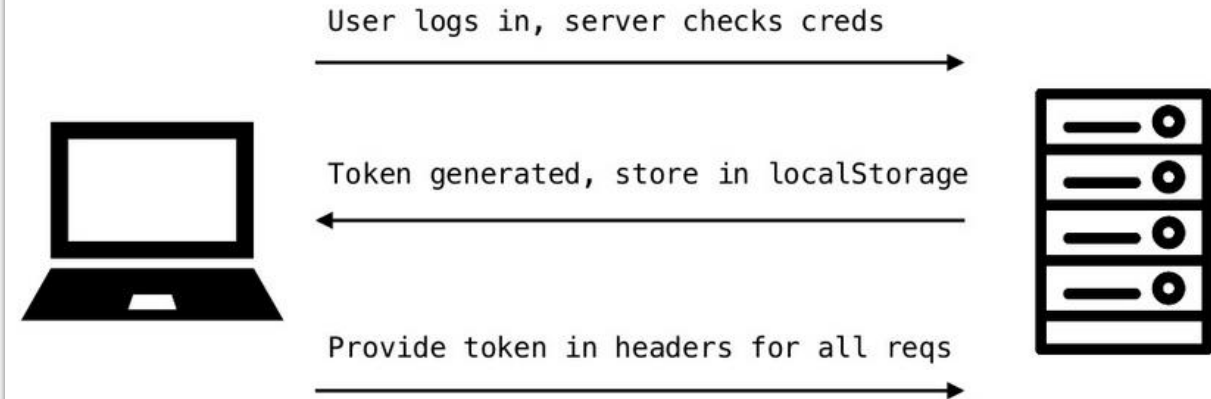


Cookies: WebForms, asp.net mvc, etc

Sesión: Necesitan ser guardas en el servidor, -Escalable

Datos: Contiene la sessionID, AUTH del usuario

Token-Based Authentication Systems



Tokens: Api key, OAuth2, openID, SSO, etc.

Sesión: Se almacena en cada cliente, +Escalable

Datos: Contiene información del usuario



JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.

JSON Web Token

JSON Web Token (abreviado **JWT**) es un [estándar abierto](#) basado en [JSON](#) propuesto por [IETF](#) ([RFC 7519](#)) para la creación de **tokens de acceso** que permiten la propagación de identidad y privilegios o *claims* en inglés. Por ejemplo, un servidor podría generar un token indicando que el usuario tiene privilegios de administrador y proporcionarlo al un cliente. El cliente entonces podría utilizar el token para probar que está actuando como un administrador en el cliente o en otro sistema. El token está firmado por la clave del servidor, así que el cliente y el servidor son ambos capaz de verificar que el token es legítimo. Los JSON Web Tokens están diseñados para ser compactos, poder ser enviados en las URLs **-URL-safe-** y ser utilizados en escenarios de [Single Sign-On](#) (SSO). Los privilegios de los JSON Web Tokens puede ser utilizados para propagar la identidad de usuarios como parte del proceso de [autenticación](#) entre un [proveedor de identidad](#) y un [proveedor de servicio](#), o cualquiera otro tipo de privilegios requeridos por procesos empresariales.^{1 2 3 4}

https://es.wikipedia.org/wiki/JSON_Web_Token

JSON Web Token (JWT) Specification

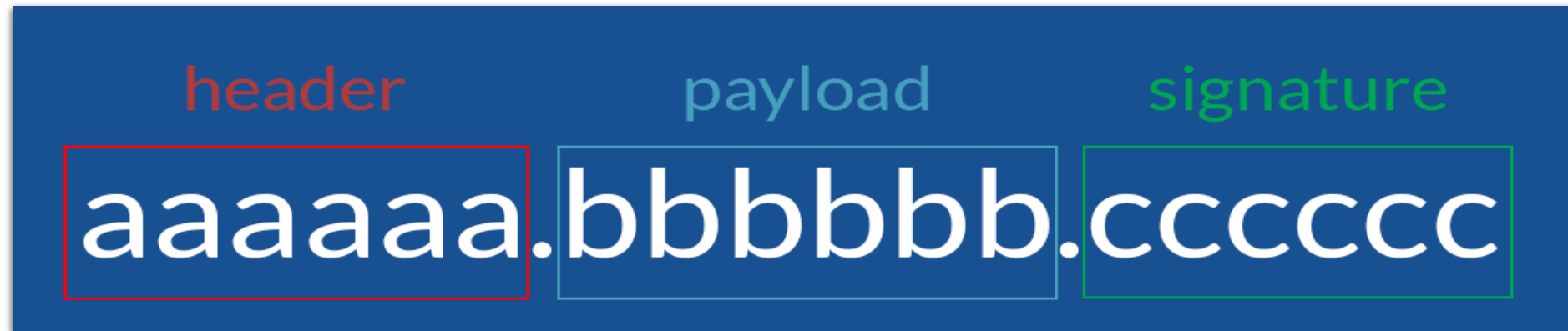
Abstract

JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

<https://tools.ietf.org/html/rfc7519>



ANATOMIA DEL TOKEN



HEADER: Indica el algoritmo y tipo de Token.

PAYLOAD: Datos de usuario/claims

SIGNATURE: la firma, para verificar que el token es válido.



ESTRUCTURA DEL TOKEN (Claims)

Registered claims

jti	→	Id del token: String
iss	→	Issuer (emisor): StringOrUri
aud	→	Audiencia: StringOrUri
sub	→	Subject (tema): StringOrUri
iat	→	Cuándo se creó: NumericDate
exp	→	Cuándo expira: NumericDate
nbf	→	Tiempo hasta validez: NumericDate

Claims: No son obligatorios.

Claims: Se recomienda seguir este formato.

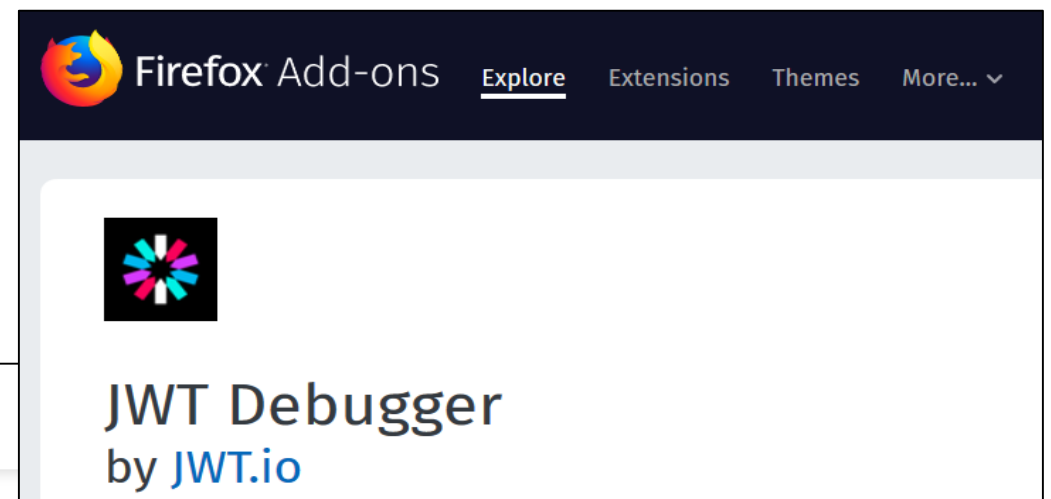
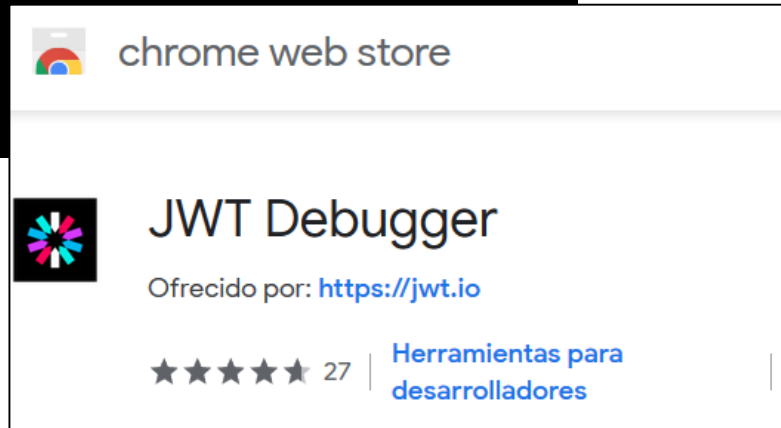
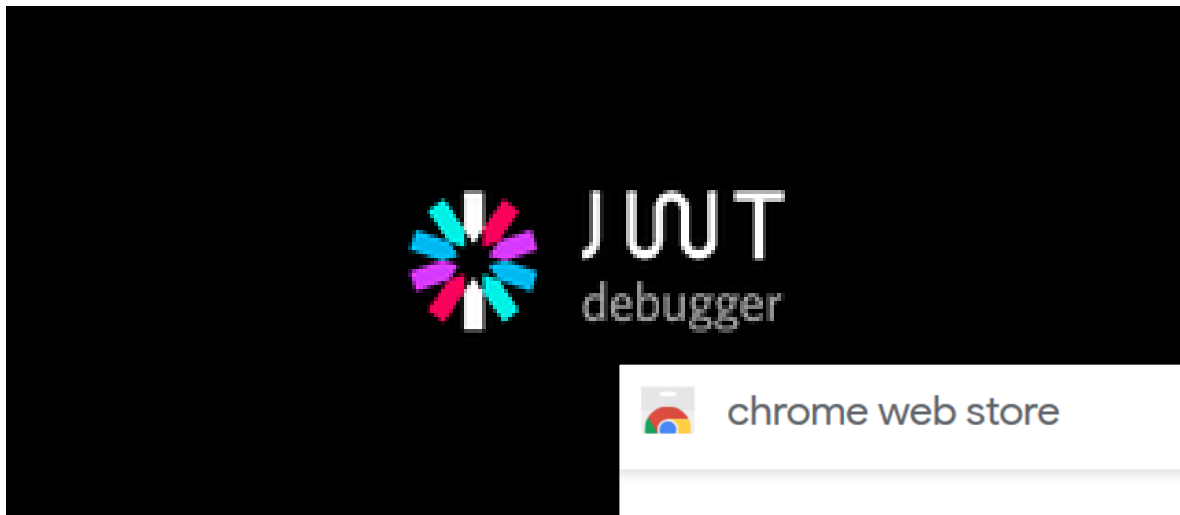
Claims: No todas las librerías .NET los implementan.

jti: Es muy útil para usar Tokens de un solo uso y evitar ataques.

Especificación: <https://tools.ietf.org/html/rfc7519>



NUESTRO AMIGOS DEBUGGERS





JWT Debugger Libraries Introduction Ask Get a T-shirt! Crafted by Auth0

Debugger

ALGORITHM HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWVhbnR5dWV9LjJVA950rM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "HS256",  "typ": "JWT"}
```

PAYLOAD: DATA

```
{  "sub": "1234567890",  "name": "John Doe",  "admin": true}
```

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  secret)
```

☐ secret base64 encoded

☒ Signature Verified

JWT Debugger Libraries Introduction Ask Get a T-shirt! Crafted by Auth0

Debugger

ALGORITHM HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWVhbnR5dWV9LjJVA950rM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded EDIT THE PAYLOAD AND SECRET (ONLY HS256 SUPPORTED)

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "HS256",  "typ": "JWT"}
```

PAYLOAD: DATA

```
{  "sub": "1234567890",  "name": "John Doe",  "admin": true}
```

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  otro-secret)
```

☐ secret base64 encoded

☒ Invalid Signature

DEMO: Lo importante es el **SECRET** con el que firmamos el token y no debemos darlo a nadie.



JWT LIBRERIAS Y VULNERABILIDADES

<https://docs.microsoft.com/en-us/security-updates>

Security Advisories and Bulletins

📅 10/11/2017 • ⌚ 2 minutes to read • Contributors 🐾

In this library you will find the following security documents that have been released by the Microsoft Security Response Center (MSRC). The MSRC investigates all reports of security vulnerabilities affecting Microsoft products and services, and releases these documents as part of the ongoing effort to help you manage security risks and help keep your systems protected.

- [Security Bulletins](#)
- [Security Bulletin Summaries](#)
- [Security Advisories](#)
- [Microsoft Vulnerability Research Advisories](#)
- [Acknowledgments](#)
- [Glossary](#)



JWT LIBRERIAS Y VULNERABILIDADES

Libraries for Token Signing/Verification

FILTER BY All

Warning: Critical vulnerabilities in JSON Web Token libraries with asymmetric keys. [Learn more](#)

.NET		.NET		.NET (RT)	
✓ Sign	✓ HS256	✓ Sign	✓ HS256	✓ Sign	✓ HS256
✓ Verify	✓ HS384	✓ Verify	✓ HS384	✓ Verify	✓ HS384
✓ iss check	✓ HS512	✗ iss check	✓ HS512	✗ iss check	✓ HS512
✓ sub check	✓ RS256	✗ sub check	✓ RS256	✗ sub check	✓ RS256
✓ aud check	✓ RS384	✗ aud check	✓ RS384	✗ aud check	✓ RS384
✓ exp check	✓ RS512	✗ exp check	✓ RS512	✗ exp check	✓ RS512
✓ nbf check	✓ ES256	✗ nbf check	✓ ES256	✗ nbf check	✓ ES256
✓ iat check	✓ ES384	✗ iat check	✓ ES384	✗ iat check	✓ ES384
✓ jti check	✓ ES512	✗ jti check	✓ ES512	✗ jti check	✓ ES512

Microsoft 302 View Repo

Install-Package System.IdentityModel.Tokens.Jwt

DV 378 View Repo

Install-Package jose-jwt

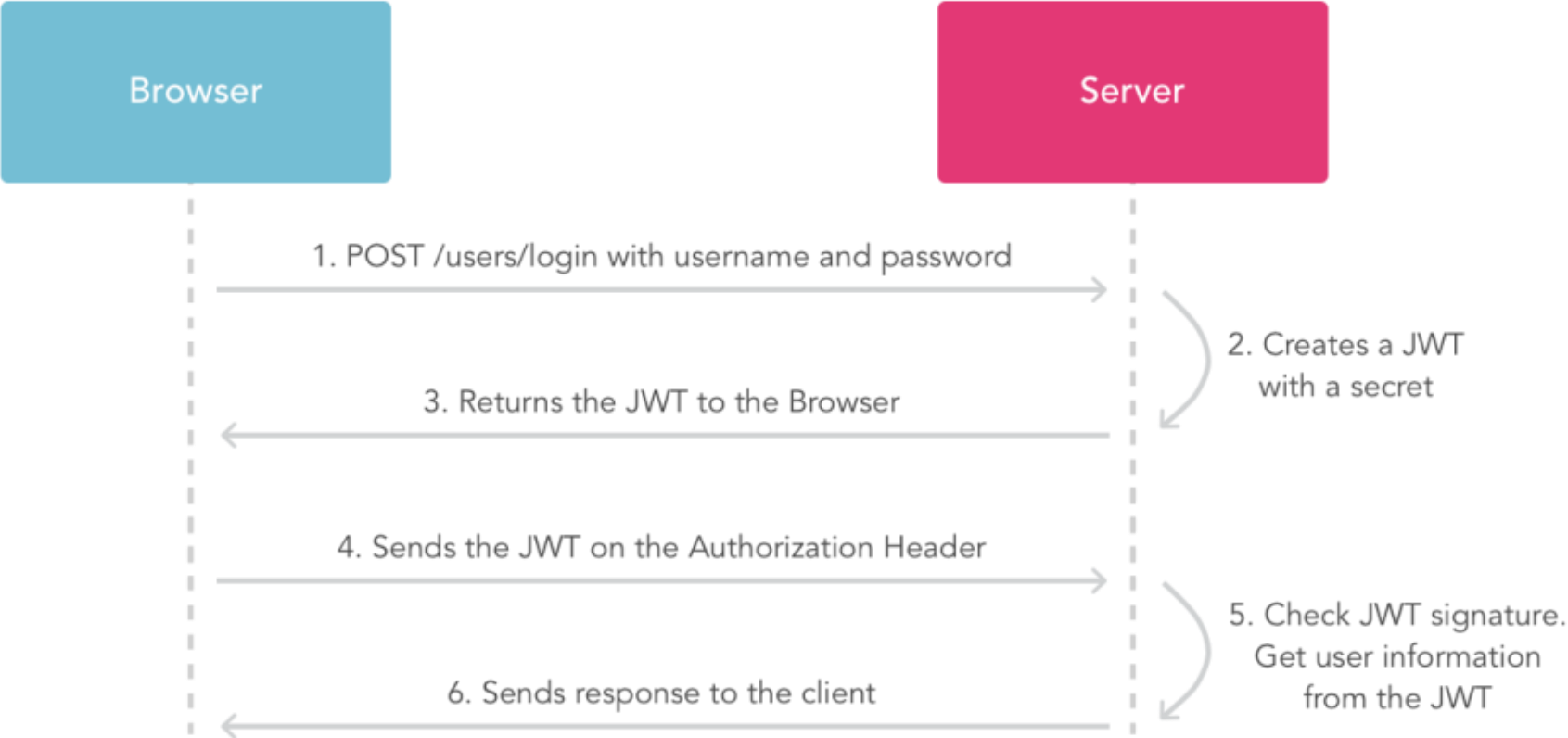
DV View Repo

Install-Package jose-rt

Vulnerabilities: <https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/3214296>

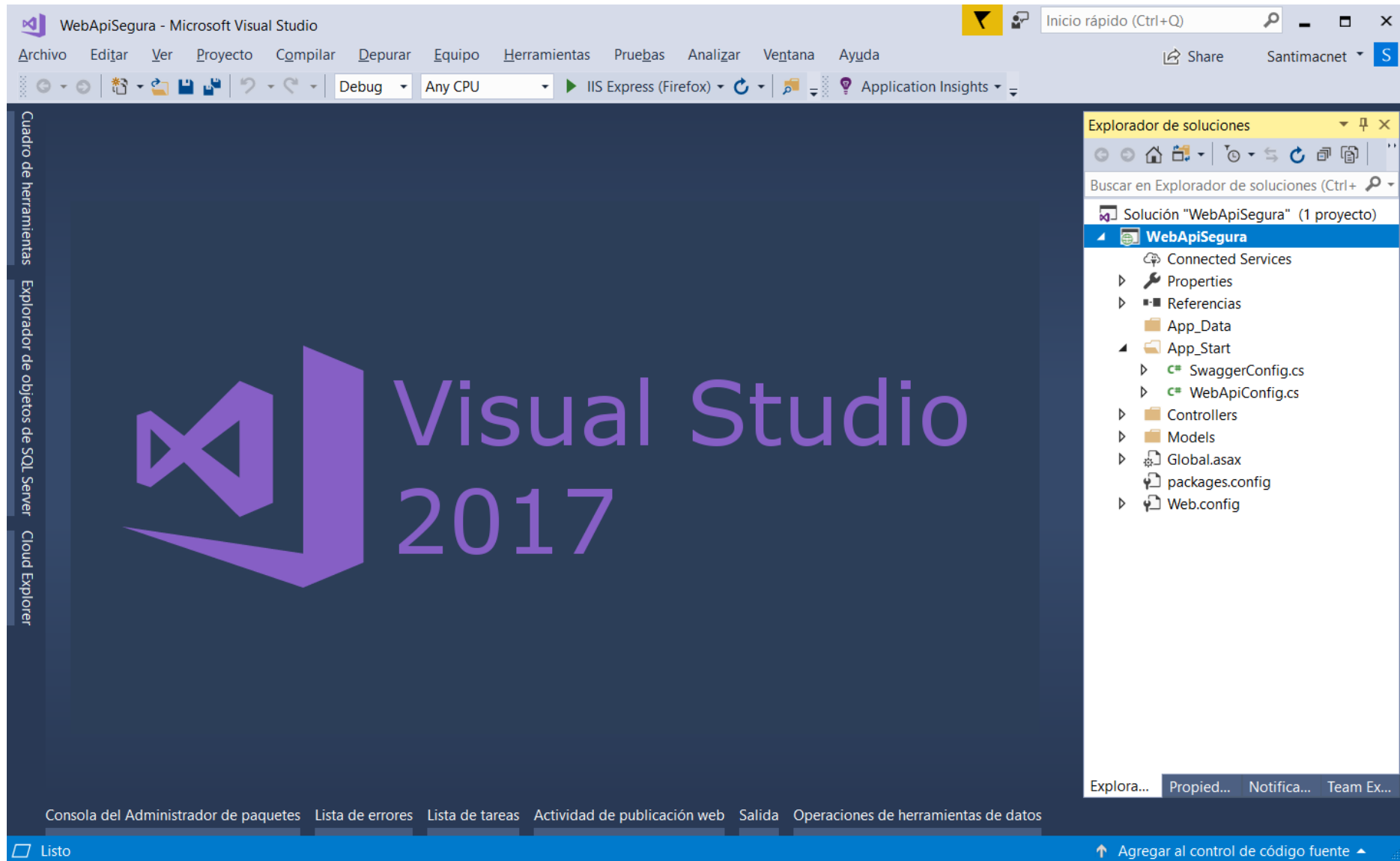


Ciclo de vida de un Token

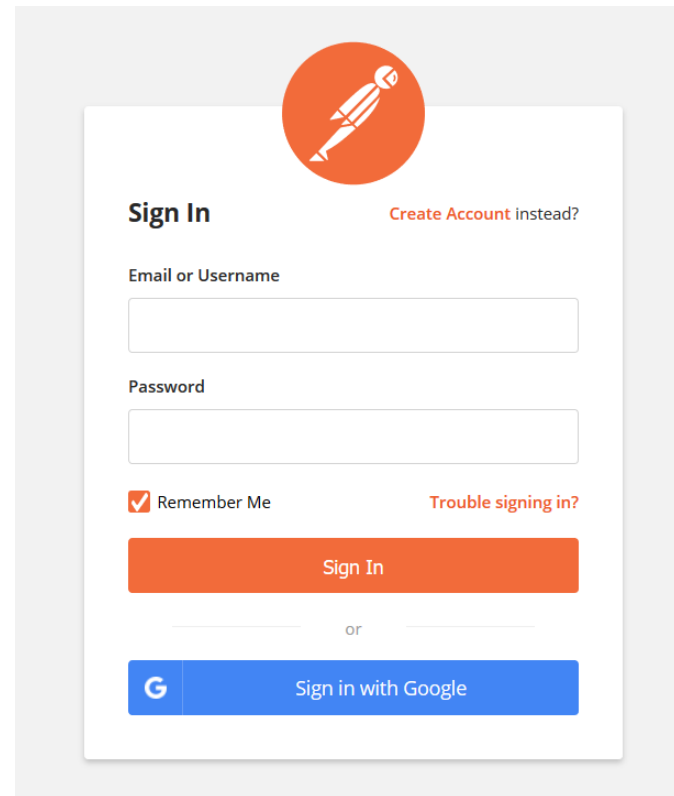
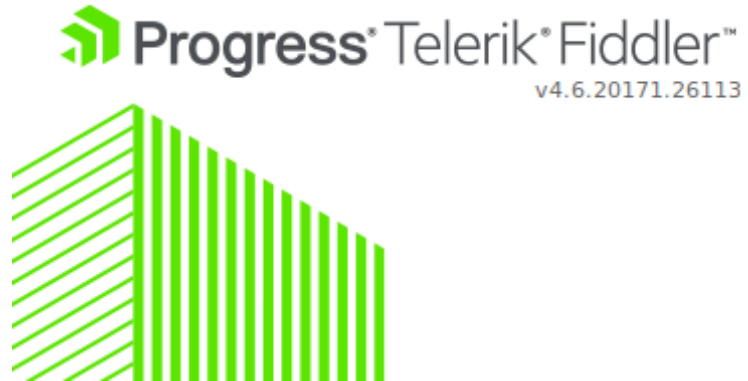




DEMO ASP.NET WEB API



DEBUGGERS

A screenshot of the Fiddler web application's sign-in page. At the top center is an orange circular icon containing a white silhouette of a person with a bow and arrow. Below this is the 'Sign In' heading, with a link 'Create Account instead?' to its right. The form contains two input fields: 'Email or Username' and 'Password'. Below the password field is a checkbox labeled 'Remember Me' and a link 'Trouble signing in?'. A large orange 'Sign In' button is positioned below the form fields. Below the button is a horizontal line with the word 'or' in the center. At the bottom is a blue button with a white 'G' icon and the text 'Sign in with Google'.

CUESTIONES CLAVE

- Que pasa cuando recibo el token en mi controlador
- Que pasa cuando caduca el token en mi aplicación
- Que pasa cuando realizamos logout en app/web
- Que pasa con mis token en devlocal y producción
- Que pasa si tengo varias API REST que usan JWT
- Quien y donde se gestionan los usuarios de mi API

PREGUNTAS



REFERENCIAS



- <https://enmilocalfunciona.io/construyendo-una-web-api-rest-segura-con-json-web-token-en-net-parte-i/>
- <https://enmilocalfunciona.io/construyendo-una-web-api-rest-segura-con-json-web-token-en-net-parte-ii/>
- <https://enmilocalfunciona.io/construyendo-una-web-api-rest-segura-con-json-web-token-en-net-parte-iii/>
- <https://github.com/santimacnet/WebAPI-Segura-JWT>

- <https://jwt.io>
- <https://www.jsonwebtoken.io>
- <https://tools.ietf.org/html/rfc7519>
- <https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/3214296>
- <https://auth0.com/blog/ten-things-you-should-know-about-tokens-and-cookies/>

GRACIAS



www.atsistemas.com

902 888 902