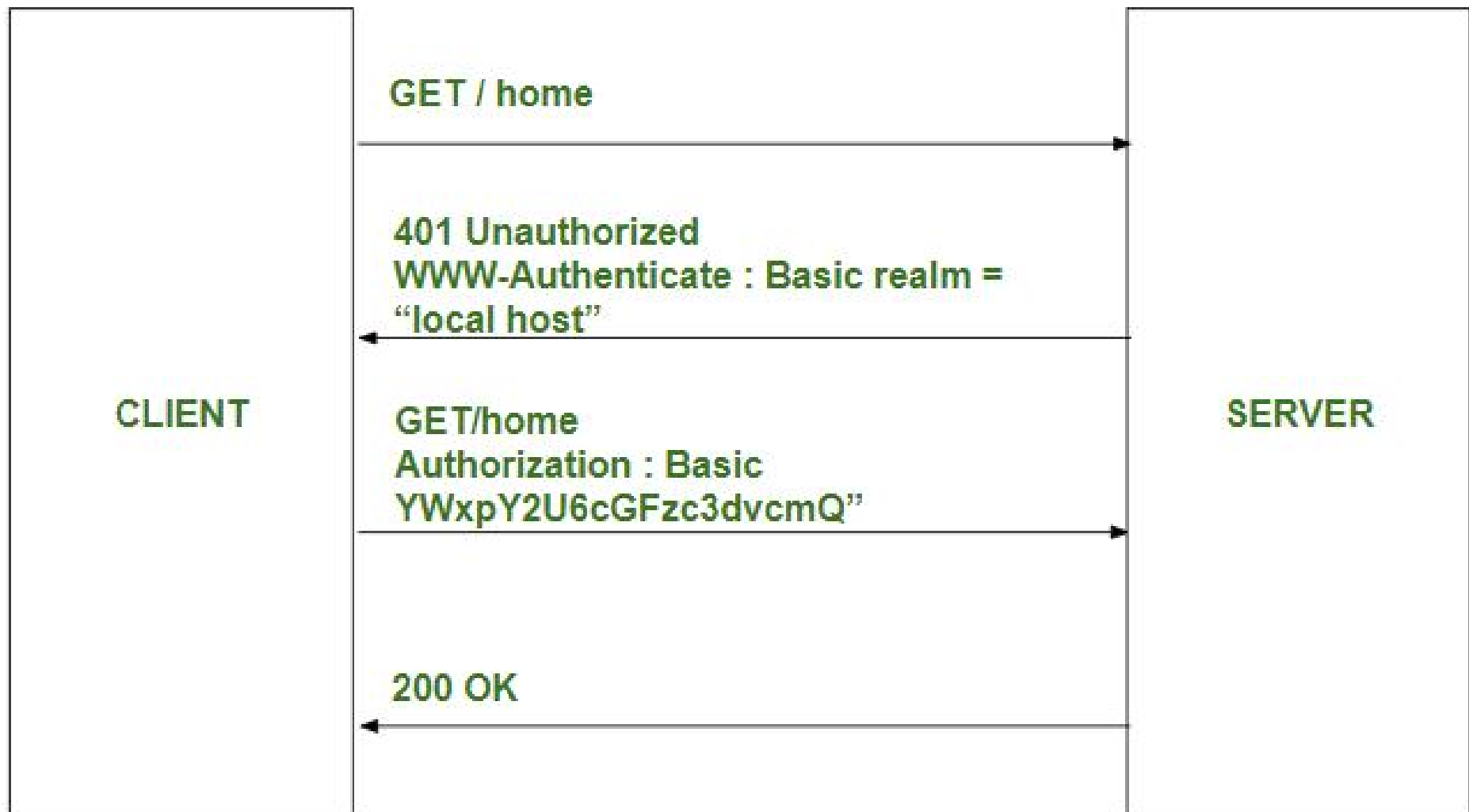


HTTP Authentication



Basic authentication is defined in [RFC 2617, HTTP Authentication: Basic and Digest Access Authentication](#).

Advantages

- Internet standard.
- Supported by all major browsers.
- Relatively simple protocol.

Disadvantages

- User credentials are sent in the request.
- Credentials are sent as plaintext.
- Credentials are sent with every request.
- No way to log out, except by ending the browser session.
- Vulnerable to cross-site request forgery (CSRF); requires anti-CSRF measures.

Because the credentials are sent unencrypted, Basic authentication is only secure over HTTPS.

ApiConfig.csMyMessageHandler1.csProductsController.cs

WebAPIHello.WebApiConfigRegister(HttpCon

```
ic void Register(HttpConfiguration config)

MessageHandlers.Add(new MyMessageHandler1());

g.MessageHandlers.Add(new APIKeyHandler("12345"));
```

Controller...

New Item...Ctrl+Shift+A

Existing Item...Shift+Alt+A

New Scaffolded Item...

New Folder

Add ASP.NET Folder

REST API Client...

New Azure WebJob Project

Existing Project as Azure WebJob

TypeScript File

TypeScript JSX File

HTML Page

JavaScript File

Style Sheet

Web Form

Class...

View in Browser (Firefox)Ctrl+Shift+W

Browse With...

Add

Scope to This

New Solution Explorer View

Exclude From Project

CutCtrl+X

CopyCtrl+C

PasteCtrl+V

DeleteDel

Rename

Open Folder in File Explorer

PropertiesAlt+Enter

Solution Explorer

Search Solution Explorer (Ctrl+;)

WebApiConfig.cs

Areas

Content

Controllers

fonts

Helpers

APIKeyHandler.cs

Log2Attribute.cs

LogAttribute.cs

MyExceptionHandlerAttribute.cs

MyMessageHandler1.cs

UpperCaseAttribute.cs

Models

AccountBindingModels.cs

AccountViewModels.cs

IdentityModels.cs

Product.cs

Providers

Results

Scripts

Views

favicon.ico

Global.asax

packages.config

Ch 15INS

Publish

Add New Item - WebAPIHello

Installed

Sort by: Default



Search Installed Templates (Ctrl+E)

Visual C#

- Code
- Data
- General
- Web
- Windows Forms
- WPF
- Silverlight
- SQL Server
- Storm Items
- Workflow

Online

	Class	Visual C#
	Class for U-SQL	Visual C#
	Interface	Visual C#
	ADO.NET Entity Data Model	Visual C#
	Application Manifest File	Visual C#
	Assembly Information File	Visual C#
	Class Diagram	Visual C#
	Code Analysis Rule Set	Visual C#
	Code File	Visual C#

[Click here to go online and find templates.](#)

Type: Visual C#

An empty class declaration

Name: APISecurity.cs

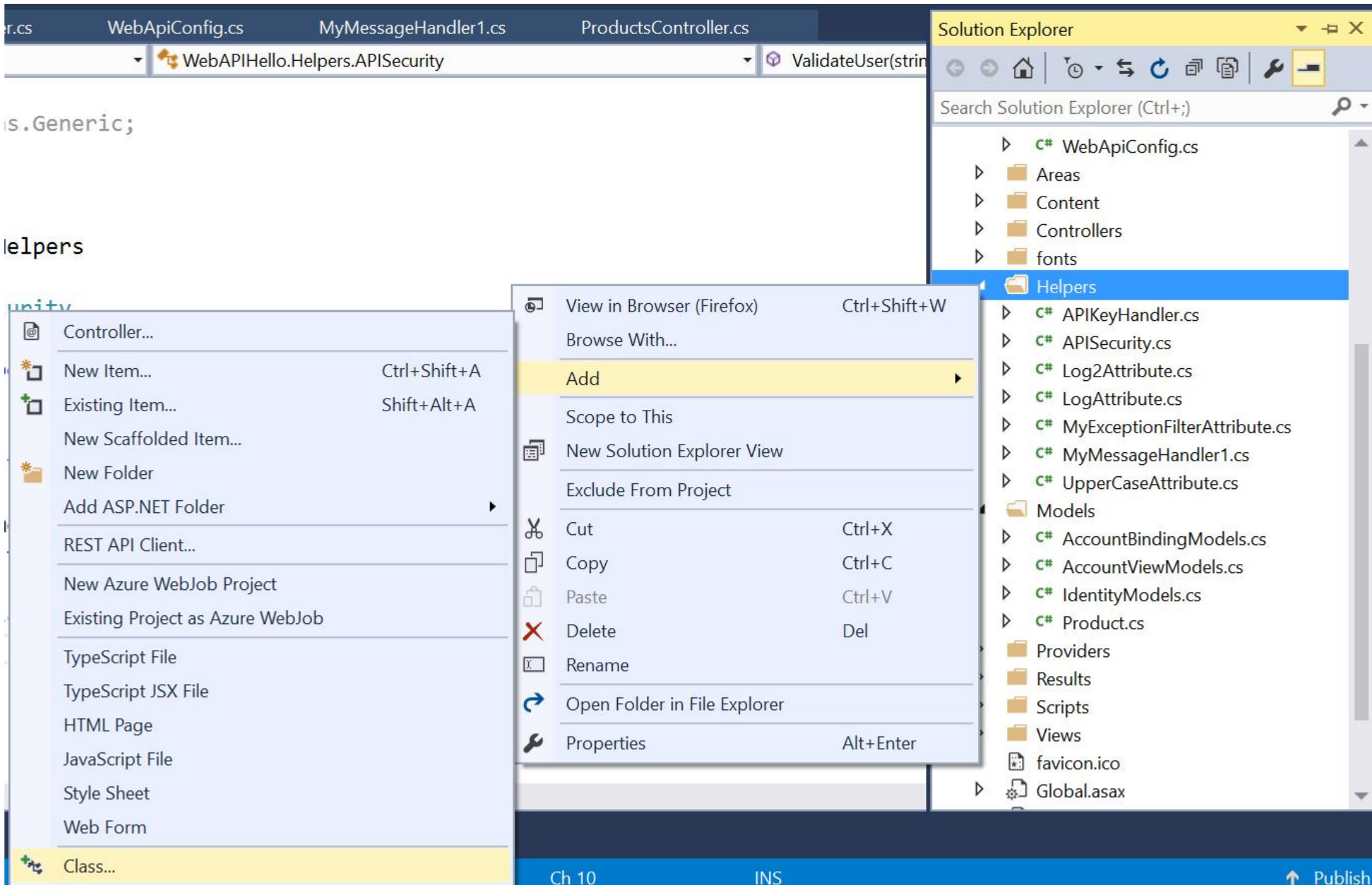
Add

Cancel

```
namespace WebAPIHello.Helpers
{
    public class APISecurity
    {
        public static bool ValidateUser(string username, string password)
        {
            if (string.IsNullOrEmpty(username) || string.IsNullOrEmpty(password))
                return false;

            if (username.Equals("student") && password.Equals("ddu"))
                return true;

            return false;
        }
    }
}
```

Add New Item - WebAPIHello

Installed

Visual C#

- Code
- Data
- General
- Web
- Windows Forms
- WPF
- Silverlight
- SQL Server
- Storm Items
- Workflow

Online

Sort by: Default



Class

Visual C#



Class for U-SQL

Visual C#



Interface

Visual C#



ADO.NET Entity Data Model

Visual C#



Application Manifest File

Visual C#



Assembly Information File

Visual C#



Class Diagram

Visual C#



Code Analysis Rule Set

Visual C#



Code File

Visual C#

[Click here to go online and find templates.](#)

Search Installed Templates (Ctrl+E)

Type: Visual C#

An empty class declaration

Name: BasicAuthenticationAttribute.cs

Add

Cancel

```
1 using System;
2 using System.Collections.Generic;
3 using System.Linq;
4 using System.Web;
5 using System.Web.Http.Controllers;
6 using System.Web.Http.Filters;
7 using System.Net.Http;
8 using System.Net;
9 using System.Text;
10
11 namespace ProductsApp.Helpers
12 {
13     public class BasicAuthenticationAttribute : AuthorizationFilterAttribute
14     {
15         public override void OnAuthorization(HttpContext actionContext)
16         {
17             if (actionContext.Request.Headers.Authorization == null)
18             {
19                 HttpResponseMessage resp = new HttpResponseMessage(HttpStatusCode.Unauthorized);
20                 resp.Headers.Add("WWW-Authenticate", "Basic realm='Account Page'");
21                 actionContext.Response = resp;
22             }
23             else
24             {
25                 string authString = actionContext.Request.Headers.Authorization.Parameter;
26                 string origString = Encoding.UTF8.GetString(Convert.FromBase64String(authString));
```


WebApiConfig.cs BasicAuthenticationAttribute.cs* APISecurity.cs ProductsController.cs

ProductsApp ProductsApp.Helpers.BasicAuthenticationAttribute OnAuthorization(HttpContext actionContext)

```
11 namespace ProductsApp.Helpers
12 {
13     public class BasicAuthenticationAttribute : AuthorizationFilterAttribute
14     {
15         public override void OnAuthorization(HttpContext actionContext)
16         {
17             if (actionContext.Request.Headers.Authorization == null) {
18                 HttpResponseMessage resp = new HttpResponseMessage(HttpStatusCode.Unauthorized);
19                 resp.Headers.Add("WWW-Authenticate", "Basic realm='Account Page'");
20                 actionContext.Response = resp;
21             }
22             else {
23                 string authString = actionContext.Request.Headers.Authorization.Parameter;
24                 string origString = Encoding.UTF8.GetString(Convert.FromBase64String(authString));
25
26                 string username = origString.Split(':')[0];
27                 string password = origString.Split(':')[1];
28
29                 if (!APISecurity.ValidateUser(username, password)) {
30                     actionContext.Request.CreateResponse(HttpStatusCode.Unauthorized);
31                 }
32             }
33             base.OnAuthorization(actionContext);
34         }
35     }
36 }
```

```
namespace WebAPIHello.Controllers
{
    // [Log]
    // [Log2]
    [BasicAuthentication] ←
    public class ProductsController : ApiController
    {
        static List<Product> products = new List<Product>
        {
            new Product() { ProductId=1, ProductName="Monitor",      ProductPrice=10000 },
            new Product() { ProductId=2, ProductName="Keyboard",     ProductPrice=1500 },
            new Product() { ProductId=3, ProductName="Mouse",        ProductPrice=400  }
        }; // [AllowAnonymous]
        public IEnumerable<Product> GetProducts()
        {
            return products;
        }
    }
}
```

```
] namespace WebAPIHello
{
]     public static class WebApiConfig
    {
]         public static void Register(HttpConfiguration config)
        {

            config.Filters.Add(new BasicAuthenticationAttribute());

            //config.MessageHandlers.Add(new MyMessageHandler1());
        }
    }
}
```



HTTP Error 403.14 - Forbidden

The Web server is configured to not list the contents of this directory.

IIS 10.0 Detailed Error - 403.14 X +



localhost:12345/api/products

HTTP Error 403.14 - Forbidden

The Web server is configured to not list the contents of this directory.

Most likely causes:

- A default document is not configured for the requested URL, and directory browsing is not enabled on the server.



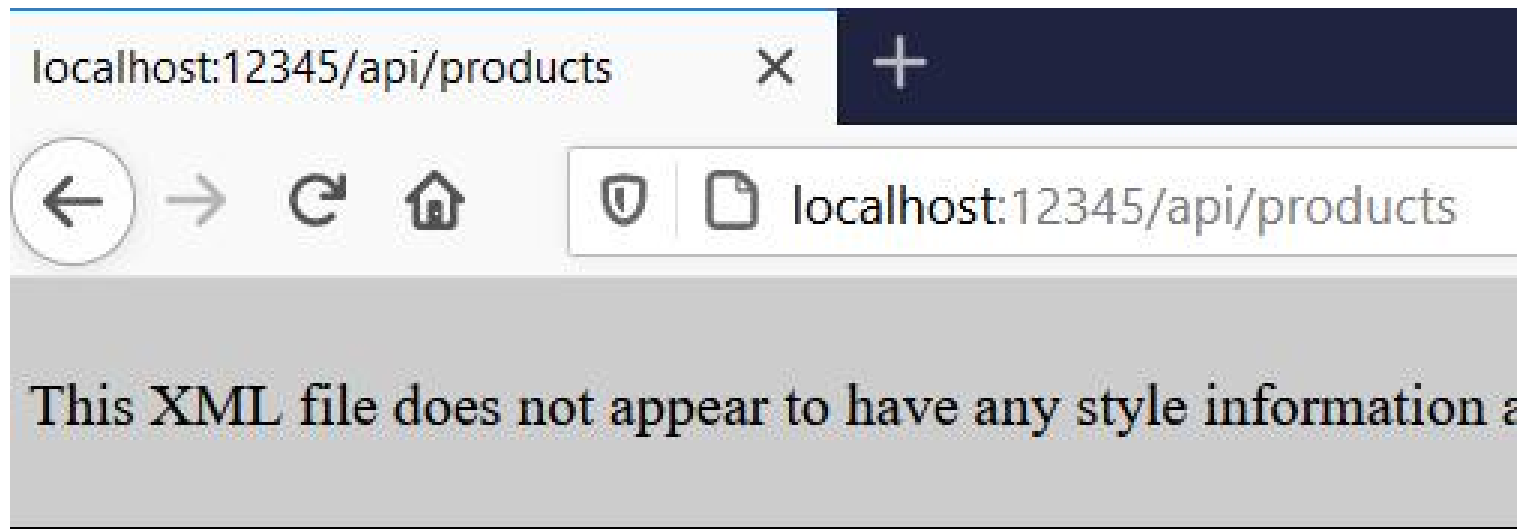
http://localhost:12345 is requesting your username and password.

User Name: student

Password: ...

OK

Cancel



```
—<ArrayOfProduct>
  —<Product>
    <prodCategory>Groceries</prodCategory>
    <prodId>1</prodId>
    <prodName>Tomato Soup</prodName>
    <prodPrice>100</prodPrice>
  </Product>
  —<Product>
    <prodCategory>Toys</prodCategory>
    <prodId>2</prodId>
    <prodName>Yo-yo</prodName>
    <prodPrice>25.50</prodPrice>
  </Product>
  —<Product>
    <prodCategory>Hardware</prodCategory>
    <prodId>3</prodId>
    <prodName>Hammer</prodName>
    <prodPrice>55.50</prodPrice>
  </Product>
</ArrayOfProduct>
```

GET

⌵

http://localhost:12345/api/products

Send

⌵

- Params
- Authorization
- Headers (10)
- Body ●
- Pre-request Script
- Tests
- Settings
- Cookies

Type

Inherit aut...⌵

The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)

This request is not inheriting any authorization helper at the moment. Save it in a collection to use the parent's authorization helper.

Body

Cookies

Headers (10)

Test Results

🌐

Status: 401 Unauthorized

Time: 119 ms

Size: 367 B

Save Response ⌵

KEY	VALUE
Cache-Control ⓘ	no-cache
Pragma ⓘ	no-cache
Expires ⓘ	-1
Server ⓘ	Microsoft-IIS/10.0
WWW-Authenticate ⓘ	Basic relm='Account Page'
X-AspNet-Version ⓘ	4.0.30319
X-SourceFiles ⓘ	=?UTF-8?B?RDpcZG90bmV0XHdlYmFwaVxQcm9kdWN0c0FwcFwQcm9kdW...

http://localhost:49998/api/products

Save

GET

http://localhost:12345/api/products

Send

Params Authorization Headers (10) Body Pre-request Script Tests Settings Cookies

Type

Inherit aut... ^

The authorization header is automatically generated for the request. [Learn more about authentication](#)

Inherit auth from parent

No Auth

API Key

Bearer Token

Basic Auth

Digest Auth

OAuth 1.0

OAuth 2.0

Hawk Authentication

AWS Signature

NTLM Authentication [...]

Akamai EdgeGrid

This request is not inheriting any authorization helper at the moment. Save it in a collection to use the parent's authorization helper.

Body Cookies Headers Status: 401 Unauthorized Time: 119 ms Size: 367 B Save Response

KEY	VALUE
Cache-Control	no-cache
Pragma ⓘ	no-cache
Expires ⓘ	-1
Server ⓘ	Microsoft-IIS/10.0
WWW-Authenticate	Basic realm='Account Page'
X-AspNet-Version	4.0.30319
X-SourceFiles ⓘ	=?UTF-8?B?RDpcZG90bmV0XHdIYmFwaVxQcm9kdWN0c0FwcFwQcm9kdW...

GET

http://localhost:12345/api/products

Send

Params

Authorization

Headers (11)

Body

Pre-request Script

Tests

Settings

Cookies

Type

Basic Auth

The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)

Username

student

Password

...

ⓘ Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Body

Cookies

Headers (10)

Test Results

⌐ Status: 401 Unauthorized

Time: 119 ms

Size: 367 B

Save Response

KEY	VALUE
Cache-Control ⓘ	no-cache
Pragma ⓘ	no-cache
Expires ⓘ	-1
Server ⓘ	Microsoft-IIS/10.0
WWW-Authenticate ⓘ	Basic realm='Account Page'
X-AspNet-Version ⓘ	4.0.30319
X-SourceFiles ⓘ	=?UTF-8?B?RDpcZG90bmV0XHdlYmFwaVxQcm9kdWN0c0FwcFwQcm9kdW...

GET

http://localhost:12345/api/products

Send

- Params
- Authorization
- Headers (11)
- Body
- Pre-request Script
- Tests
- Settings
- Cookies

Type

Basic Auth

The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)

ⓘ Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Username

student

Password

...

- Body
- Cookies
- Headers (10)
- Test Results
- Status: 200 OK
- Time: 410 ms
- Size: 594 B
- Save Response

KEY	VALUE
Cache-Control ⓘ	no-cache
Pragma ⓘ	no-cache
Content-Type ⓘ	application/json; charset=utf-8
Expires ⓘ	-1
Server ⓘ	Microsoft-IIS/10.0
X-AspNet-Version ⓘ	4.0.30319
X-SourceFiles ⓘ	=?UTF-8?B?RDpcZG90bmV0XHdlYmFwaVxQcm9kdWN0c0FwcFwQcm9kdW...

GET

http://localhost:12345/api/products

Send

Params

Authorization ●

Headers (11)

Body ●

Pre-request Script

Tests

Settings

Cookies

Type

Basic Auth

The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)

⚠ Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Username

student

Password

...

Body

Cookies

Headers (10)

Test Results



Status: 200 OK

Time: 410 ms

Size: 594 B

[Save Response](#)

Pretty

Raw

Preview

Visualize

JSON



```
1  [
2    {
3      "prodId": 1,
4      "prodName": "Tomato Soup",
5      "prodCategory": "Groceries",
6      "prodPrice": 100.0
7    },
8    {
9      "prodId": 2,
10     "prodName": "Yo-yo",
11     "prodCategory": "Toys",
```

GET

http://localhost:12345/api/products/3

Send

Params Authorization Headers (11) Body Pre-request Script Tests Settings

Cookies

Type

Basic Auth

The authorization header will be automatically generated when you send the request.

[Learn more about authorization](#)

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. [Learn more about variables](#)

Username

student

Password

...

Body Cookies Headers (10) Test Results



Status: 200 OK

Time: 56 ms

Size: 440 B

Save Response

Pretty

Raw

Preview

Visualize

JSON



```
1 {  
2   "prodId": 3,  
3   "prodName": "Hammer",  
4   "prodCategory": "Hardware",  
5   "prodPrice": 55.50  
6 }
```

GET

http://localhost:12345/api/products/3

Send

Params

Authorization

Headers (11)

Body

Pre-request Script

Tests

Settings

Cookies

Headers

9 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets
<input checked="" type="checkbox"/>	Content-Type	application/json				
<input checked="" type="checkbox"/>	Accept	application/xml				
	Key	Value	Description			

Body

Cookies

Headers (10)

Test Results

Status: 200 OK

Time: 27 ms

Size: 612 B

Save Response

Pretty

Raw

Preview

Visualize

XML

```
1 <Product xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.datacontract.org/2004/07/ProductsApp.Models">
2   <prodCategory>Hardware</prodCategory>
3   <prodId>3</prodId>
4   <prodName>Hammer</prodName>
5   <prodPrice>55.50</prodPrice>
6 </Product>
```

GET ⌵ http://localhost:12345/api/products/3 Send ⌵

Params Authorization ● Headers (11) Body ● Pre-request Script Tests Settings Cookies

Headers ⚡ Hide auto-generated headers

	KEY	VALUE	DESCRIPTION	⋮	Bulk Edit	Presets ⌵
<input checked="" type="checkbox"/>	Authorization ⓘ	Basic c3R1ZGVudDpkZHU=				
<input checked="" type="checkbox"/>	Postman-Token ⓘ	<calculated when request is sent>				
<input checked="" type="checkbox"/>	Content-Type ⓘ	text/plain				
<input type="checkbox"/>						

Body Cookies Headers (10) Test Results 🌐 Status: 200 OK Time: 27 ms Size: 612 B Save Response ⌵

Pretty Raw Preview Visualize XML ⌵ ≡ 📄 🔍

```
1 <Product xmlns:i="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.datacontract.org/2004/07/ProductsApp.Models">
2   <prodCategory>Hardware</prodCategory>
3   <prodId>3</prodId>
4   <prodName>Hammer</prodName>
5   <prodPrice>55.50</prodPrice>
6 </Product>
```

localhost:12345/api/products



Search

Developer Tools - http://localhost:12345/api/products

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other Persist Logs Disable cache Filter URLs

S... Me F... D... C... T... Headers Cookies Params Response Timings Stack Trace

401 GET pr... loc... JS doc... plain 401



Request URL: http://localhost:12345/api/products

Request method: GET

Remote address: [::1]:12345

Status code: 401 Unauthorized

Edit and Resend

Raw headers

Version: HTTP/1.1

Filter headers

Response headers (408 B)

Cache-Control: no-cache

Content-Length: 0

Date: Tue, 20 Mar 2018 19:10:25 GMT

Expires: -1

Pragma: no-cache

Server: Microsoft-IIS/10.0



One request

0 B / 408 B transferred

Finish: 0 m

New Request

Send

Cancel

GET

http://localhost:12345/api/products

Request Headers:

Host: localhost:12345

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0, no-cache

Authorization: Basic c3R1ZGVudDpkZHU=

Request Body:

Headers	Cookies	Params	Response	Timings	Stack Trace
Request URL: http://localhost:12345/api/products					
Request method: GET					
Remote address: [::1]:12345					
Status code: ● 200 OK ⓘ Edit and Resend Raw headers					
Version: HTTP/1.1					
⌵ Filter headers					
▼ Response headers (420 B)					
ⓘ Cache-Control: no-cache					
ⓘ Content-Length: 481					
ⓘ Content-Type: application/xml; charset=utf-8					
ⓘ Date: Tue, 20 Mar 2018 19:14:07 GMT					
ⓘ Expires: -1					
ⓘ Pragma: no-cache					
ⓘ Server: Microsoft-IIS/10.0					
X-AspNet-Version: 4.0.30319					
X-Powered-By: ASP.NET					
X-SourceFiles: =?UTF-8?B?QzpcVXNlcnNcTEVOT1ZP...UhIbGxvXGFwaVxwcm9kdWN0cw==?=					
▼ Request headers (430 B)					
ⓘ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8					
ⓘ Accept-Encoding: gzip, deflate					
ⓘ Accept-Language: en-US,en;q=0.5					
ⓘ <u>Authorization: Basic c3R1ZGVudDpkZHU=</u>					
ⓘ Cache-Control: max-age=0, no-cache					
ⓘ Connection: keep-alive					
ⓘ Host: localhost:12345					
ⓘ Pragma: no-cache					
ⓘ Upgrade-Insecure-Requests: 1					
ⓘ User-Agent: Mozilla/5.0 (Windows NT 10.0; ...) Gecko/20100101 Firefox/58.0					

New Request

Send Cancel

GET

http://localhost:12345/api/products

Request Headers:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0, no-cache

Authorization: Basic c3R1ZGVudDpkZHU=

Pragma: no-cache

Accept: application/json

Request Body:

Headers	Cookies	Params	Response	Timings	Stack Trace
Request URL: http://localhost:12345/api/products					
Request method: GET					
Remote address: [::1]:12345					
Status code: 200 OK ⓘ Edit and Resend Raw headers					
Version: HTTP/1.1					
⌵ Filter headers					
▼ Response headers (421 B)					
ⓘ Cache-Control: no-cache					
ⓘ Content-Length: 186					
ⓘ Content-Type: application/json; charset=utf-8					
ⓘ Date: Tue, 20 Mar 2018 19:20:37 GMT					
ⓘ Expires: -1					
ⓘ Pragma: no-cache					
ⓘ Server: Microsoft-IIS/10.0					
X-AspNet-Version: 4.0.30319					
X-Powered-By: ASP.NET					
X-SourceFiles: =?UTF-8?B?QzpcVXNlcnNcTEVOT1ZP...UhIbGxvXGFwaVxwcm9kdWN0cw==?=					
▼ Request headers (383 B)					
ⓘ Accept: application/json					
ⓘ Accept-Encoding: gzip, deflate					
ⓘ Accept-Language: en-US,en;q=0.5					
ⓘ Authorization: Basic c3R1ZGVudDpkZHU=					
ⓘ Cache-Control: max-age=0, no-cache					
ⓘ Connection: keep-alive					
ⓘ Host: localhost:12345					
ⓘ Pragma: no-cache					
ⓘ Upgrade-Insecure-Requests: 1					
ⓘ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36					

Inspector Console Debugger Style Editor Performance Memory Network Storage

All HTML CSS JS XHR Fonts Images Media WS Other ☐ Persist Logs ☐ Disable cache Filter URLs

S...	Me	F...	D...	C...	T...	T...	S...	Headers	Cookies	Params	Response	Timings	Stack Trace
401	GET	pr...	loc...	doc...	plain	408 B	0 B	Filter properties					
200	GET	pr...	loc...	other	xml	901 B	481 B	JSON					
200	GET	pr...	loc...	other	json	607 B	186 B	0: {...}					

productId: 1

productName: Monitor

productPrice: 10000

1: {...}

productId: 2

productName: Keyboard

productPrice: 1500

2: {...}

productId: 3

productName: Mouse

productPrice: 400

Response payload

1 [{"productId":1,"productName":"Monitor","productPrice":10000.0},{productId:2,"productName":"Keyboard","productPrice":1500.0}