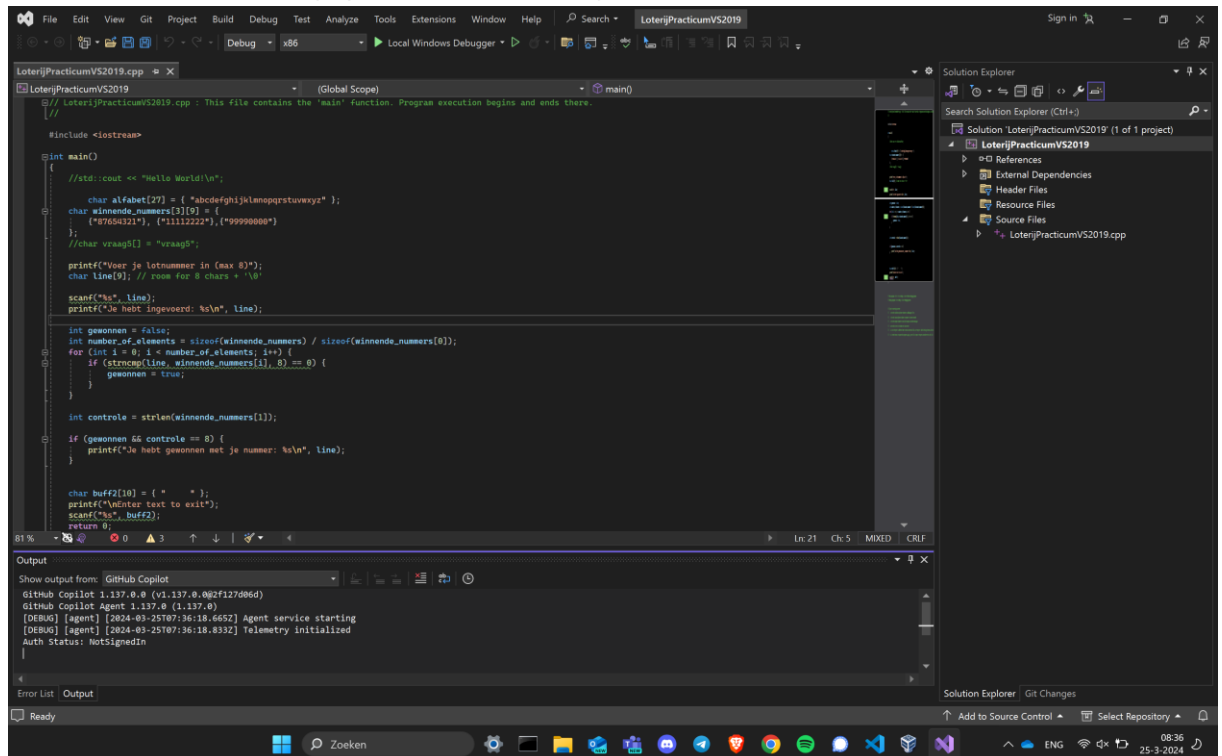


CST1 - Practicum les 6 –Integer overflow en Secure Defaults voor TLS

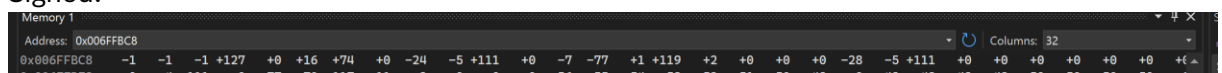
Opdracht 1: Integers overflow in C

1. Pak de code van het vorige practicum er weerbij



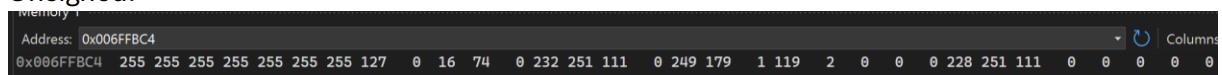
2. Laat zien mbv het memory window wat het verschil is tussen een signed en unsigned integer. Welke bit waardes heeft welk getal

Signed:



Address	Value
0x006FFBC8	-1

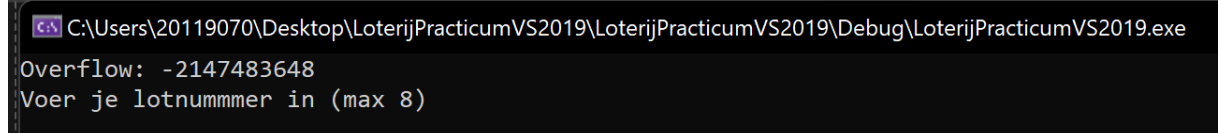
Unsigned:



Address	Value
0x006FFBC4	255

3. Maak een overflow door bij een integer een getal op te tellen. Noteer je code.

```
//overflow
std::cout << "Overflow: " << 2147483647 + 1 << std::endl;
```



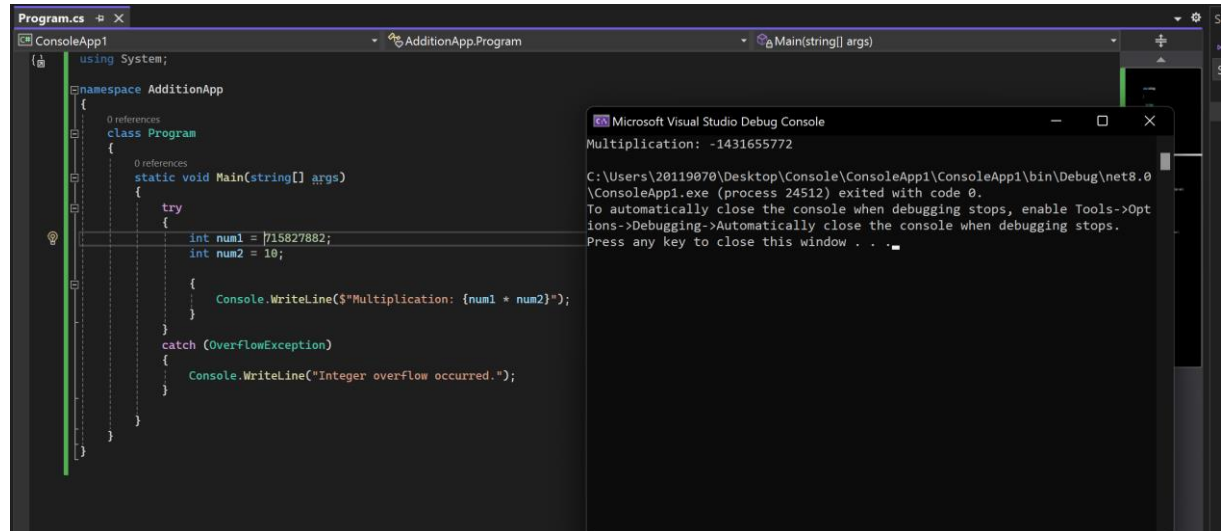
```
C:\Users\20119070\Desktop\LoterijPracticumVS2019\LoterijPracticumVS2019\Debug\LoterijPracticumVS2019.exe
Overflow: -2147483648
Voer je lotnummer in (max 8)
```

4. Wat is het effect op de waarde van getal en wat is het effect op de bit waardes?
De waarde van het getal wordt negatief. Dit komt omdat 1111 1111 1111 1111 1111 1111 1111 1110 en 1111 1111 1111 1111 1111 1111 1111 1111 de byte waardes zijn van beide getallen. Zodra er 1 byte bij komt gaat het getal van het ene uiteinde naar het andere.

Opdracht 2: Integer overflow – C#

1. Maak een console programma in C# waar je werkt met getallen.
2. Demonstreer een integer overflow voor het datatype integer (=signed) waarbij je een onverwachte uitkomst laat zien als je het getal steeds groter maakt

Ik heb hier een vermenigvuldiging van een getal met 10. Dit getal wordt zo groot dat de bitwaardes flippen en het een negatief getal wordt. De uitkomst hoort “7158278820” te zijn.



```
Program.cs # X
ConsoleApp1
AdditionApp.Program
Main(string[] args)

using System;

namespace AdditionApp
{
    class Program
    {
        static void Main(string[] args)
        {
            try
            {
                int num1 = 715827882;
                int num2 = 10;

                Console.WriteLine($"Multiplication: {num1 * num2}");
            }
            catch (OverflowException)
            {
                Console.WriteLine("Integer overflow occurred.");
            }
        }
    }
}
```

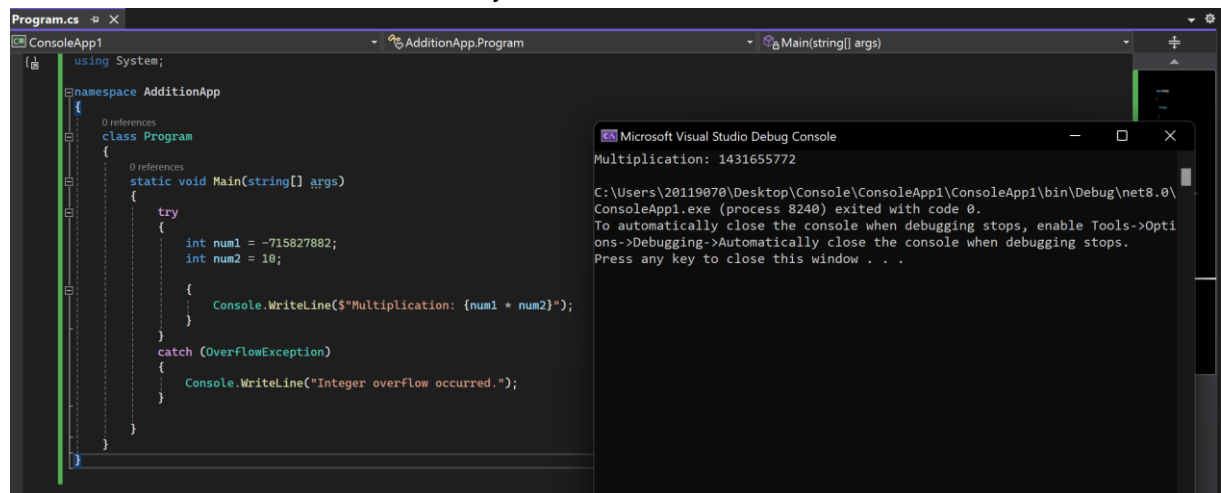
Microsoft Visual Studio Debug Console

Multiplication: -1431655772

C:\Users\20119070\Desktop\Console\ConsoleApp1\ConsoleApp1\bin\Debug\net8.0\ConsoleApp1.exe (process 24512) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .

3. Idem maar dan als je het getal steeds kleiner maakt

Ik heb hier een vermenigvuldiging van een getal met 10. Dit getal wordt zo klein dat de bitwaardes flippen en het een positief getal wordt. De uitkomst hoort “-7158278820” te zijn.



```
Program.cs # X
ConsoleApp1
AdditionApp.Program
Main(string[] args)

using System;

namespace AdditionApp
{
    class Program
    {
        static void Main(string[] args)
        {
            try
            {
                int num1 = -715827882;
                int num2 = 10;

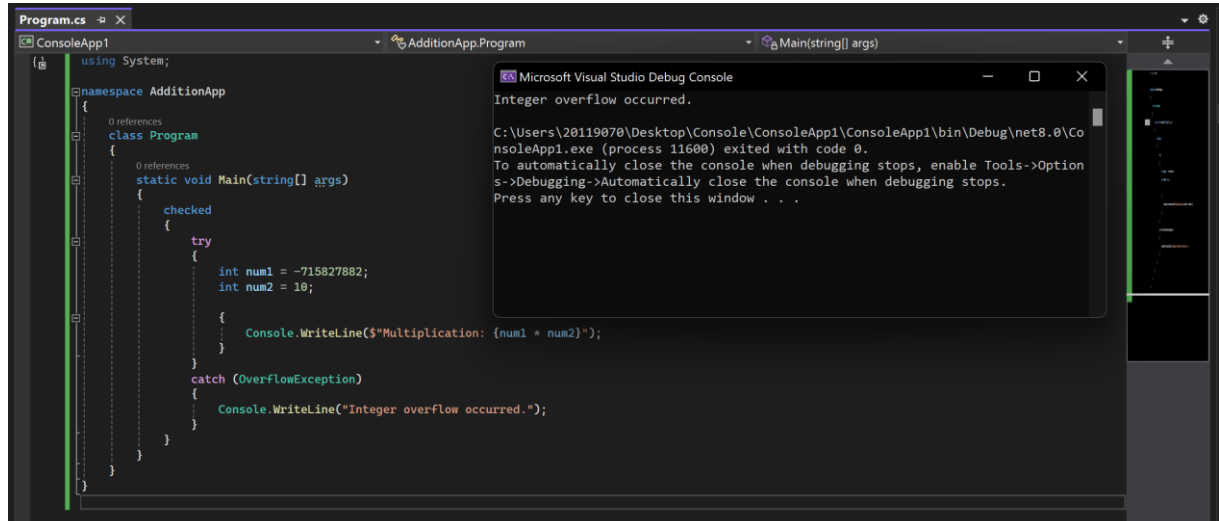
                Console.WriteLine($"Multiplication: {num1 * num2}");
            }
            catch (OverflowException)
            {
                Console.WriteLine("Integer overflow occurred.");
            }
        }
    }
}
```

Microsoft Visual Studio Debug Console

Multiplication: 1431655772

C:\Users\20119070\Desktop\Console\ConsoleApp1\ConsoleApp1\bin\Debug\net8.0\ConsoleApp1.exe (process 8240) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .

4. Maak een variant waarbij de overflow een foutmelding oplevert.



5. *Converteer een integer naar een short. Waarom is nu casting nodig?*
Dit komt doordat een short een kleinere range waarden heeft dan een int. Als je rechtstreeks een int aan een short zou toewijzen, loop je het risico dat je gegevens verliest als de gehele getalwaarde buiten het bereik valt dat door een short kan worden vertegenwoordigd.
6. *Geef een voorbeeld waarbij de casting tijdens het runnen een foutmelding geeft en geen foutmelding*
7. `using System;`
- 8.
9. `class Program`
10. `{`
11. `static void Main(string[] args)`
12. `{`
13. `int geheelGetalWaarde = 1000;`
14. `short kortWaarde = geheelGetalWaarde; // Dit zal een`
`compilatiefout veroorzaken`
- 15.
16. `// Om het te laten werken, moet je expliciet casten`
17. `//short kortWaarde = (short)geheelGetalWaarde;`
- 18.
19. `Console.WriteLine(kortWaarde);`
20. `}`
21. `}`

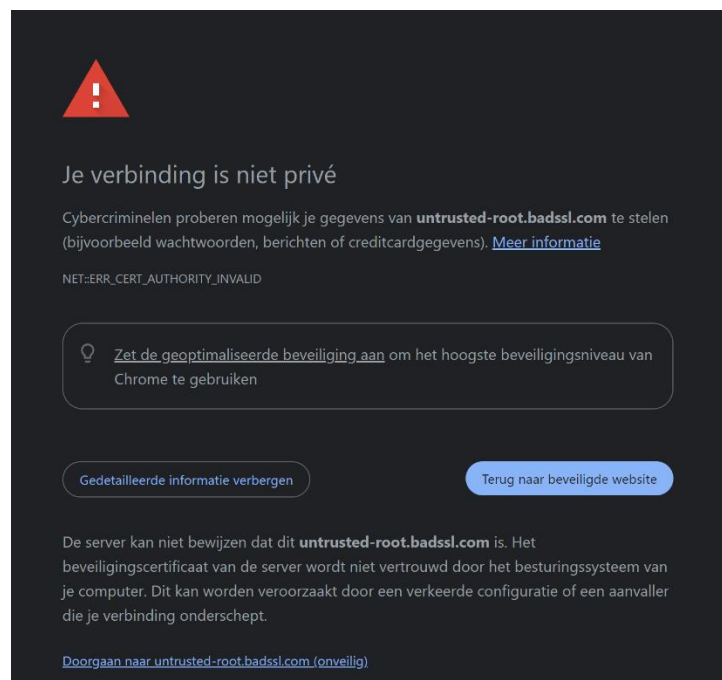
Opdracht 3: TLS defaults

1. Schrijf op hoe de browser reageert op het openen van een link op [badssl.com](https://revoked.badssl.com)
 - a. Zoek 2 opties waarbij je ondanks een waarschuwing van de browser als gebruiker toch door kan gaan. Geef ook een uitleg wat er aan de hand is

Bij de pagina revoked kan de gebruiker toch door gaan ondanks de waarschuwing. Deze waarschuwing houdt in dat het certificaat is verlopen.

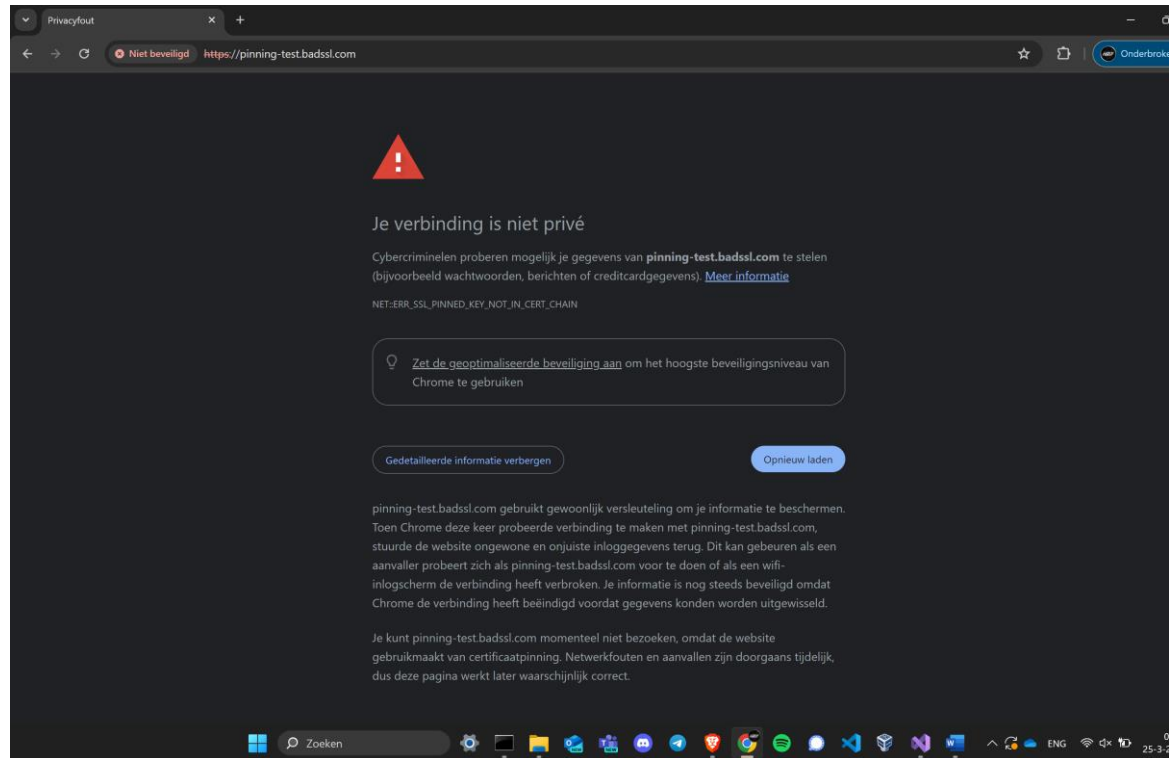


Bij de pagina untrusted-root kan de gebruiker toch door gaan ondanks de waarschuwing. De waarschuwing houdt in dat het certificaat niet wordt vertrouwd aangezien het niet vanuit de root CA komt.

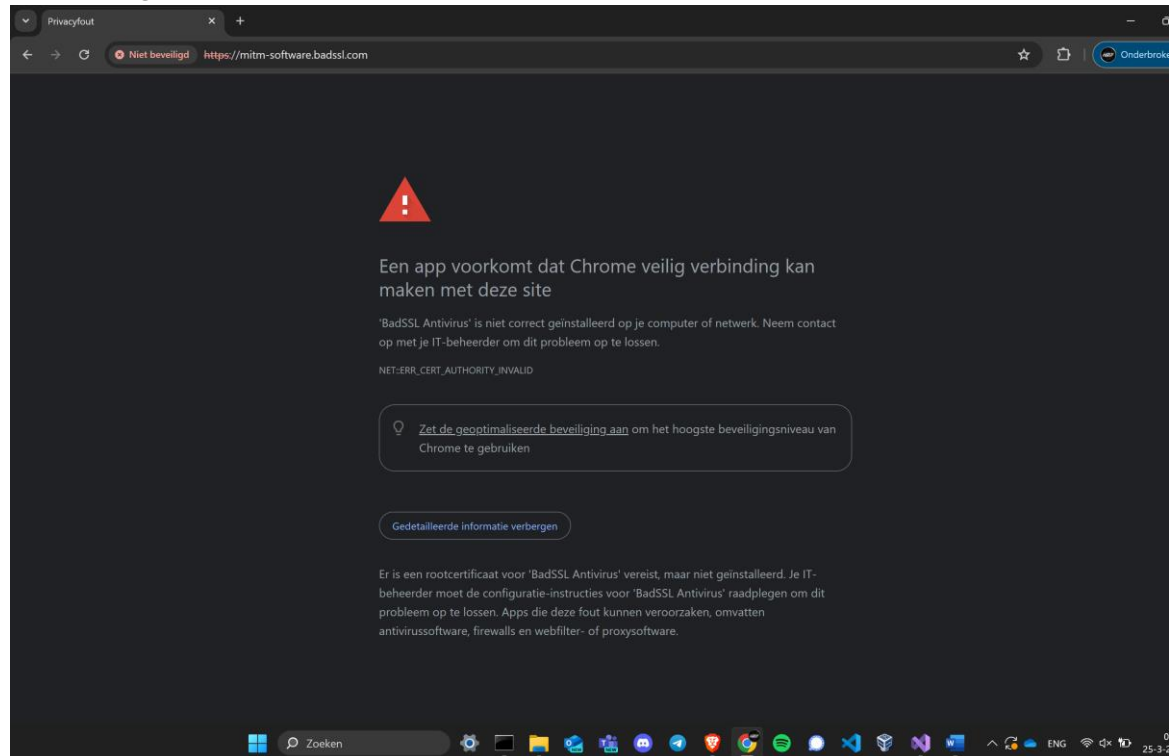


b. Zoek 2 opties waarbij de browser een error geeft (als gebruiker kan je niet doorgaan)

1. De pagina “pinning-test” geeft geen optie om door te gaan.



2. Hetzelfde geldt voor “mitm-software”.



Gebruik gemaakt van Chrome Versie 123.0.6312.59 (Officiële build) (64-bits)

Wat zijn de default instellingen van de curl?

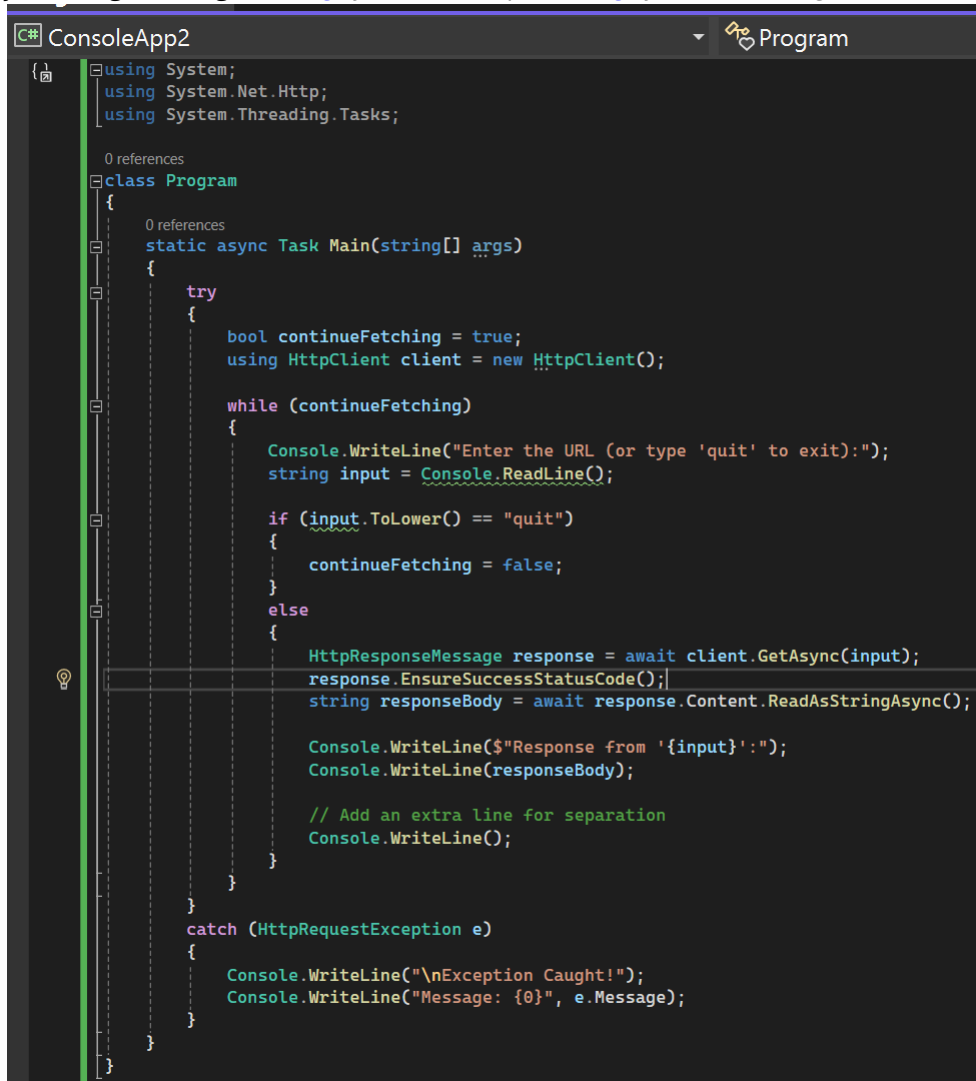
2. *Dit is een bekende command line tool voor een http request. Geef 2 voorbeelden van opties die je als gebruiker kan instellen maar vanuit security oogpunt af te raden zijn.*
 1. -k of --insecure: staat verbindingen toe die niet veilig zijn (HTTP) en zet de controle op een SSL-certificaat uit.
 2. -u of --user: laat de gebruiker een gebruikersnaam en wachtwoord opgeven voor serverauthenticatie (gebruiker:wachtwoord). Hierdoor wordt deze informatie bloot gesteld aan iedereen met toegang tot het systeem.

Wat zijn de default instellingen van een https in een C# programma?

Te gebruiken class: HttpClient

<https://learn.microsoft.com/en-us/dotnet/api/system.net.http.httpclient?view=net-7.0>

- a) Maak een C# programma met de gegeven voorbeeld code. NB: voor dit voorbeeld moet je 2 using toevoegen: `using System.Net.Http;` en `using System.Threading.Tasks;`



```
using System;
using System.Net.Http;
using System.Threading.Tasks;

class Program
{
    static async Task Main(string[] args)
    {
        try
        {
            bool continueFetching = true;
            using HttpClient client = new HttpClient();

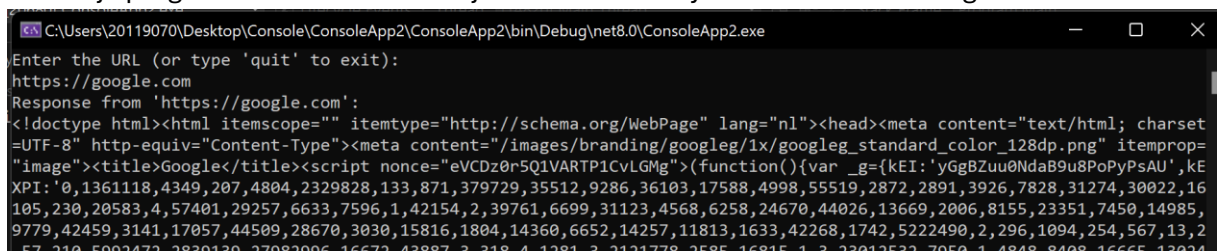
            while (continueFetching)
            {
                Console.WriteLine("Enter the URL (or type 'quit' to exit):");
                string input = Console.ReadLine();

                if (input.ToLower() == "quit")
                {
                    continueFetching = false;
                }
                else
                {
                    HttpResponseMessage response = await client.GetAsync(input);
                    response.EnsureSuccessStatusCode();
                    string responseBody = await response.Content.ReadAsStringAsync();

                    Console.WriteLine($"Response from '{input}':");
                    Console.WriteLine(responseBody);

                    // Add an extra line for separation
                    Console.WriteLine();
                }
            }
        }
        catch (HttpRequestException e)
        {
            Console.WriteLine("\nException Caught!");
            Console.WriteLine("Message: {0}", e.Message);
        }
    }
}
```

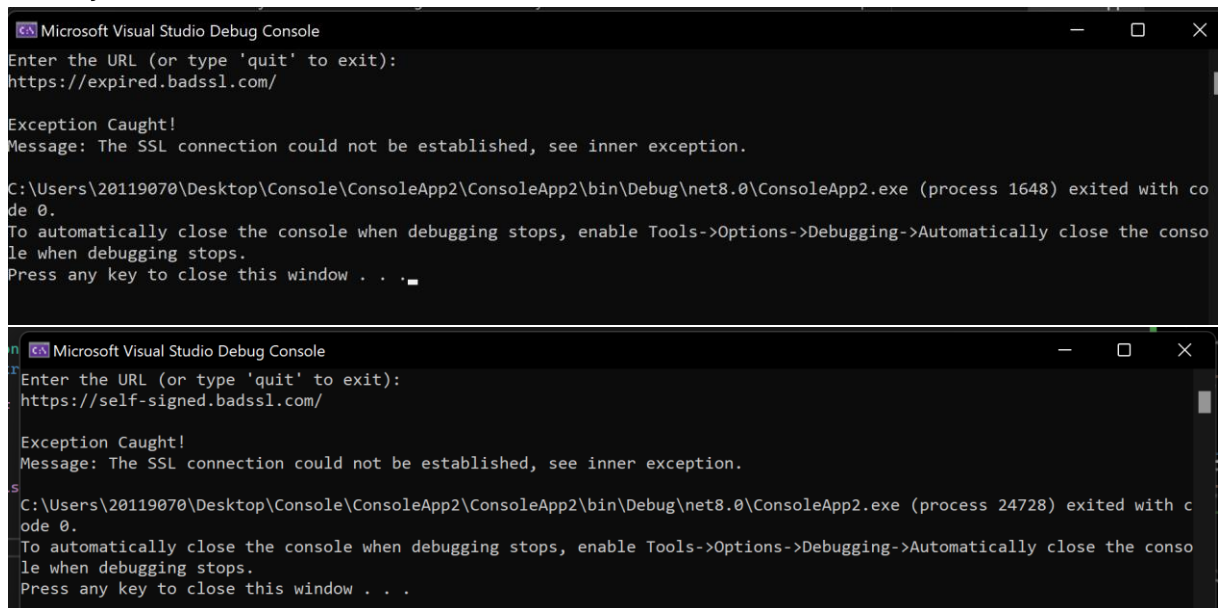
- b) Test of je programma werkt? NB: Zie je ook waar nu asynchrone code wordt gebruikt?



```
C:\Users\20119070\Desktop\Console\ConsoleApp2\ConsoleApp2\bin\Debug\net8.0\ConsoleApp2.exe
Enter the URL (or type 'quit' to exit):
https://google.com
Response from 'https://google.com':
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="nl"><head><meta content="text/html; charset=
=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/google/1x/google_standard_color_128dp.png" itemprop=
"image"><title>Google</title><script nonce="eVCDz0r5Q1VARTP1CvLGMg">(function(){var _g={kEI:'yGgBZuu0NdaB9u8PoPyPsAU',kE
XPI:'0,1361118,4349,207,4804,2329828,133,871,379729,35512,9286,36103,17588,4998,55519,2872,2891,3926,7828,31274,30022,16
105,230,20583,4,57401,29257,6633,7596,1,42154,2,39761,6699,31123,4568,6258,24670,44026,13669,2006,8155,23351,7450,14985,
9779,42459,3141,17057,44509,28670,3030,15816,1804,14360,6652,14257,11813,1633,42268,1742,5222490,2,296,1094,254,567,13,2
57,210,5992472,2839139,27982996,16672,43887,3,318,4,1281,3,2121778,2585,16815,1,3,23012532,7950,1,4848,8408,16665,13024
```

De code is asynchrone. Er werd gewacht op mijn input voor een URL. Alleen dan pas komt er een response. Hierdoor is de code asynchrone.

- c) Test nu op minimaal 2 voorbeelden uit *badssl.com*. Wat doet het programma? En hoe duidelijk is het antwoord?



The image shows two screenshots of the Microsoft Visual Studio Debug Console. The top screenshot shows the program running and attempting to connect to `https://expired.badssl.com/`. It then throws an exception: "Exception Caught! Message: The SSL connection could not be established, see inner exception." The bottom screenshot shows the program running and attempting to connect to `https://self-signed.badssl.com/`. It also throws an exception: "Exception Caught! Message: The SSL connection could not be established, see inner exception." Both screenshots show the program exiting with code 0 and provide instructions on how to close the console window.

```
Microsoft Visual Studio Debug Console
Enter the URL (or type 'quit' to exit):
https://expired.badssl.com/

Exception Caught!
Message: The SSL connection could not be established, see inner exception.

C:\Users\20119070\Desktop\Console\ConsoleApp2\ConsoleApp2\bin\Debug\net8.0\ConsoleApp2.exe (process 1648) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

```
Microsoft Visual Studio Debug Console
Enter the URL (or type 'quit' to exit):
https://self-signed.badssl.com/

Exception Caught!
Message: The SSL connection could not be established, see inner exception.

C:\Users\20119070\Desktop\Console\ConsoleApp2\ConsoleApp2\bin\Debug\net8.0\ConsoleApp2.exe (process 24728) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

Er ontstaat een exception. Dit komt omdat de SSL verbinding niet geldig is. Er wordt gebruik gemaakt van een TLS verbinding die ouder is dan wordt gesupport.

- d) Kan iets vinden welke versies van TLS deze class nu ondersteund in de documentatie van deze class

Dit hangt van de versie af die je hebt gedownload. .NET 4.5 support standaard TLS 1.2, .NET 5 1.2 en 1.3, .NET 6.0 support 1.3.

- e) Zie de volgende link: <https://learn.microsoft.com/en-us/dotnet/api/system.net.http.httpclienthandler.servercertificatecustomvalidationcallback?view=net-7.0>. Laat zien dat als je dit instelt, nu minimaal 1 onveilige TLS verbinding wel is toegestaan.

```
C:\Users\20119070\Desktop\Console\ConsoleApp2\ConsoleApp2\bin\Debug\net8.0\ConsoleApp2.exe
Enter the URL (or type 'quit' to exit):
https://expired.badssl.com/
Response from 'https://expired.badssl.com/':
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="shortcut icon" href="/icons/favicon-red.ico"/>
  <link rel="apple-touch-icon" href="/icons/icon-red.png"/>
  <title>expired.badssl.com</title>
  <link rel="stylesheet" href="/style.css">
  <style>body { background: red; }</style>
</head>
<body>
<div id="content">
  <h1 style="font-size: 12vw;">
    expired.<br>badssl.com
  </h1>
</div>

</body>
</html>

Enter the URL (or type 'quit' to exit):
```

- f) Zal de vorige aanpassing altijd in een security code review altijd opgemerkt worden. Je laat hiermee onveilige sites toe dus ik denk dat er altijd wel een opmerking van gemaakt zal worden alleen verschilt dit of het opgemerkt wordt als een issue of niet.