Lab 2: HTTP Requests and Responses

QUICK REVIEW

The HyperText Transfer Protocol (HTTP) had been in vogue since its first appearance. Ever since it was implemented for making it easier for scientists to share and access data, security was always an afterthought. As security breaches happened, new security patches were invented and bolted on. What is vulnerable, needs to be protected. There is a myriad of aspects to consider when looking to secure a site, and HTTP headers are a good place to start. Most of them are not all that complicated to implement. Keeping up with HTTP security headers best practices provides another security layer on top of your web assets.
When a user tries to access a page, his browser requests it from a web server. The server then responds with the content along with appropriate HTTP Response Headers which contain meta data, status error codes, cache rules and so on. A big subset of those headers are security headers which instruct your browser exactly how to behave when it handles your website's content and data.
HTTP security headers are a great way to tighten your website's security. There is actually no logic scenario when you shouldn't use them. By setting up your security headers correctly not only you help protect your site, but your users as well. This will also help you cut down on security flaws and working hours invested in tracking and fixing them. Setting security headers, the right way and keeping them up to date will greatly reduce the amount of risk mitigation actions needed in the future.
In this Lab, we will take a deeper look at the http requests and responses.

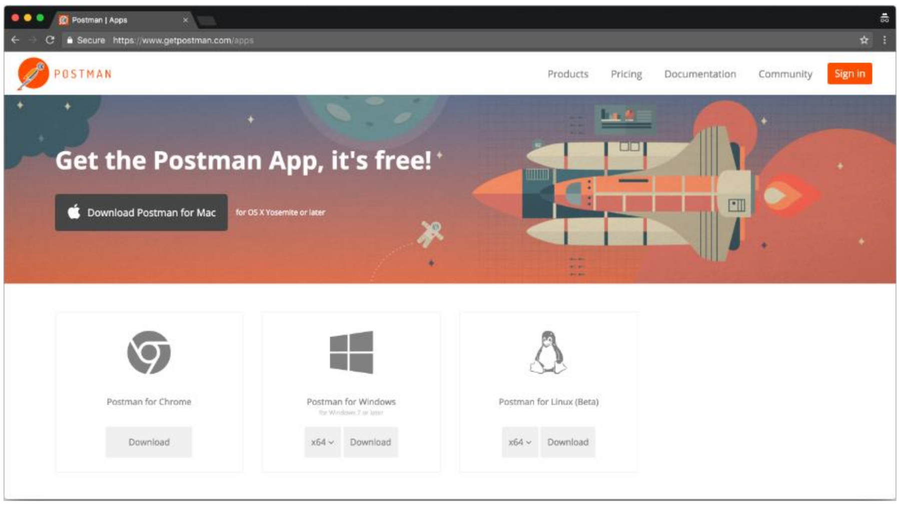
Important Notice:

Please carefully read the disclaimer declaration on the course webpage, before you start the lab practice, and make sure you fully understand all statements. The disclaimer is available on https://hogeschool.github.io/INFANL01-9.

LAB PRACTICES

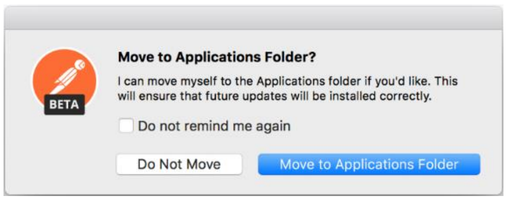
2.1. Installation of Postman

Postman is a powerful tool for performing integration testing with your API. It allows for repeatable, reliable tests that can be automated and used in a variety of environments and includes useful tools for persisting data and simulating how a user might be interacting with the system. Postman is available as a native app for macOS, Windows, and Linux operating systems. To install Postman, go to the apps page available on https://www.getpostman.com and click Download for macOS / Windows / Linux depending on your platform.



- **macOS installation**

Once you've downloaded and unzipped the app, double click on Postman. You will be prompted to move file into the "Applications" folder. Click "Move to Applications Folder" to ensure future updates can be installed correctly. The app will open after the prompt.



Move to Applications Folder?

I can move myself to the Applications folder if you'd like. This will ensure that future updates will be installed correctly.

- **Windows installation**
  - Download the setup file
  - Run the installer
- **Linux installation**

  For installation on Linux, perform the following steps:

  - First download and unzip the file
  - And then create a desktop file by name `Postman.desktop`. Create the `Postman.desktop` file in the following location:

```
~/.local/share/applications/Postman.desktop
```

Use the content below in the above file:

```
[Desktop Entry]
Encoding=UTF-8
Name=Postman
Exec=YOUR_INSTALL_DIR/Postman/app/Postman %U
Icon=YOUR_INSTALL_DIR/Postman/app/resources/app/assets/icon.png
Terminal=false
Type=Application
Categories=Development;
```

Once the `Postman.desktop` file is created, the Postman app can be opened using application launchers. You can check your desktop and double-click the Postman icon.

Note:

1. Avoid starting postman using `sudo` command, this will create permission issues on the files created by postman.
2. Make sure you have read/write permission for `~/.config` folder where Postman stores the information
3. If you are an Ubuntu 18 user, you must additionally install libgconf-2-4 package to ensure a smooth Postman run. This package, shipped by default until Ubuntu version 18, has been dropped, and is mandatory for Postman to run. Use the following command to install `libgconf-2-4`:

```
apt-get install libgconf-2-4
```

2.2. GET Request and Response using Postman

- **Choose your method**

  In this example, we are making a **GET** request to retrieve data from the server.

- **Enter a URL** (LIST USERS)

  Now let's send our first API request! Enter https://reqres.in/api/users?page=2 into the URL field.

- **Send a request**

  Click the "Send" button and inspect the returned response body.

Look at the response header and discuss it in your group.
Retry the request with different page numbers and find how many pages are available on the database.

2.3. GET Request and Response using Online Tool

Using API tester tool, you can make HTTP requests, extract values from the responses, assert the values are correct, reuse variables across steps, or inject custom logic using JavaScript. API tester Beta version is available on https://apitester.com.
Repeat Practice 2.2 using this online tool.
Compare the results with the results of Practice 2.2 and discuss it in your group.

2.4. More GET Requests and Responses

Repeat Practices 2.2 and 2.3 for the following URLs:

https://reqres.in/api/users/2 (SINGLE USER)
https://reqres.in/api/users/23 (SINGLE USER NOT FOUND)
https://reqres.in/api/unknown (LIST <RESOURCE>)
https://reqres.in/api/unknown/2 (SINGLE <RESOURCE>)
https://reqres.in/api/unknown/23 (SINGLE <RESOURCE> NOT FOUND)

2.5. POST Request and Response

Repeat Practices 2.2 and 2.3 with the **POST** request for the following URLs, using the given data below:

2.5.1. https://reqres.in/api/users (CREATE)

```
{
    "name": "morpheus",
    "job": "leader"
}
```

2.5.2. https://reqres.in/api/register (REGISTER - SUCCESSFUL)

```
{
    "email": "sydney@fife",
    "password": "pistol"
}
```

2.5.3. https://reqres.in/api/register (REGISTER - UNSUCCESSFUL)

```
{
     "email": "sydney@fife"
}
```

2.5.4. https://reqres.in/api/login (LOGIN - SUCCESSFUL)

```
{
    "email": "peter@klaven",
    "password": "cityslicka"
}
```

2.5.5. https://reqres.in/api/login (LOGIN - UNSUCCESSFUL)

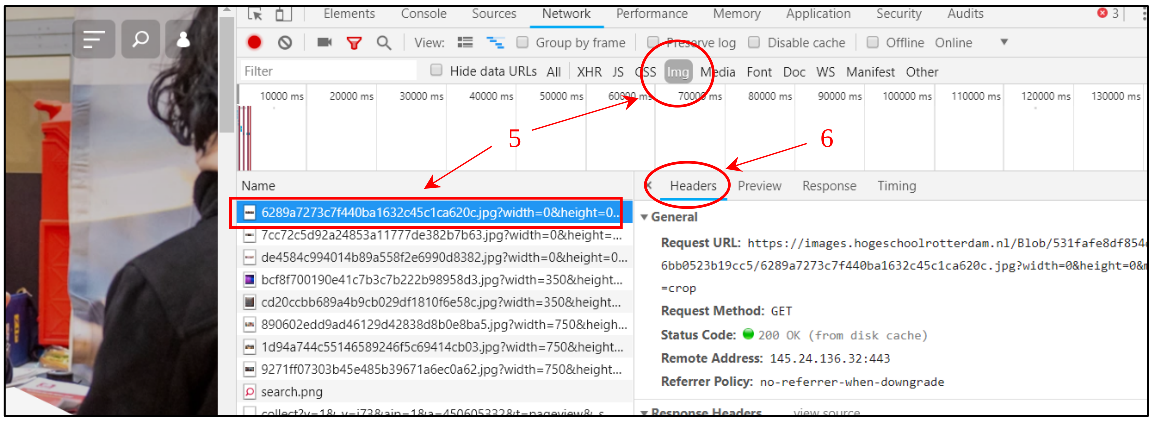
```
{
    "email": "peter@klaven"
}
```

2.6. Referer Header

In this practice, we would like to look at Refer Header using Google Chrome.

For this purpose, open your Google Chrome (if you do not have Google Chrome, please install it).
Follow the instructions below and note your observations:

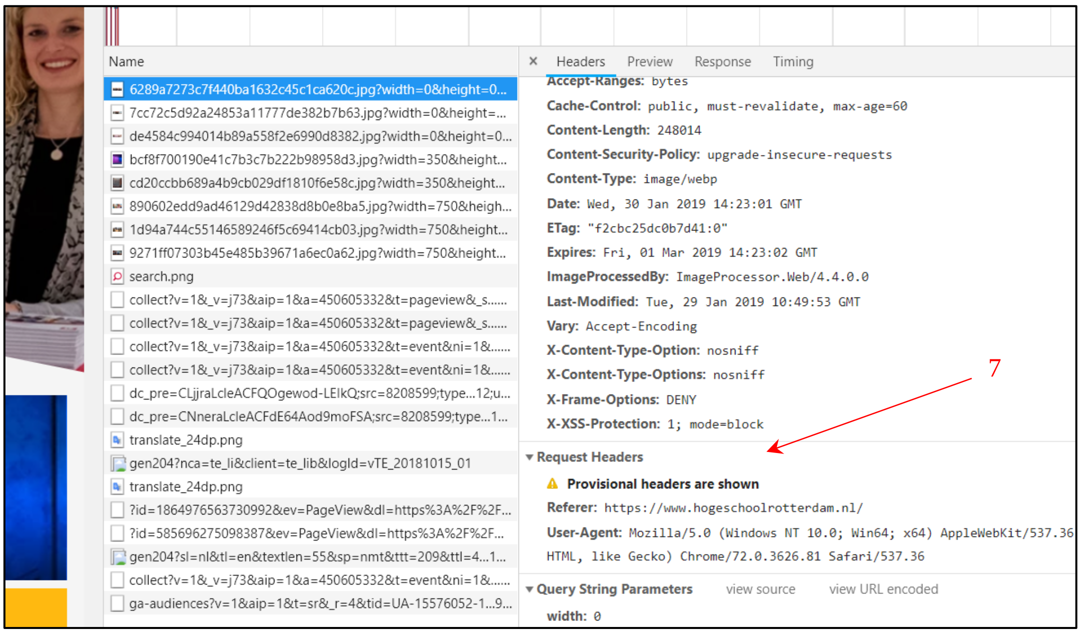
1. Go to `https://www.hogeschoolrotterdam.nl/`
2. In the `Developer Tools` (you can find it in Chrome Menu), go to the `Network` view (If it was not open when you loaded the page, you will need to reload to get it populated).
3. Click on the main page request (It should be at the top of the list).
4. When you click, the right pane will probably show the HTML for it.
5. Click on `Img` tab, then Select an image in the list.



```
6289a7273c7f440ba1632c45c1ca620c.jpg?width=0&height=0...
7cc72c5d92a24853a11777de382b7b63.jpg?width=0&height=...
de4584c994014b89a558f2e6990d8382.jpg?width=0&height=0...
bcf8f700190e41c7b3c7b222b98958d3.jpg?width=350&height...
cd20ccbb689a4b9cb029df1810f6e58c.jpg?width=350&height...
890602edd9ad46129d42838d8b0e8ba5.jpg?width=750&heigh...
1d94a744c55146589246f5c69414cb03.jpg?width=750&height...
9271ff07303b45e485b39671a6ec0a62.jpg?width=750&height...
search.png
```

```
▼ General
   Request URL: https://images.hogeschoolrotterdam.nl/Blob/531fafe8df854
   6bb0523b19cc5/6289a7273c7f440ba1632c45c1ca620c.jpg?width=0&height=0&
   =crop
   Request Method: GET
   Status Code: ● 200 OK (from disk cache)
   Remote Address: 145.24.136.32:443
   Referrer Policy: no-referrer-when-downgrade
▼ Response Headers    view source
```

6. Click on the `Headers` tab on the right side.
7. The Referer is shown in the list of `Request Headers` on the right panel (Scroll down to find it).

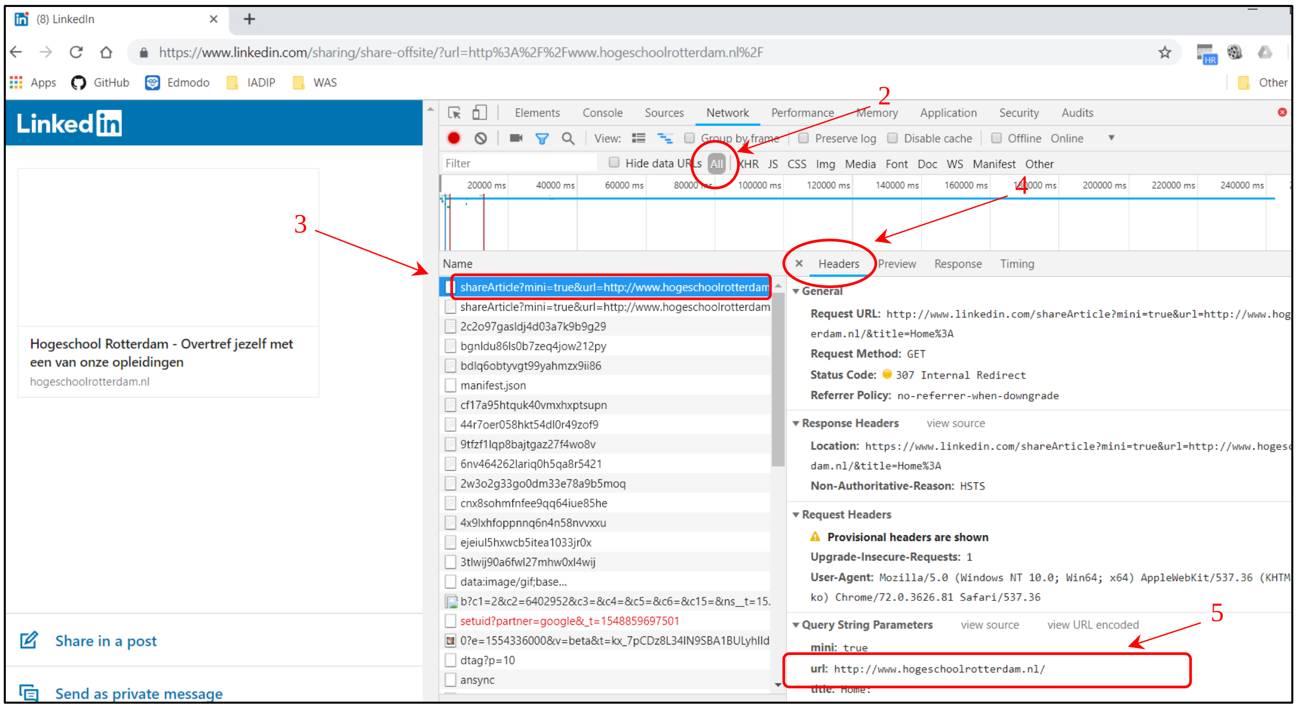


```
6289a7273c7f440ba1632c45c1ca620c.jpg?width=0&height=0...
7cc72c5d92a24853a11777de382b7b63.jpg?width=0&height=...
de4584c994014b89a558f2e6990d8382.jpg?width=0&height=0...
bcf8f700190e41c7b3c7b222b98958d3.jpg?width=350&height...
cd20ccbb689a4b9cb029df1810f6e58c.jpg?width=350&height...
890602edd9ad46129d42838d8b0e8ba5.jpg?width=750&heigh...
1d94a744c55146589246f5c69414cb03.jpg?width=750&height...
9271ff07303b45e485b39671a6ec0a62.jpg?width=750&height...
search.png
collect?v=1&_v=j73&aip=1&a=450605332&t=pageview&_s......
collect?v=1&_v=j73&aip=1&a=450605332&t=pageview&_s......
collect?v=1&_v=j73&aip=1&a=450605332&t=event&ni=1&......
collect?v=1&_v=j73&aip=1&a=450605332&t=event&ni=1&......
dc_pre=CLjjraLcleACFQOgewod-LElkQ;src=8208599;type...12;u...
dc_pre=CNneraLcleACFdE64Aod9moFSA;src=8208599;type...1...
translate_24dp.png
gen204?nca=te_li&client=te_lib&logId=vTE_20181015_01
translate_24dp.png
?id=1864976563730992&ev=PageView&dl=https%3A%2F%2F...
?id=585696275098387&ev=PageView&dl=https%3A%2F%2F...
gen204?sl=nl&tl=en&textlen=55&sp=nmt&ttt=209&ttl=4...1...
collect?v=1&_v=j73&aip=1&a=450605332&t=event&ni=1&......
ga-audiences?v=1&aip=1&t=sr&_r=4&tid=UA-15576052-1...9...
```

```
   Accept-Ranges: bytes
   Cache-Control: public, must-revalidate, max-age=60
   Content-Length: 248014
   Content-Security-Policy: upgrade-insecure-requests
   Content-Type: image/webp
   Date: Wed, 30 Jan 2019 14:23:01 GMT
   ETag: "f2cbc25dc0b7d41:0"
   Expires: Fri, 01 Mar 2019 14:23:02 GMT
   ImageProcessedBy: ImageProcessor.Web/4.4.0.0
   Last-Modified: Tue, 29 Jan 2019 10:49:53 GMT
   Vary: Accept-Encoding
   X-Content-Type-Option: nosniff
   X-Content-Type-Options: nosniff
   X-Frame-Options: DENY
   X-XSS-Protection: 1; mode=block
▼ Request Headers
   ⚠ Provisional headers are shown
   Referer: https://www.hogeschoolrotterdam.nl/
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   HTML, like Gecko) Chrome/72.0.3626.81 Safari/537.36
▼ Query String Parameters    view source    view URL encoded
   width: 0
```

2.6.1. LinkedIn

1. On the page of HR, click on the LinkedIn icon, at the bottom of page.
2. Click on `all` items tab.
3. On the `Name` column, click on the first item (you may try other objects too).
4. On the right column, click on the `Headers` tab.
5. At the bottom, in `Query String Parameters` section or other sections, try to find the refere URL: `https://www.hogeschoolrotterdam.nl/`



```
shareArticle?mini=true&url=http://www.hogeschoolrotterdam
shareArticle?mini=true&url=http://www.hogeschoolrotterdam
2c2o97gasldj4d03a7k9b9g29
bgnldu86ls0b7zeq4jow212py
bdlq6obtyvgt99yahmzx9ii86
manifest.json
cf17a95htquk40vmxhxptsupn
44r7oer058hkt54dl0r49zof9
9tfzf1lqp8bajtgaz27f4wo8v
6nv464262lariq0h5qa8r5421
2w3o2g33go0dm33e78a9b5moq
cnx8sohmfnfee9qq64iue85he
4x9lxhfoppnnq6n4n58nvvxxu
ejeiul5hxwcb5itea1033jr0x
3tlwij90a6fwl27mhw0xl4wij
data:image/gif;base...
b?c1=2&c2=6402952&c3=&c4=&c5=&c6=&c15=&ns__t=15.
setuid?partner=google&_t=1548859697501
0?e=1554336000&v=beta&t=kx_7pCDz8L34IN9SBA1BULyhlld
dtag?p=10
ansync
```

```
▼ General
  Request URL: http://www.linkedin.com/shareArticle?mini=true&url=http://www.hog
  erdam.nl/&title=Home%3A
  Request Method: GET
  Status Code: ● 307 Internal Redirect
  Referrer Policy: no-referrer-when-downgrade
▼ Response Headers    view source
  Location: https://www.linkedin.com/shareArticle?mini=true&url=http://www.hoges
  dam.nl/&title=Home%3A
  Non-Authoritative-Reason: HSTS
▼ Request Headers
  ⚠ Provisional headers are shown
  Upgrade-Insecure-Requests: 1
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
  ko) Chrome/72.0.3626.81 Safari/537.36
▼ Query String Parameters    view source    view URL encoded
  mini: true
  url: http://www.hogeschoolrotterdam.nl/
  title: Home:
```

2.6.2. Instagram

Return to HR main page and Repeat the practice 2.6.1 for Instagram link.

Further Exercises (Homework)

1. If you could not complete all the Lab practices in the class, please complete them at home and note your observations.