

Meilenstein 1 Aufgabe 6.1

```
<!--  
- Praktikum DBWT. Autoren:  
- Alexander, Matthew, 3532885  
- Bryan, Nathanael Joestin, 3517701  
-->
```

1. Request Method

Hier wird die GET Method verwendet, um die Ressource
"https://www.fh-aachen.de/hochschule/bibliothek/" vom Server anzufordern.

2. Status Code

Status Code 200 bedeutet Operation erfolgreich.

3. Content Type

Dieser MIME-Typ besteht aus dem Medientyp text & dem Subtyp html,
somit text/html. Das heißt, diese Ressource ist eine HTML-Datei.

4. Accept

Accept in dem Header zeigt an, welche *Formate* der Client in der Antwort
unterstützt

(text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8)

Es gibt den q-Faktor von dem Antwortformat, das die Priorität beschreibt.

Wert	Priorität
text/html	1
application/xhtml+xml	1
image/avif	1
image/webp	1
image/apng	1
application/xml	0.9
/	0.8

Wenn es kein q-Faktor gibt, so gilt der Wert 1.

5. Cache Control

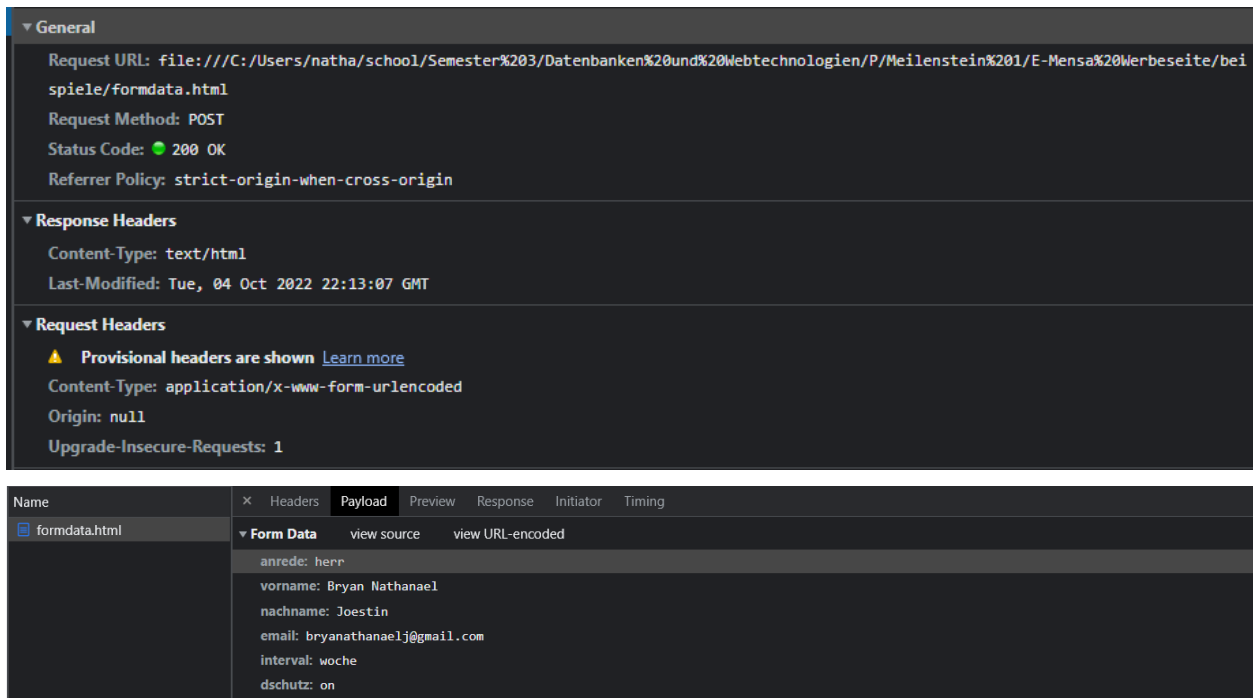
Dieser Attribut überträgt die Response & Request Direktiven für Cache-Steuerung. Die Response Direktiven sind hier *private*, die Zwischenspeicherung nur für genau den anfragenden Client erlaubt, und *no-store*, die gar keine Caches zur Antwortspeicherung erlaubt & daher führt immer zu neuem Request. Die einzelne Request Direktive ist hier *max-age=0*, die bedeutet, diese Ressource kann maximal in 0 Sekunden als aktuell betrachtet werden.

```
▼ General
Request URL: https://www.fh-aachen.de/hochschule/bibliothek/
Request Method: GET
Status Code: 200 OK
Remote Address: 149.201.122.100:443
Referrer Policy: strict-origin-when-cross-origin

▼ Response Headers View source
Cache-Control: private, no-store
Connection: keep-alive
Content-Encoding: gzip
Content-Language: de
Content-Length: 13502
Content-Type: text/html; charset=utf-8
Date: Tue, 04 Oct 2022 22:07:59 GMT
Permissions-Policy: geolocation=(self), microphone=()
Referrer-Policy
Server: nginx/1.18.0 (Ubuntu)
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block

▼ Request Headers View source
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.7
Cache-Control: max-age=0
Connection: keep-alive
Cookie: _pk_id.4.19d4=ee7ddd9a23aabd82.1656148004.; fhac_cookiemodal-selection=[%22essential%22%2C%22analytics%22%2C%22search%22]; fe_ttypo_user=b82b553e527d31e5c4565390e9168646; _pk_ref.4.19d4=%5B%22%22%2C%22%22%2C1664918698%2C%22https%3A%2F%2Fwww.google.com%2F%22%5D
Host: www.fh-aachen.de
```

Meilenstein 1 Aufgabe 6.2



Attribute Header

- 1. Request URL:**
Die Adresse der Webseite in meinen Rechner bestimmen.
- 2. Request Method:**
POST überträgt die Body-Daten an den Server.
- 3. Status Code:**
200 OK heißt die Operation erfolgreich ausgeführt wird.
- 4. Referrer Policy:**
strict-origin-when-cross-origin bietet mehr Privatsphäre. Nur der Ursprung (Origin) wird gesendet, um private Informationen zu schützen.
- 5. Content-Type (Response):**
Der Server sendet .html-Datei zurück.
- 6. Last-Modified:**
Zeigt an, wann das Dokument zuletzt geändert wurde
- 7. Content-Type (Request):**
Der Client fragt den Server in der Form von application/x-www-form-urlencoded an.

8. **Origin:** null. Das heißt wenn die Anforderung von einer Datei auf dem Computer eines Benutzers kommt und nicht von einer gehosteten Webseite

9. **Upgrade-Insecure-Request: 1**

Anforderung zum Senden eines Signals an den Server, das die Präferenz des Clients für eine verschlüsselte und authentifizierte Antwort ausdrückt.