

Datenbanken und Webtechnologie

Meilenstein 1

Aufgabe 6a)

Wie sieht der Header in der Anfrage genau aus?

Der Header ist aufgeteilt in Übersicht, Anfrage und Antwort.

Wie sieht die Antwort aus?

Antwort:

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

Content-Encoding: gzip

Content-Language: de

X-XSS-Protection: 1; mode=block

Referrer-Policy

Cache-Control: private, no-store

Date: Tue, 04 Oct 2022 11:28:30 GMT

Content-Length: 13502

Connection: keep-alive

X-Content-Type-Options: nosniff

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

Server: nginx/1.18.0 (Ubuntu)

Permissions-Policy: geolocation=(self), microphone=()

Strict-Transport-Security: max-age=31536000

Beschreiben sie mindestens 5 der verwendeten Attribute

- Content type: beschreibt das Format
- UTF8: ist die am weitesten verbreitete Kodierung für Unicode-Zeichen (8 Bit-Transformation Format)
- Cache Control: private = nur für den angefragten Client gewünscht (geteilter Cache, darf nicht gespeichert werden). No-store = keine Cache (egal wo)dürfen die Antwort speichern
- Connection: Keep alive bedeutet = Verbindung offen lassen (falls der Client noch eine Anfrage startet)
- HTTP/1.1 200 OK: 1.1 ist die momentane HTTP Version, 200 OK

Aufgabe 2, Wie sieht der Header der Anfrage beim Abschicken des Formulars "beispiele/newsletteranmeldung.html" aus?

× Vorschau **Header** Cookies Größen Zeitverh. Sicherheit

Übersicht

URL: http://localhost:63342/E-Mensa%20Werbeseite/beispiele/formdata.html
Status: 404 Not Found
Quelle: Netzwerk
Adresse: 127.0.0.1:63342

Anfrage

GET /E-Mensa%20Werbeseite/beispiele/formdata.html **HTTP/1.1**
Cookie: Phpstorm-4e07ea5e=b2f224e8-8fb7-4e69-a51e-838701a3161d
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Host: localhost:63342
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.5 Safari/605.1.15
Accept-Language: de-DE,de;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive

Antwort

HTTP/1.1 404 Not Found
X-Content-Type-Options: nosniff
Content-Type: text/html
Date: Thu, 06 Oct 2022 06:26:40 GMT
X-Frame-Options: SameOrigin
X-XSS-Protection: 1; mode=block
Content-Length: 92

Vary: origin
Server: PhpStorm 2022.2.2

Anfragedaten

MIME-Typ: application/x-www-form-urlencoded
Anrede: Herr
Vorname: df
Nachname: refref
Email: efrefref
Abteilung: Tag
Infos: on

Wie sieht der Body der Anfrage aus? Beschreiben Sie jedes Attribut im HTTP Header und dessen Bedeutung.

Content-Type: application/x-www-form-urlencoded

- MIME-Typ des Bodys (hier genutzt für POST- und PUT-Operationen)

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

- Kann der Server in diesem Beispiel den Inhalt der angeforderten Ressource sowohl als HTML als auch als Bild im GIF-Format an den Client senden, führt der Accept-Header der Anfrage dazu, dass als Inhaltstyp der Antwort HTML gewählt wird.

Accept-Encoding: gzip, deflate

- Welche komprimierten Formate der Client unterstützt. Über Content Negotiation wird eine passend komprimierte Datei ausgeliefert.

Accept-Language: de-DE,de;q=0.9

- Welche Sprachen der Client akzeptiert. Falls der Server passend eingerichtet ist und die Sprachversionen vorhanden sind, wird über Content Negotiation die passende Datei ausgeliefert.

Host: localhost:63342

- Domain-Name des Servers, zwingend vorgeschrieben seit HTTP/1.1 und nötig für namensbasierte Hosts. Bei Fehlen dieses Headers muss der Server nach Definition mit `400 Bad Request` antworten.

Origin: http://localhost:63342

- Der HTTP-Anforderungsheader (Origin Hypertext Transfer Protocol) gibt den Ursprung der Anfrage an. Dieser Header enthält keine Pfadinformationen. Es ähnelt dem Referer - Header, aber im Gegensatz zu diesem Header gibt der Origin-Header nicht den gesamten Pfad an. 1. gibt das verwendete Protokoll an (http). 2. Gibt Domänenname oder IP des Servers 3. Optional die Nummer des TCP-Ports

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.5 Safari/605.1.15

- Der User-Agent-String des Clients. In ihm stehen Informationen über den Client, sodass z. B. ein serverseitiges Skript an verschiedene Browser angepasste Inhalte ausliefern kann (z. B. bei Downloadseiten, bei denen für Mac OS andere Links angeboten werden sollen als für Microsoft Windows)

Connection: keep-alive

- Welchen Typ von Verbindung der Client bevorzugt.

Upgrade-Insecure-Requests: 1

- Upgrade-Insecure-Requests ist ein Anfragetyp-Header. Er sendet ein Signal an den Server, das die Präferenz des Clients für eine verschlüsselte und authentifizierte Antwort zum Ausdruck bringt, und er kann die HTTP-Header-Direktive Content-Security-Policy für Upgrade-Insecure-Requests erfolgreich verarbeiten.

Referer: <http://localhost:63342/E>

[Mensa%20Werbeseite/beispiele/newsletteranmeldung.html? ijt=lq4lq4b5183uiab8b2l0dbkvno& ij_reload=RELOAD ON SAVE](#)

- Im Feld Referer ist der URL der verweisenden Seite enthalten. Klickt man also auf der Hauptseite der deutschsprachigen Wikipedia einen Link an, so sendet der Browser dem Server der aufgerufenen Seite ein Headerfeld wie im Beispiel.

Content-Length: 83

- Länge des Bodys in Bytes

Cookie: Phpstorm-4e07ea5e=b2f224e8-8fb7-4e69-a51e-838701a3161d

- Ein http Cookie

Antwort

HTTP/1.1 404 Not Found

- 404 Fehlermeldung - Er gibt an, dass eine angeforderte Datei oder Seite nicht verfügbar ist.

X-Content-Type-Options: nosniff

- Der HTTP-Antwort-Header X-Content-Type-Options ist eine Markierung, die vom Server verwendet wird, um anzuzeigen, dass die in den Content-Type-Headern angegebenen MIME-Typen befolgt und nicht verändert werden sollen. Der Header ermöglicht es Ihnen, MIME-Typ-Sniffing zu vermeiden, indem er angibt, dass die MIME-Typen absichtlich konfiguriert sind.

Content-Type: text/html

- Der MIME-Typ der angeforderten Datei. Er kann nicht mit einer Charset-Angabe im HTML-Header überschrieben werden.

Access-Control-Allow-Credentials: true

- Der Antwort-Header Access-Control-Allow-Credentials teilt den Browsern mit, ob die Antwort dem JavaScript-Code des Frontends zugänglich gemacht werden soll, wenn der Anmeldemodus der Anfrage (Request. credentials) include lautet.

Access-Control-Allow-Origin: <http://localhost:63342>

- der Access-Control-Allow-Origin-Response-Header gibt an, ob die Antwort mit dem anfragenden Code des angegebenen Ursprungs geteilt werden kann.
-

Date: Thu, 06 Oct 2022 07:06:35 GMT

- Datum und Zeit zum Sendezeitpunkt der Anfrage

X-Frame-Options: SameOrigin

- X-Frame-Options:SAMEORIGIN - Dies bedeutet, dass die Seite nur in einem Frame auf einer Seite mit demselben Ursprung wie sie selbst eingebettet werden kann.

X-XSS-Protection: 1; mode=block

- Filter für Cross-Site-Scripting (XSS)

Content-Length: 92

- Länge des Bodys in Bytes

Vary: origin

- Zeigt Downstream-Proxys, wie sie anhand der Headerfelder zukünftige Anfragen behandeln sollen, also ob die gecachte Antwort genutzt werden kann oder eine neue Anfrage gestellt werden soll.

Server: PhpStorm 2022.2.2

- Serverkennung (so wie `User-Agent` für den Client ist, ist `Server` für die Serversoftware).