Assignment 1

Task 1

**1.1**

Trying 199.232.137.140...

Connected to reddit.map.fastly.net.

Escape character is '^]'.

HTTP/1.1 301 Moved Permanently

Retry-After: 0

Location: https://www.reddit.com/r/TUDelft

Content-Length: 0

Accept-Ranges: bytes

Date: Thu, 23 Dec 2021 21:02:04 GMT

Via: 1.1 varnish

Connection: close

Cache-Control: private, max-age=3600

Strict-Transport-Security: max-age=31536000; includeSubdomains

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Server: snooserv

X-Clacks-Overhead: GNU Terry Pratchett

We need to use openssl to access the resource at https://www.reddit.com/r/TUDelft.



CONNECTED(00000003)

---

Certificate chain

0 s:C = US, ST = CALIFORNIA, L = SAN FRANCISCO, O = Reddit Inc., CN = \*.reddit.com

i:C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1

1 s:C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1

i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA

---

Server certificate

-----BEGIN CERTIFICATE-----

MIIGvjCCBaagAwIBAgIQBoGik7Q5uQ63ikN3LuvhuTANBgkqhkiG9w0BAQsFADBP

MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQDEyBE

aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yMTEwMDUwMDAwMDBa

Fw0yMjA0MDIyMzU5NTlaMGcxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDQUxJRk9S

TklBMRYwFAYDVQQHEw1TQU4gRlJBTkNJU0NPMRQwEgYDVQQKEwtSZWRkaXQgSW5j

LjEVMBMGA1UEAwwMKi5yZWRkaXQuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A

MIIBCgKCAQEAz+maVKOkGuIpLUWBcrOoi0zOK7ui1z2eaWzzMtForAMdGnBV+IZa

QtyQ5++Gfv1TbOrAOKUntMp6luNeClruZSCzltfkOpk9eHJ9XWEUPrpFFCLbBVu9

1sl0EYvdWsplUlEgilO1zdDXr0UiyU0ptz14arWfA79ESEjl3EMIcCgfAumn5d9u

OQEkbOWAogF0Ed53rsoVVQoW+HVFVqdUlQ0boiQBdec9lKKDB8DbAEfdCC45zVjG

zA8Hhw4fmx1l4AlDqP2tLE2qNm2GhXjctrmexVjFG2t4nyihXllf92wvsEEGRZ8X

9pxVJTd/tfteIXPbe+u5DIE1ApPYcpfCBwIDAQABo4IDfDCCA3gwHwYDVR0jBBgw

FoAUt2ui6qiqhIx56rTaD5iyxZV2ufQwHQYDVR0OBBYEFHHgUNHngFL7IxRlnUOn

jTGqVmkmMCMGA1UdEQQcMBqCCnJlZGRpdC5jb22CDCoucmVkZGl0LmNvbTAOBgNV

HQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMIGPBgNV

HR8EgYcwgYQwQKA+oDyGOmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2Vy

dFRMU1JTQVNIQTI1NjIwMjBDQTEtNC5jcmwwQKA+oDyGOmh0dHA6Ly9jcmw0LmRp

Z2ljZXJ0LmNvbS9EaWdpQ2VydFRMU1JTQVNIQTI1NjIwMjBDQTEtNC5jcmwwPgYD

VR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDovL3d3dy5kaWdp

Y2VydC5jb20vQ1BTMH8GCCsGAQUFBwEBBHMwcTAkBggrBgEFBQcwAYYYaHR0cDov

L29jc3AuZGlnaWNlcnQuY29tMEkGCCsGAQUFBzAChj1odHRwOi8vY2FjZXJ0cy5k

aWdpY2VydC5jb20vRGlnaUNlcnRUTFNSU0FTSEEyNTYyMDIwQ0ExLTEuY3J0MAwG

A1UdEwEB/wQCMAAwggF/BgorBgEEAdZ5AgQCBIIBbwSCAWsBaQB3ACl5vvCeOTkh

8FZzn2Old+W+V32cYAr4+U1dJlwlXceEAAABfFC72CcAAAQDAEgwRgIhAOPvkGqz

OfXSiPNKqhmsc0c7M21/QkrpN1hcI4V20ttLAiEAhqdnqhRwbHLCM+tU3okCDOx0

PV5LtF7e96gYK90TvbYAdwBRo7D1/QF5nFZtuDd4jwykeswbJ8v3nohCmg3+1IsF

5QAAAXxQu9gNAAAEAwBIMEYCIQC+O/YXHqd5PEjBJXYXIVW1VminlyF+3zNnPX1O

5fKEXQIhALCTn2R0W9ru9zNIKgXbQ+eWVA45kpLSfLvo2GJe9i5MAHUAQcjKsd8i

RkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvYAAAF8ULvXsgAABAMARjBEAiBjxvP+

oo6SQ8pqoXSiunzRoO32V8mCSq7H+Q8TkqQrugIgJEFPFIrGZme9HncBIOHDzJXO

A+OhGc5/x3mJWW/IuEEwDQYJKoZIhvcNAQELBQADggEBABC4VDLWAFqbVjb85A/O

vn3S/I5Pv8+oOMMBZgEwh58EAxwdy0MCSjdQ5G5vrYRk7a3jtq0SNtVNIqgu722M

CyGb8lVv7Sc1AP4OHK/BpoBiLFf9vNlufBhnbg9eortk50qYUdW2/Qr8FRryv+cX

LJCXqwSqXEjWVq7b2y48bP5QkFIsGe5acxbGGtYN8hu9cXDWfHcGYPgmGYYTqJIW

7Gz6UCApMZXSA5iqIA7TWphkQJiOQut445kd60IdFwm307Wb9YoZ+h9cFHUkQWgX

35sxnmCoOR/3NzgFGwS+8E9zRUDCYldcCu7a01L3/EPZjtfKWwzKpSnCzEqJs2ZB

1sg=

-----END CERTIFICATE-----

subject=C = US, ST = CALIFORNIA, L = SAN FRANCISCO, O = Reddit Inc., CN = \*.reddit.com

issuer=C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1

---

No client certificate CA names sent

Peer signing digest: SHA256

Peer signature type: RSA-PSS

Server Temp Key: X25519, 253 bits

---

SSL handshake has read 3513 bytes and written 386 bytes

Verification: OK

---

New, TLSv1.3, Cipher is TLS\_AES\_256\_GCM\_SHA384

Server public key is 2048 bit

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

Early data was not sent

Verify return code: 0 (ok)

---

HTTP/1.1 200 OK

Connection: keep-alive

Cache-control: private, s-maxage=0, max-age=0, must-revalidate, no-store

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

Accept-Ranges: bytes

Date: Thu, 23 Dec 2021 21:09:44 GMT

Via: 1.1 varnish

Vary: Accept-Encoding

Set-Cookie: loid=0000000000hv2cb74s.2.1640293783019.Z0FBQUFBQmh4T1dYbXgzdW1JUnRuV3FQUng5b3dwRHFwRlp5RVdoYU43U2lWdHVoNmExcG1wNFNDU20xaVVJYkJLZXN4dHJtQnZVdTNoTklSaE90ckZ6TzNHWFg1VmhHVm5xUVF6SnRuajM1SWV6NmJxNkVPZXBhSGRPQ3R3RmZtcUZJekVRTGV3bHU; path=/; expires=Sat, 23 Dec 2023 21:09:43 GMT; domain=.reddit.com; samesite=none; secure

Set-Cookie: session\_tracker=fkhkennfcgkhedcbrd.0.1640293784036.Z0FBQUFBQmh4T1dZXzZCYzVSamxxTHpWcVNTZXV3cWhNVWZWS180NWxrMGVKa0NfUmx3Sm9FZ29sOG1zOEowaFlWdHBFdGwxNkMxaUdVYUFHaXJtTTFjQ2k5UnNIbTlvQ05ZYmg5dTgteGJQLUFCUFl4RXFqM1FpQVlIU2p4MUJvN2I5anNVZVFzWEg; path=/; domain=.reddit.com; secure; SameSite=None; Secure

Set-Cookie: token\_v2=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2NDAyOTcyNjMsInN1YiI6Ii0tX1Y2QjVYTlJPUENsVXFSclAxYkFOUlVBZm9BZlEiLCJsb2dnZWRJbiI6ZmFsc2UsInNjb3BlcyI6WyIqIiwiZW1haWwiLCJwaWkiXX0.EKBVN6zPmD9YC79Jl2nsBQoTqs6uj083K-JhANBlQfA; Path=/; Domain=reddit.com; Expires=Sat, 23 Dec 2023 21:09:43 GMT; HttpOnly; Secure

Set-Cookie: csv=2; Max-Age=63072000; Domain=.reddit.com; Path=/; Secure; SameSite=None

Set-Cookie: edgebucket=fvuLbcyzGg0eU97ZU4; Domain=reddit.com; Max-Age=63071999; Path=/; secure

Strict-Transport-Security: max-age=31536000; includeSubdomains

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

X-XSS-Protection: 1; mode=block

Server: snooserv

X-Clacks-Overhead: GNU Terry Pratchett

**1.3**

It is used to specify browser caching policies such as how and where a resource is cached and how long it is valid. In this case, the resource is must constantly be resent (“cache-control: max-age=0, must-revalidate”).

**1.4**

We learn it supports gzip, enflate and br (“Accept-Encoding: gzip, deflate, br”) by looking at the request header.

Task 2

**2.1**

It does not allow the creation of the resource.

Trying 52.5.64.83...

Connected to httpbin.org.

Escape character is '^]'.

HTTP/1.1 404 NOT FOUND

Date: Thu, 23 Dec 2021 22:07:47 GMT

Content-Type: text/html

Content-Length: 233

Connection: keep-alive

Server: gunicorn/19.9.0

Access-Control-Allow-Origin: \*

Access-Control-Allow-Credentials: true

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<title>404 Not Found</title>

<h1>Not Found</h1>

<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>

**2.2 ?**

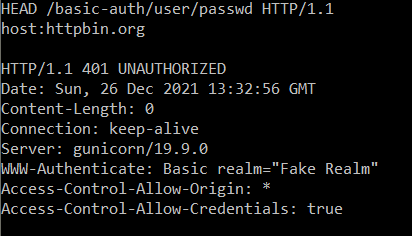
If it is smaller, we get a 400 Bad Request message and if it is larger, we don’t get a response until we input the number of characters we gave as the Content-length.

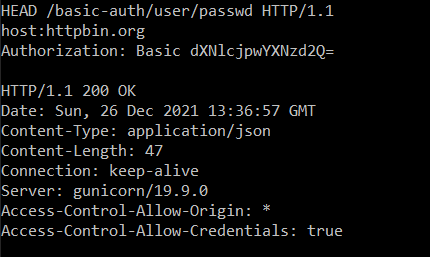
Task 3

**3.1 ?**

I don’t have to re-enter the username and password because the browser uses the same connection even when I refresh the page (it doesn’t close the connection).

**3.2 ?** I receive status code 401.

****

****

If i close the connection and start a new one I get status code 401. It isn’t the same behaviour as in the browser because the browser doesn’t close the connection, but I did.

Task 4