TP 05

1 Protocole HTTP

- Le port du protocol `HTTP` est le port `80` (notez que pour le `https` le port est le 443).

1.1 Méthode `HEAD`

- Pour chaque domaine vous trouverez ci-dessous sur quelle machine est implanté le serveur, quel est le type de ce serveur et quelle est la classe de réponse :
    - Pour www.emi.u-bordeaux.fr :
        - Avec la commande `telnet www.emi.u-bordeaux.fr 80` et la requête suivante :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.emi.u-bordeaux.fr
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Mar 2020 13:50:36 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Tue, 18 Jun 2019 14:49:52 GMT
ETag: "bf8b8-2467-58b9a39b56818"
Accept-Ranges: bytes
Content-Length: 9319
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

Connection closed by foreign host.
```

        - Machine où est implantée le serveur : `Linux` avec la distrbution `Debian`.
        - Type du serveur : `Apache 2.2.22`.
        - Classe de réponse : `2xx successful` car le code http est 200.

- Pour www.labri.fr :
  - Avec la commande `telnet www.labri.fr 80` et la requête suivante :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.labri.fr
```

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 30 Mar 2020 13:56:20 GMT
Server: Apache
Location: https:///error/HTTP_BAD_REQUEST.html.var
Content-Length: 248
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```

  - Machine où est implantée le serveur : `Linux`.
  - Type du serveur : `Apache`.
  - Classe de réponse : `3xx redirection` car le code http est 301.
- Pour www.archlinux.org :
  - Avec la commande `telnet www.archlinux.org 80` et la requête suivante :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.archlinux.org
```

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.16.1
Date: Mon, 30 Mar 2020 14:12:19 GMT
Content-Type: text/html
Content-Length: 169
Connection: close
Location: https://www.archlinux.org/

Connection closed by foreign host.
```

- Machine où est implantée le serveur : `Linux` certainement la distribution `Archlinux`.
- Type du serveur : `nginx 1.16.1`.
- Classe de réponse : `3xx redirection` car le code http est 301.

- Pour www.perdu.com :
  - Avec la commande `telnet www.perdu.com 80` et la requête suivante :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.perdu.com
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Mar 2020 14:13:13 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Last-Modified: Thu, 02 Jun 2016 06:01:08 GMT
ETag: "cc-5344555136fe9"
Accept-Ranges: bytes
Content-Length: 204
Cache-Control: max-age=600
Expires: Mon, 30 Mar 2020 14:23:13 GMT
Vary: Accept-Encoding,User-Agent
Content-Type: text/html

Connection closed by foreign host.
```

  - Machine où est implantée le serveur : `Linux`.
  - Type du serveur : `Apache`.
  - Classe de réponse : `2xx successful` car le code http est 200.

1.2 Classes de réponse

- Succès :
  - Avec la commande `telnet magicorp.fr 80` et la requête ci-dessous j'obtiens la classe 2xx :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.magicorp.fr
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 5794
ETag: W/"16a2-N5Oz8uDz1wPbVVbe+/Rgn3yCBVQ"
set-cookie:
connect.sid=s%3Al_XQq3Wa4yFwxM_l6kfyo4gSAgbfxbjx.o3k4wEh3JxfJNXUO5YNs
9H5ul3Ler3Gn3yZWJ4My2o8; Domain=.magicorp.fr; Path=/; HttpOnly
Date: Mon, 30 Mar 2020 14:50:31 GMT
Connection: close

Connection closed by foreign host.
```

- Erreur client :
  - Avec la commande `telnet magicorp.fr 80` et la requête ci-dessous j'obtiens la classe 4xx :

```
HEAD /toto HTTP/1.0
User-Agent: telnet
Host: www.magicorp.fr
```

```
HTTP/1.1 404 Not Found
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 10
ETag: W/"a-/8nFET8AoFHgR39QmkbW0gX342M"
set-cookie:
connect.sid=s%3A0EDklZbF30HAHBRW9tDM4MXA3kso_ewL.13yaI3Drqy26dNrt%2F4S1O7r
6KOOLnMwQaIeZVJ%2Bwvs4; Domain=.magicorp.fr; Path=/; HttpOnly
Date: Mon, 30 Mar 2020 14:56:07 GMT
Connection: close

Connection closed by foreign host.
```

- Inchangé :
  - Avec la commande `telnet www.perdu.com 80` et la requête ci-dessous j'obtiens la classe 3xx :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: www.perdu.com
If-Modified-Since: Thu, 02 Jun 2016 06:01:08 GMT
```

```
HTTP/1.1 304 Not Modified
Date: Mon, 30 Mar 2020 15:10:26 GMT
Server: Apache
Connection: Upgrade, close
ETag: "cc-5344555136fe9"
Expires: Mon, 30 Mar 2020 15:20:26 GMT
Cache-Control: max-age=600
Vary: User-Agent,Accept-Encoding

Connection closed by foreign host.
```

- Redirection :
  - Avec la commande `telnet magicorp.fr 80` et la requête ci-dessous j'obtiens la classe 3xx :

```
HEAD / HTTP/1.0
User-Agent: telnet
Host: magicorp.fr
```

```
HTTP/1.1 307 Temporary Redirect
X-Powered-By: Express
Location: http://www.magicorp.fr/
Vary: Accept
Content-Type: text/plain; charset=utf-8
Content-Length: 58
set-cookie:
connect.sid=s%3At2x6B5QMQEj3H5PaFFY0KJbkICXNI_d5.OIeAwZwM3JPvXMxYtLCC
RheTPqvPcfi8qt6LCVic7SU; Domain=.magicorp.fr; Path=/; HttpOnly
Date: Mon, 30 Mar 2020 15:04:40 GMT
Connection: close

Connection closed by foreign host.
```

ça nous redirige car la réponse a pour code http "301 Moved Permanently".

1.3 Méthode `GET` simple et entêtes

Avec la commande `telnet bruno.pinaud.emi.u-bordeaux.fr 80` et la requête suivante :

```
GET /test-redir HTTP/1.0
User-Agent: telnet
Host: bruno.pinaud.emi.u-bordeaux.fr
```

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 30 Mar 2020 15:34:44 GMT
Server: Apache
Location: http://www.u-bordeaux.fr
Content-Length: 232
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://www.u-bordeaux.fr">here</a>.</p>
</body></html>
Connection closed by foreign host.
```

Avec la commande `wget --server-response http://bruno.pinaud.emi.u-bordeaux.fr/test-redir` :

```
--2020-03-30 17:32:32--  http://bruno.pinaud.emi.u-bordeaux.fr/test-redir
Resolving bruno.pinaud.emi.u-bordeaux.fr (bruno.pinaud.emi.u-bordeaux.fr)...
147.210.12.220, 2001:660:6101:800:252::9
Connecting to bruno.pinaud.emi.u-bordeaux.fr (bruno.pinaud.emi.u-
bordeaux.fr)|147.210.12.220|:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 301 Moved Permanently
  Date: Mon, 30 Mar 2020 15:32:32 GMT
  Server: Apache
  Location: http://www.u-bordeaux.fr
  Content-Length: 232
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1
Location: http://www.u-bordeaux.fr [following]
--2020-03-30 17:32:32--  http://www.u-bordeaux.fr/
Resolving www.u-bordeaux.fr (www.u-bordeaux.fr)... 147.210.215.26
Connecting to www.u-bordeaux.fr (www.u-bordeaux.fr)|147.210.215.26|:80...
connected.
HTTP request sent, awaiting response...
  HTTP/1.0 302 Found
  Location: https://www.u-bordeaux.fr/
  Content-Type: text/html
  Content-Length: 170
Location: https://www.u-bordeaux.fr/ [following]
--2020-03-30 17:32:32--  https://www.u-bordeaux.fr/
Connecting to www.u-bordeaux.fr (www.u-bordeaux.fr)|147.210.215.26|:443...
connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Server: Apache/2.2.22 (Debian)
  X-Powered-By: PHP/5.4.35-0+deb7u2
  Cache-Control: public, s-maxage=60, max-age=40
  vary: X-User-Hash,Accept-Encoding
  x-location-id: 527
  x-content-digest: ezlocation/527/ena4df4c31ff1a754225f5d10fa56a647d4f2da2df
  Expires: Mon, 30 Mar 2020 15:08:51 GMT
  Content-Language: fr
  Content-Type: text/html; charset=UTF-8
  Transfer-Encoding: chunked
  Date: Mon, 30 Mar 2020 15:32:33 GMT
  X-Varnish: 1721732874 1721689436
  Age: 1462
  Via: 1.1 varnish
  Connection: keep-alive
  X-Cache: HIT
  X-Cache-Hits: 258
Length: unspecified [text/html]
Saving to: ‘test-redir’
```

```
test-redir       [   <=>                                 ] 166,90K   369KB/s
in 0,5s

2020-03-30 17:32:33 (369 KB/s) - ‘test-redir’ saved [170909]
```

- Dans un premier temps avec le client Chrome ou wget on obtient la même chose qu'avec le client telnet mais le client Chrome ou wget effectue la redirection automatiquement et fait les requêtes suivantes.

1.4 Méthode `GET` avec ou sans `Host:`

- Lorsque je fait cette commande `telnet bruno.pinaud.emi.u-bordeaux.fr 80` avec la requête `GET / HTTP/1.0\n\n` je n'obtiens pas la même page que dans le navigateur. La cause de cette différence est du au fait qu'il y a un seul serveur qui s'occupe des requêtes à destination des hosts `<prenom>.<nom>.emi.u-bordeaux.fr` ce qui a pour effet, si on ne précise pas le champ `Host:...`, de nous rediriger sur la page par défaut. Dans le navigateur le champ `Host:...` est complété automatiquement ce qui fait que le serveur permet l'accès aux ressources de l'host `bruno.pinaud.emi.u-bordeaux.fr`. Pour en arriver à cette conclusion j'ai effectué la commande `telnet` avec l'host `charles.goedefroit.emi.u-bordeaux.fr` ce qui m'a donné la même page.

> Avec la commande `telnet`

```
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 30 Mar 2020 15:51:09 GMT
Server: Apache
Last-Modified: Thu, 03 Feb 2011 14:29:55 GMT
ETag: "1f55-49b61996c7ec0"
Accept-Ranges: bytes
Content-Length: 8021
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
[...]
```

1.5 HTTP + SSL = HTTPS

Je teste la commande `openssl s_client -crlf -connect home.magicorp.fr:https` avec la requête `http` suivante :

```
GET / HTTP/1.0
User-Agent: openssl
Host: home.magicorp.fr
```

Si je teste sur mon site `home.magicorp.fr` en `https` j'obtiens l'échange ci-dessous (notez que la réponse me redirige vers la page login) :

```
CONNECTED(00000005)
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = home.magicorp.fr
verify return:1
---
Certificate chain
 0 s:CN = home.magicorp.fr
   i:C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
 1 s:C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
   i:O = Digital Signature Trust Co., CN = DST Root CA X3
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFfjCCBGagAwIBAgISBMftMDMkEcgnDjhAfS98R2waMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIQYDVQQD
ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSBYMzAeFw0yMDA0MDgxMTA1MTlaFw0y
MDA3MDcxMTA1MTlaMBsxGTAXBgNVBAMTEGhvbWUubWFnaWNvcnAuZnIwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQD0qC7GpySYddvO1flQMeWMgjEkWv/N
KetlYMnygViH/LTSkwCbaDLA5rbUuNX0yobeUJzdjEnEEB5GfDRzKLIHR0/rkcCm
wbfAE/BolZC4gbZedygiAQ2N4XXozkiMGehZXpVSeu10OWlC2AsA9kJZjbS8M79k
yZZIAJzOYeW16ZdWE5NlXVUeyRN/3T9NHSoMSzWClSMA407gWuK/3pJGhfkGJe0O
cc/NGqyhTLE1TgU5ttvGXkMwbHh6zYqnK94gY5H5CKp7Oo6734Sa66Qni/Z9ViAZ
exRSfpxk/MOZcc+BZtp0bSpHOHzqPpRj8k2w/aZDl+I4m5WHCDdd1IlpAgMBAAGj
ggKLMIIChzAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFNm5e5/SR73n0FsTfbji9O+o
DCjjMB8GA1UdIwQYMBaAFKhKamMEfd265tE5t6ZFZe/zqOyhMG8GCCsGAQUFBwEB
BGMwYTAuBggrBgEFBQcwAYYiaHR0cDovL29jc3AuaW50LXgzLmxldHNlbmNyeXB0
Lm9yZzAvBggrBgEFBQcwAoYjaHR0cDovL2NlcnQuaW50LXgzLmxldHNlbmNyeXB0
Lm9yZy8wQQYDVR0RBDowOIIQaG9tZS5tYWdpY29ycC5mcoISb2N0YXZlLm1hZ2lj
b3JwLmZyghB0bzBhLm1hZ2ljb3JwLmZyMEwGA1UdIARFMEMwCAYGZ4EMAQIBMDcG
CysGAQQBgt8TAQEBMCgwJgYIKwYBBQUHAgEWGmh0dHA6Ly9jcHMubGV0c2VuY3J5
cHQub3JnMIIBBAYKKwYBBAHWeQIEAgSB9QSB8gDwAHYA5xLysDd+GmL7jskMYYTx
6ns3y1YdESZb8+DzS/JBVG4AAAFxWa4wTwAABAMARzBFAiEAsN2XWlmf0a/towfx
BfNXX0d5+woJHn3Bafsn61iev4UCIDx0/rXNEtqRat8hJnC62OAWKoZE/fvNIE38
vL/4OAHfAHYAsh4FzIuizYogTodm+Su5iiUgZ2va+nDnsklTLe+LkF4AAAFxWa4w
UAAABAMARzBFAiAiZY8YORslS7L6YGNBEb0649i9a2qpic/kP2MhwExFRwIhAMfP
CJCQuZziTkmT4xwnzB/XNJwXUdZoQOXeOXTh93+vMA0GCSqGSIb3DQEBCwUAA4IB
AQCcl3uKLwgiPGKFtAcqhD+5Ous8e05L/BLOZHuJ3AXum3RtUzOpTcbkmiDx6rBP
AtmQ4sCQaRlbtdyQuMmZwK/9Asxt8HoZFQHCRszgNLy5ycGrWO7+Ly5SV23MOutD
2klIElM6jTX8R6F+PM5HOwLmdgxrXpm504gJfUIW1abmHAHPZ2Gm8COY6hYPtOgs
wtU9bjj2YBGFYR+hePZfI71j9EuOtdD5zO7TfUB4foDFCCdI6UBdauVs+s3mmErO
B2qcvpIG0mYN6FMhPH8Mb8kixwAoB4iIWsR1hFiyxGWNnzgjgjdeYdqyVzlvqZ0c
w3lTOaSjhKD0oZfI24FikvAh
-----END CERTIFICATE-----
subject=CN = home.magicorp.fr
```

```
issuer=C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 3293 bytes and written 444 bytes
Verification: OK
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
25A6A0D88E300869A6409EC247CCD3FAE2330913733FDCCC8A48466855089FF3
    Session-ID-ctx:
    Master-Key:
CB6F8F0340093B53C3BEF5A154F9CC1CBE3EBB1E645700FB059696647AE9A419BFB3C26ACAB91E4
6B07EE6853A12393C
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - d4 8f be 00 c9 fe 5e 29-0b 40 83 57 87 f1 8f 9c   ......^).@.W....
    0010 - 6c c8 01 64 82 06 f9 15-8c f5 cd 52 f5 70 9c cc   l..d.......R.p..
    0020 - 66 44 a4 e6 86 59 d5 c2-5d eb 3d e6 38 7a 13 07   fD...Y..].=.8z..
    0030 - 14 c8 10 81 3a 70 f3 d9-81 9a dd 81 81 f4 e1 79   ....:p.........y
    0040 - 84 13 67 ae 8c f2 b9 32-5a 94 ef cd 31 10 ee cf   ..g....2Z...1...
    0050 - cf de 24 97 ba 04 02 04-b7 90 bb 31 30 32 27 7e   ..$........102'~
    0060 - 39 50 7e bd 08 e6 b8 b4-e1 b7 18 09 18 47 5e 83   9P~..........G^.
    0070 - 3b fc 81 e4 37 01 cc 5b-5b 8b ca eb de b0 52 68   ;...7..[[.....Rh
    0080 - 1b c4 65 1d fc 42 65 fd-9c 17 d3 f0 73 79 62 f7   ..e..Be.....syb.
    0090 - 0e e7 04 07 67 ae 95 f5-27 e2 a0 5f b1 ab c7 63   ....g...'._...c
    00a0 - 32 ea 52 eb fd 28 b5 6b-7a 52 71 e3 38 fa 99 e3   2.R..(.kzRq.8...
    00b0 - f4 c2 c5 d2 d5 f1 95 0b-06 d9 bb 9c e0 60 55 b5   .............`U.
    00c0 - 08 25 ef 80 18 04 9d 40-7a 18 52 a5 17 70 96 b9   .%.....@z.R..p..

    Start Time: 1586421747
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
---
GET / HTTP/1.0
User-Agent: openssl
Host: home.magicorp.fr
```

```
HTTP/1.0 302 Found
Date: Thu, 09 Apr 2020 08:42:28 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=j7f110fii6b78t6rp1ssohbibe; path=/; secure; HttpOnly;
SameSite=lax
Cache-Control: max-age=0, must-revalidate, private
Location: https://home.magicorp.fr/login
pragma: no-cache
expires: -1
Content-Length: 364
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh"
content="0;url=https://home.magicorp.fr/login" />

        <title>Redirecting to https://home.magicorp.fr/login</title>
    </head>
    <body>
        Redirecting to <a
href="https://home.magicorp.fr/login">https://home.magicorp.fr/login</a>.
    </body>
</html>closed
```

2 Vos traces

- Ma machine n'a pas été identifiée. Seul mon fournisseur d'accès Internet (FAI), l'adresse ip du routeur (Adresse ip publique) et le noeud réseau rattaché. La localité n'est pas bonne et le nom d'hote est remplacé par l'adresse ip car il n'est pas disponible
    - ADRESSE IP LOCALE : …
    - ADRESSE IP PUBLIQUE : 37.167.199.127
    - NOM D'HÔTE : 37.167.199.127
    - FAI FREEM
    - NŒUD RÉSEAU RATTACHÉ : AS51207 Free Mobile SAS
    - LOCALITÉ : Ville Vic-Fezensac Région Occitanie Pays France

3 Cookies et formulaires

Pour Google Chrome le fichier `Cookies` se trouve à cette adresse `~/.config/google-chrome/Profile 1/Cookies`.

Lorsque je soumets le formulaire, le serveur me répond avec ces deux lignes dans l'entete de la réponse :

```
Set-Cookie: nom=charles; expires=Sun, 12-Apr-2020 13:30:16 GMT; Max-Age=60
Set-Cookie: fruit=bannane; expires=Sun, 12-Apr-2020 13:30:16 GMT; Max-Age=60
```

Dans la base de données sqlite je constate que les cookies expirent au bout de 60 secondes. De plus on voit aussi que les cookies sont enregistrés en temps universel (UTC).

> Toutes les questions suivantes sont faites dans le dossier `src`

4 Les langages du world wide web

4.1 Une page statique

4.1.1 En-tête et métadonnées

4.1.2 Structure du document

4.2 Un coup de peinture

4.2.1 Inclusion de CSS

4.2.2 Mise en pratique

4.2.3 Bonus

4.3 Contenu dynamique, côté client

4.3.1 Masquage de contenu

4.3.2 Bonus : Un coup de peinture, phase II

4.4 Contenu dynamique, côté serveur

4.4.1 Fortune PHP