TP 2 HTTPS CONNEXION

Esteban Becker

05/05/2023

1 Vérification du serveur http

Dans le code nous avons modifié la ligne suivante :

```
1    # definir le message secret
2    SECRET_MESSAGE = "Je_suis_un_super_mot_de_passe" # A modifier
3    app = Flask(__name__)
```

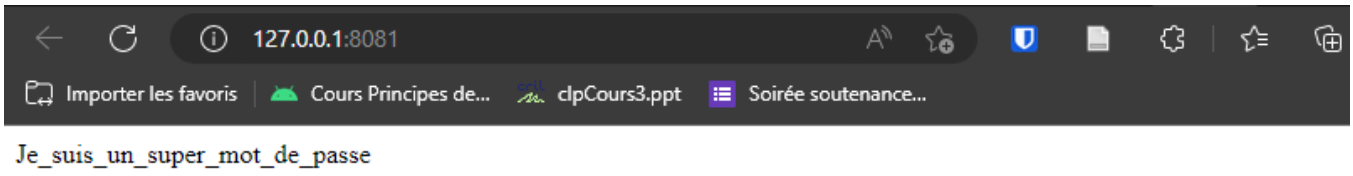

FIGURE 1 – Capture d'écran du Navigateur

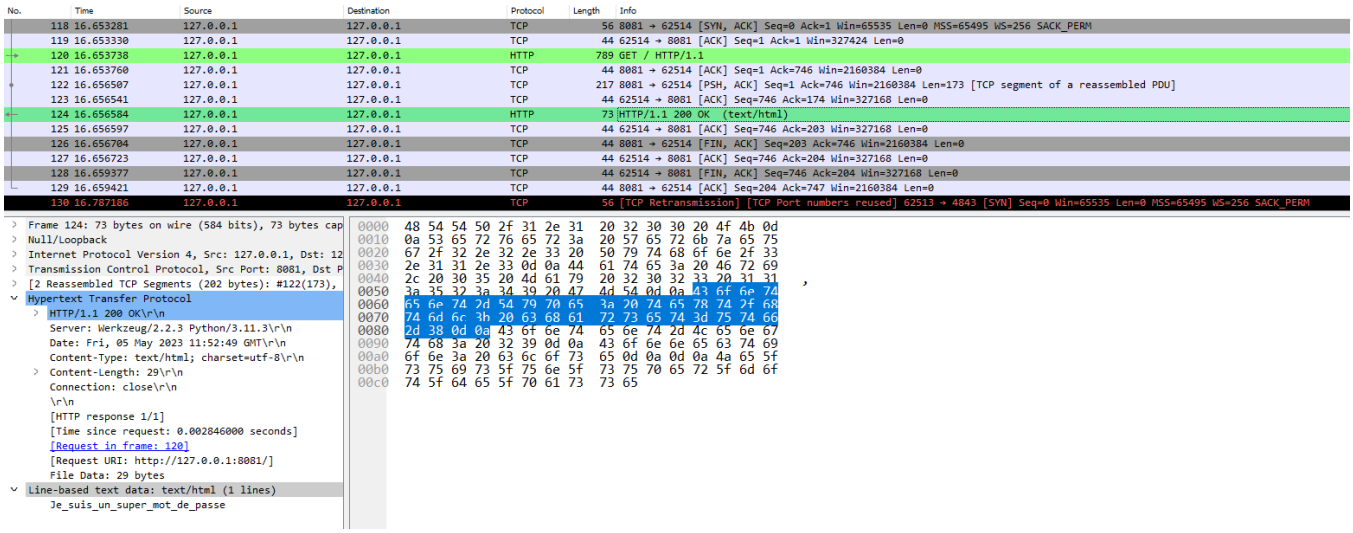

FIGURE 2 – Capture d'écran de Wireshark

Ainsi dans a capture Wireshark nous avons sélectionné l'interface du réseau local de la machine, une fois la capture lancé, nous recherchons les emplacements où le protocole utilisé est HTTP. Deux paquets sont alors détectés. Il y a le paquet get, qui est celui de demande de la page, ensuite, il y a le paquet de réponse. Dans la réponse on peut voir que le mot de passe est en clair, ce qui est une faille de sécurité. Le mot de passe est dans la requête hexadécimale à droite, mais dans le panel de gauche, Wireshark nous donne la traduction en ASCII, ce qui correspond au mot de passe défini dans le code python.

2 Génération du certificat de l'autorité de certification

Afin de faire fonctionner le code, il a fallu mettre les bons paramètres dans chaque fonction.
Pour le certificat, les paramètres sont les suivants :

```
1
2     CA_PASSWORD = "XsFa$qN2H9bq^&Y@osMdR5Nqn6T2oDghC&Zij*xgSzXW!7m*
      hYDToVZukWFKVsaZo9hjSaprUftufpimcSdvhg2k!BwcZp5E4LjGoFEe$QHkLv65ozk*MGee8#BFfsHL"
3     CA_CONFIGURATION = Configuration("FR", "Territoire de Belfort", "Belfort", "
      EstebanBecker_CA", "localhost")
```

Le mot de passe a été généré en utilisant un générateur aléatoire de mots de passes.
La clé publique est la suivante :

```
PS C:\Users\esteb\OneDrive - Universite De Technologie De Belfort-Montbeliard\Cours\UTBM\INFO02\RS40\https_connexion> &
C:/Users/esteb/miniconda3/envs/myenv/python.exe "c:/Users/esteb/OneDrive - Universite De Technologie De Belfort-Montbeli
ard/Cours/UTBM/INFO02/RS40/https_connexion/build.py"
CA public key :
[<Certificate(PEM string with SHA-1 digest '114a96a6ef20c02a922c39ff0a851d5ba6adf34a')>]
file content :
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIUIB30hfwmJIIDX2w0BNB1YWBhm5owDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCRlIxHjAcBgNVBAgMFVRlcnJpdG9pcmUgZGUgQmVsZm9y
dDEQMA4GA1UEBwwHQmVsZm9ydDEZMBcGA1UECgwQRXN0ZWJhbkJlY2tlcl9DQTES
MBAGA1UEAwwJbG9jYWxob3N0MB4XDTIzMDUwNTEzMTAyOFoXDTIzMDcwNDEzMTAy
OFowbjELMAkGA1UEBhMCRlIxHjAcBgNVBAgMFVRlcnJpdG9pcmUgZGUgQmVsZm9y
dDEQMA4GA1UEBwwHQmVsZm9ydDEZMBcGA1UECgwQRXN0ZWJhbkJlY2tlcl9DQTES
MBAGA1UEAwwJbG9jYWxob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAz7q9NbvFOzVT8TqUdRtTO6lICQAdgyZ3zcY14h2VB9l82WEQSh7crs4S004R
fxbtRscqdbrBDfI85TaypQIZ9pqhWJB/mtmeetRNdOefW3xIYk+yaDLiPgLS3MHX
vF/42YOZx3ZQxelWvgbfmwf2dk9gqSzawpwPJbX10BkEMppWH4wF80FN7W+/ojMs
wctUlUDelELo3/sjZ+VJH3Vi4Il5xR1ckyFsjmMSWVwWdIrbCHHvTp/DfS5tBFr5
TZem9c77WzA3d2+g8nT+HDUEJ0uo+dN84l+YiZUwB3q+arOGxniScaPObtb4MADt
pQS5/ciXlovwIASLusUym/daMQIDAQABoxMwETAPBgNVHRMBAf8EBTADAQH/MA0G
CSqGSIb3DQEBCwUAA4IBAQCM67UyFoK6pmfmqkv2FC/TdIaD5t3Mf9fnN+GSrvNx
1KqG6MXoZhk8hsAmieqTd0a59LvXWIWr/mmyEp3F6u2iKjaTalCtCnVTzaBFj9Gb
ijfBDO9sweIHT2ebiAdAp9yvzYzqfH09r4YJEawKk4SWDtk/gGxeIB0oivOXWz6T
jm55X1usLs6cZsocQaqWI3FrTrFwBh4VyQN7S9e8uEh6rwCAaaoYFB8ZhkhiG68S
Y5aq7/eEGihKyOeLoqIhy6pLSL85RPEFQRV+iSbWggNgxK0pQBrxnurXFW7YJN4v
0RB0OuVWA6icrsjp/tRiYw8XRTYc4ijtpXliK6cisjap
-----END CERTIFICATE-----

finished ...
```

FIGURE 3 – Capture d'écran de Wireshark

En déchiffrant la clé publique avec la ligne suivante :

```
1     cert = x509.load_pem_x509_certificate(pem_data[0].as_bytes(), default_backend())
```

On obtient les informations suivantes :

```
PS C:\Users\esteb\OneDrive - Universite De Technologie De Belfort-Montbeliard\Cours\UTBM\INFO02\RS40\https_connexion> & C:/Users/esteb/miniconda3/envs/myenv/pyt
hon.exe "c:/Users/esteb/OneDrive - Universite De Technologie De Belfort-Montbeliard/Cours/UTBM/INFO02/RS40/https_connexion/build.py"
CA public key :
<Name(C=FR,ST=Territoire de Belfort,L=Belfort,O=EstebanBecker CA,CN=localhost)>
```

FIGURE 4 – Certificat déchiffré