

TP 2 HTTPS CONNEXION

Esteban Becker

05/05/2023

1 Vérification du serveur http

Dans le code nous avons modifié la ligne suivante :

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

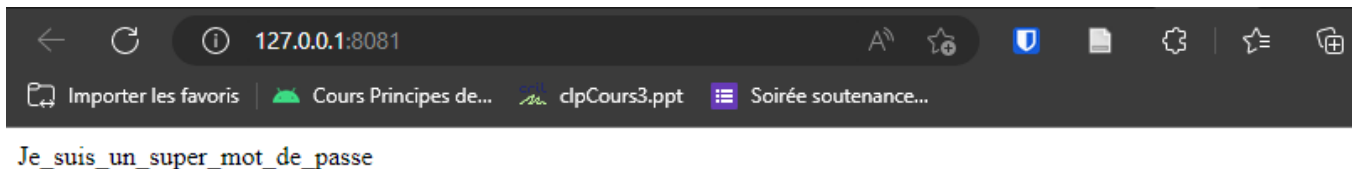


FIGURE 1 – Capture d'écran du Navigateur

No.	Time	Source	Destination	Protocol	Length	Info
118	16.653281	127.0.0.1	127.0.0.1	TCP	56	8081 → 62514 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
119	16.653330	127.0.0.1	127.0.0.1	TCP	44	62514 → 8081 [ACK] Seq=1 Ack=1 Win=327424 Len=0
120	16.653738	127.0.0.1	127.0.0.1	HTTP	789	GET / HTTP/1.1
121	16.653760	127.0.0.1	127.0.0.1	TCP	44	8081 → 62514 [ACK] Seq=1 Ack=746 Win=2160384 Len=0
122	16.656507	127.0.0.1	127.0.0.1	TCP	217	8081 → 62514 [PSH, ACK] Seq=1 Ack=746 Win=2160384 Len=173 [TCP segment of a reassembled PDU]
123	16.656541	127.0.0.1	127.0.0.1	TCP	44	62514 → 8081 [ACK] Seq=746 Ack=174 Win=327168 Len=0
124	16.656584	127.0.0.1	127.0.0.1	HTTP	73	HTTP/1.1 200 OK (text/html)
125	16.656597	127.0.0.1	127.0.0.1	TCP	44	62514 → 8081 [ACK] Seq=746 Ack=203 Win=327168 Len=0
126	16.656704	127.0.0.1	127.0.0.1	TCP	44	8081 → 62514 [FIN, ACK] Seq=203 Ack=746 Win=2160384 Len=0
127	16.656723	127.0.0.1	127.0.0.1	TCP	44	62514 → 8081 [ACK] Seq=746 Ack=204 Win=327168 Len=0
128	16.659377	127.0.0.1	127.0.0.1	TCP	44	62514 → 8081 [FIN, ACK] Seq=746 Ack=204 Win=327168 Len=0
129	16.659421	127.0.0.1	127.0.0.1	TCP	44	8081 → 62514 [ACK] Seq=204 Ack=747 Win=2160384 Len=0
130	16.787106	127.0.0.1	127.0.0.1	TCP	56	[TCP Retransmission] [TCP Port numbers reused] 62513 → 4843 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM

> Frame 124: 73 bytes on wire (584 bits), 73 bytes captured

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 8081, Dst Port: 62514, Seq: 746, Ack: 203, Win: 327168, Len: 0

> [2 Reassembled TCP Segments (202 bytes): #122(173), #123(29)]

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK

> Server: Werkzeug/2.2.3 Python/3.11.3

> Date: Fri, 05 May 2023 11:52:49 GMT

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

> Content-Length: 29

> Connection: close

> [HTTP response 1/1]

> [Time since request: 0.002846000 seconds]

> [Request in frame: 120]

> [Request URI: http://127.0.0.1:8081/]

> File Data: 29 bytes

> Line-based text data: text/html (1 lines)

Je_suis_un_super_mot_de_passe

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 CA_PASSWORD = "XsFa$qN2H9bq~&Y@osMdR5Nqn6T2oDghC&Zij*xgSzXW!7m*  
2 hYDTToVZukWFKVsaZo9hjSaprUftufpimcSdvhg2k!BwcZp5E4LjGoFEe$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/INFORM02/RS40/https_connexion/build.py"  
CA public key :  
[<Certificate(PEM string with SHA-1 digest '114a96a6ef20c02a922c39ff0a851d5ba6adf34a')>]  
file content :  
-----BEGIN CERTIFICATE-----  
MIIDFTCCAmIwAwIBAgIUIB30hfwmJIIDIX2w0BNB1YwBhm5owDQYJKoZIhvcNAQEL  
BQAwbjELMAkGA1UEBhMCRLlXhJAcBgNVBAgMFVRlcnJpdG9pcmlUgZGUGQmVsZm9y  
dDEQMA4GA1UEBmVHQMVsZm9ydDEZMBcGA1UECgwQRXN0ZWJhbGJlY2t1c19DQTES  
MBAGA1UEAwJjbG9jYXRob3N0MB4XDTEzMDUwNTEzMAY0FoXDTIzMDUwNDEzMAY  
OFowbjELMAkGA1UEBhMCRLlXhJAcBgNVBAgMFVRlcnJpdG9pcmlUgZGUGQmVsZm9y  
dDEQMA4GA1UEBmVHQMVsZm9ydDEZMBcGA1UECgwQRXN0ZWJhbGJlY2t1c19DQTES  
MBAGA1UEAwJjbG9jYXRob3N0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC  
AQEAz7q9NbVFOzVT8TqUdRtTO6lICQAdgyZ3zcY14h2VB9182WEQSh7crs4S004R  
fxbtRscqdbRBDfI85TaypQIZ9pqhWJB/mtmeetRNdeFw3xIYk+yaDLiPgLS3MHX  
vF/42YOZx3ZQxe1WVgbfmmwf2dk9gqSzaawpWpJbX10BkEMppWH4wF80FN7W+/oJMs  
wctULUdeLELo3/sjZ+VJH3Vi4I15xR1ckyFsjmMSwWwIdIrbCHHvTp/DfS5tBFr5  
TZem9c77WzA3d2+g8nT+HDUEJ0uo+dN841+YiZUwB3q+arOGxniScaP0btb4MADt  
pQ55/ciXlovwIASLusUym/damQIDAQABoxMwETAPBgNVHRMBAf8EBTADAQH/MA0G  
CSqGSIb3DQEBCwUAA4IBAQCm67UyFok6pmmfmqkv2FC/TdIaD5t3Mf9fnN+GSrvNx  
1KqG6MXoZhk8hsAmieqTd0a59LvXWlwr/mmyEp3F6u2iKjaTalcTcnVTzaBFj9Gb  
ijfBD09sweIHT2ebiAdAp9yvzYzqfH09r4YJEawKk4Swdtk/gGxeIB0oivOXWz6T  
jm55X1usLS6cZsocQaqWI3FrTrFwBh4VvYQN7S9e8uEh6rWCAaaoYFB8Zhkhig68S  
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/python.exe "c:/Users/esteb/OneDrive - Universite De Technologie De Belfort-Montbeliard/Cours/UTBM/INFORM02/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