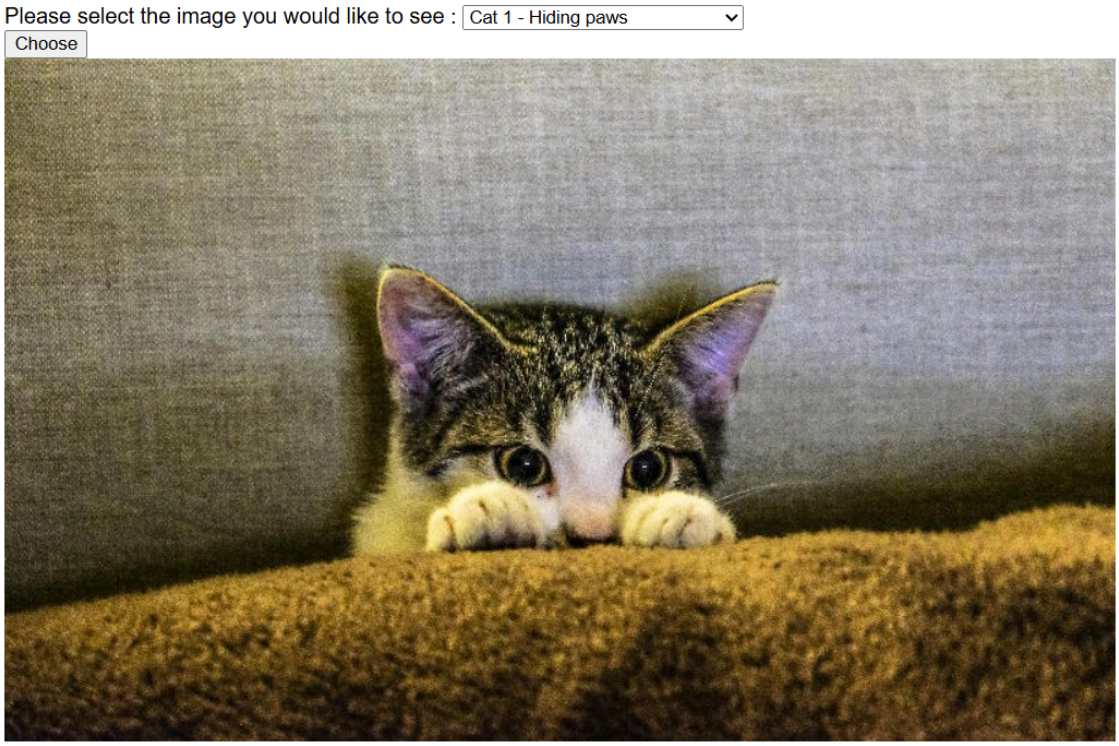
Web - Path Traversal - 125 points

Kévin DUVERGER

Table des matières

1 Résolution Path Traversal :

On peut encore commencer par se connecter au serveur (sur `http://146.59.227.136:23424`) et en appuyant sur `choose` on peut avoir une belle image de chat :



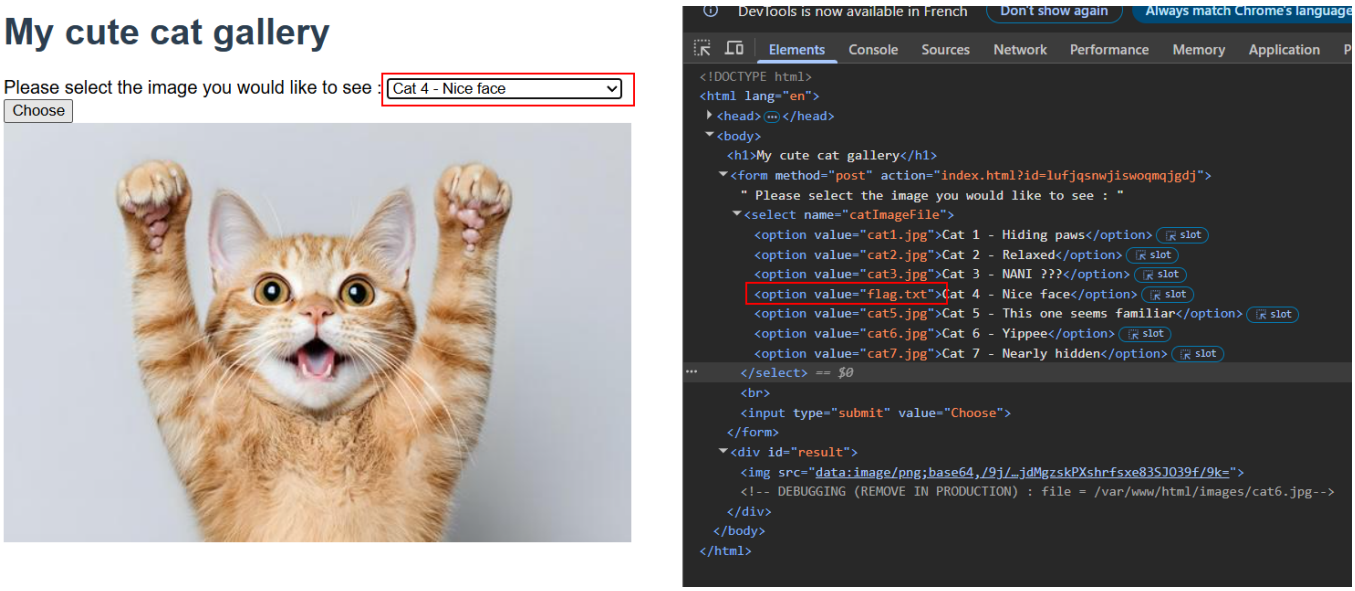
Pour le fun, on peut aller explorer les différentes images sur cette plateforme :

C'est donc une galerie d'images de chats, et nous devons trouver un moyen de le hacker. Encore une fois, une bonne technique est d'aller voir dans le code source ce qu'il se passe :

```
    <input type="submit" value="Choose">
  </form>
 ▼<div id="result"> == $0
    <img src="…jdMgzskPXshrfsxe83SJO39f/9k=">
    <!-- DEBUGGING (REMOVE IN PRODUCTION) : file = /var/www/html/images/cat6.jpg-->
  </div>
</body>
```

Comme on peut le voir, il y a un commentaire de debug qui n'a pas été retiré. Ce dernier combiné avec la structure du `select` juste avant nous indique que le nom du fichier dans `value` est concaténé à `/var/www/html/images/`. En changeant le nom du fichier dans les options, on peut donc potentiellement essayer de se déplacer dans la hiérarchie de fichiers sur le serveur !

La description du challenge nous dit que le fichier à trouver se nomme `flag.txt` et qu'il est sur le serveur web. Une première tentative est donc de tester `flag.txt` ce qui accédera au fichier `/var/www/html/images/flag.txt` :



La solution qui a été choisie est de remplacer l'une des valeurs des options par `flag.txt`, on purra ensuite appuyer sur `choose` avec la bonne sélection. Voici le code base64 de l'image :

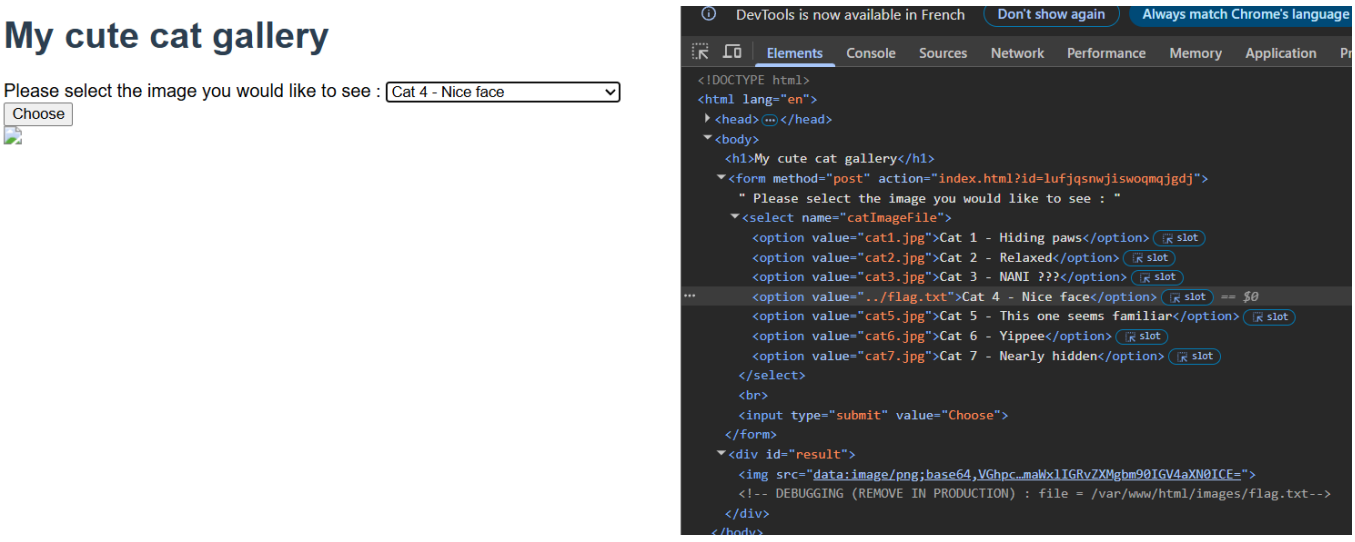
```
VGhpcyBmaWxlIGRvZXMgbm90IGV4aXN0ICE=
```

Ce dernier se décode en :

```
This file does not exist !
```

Ce n'était donc probablement pas le bon endroit.

On peut donc ensuite essayer de remonter un cran dans la hiérarchie, ce que l'on peut obtenir avec `../flag.txt` :



Voici le base64 que l'on obtient cette fois-ci :

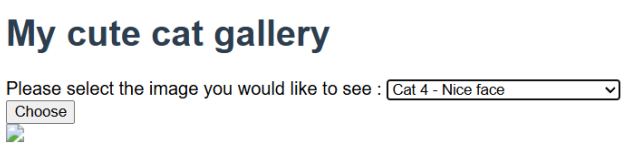
```
WWF5IHlvdSBwYXNzZWQgbGV2ZWwgMSwgeW91IGFyZSBub3cgZm9yYmlkZGVuIGZyb20gdXNpbmcgIi4uIiBvciAiLyIgIQ==
```

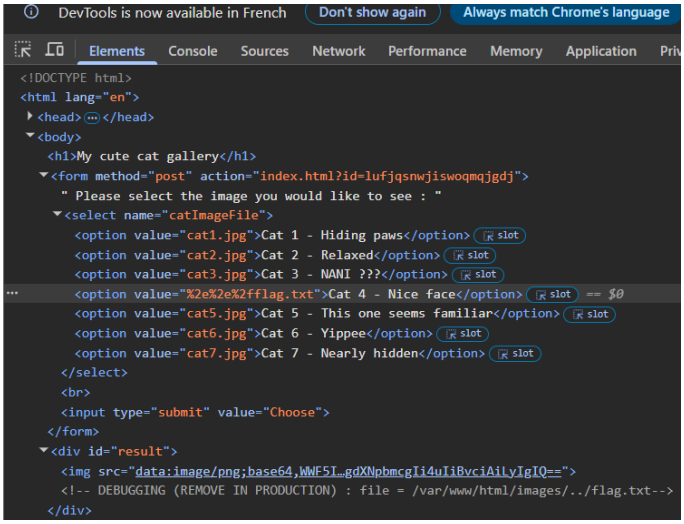
Et voici ce vers quoi il se décode :

```
Yay you passed level 1, you are now forbidden from using ".." or "/" !
```

Nous n'avons donc maintenant plus la possibilité de mettre `..` ou `/` dans le chemin.

La solution consiste à **encoder** l'URL, de cette façon ils n'apparaîtront plus directement dans la requête ! Pour ce faire, on peut remplacer le `.` par `%2e` et le `/` par `%2f` ce qui nous donne :





Voici le base64 que l'on obtient cette fois-ci :

```
WWF5IHlvdSB3b24sIGhlcmUgaXMgdGhlIGZsYWcgOiBjcnlwdGlzQ1RGe3A0dGhfdHI0djNyczRsXzFzX3MwX2Z1bn0=
```

Et voici ce vers quoi il se décode :

```
Yay you won, here is the flag : cryptisCTF{p4th_tr4v3rs4l_1s_s0_fun}
```

Nous avons donc le flag !