Tell Me Your Secret 2

Auteur: bWlrYQ

1. Recon

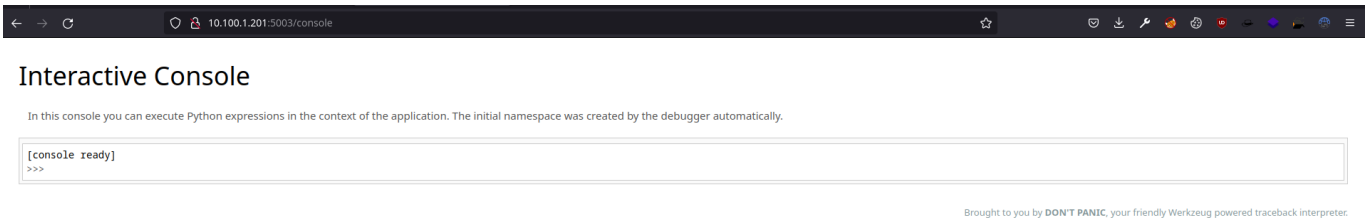
Il semble que le développeur n'ait rien appris, donnons lui une bonne leçon. Cette fois-ci le code source n'est pas à disposition, cela signifie que la faille de signature des cookies a été corrigée, cherchons ailleurs.

```
<!doctype html>
<html lang="en">
    <head>
        <meta charset="utf-8">
            <meta name="viewport" content="width=device-width, initial-scale=1">
            <title>Secret Website</title>
    </head>
    <body>
            <div class="center">
                <h1>Welcome to my super website !</h1>
                <h3>Do you think that you can hack my website once again ? Never !
</h3>
            </div>

            <style>

            .center {
            margin-top: 300px;
            text-align: center;
            }

            </style>
    </body>
</html>
<!-- TODO : Turn off this debug mode for prod -->
```

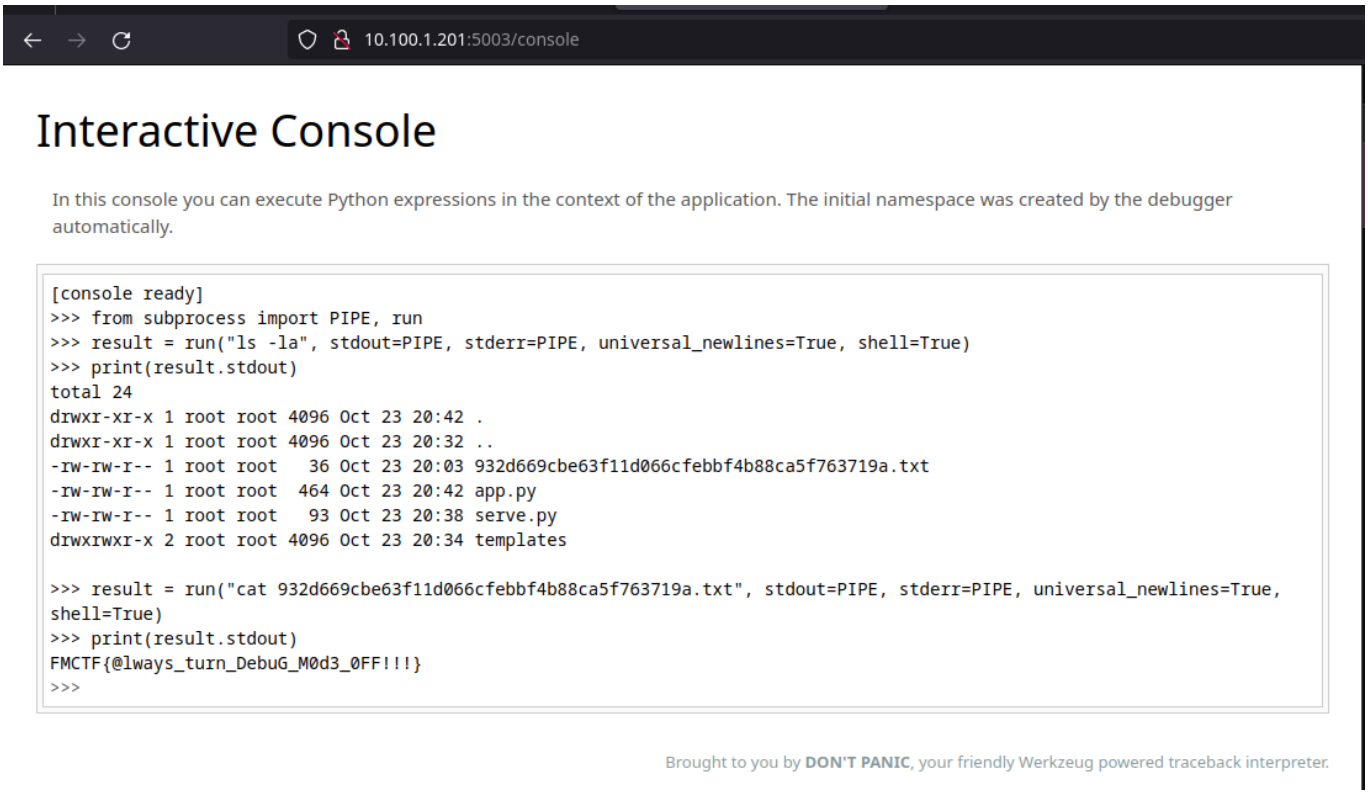
Le code source nous indique qu'il faut éteindre le mode de débug pour pouvoir partir en prod. Grave erreur de la part du développeur tête en l'air. Flask possède un mode de debug accessible via code pin sur l'endpoint `/console`

2. Exploitation

L'endpoint est accessible sans code pin car le développeur a dû le désactiver, si la variable d'environnement `WERKZEUG_DEBUG_PIN=off` est présentee, alors il n'y a pas de pin. Ce qui signifie qu'on peut exécuter des commandes sur l'hôte



On va faire en sorte de lire les fichiers puis le flag.



Flag: FMCTF{@lways_turn_DebuG_M0d3_0FF!!!}